Dubai Electronic Security Center

RFQ 762640: DNS and Data Security and Visibility

Technical Proposal_v1

08th December 2025

Bid Reference: ICTCommercial-21-10-2025- 13205

Subject to content

Your Smart ICT Partner.
Helping you scale up your digital transformation

Confidentiality Statement

Emirates Integrated Telecommunications Company (EITC), PJSC
P.O.Box 502666
Dubai, U.A.E.
Version 1.0

This document contains proprietary and confidential information. All information submitted to the Dubai Electronic Security Center (DESC), Customer, the ("Confidential Information") is provided in strictest confidence for the purposes of the requirement. DESC undertakes that it shall not use or disclose any Confidential Information contained herein except in the context of its business dealings with Emirates Integrated Telecommunications Company, EITC ("du"). DESC undertakes that it shall ensure that all present and future employees, consultants, advisors or contractors of DESC Team shall adhere to confidentiality on the same terms.

DESC shall procure that its employee's consultants, advisors or contractors must not disclose any Confidential Information concerning this document to any other third party except to the extent those matters are generally known to and are available for use by the public or where such third party has, subject to du's consent, signed an appropriate NDA. DESC also agrees not to duplicate or distribute or permit others to duplicate or distribute any Confidential Information (including any material contained herein) without the express written consent of du.

du retains all title, ownership and intellectual property rights in the information, material and trademarks contained herein (unless expressly accredited to a third party, in which case such intellectual property shall remain vested in such third party), including all supporting documentation, contractual templates, files, marketing material and multimedia.

BY ACCEPTING THIS DOCUMENT, DESC AGREES TO BE BOUND BY THE AFOREMENTIONED STATEMENTS.

The proposal set out in this document is strictly subject to contract and further commercial discussion and shall not create any legally binding obligations as between du and DESC Team and is subject to the parties entering into a legally binding agreement, on terms to be negotiated and agreed between the parties.

Table of Content

Confidentiality Statement....1
Table of Content....2
1. Executive Summary....5
1.1 Full Compliance & Exceeding Expectations....5
1.2 Solution Overview – A Unified National Cybersecurity Shield....5
1.3 Unique Value Proposition – Why du....6
2. Response to Instructions....8
3. Statements of Compliance....9
4. Secure DNS and Internet Traffic Monitoring Platform for Dubai Electronic Security Center (DESC) - Roadmap....10
4.1 Key Requirements – as per RFP....10
5. Our Understanding & Objectives of DESC....11
5.1 Proposed Security Monitoring & Observability Blue Print....11
6. Proposed Solution Options & Summary of Deliverables....12
6.1 Summary of Proposed High-Level Solution....13
6.2 Technology Stack....14
7. Bill of Quantity – BoQ....15
7.1 Data Lake....15
7.2 DNS Security....16
7.3 NetScout Packet Broker - Aggregation....17
7.4 Datacenter Networking....18
7.5 Network Security....22
7.6 DELL on Nutanix....24
7.7 FortiSOAR....56
7.8 S3 Storage - Optional....56
7.9 Building AI Automation Stack....59
7.10 Managed Services....69
7.11 VAPT....70

8. Proposed Solution Components.....71
8.1 Solution Architecture [High Level].....71
8.2 Network Architecture [High Level].....72
8.3 Internet and GIN connectivity – per site.....73
8.4 Network Design of Link Termination of 10 Gigs carrying Tapped Traffic from Service Provider. 74
8.5 Network Design for L3 MPLS carrying DNS logs from service providers.....75
8.6 Technical Datasheets.....76
9. Proposed Solution Details.....76
9.1 du Datacentre's Overview.....76
9.2 Security & Observability Platform Development.....79
9.3 Phase 0: Network and Security Infrastructure deployment.....80
9.4 Phase 1: DNS Security Enforcement and Data Ingestion & Phase 2: Internet Traffic Collection, Ingestion of Large Data Sets In Data Lake And Enhanced Analytics Using Internet Oriented Security Use Cases.....89
9.5 Phase 3: Protective DNS Stack Implementation.....138
9.6 Phase 4: Building AI Automation Stack - (ROADMAP).....142
10. Engagement Model: Implementation and Managed Service Transition.....148
10.1 Phase 1: Implementation and Deployment.....149
10.2 Phase 2: Handover to Operations.....149
11. Scope of Work.....149
11.1 Project Initiation and Design.....149
11.2 Phase 0: Network And Security Infrastructure Deployment.....150
11.3 Phase 1: DNS Security Enforcement And Data Ingestion Foundation.....186
11.4 Phase 2: Internet Traffic Collection, Ingestion Of Large Data Sets In Data Lake And Enhanced Analytics Using Internet Oriented Security Use Cases.....191
11.5 Phase 3: Protective DNS Stack Implementation.....196
11.6 Phase 4: Building AI Automation Stack - (ROADMAP).....197
11.7 Operate for 24 Months.....198
11.8 Final Project Ownership Transfer and Exit Fee.....256
12. Hardware Support and Maintenance.....257
13. Project Responsibilities.....257

13.1 Du Responsibilities....257
13.2 Assumptions....258
13.3 DESC Responsibilities....259
13.4 Project Management Approach....261
13.5 Risk Management Approach....262
13.6 Issues Management Approach....263
13.7 Quality Management Approach....265
13.8 Document Management Approach....266
13.9 Project Implementation Timelines....269
13.10 Delivery Lead Times....271
13.11 Project Team Structure....271
13.12 Resource Profiles....272
14. Customer References....273
15. Technical Attachments and Annexures :....277
16. Company Profile....278
16.1 Company Profile EITC (du)....278
16.2 Ownership & Organization Structure....281
16.3 Company General Data....282
16.4 Financial report....283
17. End of Document....284

1. Executive Summary

du, in strategic partnership with best-in-class technology leaders including Cisco, Fortinet, NetScout, Elastic, Infoblox, Nutanix, Dell, Cyware, and its partner GBM, proudly submits this comprehensive and fully compliant technical and commercial proposal in response to the Dubai Electronic Security Center (DESC) Request for Proposal for the design, development, implementation, and operation of a **Secure DNS and Internet Traffic Monitoring & Observability Platform** with geo-redundancy within the Emirate of Dubai.

This proposal delivers a future-proof, sovereign, and fully integrated cybersecurity ecosystem that exceeds every requirement of the RFP while introducing **two carefully curated solution options** for the Data Lake and Protective DNS, enabling DESC to select the optimal combination of performance, innovation, and commercial value.

1.1 Full Compliance & Exceeding Expectations

- 100 % compliance with all technical, operational, regulatory, and contractual requirements, including NCEMA Tier III datacenter standards, data sovereignty within Dubai/UAE, as readiness of compliance such as PDPL, ISR, NIST 800-53, and ISO 27001/22301.
- Complete adherence to the Build-Operate-Transfer (BOT) model with structured knowledge transfer, Emiratization targets, and a risk-free 6-month transition-out.
- All phases (0–3) delivered on schedule with clear milestones, deliverables, and acceptance criteria.
- Geo-redundant deployment across two sovereign du datacenters in separate Emirates, connected via diverse, dedicated dark fibre with <5 ms latency, delivering 99.999 % platform availability.

1.2 Solution Overview – A Unified National Cybersecurity Shield

du proposes a state-of-the-art, multi-layered Security Monitoring & Observability Platform built on four foundational pillars:

1. **Secure & Resilient Infrastructure (Phase 0)**
   Cisco Nexus 9000 fabric with 400G MACsec encryption, Fortinet next-generation firewalls with AI-powered FortiGuard services, NetScout Omnis packet intelligence, and hyper-converged Dell/Nutanix or Cisco/Nutanix compute — all hosted in du's Tier III-certified, concurrently maintainable datacenters.
2. **Centralized Data Lake & Advanced Analytics (Phases 1–2)**
   Choice of Elastic or FortiSIEM as the sovereign data lake, ingesting 14+ TB/day (as per RFP Clarification QnA-4, Line 131-132) of enriched DNS and Internet traffic metadata from both service providers (du & Etisalat) via NetScout Omnis AI Sensors & Streamers. Elastic delivers

superior scale, 1,200+ MITRE ATT&CK detection rules, machine-learning anomaly detection, and tiered storage for 9–18 months retention.

3. **Protective DNS Enforcement (Phase 3)**
   Choice of Infoblox or Efficient IP PDNS stack with 100K QPS capacity per site, Advanced DNS Protection, reputation/behavioural blocking, and seamless DNSTAP log export to the data lake. Traffic redirection executed via binding DESC directive to both service providers.
4. **Phase 4 – Building AI Automation Stack- Road Map**
   Phase 4 proposes developing an AI-driven solution on the existing security data lake to streamline cybersecurity operations. The high-level vision uses Red Hat OpenShift AI, an MLOps platform for building, training, and deploying secure predictive and generative AI models, including sovereign AI. OpenShift AI offers core tools like JupyterLab, RAG, KServe, and vLLM for model building, serving, and monitoring, and it is accelerated by NVIDIA NIM/GPUs. The solution also integrates Elasticsearch Relevance Engine (ESRE), which provides a vector database and hybrid search capabilities crucial for building Generative AI and RAG applications based on semantic relevance. This phase is currently a non-binding roadmap direction requiring further study before implementation.

5. **AI-Driven Operations & Managed Services**
   24-month Operate & Transform engagement by duTech, progressive automation of high-confidence workflows, AI/ML threat hunting uplift, full ITIL governance, and aggressive Emiratization targets culminating in complete operational sovereignty for DESC at handover.

1.3 Unique Value Proposition – Why du

- **National Strategic Partner**: As the UAE's digital transformation enabler (Dubai Pulse, Hassantuk, WIFI UAE, Blockchain PaaS), du brings unmatched local expertise, regulatory influence, and proven ability to orchestrate service provider cooperation.
- **Sovereign, Secure, and Resilient**: All data remains within UAE borders in du's world-class facilities with physical separation, 24×7-armed security, biometric access, and full auditability.
- **Innovation Leadership**: First-to-market integration of Elastic + NetScout + Infoblox at this scale in the region, delivering real-time behavioural analytics, DNS tunnelling detection, C2 beaconing identification, and data exfiltration prevention.
- **Commercial & Operational Excellence**: Highly competitive pricing, flexible optionality, zero-capex hosting in du datacenters, and a conservative, stability-first transformation roadmap that reduces operational noise while progressively introducing automation and AI.
- **Emiratization & Knowledge Transfer**: Structured program achieving >60 % Emirati staffing by the end of 3-year operational phase, comprehensive training, runbooks, and capability transfer ensuring DESC's long-term independence.

du is uniquely positioned to deliver this mission-critical national capability on time, within budget, and with absolute reliability. We are fully committed to partnering with DESC to protect Dubai's digital ecosystem today and for decades to come.

We look forward to your positive consideration and to commencing this strategic partnership.

Submitted by:

Badr Abdulla
Account Manager – DESC
Mobile : +971559535316
Email : Badr.Abdalla@du.ae

2. Response to Instructions

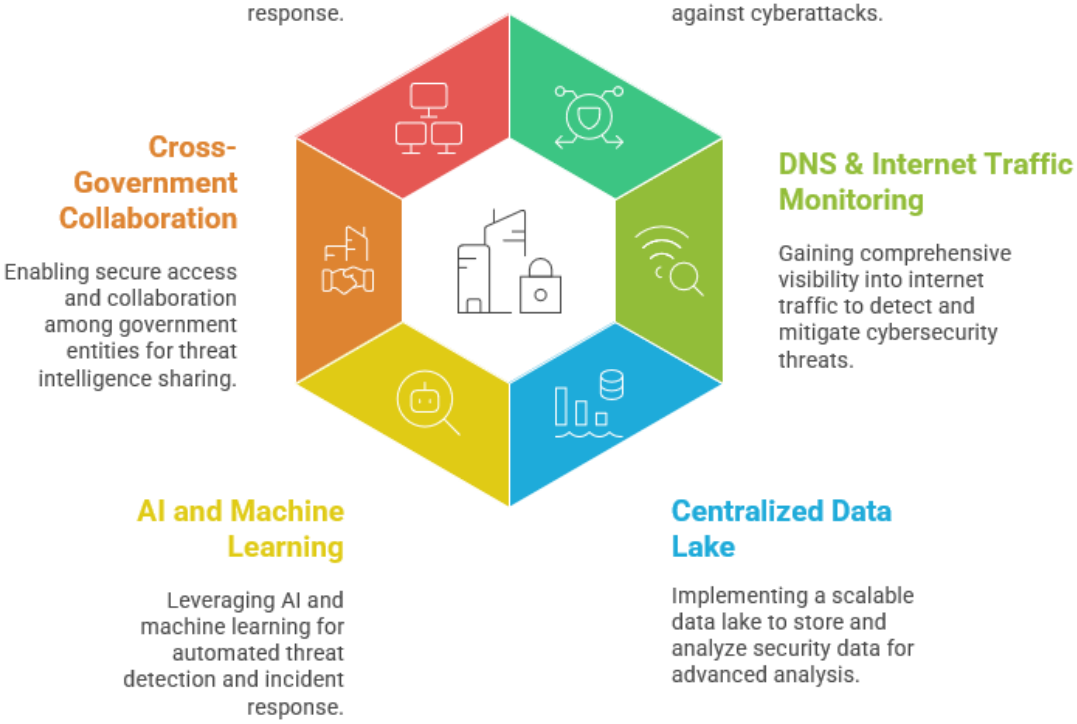
Refer to Attachment : du - Response to Instructions - DESC RFQ 762640 - DNS, Internet Security, and Observability Project_v1

3. Statements of Compliance.

Refer to Attachment : du - Response to Compliance - DESC RFQ 762640 - DNS, Internet Security, and Observability Project_v1

4. Secure DNS and Internet Traffic Monitoring Platform for Dubai Electronic Security Center (DESC) - Roadmap

4.1 Key Requirements – as per RFP



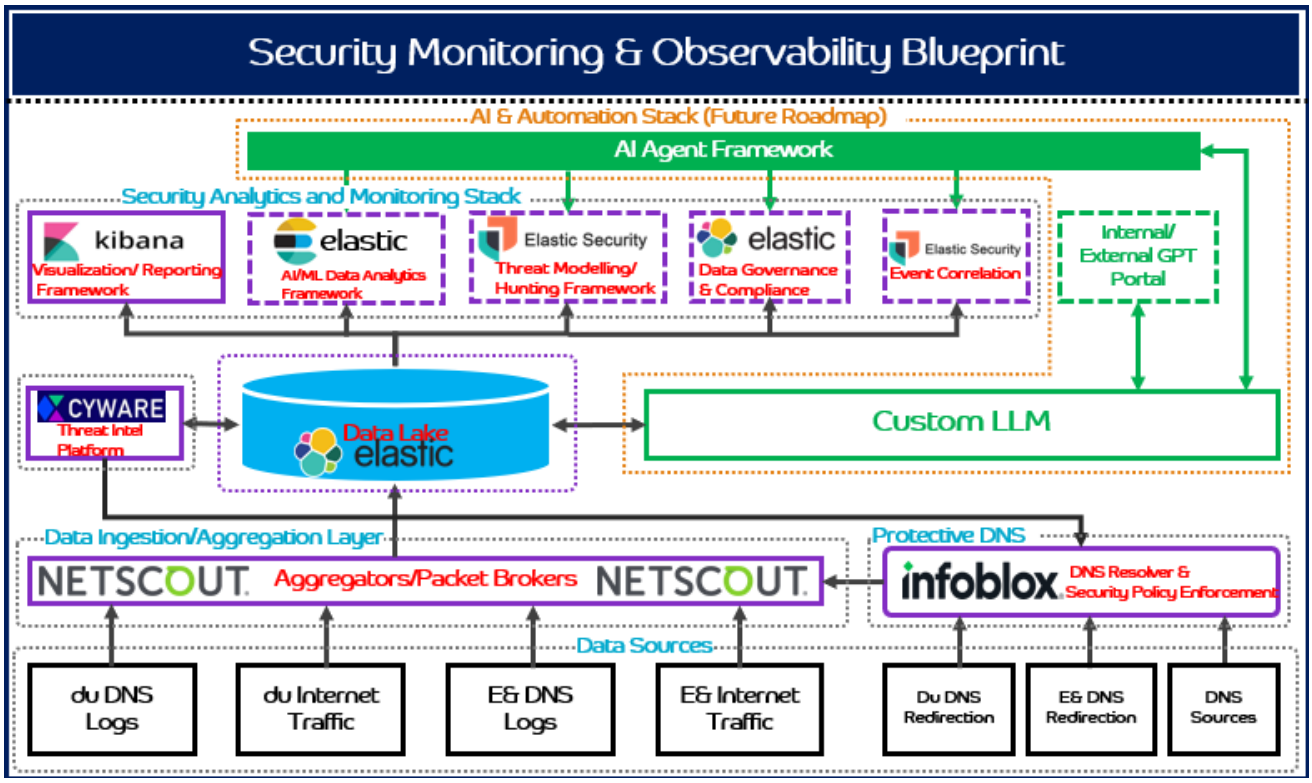
5. Our Understanding & Objectives of DESC

The Dubai Electronic Security Center (DESC) is seeking proposals for the design, development, and implementation of a state-of-the-art cybersecurity and observability platform with geo-redundancy within the emirate of Dubai. The platform will provide comprehensive DNS security, internet traffic monitoring, and advanced security analytics to enhance the cybersecurity posture of government departments and entities across Dubai.

The main objectives of DESC are as under:

- Build a Secure & Redundant DNS Security Platform
- Establish Comprehensive Internet Traffic Monitoring & Security
- Develop a Centralized Data Lake for Security & Observability
- Leverage AI, Machine Learning & Cognitive Security Analytics
- Enable Cross-Government Collaboration & Compliance Enforcement
- Deliver an Integrated Security Monitoring & Observability Center Framework

5.1 Proposed Security Monitoring & Observability Blue Print



6. Proposed Solution Options & Summary of Deliverables

Characteristic	Option 1: Infoblox + Elastic Preferred Solution from du	Option 2 : Efficient IP + FortiSIEM Cost Effective – Alternative to Preferred Solution
Solution Mix for DNS security and Data Lake	Infoblox for DNS and PDNS, Elastic Enterprise for Data Lake	Efficient IP for DNS and PDNS, FortiSIEM Data Lake
Common Structure	NetScout, Fortinet, Cisco Routers, Professional Service Rack Colocation, Endpoint Security, Inter RACK Cabling, Internet Connectivity, DC/DR Colocation, Interconnection, SOC/Cloud Managed Services, Emiratization, Governance	NetScout, Fortinet, Cisco Routers, Professional Service Rack Colocation, Endpoint Security, Inter RACK Cabling, Internet Connectivity, DC/DR Colocation, Interconnection, SOC/Cloud Managed Services, Emiratization, Governance
Virtualization, Compute & Storage	Cisco, Nutanix, Commvault	Dell, Nutanix, Commvault
Optional Services	FortiSOAR, Cisco EVPN with GW	FortiSOAR, Cisco EVPN with GW
Value Added Services	DC/DR 10gig Interconnection (3rd. year charge), Cyware Threat Intel Platform (after 3 years)	DC/DR 10 gig Interconnection (3rd. year charge), Cyware Threat Intel Platform (after 3 years)

6.1 Summary of Proposed High-Level Solution

RFP Phase	Solution Component	Technology Stack	Key Deliverables	Value to DESC
Phase 0	Datacentre Build		Building the DC component	Two Tier 3 facility in Dubai to host the entire solution as per the requirements set forward by DESC
	Networking	Cisco (Core/Spine/Leaf)	Nexus 9332D-GX2B (Core/Spine with MACsec)	400G-capable, MACsec-encrypted, highly resilient fabric; future-proof performance and automation
			Nexus 93180YC-FX3 (Leaf)	
			Catalyst 8570-G2 (Perimeter Routers)	
			ACI-ready design	
	Security	Fortinet	FortiGate 901G (Perimeter UTP)	AI-powered NGFW + ZTNA + application delivery; excellent edge and segmentation protection
			FortiGate 3201F (DC with IPS)	
			FortiGate 121G (OOB)	
			FortiADC 5000F (Internal ADC + WAF)	
	Aggregation layer	NetScout Omnis	Omnis AI Sensors + Streamers (2×100G ASI NICs)	Industry-best DPI and metadata enrichment; 99 % deduplication accuracy; enables high-fidelity analytics in data lake
			nGenius PFS 7000 packet brokers	
			ISNG probes for deduplication & metadata extraction	
			Cold-standby redundancy	
Phase 1	Compute & Storage	Dell on Nutanix (Elastic or FortiSIEM)	Dell XC Series hyper-converged on Nutanix	Optimal price/performance for Elastic or FortiSIEM workloads; simplified management
		Cisco on Nutanix (Elastic or FortiSIEM)	Cisco UCS on Nutanix	Preferred if deeper Cisco integration desired
		S3 Storage (Optional)	Object storage for snapshot repository	Cost-effective long-term backup/DR storage
	Data Lake	Elastic - Option 1	Central Elastic Stack deployment (Elasticsearch, Kibana, Logstash)	Highest scalability for 14+ TB/day, superior ML/analytics, open ecosystem, lowest TCO via tiered storage, maximum flexibility and integration capability.
			Tiered storage (Hot 30/Warm 60/Cold 90-270 days)	
			Active/Active DNS + Active/Passive Internet Traffic geo-redundancy	Faster and Seamless quiring across the HOT, COLD and FROZEN data store with no dependency manual retrieving of d availability historical data
			1,200+ MITRE ATT&CK rules + ML anomaly detection	
			Real-time dashboards, alerting, REST APIs	
			Full integration with NetScout, Cyware, future AI stack	
		FortiSIEM - Option 2	FortiSIEM as unified SIEM + data lake	Strong if customer prefers single-vendor Fortinet stack
			FortiGuard AI/ML threat intel	

			Integrated security fabric dashboards	
Phase 2	Internet Data Ingestion into DataLake	Connectivity	Feed from Internet Service provider - du and e&	
		Elastic / FortiSIEM	Use case development for Security Monitoring and Observability	
Phase 3	Building Protective DNS Platform			
		Infoblox - Option 1	8 × DNS servers (4 per site) supporting 100K QPS	Market-leading DNS threat prevention, proven at scale in UAE (du, Etisalat, DEWA, Dubai Police, etc.), seamless data lake integration, lowest operational risk
			Infoblox Grid + Advanced DNS Protection (ADP)	
			Reputation, behavioural, signature-based blocking	
			DNSTAP log export to data lake	
			Centralized Grid management with DR backup	
		Efficient IP - Option 2	8 × DNS servers (4 per site)	Acceptable alternative for cost reduction;
			Basic DNS security features + log export	
	Managed Services	du	Full implementation + 24-month operate & transform	Complete operational ownership, progressive automation/AI adoption, local talent development, zero-risk transition-in/out, full compliance and SLA adherence
			Optional Item | ManageEngine suite (OpManager, ServiceDesk+, Endpoint Central, Analytics+) - optional items for DESC to decide.	
			Emiratization plan	
			Structured 6-month exit/transition	

6.2 Technology Stack

Technology	Proposed Solution	
	Option 1	**Option 2**
Data lake / SIEM / Visualization	Elastic	FortiSIEM
Packet Broker	NetScout PF 7000 (HW)	NetScout PF 7000 (HW)
	ISNG (HW)	ISNG (HW)
	AI Sensor (HW)	AI Sensor (HW)
	AI Streaner (VM)	AI Streaner (VM)
PDNS	Infoblox IB Flex DMZ Servers	Efficient IP
Threat Intelligence Platform	Cyware	Cyware
EDR	TrendMicro	TrendMicro
Compute	Cisco UCS or Dell XC770 Core	Cisco UCS or Dell XC770 Core
Virtualization	Nutanix	Nutanix

Storage	Nutanix S3 / Object Store	Nutanix NFS / Powerscale
Backup	Commvault	Commvault
Operating System	Ubuntu	Ubuntu
Internet Routers	Cisco 8570G2	Cisco 8570G2
Internet Firewalls	Fortigate FG 901G	Fortigate FG 901G
Internet Switches	Cisco N9K-C93180-FX3	Cisco N9K-C93180-FX3
DMZ Switches	Cisco N9K-C9332D-GX2B	Cisco N9K-C9332D-GX2B
Core Switches	Cisco N9K-C9332D-GX2B	Cisco N9K-C9332D-GX2B
Spine Switches	Cisco N9K-C9332D-GX2B	Cisco N9K-C9332D-GX2B
Leaf Switches	Cisco N9K-C93180-FX3	Cisco N9K-C93180-FX3
DC Firewalls	Fortigate FG 3201F	Fortigate FG 3201F
DC ADC	Fortinet FAD 5000F	Fortinet FAD 5000F
OOB Firewalls	FG 121G	FG 121G
OOB Switches	9200-48T	9200-48T
OOB Authentication	Forti Authenticator VM with MFA	Forti Authenticator VM with MFA
Console Management	Opengear	Opengear
Firewall Central Mgmt	FortiManager VM	FortiManager VM
Firewall Logging	FortiAnalyzer VM	FortiAnalyzer VM
TACACS	Cisco ISE VM	Cisco ISE VM

7. Bill of Quantity – BoQ

7.1 Data Lake

Option 1 - Elastic

#	Product	Description	Qty
		Elastic	
1	Enterprise Resource Unit - 64GB	Enterprise Resource Unit - 64GB	165
2	Elastic Training subscriptions (Professional)	Elastic Training subscriptions (Professional)	2

Option 2 - FortiSIEM

#	Product	Description	Qty

		FortiSIEM	
1	FC6-10-SMGS1-1026-02-36	FortiSIEM GB Subscription License 3 Year FortiSIEM Subscription license for minimum 2000GB+ Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.	13500
2	FC2-10-SMGS1-182-02-36	FortiSIEM GB Advanced Agent Subscription License 3 Year Per Agent Subscription License for 500 - 999 Agents. Providing File Integrity Monitoring (Windows, Linux), log & performance monitoring	500
3	FCI-10-SMGS1-149-02-36	FortiSIEM GB Indicators of Compromise (IOC) Service 3 Year FortiGuard Indicators of Compromise (IOC) Service (for 1 - 15000GB/Day of Logs)	1

7.2 DNS Security

Option 1 : Infoblox

#	Product	Description	Qty
Infoblox			
Management & Caching Recursive DNS			
1	IB-SPLA-SWSUB-FLEXACTIVATION-9	Subscription grid activation license for IB-FLEX. Requires one per Grid	1
2	IB-SPLA-SWSUB-REC-Q-100K-9	Recursive DNS for IB-FLEX, 100,000 qps capacity	1
3	IB-SPLA-SWSUB-DCA-Q-100K-9	DNS Cache Acceleration for IB-FLEX, 100,000 qps capacity	1
DNS Infrastructure Protection			
4	IB-SPLA-SWSUB-ADPR-100K-9	Advanced DNS Protection subscription for IB-FLEX, 100,000 qps capacity	1
DNS Security			
5	IB-SPLA-SUB-THREAT-ADV-S100K	IB-SPLA-SUBTHREATADV-S-100K	1
6	IB-SPLA-SUB-CC-S-100K-1M	Infoblox content categorization feed subscription of 100,000 provisioned subscribers up to 900,000 provisioned subscribers	1
Reporter			
7	TR-SWBSUB-5005-ACTIVATION	TR-5005 Reporting & Analytics Software Bundle, activation, requires Infoblox Reporting and Analytics Subscription License	1
8	TR-SWTL-5GB-9	Reporting and Analytics Subscription License, 1 License per Grid, requires Reporting and Analytics HW or Activation Software Bundle	1

Option 2 : Efficient IP

#	SKU	Description	Qty

Centralized Management "2 V-Appliances in main DC and one V-Appliance in DR DC"			
1	SDS-1170-DDI-3YS-GM	3 Year Period Subscription for SOLIDserver 1170 software appliance DNS-DHCP-IPAM Services - 24/7 support services	3
4 V-Appliances "DC01" 3M-QPS each V- Appliance			
2	BLAST-4070-3YS-GM	3 Year Period Subscription for SOLIDserver 4070 DNS BLAST software appliance - 24/7 support services	4
4 V-Appliances "DC02" 3M-QPS each V- Appliance			
3	BLAST-4070-3YS-GM	3 Year Period Subscription for SOLIDserver 4070 DNS BLAST software appliance - 24/7 support services	4
DNS Firewall Feeds			
4	SDS-4070-DITC-T3-EX-3YS-SM	3 Year Subscription - Elite service plan extension (DNS IC Investigate Only) for SOLIDserver 4070 DDI appliances - 8x5 support services	1
Reporter			
5	RPT_EE	Advanced Reporter	2

7.3 NetScout Packet Broker - Aggregation

#	Product	Description	Qty
NetScout			
PFS			
1	PFOSN-YRE-02-C4M	Packet Flow Operating System (PFOS) Software for Certified PFS	4
2	E1FCNANRE000	NETSCOUT Certified PFS	4
3	321-2318	Transceiver, QSFP28, 100GBase-SR4 or 4x25GBase-SR, MM, MPO, 8-pack	6
4	321-2317	Transceiver, QSFP28, 100GBase-LR4, SM, LC, 10km, 8-pack	4
ISNG			
5	C-04802-M00-2-SW-C4M	NETSCOUT Certified InfiniStreamNG Software, for use with NETSCOUT 2-Port 100G ASI Accelerator NIC (QSFP28) on C-04800 M series certified appliance hardware, purchased separately.	2
6	A-04802-M00-2-HW-C4M	NETSCOUT Certified InfiniStreamNG 2-Port 100G ASI Accelerator NIC (QSFP28), 2-Socket, for use with C-04800 M series certified appliance hardware, purchased separately.	4
17	C-04800-WSMA2	NETSCOUT Certified server, 1U, Dual 24-core CPUs, 512GB RAM, 64TB (4x 16TB), AC Power	4
AI Sensor			
7	Z-05002-000-2-C4M	Qualified Omnis AI Sensor software, includes NETSCOUT 2-Port 100G ASI Accelerator NIC, 2 socket	2
8	C-04800-WSMA2	NETSCOUT Certified server, 1U, Dual 24-core CPUs, 512GB RAM, 64TB (4x 16TB), AC Power	4

9	A-04802-M00-2-HW-C4M	NETSCOUT Certified InfiniStreamNG 2-Port 100G ASI Accelerator NIC (QSFP28), 2-Socket, for use with C-04800 M series certified appliance hardware, purchased separately.	4
AI Streamer			
10	979V0L-C4W	Omnis AI Streamer - 5 interfaces	2
11	VM - Virtual Machine	AI Streamer Server	2
12	VM - Virtual Machine	nCM Server	2

7.4 Datacenter Networking

#	Product	Description	Qty
Cisco Networking			
Internet Routers			
1	C8570-G2	Cisco 8500 Secure Router, C8570-G2	4
2	CON-L14HR-C8570G2A	CX LEVEL 1 24X7X4 Cisco 8570 Secure Ro	4
3	MEM-C85G2-32GB	32GB DRAM	4
4	SSD-C85G2-480GB	480GB SSD	4
5	C85G2-ACCKIT-19	19" Rack Mount	4
6	C8500-RFID-1R	Cisco C8500 RFID - 1RU	4
7	NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment	4
8	R-OS-XL-E	Cisco OS Essentials - XLarge (Embedded, Perpetual)	4
9	IOSXE-AUTO-MODE	IOS XE Autonomous for Unified image	4
10	SC85G2UK9-1715	IOS XE 17.15	4
11	PWR-CH1-750WACR	750W AC Power Supply	8
12	CAB-C13-C14-AC	Power cord, C13 to C14 (recessed receptacle), 10A	8
13	QSFP-40G-SR-BD	QSFP40G BiDi Short-reach Transceiver	16
14	CISCO-ROUT-SUB	Cisco Secure Routing Subscription	2
15	LIC-ROS-XL-A	Cisco Routing Advantage Lic - XLarge	4
16	LIC-R-OP-CC	Cisco On-Prem Catalyst Center Management for Routing	4
Interconnect Switches			
17	N9K-C93180-FX3-B8C	2xNexus 93180YC-FX3 w/ 8x 100G Optics	2
18	CON-SSSNP-N931FB8C	SOLN SUPP 24X7X4 2xNexus 93180YC-FX3	2
	N9K-C93180YC-FX3B	Nexus 93180YC-FX3 bundle PID	2
	CON-SSSNP-N9KC93X1	SOLN SUPP 24X7X4 Nexus 93180YC-FX3 bundle PID	2
	N9K-C93180YC-FX3B	Nexus 93180YC-FX3 bundle PID	2
	CON-SSSNP-N9KC93X1	SOLN SUPP 24X7X4 Nexus 93180YC-FX3 bundle PID	2
	NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	4
	MODE-NXOS	Mode selection between ACI and NXOS	4
	DCN-AI	Select if this product will be used for AI ML Applications	2
	NXOS-CS-10.4.2F	Nexus 9300, 9500, 9800 NX-OS SW 10.4.2 (64bit) Cisco Silicon	2
	NXK-MEM-16GB	Additional memory of 16GB for Nexus Switches	2
	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	2
	NXA-FAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow	8

NXA-PAC-650W-PI	Nexus NEBs AC 650W PSU - Port Side Intake	4
CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	4
N9K-PICK-SR-1.2	PID to select QSFP-100G-SR 1.2 Optic in the bundle	2
QSFP-100G-SR1.2	100G SR1.2 BiDi QSFP Transceiver, LC, 100m OM4 MMF	8
NXOS-CS-10.4.2F	Nexus 9300, 9500, 9800 NX-OS SW 10.4.2 (64bit) Cisco Silicon	2
NXK-MEM-16GB	Additional memory of 16GB for Nexus Switches	2
NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	2
NXA-FAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow	8
NXA-PAC-650W-PI	Nexus NEBs AC 650W PSU - Port Side Intake	4
CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	4
N9K-PICK-SR-1.2	PID to select QSFP-100G-SR 1.2 Optic in the bundle	2
QSFP-100G-SR1.2	100G SR1.2 BiDi QSFP Transceiver, LC, 100m OM4 MMF	8
C1A1TN9300XF-3Y	DCN Advantage Term N9300 XF, 3Y	4
SVS-B-N9K-ADV-XF	EMBEDDED SOLN SUPPORT SWSS FOR NEXUS 9K	4
SW-AI	Select if this product will be used for AI ML Applications	2
DMZ Switches / Aggregation switches		
N9K-C9332D-GX2B	Nexus 9300 Series, 32p 400G Switch	8
CON-SSSNP-N9KC9D3X	SOLN SUPP 24X7X4 Nexus 9300 Series, 32p 400G QSFP-DD	8
MODE-NXOS	Mode selection between ACI and NXOS	8
NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	8
NXOS-CS-10.6.1F	Nexus 9300, 9500, 9800 NX-OS SW 10.6.1 (64bit) Cisco Silicon	8
NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	8
NXA-SFAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow /w EEPROM	48
NXA-PAC-1500W-PI	Nexus 1500W PSU port-side Intake	16
CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	16
NXOS-SLP-INFO-9K	Info PID for Smart Licensing using Policy for N9K	8
DCN-AI	Select if this product will be used for AI ML Applications	8
C1A1TN9300XF2-3Y	Data Center Networking Advantage Term N9300 XF2, 3Y	8
DCN-ADOPT-BAS	Nexus(DCN) - Virtual adopt session http://cs.co/requestCSS	8
SW-AI	Select if this product will be used for AI ML Applications	8
QSFP-100G-SR1.2	100G SR1.2 BiDi QSFP Transceiver, LC, 100m OM4 MMF	32
100GQSFP-SR1.2-4	4 units of QSFP-100G-SR1.2	16
SVS-B-N9K-ADV-XF2	EMBEDDED SOLN SUPPORT SWSS FOR NEXUS 9K	8
Core Switches		
N9K-C9332D-GX2B	Nexus 9300 Series, 32p 400G Switch	4
CON-SSSNP-N9KC9D3X	SOLN SUPP 24X7X4 Nexus 9300 Series, 32p 400G QSFP-DD	4
MODE-NXOS	Mode selection between ACI and NXOS	4
NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	4
NXOS-CS-10.6.1F	Nexus 9300, 9500, 9800 NX-OS SW 10.6.1 (64bit) Cisco Silicon	4
NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	4
NXA-SFAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow /w EEPROM	24
NXA-PAC-1500W-PI	Nexus 1500W PSU port-side Intake	8

CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	8
NXOS-SLP-INFO-9K	Info PID for Smart Licensing using Policy for N9K	4
DCN-AI	Select if this product will be used for AI ML Applications	4
C1A1TN9300XF2-3Y	Data Center Networking Advantage Term N9300 XF2, 3Y	4
DCN-ADOPT-BAS	Nexus(DCN) - Virtual adopt session http://cs.co/requestCSS	4
SW-AI	Select if this product will be used for AI ML Applications	4
QSFP-100G-SR1.2	100G SR1.2 BiDi QSFP Transceiver, LC, 100m OM4 MMF	16
100GQSFP-SR1.2-4	4 units of QSFP-100G-SR1.2	8
SVS-B-N9K-ADV-XF2	EMBEDDED SOLN SUPPORT SWSS FOR NEXUS 9K	4
Spine Switches		
N9K-C9332D-GX2B	Nexus 9300 Series, 32p 400G Switch	4
CON-SSSNP-N9KC9D3X	SOLN SUPP 24X7X4 Nexus 9300 Series, 32p 400G QSFP-DD	4
MODE-NXOS	Mode selection between ACI and NXOS	4
NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	4
NXOS-CS-10.6.1F	Nexus 9300, 9500, 9800 NX-OS SW 10.6.1 (64bit) Cisco Silicon	4
NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	4
NXA-SFAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow /w EEPROM	24
NXA-PAC-1500W-PI	Nexus 1500W PSU port-side Intake	8
CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	8
NXOS-SLP-INFO-9K	Info PID for Smart Licensing using Policy for N9K	4
DCN-AI	Select if this product will be used for AI ML Applications	4
C1A1TN9300XF2-3Y	Data Center Networking Advantage Term N9300 XF2, 3Y	4
DCN-ADOPT-BAS	Nexus(DCN) - Virtual adopt session http://cs.co/requestCSS	4
SW-AI	Select if this product will be used for AI ML Applications	4
QSFP-100G-SR1.2	100G SR1.2 BiDi QSFP Transceiver, LC, 100m OM4 MMF	16
100GQSFP-SR1.2-4	4 units of QSFP-100G-SR1.2	8
SVS-B-N9K-ADV-XF2	EMBEDDED SOLN SUPPORT SWSS FOR NEXUS 9K	4
Leaf Switches		
N9K-C93180-FX3-B8C	2xNexus 93180YC-FX3 w/ 8x 100G Optics	4
CON-SSSNP-N931FB8C	SOLN SUPP 24X7X4 2xNexus 93180YC-FX3	4
N9K-C93180YC-FX3B	Nexus 93180YC-FX3 bundle PID	4
CON-SSSNP-N9KC93X1	SOLN SUPP 24X7X4 Nexus 93180YC-FX3 bundle PID	4
N9K-C93180YC-FX3B	Nexus 93180YC-FX3 bundle PID	4
CON-SSSNP-N9KC93X1	SOLN SUPP 24X7X4 Nexus 93180YC-FX3 bundle PID	4
NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	8
MODE-NXOS	Mode selection between ACI and NXOS	8
DCN-AI	Select if this product will be used for AI ML Applications	4
NXOS-CS-10.4.2F	Nexus 9300, 9500, 9800 NX-OS SW 10.4.2 (64bit) Cisco Silicon	4
NXK-MEM-16GB	Additional memory of 16GB for Nexus Switches	4
NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	4
NXA-FAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow	16
NXA-PAC-650W-PI	Nexus NEBs AC 650W PSU - Port Side Intake	8

CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	8
N9K-PICK-SR-1.2	PID to select QSFP-100G-SR 1.2 Optic in the bundle	4
QSFP-100G-SR1.2	100G SR1.2 BiDi QSFP Transceiver, LC, 100m OM4 MMF	16
NXOS-CS-10.4.2F	Nexus 9300, 9500, 9800 NX-OS SW 10.4.2 (64bit) Cisco Silicon	4
NXK-MEM-16GB	Additional memory of 16GB for Nexus Switches	4
NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	4
NXA-FAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow	16
NXA-PAC-650W-PI	Nexus NEBs AC 650W PSU - Port Side Intake	8
CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	8
N9K-PICK-SR-1.2	PID to select QSFP-100G-SR 1.2 Optic in the bundle	4
QSFP-100G-SR1.2	100G SR1.2 BiDi QSFP Transceiver, LC, 100m OM4 MMF	16
C1A1TN9300XF-3Y	DCN Advantage Term N9300 XF, 3Y	8
SVS-B-N9K-ADV-XF	EMBEDDED SOLN SUPPORT SWSS FOR NEXUS 9K	8
SW-AI	Select if this product will be used for AI ML Applications	4
OOB Management		
C9200-48T-A	Catalyst 9200 48-port data only, Network Advantage	6
CON-SNT-C920048T	SNTC-8X5XNBD Catalyst 9200 48-port data only, Network	6
C9200-DNA-A-48	C9200 Cisco DNA Advantage, 48-Port Term Licenses	6
C9200-DNA-A-48-3Y	C9200 Cisco DNA Advantage, 48-Port, 3 Year Term License	6
C9200-NW-A-48	C9200 Network Advantage, 48-port license	6
CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	12
C9200-NM-4X	Catalyst 9200 4 x 10G Network Module	6
PWR-C6-125WAC/2	125W AC Config 6 Power Supply - Secondary Power Supply	6
C9K-ACC-RBFT	RUBBER FEET FOR TABLE TOP SETUP 9200 and 93xx	6
C9K-ACC-SCR-4	12-24 and 10-32 SCREWS FOR RACK INSTALLATION, QTY 4	6
CAB-GUIDE-1RU	1RU CABLE MANAGEMENT GUIDES 9200 and 9300	6
NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment	6
C9200-STACK-KIT	Cisco Catalyst 9200 Stack Module	6
STACK-T4-1M	1M Type 4 Stacking Cable	6
C9200-STACK	Catalyst 9200 Stack Module	12
Cisco ISE		
ISE-SEC-SUB	Cisco Identity Service Engine Subscription	2
ISE-P-LIC	Cisco Identity Service Engine Premier Subscription	200
SVS-ISE-SUP-B	Cisco Support Standard for ISE	2
L-ISE-TACACS-ND=	Cisco ISE Device Admin Node License	2
R-ISE-VMC-K9=	Cisco ISE Virtual Machine Common PID	2
CON-L1SW-RISE9KVM	ENH SW Cisco ISE Virtual Machine	2
Optics		
QSFP-40/100-SRBD=	100G and 40GBASE SR-BiDi QSFP Transceiver, LC, 100m OM4 MMF	300
QSFP-40G-SR-BD=	QSFP40G BiDi Short-reach Transceiver	80
SFP-25G-SR-S=	25GBASE-SR SFP Module	160

	CVR-QSFP28-SFP25G=	100G to SFP25G adapter	40
	SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	160
	CVR-QSFP-SFP10G=	QSFP to SFP10G adapter	40
	SFP-10G-LR-S=	10GBASE-LR SFP Module, Enterprise-Class	10
	GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	30

7.5 Network Security

#	Product	Description	Qty
Fortinet			
FortiManager			
22	FC1-10-FMGVS-258-01-36	FortiManager-VM Subscription License with Support 3 Year Subscription license for 10 devices/vdoms managed by FortiManager VM S-series, including FortiCare Premium.	1
23	FC1-10-FMGVS-1118-01-36	FortiManager-VMS FortiAI Subscription 3 Year Generative AI powered central management service, utilizing large language models (LLMs) for real-time assistance in orchestration, automation and monitoring for 10 devices/vdoms	1
FortiAnalyzer			
24	FC3-10-AZVMS-465-01-36	FortiAnalyzer-VM Subscription License with Support 3 Year Subscription license for 500 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service.	1
25	FC3-10-AZVMS-1118-01-36	FortiAnalyzer-VMS FortiAI Subscription 3 Year Generative AI powered security service utilizing large language models (LLMs) for real-time assistance in SOC analysis, incident investigation, triage and response (500 GB/Day of logs)	1
Perimeter Firewall			
26	FG-901G	FortiGate-901G 4x 25G SFP28 slots, 4 x 10GE SFP+ slots, 17 x GE RJ45 ports (including 1 x MGMT port, 16 x switch ports), 1 X 2.5G HA port, 8 x GE SFP slots, SPU NP7 and CP9 hardware accelerated, 2x 480GB onboard SSD storage, dual AC PSU.	4
27	FC-10-FG9H1-950-02-36	FortiGate-901G 3 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	4
28	FN-TRAN-SFP28-SR	25GE SFP28 transceiver module, short range 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots	8
29	FN-TRAN-SFP+SRI	10 GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 400m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP+ slots	8
DC Firewall			

30	FG-3201F	FortiGate-3201F 4x 400 GE QSFP-DD slots, 4x ULL SFP28 ports, and 12x 50 GE SFP56 slots (including 10x ports, 2x HA ports), 2x 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2x 960GB SSD onboard storage, and 2 AC power supplies	4
31	FC-10-F32F1-928-02-36	FortiGate-3201F 3 Year Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium)	4
32	FN-TRAN-QSFP28-SR	100GE QSFP28 transceivers 100 GE QSFP28 transceiver module, short range 100m, MPO-12 connector, four-channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP28 slots	8
33	FN-TRAN-QSFP+SR	40GE QSFP+ transceivers, short range 40 GE QSFP+ transceiver module, short range 150m, MPO-12 connector, four channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP+/QSFP28 slots	16
34	FN-TRAN-SFP+SRI	10 GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 400m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP+ slots	8
ADC with 100 Gbps			
35	FAD-5000F	FortiADC-5000F Application Delivery Controller - 4x 100GbE QSFP28 ports, 8 x 40GbE QSFP ports, 1 x GbE RJ45 management port, 1x 960G SSD, dual AC power supplies	4
36	FC-10-FD5KF-732-02-36	FortiADC-5000F 3 Year AI Security - Application Security Bundle Plus Threat Analytics, FortiGuard Advanced Bot Protection - (7M monthly requests), and FortiCare Premium	4
37	FN-TRAN-QSFP28-SR	100GE QSFP28 transceivers 100 GE QSFP28 transceiver module, short range 100m, MPO-12 connector, four-channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP28 slots	8
38	FN-TRAN-QSFP+SR	40GE QSFP+ transceivers, short range 40 GE QSFP+ transceiver module, short range 150m, MPO-12 connector, four channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP+/QSFP28 slots	8
39	FN-TRAN-SFP+SRI	10 GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 400m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP+ slots	8
OOB Firewall and Authenticator			
40	FG-121G	FortiGate-121G 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, SP5 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies	2
41	FC-10-F121G-950-02-36	FortiGate-121G 3 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	2

42	FAC-VM-BASE	VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms	4
43	FC1-10-0ACVM-248-02-36	FortiCare Premium Support (1 - 500 USERS)	4
44	FTM-ELIC-100	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic license certificate. License transfer between devices is not allowed.	1

7.6 DELL on Nutanix

7.6.1 Option 1 - Dell on Nutanix

7.6.1.1 Dell on Nutanix for Elastic

#	SKU	Description	Qty
1		XC770 Core - ELK Primary	13
	210-BSPP	Dell XC770 Core	1
	634-CZSL	Nutanix OS for AHV 1.0	1
	321-BLJY	EDSFF E3.S Chassis with up to 16 Drives (NVMe Gen5) Direct Drives, Smart Flow	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1
	379-BDCO	Additional Processor Selected	1
	412-BBJV	Heatsink for 2 CPU with GPU Configuration (CPU greater than 250W)	1
	370-AAIP	Performance Optimized	1
	370-BCCX	6400MT/s RDIMMs	1
	370-BCGL	96GB RDIMM, 6400MT/s, Dual Rank	16
	780-BCDO	C30, No RAID for NVME chassis	1
	405-AACD	No Controller	1
	400-ABHL	No Hard Drive	1
	345-BKBJ	15.36TB NVMe Read Intensive AG Drive E3s Gen5 with carrier	7
	384-BBBL	Performance BIOS Settings	1
	800-BBDM	UEFI BIOS Boot Mode with GPT Partition	1
	384-BFCL	HCI 2U High Performance Gold Fan	1
	450-BCWT	Dual, Redundant (1+1),Hot-Plug MHS Power Supply, 1500W MM, Titanium	1

	450-AADY	C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord	2
	330-BCXY	Riser Config 6-1, Rear Half Length, 4x16 FH Slots (Gen5), 1x8/1x16 OCP (Gen5), 2nd OCP x16 (Gen5)	1
	540-BCRX	Broadcom 57504 Quad Port 10/25GbE, SFP28, OCP 3.0 NIC	1
	470-BCHM	Rear Filler Blank for BOSS/OCP	1
	379-BDSQ	GPU Enablement	1
	407-BBXX	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	4
	403-BDMM	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80)	1
	329-BLHN	HCI 770 Motherboard, WW	1
	634-CSHS	Secure Enterprise Key Manager License 3.0	1
	634-CSHT	Secured Component Verification	1
	634-CSHY	iDRAC10, Enterprise 17G	1
	340-DVTG	HCI 770 Shipping	1
	340-DVTK	HCI Shipping EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungar/Greek/Arab)	1
	340-DVSN	HCI 2U Shipping Material	1
	389-FKXS	HCI, No CCC, No CE Label Marking	1
	350-BDGJ	XC770-16 QR Label	1
	325-BGMM	2U Bezel, Standard, XC Core	1
	770-BDZO	2U Combo Drop-In/Stab-In Rails (B22)	1
	379-BCQV	iDRAC Group Manager, Enabled	1
	379-BETF	iDRAC Legacy Password for OCP cards	1
	350-BDFH	2U Quick Sync Type Left Ear Module	1
	865-BCIF	ProSupport Plus and 4Hr Mission Critical Extension, 24 Month(s)	1
	865-BCIG	ProSupport Plus and 4Hr Mission Critical Initial, 12 Month(s)	1
	683-BCXR	ProDeploy Plus Dell Storage XC Series Appliance	1
	709-BBML	Parts Only Warranty 12 Months	1
	470-AEYU	No Cables Required	1
2		XC770 Core - ELK DR	4
	210-BSPP	Dell XC770 Core	1
	634-CZSL	Nutanix OS for AHV 1.0	1
	321-BLJY	EDSFF E3.S Chassis with up to 16 Drives (NVMe Gen5) Direct Drives, Smart Flow	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1

379-BDCO	Additional Processor Selected	1
412-BBJV	Heatsink for 2 CPU with GPU Configuration (CPU greater than 250W)	1
370-AAIP	Performance Optimized	1
370-BCCX	6400MT/s RDIMMs	1
370-BCGL	96GB RDIMM, 6400MT/s, Dual Rank	16
780-BCDO	C30, No RAID for NVME chassis	1
405-AACD	No Controller	1
400-ABHL	No Hard Drive	1
345-BKBJ	15.36TB NVMe Read Intensive AG Drive E3s Gen5 with carrier	6
384-BBBL	Performance BIOS Settings	1
800-BBDM	UEFI BIOS Boot Mode with GPT Partition	1
384-BFCL	HCI 2U High Performance Gold Fan	1
450-BCWT	Dual, Redundant (1+1),Hot-Plug MHS Power Supply, 1500W MM, Titanium	1
450-AADY	C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord	2
330-BCXY	Riser Config 6-1, Rear Half Length, 4x16 FH Slots (Gen5), 1x8/1x16 OCP (Gen5), 2nd OCP x16 (Gen5)	1
540-BCRX	Broadcom 57504 Quad Port 10/25GbE, SFP28, OCP 3.0 NIC	1
470-BCHM	Rear Filler Blank for BOSS/OCP	1
379-BDSQ	GPU Enablement	1
407-BBXX	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	4
403-BDMM	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80)	1
329-BLHN	HCI 770 Motherboard, WW	1
634-CSHS	Secure Enterprise Key Manager License 3.0	1
634-CSHT	Secured Component Verification	1
634-CSHY	iDRAC10, Enterprise 17G	1
340-DVTG	HCI 770 Shipping	1
340-DVTK	HCI Shipping EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungar/Greek/Arab)	1
340-DVSN	HCI 2U Shipping Material	1
389-FKXS	HCI, No CCC, No CE Label Marking	1
350-BDGJ	XC770-16 QR Label	1
325-BGMM	2U Bezel, Standard, XC Core	1
770-BDZO	2U Combo Drop-In/Stab-In Rails (B22)	1
379-BCQV	iDRAC Group Manager, Enabled	1
379-BETF	iDRAC Legacy Password for OCP cards	1
350-BDFH	2U Quick Sync Type Left Ear Module	1

	865-BCIF	ProSupport Plus and 4Hr Mission Critical Extension, 24 Month(s)	1
	865-BCIG	ProSupport Plus and 4Hr Mission Critical Initial, 12 Month(s)	1
	683-BCXR	ProDeploy Plus Dell Storage XC Series Appliance	1
	709-BBML	Parts Only Warranty 12 Months	1
	470-AEYU	No Cables Required	1
3		XC SW Lic - Primary cluster	1
	210-BPFM	XC Nutanix SW License	1
	143-BVYB	NCM Starter Production SW Lic 3YR, Z4	1664
	143-BVWN	NCI Professional Production SW Lic 3YR, Z4	1664
4		XC SW Lic - DR cluster	1
	210-BPFM	XC Nutanix SW License	1
	143-BVYB	NCM Starter Production SW Lic 3YR, Z4	512
	143-BVWN	NCI Professional Production SW Lic 3YR, Z4	512
#	SKU	Description	Qty
1		ObjectScale X560	6
	210-BQRC	ObjectScale X560 Node - FLD	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	345-BLRG	16TB ISE	1
	800-BBQV	Informational Purposes Only	1
	709-BFLX	Parts Only Warranty 36Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	683-BLYR	ProDeploy Plus ObjectScale and ECS Appliance	1
2		ObjectScale Appliance Software	6

	210-BQRW	ObjectScale Software Base	1
	800-BBQV	Informational Purposes Only	1
	149-BCDV	ObjectScale Gen4 Base License=ID	1
	149-BCDW	ObjectScale D@RE License=ID	1
	149-BCFB	ObjectScale Gen4 Capacity License 1TB=CB	192
	800-BBQV	Informational Purposes Only	1
	487-BNJR	ProSupport Plus ObjectScale Sftwr Spt-Maint, 36 Month(s)	1
3		ObjectScale Backend Switches	2
	210-BQQZ	ObjectScale S5248F Switch FLD ROW	1
	470-BDNT	ObjectScale X560 BackEnd Cable Kit - FLD	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BFLX	Parts Only Warranty 36Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
4		ObjectScale Frontend Switches	2
	210-BQQZ	ObjectScale S5248F Switch FLD ROW	1
	470-BDNN	ObjectScale X560 FrontEnd Cable Kit - FLD	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BFLX	Parts Only Warranty 36Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
5		ObjectScale Accessories	1
	210-BQRG	ObjectScale Accessories Base	1
	389-FLCS	ObjectScale X560 Cable Label Kit - FLD	1
	470-BBPB	Cable Kit 25G 5M Front End	6
	470-BBPC	Cable Kit 25G 5M Back End	6
	389-FPCH	ObjectScale X560 Install Kit - FLD	6
	750-BBGL	Module 10GB SR QTY2	4
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BHSC	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
6		ObjectScale Services	1
	210-BKCZ	Object Storage Services	1
	519-BGJS	ProDeploy Additional Deployment Time: 8 Hours Onsite File and Object Storage Tech Resource	1

7		ObjectScale X560	5
	210-BQRC	ObjectScale X560 Node - FLD	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	345-BLSD	4TB ISE	1
	800-BBQV	Informational Purposes Only	1
	709-BFLX	Parts Only Warranty 36Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	683-BLYR	ProDeploy Plus ObjectScale and ECS Appliance	1
8		ObjectScale Appliance Software	5
	210-BQRW	ObjectScale Software Base	1
	800-BBQV	Informational Purposes Only	1
	149-BCDV	ObjectScale Gen4 Base License=ID	1
	149-BCDW	ObjectScale D@RE License=ID	1
	149-BCFB	ObjectScale Gen4 Capacity License 1TB=CB	48
	800-BBQV	Informational Purposes Only	1
	487-BNJR	ProSupport Plus ObjectScale Sftwr Spt-Maint, 36 Month(s)	1
9		ObjectScale Backend Switches	2
	210-BQQZ	ObjectScale S5248F Switch FLD ROW	1
	470-BDNT	ObjectScale X560 BackEnd Cable Kit - FLD	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BFLX	Parts Only Warranty 36Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
10		ObjectScale Frontend Switches	2

	210-BQQZ	ObjectScale S5248F Switch FLD ROW	1
	470-BDNN	ObjectScale X560 FrontEnd Cable Kit - FLD	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BFLX	Parts Only Warranty 36Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
11		ObjectScale Accessories	1
	210-BQRG	ObjectScale Accessories Base	1
	389-FLCS	ObjectScale X560 Cable Label Kit - FLD	1
	470-BBPB	Cable Kit 25G 5M Front End	5
	470-BBPC	Cable Kit 25G 5M Back End	5
	389-FPCH	ObjectScale X560 Install Kit - FLD	5
	750-BBGL	Module 10GB SR QTY2	4
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BHSC	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
12		ObjectScale Services	1
	210-BKCZ	Object Storage Services	1
	519-BGJS	ProDeploy Additional Deployment Time: 8 Hours Onsite File and Object Storage Tech Resource	1
Canonical Ubuntu			
OS	Canonical	Ubuntu pro for enterprises with Infra support 24x7	
Product Number	**Description**	**Description**	
Backup	Commvault	Commvault backup SW + Services+ Cyber resiliency	
	CV-UBKRC-FT-31	Commvault Cloud Backup & Recovery Software for Unstructured Data, Per Front-End Terabyte, Subscription 3 - Year, Upfront Payment	500
	PS	Commvault Professional Services for Implementation	Lot
#	SKU	Dell Hardware for Commvault	Qty
1		ME5084 - Full Configuration - [EMEA_ME5084]	1
	210-BBSE	Dell ME5084 Storage Array	1
	340-DCJI	PowerVault MExxxx Shipping, EMEA1	1
	389-EEUQ	PowerVault ME 5U-84, CE Label Marking	1
	403-BCPV	32Gb FC Type-B 8 Port Dual 5U Controller	1
	492-BDCW	2X SFP+, FC32, 32GB	1

	492-BDCW	2X SFP+, FC32, 32GB	1
	492-BDCW	2X SFP+, FC32, 32GB	1
	492-BDCW	2X SFP+, FC32, 32GB	1
	161-BCNL	24TB Hard Drive 12Gbps SAS ISE 7.2K 512e 3.5in Hot-Plug, AG Drive	70
	770-BCVH	Rack Rails 5U	1
	450-ALXP	Power Supply, 2200W, Redundant, WW	1
	450-AEJI	C19 to C20, PDU Style, 2.5M Power Cord	2
	199-BIBF	ProSupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	709-BDHL	Parts Only Warranty 36 Months	1
	683-BCNS	ProDeploy Plus Storage ME 5XXX 5U	1
2		PowerEdge R470 - Full Configuration - [EMEA_R470]	2
	210-BNMR	PowerEdge R470 Server, Enterprise	1
	321-BLDY	2.5" Chassis with up to 8 Hard Drives (SAS/SATA), Smart Flow, Rear IO, H965i	1
	338-CTBL	Intel Xeon 6 Performance 6521P 2.6G, 24C/48T, 144M Cache, Turbo, (225W) DDR5-6400	1
	412-BBLP	Extended heatsink with DIMM blanks	1
	370-AAIP	Performance Optimized	1
	370-BCCX	6400MT/s RDIMMs	1
	370-BCCY	32GB RDIMM, 6400MT/s, Dual Rank	8
	780-BCDS	Unconfigured RAID	1
	403-BDMY	PERC H965i Controller, Front, DCMHS	1
	400-AXSK	3.84TB SSD SATA Read Intensive 6Gbps 512e 2.5in Hot-plug AG Drive, 1 DWPD	4
	384-BBBH	Power Saving BIOS Settings	1
	800-BBDM	UEFI BIOS Boot Mode with GPT Partition	1
	384-BDQL	PowerEdge 1U High Performance Silver Fan	1
	450-BCWW	Dual,Redundant(1+1),Hot-PlugMHSPowerSupply,800WMM(100-240Vac)	1
	450-AADY	C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord	2
	330-BCWK	Riser Config 6, 2x16 FH Slots (Gen5), 1x16 Onboard OCP	1
	330-BCYF	PowerEdge R470 Motherboard fo RTS 1.1, ROW	1
	540-BFPV	Broadcom 57414 Dual Port 25GbE SFP28 Adapter, OCP 3.0 NIC +Sec	1
	780-BCZQ	No OCP Blanks or Cables Required	1
	540-BFXP	Broadcom 57414 25GbE SFP28 Dual Port Adapter, PCIe Full Height +Sec	1
	406-BBXN	Marvell QLE2772 Dual Port Fibre Channel 32Gbps HBA Adapter, PCIe Full Height +Sec	1
	470-AEYU	No Cables Required	1

	325-BFXF	PowerEdge 1U Standard Bezel	1
	350-BDDK	Dell Luggage Tag for x8 and x10 Chassis	1
	470-BCHM	Rear Filler Blank for BOSS/OCP	1
	605-BBFL	Enterprise Linux OS, Non Factory Installed, Requires Subscription Selection	1
	605-BBFN	No Media Required	1
	528-CHFN	RHEL, 1-2SKT,3yr Premium Subscription,Virtual Datacenters, Digitally Fulfilled	1
	634-CSHS	Secure Enterprise Key Manager License 3.0	1
	634-CSHT	Secured Component Verification	1
	634-CSHY	iDRAC10, Enterprise 17G	1
	379-BFXS	Dell Connectivity Client - Enabled	1
	634-CZRP	Dell Connectivity Module 17G	1
	350-BCYJ	Blank Left Ear Module	1
	379-BETE	iDRAC Force Change Password for OCP cards	1
	770-BECD	ReadyRails Sliding Rails (A15)	1
	340-DRWG	PowerEdge Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew)	1
	340-DSJD	PowerEdge R470 Shipping	1
	340-DNSY	PowerEdge 1U Shipping Material	1
	389-FHHX	PowerEdge CCC, No CE Label Marking	1
	407-BBXX	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	4
	709-BBIX	Parts Only Warranty 12 Months	1
	865-BBLP	ProSupport Plus and 4Hr Mission Critical Extension, 24 Month(s)	1
	865-BBLQ	ProSupport Plus and 4Hr Mission Critical Initial, 12 Month(s)	1
	683-BBGH	ProDeploy Plus PowerEdge R Series 1u2u	1
Description		Services	
DU Services		Professional Services	Lot

- Backup storage required **1,150 TB**
- 2x Media agent server
  - 24x CPU
  - 192GB memory
  - 10.2TB SSD
  - 2x 2-port 10/25GB network card
  - 1x 2-poer FC HBA
  - RedHat OS

7.6.1.2 Dell on Nutanix for FortiSIEM

#	SKU	Description	Qty
1		XC770 Core - FortiSIEM Primary	8
	210-BSPP	Dell XC770 Core	1
	634-CZSL	Nutanix OS for AHV 1.0	1
	321-BLJY	EDSFF E3.S Chassis with up to 16 Drives (NVMe Gen5) Direct Drives, Smart Flow	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1
	379-BDCO	Additional Processor Selected	1
	412-BBJV	Heatsink for 2 CPU with GPU Configuration (CPU greater than 250W)	1
	370-AAIP	Performance Optimized	1
	370-BCCX	6400MT/s RDIMMs	1
	370-BCCZ	64GB RDIMM, 6400MT/s, Dual Rank	8
	780-BCDO	C30, No RAID for NVME chassis	1
	405-AACD	No Controller	1
	400-ABHL	No Hard Drive	1
	400-BOMO	7.68TB NVMe Read Intensive AG Drive E3s Gen5 with carrier	8
	384-BBBL	Performance BIOS Settings	1
	800-BBDM	UEFI BIOS Boot Mode with GPT Partition	1
	384-BFCL	HCI 2U High Performance Gold Fan	1
	450-BCWT	Dual, Redundant (1+1),Hot-Plug MHS Power Supply, 1500W MM, Titanium	1
	450-AADY	C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord	2
	330-BCXY	Riser Config 6-1, Rear Half Length, 4x16 FH Slots (Gen5), 1x8/1x16 OCP (Gen5), 2nd OCP x16 (Gen5)	1
	540-BCRX	Broadcom 57504 Quad Port 10/25GbE, SFP28, OCP 3.0 NIC	1
	470-BCHM	Rear Filler Blank for BOSS/OCP	1
	379-BDSQ	GPU Enablement	1
	407-BBXX	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	4
	403-BDMM	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80)	1
	329-BLHN	HCI 770 Motherboard, WW	1
	634-CSHS	Secure Enterprise Key Manager License 3.0	1
	634-CSHT	Secured Component Verification	1
	634-CSHY	iDRAC10, Enterprise 17G	1
	340-DVTG	HCI 770 Shipping	1
	340-DVTK	HCI Shipping EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungar/Greek/Arab)	1
	340-DVSN	HCI 2U Shipping Material	1
	389-FKXS	HCI, No CCC, No CE Label Marking	1
	350-BDGJ	XC770-16 QR Label	1
	325-BGMM	2U Bezel, Standard, XC Core	1
	770-BDZO	2U Combo Drop-In/Stab-In Rails (B22)	1

	379-BCQV	iDRAC Group Manager, Enabled	1
	379-BETF	iDRAC Legacy Password for OCP cards	1
	350-BDFH	2U Quick Sync Type Left Ear Module	1
	865-BCIF	ProSupport Plus and 4Hr Mission Critical Extension, 24 Month(s)	1
	865-BCIG	ProSupport Plus and 4Hr Mission Critical Initial, 12 Month(s)	1
	683-BCXR	ProDeploy Plus Dell Storage XC Series Appliance	1
	709-BBML	Parts Only Warranty 12 Months	1
	470-AEYU	No Cables Required	1
2		XC770 Core - FortiSIEM DR	4
	210-BSPP	Dell XC770 Core	1
	634-CZSL	Nutanix OS for AHV 1.0	1
	321-BLJY	EDSFF E3.S Chassis with up to 16 Drives (NVMe Gen5) Direct Drives, Smart Flow	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1
	338-CSKJ	Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	1
	379-BDCO	Additional Processor Selected	1
	412-BBJV	Heatsink for 2 CPU with GPU Configuration (CPU greater than 250W)	1
	370-AAIP	Performance Optimized	1
	370-BCCX	6400MT/s RDIMMs	1
	370-BCCZ	64GB RDIMM, 6400MT/s, Dual Rank	16
	780-BCDO	C30, No RAID for NVME chassis	1
	405-AACD	No Controller	1
	400-ABHL	No Hard Drive	1
	345-BKBJ	15.36TB NVMe Read Intensive AG Drive E3s Gen5 with carrier	8
	384-BBBL	Performance BIOS Settings	1
	800-BBDM	UEFI BIOS Boot Mode with GPT Partition	1
	384-BFCL	HCI 2U High Performance Gold Fan	1
	450-BCWT	Dual, Redundant (1+1),Hot-Plug MHS Power Supply, 1500W MM, Titanium	1
	450-AADY	C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord	2
	330-BCXY	Riser Config 6-1, Rear Half Length, 4x16 FH Slots (Gen5), 1x8/1x16 OCP (Gen5), 2nd OCP x16 (Gen5)	1
	540-BCRX	Broadcom 57504 Quad Port 10/25GbE, SFP28, OCP 3.0 NIC	1
	470-BCHM	Rear Filler Blank for BOSS/OCP	1
	379-BDSQ	GPU Enablement	1
	407-BBXX	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	4
	403-BDMM	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80)	1
	329-BLHN	HCI 770 Motherboard, WW	1
	634-CSHS	Secure Enterprise Key Manager License 3.0	1
	634-CSHT	Secured Component Verification	1
	634-CSHY	iDRAC10, Enterprise 17G	1
	340-DVTG	HCI 770 Shipping	1

	340-DVTK	HCI Shipping EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungar/Greek/Arab)	1
	340-DVSN	HCI 2U Shipping Material	1
	389-FKXS	HCI, No CCC, No CE Label Marking	1
	350-BDGJ	XC770-16 QR Label	1
	325-BGMM	2U Bezel, Standard, XC Core	1
	770-BDZO	2U Combo Drop-In/Stab-In Rails (B22)	1
	379-BCQV	iDRAC Group Manager, Enabled	1
	379-BETF	iDRAC Legacy Password for OCP cards	1
	350-BDFH	2U Quick Sync Type Left Ear Module	1
	865-BCIF	ProSupport Plus and 4Hr Mission Critical Extension, 24 Month(s)	1
	865-BCIG	ProSupport Plus and 4Hr Mission Critical Initial, 12 Month(s)	1
	683-BCXR	ProDeploy Plus Dell Storage XC Series Appliance	1
	709-BBML	Parts Only Warranty 12 Months	1
	470-AEYU	No Cables Required	1
3		XC SW Lic - Primary cluster	1
	210-BPFM	XC Nutanix SW License	1
	143-BVYB	NCM Starter Production SW Lic 3YR, Z4	1024
	143-BVWN	NCI Professional Production SW Lic 3YR, Z4	1024
4		XC SW Lic - DR cluster	1
	210-BPFM	XC Nutanix SW License	1
	143-BVYB	NCM Starter Production SW Lic 3YR, Z4	512
	143-BVWN	NCI Professional Production SW Lic 3YR, Z4	512
#	SKU	Description	Qty
1		PowerScale A310	4
	210-BQVB	A310 L3 ISE Node	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	400-BTCL	ISE 240TB (15x16TB)	1
	400-BTCZ	ISE 800GB SSD - A310/0	2
	590-TFQM	2x25GbE (SFP28) W/O OPTICS	1
	590-TFQJ	2x25GbE (SFP28) Back-end W/O OPTICS	1
	407-BCIU	Transceivers/Optic/SFP+/SR/10GbE/2 GEN6	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BDXM	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	683-BBNR	ProDeploy Plus PowerScale Node	1
2		PowerScale Archive/Hybrid Chassis	1
	210-BQWX	Base Chassis - Normal A31-Series	1
	350-BDGL	4U Bezel UDS	1

	709-BDXL	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
3		PowerScale Hybrid Additional Software	4
	210-BQVG	PowerScale Hybrid Software - VP	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	151-BCLV	SmartQuotas Base License Bundle A310/A3100 L3 =ID	1
	151-BCMG	SnapShotIQ Base License Bundle A310/A3100 L3 =ID	1
	151-BCMY	Enterprise Bundle A310/A3100 L3=ID	1
	151-BCHY	SmartQuotas Capacity License Bundle A3 Tier 3 L3=CB	240
	151-BCJP	SnapShotIQ Capacity License Bundle A3 L3=CB	240
	151-BCMT	Enterprise Bundle Capacity A310/A3100 L3=CB	240
	151-BBEH	HDFS for OneFS ($0.00)	1
	800-BBQV	Informational Purposes Only	1
	151-BCKV	SmartDedupe Base License A310/A3100 L3=ID	1
	151-BCKC	SmartDedupe Capacity License A310/A3100 L3=CB	240
	487-BDZG	ProSupport Plus Additional Software Support-Maintenance, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
4		PowerScale Archive/Hybrid OE Software	4
	210-BQVG	PowerScale Hybrid Software - VP	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	149-BCCY	OneFS Base License A310/A3100 12-20TB L3=ID	1
	800-BBQV	Informational Purposes Only	1
	149-BCCW	OneFS Capacity A310/A3100 L3=CB	240
	800-BBQV	Informational Purposes Only	1
	487-BEBP	ProSupport Plus OneFS Hybrid Software Support-Maintenance, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
5		PowerScale Switches	1
	210-AWOS	S4112F Dell Networking Switch	1
	528-CKSS	OS10 Enterprise Software, S4112F	1
	343-BBJX	User Documentation EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungarian/Greek/Arab)	1
	750-ACVX	S4112F Install Kit	1
	750-ACVY	DELL Switch, Dual Tray Kit for S4112F, 1U	1
	750-ACWB	EMC GEN3 Switch Rail 22-31in Offset Kit, S4112F	1
	709-BDXY	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
6		PowerScale Switches	1

	210-AWOS	S4112F Dell Networking Switch	1
	528-CKSS	OS10 Enterprise Software, S4112F	1
	343-BBJX	User Documentation EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungarian/Greek/Arab)	1
	800-BBQV	Informational Purposes Only	1
	709-BDXY	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
7		PowerScale Archive/Hybrid Accessories	1
	210-AYYS	Accessories Virtual Base - VI	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	450-AJHP	PWCRD KIT for Normal Chassis	2
	470-AFFZ	100G to 25G Breakout (4)SFP28 to (1)Q28 DAC 3M	2
8		PowerScale Services	1
	210-AYWM	PowerScale Services	1
	519-BGJS	ProDeploy Additional Deployment Time: 8 Hours Onsite File and Object Storage Tech Resource	1
	519-BDCB	ProDeploy Plus Addon PowerScale Enterprise Bundle	1
9		PowerScale A310	4
	210-BQVB	A310 L3 ISE Node	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	400-BTCL	ISE 240TB (15x16TB)	1
	400-BTCZ	ISE 800GB SSD - A310/0	2
	590-TFQM	2x25GbE (SFP28) W/O OPTICS	1
	590-TFQJ	2x25GbE (SFP28) Back-end W/O OPTICS	1
	407-BCIU	Transceivers/Optic/SFP+/SR/10GbE/2 GEN6	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	709-BDXM	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	683-BBNR	ProDeploy Plus PowerScale Node	1
10		PowerScale Archive/Hybrid Chassis	1
	210-BQWX	Base Chassis - Normal A31-Series	1
	350-BDGL	4U Bezel UDS	1
	709-BDXL	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
11		PowerScale Hybrid Additional Software	4
	210-BQVG	PowerScale Hybrid Software - VP	1
	800-BBQV	Informational Purposes Only	1

	800-BBQV	Informational Purposes Only	1
	151-BCLV	SmartQuotas Base License Bundle A310/A3100 L3 =ID	1
	151-BCMG	SnapShotIQ Base License Bundle A310/A3100 L3 =ID	1
	151-BCMY	Enterprise Bundle A310/A3100 L3=ID	1
	151-BCHY	SmartQuotas Capacity License Bundle A3 Tier 3 L3=CB	240
	151-BCJP	SnapShotIQ Capacity License Bundle A3 L3=CB	240
	151-BCMT	Enterprise Bundle Capacity A310/A3100 L3=CB	240
	151-BBEH	HDFS for OneFS ($0.00)	1
	800-BBQV	Informational Purposes Only	1
	151-BCKV	SmartDedupe Base License A310/A3100 L3=ID	1
	151-BCKC	SmartDedupe Capacity License A310/A3100 L3=CB	240
	487-BDZG	ProSupport Plus Additional Software Support-Maintenance, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
12		PowerScale Archive/Hybrid OE Software	4
	210-BQVG	PowerScale Hybrid Software - VP	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	149-BCCY	OneFS Base License A310/A3100 12-20TB L3=ID	1
	800-BBQV	Informational Purposes Only	1
	149-BCCW	OneFS Capacity A310/A3100 L3=CB	240
	800-BBQV	Informational Purposes Only	1
	487-BEBP	ProSupport Plus OneFS Hybrid Software Support-Maintenance, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
13		PowerScale Switches	1
	210-AWOS	S4112F Dell Networking Switch	1
	528-CKSS	OS10 Enterprise Software, S4112F	1
	343-BBJX	User Documentation EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungarian/Greek/Arab)	1
	750-ACVX	S4112F Install Kit	1
	750-ACVY	DELL Switch, Dual Tray Kit for S4112F, 1U	1
	750-ACWB	EMC GEN3 Switch Rail 22-31in Offset Kit, S4112F	1
	709-BDXY	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	800-BBQV	Informational Purposes Only	1
14		PowerScale Switches	1
	210-AWOS	S4112F Dell Networking Switch	1
	528-CKSS	OS10 Enterprise Software, S4112F	1
	343-BBJX	User Documentation EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungarian/Greek/Arab)	1
	800-BBQV	Informational Purposes Only	1
	709-BDXY	Parts Only Warranty 36 Months, 36 Month(s)	1
	199-BJZR	Prosupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1

	800-BBQV	Informational Purposes Only	1
15		PowerScale Archive/Hybrid Accessories	1
	210-AYYS	Accessories Virtual Base - VI	1
	800-BBQV	Informational Purposes Only	1
	800-BBQV	Informational Purposes Only	1
	450-AJHP	PWCRD KIT for Normal Chassis	2
	470-AFFZ	100G to 25G Breakout (4)SFP28 to (1)Q28 DAC 3M	2
16		PowerScale Services	1
	210-AYWM	PowerScale Services	1
	519-BGJS	ProDeploy Additional Deployment Time: 8 Hours Onsite File and Object Storage Tech Resource	1
	519-BDCB	ProDeploy Plus Addon PowerScale Enterprise Bundle	1
Canonical Ubuntu			
OS	Canonical	Ubuntu pro for enterprises with Infra support 24x7	
Product Number	**Description**	**Description**	
Backup	CV-UBKRC-FT-31	Commvault Cloud Backup & Recovery Software for Unstructured Data, Per Front-End Terabyte, Subscription 3 - Year, Upfront Payment	900
	PS	Commvault Professional Services for Implementation	Lot
#	SKU	Dell Hardware for Commvault	Qty
1		ME5084 - Full Configuration - [EMEA_ME5084]	1
	210-BBSE	Dell ME5084 Storage Array	1
	340-DCJI	PowerVault MExxxx Shipping, EMEA1	1
	389-EEUQ	PowerVault ME 5U-84, CE Label Marking	1
	403-BCPV	32Gb FC Type-B 8 Port Dual 5U Controller	1
	492-BDCW	2X SFP+, FC32, 32GB	1
	492-BDCW	2X SFP+, FC32, 32GB	1
	492-BDCW	2X SFP+, FC32, 32GB	1
	492-BDCW	2X SFP+, FC32, 32GB	1
	161-BCNL	24TB Hard Drive 12Gbps SAS ISE 7.2K 512e 3.5in Hot-Plug, AG Drive	70
	770-BCVH	Rack Rails 5U	1
	450-ALXP	Power Supply, 2200W, Redundant, WW	1
	450-AEJI	C19 to C20, PDU Style, 2.5M Power Cord	2
	199-BIBF	ProSupport Plus and 4Hr Mission Critical Initial, 36 Month(s)	1
	709-BDHL	Parts Only Warranty 36 Months	1
	683-BCNS	ProDeploy Plus Storage ME 5XXX 5U	1
2		PowerEdge R470 - Full Configuration - [EMEA_R470]	2
	210-BNMR	PowerEdge R470 Server, Enterprise	1
	321-BLDY	2.5" Chassis with up to 8 Hard Drives (SAS/SATA), Smart Flow, Rear IO, H965i	1

338-CTBL	Intel Xeon 6 Performance 6521P 2.6G, 24C/48T, 144M Cache, Turbo, (225W) DDR5-6400	1
412-BBLP	Extended heatsink with DIMM blanks	1
370-AAIP	Performance Optimized	1
370-BCCX	6400MT/s RDIMMs	1
370-BCCY	32GB RDIMM, 6400MT/s, Dual Rank	8
780-BCDS	Unconfigured RAID	1
403-BDMY	PERC H965i Controller, Front, DCMHS	1
400-AXSK	3.84TB SSD SATA Read Intensive 6Gbps 512e 2.5in Hot-plug AG Drive, 1 DWPD	4
384-BBBH	Power Saving BIOS Settings	1
800-BBDM	UEFI BIOS Boot Mode with GPT Partition	1
384-BDQL	PowerEdge 1U High Performance Silver Fan	1
450-BCWW	Dual,Redundant(1+1),Hot-PlugMHSPowerSupply,800WMM(100-240Vac)	1
450-AADY	C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord	2
330-BCWK	Riser Config 6, 2x16 FH Slots (Gen5), 1x16 Onboard OCP	1
330-BCYF	PowerEdge R470 Motherboard fo RTS 1.1, ROW	1
540-BFPV	Broadcom 57414 Dual Port 25GbE SFP28 Adapter, OCP 3.0 NIC +Sec	1
780-BCZQ	No OCP Blanks or Cables Required	1
540-BFXP	Broadcom 57414 25GbE SFP28 Dual Port Adapter, PCIe Full Height +Sec	1
406-BBXN	Marvell QLE2772 Dual Port Fibre Channel 32Gbps HBA Adapter, PCIe Full Height +Sec	1
470-AEYU	No Cables Required	1
325-BFXF	PowerEdge 1U Standard Bezel	1
350-BDDK	Dell Luggage Tag for x8 and x10 Chassis	1
470-BCHM	Rear Filler Blank for BOSS/OCP	1
605-BBFL	Enterprise Linux OS, Non Factory Installed, Requires Subscription Selection	1
605-BBFN	No Media Required	1
528-CHFN	RHEL, 1-2SKT,3yr Premium Subscription,Virtual Datacenters, Digitally Fulfilled	1
634-CSHS	Secure Enterprise Key Manager License 3.0	1
634-CSHT	Secured Component Verification	1
634-CSHY	iDRAC10, Enterprise 17G	1
379-BFXS	Dell Connectivity Client - Enabled	1
634-CZRP	Dell Connectivity Module 17G	1
350-BCYJ	Blank Left Ear Module	1
379-BETE	iDRAC Force Change Password for OCP cards	1
770-BECD	ReadyRails Sliding Rails (A15)	1
340-DRWG	PowerEdge Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew)	1
340-DSJD	PowerEdge R470 Shipping	1
340-DNSY	PowerEdge 1U Shipping Material	1
389-FHHX	PowerEdge CCC, No CE Label Marking	1

	407-BBXX	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	4
	709-BBIX	Parts Only Warranty 12 Months	1
	865-BBLP	ProSupport Plus and 4Hr Mission Critical Extension, 24 Month(s)	1
	865-BBLQ	ProSupport Plus and 4Hr Mission Critical Initial, 12 Month(s)	1
	683-BBGH	ProDeploy Plus PowerEdge R Series 1u2u	1
Description		Services	
DU Services		Professional Services	Lot

- Backup storage required **1,200TB**
- 2x Media agent server
  - 24x CPU
  - 192GB memory
  - 10.2TB SSD
  - 2x 2-port 10/25GB network card
  - 1x 2-port FC HBA
  - RedHat OS

7.6.2 Option 2 - Cisco on Nutanix

7.6.2.1 Cisco on Nutanix for Elastic

Line Number	Part Number	Description	Qty
	PrimarySite_InternetTraffic		
1.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
1.1	HCINX220C-M8E3S	Cisco Compute Hyperconverged HCI 220cM8 E3.S Nutanix Node	13
1.1.0.1	CON-SNTP-HCINXE3S	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 220cM8	13
1.1.1	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	13
1.1.2	HCI-CPU-I6767P	Intel I6767P 2.4GHz/350W 64C/336MB DDR5 6400MT/s	26
1.1.3	HCI-MRX96G2RF5	96GB DDR5-6400 RDIMM 2Rx4 (24Gb)	208
1.1.4	HCI-NVE115T3K1V	15.3TB E3.S1T KCD8XPJE HgPerf MedEnd Gen5 1X NVMe (SIE SCEF)	91
1.1.5	HCI-P-V5Q50G	Cisco VIC 15425 4x 10/25/50G PCIe C-Series w/Secure Boot	13
1.1.6	COMPUTE-OTHER	Compute Other Use Case	13
1.1.7	NTNX-HCI	Nutanix HCI Use Case	13
1.1.8	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	13
1.1.9	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	13

1.1.10	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	13
1.1.11	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	13
1.1.12	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	208
1.1.13	UCSC-LPC25-1485-D	Low profile bracket for VIC15425	13
1.1.14	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	26
1.1.15	UCSC-E3S1T-F	UCS C-Series E3.S 1T Drive Filler	117
1.1.16	CBL-E3S-220M8-P1	C220M8 Y cable MB P1 to E3.S BP	13
1.1.17	CBL-E3S-220M8-P2	C220M8 Y cable MB P2 to E3.S BP	13
1.1.18	CBL-E3S-220M8-P3	C220M8 Y cable MB P3 to E3.S BP	13
1.1.19	CBL-E3S-220M8-P4	C220M8 Y cable MB P4 to E3.S BP	13
1.1.20	UCSC-M2I-220M8	UCS C220 M8 internal M.2 module	13
1.1.21	HCI-M2-480G	480GB M.2 SATA SSD	26
1.1.22	UCSC-FBRS-C220-D	C220M7 HH Riser3 blank	13
1.1.23	UCSC-FBRS2-C220M7	C220 M7 Riser2 HH Filler Blank	13
1.1.24	HCI-RIS1A-220M8	HCI C220 M8 Riser 1A PCIe Gen5 x16 HH	13
1.1.25	HCI-MLOM	Cisco VIC Connectivity	13
1.1.26	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	13
1.1.27	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	26
1.1.28	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	26
1.2	NTX-SW	Nutanix Software 3Y and above	1
1.2.1	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
1.2.2	NT-NCI-PRO-PR	NCI Pro SW LIC & Production SW Supp per Core	1664
1.3	NTX-NCI-USE-CASE	Nutanix NCI Software License Use case	1
1.3.1	NT-ON-PREM-UCS	Use Case to License Nutanix SW on Certified Cisco UCS HW	1
1.4	CNDL-DESELECT-D	Conditional Deselect	1
1.4.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
	MainObjects_InternetTraffic_DNSTraffic		
2.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
2.1	HCINX240C-M8L	Cisco Compute Hyperconverged HCI 240cM8 LFF Nutanix Node	7

2.1.0.1	CON-SNTP-HCIN2M8L	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 240cM8	7
2.1.1	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	7
2.1.2	HCI-CPU-I6515P	Intel I6515P 2.3GHz/150W 16C/72MB DDR5 6400MT/s	14
2.1.3	HCI-MRX16G1RE5	16GB DDR5-6400 RDIMM 1Rx8 (16Gb)	112
2.1.4	HCI-HDL24TW1S74K	24TB 3.5in 12G SAS 7.2K RPM 4K Front Load WD HDD	56
2.1.5	HCI-HDM24TW1S74K	24TB 3.5in 12G SAS 7.2K RPM 4K Top Load WD HDD	14
2.1.6	HCI-P-V5Q50G	Cisco VIC 15425 4x 10/25/50G PCIe C-Series w/Secure Boot	7
2.1.7	NTNX-NUS	Nutanix Unified Storage (NUS) Use Case	7
2.1.8	HCI-HBAMP1LL32	24G Tri-Mode M1 HBA for 32 LFF Drives	7
2.1.9	HCI-SD76TKA1X-EV	7.6TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	14
2.1.10	HCI-SD76TKA1X-EV	7.6TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	14
2.1.11	HCI-M2-480G	480GB M.2 SATA SSD	14
2.1.12	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	7
2.1.13	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	7
2.1.14	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	7
2.1.15	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	7
2.1.16	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	14
2.1.17	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	112
2.1.18	UCSC-FBRS3-C245	C245 M8 2U Riser3 Filler Blank, Non-Perforated	7
2.1.19	UCSC-BBLKD-L3	C-Series M8 LFF drive blanking panel	28
2.1.20	CBL-RISB-C240M8L	C240M8 LFF cable RAID to Riser 1B&3B	7
2.1.21	CBL-MP-240M8L-C	C240M8 LFF CFG cable Riser1B to MP	7
2.1.22	CBL-MP-240M8L-P	C240M8 LFF PWR cable Riser1B to MP	7
2.1.23	UCSC-MPKIT-240M8L	UCS C240M8L MID PLANE KIT 4x3.5" HDD	7
2.1.24	UCSC-M2I-240M8L	UCS C240 M8L Internal M.2 module	7

2.1.25	HCI-RIS1B-240M8	HCI C240 M8 Riser 1B support 2xSFF drives	7
2.1.26	HCI-RIS3B-240M8	HCI C240 M8 Riser 3B support 2xSFF drives (CPU2)	7
2.1.27	HCI-RIS2A-240M8	HCI C240 M8 Riser 2A PCIe Gen5 (x8, x16, x8) (CPU2)	7
2.1.28	HCI-MLOM	Cisco VIC Connectivity	7
2.1.29	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	7
2.1.30	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	14
2.1.31	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	14
2.2	NTX-SW	Nutanix Software 3Y and above	1
2.2.1	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
2.2.2	NT-NCM-STR-PR	NCM Starter SW LIC & Production SW Supp per Core	224
2.2.3	NT-NUS-STR-PR	NUS Starter SW License & Production SW Supp for 1 TiB	700
2.3	CNDL-DESELECT-D	Conditional Deselect	1
2.3.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
	DRSite_InternetTraffic		
3.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
3.1	HCINX220C-M8E3S	Cisco Compute Hyperconverged HCI 220cM8 E3.S Nutanix Node	4
3.1.0.1	CON-SNTP-HCINXE3S	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 220cM8	4
3.1.1	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	4
3.1.2	HCI-P-V5Q50G	Cisco VIC 15425 4x 10/25/50G PCIe C-Series w/Secure Boot	4
3.1.3	NTNX-HCI	Nutanix HCI Use Case	4
3.1.4	HCI-M2-480G	480GB M.2 SATA SSD	8
3.1.5	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	4
3.1.6	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	4
3.1.7	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	4

3.1.8	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	4
3.1.9	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	64
3.1.10	UCSC-FBRS-C220-D	C220M7 HH Riser3 blank	4
3.1.11	UCSC-LPC25-1485-D	Low profile bracket for VIC15425	4
3.1.12	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	8
3.1.13	UCSC-FBRS2-C220M7	C220 M7 Riser2 HH Filler Blank	4
3.1.14	UCSC-E3S1T-F	UCS C-Series E3.S 1T Drive Filler	40
3.1.15	CBL-E3S-220M8-P1	C220M8 Y cable MB P1 to E3.S BP	4
3.1.16	CBL-E3S-220M8-P2	C220M8 Y cable MB P2 to E3.S BP	4
3.1.17	CBL-E3S-220M8-P3	C220M8 Y cable MB P3 to E3.S BP	4
3.1.18	CBL-E3S-220M8-P4	C220M8 Y cable MB P4 to E3.S BP	4
3.1.19	UCSC-M2I-220M8	UCS C220 M8 internal M.2 module	4
3.1.20	HCI-RIS1A-220M8	HCI C220 M8 Riser 1A PCIe Gen5 x16 HH	4
3.1.21	HCI-MLOM	Cisco VIC Connectivity	4
3.1.22	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	4
3.1.23	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	8
3.1.24	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	8
3.1.25	COMPUTE-AI	Compute Artificial Intelligence Use Case	4
3.1.26	HCI-CPU-I6767P	Intel I6767P 2.4GHz/350W 64C/336MB DDR5 6400MT/s	8
3.1.27	HCI-MRX96G2RF5	96GB DDR5-6400 RDIMM 2Rx4 (24Gb)	64
3.1.28	HCI-NVE115T3K1V	15.3TB E3.S1T KCD8XPJE HgPerf MedEnd Gen5 1X NVMe (SIE SCEF)	24
3.2	NTX-SW	Nutanix Software 3Y and above	1
3.2.1	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
3.2.2	NT-NCI-PRO-PR	NCI Pro SW LIC & Production SW Supp per Core	512
3.3	NTX-NCI-USE-CASE	Nutanix NCI Software License Use case	1
3.3.1	NT-ON-PREM-UCS	Use Case to License Nutanix SW on Certified Cisco UCS HW	1
3.4	CNDL-DESELECT-D	Conditional Deselect	1
3.4.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
	DRObjects_InternetTraffic_DNSTraffic		

4.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
4.1	HCINX240C-M8L	Cisco Compute Hyperconverged HCI 240cM8 LFF Nutanix Node	5
4.1.0.1	CON-SNTP-HCIN2M8L	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 240cM8	5
4.1.1	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	5
4.1.2	HCI-CPU-I6520P	Intel I6520P 2.4GHz/210W 24C/144MB DDR5 6400MT/s	10
4.1.3	HCI-SD76TKA1X-EV	7.6TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	10
4.1.4	HCI-HDL20TT1S74K	20TB 3.5in 12G SAS 7.2K RPM 4K Toshiba HDD	50
4.1.5	HCI-P-V5Q50G	Cisco VIC 15425 4x 10/25/50G PCIe C-Series w/Secure Boot	5
4.1.6	NTNX-NUS	Nutanix Unified Storage (NUS) Use Case	5
4.1.7	HCI-MRX16G1RE5	16GB DDR5-6400 RDIMM 1Rx8 (16Gb)	80
4.1.8	HCI-HBAMP1LL32	24G Tri-Mode M1 HBA for 32 LFF Drives	5
4.1.9	HCI-SD76TKA1X-EV	7.6TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	10
4.1.10	HCI-M2-480G	480GB M.2 SATA SSD	10
4.1.11	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	5
4.1.12	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	5
4.1.13	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	5
4.1.14	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	5
4.1.15	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	10
4.1.16	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	80
4.1.17	UCSC-FBRS3-C245	C245 M8 2U Riser3 Filler Blank, Non-Perforated	5
4.1.18	UCSC-BBLKD-L3	C-Series M8 LFF drive blanking panel	10
4.1.19	CBL-RISB-C240M8L	C240M8 LFF cable RAID to Riser 1B&3B	5
4.1.20	CBL-MP-240M8L-C	C240M8 LFF CFG cable Riser1B to MP	5
4.1.21	CBL-MP-240M8L-P	C240M8 LFF PWR cable Riser1B to MP	5
4.1.22	UCSC-GPUAD-240M8L	GPU AIR DUCT FOR C240M8 LFF	5
4.1.23	UCSC-M2I-240M8L	UCS C240 M8L Internal M.2 module	5

4.1.24	HCI-RIS1B-240M8	HCI C240 M8 Riser 1B support 2xSFF drives	5
4.1.25	HCI-RIS3B-240M8	HCI C240 M8 Riser 3B support 2xSFF drives (CPU2)	5
4.1.26	HCI-RIS2A-240M8	HCI C240 M8 Riser 2A PCIe Gen5 (x8, x16, x8) (CPU2)	5
4.1.27	HCI-MLOM	Cisco VIC Connectivity	5
4.1.28	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	5
4.1.29	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	10
4.1.30	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	10
4.2	NTX-SW	Nutanix Software 3Y and above	1
4.2.1	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
4.2.2	NT-NCM-STR-PR	NCM Starter SW LIC & Production SW Supp per Core	240
4.2.3	NT-NUS-STR-PR	NUS Starter SW License & Production SW Supp for 1 TiB	150
4.3	CNDL-DESELECT-D	Conditional Deselect	1
4.3.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
5.0	DC-MGT-SAAS	Cisco Intersight SaaS	1
5.1	DC-MGT-IS-SAAS-ES	Infrastructure Services SaaS/CVA - Essentials	29
5.2	SVS-DCM-SUPT-BAS	Cisco Support Standard for DCM	1
5.3	DC-MGT-UCSC-1S	UCS Central Per Server - 1 Server License	29
5.4	DC-MGT-ADOPT-BAS	Intersight - Virtual adopt session http://cs.co/requestCSS	1
6.0	SFP-25G-SR-S=	25GBASE-SR SFP Module	116
	Encryption License For Main Site Object Storage		
7.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
7.1	NTX-SW	Nutanix Software 3Y and above	1
7.1.1	NT-A-NUS-SEC-PR	NUS Security add-on SW LIC & Production SW Supp 1 TiB	700

7.1.2	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
7.2	CNDL-DESELECT-D	Conditional Deselect	1
7.2.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
	Encryption License For DR Object Storage		
8.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
8.1	NTX-SW	Nutanix Software 3Y and above	1
8.1.1	NT-A-NUS-SEC-PR	NUS Security add-on SW LIC & Production SW Supp 1 TiB	150
8.1.2	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
8.2	CNDL-DESELECT-D	Conditional Deselect	1
8.2.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
Services			
9.1	CNS-INF-A-SVC-DEP-ONP-AHV	Service, Infrastructure Deployment - On-Premises NCI Cluster - Nutanix AHV with In-person Delivery. For each quantity purchased, deployment is limited to 1 node. A maximum of 64 nodes distributed in up to 4 on-premises NCI clusters of a single hypervisor type at a single physical site. Delivery: In-person Deployment including in-person rack and stack of on-premises NCI cluster nodes.	26
9.2	CNS-INF-A-SVC-DRD-LEAP	Service, Nutanix NCI Disaster Recovery Deployment with Async/NearSync Replication with Protection Policies and Recovery Plans. For each quantity purchased, deployment is limited to one source cluster and one target cluster. Source and target clusters can be a combination of on-premises NCI or NC2 clusters.	1

9.3	CNS-INF-A-WRK-DSGN-ADV-MS-SD-INP	Service, Infrastructure Design Advanced Edition for Multisite with Standard Documentation and In-person Delivery. For each quantity purchased, design is limited to a single production environment spanning multiple physical sites, public cloud regions, availability zones, or resource locations. Design is limited to 2 distinct site patterns, though multiple instances of each pattern can be deployed (common for hub-spoke or branch office architectures). Delivery: In-person Workshop and Virtual Documentation.	1
9.4	CNS-NUS-A-SVC-DEP-ESS-OBJ	Service, Nutanix Unified Storage Deployment Essential Edition for Objects. For each quantity purchased, deployment is limited to a single instance of NUS Objects on an on-premises NCI or NC2 cluster deployed within a single physical site.	4
9.5	CNS-NUS-A-WRK-DSGN-ESS-OBJ	Service, Nutanix Unified Storage Design Workshop Essential Edition for Objects. For each quantity purchased, design is limited to a single instance of NUS Objects on an on-premises NCI or NC2 cluster deployed within a single physical site.	1
9.6	FLEX-CST-CR	Service, Nutanix Professional Services Flex Credits. Pre-paid fees for Nutanix Professional Services.	500
Backup			
	Commvault	Commvault HW+SW+Services+Cyber Resiliency	500 TB
10.1			
Canonical Ubuntu			
	Canonical	Ubuntu pro for enterprises with Infra support 24x7	

7.6.2.2 Cisco on Nutanix for FortiSIEM

Line Number	Part Number	Description	Qty

	Main - Forti SIEM		
1.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
1.1	HCINX220C-M8E3S	Cisco Compute Hyperconverged HCI 220cM8 E3.S Nutanix Node	8
1.1.0.1	CON-SNTP-HCINXE3S	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 220cM8	8
1.1.1	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	8
1.1.2	HCI-CPU-I6767P	Intel I6767P 2.4GHz/350W 64C/336MB DDR5 6400MT/s	16
1.1.3	HCI-P-V5Q50G	Cisco VIC 15425 4x 10/25/50G PCIe C-Series w/Secure Boot	8
1.1.4	COMPUTE-OTHER	Compute Other Use Case	8
1.1.5	HCI-M2-480G	480GB M.2 SATA SSD	16
1.1.6	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	8
1.1.7	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	8
1.1.8	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	8
1.1.9	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	8
1.1.10	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	192
1.1.11	UCSC-FBRS-C220-D	C220M7 HH Riser3 blank	8
1.1.12	UCSC-LPC25-1485-D	Low profile bracket for VIC15425	8
1.1.13	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	16
1.1.14	UCSC-FBRS2-C220M7	C220 M7 Riser2 HH Filler Blank	8
1.1.15	UCSC-E3S1T-F	UCS C-Series E3.S 1T Drive Filler	64
1.1.16	CBL-E3S-220M8-P1	C220M8 Y cable MB P1 to E3.S BP	8
1.1.17	CBL-E3S-220M8-P2	C220M8 Y cable MB P2 to E3.S BP	8
1.1.18	CBL-E3S-220M8-P3	C220M8 Y cable MB P3 to E3.S BP	8
1.1.19	CBL-E3S-220M8-P4	C220M8 Y cable MB P4 to E3.S BP	8
1.1.20	UCSC-M2I-220M8	UCS C220 M8 internal M.2 module	8
1.1.21	HCI-RIS1A-220M8	HCI C220 M8 Riser 1A PCIe Gen5 x16 HH	8
1.1.22	HCI-MLOM	Cisco VIC Connectivity	8
1.1.23	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	8
1.1.24	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	16
1.1.25	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	16
1.1.26	NTNX-HCI	Nutanix HCI Use Case	8

1.1.27	HCI-MRX64G2RE5	64GB DDR5-6400 RDIMM 2Rx4 (16Gb)	64
1.1.28	HCI-NVE17T6K1V	7.6TB E3.S1T KCD8XPJE HgPerf MedEnd Gen5 1X NVMe (SIE SCEF)	64
1.2	NTX-SW	Nutanix Software 3Y and above	1
1.2.1	NT-NCI-PRO-PR	NCI Pro SW LIC & Production SW Supp per Core	1024
1.2.2	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
1.3	NTX-NCI-USE-CASE	Nutanix NCI Software License Use case	1
1.3.1	NT-ON-PREM-UCS	Use Case to License Nutanix SW on Certified Cisco UCS HW	1
1.4	CNDL-DESELECT-D	Conditional Deselect	1
1.4.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
	DR - Forti SIEM		
2.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
2.1	NTX-SW	Nutanix Software 3Y and above	1
2.1.1	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
2.1.2	NT-NCI-PRO-PR	NCI Pro SW LIC & Production SW Supp per Core	512
2.2	NTX-NCI-USE-CASE	Nutanix NCI Software License Use case	1
2.2.1	NT-ON-PREM-UCS	Use Case to License Nutanix SW on Certified Cisco UCS HW	1
2.3	CNDL-DESELECT-D	Conditional Deselect	1
2.3.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
2.4	HCINX220C-M8E3S	Cisco Compute Hyperconverged HCI 220cM8 E3.S Nutanix Node	4
2.4.0.1	CON-SNTP-HCINXE3S	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 220cM8	4
2.4.1	COMPUTE-OTHER	Compute Other Use Case	4
2.4.2	NTNX-HCI	Nutanix HCI Use Case	4
2.4.3	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	4
2.4.4	HCI-MRX64G2RE5	64GB DDR5-6400 RDIMM 2Rx4 (16Gb)	64
2.4.5	HCI-NVE115T3K1V	15.3TB E3.S1T KCD8XPJE HgPerf MedEnd Gen5 1X NVMe (SIE SCEF)	32
2.4.6	HCI-M2-480G	480GB M.2 SATA SSD	8
2.4.7	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	4
2.4.8	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	4

2.4.9	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	4
2.4.10	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	4
2.4.11	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	64
2.4.12	UCSC-FBRS-C220-D	C220M7 HH Riser3 blank	4
2.4.13	UCSC-LPC25-1485-D	Low profile bracket for VIC15425	4
2.4.14	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	8
2.4.15	UCSC-FBRS2-C220M7	C220 M7 Riser2 HH Filler Blank	4
2.4.16	UCSC-E3S1T-F	UCS C-Series E3.S 1T Drive Filler	32
2.4.17	CBL-E3S-220M8-P1	C220M8 Y cable MB P1 to E3.S BP	4
2.4.18	CBL-E3S-220M8-P2	C220M8 Y cable MB P2 to E3.S BP	4
2.4.19	CBL-E3S-220M8-P3	C220M8 Y cable MB P3 to E3.S BP	4
2.4.20	CBL-E3S-220M8-P4	C220M8 Y cable MB P4 to E3.S BP	4
2.4.21	UCSC-M2I-220M8	UCS C220 M8 internal M.2 module	4
2.4.22	HCI-CPU-I6767P	Intel I6767P 2.4GHz/350W 64C/336MB DDR5 6400MT/s	8
2.4.23	HCI-RIS1A-220M8	HCI C220 M8 Riser 1A PCIe Gen5 x16 HH	4
2.4.24	HCI-MLOM	Cisco VIC Connectivity	4
2.4.25	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	4
2.4.26	HCI-P-V5Q50G	Cisco VIC 15425 4x 10/25/50G PCIe C-Series w/Secure Boot	4
2.4.27	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	8
2.4.28	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	8
	NFS Main DC		
3.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1
3.1	HCINX240C-M8L	Cisco Compute Hyperconverged HCI 240cM8 LFF Nutanix Node	6
3.1.0.1	CON-SNTP-HCIN2M8L	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 240cM8	6
3.1.1	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	6
3.1.2	HCI-CPU-I6515P	Intel I6515P 2.3GHz/150W 16C/72MB DDR5 6400MT/s	12
3.1.3	HCI-MRX16G1RE5	16GB DDR5-6400 RDIMM 1Rx8 (16Gb)	96
3.1.4	HCI-HDL24TW1S74K	24TB 3.5in 12G SAS 7.2K RPM 4K Front Load WD HDD	60
3.1.5	NTNX-NUS	Nutanix Unified Storage (NUS) Use Case	6
3.1.6	HCI-HBAMP1LL32	24G Tri-Mode M1 HBA for 32 LFF Drives	6
3.1.7	HCI-M2-480G	480GB M.2 SATA SSD	12

3.1.8	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	6
3.1.9	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	6
3.1.10	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	6
3.1.11	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	6
3.1.12	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	12
3.1.13	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	96
3.1.14	UCSC-FBRS3-C245	C245 M8 2U Riser3 Filler Blank, Non-Perforated	6
3.1.15	UCSC-BBLKD-L3	C-Series M8 LFF drive blanking panel	12
3.1.16	CBL-RISB-C240M8L	C240M8 LFF cable RAID to Riser 1B&3B	6
3.1.17	CBL-MP-240M8L-C	C240M8 LFF CFG cable Riser1B to MP	6
3.1.18	CBL-MP-240M8L-P	C240M8 LFF PWR cable Riser1B to MP	6
3.1.19	UCSC-M2I-240M8L	UCS C240 M8L Internal M.2 module	6
3.1.20	HCI-RIS3B-240M8	HCI C240 M8 Riser 3B support 2xSFF drives (CPU2)	6
3.1.21	HCI-MLOM	Cisco VIC Connectivity	6
3.1.22	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	6
3.1.23	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	12
3.1.24	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	12
3.1.25	HCI-SD15TKA1X-EV	15.3TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	12
3.1.26	HCI-SD15TKA1X-EV	15.3TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	12
3.1.27	UCSC-FBRS2-C240-D	C240 M7/M8 2U Riser2 Filler Blank	6
3.1.28	UCSC-GPUAD-240M8L	GPU AIR DUCT FOR C240M8 LFF	6
3.1.29	HCI-RIS1B-240M8	HCI C240 M8 Riser 1B support 2xSFF drives	6
3.2	NTX-SW	Nutanix Software 3Y and above	1
3.2.1	NT-NUS-PRO-PR	NUS Pro SW License & Production SW Supp for 1 TiB	700
3.2.2	NT-NCM-STR-PR	NCM Starter SW LIC & Production SW Supp per Core	192
3.2.3	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
3.3	CNDL-DESELECT-D	Conditional Deselect	1
3.3.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
	NFS DR		
4.0	HCI-M8-NTNX-MLB	Cisco Compute Hyperconverged M8 with Nutanix MLB	1

4.1	HCINX240C-M8L	Cisco Compute Hyperconverged HCI 240cM8 LFF Nutanix Node	6
4.1.0.1	CON-SNTP-HCIN2M8L	SNTC-24X7X4 Cisco Compute Hyperconverged HCI 240cM8	6
4.1.1	HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	6
4.1.2	HCI-CPU-I6515P	Intel I6515P 2.3GHz/150W 16C/72MB DDR5 6400MT/s	12
4.1.3	HCI-MRX16G1RE5	16GB DDR5-6400 RDIMM 1Rx8 (16Gb)	96
4.1.4	HCI-HDL24TW1S74K	24TB 3.5in 12G SAS 7.2K RPM 4K Front Load WD HDD	60
4.1.5	NTNX-NUS	Nutanix Unified Storage (NUS) Use Case	6
4.1.6	HCI-HBAMP1LL32	24G Tri-Mode M1 HBA for 32 LFF Drives	6
4.1.7	HCI-M2-480G	480GB M.2 SATA SSD	12
4.1.8	HCI-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	6
4.1.9	HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	6
4.1.10	HCI-TPM-002D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	6
4.1.11	HCI-AOSAHV-73-SWK9	HCI AOS AHV 7.3 SW	6
4.1.12	UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	12
4.1.13	UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	96
4.1.14	UCSC-FBRS3-C245	C245 M8 2U Riser3 Filler Blank, Non-Perforated	6
4.1.15	UCSC-BBLKD-L3	C-Series M8 LFF drive blanking panel	12
4.1.16	CBL-RISB-C240M8L	C240M8 LFF cable RAID to Riser 1B&3B	6
4.1.17	CBL-MP-240M8L-C	C240M8 LFF CFG cable Riser1B to MP	6
4.1.18	CBL-MP-240M8L-P	C240M8 LFF PWR cable Riser1B to MP	6
4.1.19	UCSC-M2I-240M8L	UCS C240 M8L Internal M.2 module	6
4.1.20	HCI-RIS3B-240M8	HCI C240 M8 Riser 3B support 2xSFF drives (CPU2)	6
4.1.21	HCI-MLOM	Cisco VIC Connectivity	6
4.1.22	HCI-M-V5Q50GV2	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	6
4.1.23	HCI-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	12
4.1.24	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	12
4.1.25	HCI-SD15TKA1X-EV	15.3TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	12
4.1.26	HCI-SD15TKA1X-EV	15.3TB 2.5in Enter Value 24G SAS Kioxia PM7 SSD (1X)	12
4.1.27	UCSC-FBRS2-C240-D	C240 M7/M8 2U Riser2 Filler Blank	6

4.1.28	UCSC-GPUAD-240M8L	GPU AIR DUCT FOR C240M8 LFF	6
4.1.29	HCI-RIS1B-240M8	HCI C240 M8 Riser 1B support 2xSFF drives	6
4.2	NTX-SW	Nutanix Software 3Y and above	1
4.2.1	SVS-NT-SUP	Entitlement ONLY for Nutanix Cloud Infrastructure SW	1
4.2.2	NT-NCM-STR-PR	NCM Starter SW LIC & Production SW Supp per Core	192
4.2.3	NT-NUS-PRO-PR	NUS Pro SW License & Production SW Supp for 1 TiB	700
4.3	CNDL-DESELECT-D	Conditional Deselect	1
4.3.1	OPTOUT-DISTI-ONLY	For Disti when ordering mandatory licenses separately	1
5.0	SFP-25G-SR-S=	25GBASE-SR SFP Module	96
6.0	DC-MGT-SAAS	Cisco Intersight SaaS	1
6.1	DC-MGT-IS-SAAS-ES	Infrastructure Services SaaS/CVA - Essentials	24
6.2	SVS-DCM-SUPT-BAS	Cisco Support Standard for DCM	1
6.3	DC-MGT-UCSC-1S	UCS Central Per Server - 1 Server License	24
6.4	DC-MGT-ADOPT-BAS	Intersight - Virtual adopt session http://cs.co/requestCSS	1
Services			
11.1	CNS-INF-A-SVC-DEP-ONP-AHV	Service, Infrastructure Deployment - On-Premises NCI Cluster - Nutanix AHV with In-person Delivery. For each quantity purchased, deployment is limited to 1 node. A maximum of 64 nodes distributed in up to 4 on-premises NCI clusters of a single hypervisor type at a single physical site. Delivery: In-person Deployment including in-person rack and stack of on-premises NCI cluster nodes.	26
11.2	CNS-INF-A-SVC-DRD-LEAP	Service, Nutanix NCI Disaster Recovery Deployment with Async/NearSync Replication with Protection Policies and Recovery Plans. For each quantity purchased, deployment is limited to one source cluster and one target cluster. Source and target clusters can be a combination of on-premises NCI or NC2 clusters.	1
11.3	CNS-INF-A-WRK-DSGN-ADV-MS-SD-INP	Service, Infrastructure Design Advanced Edition for Multisite with Standard Documentation and In-person Delivery. For each quantity purchased, design is limited to a single production environment spanning multiple physical sites, public cloud regions, availability zones, or resource locations. Design is limited to 2 distinct site patterns, though multiple	1

		instances of each pattern can be deployed (common for hub-spoke or branch office architectures). Delivery: In-person Workshop and Virtual Documentation.	
11.4	CNS-NUS-A-SVC-DEP-ESS-OBJ	Service, Nutanix Unified Storage Deployment Essential Edition for Objects. For each quantity purchased, deployment is limited to a single instance of NUS Objects on an on-premises NCI or NC2 cluster deployed within a single physical site.	4
11.5	CNS-NUS-A-WRK-DSGN-ESS-OBJ	Service, Nutanix Unified Storage Design Workshop Essential Edition for Objects. For each quantity purchased, design is limited to a single instance of NUS Objects on an on-premises NCI or NC2 cluster deployed within a single physical site.	1
11.6	FLEX-CST-CR	Service, Nutanix Professional Services Flex Credits. Pre-paid fees for Nutanix Professional Services.	500
Backup			
	Commvault	Commvault HW+SW+Services+Cyber Resiliency	1.2PB
12.1			
Canonical Ubuntu			
	Canonical	Ubuntu pro for enterprises with Infra support 24x7	

7.7 FortiSOAR

SOAR		
SOAR with 1 named and 5 concurrent Account (Analyst) with DR		
FC-10-SRVMS-390-02-36	FortiSOAR Multi-Tenant Subscription License 3 Year FortiSOAR Multi-Tenant Subscription plus FortiCare Premium and FortiCare Best Practice Service - 2 User Logins included	1
FC-10-SRVMS-1121-02-36	FortiSOAR HA Subscription License 3 Year FortiSOAR HA-only Subscription license plus FortiCare Premium, which will be limited to serve as the HA node in a clustered environment.	2
FC-10-SRVMS-384-02-36	FortiSOAR Enterprise & Multi Tenant Subscription License 3 Year FortiSOAR User Seat License Subscription - One Additional User Login	4
FC-10-SRVMS-592-02-36	FortiSOAR Threat Intel Management Service 3 Year Subscription Service for FortiSOAR Threat Intel Management Service including FortiGuard Premium Threat Feed.	1

7.8 S3 Storage - Optional

Main

Line Number	Part Number	Description	Service Duration (Months)	Estimated Lead Time (Days)
VAST for Main				
1.0	VAST-DATA-MLB	VAST Software and Hardware MLB	---	N/A
1.1	DC-MGT-SAAS	Cisco Intersight SaaS	---	N/A
1.1.1	DC-MGT-IS-SAAS-ES	Infrastructure Services SaaS/CVA - Essentials	---	3
1.1.2	SVS-DCM-SUPT-BAS	Cisco Support Standard for DCM	---	3
1.1.3	DC-MGT-UCSC-1S	UCS Central Per Server - 1 Server License	---	3
1.1.4	DC-MGT-ADOPT-BAS	Intersight - Virtual adopt session http://cs.co/requestCSS	---	3
1.2	UCSC-C225M8N-EBOX	UCS C225 M8 1U Rack Server for VAST EBOX	---	94
1.2.0.1	CON-SNTP-UCSC2M8X	SNTC-24X7X4 UCS C225 M8 1U Rack Server for VAST with	36	N/A
1.2.1	ISM-MANAGED	Deployment mode for C Series Servers in Standalone mode	---	21
1.2.2	UCS-CPU-A9454P	AMD 9454P 2.75GHz 290W 48C/256MB Cache DDR5 4800MT/s	---	35
1.2.3	UCS-MRX32G1RE3	32GB DDR5-5600 RDIMM 1Rx4 (16Gb)	---	21
1.2.4	UCSC-RIS1C-225M8	C225 M8 1U Riser 1C PCIe Gen5 x16 FH	---	56
1.2.5	UCSC-RIS3C-225M8	C225 M81U Riser 3C PCIe Gen5 x16 FH	---	21
1.2.6	UCSC-O-ID10GC-D	Intel X710T2LOCPV3G1L 2x10GbE RJ45 OCP3.0 NIC	---	21
1.2.7	UCS-NVB15T3O1L	15.3TB 2.5in U.2 15mm SolidigmP5316 HgPerf LowEnd <0.5X NVMe	---	21
1.2.8	UCS-NVB960M1H	960GB 2.5in U.3 15mm Micron XTR Hg Perf Ext End 60X NVMe	---	21
1.2.9	UCSC-P-N7D200GF	MCX755106AS-HEAT:CX-7 2x200GbE QSFP112 PCIe Gen5x16, VPI NIC	---	21
1.2.10	UCSC-P-N7D200GF	MCX755106AS-HEAT:CX-7 2x200GbE QSFP112 PCIe Gen5x16, VPI NIC	---	21
1.2.11	UCS-M2-960G-D	960GB M.2 SATA Micron G2 SSD	---	35
1.2.12	UCS-M2-HWRAID-D	Cisco Boot optimized M.2 Raid controller	---	21

1.2.13	UCSC-PSU1-1200W-D	1200w AC Titanium Power Supply for C-series Rack Servers	---	21
1.2.14	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	---	7
1.2.15	CIMC-LATEST-D	IMC SW (Recommended) latest release for C-Series Servers.	---	21
1.2.16	UCSC-RAIL-D	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	---	21
1.2.17	UCS-TPM2-002D-D	TPM 2.0 FIPS 140-2 MSW2022 compliant AMD M8 servers	---	21
1.2.18	UCSC-HSLP-C225M8	UCS C225 M8 Heatsink	---	21
1.2.19	UCSC-OCP3-KIT-D	C2XX OCP 3.0 Interposer W/Mech Assy	---	21
1.3	VAST-DATA-SPLUS	SolutionsPlus: VAST DATA Software and Services	---	N/A
1.3.1	VAST-SW-100TB	VAST Data software subscription (100TB)	---	3
1.3.2	VAST-SW-1CPU-CORE	VAST 1xCPU CORE	---	N/A
1.3.3	VAST-PS-COPILOT	Co-Pilot: Monitoring,Upgrades,Expansions,System Management	---	3
1.3.4	VAST-PS	Installation Services for VAST SW (Supports up to 12 Eboxes)	---	3
1.3.5	SAAS-OTHER	Other Use Case	---	3
1.4	N9K-C9332D-GX2B	Nexus 9300 Series, 32p 400G Switch	---	63
1.4.0.1	CON-SSSNP-N9KC9D3X	SOLN SUPP 24X7X4 Nexus 9300 Series, 32p 400G QSFP-DD	36	N/A
1.4.1	MODE-NXOS	Mode selection between ACI and NXOS	---	21
1.4.2	NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	---	14
1.4.3	NXOS-CS-10.6.1F	Nexus 9300, 9500, 9800 NX-OS SW 10.6.1 (64bit) Cisco Silicon	---	21
1.4.4	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	---	14
1.4.5	NXA-SFAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow /w EEPROM	---	14
1.4.6	NXA-PAC-1500W-PI	Nexus 1500W PSU port-side Intake	---	14
1.4.7	CAB-9K10A-UK	Power Cord, 250VAC 10A BS1363 Plug (13 A fuse), UK	---	7
1.4.8	NXOS-SLP-INFO-9K	Info PID for Smart Licensing using Policy for N9K	---	21

1.4.9	DCN-AI	Select if this product will be used for AI ML Applications	---	3
1.4.10	C1A1TN9300XF2-3Y	Data Center Networking Advantage Term N9300 XF2, 3Y	---	3
1.4.11	DCN-ADOPT-BAS	Nexus(DCN) - Virtual adopt session http://cs.co/requestCSS	---	3
1.4.12	SW-AI	Select if this product will be used for AI ML Applications	---	21
1.4.13	SVS-B-N9K-ADV-XF2	EMBEDDED SOLN SUPPORT SWSS FOR NEXUS 9K	---	3
1.5	QDD-2Q200-CU3M=	400G QSFP56-DD to 2x200G QSFP56 Copper Breakout Cable, 3m	---	17

DR

Sku	Description	Qty
DF-3015-V2	Ceres V2 Enclosure: 1U HA Enclosure (up to 60GB/s): incl. 338TB NVMe Flash, 6.4TB SCM, 2x Bluefield 3 DPUs, 4 x 200Gb/QSFP112 (ETH or IB)	1
1U-1N-GEN5-2NIC	Single Server 1U Chassis inc (Dual NIC, Dual Port 200Gb's QSFP112 or Dual Port HDR200 QSFP112)	3
AOC-CABLES	Fiber optic cables and SFPs	1
ETH-NVMEF-1X32-200G	1 * 32 Port 1U 200G NVMe Fabric Ethernet Switch	2

SKU	Description	Qty	TERM (Months)
SW-U-100	100TB Useable 1-Month Gemini Services Term	3	36
SW-CORE-1	Single CPU Core 1-Month Gemini Services Term Total CPU Core within the scope of this quote: The total required licensable CPU cores : 101	101	36
COPILOT		1	36
INSTALL	VAST Data Installation Services	1	

7.9 Building AI Automation Stack

7.9.1 Dell Hardware

Product Name	Module Name	Option Name	SKUs	Qty	Product Qty

EMEA_XE7740 - Full Configuration - [EMEA_XE7740]				3
	PowerEdge XE7740	PowerEdge XE7740	210-BPMK	1
	Chassis Configuration	XE7740 4U Chassis, 8 x E3.S NVMe	321-BLXN, 412-BCFN, 470-BCZG	1
	Processor	Intel® Xeon® 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	338-CSKJ	1
	Additional Processor	Intel® Xeon® 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400	338-CSKJ, 379-BDCO	1
	PCIe Riser	Riser Config 0-1, No Riser, No NVLINK Bridge, XE7740	330-BDCR	1
	Processor Thermal Config	Heatsink for 2 CPU Configuration	412-BCCN	1
	Memory Configuration Type	Performance Optimized	370-AAIP	1
	Memory DIMM Type and Speed	6400MT/s RDIMMs	370-BCCX	1
	Memory Capacity	32GB RDIMM, 6400MT/s, Dual Rank	370-BCCY	32
	RAID Configuration	C30, No RAID for NVME chassis	780-BCDO	1
	RAID/Internal Storage Controllers	No Controller	405-AACD	1
	Hard Drives	No Hard Drive	400-ABHL	1
	Hard Drives (PCIe SSD/Flex Bay)	1.92TB Data Center NVMe Read Intensive AG Drive E3s Gen5 with carrier	345-BKFR	2
	Power Management BIOS Settings	Performance BIOS Setting	384-BBBL	1
	Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition	800-BBDM	1
	Fans	PowerEdge 1U High Performance Platinum Fan	384-BDXS	1
	Power Supply	Octa, Redundant(4+4), Hot-Plug MHS Power Supply,	450-BDWV	1

		3200W MM HLAC (200-240Vac), Titanium		
	Power Cords	C19 to C20, 250V, 0.6m Power Cord	450-AAXT	8
	Motherboard	XE7740 System Motherboard	631-BCHH	1
	Multi Selection Network Adapter	No OCP Card, No Primary MAC Address	780-BCZG	1
	Bezel	PowerEdge 4U Standard Bezel	325-BGCM, 350-BDDP	1
	OCP 3.0 Accessories	No OCP - 1 Rear Blank	470-BCHM	1
	GPU Acceleration Cards	NVIDIA H200 NVL, PCIe, 450W for R-series, 600W for XE Servers, 141GB Passive, DW Full Height GPU	490-BKPN	8
	Additional Network Cards	Broadcom 57608 Dual Port 200G (Single Port 400GbE) QSFP112 Adapter, PCIe Full Height	540-BFFM	1
	GPU/FPGA/Acceleration Cables	GPU Factory Installed CEM Cables for DW GPU (8 GPUs) 600W	470-BDXH, 490-BLDK	1
	Boot Optimized Storage Cards	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80) Front	403-BDMM, 470-BCVT	1
	Optics and Cables for Network Adapters	Dell, Transceiver, 400GbE-Q112-EDR4, 2km MMF over 4 pair of SMF	407-BDHV	1
	Operating System	No Operating System	611-BBBF	1
	OS Media Kits	No Media Required	605-BBFN	1
	Embedded Systems Management	iDRAC10 Datacenter 17G with OpenManage Enterprise Advance Plus	634-CSGX, 634-CSHS, 634-CSHT, 634-CSHV	1
	Embedded Systems Management	Dell Connectivity Client - Enabled 17G	379-BFXS, 634-CZRP	1
	KVM	Blank Left Ear Module, XE774X	269-BBBH	1
	BMC Password	Legacy Password, No LOM, No OCP	379-BFRP	1
	Rack Rails	XE774x Sliding Ready Rail	770-BFPG	1
	Shipping	PowerEdge XE7740 Shipping EMEA1	340-DRWG, 340-DTWP	1

		(English/French/German/Spanish/Russian/Hebrew)		
	Regulatory	PowerEdge No CCC, CE Label Marking	389-FHJB	1
	Shipping Material	XE7745 Shipping Material	340-DSGQ	1
	Customer Notifications	Heavy device requires lift-assist cart for onsite service; otherwise, delays or extra fees may apply	883-17744	1
	Dell Services: Hardware Support	Parts Only Warranty 12Months, 12 Month(s)	709-BFTZ	1
	Dell Services: Extended Service	ProSupport Plus and 4Hr Mission Critical, 36 Month(s)	865-BBLP, 865-BBLQ	1
	ProDeploy Field Deployment Services	ProDeploy Plus PowerEdge XE Series 3U4U	683-BDSF	1
	Anti-Theft Device & Asset Tagging	Asset Tag - ProSupport (Website, barcode, Onboard MacAddress)	293-10025	1
	Shipping Box Labels - Standard	Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM)	293-10049	1
PowerEdge R670 - Full Configuration - [EMEA_R670]				3
	Base	PowerEdge R670 Server	210-BNZH	1
	Chassis Configuration	Chassis with up to 8 E3.S NVMe Direct Drives	780-BCYY	1
	Processor	Intel® Xeon® 6 Performance 6505P 2.2G, 12C/24T, 24GT/s, 48M Cache, Turbo, (150W) DDR5-6400	338-CTBJ	1
	Additional Processor	Intel® Xeon® 6 Performance 6505P 2.2G, 12C/24T, 24GT/s, 48M Cache, Turbo, (150W) DDR5-6400	338-CTBJ, 379-BDCO	1
	Thermal Configuration	Heatsink for 2 CPU configuration (CPU less than 185W)	412-BCDV	1
	Memory Configuration Type	Performance Optimized	370-AAIP	1

	Memory DIMM Type and Speed	6400MT/s RDIMMs	370-BCCX	1
	Memory Capacity	32GB RDIMM, 6400MT/s, Dual Rank	370-BCCY	8
	RAID Configuration	C30, No RAID for NVME chassis	780-BCDO	1
	RAID/Internal Storage Controllers	No Controller	405-AACD	1
	Hard Drives	No Hard Drive	400-ABHL	1
	BIOS and Advanced System Configuration Settings	Power Saving BIOS Setting	384-BBBH	1
	Hard Drives (PCIe SSD/Flex Bay)	1.92TB Data Center NVMe Read Intensive AG Drive E3s Gen5 with carrier	345-BKFR	2
	Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition	800-BBDM	1
	Fans	PowerEdge 1U High Performance Silver Fan	384-BDQL	1
	Embedded Systems Management	iDRAC10 Datacenter 17G with OpenManage Enterprise Advance Plus	634-CSGX, 634-CSHS, 634-CSHT, 634-CSHV	1
	Embedded Systems Management	Dell Connectivity Client - Enabled 17G	379-BFXS, 634-CZRP	1
	Power Supply	Dual, FTR(1+1),Hot-Plug MHS Power Supply, 1500W MM (100-240Vac) Titanium	450-BCXC	1
	Power Cords	Rack Power Cord 2M (C13/C14 10A)	450-AADY	2
	PCIe Riser	Riser Config 6, Rear 2x16 LP Slots (Gen5), 1x16 OCP, 1x8/x16 OCP	330-BCSJ	1
	Motherboard	PowerEdge R670 Motherboard for RTS 1.2, ROW	338-CRXD	1
	OCP 3.0 Network Adapters	Broadcom 57608 Dual Port 200GbE (Single Port 400GbE) QSFP112 Adapter, OCP 3.0 NIC	540-BFPW	1

	Additional Network Cards	Broadcom 57414 25GbE SFP28 Dual Port Adapter, PCIe Low Profile +Sec	540-BFXN	1
	OCP 3.0 Accessories	1 OCP - 1 Rear Blank, No Cable	470-BCHM	1
	BMC Password	iDRAC Legacy Password for OCP cards	379-BETF	1
	Bezel	No Bezel for E3 Chassis for x8	350-BBBW, 350-BDDS	1
	Cables	No DPUs Cable Required, No DPU	470-AEYU	1
	Boot Optimized Storage Cards	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80) Rear	403-BDMM	1
	Optics & Cables for Network Cards	Dell, Transceiver, 400GbE-Q112-EDR4, 2km MMF over 4 pair of SMF	407-BDHV	1
	Optics & Cables for Network Cards	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	407-BBXX	2
	Operating System	No Operating System	611-BBBF	1
	OS Media Kits	No Media Required	605-BBFN	1
	Rack Rails	ReadyRails Sliding Rails With Cable Management Arm	770-BDMT, 770-BECD	1
	KVM	Blank Left Ear Module	350-BCYJ	1
	Shipping	PowerEdge R670 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew)	340-DRWG, 340-DSGB	1
	Shipping Material	PowerEdge 1U Shipping Material	340-DNSY	1
	Regulatory	PowerEdge No CCC, CE Label Marking	389-FHJB	1
	ECCN	Decline Selection	817-BBBP	1
	Dell Services: Hardware Support	Parts Only Warranty 12Months, 12 Month(s)	709-BBIY	1
	Dell Services: Extended Service	ProSupport Plus and 4Hr Mission Critical, 36 Month(s)	865-BBLP, 865-BBLQ	1
	Infrastructure Deployment Svcs	Basic Deployment PowerEdge R Series 1u2u	683-BBGK	1
	Anti Theft Device & Asset Tagging	Asset Tag - ProSupport (Website, barcode, Onboard MacAddress)	293-10025	1

	Shipping Box Labels - Standard	Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM)	293-10049	1
PowerEdge R770 - Full Configuration - [EMEA_R770]				3
	Base	PowerEdge R770 Server	210-BNWX	1
	Chassis Configuration	2.5" Chassis with up to 8 NVMe HWRAID Drives, Front PERC 12 (H965i)	321-BLHK	1
	Processor	Intel® Xeon® 6 Performance 6515P 2.3G, 16C/32T, 24GT/s, 72M Cache, Turbo, (150W) DDR5-6400	338-CTBF	1
	Additional Processor	Intel® Xeon® 6 Performance 6515P 2.3G, 16C/32T, 24GT/s, 72M Cache, Turbo, (150W) DDR5-6400	338-CTBF, 379-BDCO	1
	Thermal Configuration	Heatsink for 2 CPU configuration (CPU less than 200W)	412-BCDL	1
	Memory Configuration Type	Performance Optimized	370-AAIP	1
	Memory DIMM Type and Speed	6400MT/s RDIMMs	370-BCCX	1
	Memory Capacity	32GB RDIMM, 6400MT/s, Dual Rank	370-BCCY	16
	RAID Configuration	C31, No RAID with NVMe and front PERC	379-BEGI	1
	RAID Controller	PERC H965i Controller, Front, DC-MHS	403-BDMY	1
	Hard Drives	No Hard Drive	400-ABHL	1
	Hard Drives (PCIe SSD/Flex Bay)	7.68TB Data Center NVMe Read Intensive AG Drive U2 with carrier	345-BJNW	6
	BIOS and Advanced System Configuration Settings	Power Saving BIOS Setting	384-BBBH	1
	Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition	800-BBDM	1

	Fans	PowerEdge 2U High Performance Gold Fan	384-BDQR	1
	Embedded Systems Management	iDRAC10, Core 17G	634-CSHW	1
	Embedded Systems Management	Dell Connectivity Client - Enabled 17G	379-BFXS, 634-CZRP	1
	Power Supply	Dual, Fully Redundant (1+1),Hot-Plug MHS Power Supply, 1500W MM, Titanium	450-BCWT	1
	Power Cords	Rack Power Cord 2M (C13/C14 10A)	450-AADY	2
	PCIe Riser	Riser Config 6-1, Rear Half Length, 4x16 FH Slots (Gen5), 1x8/1x16 OCP (Gen5), 2nd OCP x16 (Gen5)	330-BCXY	1
	Motherboard	PowerEdge R770 Motherboard for RTS1.2, ROW	338-CRTY	1
	OCP 3.0 Network Adapters	Broadcom 57608 Dual Port 200GbE (Single Port 400GbE) QSFP112 Adapter, OCP 3.0 NIC	540-BFPW	1
	Additional Network Cards	Broadcom 57414 25GbE SFP28 Dual Port Adapter, PCIe Full Height +Sec	540-BFXP	1
	OCP 3.0 Accessories	1 OCP - 1 HPM OCP Slot Cable, 1 Rear Blank	470-BCHM, 470-BCKJ	1
	BMC Password	iDRAC Legacy Password for OCP cards	379-BETF	1
	Bezel	PowerEdge 2U Standard Bezel	350-BCYM, 350-BDBP	1
	Acceleration Cards Cables	No DPUs Cable Required, No DPU	470-AEYU	1
	GPU/FPGA/Acceleration Cables	No Cables Required, No GPU Blanks	470-AEYU	1
	Boot Optimized Storage Cards	BOSS-N1 controller card + with 2 M.2 480GB (RAID 1) (22x80) Rear	403-BDMM	1
	Optics & Cables for Network Cards	Dell, Transceiver, 400GbE-Q112-EDR4, 2km MMF over 4 pair of SMF	407-BDHV	1

	Optics & Cables for Network Cards	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	407-BBXX	2
	Operating System	No Operating System	611-BBBF	1
	OS Media Kits	No Media Required	605-BBFN	1
	Rack Rails	No Rack Rails or Cable Management Arm	770-BBBS	1
	KVM	Blank Left Ear Module	350-BCYL	1
	Shipping	PowerEdge R770 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew)	340-DRWG, 340-DSDY	1
	Shipping Material	PowerEdge 2U Shipping Material	340-DPDX	1
	Regulatory	PowerEdge No CCC, CE Label Marking	389-FHJB	1
	ECCN	Decline Selection	817-BBBP	1
	Dell Services: Hardware Support	Parts Only Warranty 12Months, 12 Month(s)	709-BBIY	1
	Dell Services:Extended Service	ProSupport Plus and 4Hr Mission Critical, 36 Month(s)	865-BBLP, 865-BBLQ	1
	Infrastructure Deployment Svcs	Basic Deployment PowerEdge R Series 1u2u	683-BBGK	1
	Anti Theft Device & Asset Tagging	Asset Tag - ProSupport (Website, barcode, Onboard MacAddress)	293-10025	1
	Shipping Box Labels - Standard	Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM)	293-10049	1
PowerSwitch (Z9664F-ON) - [POWERSWITCH_Z9664F-ON]				2
	Base	PowerSwitch Z9664F-ON, 64 x 400GbE QSFP56-DD ports, IO to PSU air, 2x AC PSU	210-BCJI	1
	System Documentation	Dell EMC Z9664 Series User Guide EMEA-SAB	340-DDFX	1
	Power Cords	Power Cord, 250,16A,3M,C19,UK/IE	450-AMOJ	2
	Operating System	OS10 Enterprise, Z9664F-ON	634-BZSV	1

	QSFP Cables (40/100/200/400GbE)	Dell Networking Cable, 2x100GbE, QSFP28-DD to QSFP28-DD, Passive Copper Direct Attach, No FEC, 1M	470-ACTR	1	
	Ethernet Optics	Dell Networking Transceiver, 400GbE QSFP56-DD, LR4, 10km SMF, LC Duplex	407-BCTO	12	
	Ethernet Optics	Dell Networking Transceiver 200G-Q56-SR4	407-BDFY	6	
	Dell Services: Hardware Support	Parts Only Warranty 12Months (Emerging Only), 12 Month(s)	709-BEER	1	
	Dell Services: Extended Service	Prosupport Plus and 4Hr Mission Critical, 36 Month(s)	199-BHXU, 199-BHXV	1	
	Infrastructure Deployment Svcs	ProDeploy Plus Networking Z Series 96xx Switch	683-BCVL	1	
	Consolidation Fees - (EM-EMEA Only)	Consolidation Fee Ent	991-10021	1	
1. S5248-ON - [DELL_DATA_ANALYTICS_SWITCH_13597]					2
	Operating System	OS10 Enterprise, S5248F-ON	634-BRUN	1	
	Base	Dell S5248F-ON Switch, 48x25GbE SFP28, 4x100GbE QSFP28, 2x100GbE QSFP-DD, PSU to IO, 2xPSU	210-APFB	1	
	System Documentation	User Documentation EMEA 2	631-ABXT	1	
	Power Cords	European 220V Power Cord	450-ABOV	2	
	25/40/100G Cables with Embedded Optics	Dell Networking Cable, 2x100GbE, QSFP28-DD to QSFP28-DD, Passive Copper Direct Attach, No FEC, 1M	470-ACTR	1	
	Ethernet Optics	Dell Networking, Transceiver, 25GbE SFP28 SR, No FEC, MMF, Duplex LC	407-BBXX	12	
	Base warranty	1Yr Parts only - Minimum Warranty (Emerging Only)	709-13025, 709-17022, 709-17023, 710-73324	1	
	Support Services	3Yr ProSupport Plus and 4hr Mission Critical	528-10337, 865-85506, 865-85507	1	

	Infrastructure Deployment Svcs	ProDeploy Plus Networking S Series 5xxx Switch	683-BCTT	1
	Dell Services: OS10 Software Support	3 Years ProSupport Plus OS10 Enterprise Software Support-Maintenance	487-14700	1
	Consolidation Fees (EM-EMEA Only)	Consolidation Fee	991-10021	1

7.9.2 OpenShift Licenses

SKU	Description	Qty	Period
MW04348	Red Hat OpenShift Platform Plus (Bare Metal Node), Premium (1-2 Sockets up to 128 Cores)	3	3 Years
MCT4792	Red Hat OpenShift AI (Bare Metal Node), Premium (1-2 sockets up to 128 cores)	3	3 Years
MCT4721	Red Hat AI Accelerator, Premium (1 Accelerator)	24	3 Years

7.9.3 Elastic Search Licenses

SKU	Item Description	Qty
Elasticsearch	Enterprise Resource Unit - 64GB	48

7.10 Managed Services

Role	Min FTE	Coverage
Head of Operations / SDM	1	Onsite -Business hours + on-call
Duty Manager / MIM	1	Onsite -Business hours + on-call
Shift Lead	4	24×7 (3 shifts) Onsite & Remote
L1 Analysts (SOC)	12	24×7 (3 shifts) Onsite & Remote
L2 Specialists (NW/Sys/Cloud)	6	24×7 (3 shifts) Onsite & Remote
Threat Hunter / Detection Eng	2	Onsite -Business hours + on-call x 2 shifts
Automation Engineer SOAR/Runbook	1	Business hours
Reporting Analyst/Service Performance	1	Business hours

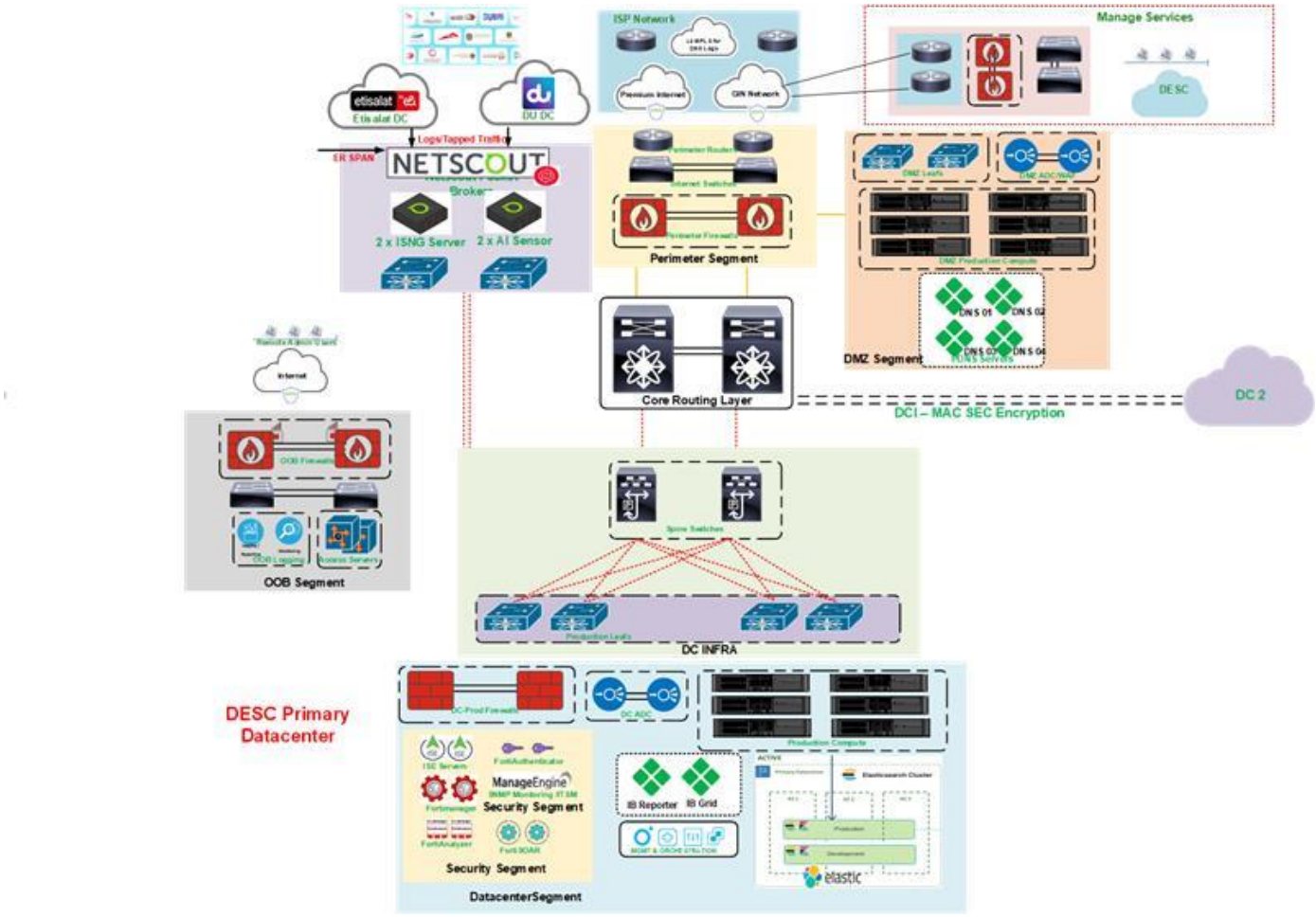
Cloud Infra Management – L1	3	24×7 remote
Cloud Infra Management – L2	3	24×7 remote
Cloud Infra Management – L3	1	24×7 remote

7.11 VAPT

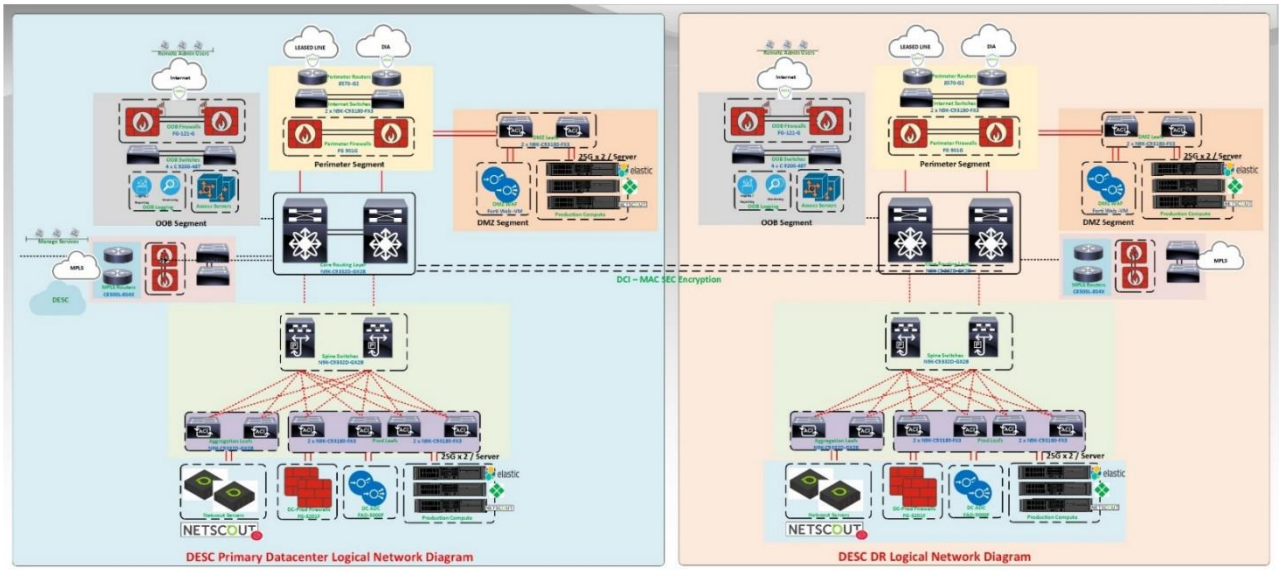
S.No	Description	Qty
1	Vulnerability Assessment	300 VMs
2	Penetration Testing	20 Public IPs
3	Trend Vision One Endpoint Security - Pro, 3Y,including: Malware Protection, Web Reputation, Behavior Monitoring and Analysis, Machine Learning capabilities, Firewall for Servers, IDS/IPS for Servers (Virtual Patching), Log Inspection, File Integrity Monitoring, Device Control, Application Control, Native XDR for Servers, Advanced Threat Protection (Sandboxing)	200 VMs

8. Proposed Solution Components

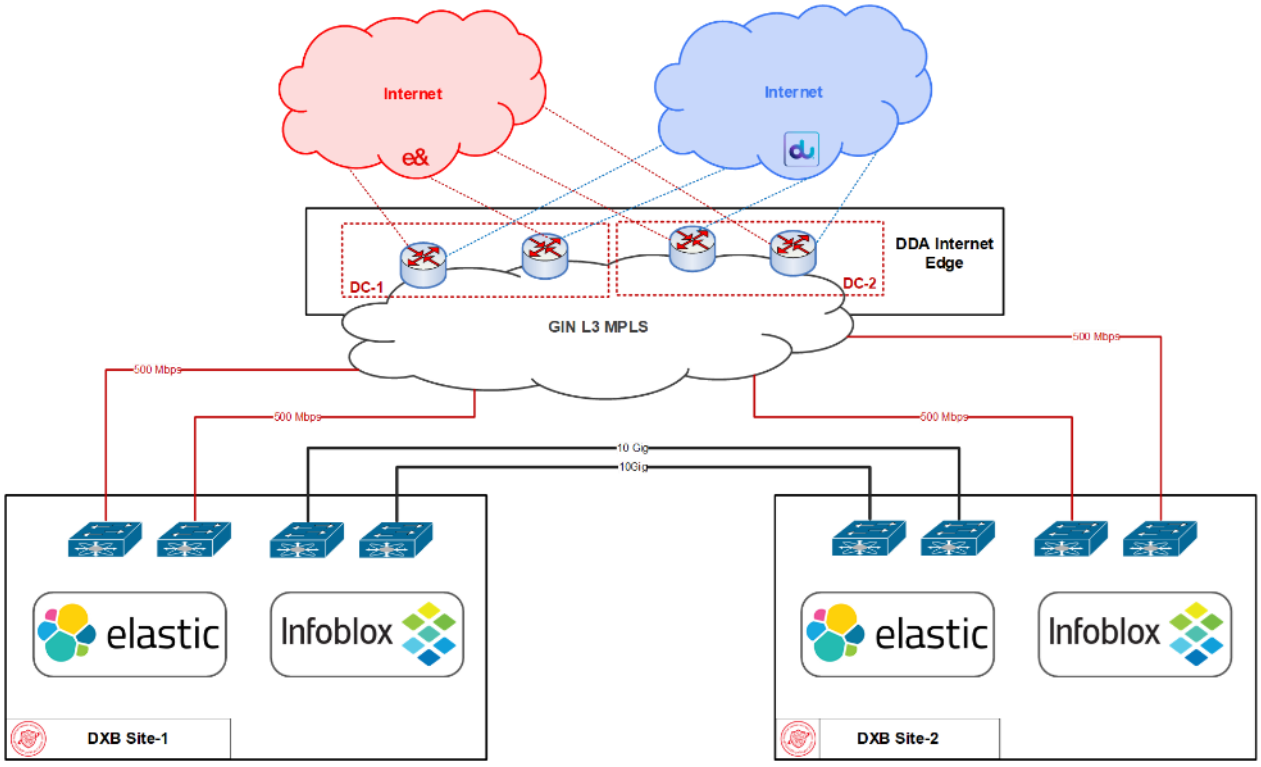
8.1 Solution Architecture [High Level]



8.2 Network Architecture [High Level]



8.3 Internet and GIN connectivity – per site



du strongly proposes DDA owned GIN network to be the main Internet breakout for the DNS traffic which should be provided by DESC / DDA. There are multiple reasons for this proposition which are as follows:

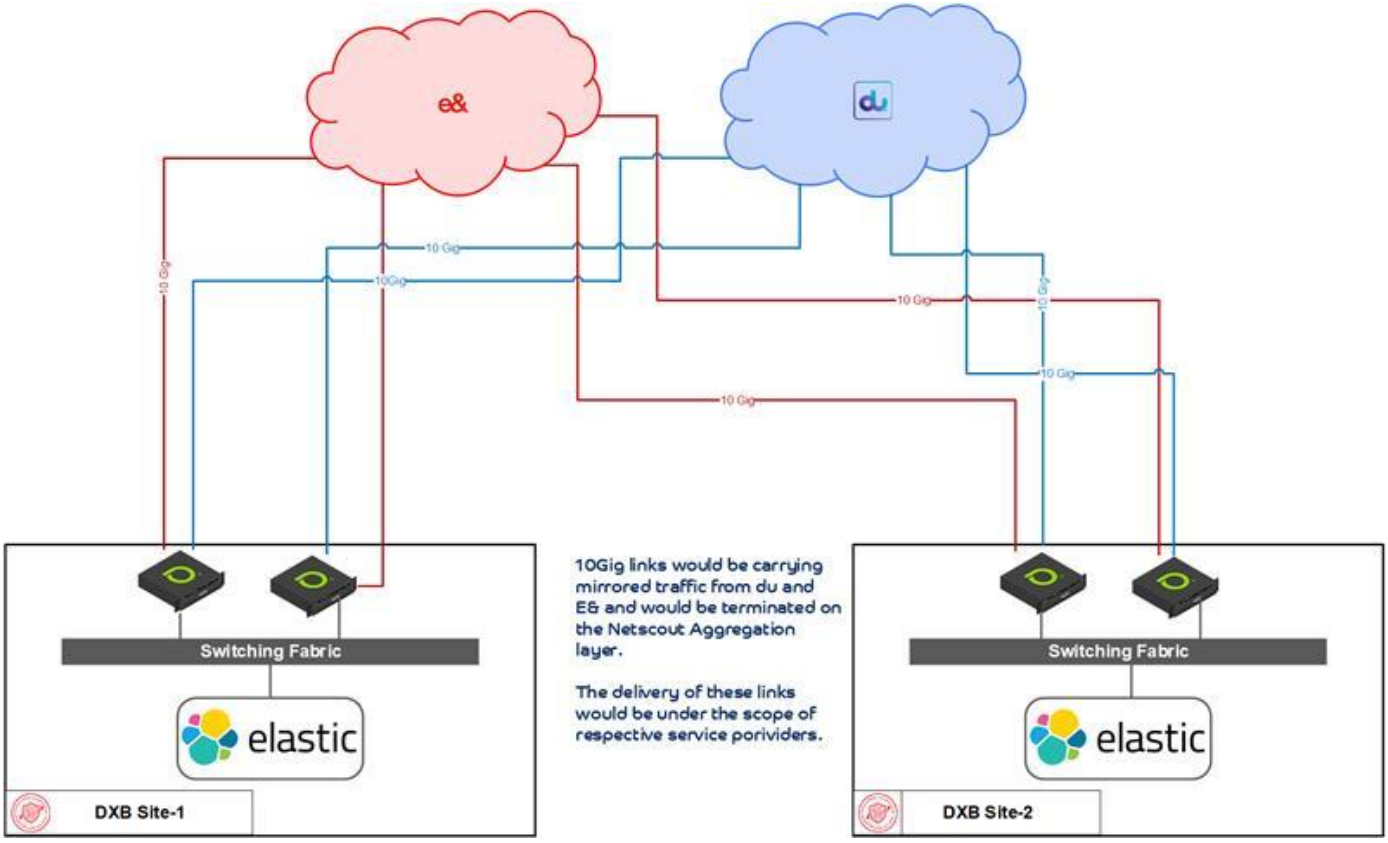
- The DDA owned GIN network has a highly available, georedundant, DDoS protected Internet Edge which has connectivity with both the service providers (du and E&). This ensures maximum resiliency in case of the failure at the service provider level.

- DDA has its own public AS and IPv4 / IPv6 prefixes. Therefore, we can assign the DDA owned public IPv4 / IPv6 to the newly built PDNS so that these IPs could be routed via du as well as E& networks simultaneously which is not the option in case, we get the Internet directly either from du or E&.

- DDA Internet edge is fully protected with multilayer DDoS protection from both the service providers. The DNS traffic of all the government departments or entities which are using GIN network could be locally routed to the newly built PDNS platform via GIN network thus minimizing the DNS resolution time for such DNS queries.

- The users who will be part of the DESC internal network will be able to have the connectivity with the platform using GIN network for the Operations and Management requirements especially for the managed services scope.

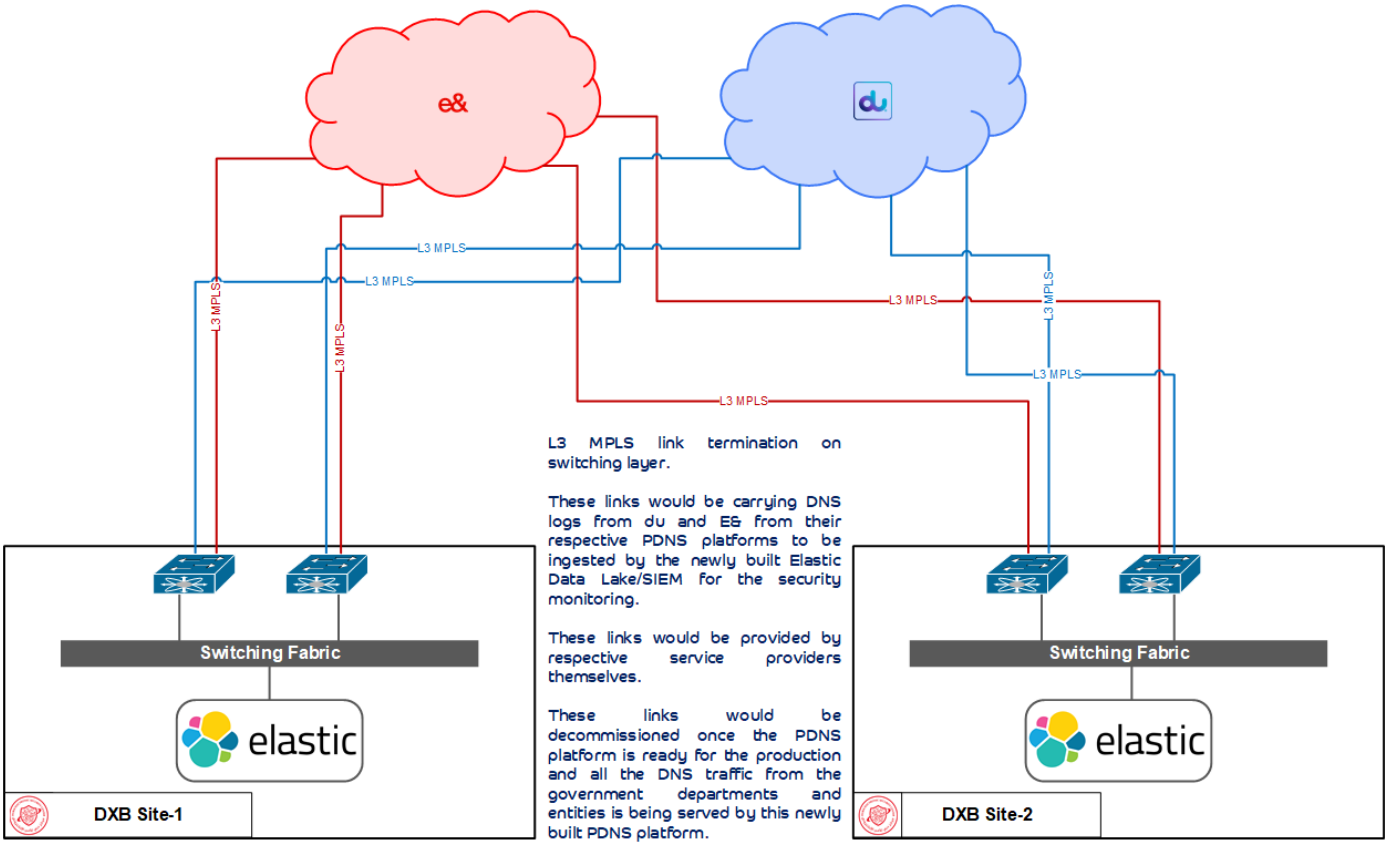
8.4 Network Design of Link Termination of 10 Gigs carrying Tapped Traffic from Service Provider.



The mirrored/tapped internet traffic from both the service providers (du and E&) would be carried to the new platform via 10G links. Each service provider has to ensure that two 10Gig links are coming from each service provider in each DC location which then would be terminated on different aggregation box. These links will carry the tapped internet traffic from the service provider Internet core as well as from the local access network of each government entity. This ensures the link level local high availability and georedundancy.

The scope of delivering of these 4x10Gig links will fall under the sole responsibility of the two service providers with each providing 2x10 Gig links per site.

8.5 Network Design for L3 MPLS carrying DNS logs from service providers.



After the Phase-1 when the Data Lake and SIEM would be fully functional and ready to ingest the logs, we are expecting both the service providers (du and E&) to provide us the DNS security logs from their respective PDNS platforms. These logs could be carried over L3 MPLS links as shown in the below network diagram. The delivery scope of these links would be exclusively under the responsibility of the services providers.

8.6 Technical Datasheets

SN	Item Description	Technical Datasheets	Reference to Solution Page / Section No.
1.	Cisco	Refer to attachment : Du Response - RFQ 762640 - 8.6 - Technical Data Sheet.zip	
2.	Dell	Refer to attachment : Du Response - RFQ 762640 - 8.6 - Technical Data Sheet.zip	
3.	Commvault	Refer to attachment : Du Response - RFQ 762640 - 8.6 - Technical Data Sheet.zip	

9. Proposed Solution Details

9.1 du Datacentre's Overview

Building a Datacenter is a major capital investment; your enterprise infrastructure must support growth with a limited budget, meet tight deployment timeframes and still leave resources for your core competencies. The "du" datacentres facilities are designed with state-of-the-art facility infrastructure to address the most stringent requirements, similar to those of government customers. We ensure security for your deployed systems within secure Datacenter facilities: secure cage spaces, 24x7x365 on-site security guards, multiple levels of access control, CCTV, access control lists, and comprehensive procedures for screening inbound deliveries.

Furthermore, our strict adherence to standardized procedures and external accreditations permit easy auditing if you wish to check the standard and quality of our delivery. Thanks to our experience with enterprises companies, we have developed procedures that are appropriate for highly secure mission critical data processing. Our datacentres are

designed and built to high standards of redundancy, security, and resiliency with the latest technologies to ensure your systems are secure and backed by the best uptime in the industry.

9.1.1 Datacenter High Level Technical Specification

The entire electrical design system is concurrently maintainable as per Tier III compliance and guidelines, the facility we are proposing for this deployment is Nautilus KIZAD Data Center in Abu Dhabi. The environment is summarized here below:

DESIGN STANDARD	REDUNDANCY / SPECIATION
Utility Power Supply	DEWA in Dubai & ADDC in Abu Dhabi Authorities, diverse dual site source utility power (Ring grid design) with N+1 Transformer's connection
Generators	Redundancy (N+1 Swing Generator) backup for full load with Day Tank + Main Reservoir (2 Bulk Tanks) for 24 hours of Concurrently Maintainable Fuel
UPS & Batteries Topology	Distributed Redundant (N+1) 400kVA synchronized (2N redundancy at rack level), Each Batteries Rooms has 2-String with (10 Years Life Batteries & 10 Minutes Autonomy)
Cooling	Cooling Towers Redundancy (2N), Chillers Redundancy (N+1), CRAC redundancy (N+20%)
Fire Protection	Fire detection (VESDA & Analogue smoke detection), Fire suppression (High pressure Water Mist for IT Rooms & FM200 Service Rooms), Water Leak (TTK digital liquid leak detection system Addressable Sensing)
Security Setup	Physical (Common areas and Terrain perimeter), Human (24 X 7 Security Officers), Electronic (EKMS for all doors, full CCTV monitoring connected to BMS control room, Biometric Access Control to whitespace)

9.1.2 Datacenter security services

Our du Datacenter offers several features for best-in-class security:

Each du Datacenter has an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. All areas of the Datacenter are monitored and recorded using CCTV, and all access points are controlled. du datacentres are staffed with 24-hour security officers. Visitors are screened upon entry to verify identity and escorted to appropriate locations. Access history is recorded for audit by customers. All shared and private cage/suite areas are equipped with security cameras, biometric hand geometry readers, and individually locked Racks (upon request).

NOTES

- Full suite of Managed Security Services including a comprehensive Security Incident and Event Management Platform
- du will provide onsite "Datacenter Customer Guidelines" which contains Guidelines of Policies and Procedures related to activities required in Datacenter

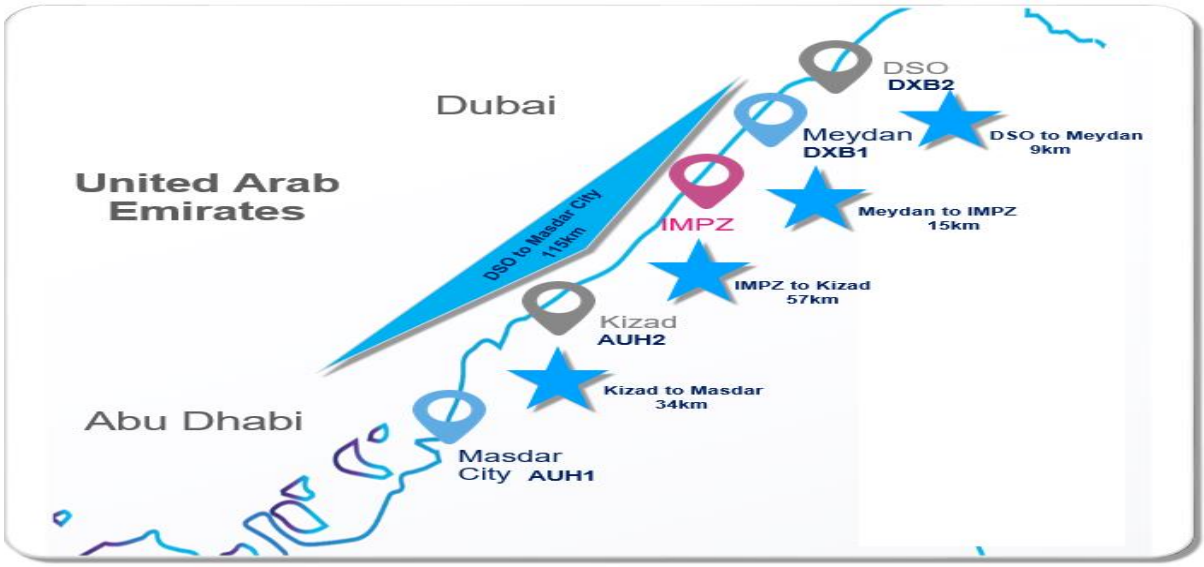
9.1.3 Datacenter risk assessment

Our du Datacenter service mitigates following risks:

- du facility is not located on or near a floodplain
- du facility is not in an area of seismic activity
- du facility is not immediately adjacent to a site/building involved in the storage of combustible or explosive materials
- No chemical processing plants within the vicinity
- There is a low risk of military action and terrorism.

9.1.4 Business continuity

du Datacenter Meet NCEMA guidelines with two facilities in two different Emirates, using two different power grids and dual carrier redundancy, the two DC facilities connected with dedicated fibre with Redundant Routes of 3-5 ms latency.



du are ISO 22301 certified for "Business Continuity Management", which cover the ability to avoid major business disruption from a disaster while addressing the principal concerns of business risk mitigation and protection. All the related plans and process documentation are highly confidential and owned by our du security team.

9.2 Security & Observability Platform Development

Proposed cybersecurity and observability platform Datacentres are built in total Four phases. This section will provide the detailed information about the proposed technology in each phase.

9.3 Phase 0: Network and Security Infrastructure deployment

Phase 0 serves as the foundational stage, designing and deploying the network and security infrastructure across the two Tier-3 datacenters in Dubai (Primary and DR), enabling the hosting of compute, storage, and IT systems for Phases 1-3 with industry-leading standards and connectivity.

9.3.1 Datacenter Networking

DU is proposing Cisco Datacenter networking for DESC Datacenter requirements.

Implementing a Cisco Data Center Networking solution offers organizations a comprehensive and advanced approach to optimizing their data center operations. With state-of-the-art technologies, Cisco's solution provides a range of benefits aimed at enhancing performance, security, scalability, and operational efficiency within the data center environment.

Key Features:

- **Scalability:** Cisco data center solutions are built to accommodate the evolving demands of modern businesses, allowing for seamless growth and integration of new services.
- **High-Performance Connectivity**: Cisco networking technologies provide high-speed and low-latency connectivity, ensuring efficient data transfer and responsive applications critical to business success.
- **Redundancy and Resilience:** Cisco's approach includes redundancy mechanisms like Virtual Port Channel (vPC) and FabricPath, ensuring network availability by minimizing single points of failure.
- **Security and Segmentation**: Cisco solutions offer advanced security measures such as network segmentation and comprehensive access control, safeguarding data and applications from threats.
- **Software-Defined Networking (SDN) Integration**: Cisco's data center networking supports software-defined networking, enabling automation and optimization of network configurations.
- **Visibility and Analytics**: Comprehensive monitoring and analytics tools enhance network visibility, enabling proactive troubleshooting and efficient performance optimization.

- **Centralized Management**: Solutions like Cisco Application Centric Infrastructure (ACI) provide centralized management and automation of data center networks, simplifying policy enforcement and network orchestration.
- **Ecosystem Integration:** Cisco's data center networking seamlessly integrates with other Cisco products, creating a cohesive ecosystem that streamlines management.
- **Regulatory Compliance**: Cisco's features assist organizations in meeting regulatory standards by incorporating audit trails, access controls, and data encryption.

Below are the DU proposed Cisco Technologies for DESC DC and DR Network.

Technology	Proposed Solution	DC Qty	DR Qty
Internet Routers	Cisco 8570G2	2	2
Internet Connectivity Switches	Cisco N9K-C93180-FX3	2	2
DMZ Switches	Cisco N9K-C9332D-GX2B	2	2
Datacenter Core Switches	Cisco N9K-C9332D-GX2B	2	2
Datacenter Spine Switches	Cisco N9K-C9332D-GX2B	2	2
Datacenter Leaf Switches	Cisco N9K-C93180-FX3	4	4
OOB Switches	9200-48T	4	2
Aggregation Layer Switches	Cisco N9K-C9332D-GX2B	2	2
TACACS	Cisco ISE VM	1	1

9.3.2 Proposed Product Details

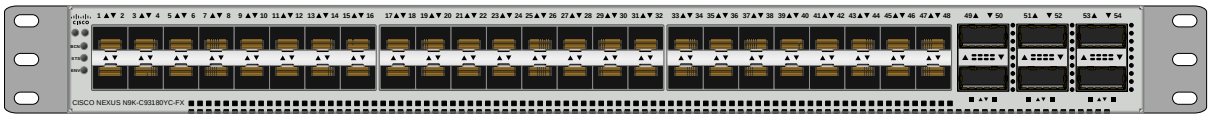
9.3.2.1 Cisco Nexus N9K-C9332D-GX2B

The Cisco Nexus 9332D-GX2B is a compact form-factor 1-rack-unit (1RU) switch that supports 25.6 Tbps of bandwidth and 4.17 bpps across 32 fixed 400G QSFP-DD ports and 2 fixed 1/10G SFP+ ports QSFP-DD ports also support native 200G (QSFP56), 100G (QSFP28), and 40G (QSFP+). Each port can also

support 4 x 10G, 4 x 25G, 4 x 50G, 4 x 100G, and 2 x 200G breakouts. The last 8 ports, marked in green, are capable of wire-rate MACsec encryption.

In DESC Infrastructure 9332-GX2B has been proposed as Core / Spine/ Aggregation layer Connectivity Switches. Also 9332-GX2B is proposed for MACSEC encryption between the datacenters.

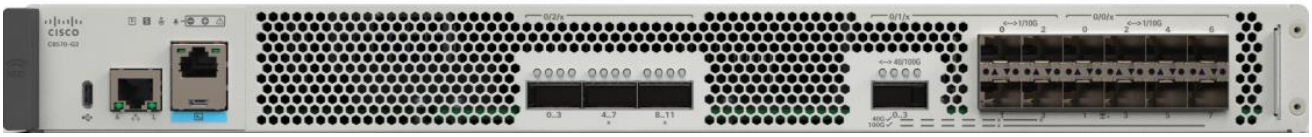
9.3.2.2 Cisco Nexus N9K-C93180-FX3



The Cisco Nexus 93180YC-FX3 Switch is a 1RU switch that supports 3.6 Tbps of bandwidth and 1.2 bpps. The 48 downlink ports on the 93180YC-FX3 are capable of supporting 1-, 10-, or 25-Gbps Ethernet, offering deployment flexibility and investment protection. The 6 uplink ports can be configured as 40 and 100-Gbps Ethernet, offering flexible migration options.

In DESC Infrastructure 93180-FX3 has been proposed as Leaf / Internet Connectivity Switches.

9.3.2.3 Cisco C8570-G2



Cisco 8500 Series Secure Routers are 1 RU fixed form factor devices. There are two models: Cisco 8550-G2 and 8570-G2. Cisco 8550-G2 provides 12 x 10GE ports, whereas the Cisco 8570-G2 provides 12 x 10GE, 2 x 40GE, and 2 x 100GE ports (max 240GE of ports enabled simultaneously).

In DESC Infrastructure 8570-G2 has been proposed as Perimeter Routers.

9.3.3 Datacenter Security

DU is proposing Fortinet Datacenter Security solution for DESC Datacenter security requirements.

Our proposed solution comprises a holistic framework that combines cutting-edge technology, proactive threat detection, and vigilant monitoring to ensure the highest level of protection for your datacentre.

Below are the DU proposed Cisco Technologies for DESC DC and DR Network.

Technology	Proposed Solution	DC Qty	DR Qty

Internet Firewalls	Fortigate FG 901G	2	2
DC Firewalls	Fortigate FG 3201F	2	2
OOB Firewalls	Fortigate FG 121G	2	2
DC ADC	Fortinet FAD 5000F	2	2
OOB Authentication	FortiAuthenticator VM with MFA	1	1
Firewall Central Mgmt & Monitoring	FMG/FAZ	1	1

9.3.3.1 Proposed Product Details

9.3.3.2 Fortigate 901G

The FortiGate 900G series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) to deliver threat protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats. Powered by a rich set of AI/ML security capabilities that extend into an integrated security

fabric platform, the FortiGate 900G Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy

enforcement and threat protection across all network segments.

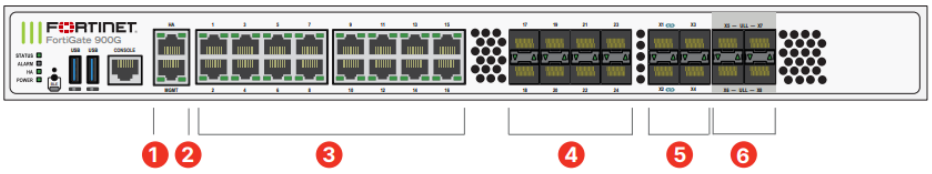
In DESC Infrastructure Fortigate 901G has been proposed as Perimeter Firewall with UTP Licenses.

Feature	Specifications

Firewall Throughput	153 Gbps
IPS Throughput	42 Gbps
NGFW Throughput	31 Gbps
Concurrent Sessions	16 Million
New Sessions	720000
SSL Inspection Throughput	16.7 Gbps
SSL Inspection CPS (IPS, avg. HTTPS)	18000
SSL Inspection Concurrent Session (IPS, avg HTTPS)	1.6 Million

Hardware

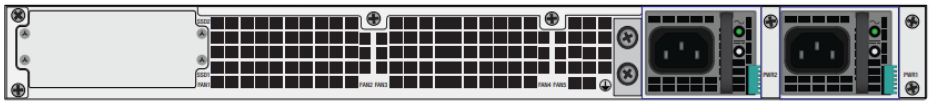
FortiGate 900G/-DC and 901G/-DC Series, Front Panel



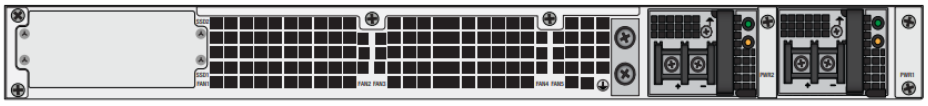
Interfaces

1. 1 × 2.5/1 GE RJ45 HA Port
2. 1 x GE RJ45 Management Port
3. 16 x GE RJ45 Ports
4. 8 x GE SFP Slots
5. 4 × 10GE/GE SFP+/SFP Slots
6. 4 × 25GE/10GE SFP28/SFP+ ULL (ultra-low latency) Slots

FortiGate 900G and 901G Series, Rear Panel



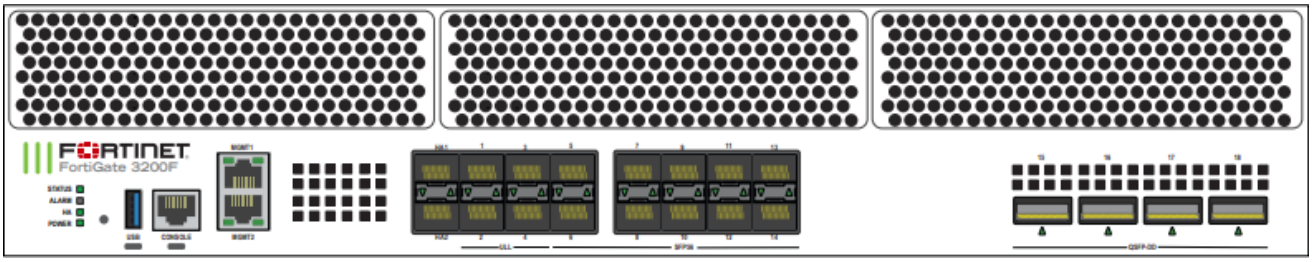
FortiGate 900G-DC and 901G-DC Series, Rear Panel



Hardware Features

NP7 | CP9 | TPM | 1RU | 25GE | 10/GE | DUAL AC | 960GB | DUAL DC

9.3.3.3 Fortigate 3201F



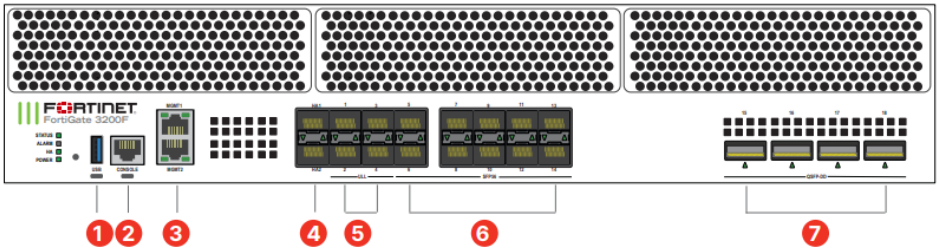
The FortiGate 3200F Series enables organizations to build security-driven networks, forming the foundation of a robust Hybrid Mesh Firewall architecture. This approach weaves security deep into their datacenter and across their hybrid IT environment, protecting any edge at any scale. Powered by a rich set of AI/ML-based FortiGuard Services and an integrated security fabric platform, the FortiGate 3200F Series delivers coordinated, automated, end-to-end threat protection across all use cases. The industry's first integrated Zero Trust Network Access (ZTNA) enforcement within an NGFW solution, FortiGate 3200F automatically controls, verifies, and facilitates user access to applications, delivering consistent convergence with a seamless user experience across your distributed network.

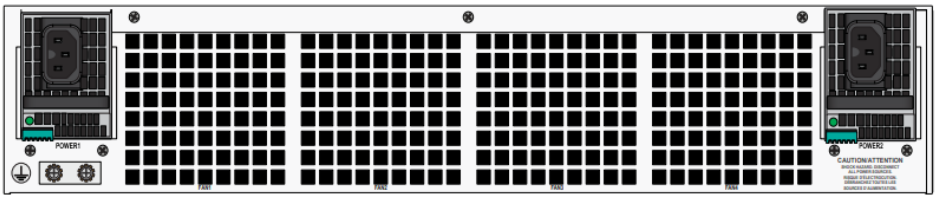
In DESC Infrastructure Fortigate 3201F has been proposed as Datacenter Firewall with IPS Licenses.

Feature	Value
Firewall Throughput	387 Gbps
IPS Throughput	63 Gbps
NGFW Throughput	47 Gbps
Concurrent Sessions	70 Million
New Sessions	800000
SSL Inspection Throughput	29 Gbps
SSL Inspection CPS (IPS, avg. HTTPS)	30000
SSL Inspection Concurrent Session (IPS, avg HTTPS)	7.4 million

Hardware

FortiGate 3200F Series





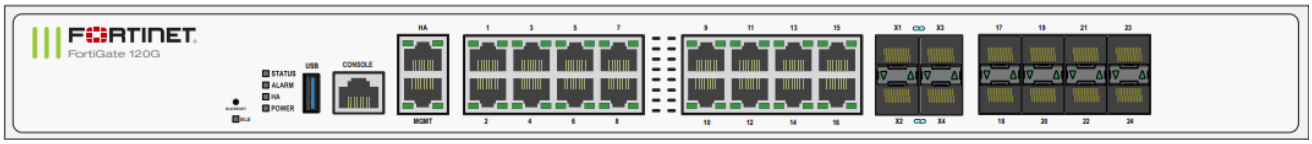
Interfaces

1. 1 x USB Port
2. 1 x RJ45 Console Port
3. 2 × 10 GE / GE RJ45 Management Ports
4. 2 × 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ HA1/HA2 Slots
5. 4 × 25 GE SFP28 / 10 GE SFP+ ULL Slots
6. 10 × 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
7. 4 × 400 GE QSFP-DD / 200 GE QSFP56 / 100 GE QSFP28 / 40 GE QSFP+ Slots

Hardware Features

NP7 | CP9 | TPM | 2RU | 400GE | DUAL AC | FortiCarrier | 1TB | 2×960GB

9.3.3.4 Fortigate 121G



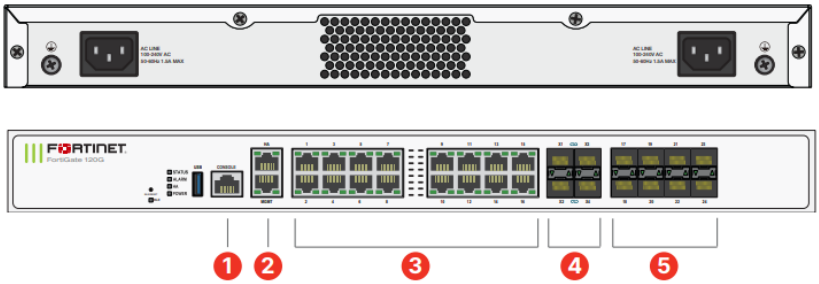
The FortiGate 120G series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) to deliver threat protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats. Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 120G Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

In DESC Infrastructure Fortigate 121G has been proposed as OOB Firewall.

Feature	Value
Firewall Throughput	39 Gbps
IPS Throughput	5.3 Gbps
NGFW Throughput	3.1Gbps
Concurrent Sessions	3 Million
New Sessions	140000
SSL Inspection Throughput	3 Gbps
SSL Inspection CPS (IPS, avg. HTTPS)	2100
SSL Inspection Concurrent Session (IPS, avg HTTPS)	315000

Hardware

FortiGate 120G/121G Series



Interfaces

1. 1x RJ45 Console Port
2. 2x RJ45 HA and Management Ports
3. 16x GE RJ45 Ports
4. 4× 10GE SFP+ FortiLink Slots
5. 8x SFP Ports

Hardware Features

SP5 | TPM | 1RU | DUAL AC | 480GB

9.3.3.5 FortiADC 5000F

FortiADC, the advanced Application Delivery Controller (ADC), optimizes application delivery, enhances performance, and ensures application security whether hosted on-premises or in the cloud.

FortiADC offers robust L4-L7 load-balancing capabilities with Scripting support for content manipulation and Advanced SSL Services (Offloading and mirroring). FortiADC also offers application acceleration, Application Access Gateway (App Portal), and built-in security features like Web Application Firewall protection for any application threats AL

(Adaptive Learning), and OWASP Top10 Compliance Policy), DDoS Protection, ZTNA, and more. With flexible deployment options (HW, VM, FortiFlex, and Cloud Providers) and integration into the Fortinet Security Fabric, FortiADC empowers businesses to deliver exceptional application experiences and security.

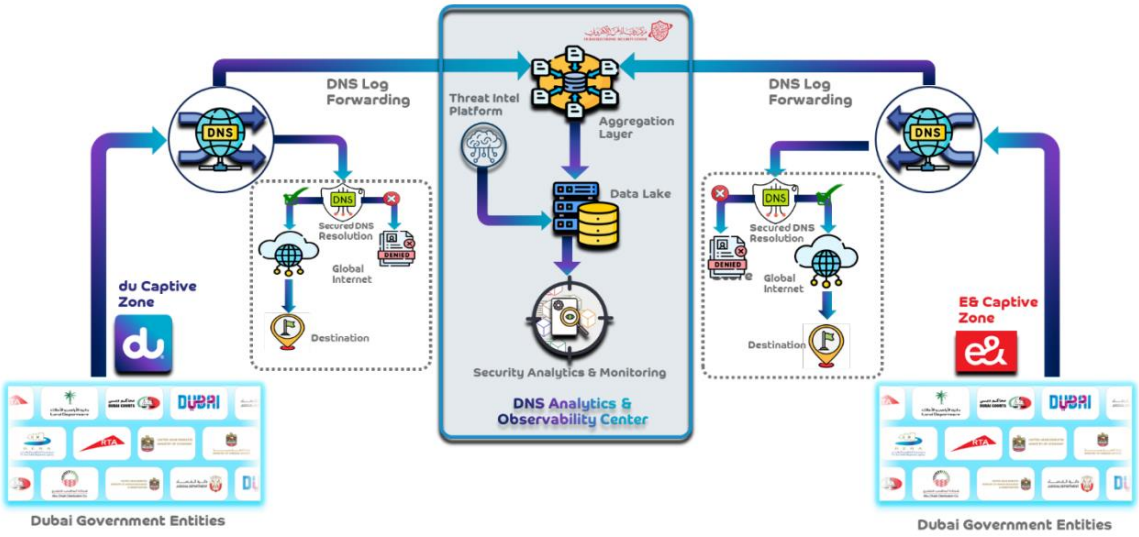
In DESC Infrastructure FortiADC 5000F has been proposed as Internal ADC.

Feature	Value
L4/L7 Throughput	220 Gbps
L4 CPS	4 M
L4 HTTP RPS	18000000
Max L4 Concurrent Connection	216000000

9.4 Phase 1: DNS Security Enforcement and Data Ingestion & Phase 2: Internet Traffic Collection, Ingestion of Large Data Sets In Data Lake And Enhanced Analytics Using Internet Oriented Security Use Cases

Phase 1 will Initiate DNS security across government entities and build the data ingestion infrastructure, Data Lake, Threat Intel Platform and Security Analytics & Monitoring stack. During this phase, DESC will rely on the service provider DNS ecosystem to enable the DNS security and provide the DNS logs for further processing because the Protective DNS (PDNS) deployment will be part of the Phase-3 of the RFP scope.

Phase 1: High Level Architecture of Traffic Flow



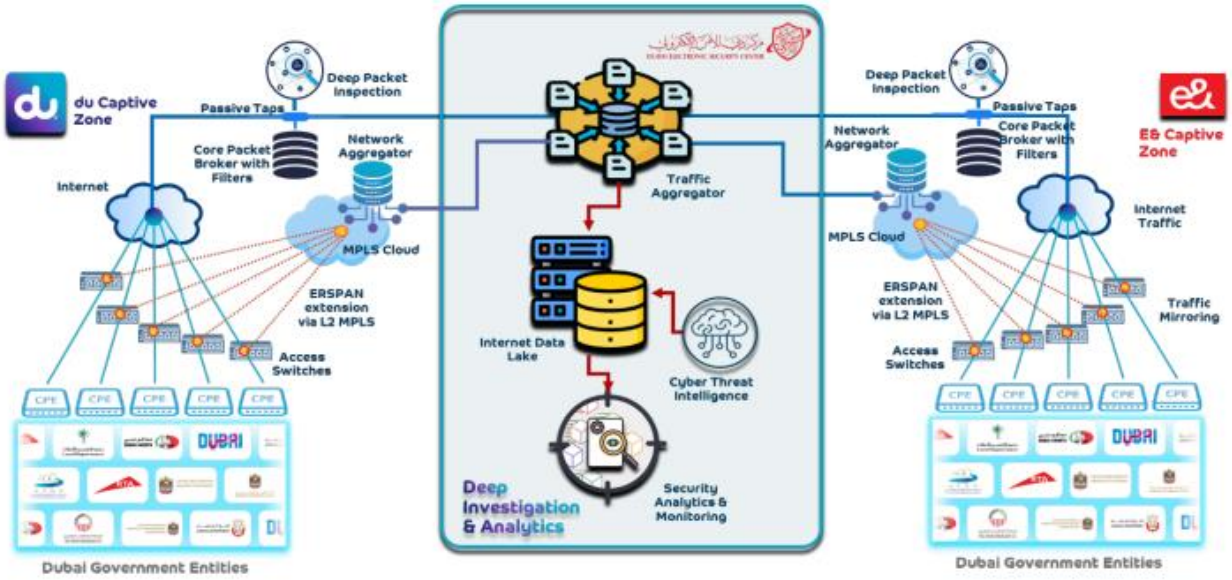
Phase 1: DNS Log and Traffic Ingestion Architecture

In Phase 1, service providers will forward DNS log information and DNS traffic from government entities to the DESC Data Lake for analytics.

- Syslog-based DNS logs will be sent directly from the service providers to Data Lake.
- In cases where raw DNS packet traffic is provided, the traffic will first be filtered (using Government Public IP addresses), then forwarded to the NetScout Packet Broker. The Packet Broker will process and extract the required metadata, which will be delivered to the Elastic Data Lake via the AI-Streamer for further analysis.

Phase 2 - Extending the functionality of the platform to capture, process and analyze Internet traffic of all the Dubai government departments and entities from service provider networks, ingesting it in the Data Lake for security monitoring and analytics for comprehensive observability and threat management.

Phase 2: High Level Architecture of Traffic Flow



The following solutions will be implemented as part of phase 2.

- Data Lake Solution & Analytics – Elastic solution Expansion.
- Data Ingestion Infrastructure – NetScout Solution Expansion.
- Threat Intelligence platform – Cyware Threat Intelligence

Phase 2: Internet Traffic Ingestion for Analytics

In Phase 2, Internet traffic will be included in addition to DNS traffic for comprehensive analytics.

1. Internet Traffic from Service Providers
    - Service providers will send Internet traffic along with DNS log information.
    - Internet traffic will be delivered to DESC using network TAPs, which are physically connected to the NetScout Packet Broker.
    - The Packet Broker will process the raw Internet traffic and generate the required metadata, which will be forwarded to the DESC Data Lake via the AI-Streamer.
2. Internet Traffic from Government Entities (SPAN/ERSPAN)
    - Service providers will also provide SPAN traffic from the government customer's Internet switch, and ERSPAN sessions terminating on the NetScout Packet Broker.
    - The Packet Broker will receive, process, and normalize the mirrored traffic.
    - The extracted metadata will then be sent to the DESC Data Lake via the AI-Streamer for analytics and correlation.

9.4.1 Data Lake Solution

DU is proposing Elastic Solution for meeting the DESC requirements.

Elastic Stack (Elasticsearch, Kibana, and Logstash) serves as a foundational component in the Dubai Electronic Security Center's (DESC) Security & Observability Architecture, functioning as the central data lake, security analytics engine, and monitoring platform. This document outlines how Elastic's capabilities align with DESC's vision of creating a robust cybersecurity framework for Dubai's government ecosystem, focusing on DNS security, internet traffic monitoring, and advanced threat detection.

Proposed solution is designed to be robust, scalable, and cyber-resilient, fully aligned with DESC's operational and regulatory requirements. Our architecture ensures seamless integration with existing DNS and observability technologies, including the ability to ingest enriched metadata from Netscout or other aggregation layers. The solution adheres to DESC's data governance and retention mandates, while supporting elastic scalability, multi-site resilience, advanced security controls, and optimized data life-cycle management.

The proposal outlines our end-to-end delivery approach—from architectural design, secured deployment, and operational enablement, through continuous support and optimization, leading to a structured and transparent transfer phase as defined within the BOT framework. Additionally, Elastic emphasizes localized capability building, ensuring that DESC's technical teams are fully enabled to independently operate, extend, and govern the platform.

With a strong foundation in modern data platforms, cybersecurity engineering, and high-scale log archiving, Elastic is committed to delivering a future-proof solution that supports DESC's mission of safeguarding Dubai's digital ecosystem.

9.4.2 Elastic as the Core Data Lake

Centralized Data Repository

Elastic will serve as the central data lake in the architecture, providing a scalable, multi-tenant repository to store and process:

- DNS logs from service providers (du and Etisalat)
- Internet traffic data from government departments and entities
- Security events and threat intelligence feeds

The platform will maintain distinct logical clusters for DNS and traffic datasets, ensuring isolation and efficiency while supporting the high-volume data requirements (78.96 TB/day for internet traffic and 1.49 TB/day for DNS traffic).

Data Retention and Storage Optimization

Elastic's tiered storage capabilities align perfectly with DESC's requirements for:

- Hot tier (30 days): Recent data for fast, real-time analytics
- Warm tier (60 days): Medium-term data for operational analytics
- Cold tier (90-270 days): Historical data for compliance and forensic analysis

This tiered approach ensures cost-effective storage while maintaining performance for active data and compliance with the specified retention periods (9 months for internet traffic and 18 months for DNS data).

Georedundant Deployment

Elastic will be deployed across dual sites in Dubai in both active/active (DNS data) and active/passive (internet traffic) configurations, ensuring:

- Real-time data replication with <500ms lag
- Sub-second failover capabilities
- 99.982% uptime in line with DESC's requirements
- Complete data sovereignty within Dubai's borders

9.4.3 Elastic as the Security Analytics Engine

Threat Detection and Response

Elastic Security will power DESC's security analytics capabilities through:

1. **Real-time Detection Rules:** Over 1,200+ built-in detection rules mapped to the MITRE ATT&CK framework to identify threats across DNS and internet traffic.
2. **Machine Learning-Based Anomaly Detection:** Leveraging Elastic's ML capabilities to detect:
    - DNS-based threats (tunneling, DGA, fast flux networks)
    - Command & Control communications
    - Data exfiltration attempts
    - Lateral movement and insider threats
3. **Threat Intelligence Integration:** Correlating observed data with threat feeds to identify known malicious domains, IPs, and patterns.

Use Case Implementation

Elastic will enable the implementation of DESC's comprehensive security use cases, including:

- DNS Traffic Use Cases: Malware C&C detection, DNS tunnelling identification, phishing detection, and policy enforcement

- Internet Traffic Use Cases: Advanced threat detection, data exfiltration monitoring, network visibility, and compliance enforcement

The platform's machine learning capabilities will support both supervised and unsupervised learning models, with the ability to import external models and continuously improve detection accuracy.

9.4.4 Elastic as the Monitoring Stack

Comprehensive Observability

Elastic Observability will provide DESC with:

1. **Visualization & Reporting Framework:** Interactive dashboards displaying real-time metrics such as:
    - Blocked query rates and top malicious domains
    - Traffic patterns and bandwidth usage
    - Security incidents and threat intelligence correlations
2. **Advanced Visualization Capabilities**: Supporting a wide range of visualization types including:
    - Bar, line, and area charts
    - Heatmaps and geographical maps
    - Network graphs and relationship diagrams

Alerting and Response Automation: Enabling:

- Real-time alerts on security incidents
- Automated responses through REST API integrations
- Case management for security incidents

Operational Monitoring

Beyond security, Elastic will provide operational monitoring of the entire platform:

- Performance metrics for DNS resolvers and packet brokers
- Health status of the infrastructure components
- Resource utilization and capacity planning

9.4.5 Integration with the Overall Architecture

Data Ingestion Layer

Elastic will integrate with the Data Aggregation/Ingestion Layer through:

- Direct ingestion of processed data from packet brokers
- Normalization of raw DNS logs and internet traffic into structured formats
- Support for high-throughput ingestion (50,000+ events per second)

Threat Intelligence Platform

Elastic will serve as the foundation for the Threat Intelligence Platform by:

- Storing and indexing threat intelligence feeds
- Enabling correlation between threat data and observed traffic
- Supporting real-time updates to detection rules based on new threat intelligence
-

AI & Automation Stack

In future phases, Elastic will integrate with the AI Automation Stack:

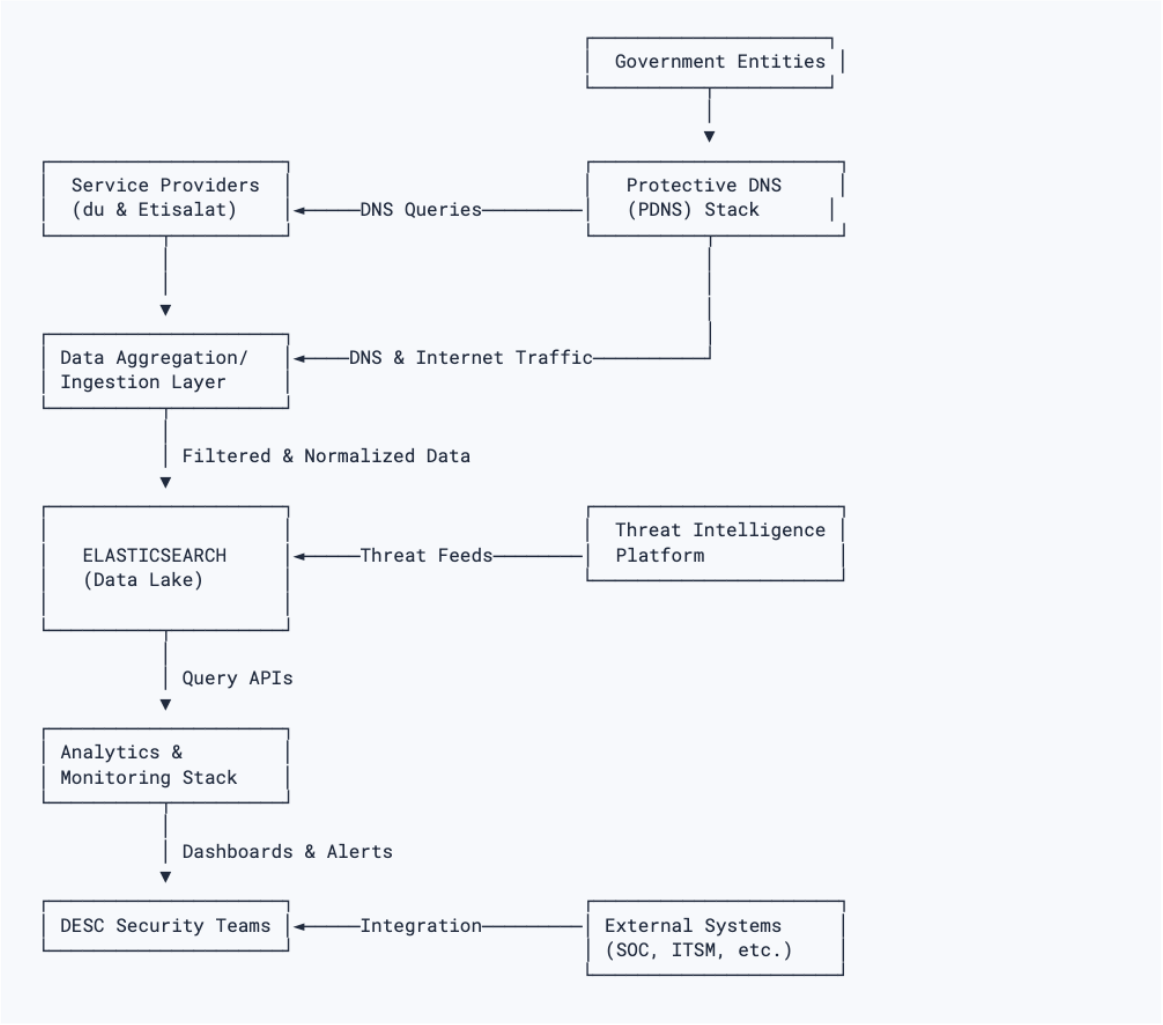
- Providing normalized data to the custom security LLM
- Supporting vector search for similarity detection
- Enabling automated workflows through the AI Agent Studio

Elastic forms the backbone of DESC's Security & Observability Architecture, delivering a unified platform for data storage, security analytics, and comprehensive monitoring. Its scalable, distributed architecture aligns perfectly with DESC's requirements for a georedundant, high-performance solution that ensures data sovereignty while enabling advanced security use cases.

By leveraging Elastic as the central data lake and analytics engine, DESC will gain comprehensive visibility into DNS and internet traffic across Dubai's government ecosystem, enhancing their ability to detect, investigate, and respond to cyber threats while ensuring compliance with regulatory requirements.

9.4.6 Elastic Integration

How Elasticsearch Will Integrate with Other Entities of the RFP and the Traffic Flow



9.4.7 Overview of Integration Architecture

Elasticsearch serves as the core data lake component within the DESC Security & Observability Architecture, integrating with multiple components across the solution. The integration architecture follows a multi-layered approach where Elasticsearch functions as the central repository for data storage, search, and analytics capabilities.

9.4.8 Integration with Data Sources and Traffic Flow

9.4.8.1 Data Aggregation/Ingestion Layer to Elasticsearch

Traffic Flow:

1. **DNS Traffic Sources:**
    - Service providers (du and Etisalat) forward DNS traffic (requests/responses) from government departments
    - Traffic is received by packet brokers in the aggregation layer
    - Packet brokers filter, deduplicate, and normalize the traffic
    - Data is forwarded to Elasticsearch via high-throughput connections (supporting 30,000+ DNS events/second)
2. **Internet Traffic Sources:**
    - Internet traffic is captured at two positions:
        - Internet Core: Filtered at service providers' core using public IP subnets
        - Access Network: Mirrored from individual access ports via ERSPAN
    - Traffic is aggregated by packet brokers with advanced deduplication (99% accuracy)
    - Normalized data is forwarded to Elasticsearch with <1ms latency
3. **Protective DNS (PDNS):**
    - PDNS logs are captured at 30K+ events/sec and encrypted with TLS 1.3
    - Logs are forwarded via syslog or gRPC to the aggregation layer
    - Initial filtering is applied (e.g., dropping non-government queries)
    - Data is relayed to Elasticsearch with sequence numbering and <1ms forwarding latency

9.4.8.2 Data Structure in Elasticsearch

Elasticsearch implements a multi-tenant architecture with:

1. **Dedicated** DNS Tenant:
    - Stores DNS logs in structured format (JSON)
    - Fields include query name, response IP, timestamp, status
    - Retention period: 18 months with tiered storage (Hot: 30 days, Cold: 60 days, Frozen: 270 days)
    - Deployed in Active/Active HA/DR configuration
2. **Internet Traffic Tenant:**
    - Stores internet traffic metadata and content
    - Normalized data includes source/destination IP, port, protocol, packet size, timestamp, application type
    - Retention period: 9 months with tiered storage (Hot: 30 days, Cold: 60 days, Frozen: 90 days)
    - Deployed in Active/Passive HA/DR configuration

9.4.8.3 Integration with Analytics and Monitoring Stack

Elasticsearch provides the foundation for the Analytics and Monitoring Stack through:

1. **RESTful APIs for Data Access:**
    - Exposes APIs for querying and accessing data
    - Supports the Analytics Stack with <1-second query latency
    - Enables seamless integration with visualization tools
2. **Event Correlation Engine:**
    - Links DNS anomalies with threat intelligence matches
    - Generates prioritized incident tickets with severity levels
    - Supports automated workflows for initial response
3. **Visualization & Reporting Framework:**
    - Powers dashboards displaying real-time metrics

- Supports exportable reports in PDF/CSV formats
- Enables drill-down capabilities for detailed analysis

9.4.8.4 Integration with Threat Intelligence Platform

Elasticsearch integrates with the Threat Intelligence Platform by:

1. **Storing and Indexing Threat Intelligence:**
    - Ingests multi-source intelligence feeds (10,000+ indicators daily)
    - Creates a searchable index tied to the Data Lake
    - Enables correlation with DNS logs and internet traffic
2. **Real-time Correlation:**
    - Identifies matches between observed traffic and known threats
    - Flags complex threats for the Analytics Stack
    - Supports weekly reports on correlated findings

9.4.8.5 External System Integration

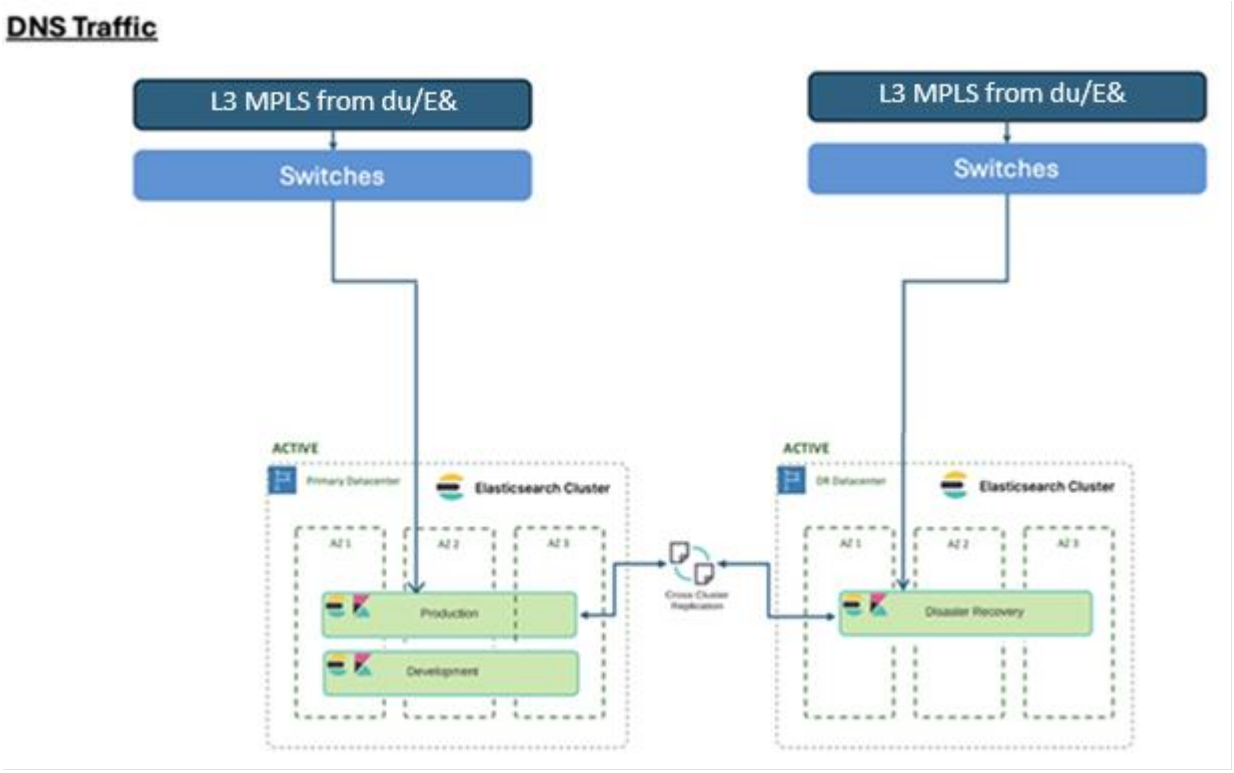
Elasticsearch enables integration with external systems through:

1. **RESTful API Gateway:**
    - Exposes 20+ APIs for government system integration
    - Supports 1,000 calls/min with OAuth 2.0 authentication
    - Enables integration with SOC tools and ITSM platforms
2. **Security Orchestration:**
    - Enables automated responses through REST API calls
    - Supports connector execution for actions like blocking IPs
    - Facilitates integration with SOAR systems and ticketing platforms
3. **Case Management Integration:**
    - Provides integration with leading case management solutions (JIRA, ServiceNow)
    - Supports both manual and automatic case creation
    - Enables attachment of artifacts related to security incidents

9.4.9 Elastic Data Structure

How Elastic would structure and store the Data across Primary and DR.

9.4.9.1 DNS Traffic Architecture



DNS Traffic Architecture - Data Flow (Phase-1)

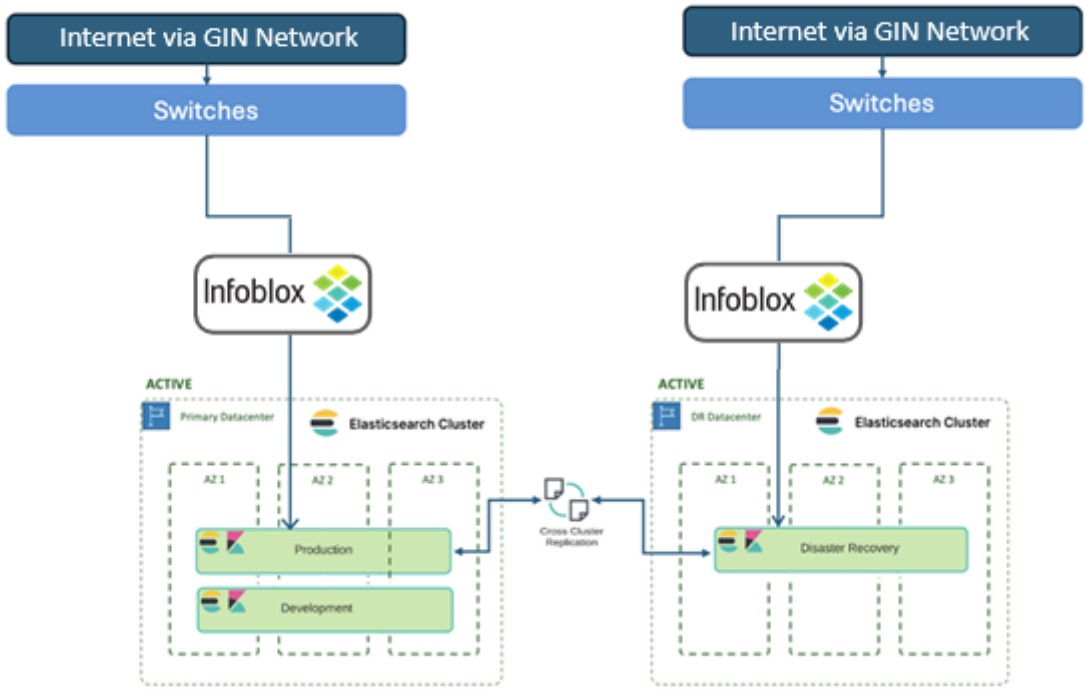
- DNS security logs sourced from the two service providers du and Etisalat after they will apply DNS security on the DNS traffic sourced from the government departments would be forwarded to the newly deployed SIEM/Data Lakes
- These logs would be carried over an L3 MPLS provided by respective service providers which would be extended to both the primary and DR datacentres.
- The alternate mechanism to carry these security logs to DESC platform is the IPSec tunnels which could be built between the service provider infrastructure and the perimeter firewalls.
- The DNS security logs would then be forwarded directly to the Elasticsearch clusters via the IP network.
- The Primary Datacentre Elasticsearch cluster (marked ACTIVE) receives the DNS traffic and distributes it across multi-zone setup for fault tolerance within the region.

- The data across the Primary and DR Elasticsearch clusters would be synced via the inter-DC 10G links.
- Within the Primary Datacenter, the cluster routes DNS data to the Production deployment (handling live queries, dashboards, and security monitoring) and the Development deployment (for testing and separate analytics).
- The DR cluster routes DNS data to its Disaster Recovery deployment, which operates as a fully functional cluster with complete read/write capabilities, not a passive standby.
- Cross-Cluster Replication (CCR) maintains bi-directional synchronization between both clusters—Production data replicates from Primary to DR, and DR data replicates back to Primary—ensuring data consistency even if one cluster temporarily loses direct ingestion.
- Both clusters actively serve user queries, allowing applications and users to access DNS data from either cluster based on geographic proximity, load balancing requirements, or availability.
- If the Primary Datacenter fails, the DR cluster receives the live DNS traffic directly applications simply redirect queries to the DR cluster.
- If the DR Datacenter fails, the Primary cluster continues operating normally with full DNS traffic ingestion and query capabilities—no failover procedures required.
- Analytics and security teams can distribute their query workload across both clusters, improving performance and reducing the load on any single cluster while maintaining access to complete DNS traffic data across both Du and Etisalat networks.

DNS Traffic Architecture - Data Flow (Phase-3)

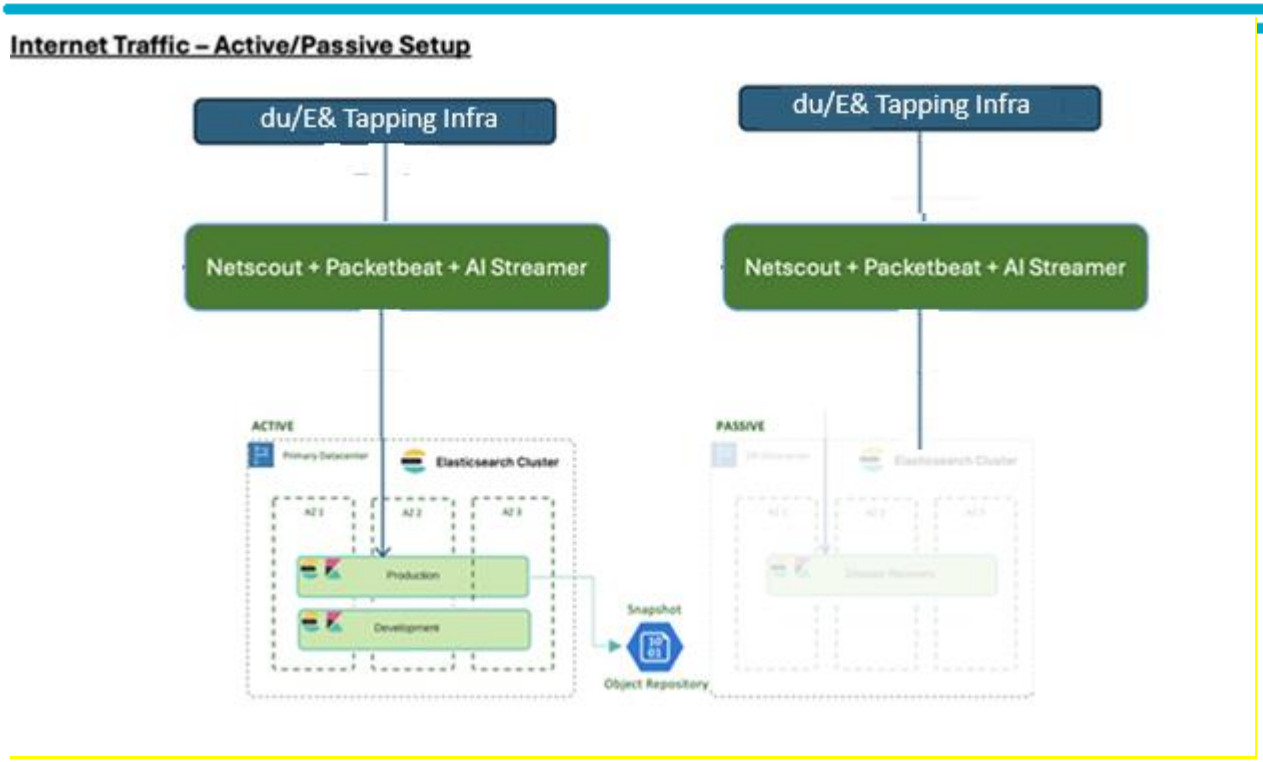
- Once the new Infoblox PDNS platform will be operational in Active/Active state in Primary and DR DCs, the DNS security would be applied locally on the DNS traffic being received from the government departments via GIN network.
- The DNS security logs will be forwarded by the corresponding Infoblox PDNS platforms to the Elasticsearch clusters locally.

DNS Traffic



- Cross-Cluster Replication (CCR) maintains bi-directional synchronization between both clusters—Production data replicates from Primary to DR, and DR data replicates back to Primary—ensuring data consistency even if one cluster temporarily loses direct ingestion.
- Both clusters actively serve user queries, allowing applications and users to access DNS data from either cluster based on geographic proximity, load balancing requirements, or availability.
- If the Primary Datacenter fails, the DR cluster receives the live DNS traffic directly applications simply redirect queries to the DR cluster.
- If the DR Datacenter fails, the Primary cluster continues operating normally with full DNS traffic ingestion and query capabilities—no failover procedures required.

9.4.9.2 Internet Traffic Active/Passive Architecture



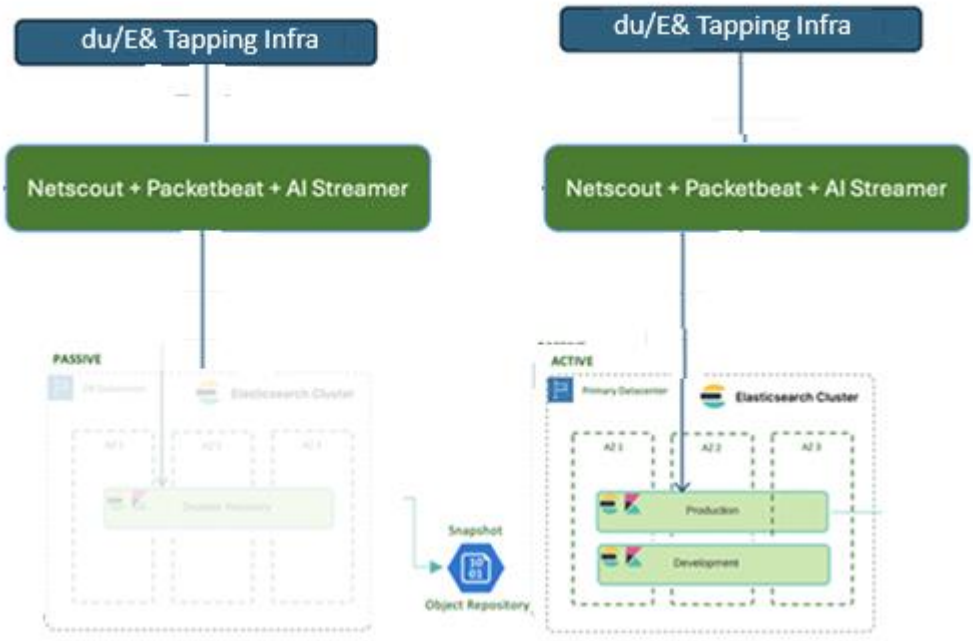
Scenario 1: Normal Operations (Active/Passive with Snapshot Backup)

- Internet traffic originates from two telecom providers—Du network on the left side and Etisalat network on the right side—generating network traffic from their respective infrastructures.
- Traffic from each provider passes through their network switches, which aggregate and forward the internet traffic from their edge infrastructure.
- Both traffic streams converge at the unified network monitoring layer (NetScout + Packetbeat + AI Streamer), which captures packets, analyzes protocols, and enriches the data with metadata.
- The processed internet traffic data flows into the Network Load Balancer, which acts as the primary distribution point routing traffic to the active cluster only.
- During normal operations, the Network Load Balancer sends ALL internet traffic data exclusively to the ACTIVE cluster in the Primary Datacenter—the passive cluster receives NO direct ingestion from the load balancer.
- The Active (Primary Datacenter) Elasticsearch cluster receives the internet traffic and distributes it across multi-zone setup for high availability.

- Within the Active cluster, internet traffic data is routed to the Production deployment (handling live queries, dashboards, and real-time monitoring) and the Development deployment (for testing and analytics).
- The Production deployment indexes all incoming internet traffic with full read/write capabilities, enabling security teams and network operations to perform real-time analysis, threat detection, and traffic pattern monitoring.
- The Active cluster takes automated snapshots of all indices on a scheduled basis (typically daily) and stores them in an Object Repository (S3, Azure Blob Storage, or similar cloud storage).
- These snapshots capture the complete state of internet traffic data including all indices, cluster configuration, and metadata, providing a point-in-time backup for disaster recovery.
- The Passive (DR Datacenter) Elasticsearch cluster remains in standby mode during normal operations—it is NOT receiving live traffic ingestion and is NOT receiving Cross-Cluster Replication (unlike the DNS active/passive setup).
- The Passive cluster has access to the same Object Repository where snapshots are stored, allowing it to restore data when needed during a failover event.
- The Passive cluster maintains its infrastructure across multi-zone setup in the DR location but operates at minimal capacity with the Disaster Recovery deployment ready but not actively processing data.

Scenario 2: Failure Event Trigger (Active Cluster Fails - Passive Promotion)

Internet Traffic – Active/Passive Setup



- The Active cluster in the Primary Datacenter experiences a failure event (datacenter outage, cluster health RED status, network partition, or disaster), triggering automated failure detection after threshold breaches (typically 5 minutes of unavailability).
- Automated monitoring and alerting systems detect the Active cluster failure and immediately notify the operations team while initiating the automated failover runbook.
- The Primary Datacenter is now marked as PASSIVE (shown grayed out in the diagram with X marks), indicating it is no longer accepting traffic or processing data—both Production and Development deployments are offline.
- The DR Datacenter is promoted from PASSIVE to ACTIVE status, preparing to take over all internet traffic ingestion and processing responsibilities.
- The failover process begins with the Passive cluster accessing the Object Repository to restore the most recent snapshot, retrieving the last known good state of internet traffic data from the Active cluster.
- The snapshot restore operation loads all indices, cluster state, and configuration from the Object Repository into the now-promoted Active cluster in the DR Datacenter across its three availability zones.

- Once the restore completes, the Disaster Recovery deployment converts from read-only standby to a fully operational production deployment with complete read/write capabilities.
- The Network Load Balancer is reconfigured (either manually or through automated failover scripts) to redirect internet traffic from the failed Primary Datacenter to the newly active DR Datacenter cluster.
- The monitoring layer (NetScout + Packetbeat + AI Streamer) updates its output configuration to send processed internet traffic data to the DR cluster's ingestion endpoints instead of the failed Primary cluster.
- The DR cluster begins accepting live internet traffic from both Du and Etisalat networks through the load balancer, resuming real-time indexing and analysis capabilities.
- Applications, dashboards, security monitoring tools, and analytics platforms are redirected to query the newly active DR cluster by updating connection endpoints, DNS records, or load balancer configurations.
- To minimize data loss, the monitoring layer may have buffered internet traffic locally during the failover window, which can be replayed to the newly active cluster once it's operational, reducing the actual RPO.
- The newly active DR cluster continues operating as the primary production cluster, processing all internet traffic from both telecom providers and serving all query requests from users and applications.

The DR cluster now takes over the snapshot responsibility, creating new backups to the Object Repository to ensure continued disaster recovery capability from its new active role

9.4.9.3 Failback Process (Restoring Original Primary Datacenter)

- Once the original Primary Datacenter is restored, brought back online, and validated as healthy, a failback plan is developed to return to the normal active/passive configuration.
- The restored Primary Datacenter cluster accesses the Object Repository and restores the most recent snapshots created by the current Active (DR) cluster to synchronize data.
- After restoration is complete, any internet traffic data ingested by the DR cluster during the failover period that wasn't captured in snapshots is synchronized via CCR

9.4.10 Security Use Cases (DNS)

All the DNS security use cases outlined above can be fully achieved using the Elastic platform. Elastic will rely on NetScout as the primary source for DNS and HTTP metadata collected from both ISPs, ensuring complete visibility into all outbound and inbound traffic. Once the enriched metadata is ingested into Elastic, we can apply Machine Learning jobs, ES|QL analytics, threat intelligence correlation, and custom detection rules to identify threats such as C2 communication, DNS tunnelling, DGAs, typo squatting, fast-flux behavior, exfiltration attempts, DoH misuse, and policy violations. This combined approach provides a comprehensive and scalable DNS-security detection framework powered by high-quality NetScout telemetry and Elastic's advanced analytics.

Use Case	Description	Detection Method	Elastic Comments
Malware C&C Communication	Detects malware communicating with command-and-control servers.	Look for repeated queries to known malicious domains or domains with randomized patterns (DGAs).	We can enrich the logs with threat intelligence data and use the built-in DGA detection machine learning jobs in Elastic to detect this threat.
DNS Tunneling	Identifies covert data exfiltration via DNS requests.	Analyze unusually long domain names, high TXT/NULL record usage, or	We can use Machine Learning (ML) or ES|QL queries in Elastic to detect

Use Case	Description	Detection Method	Elastic Comments
		abnormal query volume.	abnormally long domain names, high TXT/NULL record usage, and unusual DNS query volumes indicating potential tunneling activity.
Phishing & Typosquatting	Detects domains mimicking legitimate brands (e.g., paypall.com).	Use regex or threat intelligence feeds to flag typosquatted domains.	We can use fuzzy searches and threat intelligence correlation in Elastic to flag typosquatted or look-alike domains
DGA Detection	Finds malware using Domain Generation Algorithms (DGAs).	Look for randomized domain strings (e.g., xyz123abc.com) in bulk queries.	We can use Elastic's built-in DGA detection ML jobs or custom ES|QL pattern analysis to identify randomized domain strings (e.g., xyz123abc.com) appearing in bulk DNS queries, which often indicate Domain Generation Algorithm (DGA) activity.
DNS Amplification Attacks	Detects DDoS attacks abusing DNS resolvers.	Monitor spikes in large DNS responses (e.g., TXT records) from external IPs.	We can use Machine Learning jobs with high-count aggregation metrics

Use Case	Description	Detection Method	Elastic Comments
			on DNS response sizes to detect sudden spikes in large DNS responses (e.g., TXT records) originating from external IPs, indicating possible amplification attacks.
Fast Flux Networks	Identifies domains with rapidly changing IPs (low TTL) hiding botnet servers.	Track frequent IP changes for a single domain.	We can detect frequent IP changes for a single domain using a Machine Learning job or ES|QL transform that tracks the count of unique destination.ip values per domain over time. A high rate of IP churn within short intervals can indicate Fast Flux network behavior.
DNS Cache Poisoning	Detects spoofed DNS responses redirecting users to malicious IPs.	Compare DNS responses with authoritative records for mismatches. Monitor excessive NXDOMAIN responses from a single source.	We can compare the DNS answer field with authoritative field to look for a mismatch, Additionally, we can use ES|QL or ML jobs to monitor excessive NXDOMAIN responses from

Use Case	Description	Detection Method	Elastic Comments
			a single source, which is a strong indicator of reconnaissance or DGA activity.
Internal Reconnaissance	Spots attackers mapping internal networks.	Compare DNS responses with authoritative records for mismatches; monitor excessive NXDOMAIN responses from a single source.	We can compare the DNS answer field with authoritative field to look for a mismatch, Additionally, we can use ES|QL or ML jobs to monitor excessive NXDOMAIN responses from a single source, which is a strong indicator of reconnaissance or DGA activity.
Shadow IT Detection	Identifies unauthorized cloud service or domain shadowing usage (e.g., Dropbox, AWS).	Flag queries to domains not whitelisted in corporate policies; look for unusual subdomains (e.g., update.microsoft.evildomain.com).	We can detect this by comparing DNS queries against a whitelisted domain policy and using threat intelligence correlation or DGA detection ML jobs to flag unusual or suspicious subdomains (e.g., update.microsoft.evildomain.

Use Case	Description	Detection Method	Elastic Comments
			com).
DNS Hijacking	Detects unauthorized DNS resolver changes.	Monitor unexpected DNS server configurations (e.g., rogue resolvers).	We can detect this by monitoring unexpected DNS resolver configurations using ES|QL queries or custom detection rules that alert when endpoints or devices send DNS traffic to non-approved or rogue DNS servers outside the corporate policy.
Botnet Traffic	Identifies devices communicating with botnet infrastructure.	Correlate DNS logs with threat intelligence feeds for known botnet domains.	We can use Elastic's built-in Indicator Match rules to automatically correlate DNS logs with threat intelligence feeds, allowing immediate detection of queries to known botnet-associated domains. This provides real-time matching against TI sources such as Abuse.ch, AlienVault OTX, and any custom threat feed ingested

Use Case	Description	Detection Method	Elastic Comments
			into Elastic.
Data Exfiltration via Subdomains	Detects data leakage through subdomain queries (e.g., data.leak.example.com).	Analyse high volumes of unique subdomains from a single source.	We can detect this using Machine Learning jobs that group DNS activity by source IP and analyse the cardinality and volume of unique subdomains queried. A sudden spike in unique subdomain requests from a single host is a strong indicator of data exfiltration or tunnelling activity.
Geographic Anomalies	Flags DNS queries resolving to unexpected countries.	Compare resolved IP geolocation with user or device baseline.	We can detect this by using Machine Learning jobs to baseline normal geolocation patterns for each user or device, and then alert when DNS-resolved IPs originate from unusual or high-risk countries, indicating possible domain abuse or malicious redirection.

Use Case	Description	Detection Method	Elastic Comments
NXDOMAIN Floods	Identifies failed DNS lookups indicating DGA failures or scanning.	Track high rates of NXDOMAIN responses per host.	We can detect this by using ES|QL queries or Machine Learning jobs to track NXDOMAIN response rates per host. A high volume of NXDOMAIN errors from a single source typically indicates DGA activity, reconnaissance, or misconfigured/malicious software.
Unauthorized DNS over HTTPS (DoH)	Detects use of encrypted DNS to bypass corporate filters.	Monitor traffic to DoH endpoints (e.g., cloudflare-dns.com).	We can detect this by monitoring traffic to known DoH endpoints using saved ES|QL/KQL queries and dashboards in Kibana
Sinkhole Alerting	Tracks infected devices communicating with sinkholed domains.	Check queries to domains seized by security researchers.	We can detect this by enriching DNS logs with threat intelligence feeds, which include domains seized or sinkholed by security researchers. Indicator Match rules can then automatically flag any

Use Case	Description	Detection Method	Elastic Comments
			queries to these known compromised or sinkholed domains.
TTL Anomalies	Detects abnormally short TTL values signaling fast-flux networks.	Analyze Time-to-Live (TTL) values in DNS records.	We can detect this by using ES|QL aggregations or Machine Learning jobs to analyze TTL values in DNS responses
Zero-Day Attack Patterns	Identifies unknown threats via behavioral anomalies.	Use machine learning to baseline normal DNS traffic and flag outliers.	We can use Elastic's Machine Learning jobs to baseline normal DNS behavior and flag anomalies. Simple high-count/low-count detectors, along with rare and population-based anomaly detection, can identify unusual query volumes or patterns indicative of zero-day or unknown threats.
Policy Violations	Enforces compliance by blocking access to restricted domains.	Match DNS queries against domain categories such as gambling, adult content, or P2P.	We can detect this by performing a look up against a DNS category database, provided by the

Use Case	Description	Detection Method	Elastic Comments
			customer, and enriching DNS logs to classify domains (e.g., gambling, adult content, P2P). Detection rules can then alert on any queries that violate corporate policies.

9.4.11 Security Use Cases (HTTP)

Use Case	Description	Implementation
1. Threat Detection & Incident Response		
Command & Control (C2) Communication Detection	Identify traffic between infected hosts and attacker-controlled servers.	Extract domain, IP, and port metadata from headers
		Analyze unusual DNS queries and beaconing patterns
		Correlate with threat intelligence feeds.
Malware Payload Detection	Detect malicious file downloads or script injection	Extract and inspect payloads using deep packet inspection (DPI).
		Analyze file signatures with YARA rules.
		Compare hashes against known malware databases (VirusTotal,

Use Case	Description	Implementation
		MISP).
Botnet & DGA-Based Communication	Detects bot-infected devices communicating via dynamically generated domains.	Analyze domain names using entropy scoring.
		Monitor for rapid DNS changes (fast flux).
		Correlate with known botnet indicators.
Phishing & Malicious Site Access	Identify users accessing phishing or malicious sites.	Extract HTTP/S headers and URL parameters.
		Cross-reference URLs with phishing threat intelligence lists
		Analyze TLS certificates for anomalies.
2. Data Exfiltration & Insider Threat Detection		
DNS Tunneling & Covert Channels	Detects data exfiltration via DNS queries.	Monitor for long, high-frequency DNS queries.
		Detects TXT record anomalies.
		Identify patterns matching DNS tunneling tools (Iodine, DNScat).
Unusual File Transfers (Exfiltration via HTTP, FTP, SMTP, etc.)	Identify unauthorized data transfers outside the organization.	Extract metadata from HTTP POST, FTP, SMTP headers.
		Analyze data size anomalies (e.g., sudden spikes in uploads).

Use Case	Description	Implementation
		Apply regex on payloads to detect sensitive data (e.g., credit card numbers, SSNs).
Encrypted Traffic Without Legitimate Business Use	Detect unauthorized encrypted channels.	Identify TLS traffic without proper SNI or certificates
		Detects non-standard ports for encrypted traffic.
Unauthorized API Calls & Cloud Storage Access	Monitor and restrict sensitive data uploaded to cloud services.	Analyze HTTP POST/PUT requests to cloud storage services (Google Drive, Dropbox, AWS S3).
		Apply steganalysis algorithms to detect hidden data.
Steganography-Based Data Exfiltration	Detects hidden data transfers in images, audio, or other media.	Extract and analyze multimedia payloads.
		Apply steganalysis algorithms to detect hidden data
3. Network Visibility & Performance Monitoring		
Application & Protocol Usage Analysis	Monitor application usage across the network.	Classify traffic using DPI (Deep Packet Inspection).
		Identify unknown applications or unauthorized services.
Bandwidth Usage & Anomaly Detection	Identify excessive bandwidth consumption by users or	Analyse traffic volume per user/IP/application.

Use Case	Description	Implementation
	services.	Detects spikes in traffic that may indicate data exfiltration or DDoS.
Network Latency & Packet Loss Monitoring	Identify latency issues in network communication.	Analyse TCP SYN-ACK delays and retransmissions.
		Extract and correlate timestamp data for network performance trends.
TLS Certificate & Encryption Analysis	Identify outdated or self-signed certificates.	Extract and analyse TLS handshake data.
		Identify weak encryption algorithms (e.g., TLS 1.0, RC4).
Peer-to-Peer (P2P) & Unauthorized Proxy Detection	Detect P2P file sharing or circumvention of security policies.	Extract protocol fingerprints from traffic.
		P2P applications (BitTorrent, Tor).
4. Attack Surface Monitoring & Compliance		
Unauthorized Use of Shadow IT Services	Identify usage of unauthorized SaaS applications.	Extract domain names from HTTP/S headers.
		Cross-reference against an approved service list.
Compliance Monitoring (HIPAA, GDPR, PCI DSS)	Ensure network traffic aligns with security regulations	Monitor for unencrypted sensitive data transfers.
		Apply compliance-specific pattern

		matching in payload analysis.
Rogue Device Detection	Identify unauthorized devices connecting to network	Correlate MAC addresses and DHCP logs.
		Detects non-compliant OS and firmware signatures
5. DDoS & Anomaly Detection		
DDoS Attack Detection (Volumetric, Slowloris, etc.)	Identify traffic anomalies indicating a denial-of-service attack.	Monitor traffic spikes to a specific IP or port.
		Detects abnormal SYN flood, UDP flood, or ICMP patterns
		Correlate traffic with known attack sources.
Reflection & Amplification Attacks	Detect traffic leveraging open resolvers for amplification.	Identify traffic from internal systems to known amplification vectors (NTP, SSDP, DNS).
		Flag high response-to-request ratio patterns.
Tor & Anonymized Traffic Detection	Identify traffic originating from anonymous sources.	Cross-check with known Tor exit nodes.
		Detects non-standard TLS handshake patterns.
6. Advanced Threat Hunting & Forensics		
Retrospective Investigation of Network Attacks	Analyse past traffic for Indicators of Compromise	Query historical traffic logs stored in the data lake

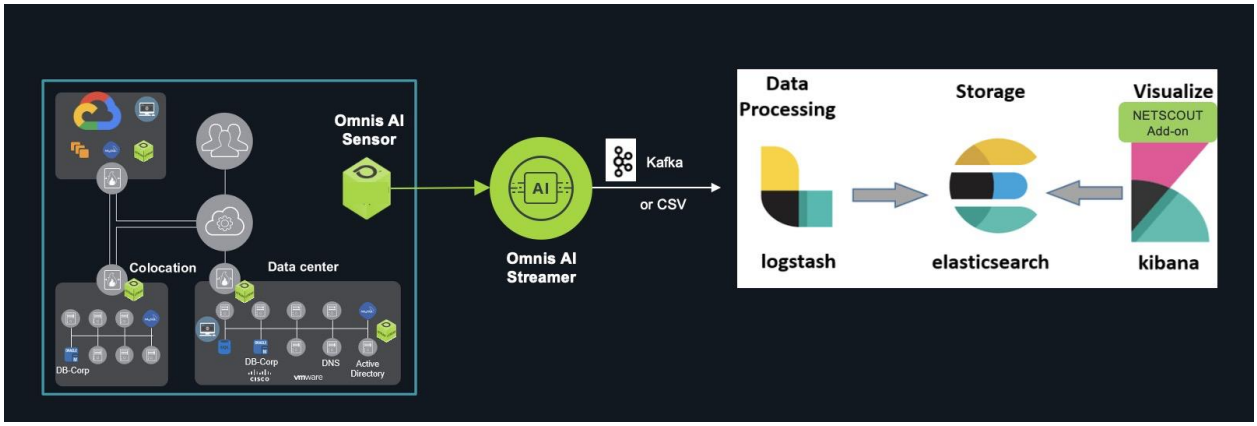
	(IoCs).	Search for IoCs based on newly discovered threats.
Attribution & Correlation of Threat Actors	Link malicious activities to specific entities.	Combine DNS, HTTP, and TLS metadata.
		Correlate multiple logs to attribute attacks to specific actors
Threat Intelligence Enrichment	Enhance logs with external intelligence feeds.	Integrate with OSINT, MISP, VirusTotal, and other TI platforms.
		Automatically flag malicious entities in logs.
7. User & Entity Behavior Analytics (UEBA)		
Abnormal User Login & Access Patterns	Detect compromised credentials or insider threats.	Correlate network logs with authentication logs.
		Identify logins from unusual geolocations.
Time-Based Access Anomalies	Detecting unusual activity outside working hours.	Identify high-risk actions performed during non-business hours.
Device Fingerprinting & Behavioural Monitoring	Track normal vs. anomalous behavior per device.	Compare current traffic patterns to historical baselines.
		Flag deviations indicating compromise.

9.4.12 Data Ingestion Infrastructure

DU is proposing NetScout Solution for meeting the DESC requirements for Data Ingestion Infrastructure. NETSCOUT is a pioneer in Deep Packet Inspection (DPI) technology and has a deep understanding of network, applications, all the protocols and the stateful interactions that make up Enterprise networks.

As enterprise networks are getting complex with numerous services offered using on-prem, cloud and hybrid models, it is becoming necessary to streamline and automate the actions for faster resolution and least manual intervention. AIOps is geared towards achieving this goal and many organizations have embraced the concept of automation. NETSCOUT's Omnis AI Insights solution offering is aimed at fulfilling the needs of AIOps initiatives with enterprise organizations and enable automation using surrounding tools and technologies. NETSCOUT's Omnis AI Insights solution offering consisting of Omnis AI Sensor and Omnis AI Streamer products facilitates automation and AIOps initiative with crisp data and metrics (where applicable) reducing data volumes significantly at source. The flexible architecture has default Omnis AI Feeds that can be used out of the box as well as custom defined feeds can be provisioned as well for targeted use cases.

9.4.13 NetScout Solution Summary



9.4.13.1 Omnis AI Feeds

Omnis AI Sensor

The NETSCOUT Omnis AI Sensor was purpose-built to help companies achieve their most ambitious business goals. It is designed to enhance service performance by gathering highly granular operational performance intelligence with DPI-derived insights at the source for accelerated troubleshooting. Through its unique scalable architecture, sensors collect invaluable intelligence to deliver unparalleled operational and business insights crucial for optimizing performance and ensuring the overall health and security of networks, applications, and services. The Omnis AI Sensor is the first step in providing the 'high-octane fuel' organizations need to sharpen their competitive edge and unlock their true potential. Omnis AI Sensor

instrumentation can be strategically deployed at network vantage points to collect real-time information on a wide array of critical metrics required to drive successful AIOps and security initiatives. It plays a pivotal role in assisting organizations' business initiatives including: Omnis AI Insights Solution The Omnis AI Sensor is a critical component of the Omnis AI Insights solution, which also includes the Omnis AI Streamer and the Omnis AI Feed.

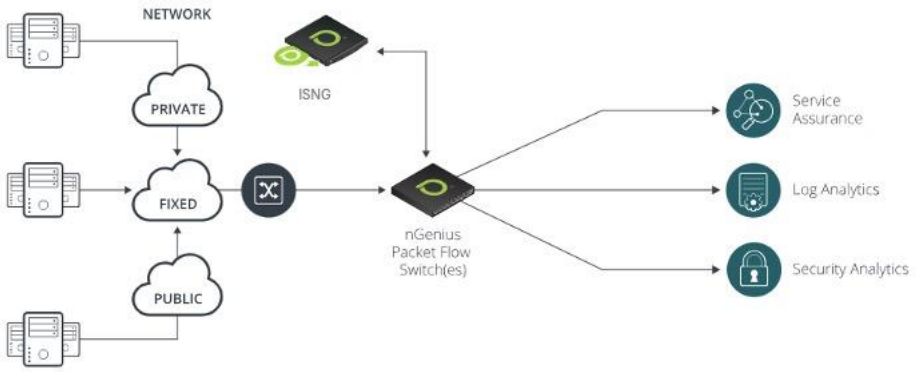
Omnis AI Streamer

The Omnis AI Streamer performs feature extraction on observability telemetry data at scale, delivering essential insights for organizations. This enables the regular feeding of high-quality, curated data into AIOps, security solutions, or data lakes for custom analysis and processing. The data, known as the Omnis AI Feed, consists of high-level operational metadata, including detailed session-level and conversation-level tables derived from Deep Packet Inspection (DPI). The data is extracted and organized into domain-specific, targeted feeds, which can be easily ingested into data lakes or streamed through pipelines to our NETSCOUT partners such as Splunk, ELK Stack, ServiceNow, Datadog, and others. NETSCOUT refines Omnis AI Feed intelligence using AI and machine learning processes on DPI data, creating enhanced telemetry to accelerate troubleshooting and enable successful business outcomes. Examples include application and service performance, service level objectives, cloud migration projects, asset management, application certificates management, unified communications, cybersecurity (threat detection, investigation, and compliance). The Omnis AI Streamer enables precise decision-making for superior results, facilitating rapid troubleshooting and protection of complex environments. The Omnis AI Feed's metadata covers services, applications, network components, and transactions—providing insights into deployment, service availability and performance, and user experience to deliver exceptional business value.

9.4.13.2 Instrumentation

nGenius PFS - Deliver cost-effective and complete packet visibility while streamlining your monitoring architecture and reducing security risks.

In response to multiple globally distributed aggregation points, NETSCOUT proposes the wire-speed nGenius PFS for high- performance monitoring, which will improve the control and distribution of IP traffic being fed into the monitoring device. The nGenius **PFS will** enable better capture monitored traffic with high-density packet aggregation and intelligent filtering capabilities, enabling a more flexible and comprehensive approach to capturing, collecting, and leveraging important packet flows. With 1GbE, 10GbE, 25GbE, 40GbE, 100GbE, and 400GbE port options, PFS offer SFP+, SFP28, QSFP+, QSFP28, and QSFP-DD ports in various 1RU and 2RU fixed configuration form factors, and support 720 Gbps to 12800 Gbps throughput with non-blocking switching fabrics.



nGenius PFS 7000 series - Expand Your Visibility Fabric with Advanced Packet Broker Functionality

PFS 7000 series operate at speeds from 1Gbps to 400Gbps. In addition to core packet broker functionality, such as filtering, load balancing, aggregation, and replication, they provide advanced capabilities including header stripping, L2GRE and VxLAN tunnel origination and termination, time stamping and inline security with the external PowerSafe TAP integration. Enabled with self-organizing mesh technology, the nGenius PFS 7000 series easily scales for massive network monitoring needs.

ISNG – Expert Packet Conditioning

ISNG is a software application enabling expert packet conditioning for service assurance and cybersecurity monitoring. The solution is built on the NETSCOUT InfiniStreamNG platform and framework leveraging patented technologies. As part of the nGenius Packet Flow System (PFS) portfolio, ISNG integrates with

NETSCOUT's packet broker products to enable expert-level capabilities, such as packet deduplication, NetFlow/IPFIX generation, header stripping, packet slicing, and masking.

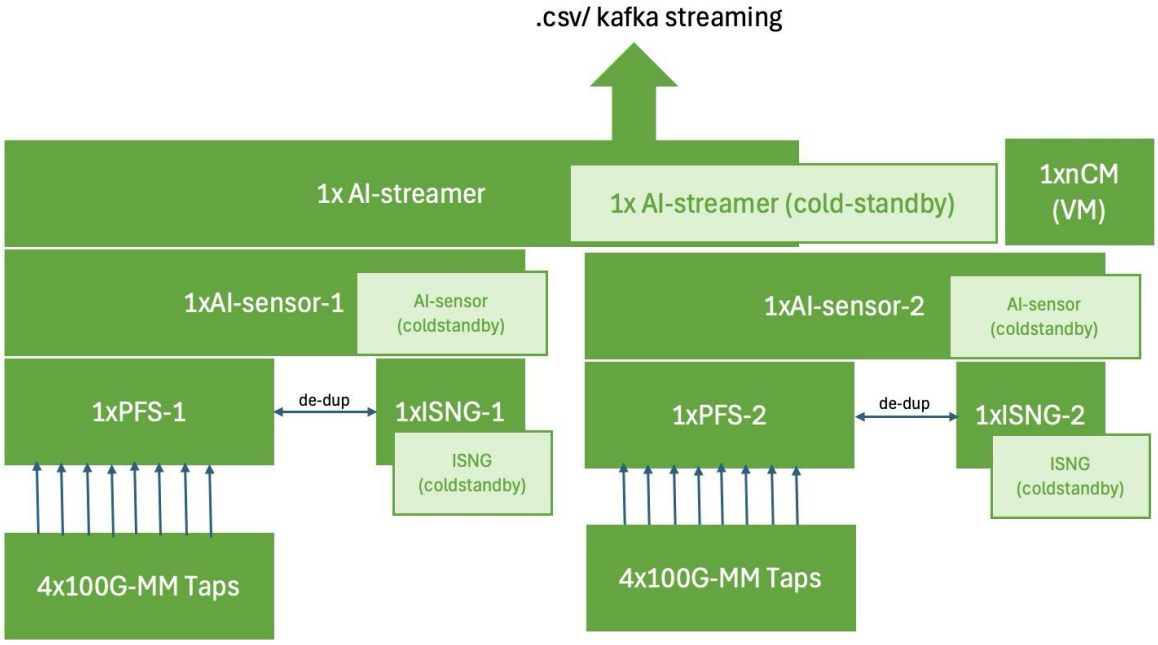
It provides a line-rate, scalable engine for expert packet conditioning and manipulation. With InfiniStreamNG as its foundation, it delivers the performance and scaling capabilities needed to process network traffic generated by millions of users using hundreds of applications. It delivers feature velocity and agility, independent of the underlying hardware platform. The common architecture across all InfiniStreamNG applications also means short learning cycles for IT personnel and operational efficiency.

NETSCOUT TAPs - Always-on Monitoring of Your IT Infrastructure

The TAP family provides network monitoring devices with full access to network traffic. Multiple options are available for various link types and speeds to maximize deployment versatility and are built for placement on any network link to enable comprehensive, always-on monitoring. Because our TAPs are never over-subscribed, they always pass every packet.

NETSCOUT TAPs are built for simplified and reliable deployment by being invisible to the network devices at both ends of the network link, and hence cause no disruption to data flows or protocol transactions.

9.4.14 DESC NetScout Solution Architecture

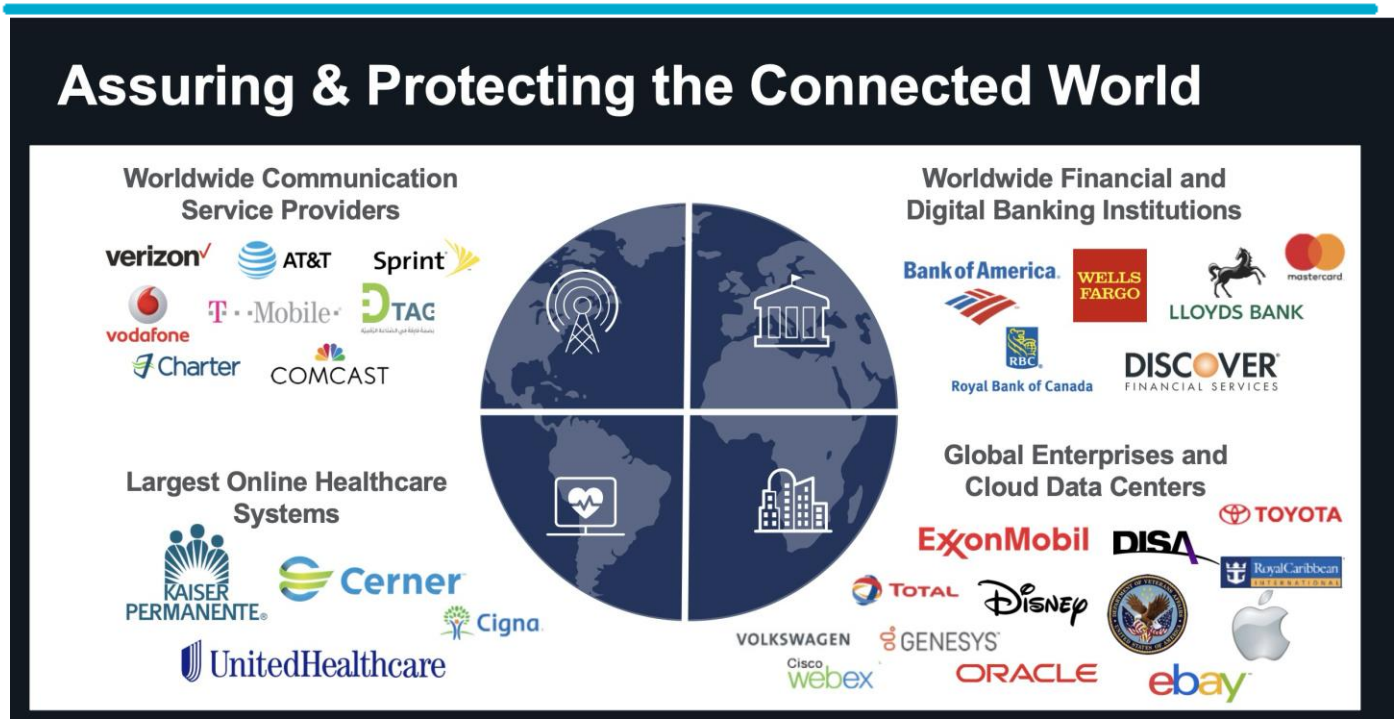


- nCM application and Omnis AI streamer application shall be installed centrally
- Omnis AI sensor (w/ 2x100G ASI NIC) to be installed in the datacenters to monitor traffic from Datacenter
- ISNG probes (w/ 2x100G ASI NIC) to be installed in each datacenter.

Redundancy

- Cold standby is provided for AI-sensors
- Cold standby is provided for ISNG probes
- Cold standby is provided for AI-streamer

9.4.15 NetScout Reference



9.4.16 Threat Intelligence Platform

Du is proposing Cyware Threat Intelligence eXchange (CTIX) Solution for meeting the DESC requirements for Threat Intelligence Platform.

CTIX is a centralized Threat Intelligence platform that helps organizations quickly detect and respond to security threats before an impact. It enables organizations to share structured Cyber Threat Intelligence (CTI). Threat Intelligence can be simply defined as the knowledge of a threat's capacity, infrastructure, motive, goals, and resources.

Following are the types of CTI you can share using CTIX:

- Technical:

  Sharing incidents that have already occurred, so that others can take precautions or work on prevention.

- Operational:

  Sharing information about potential attacks on organizations and pertinent threat actors.

- Tactical:

  Sharing information about how threat actors are going to target and the kind of strategies and tools they will be using.

- Strategic:

  Sharing information on the types of cyberattacks organizations may face in the future.

CTIX enhances an organization's interoperability and its ability to collect and disseminate threat data with other leading institutions and organizations. It enables organizations to share and access CTI. It also facilitates mutual learning and information sharing amongst subsidiaries, thereby producing a potent defensive mechanism against malicious entities. Contributing and ingesting CTI is a lot easier with STIX as all aspects of suspicion, compromise, and attribution can be represented clearly with objects and descriptive relationships. STIX information can also be visually represented by a different format. The exchange of CTI represented in STIX is communicated through Trusted Automated Exchange of Intelligence Information (TAXII) protocol over HTTPS. CTIX is defined by its capability to perform four key functions:

1. Aggregation of intelligence from multiple sources
2. Curation, normalization, enrichment of data
3. Integrations with existing security systems
4. Analysis and sharing of Threat Intelligence mechanism against malicious entities

9.4.16.1 Important of Threat Intelligence Exchange

The information shared as CTI assists in the technical, operational, tactical, and strategic defense of network-based assets. It is becoming increasingly necessary for organizations to have a CTI capability and share information with partners, peers, third party, and trusted contacts. In the ever-shifting landscape of cyber threats and attacks, access to timely information and intelligence is vital and can make a big difference in protecting organizations and firms against data breaches and security incidents.

9.4.16.2 Key Features and Capabilities

AUTOMATED INTEL INGESTION

- Automated Internal Intel Ingestion: Ingest Intel by orchestrating with multiple security tools deployed within an organization network, including SIEMs, UEBA, Antivirus, and IDS/IPS.
- Automated External Intel Ingestion: Ingest Intel from multiple sources, including TI providers, Regulatory Bodies, Peer Organizations, ISACs, Dark Web, Partner Organizations, and Subsidiaries.

- Source and Collection Management: Subscribe to multiple sources, even outside integration and in multiple formats, and make a customizable collection of them through customized polling and frequency.
- Cyware Premium Feeds (Included): Cyware's Threat Intelligence feeds to you the valuable threat data from a wide range of open and trusted sources to deliver a consolidated stream of valuable and actionable threat intelligence. Our threat intel feeds are fully compatible with STIX 1.x and 2.0, giving you the latest information on malicious malware hashes, IPs and domains uncovered across the globe in real-time.

INTEL NORMALIZATION

- Format Agnostic: Ingest data in a plethora of formats, such as MISP, STIX 1.0, STIX 2.0 MAEC, Cybox, including unstructured data from sources such as email, Free Text, Twitter etc.
- IOC conversion in multiple features: Wide-ranging format support including STIX 2.0, MISP, XML, CSV, JSON, YARA, OpenIOC, ATT&CK, MAEC, IODEF and more.
- Full Support for STIX 2.0: Full support for STIX 2.0 (JSON), as well as previous STIX versions 1.x (XML), to ensure flexible correlation, analysis, and sharing.

AUTOMATIC INTEL ENRICHMENT, CORRELATION, AND ANALYSIS

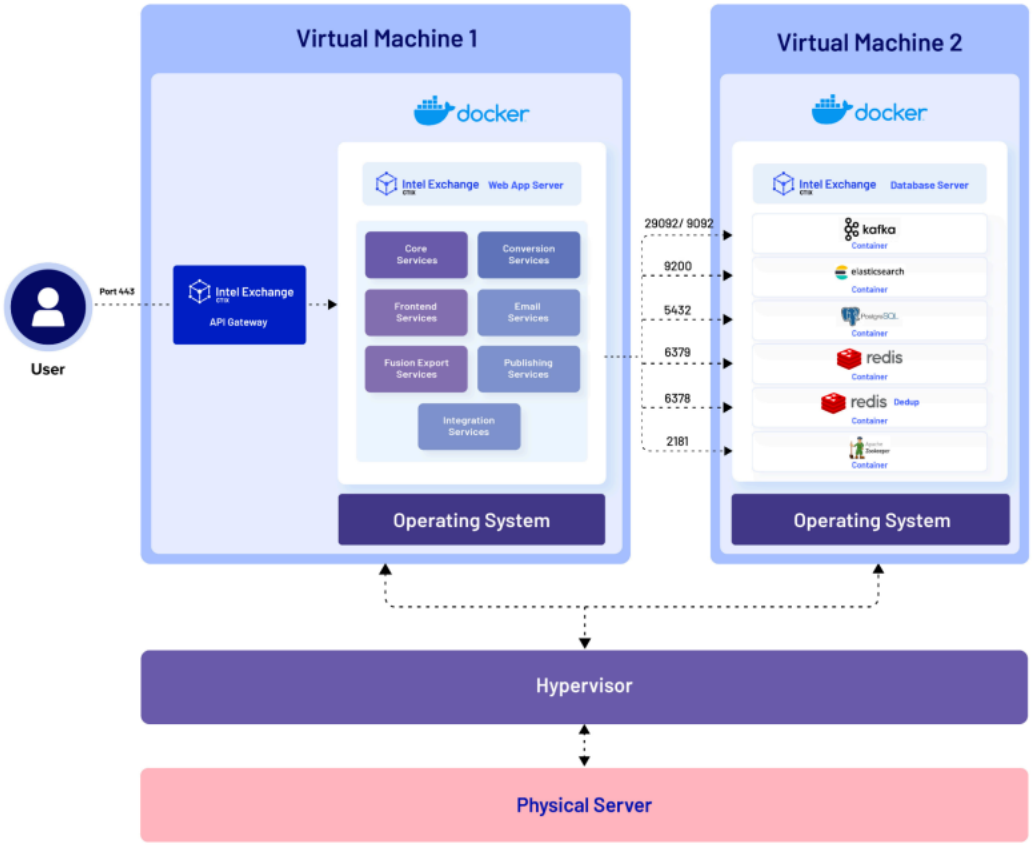
- IOC Confidence Scoring: Equips the analyst with actionable Threat Intelligence from multiple trusted sources, along with an IOC Confidence Score, on the basis of multiple parameters such as TLP, Geography, and Relation with Malware. This score allows the analyst to filter out relevant Indicators of Compromise (IOCs) automatically using rules.
- ATT&CK Navigator: Create and visualize MITRE's ATT&CK Navigator to map APT threat actor techniques and methods to identify trends across the cyber kill chain in post-exploitation hunting.
- Advanced Search and Filters: Search object and indicator types and perform an advanced search to find hidden cross-links between different attributes extracted from disparate Threat Intelligence.

- Advanced Rule Engine: Automate mundane actions, speed up Triage management, and allow the Analyst to focus more on relevant tasks using Rules module
- Indicator Deprecation: Employ customized indicator depreciation, in which the indicator expires after the decided time-span.
- TLP: RED Packages Handling: Set an expiration for TLP: RED STIX packages for secure transferring and handling of valuable tactical threat information.
- Duplicate Identification: Harness the power of machine learning for quick and efficient correlation of threat indicators, as well as the removal of duplicate data.
- Network Utility: Integrate with services such as WHOIS, VirusTotal, Shodan, Moz, and GeoIP, and empower your security analyst in accessing data collected from premium sources.

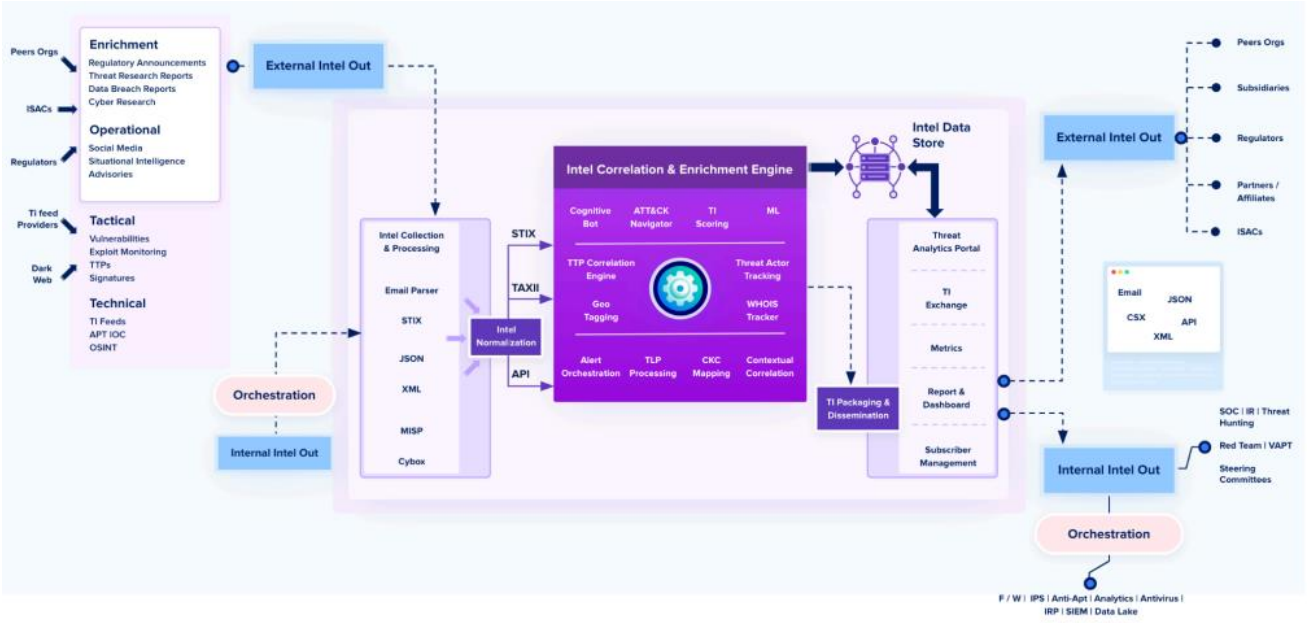
- Fang Defang: Neutralize malicious information with an obfuscated representation so it is no longer dangerous if inadvertently clicked or automatically processed in error.
- Advanced Analyst Workbench: Improve analysts' maturity and interoperability with advanced analyst workbench tools, including STIX 1.x to STIX 2.0 converter, Geo-Tagging, and WHOIS Tracker.
- Emails: Ingest Threat Intel from unstructured sources, like Email, by integrating and mapping email accounts to the CTIX dashboard. Leverage the specialized Emails module to view and analyze Intel received via Emails.
- CVSS Calculator: Capture the principal characteristics of vulnerabilities and produce a numerical score (CVSS2 or CVSS3) reflecting its severity by leveraging the built-in CVSS score calculator. Enable your analyst to process and prioritize the overall vulnerability management process effectively.

9.4.16.3 Cyware Threat Intel Exchange (TIP) Architecture

The following diagram shows a high-level two-tier deployment architecture of the Intel Exchange services on virtual machines.



The following diagram shows a high-level architecture of the Intel Exchange (CTIX).



9.4.17 SOAR – FortiSOAR – as an option

FortiSOAR is a Security Orchestration, Automation, and Response (SOAR) solution designed to help security operation centers (SOCs) efficiently handle the increasing number of security alerts and streamline their incident response processes.

It's a comprehensive platform that offers:

- Automation: FortiSOAR automates repetitive tasks, such as threat hunting, incident triage, and remediation actions, freeing up security analysts to focus on more strategic tasks
- Orchestration: It orchestrates complex workflows and integrates with various security tools, enabling seamless collaboration and information sharing between different security systems
- Response: FortiSOAR provides a unified interface for incident response, allowing security teams to quickly identify, investigate, and contain threats

9.4.17.1 Key Benefits:

- Improved Efficiency: Automation and orchestration significantly reduce manual effort and accelerate incident response times.

- Enhanced Visibility: FortiSOAR provides a centralized view of security incidents, enabling better situational awareness and faster decision-making.

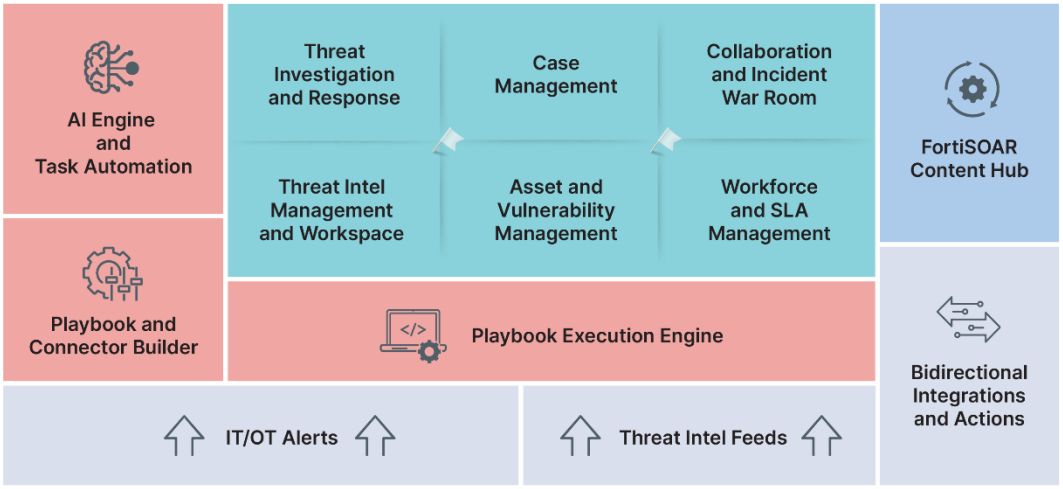
- Reduced Risk: Automated response actions and streamlined workflows minimize the impact of security breaches.

- Increased Productivity: Security analysts can focus on high-value tasks, leading to improved productivity and job satisfaction.

9.4.17.2 Highlights

- Security Incident Response: Centralized and automated alert triage, enrichment, investigation, collaboration, and response actions for IT/OT security
- Compliance Validation and Reporting Tracking, dashboards, SLAs, and reporting support IT/OT regulatory compliance management.
- Case and Workforce Management A complete solution for case management and managing and tracking task assignments, work queues, and shift calendaring.
- GenAI-powered Security Assistant Fortinet Advisor uses GenAI to guide, simplify, and automate threat investigation, response actions, and more.
- Threat Intelligence Management Automatically curates' intel from FortiGuard Labs and any public source to enrich investigations, threat hunting, and collaboration
- AI Recommendation Engine ML powers automation and decisioning, including alert grouping, threat assessment, playbook creation, and playbook suggestions
- Asset Management Centralizes asset security and risk views along with automated change management process playbooks
- Content Hub and Community An expanding library of connectors, playbooks, solutions, videos, and community contributions drive continued benefits
- Vulnerability Management Combines risk-based asset vulnerability views, task management, and automated patch and mitigation playbooks
- No/Low-code Playbooks Patented design experience provides visual drag/drop and rapid development modes to create playbooks without technical coding skills.
- OT Security Management Extended integrations and functions meet OT-specific monitoring and playbook automation requirements
- Enterprise and MSSP-Ready SaaS, on-prem, multi-tenant, dedicated and shared-tenant options support MSSP and global enterprise requirements.

9.4.17.3 Key Features



9.4.17.4 Centralize and Automate Attack Investigation and Response

Security operations center (SOC) teams are overloaded with investigating alerts and responding to threats across dozens of tools.1 Most teams struggle to keep pace, slowing their ability to discover serious attacks. Network operations center (NOC) and operational technology (OT) teams face their own monitoring and maintenance challenges, furthering security risks. Leading organizations and managed security service providers (MSSPs) use FortiSOAR to unify and optimize these critical workflows, ensuring better security while driving efficient IT/OT operations.

FortiSOAR enables organizations to centralize, standardize, and automate IT/OT security operations and critical enterprise functions. With broad integrations, rich use-case functions, hundreds of prebuilt workflows, and simple playbook creation, FortiSOAR supports best-in-class procedures tailored to your specific needs. FortiSOAR is the security operations hub that connects to everything and automates anything— helping protect your organization from attack.

9.4.17.5 Sample Use case

1. DHS Report Monitoring
2. Dynamic DNS Detection
3. Ransomware Detection and Response
4. Orangworm Attack Group Monitoring
5. SQL Injection Detection
6. ColdRoot Detection
7. Insider Threat Identification
8. Vulnerability Exploitation Monitoring
9. Suspicious Remote Access Detection
10. Suspicious PowerShell Activity
11. Suspicious Domain Generation Algorithm (DGA) Detection
12. Unauthorized Cloud Storage Access
13. Suspicious Email Attachments or Links
14. Lateral Movement Detection
15. Privileged Account Abuse Monitoring
16. Sensitive Data Exfiltration
17. Suspicious Web Shell Detection
18. Brute-Force Attack Identification
19. Unusual File Integrity Changes
20. Unauthorized Software Installation
21. Cryptocurrency Mining Detection
22. Suspicious Network Scanning Activities
23. Unusual Print Spooler Behavior
24. Unauthorized Service Account Usage
25. Suspicious Registry Modifications
26. Unusual PowerShell Script Execution
27. Suspicious Windows Management Instrumentation (WMI) Activities
28. Unauthorized Access to Sensitive Directories
29. Suspicious Scheduled Task Creation
30. Unusual Remote Desktop Protocol (RDP) Usage
31. Suspicious Windows Event Log Clearing
32. Unauthorized Microphone or Camera Access
33. Suspicious Clipboard Activity
34. Unusual Network Traffic Patterns
35. Suspicious Windows Firewall Modifications
36. Unauthorized USB Device Connections
37. Suspicious Windows Service Installations
38. Unusual Windows Registry Modifications
39. Suspicious Windows Startup Folder Changes
40. Unauthorized Access to Sensitive Files
41. Suspicious Windows Prefetch File Changes
42. Unusual Windows Event Log Entries

43. Suspicious Windows Shortcut File Modifications
44. Unauthorized Access to Shared Folders
45. Suspicious Windows Temp Folder Activities
46. Unusual Windows Service Host (svchost.exe) Behaviours
47. Suspicious Windows Task Scheduler Modifications
48. Unauthorized Access to Sensitive Registries
49. Unusual Windows System File Changes
50. Suspicious Windows User Account Modifications

9.4.17.6 Sample Playbooks ...

Enrichment Playbooks:

- User Enrichment
- Host Enrichment
- URL Enrichment
- Domain Enrichment
- File Enrichment
- IP Enrichment
- Related Log Search
- Get Host Vuln
- Get Risky User
- Get Office Compliance
- Update VIP User Watch List
- Get Alert Evidence
- Get Geo Location

Containment Playbooks:

- Block User in AD
- Isolate Host
- Restrict App Exec
- Block IP, URL, IoC
- Restrict MDE Domain
- Lock Service Principal Account
- Restrict File Hash
- Run Antivirus

Remediation Playbooks:

- Search & Destroy
- Dismiss AD Risky User
- Release MDE Machine from Isolation
- Block Brute Force Attack
- Refresh Tokens
- Update User Account from AD
- Revoke User All Active Sessions

9.4.18 Qualys VMDR® - All-in-One Vulnerability Management, Detection & Response

Discover, assess, prioritize, and patch critical vulnerabilities in real time and across your global hybrid-IT landscape— all from a single solution.

9.4.18.1 A Single app for discovery, assessment, detection, and response

The Qualys Cloud Platform, combined with its powerful, lightweight Cloud Agents, Virtual Scanners, and Network Analysis (passive scanning) capabilities, brings together all four key elements of an effective vulnerability management program into a single app unified by powerful out-of-the-box orchestration workflows. Qualys VMDR® enables organizations to automatically discover every asset in their environment, including unmanaged assets appearing on the network, inventory all hardware and software, and classify and tag critical assets. VMDR continuously assesses these assets for the latest vulnerabilities and applies the latest threat intel analysis to prioritize actively exploitable vulnerabilities. Finally, VMDR automatically detects the latest superseding patch for the vulnerable asset and easily deploys it for remediation

9.4.18.2 Built-in Orchestration

By delivering all this in a single app workflow, VMDR automates the entire process and significantly accelerates an organization's ability to respond to threats, thus preventing possible exploitation.

9.4.18.3 Key Benefits

- It's all in the cloud: No need for bulky appliances. Everything is in the cloud and ready to run.
- Easy to deploy: Deployment is incredibly simple. With unlimited virtual scanners, you can spin a scanner up and be ready to go in no time.
- Includes VM: VMDR has the same vulnerability management solution that you have come to know and trust, as well as many other great apps.
- Drastically reduce time and money: Using a single cloud platform, organizations save significant resources and the time required to otherwise install multiple agents, multiple consoles and integrations.

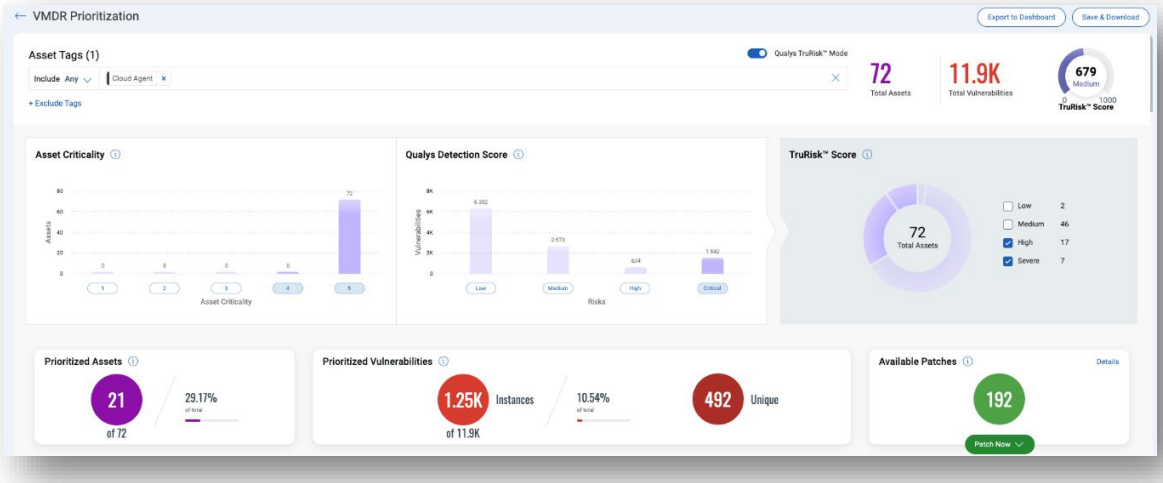


Figure 1.Asset TrueRisk Prioritization

Knowing what's active in a global hybrid-IT environment is fundamental to security. VMDR enables customers to automatically discover and categorize known and unknown assets, continuously identify unmanaged assets, and create automated workflows to manage them effectively.

After the data is collected, customers can instantly query assets and any attributes to get deep visibility into hardware, system configuration, applications, services, network information, and more.

9.4.18.4 Vulnerability Management – Real-time Vulnerability and misconfiguration detection

VMDR enables customers to automatically detect vulnerabilities and critical misconfigurations per CIS benchmarks, broken out by asset.

Misconfigurations lead to breaches and compliance failures, creating vulnerabilities on assets without common vulnerabilities and exposures (CVEs). VMDR continuously identifies critical vulnerabilities and misconfigurations on the industry's widest range of devices, operating systems and applications.

9.4.18.5 Threat Prioritization – Automated remediation prioritization

VMDR uses real-time threat intelligence and machine learning models to automatically prioritize the riskiest vulnerabilities on the most critical assets. Indicators such as Exploitable, Actively Attacked, and High Lateral Movement bubble up current vulnerabilities that are at risk while machine learning models highlight vulnerabilities most likely to become severe threats, providing multiple levels of prioritization.

9.4.18.6 Patch Management - Patching and remediation at your fingertips

After prioritizing vulnerabilities by risk, VMDR rapidly remediates targeted vulnerabilities, across any size environment, by deploying the most relevant superseding patch.

Additionally, policy-based, automated recurring jobs keep systems up to date, providing proactive patch management for security and non-security patches. This significantly reduces the vulnerabilities the operations team has to chase down as part of a remediation cycle.

9.4.18.7 Confirm and repeat

VMDR closes the loop and completes the vulnerability management lifecycle from a single pane of glass that offers real-time customizable dashboards and widgets with built-in trending. Priced on a per-asset basis and with no software to update, VMDR drastically reduces your total cost of ownership.

9.4.19 Web Application Penetration testing

Web Application Penetration Testing (WAPT) is a structured approach to identifying security vulnerabilities within web applications. It simulates real-world attacks to assess security controls, identify weaknesses,

and evaluate the impact of potential exploitation. The testing methodology aligns with industry standards such as OWASP Top 10 and NIST guidelines.

Reconnaissance / Foot printing

This phase involves gathering intelligence about the target application to identify potential attack vectors.

Passive Reconnaissance

- Search Engine Discovery: Analyze indexed pages, cached data, and search engine disclosures for sensitive information leakage.

- Metadata & Comment Analysis: Extract metadata from publicly available documents and analyze web page comments for internal references.

Active Reconnaissance

- Web Server Fingerprinting: Identify web server type, version, and configuration using tools like Nmap and WhatWeb.

- Web Application Framework Enumeration: Detect underlying technologies (e.g., PHP, .NET, Django) and third-party components.

- Application Entry Point Mapping: Identify input fields, authentication mechanisms, API endpoints, and business logic flows.

- Execution Path Mapping: Analyze user flows and backend interactions to identify critical functionalities and potential security gaps.

- Review Web Server Metafiles: Inspect files like robots.txt, .git, .env, and backup files for sensitive data exposure.

- Application Enumeration: Identify running applications, exposed endpoints, and hidden functionalities through directory brute-forcing and API analysis.

Understanding the Application

- Workflow Analysis: Evaluate user roles, authentication mechanisms, and data flows
- Input Handling: Identify input validation mechanisms, form structures, and business logic rules.

- Session Management & Authorized

9.4.20 Key Assumptions and Exclusions

- DESC will nominate Single Point of Contact (SPOC), who will be the main contact point for Du team till the completion of the project.
- Project plans will be agreed upon before commencement of the engagement or as decided mutually.
- DESC will allow 2 weeks of time between issuing the purchase order and commencement of the project.
- du will deliver all documents in English only.
- This project will be executed in a hybrid model.
- Any change in the scope mentioned above or additional effort requirement will be taken up through Change management and du will provide effort and fee for the additional scope at the time of change initiation.
- du will not implement any remediation measures. It is the responsibility of DESC to implement the recommended security controls.
    - For grey box penetration testing mode, DESC will provide two sets of test user credentials per role in the application and domain admin credentials to conduct authenticated vulnerability assessment.

9.4.21 Trend Micro Vision One - EDR

Our unified cyber security platform. Vision One provides detection and response across various layers including endpoint, cloud, email, network, identity, and OT. The platform also extends to provide attack surface risk management and zero trust secure access capabilities

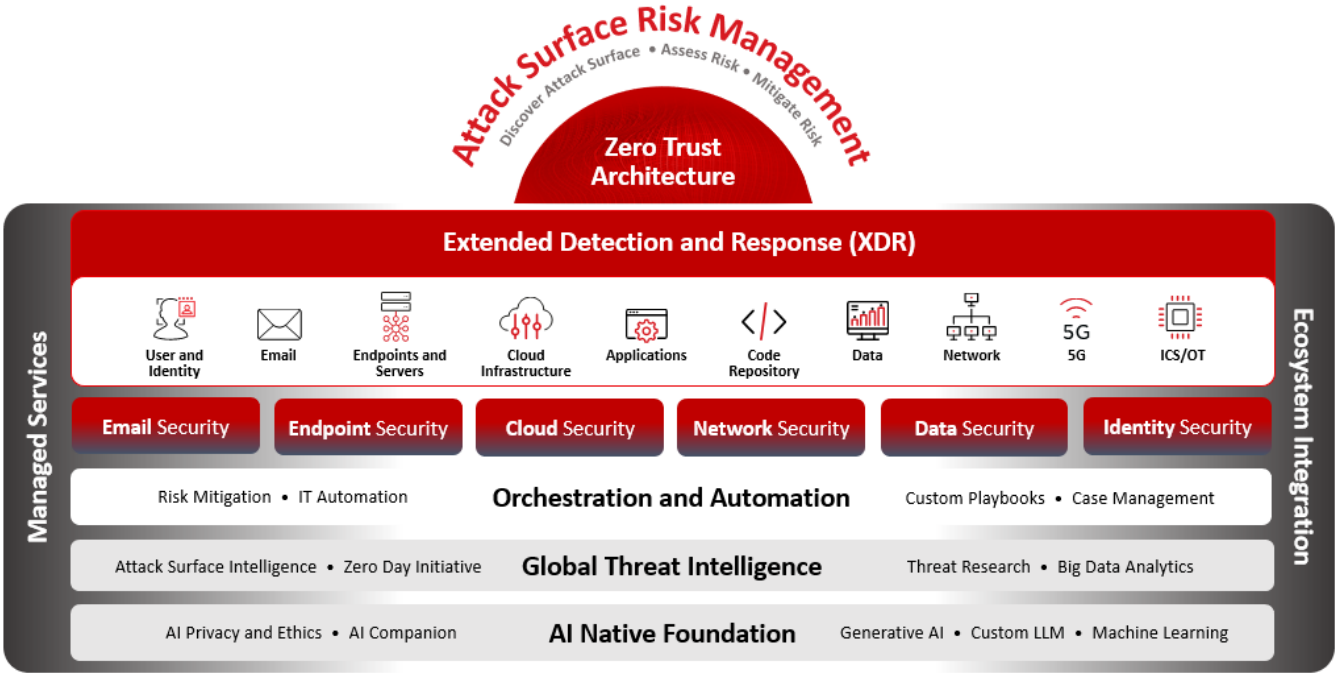
We're the first and only vendor to offer a complete attack lifecycle solution:

- Detect: Advanced detection monitors a client's specific environment for malicious content, communication, and behavior.
- Analyze: Deep threat analysis, including sandboxing and global threat intelligence, helps the client assess the attack, its characteristics and its impact.
- Adapt: Custom Protection helps clients create custom responses to these targeted attacks, such as IP blacklists, and custom spear phishing protection. The solution automatically updates the global threat intelligence network and issues these custom security updates to Trend Micro gateway, endpoint and server enforcement points. Vision One Zero Trust Secure Access provides dynamic access control to internal and external resources depending on device or user risk.
- Respond: environment-wide telemetry collection and global threat intelligence provide 360-degree contextual visibility to help the clients rapidly identify and remediate the full extent of the attack.

9.4.21.1 Trend Micro Vision One

Trend Micro Vision One is a purpose-built threat defense platform that provides added value and new benefits beyond XDR solutions, allowing you to see more and respond faster. Providing deep and broad extended detection and response (XDR) capabilities that collect and automatically correlate data across multiple security layers—email, endpoints, servers, cloud workloads, and networks—Trend Micro Vision One prevents the majority of attacks with automated protection.

Native sensors and protection points—coupled with the XDR capabilities that stitch together threat activity across layers—allow for the quick detection of complex attacks that bypass prevention. This provides an unmatched understanding of the activity data in your environment and a balanced approach to security, as teams can quickly see the story of an attack and respond faster and more confidently. The visibility and efficiency that is provided by Trend Micro Vision One makes great security teams even better, enabling them to do more with less. In addition, the Trend Micro™ Managed XDR service can augment teams with expert threat hunting and investigation.



9.4.21.2 Key Business Issues

- Stealthy threats continue to evade even the best defenses
- Disconnected security layers with siloed tools and data sets make it difficult to correlate information and detect critical threats
- Too many alerts and overloaded organizations don't have the time or resources to investigate
- Consolidated visibility into an organization's current security status, trending over time, is hard to come by and limits the ability to know what to focus on and where action should be taken

9.4.21.3 Key Advantages

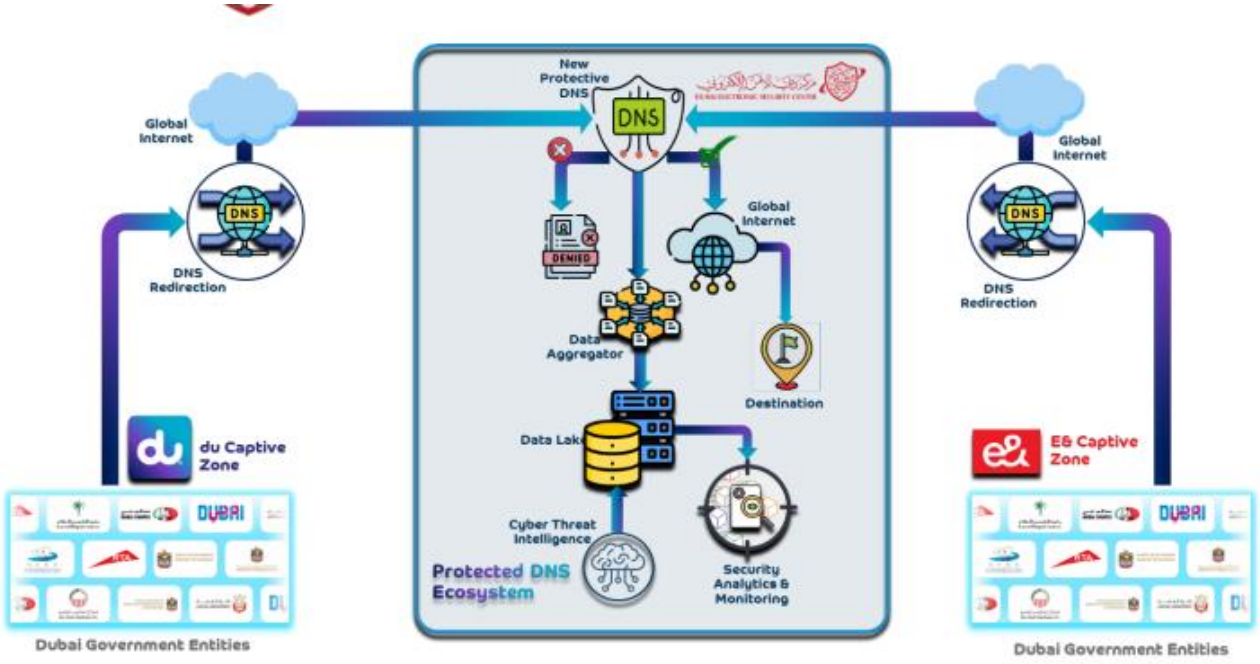
- Comprehensive protection - Trend Micro detection and prevention (including web reputation, application control, and IPS) automatically stops more attacks before they take hold.
- Deeper data - Integrated, native sensors deliver deep activity data, not just detections, across email, endpoints, servers, cloud workloads, and networks.
- Faster, earlier detection – XDR automatically ties together a series of lower-confidence activities into a higher-confidence event, surfacing fewer, prioritized alerts for action and graphically presents the story of the attack.
- More context, less noise - Incorporating Trend Micro threat intel insights together with MITRE ATT&CK mapping enriches detection and investigation to provide a deeper understanding.
- Greater risk visibility - Includes role-based views of multiple risk metrics and trends that are most meaningful to your team. An intuitive dashboard provides centralized visibility and a holistic view into what is happening in your environment, including a summary of key detections, endpoints with observable attack techniques, prioritized lists of risky devices and users, along with visibility into both approved and unapproved cloud app usage and the associated risks for that.

9.5 Phase 3: Protective DNS Stack Implementation

Phase 3 Deploy a high-availability Protective DNS (PDNS) stack using selected OEM technology across Primary and DR datacenters in Dubai, ensuring minimal downtime and robust DNS security, while optimizing the platform with AI driven automation. Once ready, the PDNS platform will receive the DNS traffic of the government departments and entities redirected by both the service providers (du & Etisalat) by overwriting the DNS IP with the IP of the new PDNS stack to be built.

DU is proposing Infoblox as the Protective DNS Stack.

Phase 1: High Level Architecture of Traffic Flow



9.5.1 Infoblox Proposed Solution

- On-prem Infoblox Grid and Grid Management
- On-prem Recursive and Caching DNS with Security enforcement
- Infoblox Threat Defense
- DNS Infrastructure Protection / Advanced DNS Protection
- Reporting and Analytics

- Infoblox Grid Empowers physical, virtual, or cloud-based DNS/DHCP/ IPAM (DDI) appliances embedded with IPAM, database and discovery of VMWare and OpenStack assets for reliable,

automated, distributed, security-hardened, highly available, and easy-to-manage core network services via a single pane of glass.

- Recursive and Caching DNS By leveraging multiple DNS Cache Acceleration appliances in a distributed Infoblox Grid™ configuration, billions of queries per second can be processed. Besides raw DNS transaction capability, Infoblox DNS Cache Acceleration delivers unprecedented low levels of DNS query latency. The Infoblox Grid™ architecture enables distributed appliances to be effectively managed from a central location or several regional locations, ensuring that configurations can scale without operational limits.
- Infoblox Threat Defense strengthens and optimizes your security posture from the foundation up. It maximizes brand protection by securing your existing networks as well as digital imperatives like SD-WAN, IoT and the cloud. It uses a hybrid architecture for pervasive, inside-out protection, powers security orchestration, automation and response (SOAR) solutions by providing rich network and threat context, optimizes the performance of the entire security ecosystem and reduces your total cost of enterprise threat defense.
- Advanced DNS Protection blocks the widest range of attacks, such as volumetric attacks, NXDOMAIN, exploits and DNS hijacking. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, ADP intelligently detects and mitigates DNS attacks while responding only to legitimate queries by using constantly updated threat intelligence, without the need to deploy security patches.
- Reporting and Analytics deliver full plug-and-play visibility through 100+ pre-built, customizable dashboards and reports, search, predictive analytics and Splunk- powered visualizations for endpoint, performance, security forensics, access logging, audit, and control.

9.5.2 Design Goal and Objectives

DESC is looking for building a Protective DNS (PDNS) for all of Dubai government entities with the goal of achieving 2 things:

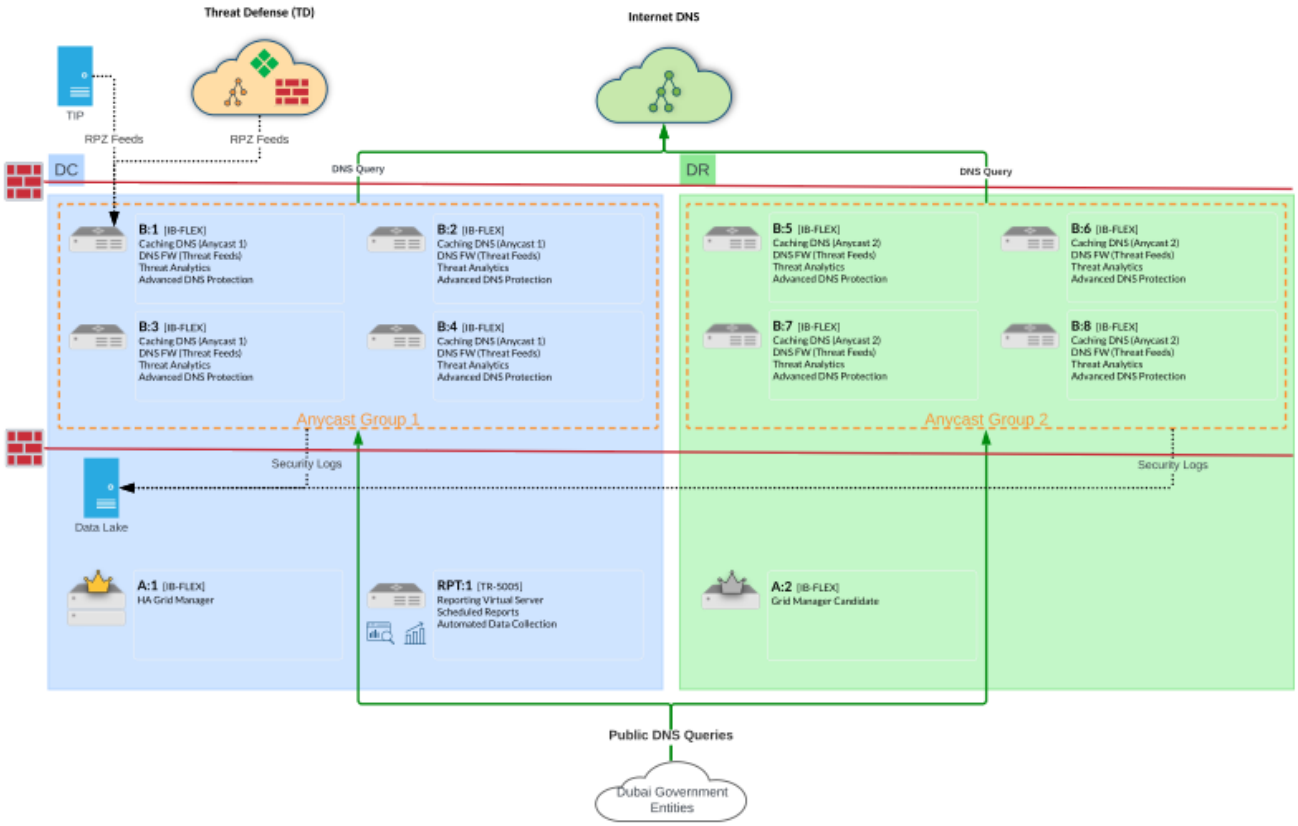
1. Providing protection for DNS traffic.
2. forwarding the logs of all DNS Security logs/violations to the data lake

The designed solution is desired to receive DNS traffic, either directly from the entities, or through redirecting the entities DNS traffic from Service Providers (DU & Etisalat) to the protective DNS infrastructure for security and visibility.

The proposed solution by Infoblox will be deployed in 2 datacenters (DC and DR) with centralized management in DC, and backup management in DR with the following characteristics:

- Each datacenter will have 4 DNS servers to support the estimated load of queries being generated by 50K users, which is estimated to be 50K Queries per Second (QPS)
- The load will be balanced equally among these 4 servers in each site to achieve up to 100K QPS using a load balancer, Anycast with ECMP, or any similar technology provided by the customer
- Full DNS Security will be provided to cover reputation-based, behavioral-based, and signature-based techniques to secure the DNS traffic.
- Security logs will be forwarded to datalake for storage, correlation and analytics
- Infoblox Reporter server will be collecting only system logs (CPU, Memory, QPS, etc)

9.5.3 High Level Solution Diagram



9.5.4 Design Assumptions:

- The solution is designed to provide recursive DNS and DNS Security for 50K QPS
- Traffic will be balanced between the 4 servers of each group equally / using a load balancer, Anycast with ECMP, or any other suitable technology
- The design is built to support up to 100K QPS in the worst-case scenario per site if the load is balanced correctly among the servers of the site.
- Infoblox Grid will receive the DNS traffic from the government entities directly via GIN network.
- Reporting Server will be used for system logs only (CPU, Memory, QPS, etc)
- Security logs will be forwarded to the data lake using DNSTAP

9.5.5 Infoblox References

- Etisalat
- DU
- DEWA
- Dubai Municipality
- RTA
- Dubai Police
- Federal TAX Authority
- Dubai Health
- Central Bank of UAE
- Ministry of Interior
- Ministry of Foreign Affairs
- DP World
- DIEZ
- DGE - Abu Dhabi Digital Authority Previously
- Sharjah Digital Department
- Dubai Airports
- ADJD
- ICP
- Emirates
- Flydubai
- Ministry of Education
- TDRA
- Fednet
- ADIB
- ADCB
- Ministry of Justice
- The Executive Council
- ADIA
- MOPA
- ADNOC
- ENOC

9.6 Phase 4: Building AI Automation Stack - (ROADMAP)

Note: The below scope is an Indicative High-Level scope and does not represent a binding services scope of Work and no commercials will be provided.

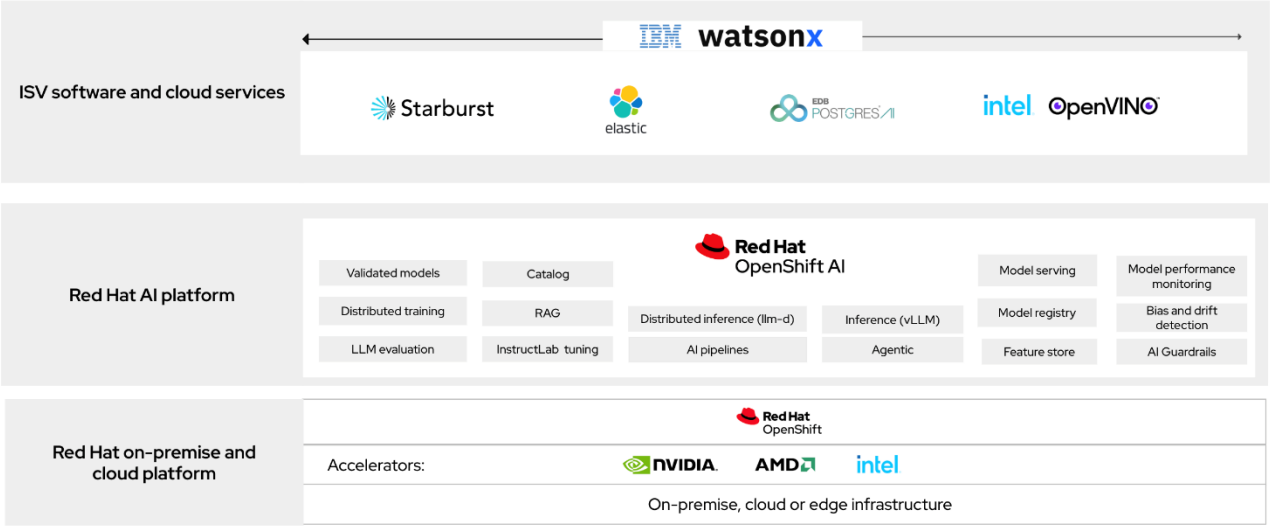
This phase is a proposed vision to develop an AI-driven solution that operates on top of the existing security data lake to enhance and streamline cybersecurity operations. The concept is designed around the current hardware and infrastructure assumptions, providing a realistic view of what could be achieved with today's capabilities. However, as AI technologies and platforms continue to evolve rapidly, the design, components, and overall architecture will likely need to be revisited and updated over time to remain aligned with new advancements and best practices.

At this stage, the roadmap focuses on high-level direction rather than delivery. No implementation or professional services are included, as the specific use cases and operational requirements must first be studied to accurately define the project scope, timeline, and resource needs.

9.6.1 OpenShift AI

Red Hat OpenShift AI is a flexible, scalable MLOps platform built with open source technologies, providing trusted and operationally consistent capabilities for teams to experiment, serve models, and deliver innovative applications. OpenShift AI accelerates the delivery of AI-enabled applications, helping organizations move from early pilots into operationally robust deployments with greater speed and control.

The platform offers an integrated user interface (UI) experience with tooling for building, training, tuning, deploying, and monitoring predictive and gen AI models. You can deploy models to hybrid cloud environments, with a specific emphasis on providing a controlled and protected footprint for sovereign and private AI. This approach makes certain that sensitive data and AI models remain within designated geographic or organizational boundaries, meeting strict regulatory and compliance requirements.



Several other core tools and capabilities provided with Red Hat OpenShift AI offer a solid foundation:

Model building and customization. Data scientists can conduct exploratory data science in a JupyterLab UI, offering out-of-the-box securely built notebook images with common Python libraries. For gen AI projects, OpenShift AI enables Retrieval Augmented Generation (RAG) and distributed InstructLab training, providing model alignment tooling to contribute skills and knowledge to genAI models more efficiently.

Model serving. Red Hat OpenShift AI provides a variety of frameworks using KServe as the core engine for model serving to simplify the deployment of predictive machine learning or foundation models to production environments. For LLMs requiring maximum scalability, OpenShift AI offers parallelized serving

with vLLM runtimes. Llm-d offers a framework for optimizing LLM inference by disaggregating the pipeline into modular services, that supports smart autoscaling and efficient request routing.

AI pipelines. Red Hat OpenShift AI offers a pipelines component that lets you orchestrate AI tasks into pipelines and build pipelines using a graphical front end. Organizations can chain together processes like data preparation, build models, and serve models.

Model monitoring. Red Hat OpenShift AI helps Ops-oriented users monitor operations and performance metrics for model servers and deployed models. Users can access out-of-the-box visualizations for performance and operations metrics or integrate data with other observability services.

Distributed workloads. Distributed workloads allow teams to accelerate data processing along with model training, tuning, and serving. This capability supports prioritization and distribution of job execution along with optimal node use. Advanced GPU support helps handle the workload demands of foundation models.

AI guardrails, bias and drift detection. Red Hat OpenShift AI provides tools to help data scientists and AI engineers monitor whether models are fair and unbiased based on the training data but also for fairness during real-world deployments. AI guardrails provide a customizable framework implementing crucial safety controls, helping ensure that models are transparent, fair, and reliable for use in production. Drift detection tools include input data distributions for deployed ML models to detect when the live data used for model inference significantly deviates from the data upon which he model was trained.

Catalog and registry. Red Hat OpenShift AI provides an internal model catalog and a curated catalog where Platform Engineers can discover, compare, and evaluate optimized gen AI models. It also provides a central registry helping data scientists and AI engineers share, modify, deploy, and track predictive and gen AI models, metadata and model artifacts.

Feature store. Manage clean, well-defined data features for ML models, enhancing performance and accelerating workflows.

9.6.2 OpenShift AI working with NVIDIA to accelerate deployment of AI solutions

As AI/ML applications become increasingly critical to business success, organizations require platforms that can handle complex workloads, optimize hardware use, and provide scalability. Scalable data processing, data analytics, ML training, and inferencing all represent highly resource intensive computational tasks. NVIDIA software makes it possible to accelerate all aspects of end-to-end data science by taking advantage of the parallel processing capabilities of GPUs.

NVIDIA NIM enhances the management and performance of NVIDIA GPUs within the Red Hat OpenShift environment, allowing AI applications to use the full potential of NVIDIA's AI software and hardware. The integration of NVIDIA NIM and Red Hat OpenShift AI allows for better resource allocation, greater efficiency, and more productive AI workload execution.

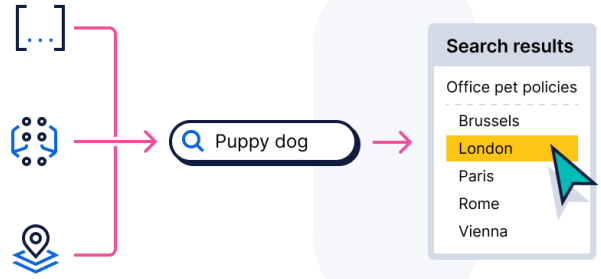
9.6.3 Elasticsearch Vector Database for Generative AI and RAG apps

Elasticsearch Relevance Engine (ESRE) is a comprehensive suite of developer tools for building generative AI and RAG applications. ESRE incorporates a vector database that stores embeddings for text, image, and video data. ESRE's native hybrid search can effectively combine results containing text, vectors, and geospatial data, with filtering, aggregations, and document-level security.

With ESRE, developers can implement vector search and semantic search, including k-nearest neighbor (kNN) and approximate nearest neighbor (ANN) search, along with support for both built-in and third-party natural language processing (NLP) models. ESRE also seamlessly integrates with key third-party ecosystem products from providers such as Cohere, LangChain, and LlamaIndex. Elasticsearch can be self-managed or deployed with Elastic Cloud.

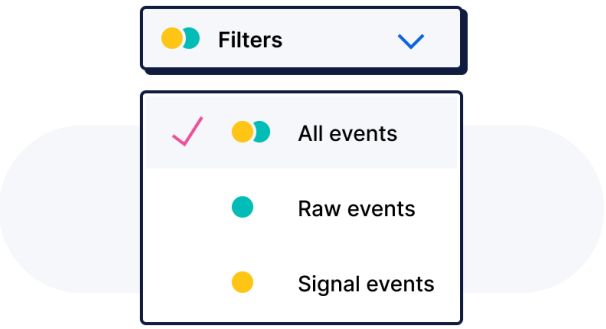
Vector search in Elasticsearch uses vector embeddings to power modern, AI-driven search experiences. With vectorized content, Elasticsearch retrieves results based on meaning and similarity, not just keywords or exact term matches.

9.6.3.1 Hybrid search that understands everything



Elasticsearch's hybrid search blends keywords, vectors, geo data, metadata, and more in a single API call. Rank results by meaning, precision, and context.

9.6.3.2 Facets and filters, without the lag

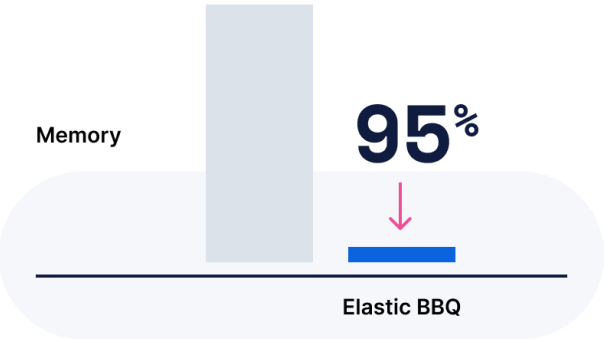


Filters and facets that run fast, even at scale — no slowdowns, no full index scans. Elastic blends aNN retrieval with filters to create the right scope, no matter the scale.

9.6.3.3 OpenAI, Anthropic, Hugging Face ... all native

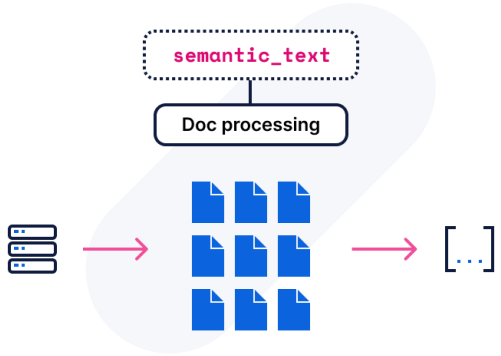
Inference APIs execute native inference with popular LLMs or built-in models for text embeddings, classification, Q&A, and more with no external ML infrastructure needed.

9.6.3.4 More vectors. Less memory. No trade-offs.



Better Binary Quantization (BBQ) reduces memory footprint up by to 95% while delivering great accuracy. Optimized distance calculations and aNN recall accelerate vector search at scale.

9.6.3.5 Semantic search, fewer steps



The semantic_text field handles mappings, embeddings, and chunking automatically — delivering truly seamless dense retrieval in a single query.

9.6.3.6 Test RAG fast — no setup needed

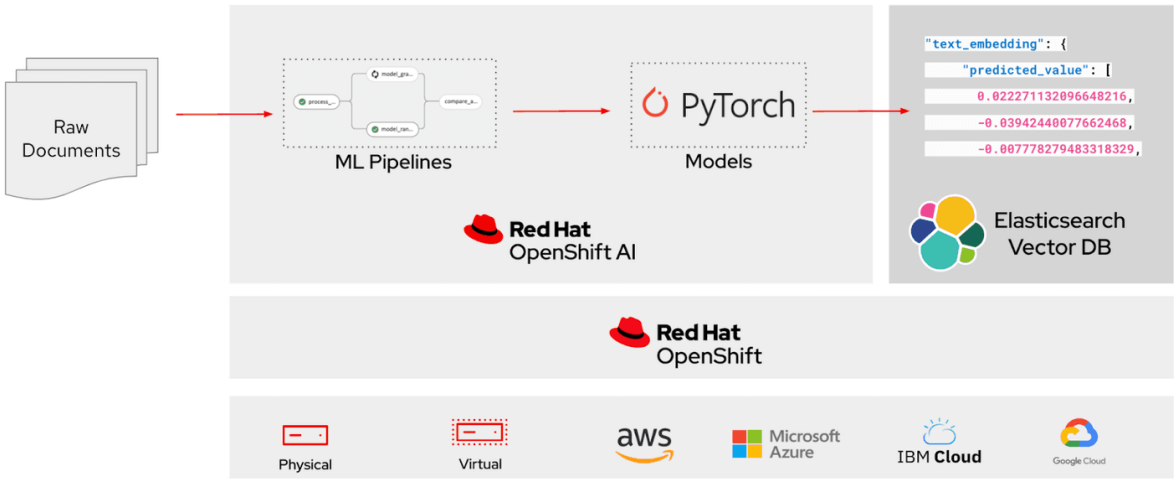
Stop the guess work. AI Playground lets you test hybrid retrieval, relevance ranking, and chunking strategies in real time, so you can fine-tune and ship tested queries with confidence.

9.6.3.7 OpenShift AI with Elasticsearch Vector DB

Elastic integrates with embedding models from the ecosystem including Red Hat OpenShift AI, Hugging Face, Cohere, OpenAI, and others via a single straightforward API call. This approach ensures clean code for managing hybrid inference for RAG workloads, with features that include:

- Chunking, connectors, and web crawlers for ingesting diverse datasets into your search layer.
- Semantic search with Elastic Learned Sparse EncodeR (ELSER), the built-in ML model, and the E5 embedding model, enabling multilingual vector search.

- Document and field-level security, implementing permissions and entitlements that map to your organization's role-based access control (RBAC).



9.6.3.8 Hardware Sizing

Node's Role	Node Type	Number of Nodes	Cores Per Node	RAM Per Node (GB)	OS Disk Per Node (GB)	Disk Per Node (TB)	GPU
OpenShift Master Nodes							
Production	BM	3	24	256	2 x 512		
OpenShift Infra Nodes							
Production	BM	3	32	512	2 x 512	6 Disks x 7.68TB	
OpenShift Worker Nodes							
Production - GPU	BM	3	128	1024	2 x 512		8 GPU

Estimated usable storage capacity is 40 to 50 TB based on compression and ODF configuration.

10. Engagement Model: Implementation and Managed Service Transition

This section details the collaborative framework for the project, outlining the roles and responsibilities of **duTech** and our selected implementation partner, **GBM,** through the project lifecycle.

10.1 Phase 1: Implementation and Deployment

The core implementation of this solution will be executed through a strategic partnership model:

- **Implementation Partner Selection:** du has selected GBM as the specialized Implementation Partner for this high-profile project.
- **GBM's Role**: The GBM team will support du team for the execution and delivery of the technical implementation scope as defined in the Statement of Work (SOW).
- **du Governance and Supervision**: Implementation activities will proceed under the strict governance and supervision of du's internal teams.
    - **du Enterprise Architects** will ensure the design and implementation adhere to du's overarching architectural principles, standards, and strategic roadmap.
    - **du Engineers** will provide technical oversight, validation, and acceptance sign-off at key project milestones. This ensures alignment with existing infrastructure and operational requirements.

10.2 Phase 2: Handover to Operations

Upon successful completion and acceptance of the implementation, a structured transition will take place to ensure seamless operational continuity:

- **Formal Handover:** The implementation team will execute a formal, documented handover process.
- **Knowledge Transfer:** Comprehensive training, documentation, and knowledge transfer sessions will be conducted by du for the Operations team.
- **Managed Service Scope**: Following the successful handover, the solution will transition to the defined Managed Service scope. The Operations team will assume responsibility for the ongoing management, maintenance, and support of the newly deployed environment.

11. Scope of Work

11.1 Project Initiation and Design

- Devices ordering
- Project Kick-off
- Design Workshops with DESC

- High Level Design Document Submission
- Low Level Design Document Submission
- Site Readiness Document Submission

11.2 Phase 0: Network And Security Infrastructure Deployment

11.2.1 Dell with Nutanix - Datacenter Infrastructure

11.2.1.1 Dell Storage XC Series Project Scope

During this part of the service, DT Services:

- Reviews and obtains the site technical requirements with the customer.
- Verifies, defines and documents environment minimum requirements and the configuration details for the solution.
- Defines the new Dell switch configurations.
- Performs physical hardware installation, including unpacking, racking, labeling, cabling, powering up, and configuring iDRAC IP address.
- Validates that the Customer's top-of-rack switch configuration meets the requirements.
- Initializes the cluster and assigns all IP addresses.
- Installs supported hypervisor, as necessary.
- Confirms Nutanix software is at the latest version, and updates as necessary.
- Creates a single storage container and Datastore.
- For vSphere XC clusters, install vCenter if required.
- Register cluster nodes in vCenter.
- For Hyper-V XC clusters, register cluster nodes with an existing SCVMM server, as necessary.
- Adds a node to an existing Nutanix cluster.
- Confirms component drivers and firmware are at latest supported version, and updates as necessary.
- Adds the Solution to Secure Connect Gateway.
- Enables CloudIQ.

- Conducts a basic Knowledge Transfer.
- Performs deployment verification.

Move used packaging materials to trash and recycling facility or other designated area within the immediate location.** Includes configuration of up to 10 filesystems and NIC teaming or bonding (up to 2).

*** Performs the installation of either the OMES Plug-In, Secure Connect Gateway and discovers newly deployed supported enterprise devices.

1 Sleds for C-Series or XR Series require a deploy service on each sled purchased. Installation of enclosure is included at no additional charge.

2 Applies to MX Series Servers only.

11.2.1.2 Dell Unity XT Project Scope

ProDeploy Plus for Dell EMC Unity X80

This service includes the following components (not to exceed the listed values):

Scope Quantities	ProDeploy Plus for Dell EMC Unity X80
Number of Dell EMC Unity Arrays	1
Number of Hosts	4
Number of Zones	16
Number of NFS/SMB Shares	5
Number of CIFS/SMB Shares	5
Number of Multiprotocol Shares	5

During this part of the service, DT Services:

- Plans and estimates a schedule for the installation and/or configuration tasks for the Services.
- Gathers Customer environment information to complete the Configuration Worksheet with details required for planning Dell EMC Unity system installation.
- Obtains and reviews Customer requirements and performs deployment planning.

- Conducts meeting to review deployment plan and validates that site and equipment are ready for installation.
- Performs planning and design for Dell EMC Unity installation and deployment.
- Documents the proposed architecture in the Deployment Plan.
- Performs pre-installation validation comparing the equipment against Configuration Worksheet including licenses, software on a service laptop or management station, and tools required for installation.
- Unpacks, racks, and installs a Disk Processor Enclosure and the backend IO module into a single Dell EMC Unity system.
- Installs the Dell EMC Unity system including racking, cabling the components, attaching to the Customer's power and IP network, powering up, and validating that the system is online
- Verifies the installation and configuration results by running a system health report.
- Configures Service Processor management interface, registers the system, installs licenses, upgrades software if required, adds DNS and NTP information, adds support credentials, and configures SupportAssist and enables CloudIQ for Storage Appliance.
- Conducts a deployment review meeting.
- Validates that the equipment is on site at the appropriate location with power and cable requirements met.
- Moves used packaging materials to trash and recycling facility or other designated area within the immediate installation location.
- Obtains Dell EMC Unity Installation Worksheet and Dell EMC Unity Configuration Report (report produced from Unisphere documenting the Dell EMC Unity configuration details) from Dell EMC personnel or the Customer and reviews it for accuracy.
- Identifies additional requirements like licenses and beneficial updates like software upgrades and communicates them to the Customer.

- Reviews deployment details with the Customer and validates that Dell EMC Unity is ready, required licenses are installed, connectivity from storage to hosts, and SupportAssist are setup.
- Documents FAST Cache and FAST VP settings.
- Reviews FAST Cache, FAST VP, or both deployment details with the Customer and validates that all requirements are met.
- Implements the Dell EMC Unity FAST VP, FAST Cache, or both, meeting Customer requirements and Dell EMC Best Practices.
- Confirms sufficient amount of flash disks are available to meet Customer's FAST Cache requirements.
- Configures storage for provisioning.
- Configures SAN zoning for host deployment.
- Reviews Host deployment details with the Customer and validates that all requirements are met.
- Implements Customer-supplied FC or iSCSI hosts with installed operating systems and supported multipath software.
- Validates sufficient amount of capacity availability to provision storage to hosts.
- Validates connectivity from storage to hosts.
- Validates hosts' access to the provisioned storage volumes.
- Reviews file deployment details with the Customer and validates that all requirements are met.
- Validates sufficient amount of capacity availability to configure file storage.
- Validates clients' access to the added shares and exports (NFS and SMB).
- Configures pools, file systems, NAS servers, shares or exports (NFS and SMB), users, quotas, and alerts.
- Configures Dell SupportAssist.
- Performs the tests in the Deployment Verification.
- Provides the Customer with the Deployment Plan and Deployment Verification documents updated with deployment results.

- Conducts a basic Knowledge Transfer.
- Coordinates project closeout.
- Registers the Customer to receive product alerts.
- * Limited to new module configuration on array

ProDeploy Plus for Dell EMC Unity Expansion Enclosure

- The ProDeploy for Dell EMC Unity Expansion Enclosure Upgrades service delivers the installation of EMC Unity hardware. The service includes the hardware installation and the deployment and configuration of the Dell EMC Unity storage system, up to 4 hosts and 16 zones.
- The DAE could be a 15 or 25-slot Disk Array Enclosure.
- This service includes the following components (not to exceed the listed values):

Scope Quantities	ProDeploy Plus for Dell EMC Unity Expansion Enclosure
Number of Dell EMC Unity Arrays	1
Number of Disk Array Enclosures	1
Number of Hosts	4
Number of Zones	16

- During this part of the service, DT Services:
- Plans and estimates a schedule for the installation and/or configuration tasks for the Services.
- Obtains and reviews Customer requirements and performs deployment planning.
- Conducts meeting to review deployment plan and validates that site and equipment are ready for installation.
- Performs planning and design for Dell EMC Unity installation and deployment.
- Documents the proposed architecture in the Deployment Plan.
- Performs pre-installation validation comparing the equipment against Configuration Worksheet including licenses, software on a service laptop or management station, and tools required for installation.
- Unpacks Unity Disk Array Enclosure and Verifies Components
- Installs enclosure onto the rails
- Verifies the status of the Unity Disk Array Enclosure
- Moves used packaging materials to trash and recycling facility or other designated area within the immediate installation location.

11.2.1.3 ObjectScale Project Scope

This service includes the following components (not to exceed the listed values):

Scope Quantities	ProDeploy Plus ObjectScale and ECS Appliance Expansion
Number of VDCs	1
Number of ObjectScale/ECS nodes to be installed	1

During this part of the service, DT Services:

- Designs and plans the ObjectScale/ECS implementation or upgrade.
- Reviews the data collected and plans the implementation.
- Finalizes the design by reviewing the proposed design.
- Conducts a deployment review meeting.
- Validates that the equipment is on site at the appropriate location with power and cable requirements met.
- Validates ObjectScale/ECS rack installation and connects to the network.
- Validates the ObjectScale/ECS appliance hardware and prepares for OS installation.
- Validates external authentication system requirements.
- Installs new expansion hardware in the rack.
- Installs and configures ObjectScale/ECS fabric software on new nodes.
- Installs cross connect switches for all flash nodes, if applicable.
- Verifies the results of installation, configuration, or both as detailed in the Deployment Verification with the Customer.
- Moves used packaging materials to trash and recycling facility or other designated area within the immediate location.

11.2.1.4 PowerScale Project Scope

This service includes the following components (not to exceed the listed values):

	ProDeploy Plus PowerScale Node
Scope Quantities	All PowerScale Products
Number of PowerScale back-end switches to install.	1
Number of PowerScale nodes to install.	1
Number of subnets to configure.	5
Number of SmartConnect zones to configure.	5
Number of authentication methods to configure (Active Directory, LDAP, or other).	5
Number of CIFS shares, NFS exports, or a combination thereof to configure.	5

During this part of the service, DT Services:

- Completes solution deployment validation.
- Performs planning and design for the product solution being deployed.
- Conducts a deployment review meeting.
- Validates that the equipment is on site at the appropriate location with power and cable requirements met.
- Installs the back-end network switches.
- Plugs in the power and network cabling.
- Installs the PowerScale hardware.
- Creates a new PowerScale cluster.
- Sets the global data protection level.
- Implements the PowerScale cluster subnets.
- Implements SmartConnect zones.
- Implements the PowerScale authentication.
- Enables email alerts and SNMP as needed.

- Implements file system shares or exports.
- Performs the required tests using the Deployment Verification document.
- Conducts remote connectivity discussion with Customer based on PM KickOff. Prepares and installs a remote connectivity solution as needed e.g. SCG5.
- Enables remote connectivity on new arrays, validates remote connectivity, registers the remote connectivity in Dell SDR Install Base.
- Conducts a basic knowledge Transfer

1 ProDeploy Plus Add-on for PowerScale Enterprise Feature Bundle

This service deploys the features included in the PowerScale Enterprise Bundle on a configured PowerScale cluster. Deployment of one instance of DataIQ or InsightIQ monitoring and analysis software is also included.

This service includes the following components (not to exceed the listed values):

	ProDeploy Plus Add-on for PowerScale Enterprise Feature Bundle
Scope Quantities	All PowerScale Products
Number of SmartDedupe to configure.	5
Number of SmartQuotas policies to configure	25
Number of SnapshotIQ schedules to configure	25

During this part of the service, DT Services:

- Performs planning and design for the product solution being deployed.
- Conducts a deployment review meeting.
- Configures NDMP (cluster side only).
- Implements SmartDedupe.
- Implements SmartQuotas policies.
- Implements SnapshotIQ policies.
- Installs and configures DataIQ or InsightIQ for a single cluster.

- Performs the required tests using the Deployment Verification document.
- Completes solution deployment validation.
- Conducts a basic Knowledge Transfer

11.2.1.5 Commvault Services

- Onsite Delivery Services

Commvault will under the Project, as more fully described herein, design for, and implement the Commvault solution, by performing the following tasks:

- Design
- Install and configure - Commvault infrastructure
- Implement & configure – Commvault Backup Agents
- Testing

11.2.1.6 Commvault Project Scope

Commvault will deliver the Services and Deliverables in the following work packages:

Project Work Packages	
Work Package 1 Design Phase	CommCell Solution Low Level Design (1 Site) ○ Onsite Technical Workshop discovery 1x day for validation of functional/technical requirements relating to the Commvault solution ○ Delivery of a Technical "Implementation Ready" Design for the Commvault infrastructures. ○ Delivery of a Test plan with the Design Document* *Test plan must be drafted and agreed in this phase to be included in Design document
Work Package 2 Core Build Knowledge Transfer	Infrastructure Core Build ○ Install & configure 1x Commserve ○ Install & configure media agents ○ Knowledge Transfer during project delivery (member of customer staff to shadow installation)

Work Package 3 Agent Deployment Knowledge Transfer	Application Agent Deployment ○ Install and configure backups for the Source data (Elastic or Fortisiem) ○ Configuration of Storage Policies, Schedule Policies and Reports & Alerts ○ Knowledge Transfer during project delivery (member of customer staff to shadow installation) *CVPS initiates the copy, customer monitors to completion
Work Package -Testing	Restore Testing & As Built Document ○ Functional testing of Core components ○ Backup and Restore testing (as per agreed test plan in WP1) ○ Create the As Built Document to record the system after the work has been caried out. ○ Knowledge Transfer during the project delivery (member of customer staff to shadow installation)

11.2.1.7 Deliverables

Phase	Activities	Deliverable	Acceptance Criteria
WP1	CommCell Solution Design	• Commvault Low Level Solution Design Document	• Commvault will facilitate 2 iterations during the review phase. • Design reviewed, approved, and signed off by Customer.
WP2	Core Installation & configuration – per design. Knowledge Transfer	• Installation and configuration of the Commvault core environments • Customer staff member (s) to join Commvault staff during project delivery for Knowledge Transfer	• Completion the Core Environment build with the Commserves, Media Agents, up and running. • Customer staff member(s) present during project delivery.
WP3	Application Agent Deployment Knowledge Transfer	• Application agents deployed on the systems outlined in Work Package 3 under Project Work Packages Section • Customer staff member (s) to join Commvault staff during project delivery for Knowledge Transfer	• Application agents installed on the client servers. • Customer staff member(s) present during project delivery.
WP4	Testing	• All tests to be agreed and outlined in the design phase. • Testing of core functions • Backup & Restore tests	• Successful testing from the agreed test plan in design phase signed off by customer

11.2.1.8 PowerEdge Servers for backup Project Scope

During this part of the service, DT Services:

- Unpack and inspect hardware

- Physical Installation
- Rack, mount, and/or position the product & components
- Install solution specific chassis components
- Install Customer-provided Dell-branded PDU(s), as needed for proper power configuration
- Install and route power cables
- Install and route data cables
- Apply customer-provided labels to newly installed cables
- Power on equipment
- Confirm server boots, check for error lights and obvious issues
- Update chassis switch firmware
- Configure an IP address on CMC / iDRAC / iKVM / OSM
- Configure first time boot info
- Update drivers, firmware, and BIOS, including chassis firmware if applicable
- Run Secured Component Verification (SVC) if applicable
- Configuration of Intel Persistent Memory; Memory Mode, AppDirect Mode: creation of namespace and filesystem at the OS level
- Configuration of equipment (physical topology, firmware levels, IP address, running diagnostics)
- Enter the RAID utility and configure the local disks or chassis shared storage into one or more RAID logical unit number ("LUN") according to Dell supported Customer specifications
- Create and assign Virtual Disks to servers that contain an operating system installed by Dell
- Verify server(s) are connected to the Virtual Disks assigned to the OS installed by Dell
- Assign chassis PCIe slots as supported by product
- Configure virtual switches
- Configure Service Console IP address
- Install and configure Operating System or Hypervisor (maximum of 8 server nodes for Modular Platforms)

- ** Microsoft Windows
- ** Red Hat Linux
- Ubuntu Server
- VMware vSphere

- Install and configure system software on deployed server
- Dell Repository Manager
- *** Dell Secure Connect Gateway
- Dell OpenManage Server Administrator (OMSA)
- Dell OpenManage Enterprise (OME) single instance
- Configure OME to discover newly deployed devices, including OOB interfaces (iDRACs) on servers, and configure SNMP forwarding on those devices
- Installation of Windows Admin Center single instance and OpenManage Integration for Microsoft Windows Admin Center plug-in
- Onboard to Dell Cloud IQ
- For VMware vSphere and Microsoft Hyper-V, the following apply:
- Cluster creation
- Basic OS install to local storage using standard defaults
- Configuration of standard virtual networking: VMware Distributed Switch or Hyper-V Virtual Networking (2 switch independent native teams, 2 External Virtual Switches, 4 VM Network adapters with VLAN access)
- Creation of up to one Virtual Machine, with customer supplied media and license
- Installation and basic configuration of hypervisor manager (either vCenter Server, WAC or)
- Configuration of VMotion or Live Migration
- Enable VMware High Availability and/or Distributed Resource Scheduler
- Install OpenManage Enterprise Integration for VMware vCenter Plugin (OMEVV) (plugin install and register vcenter)

- Networking partitioning (NPAR)
- DCB - data center bridging
- Move used packaging materials to trash and recycling facility or other designated area within the immediate location

** Includes configuration of up to 10 filesystems and NIC teaming or bonding (up to 2).

*** Performs the installation of either the OMES Plug-In, Secure Connect Gateway and discovers newly deployed supported enterprise devices.

1 Sleds for C-Series or XR Series require a deploy service on each sled purchased. Installation of enclosure is included at no additional charge.

2 Applies to MX Series Servers only.

11.2.1.9 PowerVault ME5 for backup Project Scope

This service includes the following components (not to exceed the listed values):

- Storage Array: 1
- Number of Hosts: 4
- Number of San Zones: 16

DT Services:

- Obtains and reviews the site technical requirements with the Customer to ensure that DT Services has a comprehensive understanding of their needs.
- Verifies the existing environment meets the minimum hardware and software requirements for the solution.
- Documents all requirements in a detailed report, including topology, configuration files, parameters, and other relevant information.
- Completes the Pre-deployment Validation phase, which involves verifying that all equipment is functioning as expected and meets the required specifications prior to deployment.

- Requests lift assist, if applicable.
- Installs the equipment in the rack, ensuring proper routing of power and data cables within the rack, and apply
- customer labels as required. This will ensure a safe and efficient installation process.
- Powers on the hardware and verify that it is healthy. This includes checking for any errors or issues with the
- system's functionality.
- Updates drivers, firmware, and BIOS settings, if applicable.
- Enables the platform for Secure Connect Gateway Connectivity.
- Configures and provisions storage for each host.

11.2.1.10 Deliverables

11.2.1.11 Deployment Plan

11.2.1.12 Deployment Verification

- Upon completion of a Deliverable, DT Services will submit the Deliverable to customer accompanied by an acceptance form provided by DT Services. The completion and acceptance process for this engagement consists of the following:
- Customer will review each Deliverable within five (5) business days (the "Acceptance Period") to determine whether each Deliverable satisfies the acceptance criteria in all material respects.
- If Deliverable satisfies its acceptance criteria in all material respects, Customer will furnish a written acceptance confirmation to DT Services via the acceptance form prior to the end of the Acceptance Period.
- For a Deliverable that is not accepted due to a non-conformity or defect, Customer will indicate the detailed reasons for such rejection on the acceptance form and return the acceptance form together with the associated rejected Deliverable to DT Services (a "Rejection Notice") within the Acceptance Period.

- Upon receipt of a Rejection Notice DT Services will promptly correct any defects or non-conformities to the extent required so that each Deliverable satisfies the requirements of this SOW and its acceptance criteria in all material respects.
- Thereafter, DT Services will resubmit a modified Deliverable to Customer, accompanied by the acceptance form and the process set forth above will be repeated. However, Customer will limit its review of each resubmitted Deliverable to determining whether DT Services has corrected the defects or non-conformities identified in the Rejection Notice.
- If Customer fails to provide DT Services with the above-described Rejection Notice prior to the end of the applicable Acceptance Period, then the corresponding Deliverable is deemed accepted.
- If Customer provides a Rejection Notice after the first resubmission of the Deliverable, DT Services may terminate this agreement.

11.2.1.13 Exclusions

Scope Exclusions for Dell Services

1. Activities related to the existing customer data center environment such as de/installation, re/configuration, connection, troubleshooting, etc.
2. Custom scripting, coding, performance tuning or optimization.
3. HPC/GenAI Cluster Manage, Kubernetes, AI Software.
4. Installation, configuration, or migration of any applications, web technologies, databases, virtualized networking, or other software except when explicitly described in the Project Scope above.
5. Migrations or movement of Physical to Virtual or Virtual to Virtual compute systems other than those explicitly described in the Project Scope above.
6. Connection to Direct Current power supplies. A qualified electrician must perform all connections to DC power and to safety grounds.

Scope Exclusions for Commvault Services

1. Any milestone not listed in this document
2. Configurations or implementations not included in the work packages outlined in the Project Work Packages.
3. Support ticket creation and management
4. Any architecture, consultations, and work on future projects
5. Data migration
6. Complete system re-architecture, design and/build of new services not included in this document.
7. Custom development or personalisation
8. Customer environment dependencies

11.2.2 Cisco with Nutanix - Datacenter Infrastructure

11.2.2.1 Infrastructure Design

Stage: Design

The Infrastructure Design engagement provides a comprehensive assessment of your current or planned environment to ensure readiness for deploying Nutanix Cloud Infrastructure (NCI) or NC2 clusters.

Designed as a strategic step in your hybrid cloud journey, especially during the planning and design phases, this engagement focuses on:

- Capturing both high-level architecture and low-level implementation design
- Validating integration prerequisites across identity, networking, and storage
- Aligning infrastructure components with Nutanix best practices for scalability, security, and performance
- Planning for operational readiness, including functional validation and security hardening

This engagement is especially valuable when designing new infrastructure or preparing for workload migration, ensuring your environment is optimized for deployment and future growth.

11.2.2.2 Related Services

- Infrastructure Deployment
- NC2 Deployment

11.2.2.3 Service Scope

The Infrastructure Design engagement begins with a series of collaborative workshops led by certified Nutanix consultants who bring deep technical expertise and real-world experience. These sessions are designed to deliver immediate value to your architecture and operations teams by:

- Capturing solution requirements, constraints, dependencies, and key decisions to inform both high-level architecture and low-level implementation design
- Designing cluster architecture, virtual networking, and storage aligned to Nutanix recommended practices and future growth needs

- Validating sizing and integration with identity services, IPAM/DNS, and operational dependencies
- Planning for functional validation testing and security hardening across the environment

Consultants work closely with customer stakeholders to uncover integration challenges, align workloads with recommended practices, and ensure readiness for deployment. The engagement also supports single-site and multisite disaster recovery (DR) topology design, including active/active, active/passive, and hub-spoke configurations.

By the end of the engagement, customer teams will have a validated infrastructure design covering both strategic high-level architecture and detailed low-level planning tailored to their operational goals and ready for deployment.

11.2.2.4 Advanced Edition

For customers looking for a more comprehensive design focused on migrating existing workloads and storage.

The Advanced Edition includes the following activities:

- Everything included in the Essential Edition
- Assess the current state of virtualization elements included in the design
- Assess datacenter infrastructure and rack design
- Plan for VM backup and data protection
- Design to support the migration of existing workloads and storage into the new environment
    - Review the existing environment at a high level to support sizing
    - Develop high-level migration methodology
- Design role-based access control (RBAC) and Nutanix categories/tagging
- Design security and required cloud access controls

11.2.2.5 Site Design Topology

Each edition supports a single site or multisite disaster recovery (DR) topology design.

Essential and Advanced Edition

- Single Site – Single site design in a single physical site, public cloud region, or resource location
- Multisite DR – DR active/active, active/passive, or hub-spoke design configuration
    - Including Flow Virtual Networking VPC configurations spanning multiple locations (Advanced Edition only)
    - Gather recovery point objective (RPO) and recovery point objective (RTO) requirements for workloads, including DR and replication considerations

11.2.2.6 Limitations

- Limited to general virtualization. Workload-specific designs are available that include the NCI Design, including:
    - Database Design Workshop
    - EUC Broker Design Workshop
    - AI/ML Design Workshop
- Excludes detailed migration planning. Detailed planning, including migration wave planning, is available as part of the Virtual Machine Migration Workshop.
- Excludes design for Cisco Intersight and Cisco UCS Fabric Interconnects

11.2.2.7 Advanced Editions

Single Site Design Topology

- For each quantity purchased, design is limited to a single production environment at one physical site, public cloud region, availability zone, or resource location for a single supported hypervisor

Multisite DR Design Topology

- For each quantity purchased, design is limited to a single production environment spanning multiple physical sites, public cloud regions, availability zones, or resource locations
- Design is limited to 2 distinct site patterns, though multiple instances of each pattern can be deployed (common for hub-spoke or branch office architectures)

11.2.2.8 Supported Hypervisors

- Nutanix AHV
- VMware ESXi

Note: Support for Microsoft Hyper-V requires a custom SOW.

11.2.2.9 Delivered Artifacts

Documentation Option	Delivered Artifact	Description
Workshop Documentation	Configuration Workbook	Captures all necessary settings gathered during design workshops to support solution deployment.
	Deployment Readiness Checklist (NC2 Design Only)	Captures deployment readiness based on customer-owned prerequisites. Ensures all technical, operational, and logistical elements—such as environment setup, access, configurations, and stakeholder alignment—are in place before deployment begins. This checklist helps avoid delays and supports a smooth, successful deployment experience.
Standard Documentation	Configuration Workbook	Captures all necessary settings gathered during design workshops to support solution deployment.
	Design Documentation	Captures the customer's architecture based on workshop outcomes, encompassing both high-level and low- level design. It begins with a thorough understanding of requirements, constraints, assumptions, and risks. The document provides detailed rationale for each design decision—whether aligned to industry best practices or tailored to specific customer needs—ensuring the solution is architected to meet goals across performance, availability, scalability, and more.
	Deployment Readiness	Captures deployment readiness based on

Documentation Option	Delivered Artifact	Description
	Checklist (NC2 Design Only)	customer-owned prerequisites. Ensures all technical, operational, and logistical elements—such as environment setup, access, configurations, and stakeholder alignment—are in place before deployment begins. This checklist helps avoid delays and supports a smooth, successful deployment experience.

11.2.2.10 Infrastructure Deployment

Stage: Deploy

The Infrastructure Deployment service accelerates the deployment of on-premises NCI, NCI-Compute, or Dedicated NUS clusters. Designed as a strategic step in your hybrid multicloud journey particularly during the Deploy phase—this service focuses on:

- Deploying on-premises NCI, NCI-Compute, or Dedicated NUS clusters
- Validating and configuring infrastructure based on Nutanix recommended practices and customer-provided design documentation
- Streamlining deployment workflows to reduce complexity and accelerate time-to-value
- Delivering operational readiness through comprehensive documentation and enablement

11.2.2.11 Related Services

- Infrastructure Design Workshop
- Infrastructure Deployment for NCI-Edge
- NCI Cluster Deploy or Expansion for Cisco
- Infrastructure Expansion
- NUS Design Workshop
- NUS Deployment
- NC2 Deployment

11.2.2.12 Service Scope

Certified Nutanix consultants, equipped with deep domain expertise and hands-on experience, lead the

deployment of on-premises NCI, NCI-Compute, or Dedicated NUS clusters. Following Nutanix recommended practices, along with the customer-provided design document, consultants ensure a precise and efficient deployment.

Upon completion, the consultant delivers:

- A customized As-built Guide detailing the final deployed configuration
- An updated Configuration Workbook to support ongoing operations and future scalability

This comprehensive documentation provides your teams with a validated reference for managing and maintaining the deployed on-premises NCI environment.

11.2.2.13 On-premises NCI, NCI-Compute, or Dedicated NUS Clusters

The service includes deploying up to 4 individual on-premises NCI clusters at a single physical site according to customer-provided design and configuration documentation.

The service includes the following activities:

- Review customer-provided design and configuration documentation
- Deploy and configure NCI cluster, including recommended firmware (via LCM) and AOS
- Deploy and configure the hypervisor cluster on the deployed NCI cluster
    - For VMware vSphere clusters, integrate the vSphere cluster into an existing vCenter or deploy the vCenter Server Appliance (VCSA)
    - For Microsoft Hyper-V clusters, integrate Hyper-V cluster into an existing System Center Virtual Machine Manager (VMM)
    - Configure LCM for automatic updates (online, dark site bundle, or via integrated into an existing dark site LCM webserver)
    - Deploy and integrate Prism Central
- Configure layer 2 virtual networking on hypervisor hosts
    - Configure hypervisor virtual switches

- Test and validate the deployed clusters

11.2.2.14 Additional Activities

- Enable local key management service (KMS) for encryption
- Choose one:
    - Deploy and configure a dark site LCM webserver running either IIS (Windows) or Apache (supported Linux OS) on the customer-provided VM image
    - Harden Nutanix Controller VM and AHV according to the Nutanix Security Guide
    - Install and configure non-factory installed supported hardware (RAM, LAN, SDD, HDD, etc.)
    - Install and configure hardware and drivers for GPU
        - Install host drivers
        - Deploy GPU license server
        - Configure a single test VM for vGPU

11.2.2.15 Limitations

- For each quantity purchased, deployment is limited to a single node
- Maximum of 64 nodes distributed in up to 4 on-premises NCI or dedicated NUS clusters of a single hypervisor type at a single physical site
- Excludes deployment of 1 and 2 node NCI-Edge clusters

Note: Infrastructure Deployment for NCI-Edge is available for the deployment of 1 and 2 node NCI-Edge clusters

Excludes deployment of the Cisco HCI UCS platform

Note: NCI Cluster Deployment or Expansion for Cisco is available for deployment of NCI on the Cisco HCI UCS platform.

- Excludes creation or updates to existing Design Documentation
- Excludes deployment of NUS, NCI Flow Network Security, or NCI Advanced Replication

- Excludes deployment of EUC, AI/ML, Kubernetes, or database workloads
- For VMware vSphere clusters, vCenter Server Appliance (VCSA) deployment is limited to a single standalone appliance
- Excludes integration into an external KMS
- Excludes hardening of 3rd-party components, including VMware ESXi and Microsoft Hyper-V

11.2.2.16 Supported Hypervisors

- Nutanix AHV
- VMware ESXi
- Microsoft Hyper-V

11.2.2.17 Prerequisites

- Hardware that meets all product requirements for the selected hypervisor on NCI.

Note: For information on the requirements for NCI Clusters, see Field Installation Overview in the *Field Installation Guide* on the Nutanix Support Portal.

- Customer-provided Design Document
- Completed Pre-Install Questionnaire

11.2.2.18 Required Product Licenses

- Nutanix Cloud Infrastructure (NCI) Core-based license
- Hypervisor licenses for NCI

11.2.2.19 Delivered Artifacts

- Test Plan
- As-built Guide

11.2.2.20 NCI Disaster Recovery Deployment

Stage: Deploy

The Nutanix Cloud Infrastructure (NCI) Disaster Recovery (DR) Deployment accelerates the deployment of NCI DR solutions, including Asynchronous, NearSync, Synchronous DR, Metro Availability, and Protection Domain-based DR on on-premises NCI and Nutanix Cloud Clusters (NC2) clusters. This offer is ideal for

the Deploy stage of the hybrid multicloud journey.

11.2.2.21 Related Services

- NCI Disaster Recovery Design Workshop

11.2.2.22 Service Scope

Highly skilled consultants with solid domain expertise and rich experience begin by reviewing the customer-provided DR Design Document and requirements. The consultant then deploys and configures one of the supported DR solutions according to Nutanix recommended practices and the customer- provided Design Document. After the deployment, the consultant creates a customized As-built document and updated configuration workbook to document the final configuration of the cluster(s).

Asynchronous or NearSync DR Solution Edition

For customers deploying Asynchronous or NearSync replication between on-premises availability zones. The Asynchronous or NearSync Edition includes the following activities:

Review customer-provided DR Design Documentation, RPO, and RTO requirements

- Review sizing for Nutanix snapshots
- Review requirements for Nutanix Guest Tools (NGT)
- Based upon customer-provided DR design:
    - Configure availability zones
    - Configure protection policies
    - Configure recovery plans
    - Configure custom IP mappings
- Deploy and integrate Prism Central, as required
- Test and validate recovery of nonproduction-protected VMs

Activities for the Async/NearSync Edition

- Install NGT (requires supported guest operating systems)

Protection Domain-based Solution Edition

For customers leveraging legacy Protection Domain-based Async DR and NearSync DR technologies between on-premises availability zones.

The Protection Domain-based Solution Edition includes the following activities:

- Review customer-provided DR Design Documentation, RPO, and RTO requirements
- Review sizing for Nutanix snapshots
- Review requirements for Nutanix Guest Tools (NGT)
- Based upon customer-provided DR design:
    - Configure remote sites
    - Configure protection domains
    - Assign VMs to the protection domains

  Note: NGT is required for cross-hypervisor DR
- Test and validate recovery of nonproduction-protected VMs
    - Validate recovery from the primary site protection domain
    - Validate recovery from remote site protection domain
    - Validate protection domain migration (planned event)
    - Validate protection domain activation (unplanned event)
    - Validate post-DR clean-up procedures

11.2.2.23 Limitations

- For each quantity purchased, deployment is limited to one source cluster and one target cluster. Source and target clusters can be a combination of on-premises NCI or NC2 clusters.
- Excludes design for Nutanix Multicloud Snapshot Technology (MST).

Asynchronous or NearSync DR Solution Edition

- Configuration limited to:
    - 2 availability zones

- 5 protection policies
- 5 recovery plans
- 20 custom IP mappings

- Installation of NGT limited to 5 VMs
- Test and validate recovery of up to 5 nonproduction-protected VMs

Synchronous and Metro Availability Solution Edition

- AHV configuration limited to:
  - 2 availability zones
  - 5 protection policies
  - 5 recovery plans
- ESXi configuration limited to:
  - 1 source and destination container
- Test and validate recovery of up to 5 nonproduction-protected VMs

Protection Domain-based Solution Edition

- Configure up to 10 protection domains
- Installation of NGT limited to 5 VMs
- Test and validate recovery of up to 5 nonproduction-protected VMs

Supported Hypervisors

- Nutanix AHV
- VMware ESXi

11.2.2.24 Prerequisites

- Fully supported and functional on-premises NCI or NC2 source cluster and on-premises NCI or NC2

Note: For information on the requirements for configuring Nutanix Disaster Recovery, see Disaster Recovery Requirements in the *Nutanix Disaster Recovery Guide* on the Nutanix Support Portal.

target cluster that meets all product requirements for the selected DR solution.

- Completed Pre-Install Worksheet

11.2.2.25 Required Product Licenses

- Nutanix Cloud Infrastructure (NCI)
- Hypervisor license for NCI

11.2.2.26 Delivered Artifacts

- Test Plan
- As-built Guide

11.2.2.27 NUS Deployment

Deploy

The Nutanix Unified Storage (NUS) Deployment service accelerates the deployment of NUS Files and Objects data services, providing software-defined storage solutions with in-depth expertise from highly skilled consultants. IT Storage teams have a choice of available deployment scenarios for on-premises NCI clusters, dedicated NUS clusters, or Nutanix Cloud Clusters (NC2). This offer is ideal during the Deploy stage of a hybrid multicloud journey.

11.2.2.28 Related Services

- NUS Design Workshop
- Infrastructure Design Workshop
- Infrastructure Deployment

11.2.2.29 Service Scope

Highly skilled consultants with extensive domain expertise begin with a thorough review of requirements outlined in the customer-provided Design Document. Nutanix consultants collaborate with key stakeholders to fulfil prerequisites and deploy and configure NUS. After the deployment, the consultant creates a customized As-built Guide and updated Configuration Workbook to document the final configuration of the cluster(s).

11.2.2.30 Essential Edition

For customers who want to a single instance of NUS Files or Objects on an on-premises NCI or NC2 cluster deployed within a single physical site.

The Essential Edition includes the following activities:

- Review the customer-provided Design Document, including requirements and planned configuration:
- Review and validate deployment prerequisites, including:
    - Questionnaires, Files binary, virtual networks, and IP addresses
    - Existing NCI or NC2 environment
    - Availability of other infrastructure services required for the deployment, including but not limited to Active Directory (AD), Domain Name Service (DNS), Network Time Protocol (NTP), directory services, identity services, etc
- Deploy either NUS Files or Objects
- Deploy and configure the NUS data service per the customer-provided Design Document

NUS Files

- Configure File servers
- Assign IP addresses
- Create 20 shares
- Configure Internet content adaption protocol (ICAP)
- Verify File service is accessible
- Configure security according to the Design Document
- Configure NUS Files to support workload-specific needs according to the Design Document
- Test and validate NUS deployment
- Optional Activities for NUS Files
    - Configure standard Smart Tiering
    - Deploy and configure File Analytics (NUS Files only) or Data Lens

- Assign IP addresses
- Deploy NUS Objects data service
- Create 5 Objects buckets
- Configure bucket options per the Design Document, including policies, versioning, lifecycle, and write once, read many (WORM)
- Configure certificates
- Verify NUS Objects data service is accessible
- Configure security according to Design Documentation
- Test and validate NUS Deployment
- Optional Activities for NUS Objects
- Deploy and configure Data Lens
    - Verify DR failover
- NUS Objects
    - Configure NUS Objects replication per the Design Documentation

11.2.2.31 Limitations

- Excludes software deployment other than NUS software
- Excludes deployment and/or configuration of 3rd party software such as AD, DNS, NTP, and antivirus and backup solutions
- Excludes migration of existing data to NUS Files or NUS Objects

Note: If migration is needed, specific NUS Migration services are available

11.2.2.32 Essential Edition

- For each quantity purchased, deployment is limited to a single instance of NUS Files or Objects on an on-premises NCI or NC2 cluster deployed within a single physical site
- Configuration limited to 20 Files shares or 5 Objects buckets

11.2.2.33 Supported Hypervisors

- Nutanix AHV

11.2.2.34 Prerequisites

- Fully supported and functional on-premises NCI cluster, dedicated NUS cluster, or NC2 cluster that meets all product requirements

Note: For NUS Files prerequisites, see Prerequisites in *Nutanix Files User's Guide* on the Nutanix Support Portal.

Note: For information on NUS Objects Prerequisites, see Objects Prerequisites and Limitation in *Nutanix Objects User's Guide* on the Nutanix Support Portal.

- Standard Smart Tiering for NUS Files requires that NUS Objects be deployed and configured within the environment
- Required certificates must be generated and made available by the customer
- Customer-provided Design Document
- Completed Pre-Install Questionnaire

11.2.2.35 Required Product Licenses

NCI and NC2 Clusters

- Nutanix Cloud Infrastructure (NCI)
- Nutanix Unified Storage (NUS) - Pro Edition required for NUS Files
- Hypervisor license for NCI

Dedicated NUS Clusters

- Nutanix Unified Storage (NUS) - Pro Edition required for NUS Files
- Hypervisor licenses for NUS

11.2.2.36 Delivered Artifacts

- Test Plan
- As-built Guide
- Configuration Workbook

11.2.2.37 NUS Design Workshop

Stage: Design

The Nutanix Unified Storage (NUS) Design Workshop offers IT teams comprehensive guidance and a structured approach to designing NUS on Nutanix Cloud Infrastructure (NCI). This workshop encompasses NUS Files and Nutanix Objects, addressing critical aspects such as scalability, high availability, disaster recovery, integration, and operational requirements. By focusing on collaboration and comprehensive documentation, the workshop empowers IT teams to ensure scalability, high availability (HA), and seamless integration with existing infrastructure, ultimately achieving optimal outcomes. This workshop is beneficial during the Design stage of a hybrid multicloud journey,

11.2.2.38 Related Services

- NUS Deployment
- Infrastructure Design Workshop
- Infrastructure Deployment

11.2.2.39 Service Scope

Delivered by highly skilled consultants with solid storage domain expertise and rich experience, the NUS Design Workshop service ensures that the solution requirements and required outcomes are identified. Design workshops require collaboration with key customer stakeholders from architecture, storage, virtualization, and networking teams. After the design workshop, the consultant develops a Design Document and configuration workbook that addresses conceptual, logical, and physical solution design elements.

The resulting NUS design can be deployed multiple times in various environments, such as development, test, and production, assuming the business and technical requirements remain the same.

11.2.2.40 Essential Edition

For customers who want to design a single instance of NUS Files or Objects deployed to a single physical site.

The Essential Edition includes the following activities:

- Gather and document solution requirements, constraints, assumptions, dependencies, risks, mitigations, and decisions in the workshop
- Deliver an overview of high-level architecture and concepts of either NUS Files or Objects
- Review the customer's current landscape, use cases, and operations, and identify how NUS data services fit into the existing environment
- Assess resources for the existing on-premises NCI or NC2 environment, including available storage, memory, CPU, and network connectivity
- Evaluate and define the integration of other infrastructure services required for the deployment, including but not limited to Active Directory (AD), Domain Name Service (DNS), Network Time Protocol (NTP), directory services, identity services, etc.

NUS Files

- Define NUS File shares and share types based on the use case
- Identify requirements for Files Analytics or Data Lens
- Plan NUS Files Smart Tiering
- Plan security hardening and compliance as per the Nutanix Security Operations Guide

Note: For security hardening and compliance requirements, see *Nutanix Security Operations Guide* on the Nutanix Support Portal.

- Develop a validation plan that addresses the access and management of NUS Files

Nutanix Objects

- Define Nutanix Objects Store and bucket/s
- Define bucket options, including policies, versioning, lifecycle, and write once, read many (WORM)
- Plan security hardening and compliance as per the Nutanix Security Operations Guide

NUS Files

- Design NUS Files DR options (Protection Domain or SmartDR)
- Plan NUS Files data management (Smart Tiering, Smart Sync, and self-service restore (SSR))

- Define requirements for Files Analytics or Data Lens.
- Develop a validation plan, including NUS Files failover and failback scenarios with non-production workloads.

Nutanix Objects

- Define bucket-level replication use case

11.2.2.41 Limitations

- Excludes infrastructure design for on-premises NCI, dedicated NUS, or NC2 clusters.

11.2.2.42 Essential Edition

- For each quantity purchased, design is limited to a single instance of NUS Files or Objects on an on- premises NCI or NC2 cluster deployed within a single physical site

11.2.2.43 Delivered Artifacts

- Configuration Workbook
- Design Document

11.2.3 Network Fabric Deployment

- Provide Datacenter Connectivity pre-requisites for switching
- Physical rack and stack of Cisco routers and switches in DC and DR
- Patching, firmware updates as required.
- Implement Cisco Switching Infrastructure with Leaf, Spine, Aggregation, Core, Interconnect switch and Server Farm Switches
- Implement Cisco Routers on perimeter for Internet Connectivity and MPLS connectivity.
- Configure the switchports according to the Server-side Requirements.
- Datacenter Routing Configuration for DC and DR
- Logging and Management Integration
- Integration with Centralized Authentication Server
- Minimum Base Line Configuration for Network Devices
- Security and Third-party devices Integration configuration

- UAT Testing

11.2.4 Multi-Tier Security Design

- Physical rack and stack of FortiGate Perimeter, DC and OOB Firewalls in DC and DR
- Physical rack and stack of FortiGate ADC Appliance in DC and DR
- Patching, firmware updates as required.
- Firewall Initial Policy Creation form the provided information from Customer.
- Provide Datacentre Connectivity pre-requisites for switching.
- Firewall Initial Policy Build will be limited to maximum 200 policies/NAT per Firewall
- Configuration of SSL VPN or IPsec connection for OOB
- Configuration of Virtual systems on DC and Perimeter Firewall as per the agreed Design
- Firewall Internet Link Integration with Routers
- Configuration of Applications in the ADC maximum of 50 applications
- Application Migration to ADC maximum of 50 applications
- Services Migration ADC Support
- One-Time Fine tuning of ADC Configuration rules
- Best Practises Implementation
- Integration of Firewall with Central Management
- Integration of Firewalls with Logging Servers
- Integration of Firewalls with DESC Management Tools
- Integration of Firewalls with DESC Security Tools
- Security Feature Implementation bases on Design Document
- One-Time security Profile Finetuning
- UAT Testing

11.3 Phase 1: DNS Security Enforcement And Data Ingestion Foundation

11.3.1 Data Aggregation/Ingestion Layer

- Physical rack and stack of PFS Packet broker in both DC and DR

- Physical rack and stack of Netscout AI Sensor in both DC and DR
- Physical rack and stack of Netscout ISNG in both DC and DR
- Instal AI Streamer in the Virtualization platform in both DC and DR
- Install nCM (nGenius Configuration Manager) on the Virtualization platform in both DC and DR
- Patching, firmware updates as required.
- Complete the physical connectivity for Packet broker and NetScout servers.
- Integrate Packet Broker with AI Sensor and AI Streamer.
- Integrate AI Streamer with Elastic send the logs for phase 1 if required.
- Integrate Service provider Tapping with packet broker (If required in Phase 1)
- Best Practises Implementation
- Integration of Firewalls with DESC Management Tools
- Integration of Firewalls with DESC Security Tools
- UAT Testing

11.3.2 Data Lake / Analytics and Monitoring stack Deployment

- Install and Configure Elastic search Nodes in DC and DR
- Deploy Kibana for visualization, dashboards, and analytics.
- Configure Logstash/Elastic Agent/Beats pipelines for log ingestion.
- Integrate the solution with Log Sources (NetScout / Internal security devices)
- Configure ILM policies and index templates.
- Enable monitoring and alerting features.
- Apply cluster security
- Build custom dashboards for:
- Infrastructure monitoring (CPU, RAM, storage)
- Application performance metrics
- Security event analysis (logs, events)
- Configure Kibana visualizations.

- Create drill-down views and saved searches.
- Deploy Elastic Security for SIEM
- Security Use Case Implementation as per the Design.
- Develop correlation rules for:
    - Threat detection
    - Lateral movement
    - Privilege escalation
    - Malware/IOC detections
- Configure detection alerts and integration with SOAR (If Applicable)
- Integration with DESC Management Tools
- Integration with DESC Security Tools
- UAT Testing

11.3.3 Threat Intelligence Platform

11.3.3.1 Threat Hunting for Proactive Security

11.3.3.2 Introduction:

Traditional security solutions rely on reactive measures, raising alerts only after an attack has begun. To stay ahead of sophisticated threats, we propose a proactive Threat Hunting program integrated within DESC's existing SOC operations. Our approach involves continuous investigation and analysis to identify and neutralize hidden threats before they cause damage.

11.3.3.3 Methodology:

- Threat Intelligence: We leverage industry threat intelligence feeds and our expertise to understand the latest attacker Tactics, Techniques, and Procedures (TTPs). This knowledge informs the development of customized hunting queries and investigation strategies.
- Hunting Playbook: We create a comprehensive Hunting Playbook outlining specific use cases, targeted indicators of compromise (IOCs), and investigation procedures. This playbook ensures consistency and prioritizes high-risk scenarios.
- Data Collection & Analysis: Our team utilizes security information and event management (SIEM) along with endpoint detection and response (EDR) solutions to collect and analyze logs, network traffic, and endpoint activity. Advanced analytics techniques like anomaly detection and user entity and behavior analytics (UEBA) will be employed to identify suspicious patterns.

- Hunting Cadence: We establish a regular hunting schedule, with dedicated time for analysts to conduct proactive searches based on the Hunting Playbook. Additionally, ad-hoc investigations will be triggered based on emerging threats or suspicious activity identified by SOC analysts.
- Threat Hunting Techniques: Our team utilizes various techniques like lateral movement detection, living off the land (LOLBin) attacks, and privilege escalation attempts. We will also explore advanced techniques like memory forensics and packet capture analysis for deep threat investigation.
- Collaboration & Reporting: Threat Hunters will collaborate closely with SOC analysts to ensure timely investigation and containment of identified threats. Regular reports will be generated, detailing hunting activities, findings, and recommendations for improved security posture.
- Early Threat Detection: Identify and neutralize threats before they cause significant damage.
- Improved Security Posture: Proactive hunting helps identify and address security gaps in your environment.
- Enhanced Incident Response: Threat hunting findings inform and refine incident response procedures, leading to faster and more effective mitigation.
- Reduced Attack Dwell Time: By proactively hunting for threats, we can minimize the time attackers have access to DESC systems.

11.3.3.4 Threat Hunting Process: A Deeper Dive

The Threat Hunting process within our SOC follows a structured approach to ensure efficient and effective identification of hidden threats. Here's a breakdown of the key phases:

11.3.3.5 Planning & Hypothesis Development:

- Threat Landscape Analysis: We analyse current threat intelligence and industry trends to understand the most prevalent threats targeting your sector.
- Risk Assessment: Based on DESC's specific environment and security posture, we identify high-risk areas and potential attack vectors to focus our hunting efforts.
- Hypothesis Development: Combining threat intelligence and risk assessment, we develop targeted hypotheses about potential threats and the indicators we might find.

11.3.3.6 Data Collection & Enrichment:

- Data Source Identification: We identify relevant data sources like SIEM logs, EDR data, network traffic logs, and user activity data.
- Data Enrichment: We enrich raw data with additional context, such as user information, device details, and vulnerability data for more comprehensive analysis.

- Normalization & Standardization: Data from various sources is normalized and standardized to facilitate efficient querying and analysis.

11.3.3.7 Hunting & Investigation:

- Query Development: Based on the developed hypothesis, we create tailored queries to search through the enriched data for potential indicators of compromise (IOCs) or suspicious activities.
- Threat Analyst Expertise: Experienced analysts will interpret query results, identify anomalies, and conduct deeper investigations using advanced tools and techniques.
- Threat Validation & Prioritization: Identified threats are thoroughly investigated to validate their legitimacy and prioritized based on potential impact and urgency.

11.3.3.8 Response & Remediation:

- Threat Containment: Upon confirmation of a threat, the SOC team will initiate containment actions to neutralize the threat and minimize damage.
- Incident Response: The Threat Hunting findings are integrated into the overall incident response process for effective mitigation and eradication.
- Security Posture Improvement: Identified vulnerabilities and attack vectors are reported to your security team for remediation, ultimately improving your overall security posture.

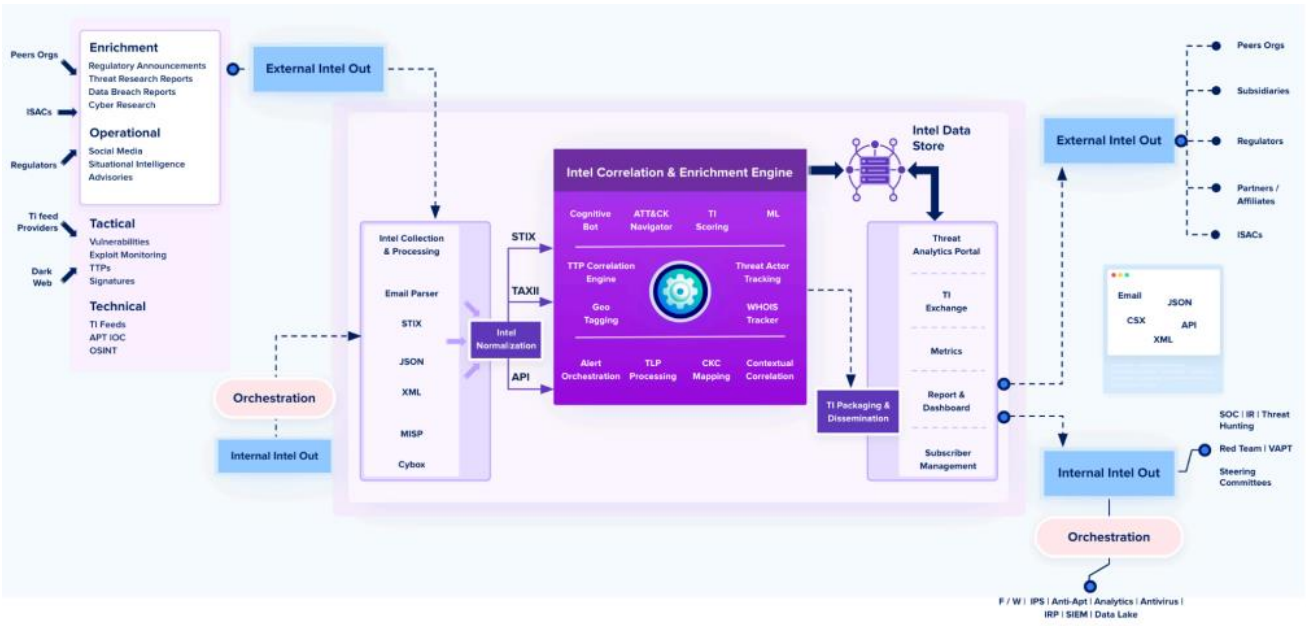
11.3.3.9 Reporting & Learning:

- Hunting Report Generation: We generate comprehensive reports detailing hunting activities, identified threats, mitigation actions taken, and recommendations for future hunts.
- Continuous Improvement: We continuously learn and adapt our hunting strategies based on findings, threat intelligence updates, and feedback from the security team. This ensures our Threat Hunting program remains effective against evolving threats.

11.3.3.10 Threat Hunting Process:

Stage	Description	Activities
Planning & Hypothesis Development	Analyse current threats and risks to develop educated guesses about potential threats.	- Threat landscape analysis (latest TTPs) - Risk assessment (identify high-risk areas) - Develop hunting hypotheses (potential threats & indicators)
Data Collection & Enrichment	Identify and collect relevant data sources, then enrich them with additional context.	- Identify data sources (SIEM logs, EDR data, network traffic logs, user activity data) - Enrich data with user information, device details, and

		vulnerability data - Normalize and standardize data from various sources
Hunting & Investigation	Create tailored queries to search enriched data for signs of malicious activity, then investigate further.	- Develop queries based on hunting hypotheses - Utilize threat analyst expertise to interpret results and identify anomalies - Conduct deeper investigations using advanced tools and techniques
Response & Remediation	Take action to contain confirmed threats, minimize damage, and eradicate them completely.	- Implement threat containment actions (isolate and neutralize) - Respond to SOC team for incident response (mitigation & eradication) - Report vulnerabilities for remediation (improve security posture)
Reporting & Learning	Generate reports detailing hunting activities, findings, and recommendations. Use this information to improve future hunts.	- Generate comprehensive hunting reports - Document findings, actions taken, and recommendations - Continuously learn and adapt hunting strategies based on results and threat intelligence updates



11.4 Phase 2: Internet Traffic Collection, Ingestion Of Large Data Sets In Data Lake And Enhanced Analytics Using Internet Oriented Security Use Cases

11.4.1 Data Aggregation/Ingestion Layer Enhancement

- Connect ISP taps to the packet broker

- Configure packet broker to receive ERSPAN traffic from entities
- Configure filtering and De-duplication rules
- Configuration to enable the Kafka/csv streams as per the playbook for traffic e.g. http, https, dns
- Verification that installed components are reachable and operating with base functionality.
- UAT testing

11.4.2 Data Lake / Analytics and Monitoring stack Enhancement

- Integration with NetScout AI Streamer for the metadata
- Deploy Elastic Security for SIEM
- Security Use Case Implementation as per the Design.
- Develop correlation rules for:
    - Threat detection
    - Lateral movement
    - Privilege escalation
    - Malware/IOC detections
- Configure detection alerts and integration with SOAR (If Applicable)
- Integration with DESC Management Tools
- Integration with DESC Security Tools
- UAT Testing

11.4.3 Threat Intelligence Platform Enhancement

11.4.3.1 Threat Intelligence Platform for Enhanced Cybersecurity

In today's rapidly evolving cybersecurity landscape, organizations face an overwhelming array of threats and must stay vigilant to protect critical systems and data. To meet this challenge, we are proud to offer a Threat Intelligence Platform as a Service (TIPaaS) that provides comprehensive, real-time threat monitoring and analysis to empower DESC's to stay ahead of emerging risks.

11.4.3.2 TIPaaS Benefits

duTech TIPaaS solution goes beyond traditional security tools to deliver advanced threat intelligence that is too suitable DESC's attack surface and risk profile. Key features include:

Continuous Threat Monitoring:

- Aggregates threat data from hundreds of global sources, including security communities and forums, vulnerability databases, and security researchers.
- Leverages machine learning and artificial intelligence to detect anomalies and identify emerging threats in real-time

Contextual Risk Assessment:

- Analyze threats in the context of DESC's assets, vulnerabilities, and security controls.
- Provides prioritized alerts and actionable insights to enable proactive risk mitigation.

Automated Threat Response:

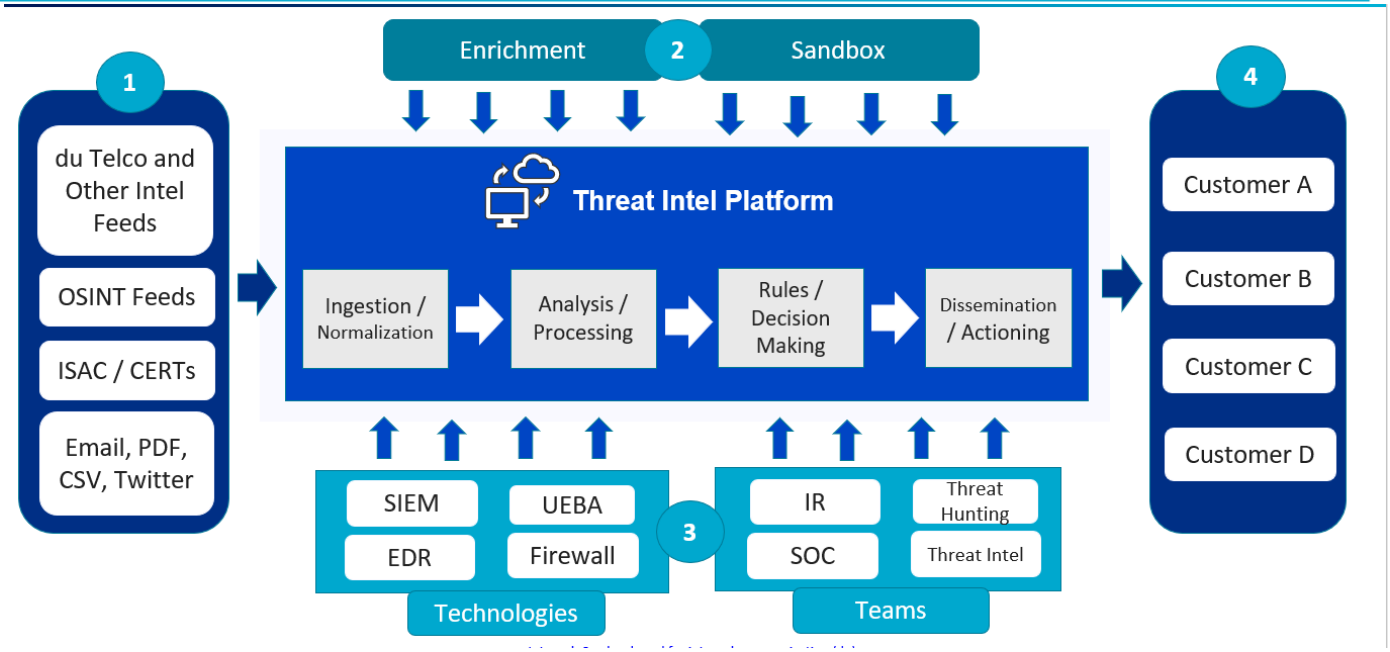
- Integrates with DESC existing security tools to enable automated threat detection and remediation workflows
- Facilitates faster incident response and minimizes the window of exposure to threats.

11.4.3.3 Benefits to DESC:

- Enhanced Cybersecurity Posture: Stay ahead of the evolving threat landscape and reduce DESC's attack surface.
- Improved Incident Response: Quickly identify, investigate, and remediate security incidents to minimize the impact on DESC business.
- Cost-Effective Security: Leverage our expertise and economies of scale to enhance DESC cybersecurity capabilities without the need for extensive in-house resources.
- Compliance and Regulatory Support: Satisfy regulatory requirements through our in-country SOC platform to demonstrate DESC with commitment to a robust security practice.

A proactive and intelligence-driven approach to cybersecurity is essential. DuTech TIPaaS solution empowers DESC to strengthen their defenses, optimize their security investments, and stay resilient in the face of evolving cyber threats.

11.4.3.4 du TIP - Threat Intel Exchange Architecture



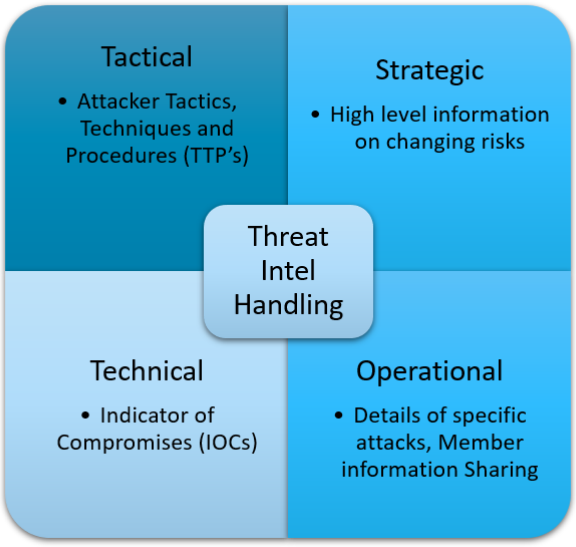
11.4.3.5 Intel Maturity Model

Maturity Indicator	Level 1	Level 2	Level 3 - duTech
Intel Requirement	~	Yes	Yes
Intel Aggregation	Yes	Yes	Yes
Automated Analysis and Scoring		Yes	Yes
Internal Collab with IR & TH		Yes	Yes
Intel Action – Detection Controls	Yes	Yes	Yes
Intel Action – Preventive Controls		~	Yes
External Collab – ISACs / CERT etc.			Yes
Intel Deprecation			Yes

11.4.3.6 Intel Handling Method

Machine Processed

- ✓ Indicators (IOC)
- ✓ Tactics and Techniques
- ✓ Exploit of Alerts
- ✓ Exploitability Mapping
- ✓ Kill Chain Mapping
- ✓ ATT&CK Mapping



Human Processed

- ✓ Threat Intel Alerts
- ✓ Threat Research Reports
- ✓ Malware Advisories
- ✓ Vulnerability Reports
- ✓ Situational Awareness

11.4.3.7 Spoke Feature

Spoke Features	Details
Intel Ingestion (SDO) Per Day	10,000
Maximum Intel Stores	1,000,000
User	25
Sources (All)	25
Rules	10
Reports	20
TAXII Inbox SDO Per Day	5,000
Enrichment (Events Per Day)	50,000
OpenAPI Per Hour	200
Rules Events	20,000
Indicators Allowed	10,000
Score Engine	10,000
Threat Investigations	Included

System Requirement For each Spoke	
vCPU	16
RAM	64
Storage with 3000 IOPS (in GB)	500 to 1000

11.5 Phase 3: Protective DNS Stack Implementation

11.5.1 Protective DNS Stack Implementation

- Installation of Infoblox virtual appliances on Virtual platform based on the approved design
- Create Grid/Reporter/ DNS appliances on the appliances.
- Verify base Grid Functionality and Configuration
- Configure Infoblox DNS and verify the functionality
- Create up to two (5) External Network Lists with a maximum of ten (10) entries defined in each.
- Up to one (1) Cloud Data Connector with up to one (1) Traffic Flow defined if applicable.
- Up to five (5) Custom Lists created within the customers CSP instance.
- Up to two (5) security policies copied from the CSP default security policy.
- Up to two (2) External Network Lists added into the security policy.
- Up to ten (10) DNS Forwarding Proxies added into the security policy.
- Up to five (5) Custom Lists added into the security policy.
- Up to five (32) RPZ security Feeds into NIOS if applicable.
- Activate Security Policy in Log Only Mode
- Add proposed reporting appliance to the Grid Manager.
- Configure Reporting Indexing Parameters.
- OEM best practices implementation
- Integration with DESC Management Tools
- Integration with DESC Security Tools
- Pre-production UAT testing of PDNS
- Production UAT testing of PDNS

11.5.2 Project Closing

- Knowledge Transfer
- As Built Documentation

- UAT Sign-Off
- Project Sign-Off

11.6 Phase 4: Building AI Automation Stack - (ROADMAP)

We acknowledge that Phase 4 represents a transformative and highly strategic initiative for DESC. This covers design & development of a sovereign, security-focused AI Automation Stack powered by a custom Large Language Model (LLM) and GPU-accelerated infrastructure, as conceptually outlined in the RFP.

At this stage, DESC has provided a high-level vision and indicative technical direction for this phase, including:

- Development of a 200+ billion parameter security-specialized LLM
- GPU compute clusters in Primary and DR datacenters within the UAE
- AI agent-based automation for analyses, prediction and reporting.
- Prompt-based Interactive Portal and AI Agent Studio for a holistic visualization
- Deep integration with existing national DNS records for observability, and threat intelligence development

We fully recognize that the detailed Scope of Work (SoW), functional and non-functional requirements, prioritized AI use cases, exact performance KPIs, governance frameworks, and the definitive Bill of Quantities (BoQ) for Phase 4 are still under discussion with DESC which shall be address as and when stage arrives.

Accordingly, we propose the following disciplined and transparent approach:

1. Joint Detailed Scope Definition (Recommended 8–12 weeks post-Phase 3 Go-Live, ideally required for data collection and profiling).
    - Conduct a series of facilitated workshops with DESC's AI Governance, and Operations teams
    - Prioritize and validate 50–75 high-impact AI use cases (e.g., automated sinkholing policy optimization, predictive geo-political threat forecasting, zero-touch compliance reporting, AI-assisted incident narration, etc.)
    - Define measurable success criteria per use case (>92 % accuracy, <100 ms inference, etc.)
    - Finalize data classification, LLM model governance, and red-teaming requirements in line with the Dubai AI Security Policy and UAE Federal AI Ethics guidelines
2. Technical & Commercial Feasibility Study
    - Updated hardware sizing using latest-generation GPUs (Blackwell/GB200 or successor)
    - Detailed BoQ and CAPEX/OPEX breakdown (including UAE-based hosting, power, cooling, and support)

- Risk register and mitigation plan specific to custom LLM development in a regulated government environment

3. Firm Fixed-Price Proposal for Phase 4
   - Only after DESC formally approves the detailed SoW and BoQ will we submit a binding technical and commercial proposal for Phase 4 implementation, maintaining full competitiveness and transparency.

This gated approach ensures that the final Phase 4 deliverables are 100 % aligned with DESC's evolved strategic priorities, budget cycles, and regulatory landscape, while eliminating the risk of scope creep or misaligned expectations.

We remain fully committed and ready to commence the joint scope definition immediately upon DESC's decision to initiate Phase 4 planning.

11.7 Operate for 24 Months

11.7.1 Understanding of Requirement

Our understanding is that the Operate phase covers a full 24-month managed services engagement that spans the complete lifecycle of transition-In, Operate, Transform and Structured Transition-out, immediately after completion and acceptance of Phase 3 (the "Service Commencement Date") for the proposed DNS cybersecurity and observability platform. We shall mobilize the 24×7 operations team, supported by specialists to run the proposed platform and IT environment using approved runbooks, governed by service delivery management, IT process management, reporting and SLA targets as mentioned in RFP.

11.7.2 Solution Architecture and Target Operating Model

du has understood the DESC's requirements and based on our understanding of DESC, DESC is looking for qualified partner for 'Operations' immediately after completion and acceptance of Phase 3 for Infrastructure, Network components, Software, Backup env & proposed DNS cybersecurity and Observability platform requirements, DUTECH' proposition is intended to ensure continuity, reduce business disruption, and help create a positive impact to DESC by delivering the following key benefits:

- Reduced risk: Ability to maintain existing services without a prolonged transition phase while implementing additional services in parallel with ongoing operations.

- Demonstrated Flexibility: Provide a flexible and scalable model for efficient delivery of IT Operations services, ability to adapt to new business requirements.
- Enhanced quality: ability to introduce new processes, tools and skills having the full knowledge of the business needs and requirements, leveraging the experience of more than 14 years delivering Managed Services to clients in the region.
- Continuous Service Improvement: Du's best practices and extensive experience empowers service delivery team to provide best in class service experience to its clients and service delivery team remains committed to provide continuous improvement to DESC. Du shall collaborate DESC with foreseeable service improvements resulting service quality improvement.
- Transformational approach: DU solution is focused on continual improvement in service and user experience. Du are committed to provide added value to existing support model and technological solutions by means of introducing best practices, recommending solutions for automation and self-help /self-service.
- Defined Governance model: with clear roles and responsibilities to improve productivity and user satisfaction

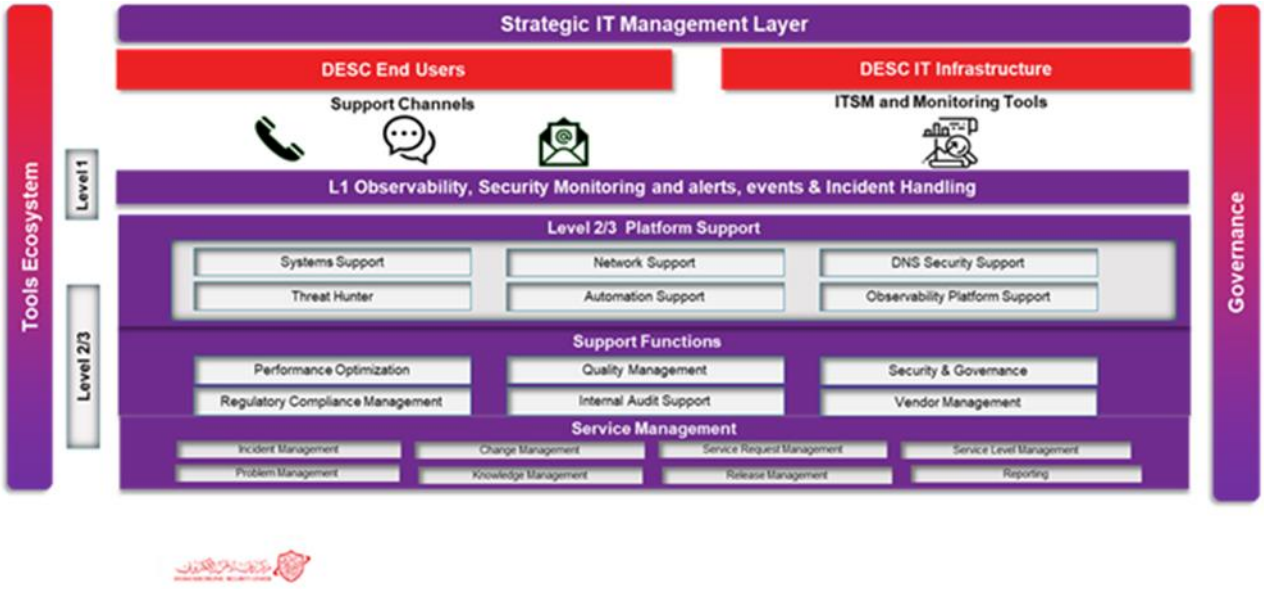
11.7.3 Target Operating Model

DU has the below-proposed operating model to provide Ongoing Support services support for proposed DNS cybersecurity and Observability platform as well as the proposed network IT infrastructure, DU understands the proposed IT landscape shall be managed by the tool stack as proposed by DU and access shall be shared with DU's support teams as required.

DU's Level 1 team shall perform Observability and security monitoring practice using DU's proposed DNS cybersecurity and Observability platform to monitor all aspects/components of the Platform, to produce security alerts (with due classification) initiating incident management. The monitoring team shall verify/tune/follow SOP-based troubleshooting and will assign unresolved tickets to the next level of support. This team will refer to SOP and run book to resolve the tickets and if they need further support, they will elevate the tickets to DU's next level of technology support services for all services Administration, Configuration & Management, Troubleshooting.

DESC's IT users/relevant stakeholders to the in-scope IT platform and infrastructure shall log tickets in DU's proposed ticketing tool with DESC's Service desk which will assign respective tickets to support teams after the initial resolution attempt to achieve first call resolution. DU's proposed advanced Observability tools shall be integrated with proposed ticketing system and its access will be granted to DU's support teams to provide IT managed services.

Du ensure compliance to DESC Technology support requirement of Hardware & Infrastructure Software maintenance support for overall third-party contracts, tools, and OEM support contracts for DNS, Internet Security & Observability platform and the Du's team shall be a support to the DESC for resolving issues along with principal vendors to assure the best response and resolution time when needed.



The operating model is designed to ensure full lifecycle management, continuous protection, operational excellence, and service assurance across all components of the DNS, Security and Observability ecosystem deployed across DESC.

Service Delivery Model Overview

DU will deliver a fully managed, outcome-based operating model built on the following principles:

- 24x7 monitoring and operations through the SOC and Observability command center
- Tiered support structure (L1 → L2 → L3) ensuring rapid triage, advanced troubleshooting and platform engineering

- Integrated DNS, Security, Observability, Compute and Storage administration
- Continuous threat detection and analytics using advanced methods and intelligence feeds
- Automation-first operations to reduce MTTR and manual touchpoints
- Predictive and proactive monitoring aligned to the SLA matrix
- ITIL-aligned process management across Incident, Problem, Change, Release and Service Continuity
- Structured reporting and governance with monthly, quarterly and on-demand reviews

11.7.4 People & Staffing Plan

To ensure stable operations over the next 24 months, we propose to establish and maintain a dedicated, highly skilled technical presence on-site at DESC premises to ensure immediate, hands-on support, operational oversight, and effective escalation management. This physical presence will be essential for delivering rapid response capabilities, seamless coordination with DESC teams, and ensuring continuous operational excellence of the proposed DNS cybersecurity and Observability platform. Our team will provide a consistent technical presence with clear ownership for the environment, enabling quick issue resolution, proactive risk identification and coordinated change execution. This approach ensures the platform runs reliably while the customer continues its transformation work and prepares for future enhancements throughout the 24-month term.

Role	FTE	Coverage	Roles & Responsibilities
Head of Operations / Service Delivery Manager (SDM)	1	Business Hours + On-Call	Primary and deputy named; overall service accountability
Duty Manager / Major Incident Manager (MIM)	1	24×7 Rostered	Owns major incident bridge, escalations
Shift Leads	4	24×7 (3 shifts)	Command center oversight; ensures handovers
L1 Analysts (SOC Operators)	12	24×7 (3 per shift)	Event triage, monitoring, ticket creation
L2 Specialists (Network / System / Cloud)	6	Extended Hours + On-Call	Deep-dive analysis, configuration, escalation
Threat Hunter / Detection Engineer	2	Business Hours	Proactive hunt, rule tuning, ML validation
Automation Engineer (SOAR / Runbooks)	1	Business Hours	Automates triage, response, and reporting
Reporting Analyst / Service Performance Lead	1	Business Hours	SLA, XLA, KPI evidence; dashboards
Cloud Infra Management – L1	3	24×7 (Remote)	Serves as the first point of contact for cloud-related technical issues
Cloud Infra Management – L2	3	24×7 (Remote)	Deal with complex, non-routine cloud environment issues that Level 1 (L1) support cannot resolve.
Cloud Infra Management – L3	1	Business Hours	SME responsible for design, stability, and optimization of the entire DESC cloud platform within this project

11.7.5 Resource CVs

The resources listed in the CV section serves as an indicative profile only and deployment will be based on best effort basis upon resource availability.

11.7.6 Process & Design Compliance

DU shall provide Service Management Service to DESCs IT Department, which includes reporting, organizing weekly & monthly Service Management meeting and reports, Service Management process document management based on ITIL process guidelines. Provide guidance and support in meeting IT

Audit requirements related to IT Service Management and IT Operations. Provide internal team KPI reports. DU's proposed IT Service Management function will support following ITIL driven processes but not limited to:

- Incident Management
- Request Fulfilment
- Event Management
- Access Management
- Monitoring and Reporting
- Routine Maintenance and Patching
- Compliance and Security
- Capacity Management
- Change Control and Deployment
- Knowledge Management
- Vendor and Supplier Management

DU will deploy ITIL aligned Service management processes and will ensure that all services are delivered as per UAE IA data privacy and data protection guidelines

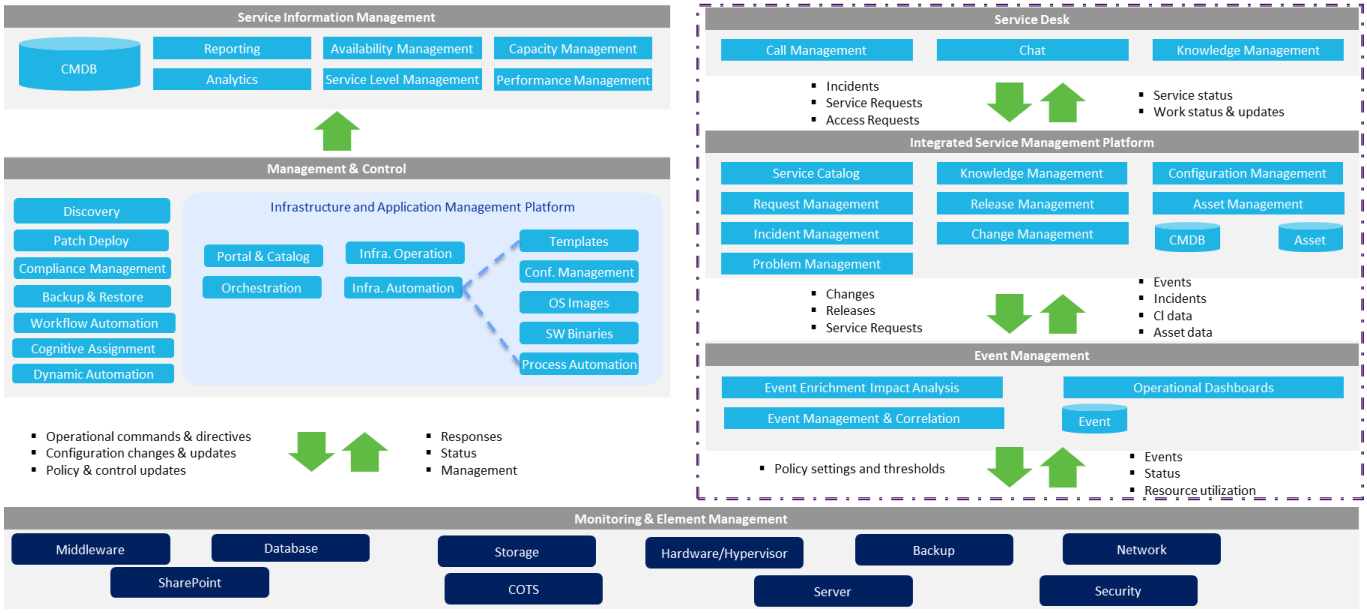


Figure 1- Service Management Driven by ITIL Framework

The core of DU's IT Service Management framework related to this proposal encompasses four key processes- Incident Management, Problem Management, Service Request Management and Change Management with critical interfaces with DESC. The next section defines and illustrates standard workflows for each process. As part of ongoing engagement, these workflows will be enhanced for DESC. Other processes, more internal to operations, like availability and capacity management, are supported by DU as part of the overall service delivery framework.

11.7.7 Incident Management

An incident is defined as an event, which causes or may cause an interruption, unexpected or an undesirable result, which leads to a reduction in the quality of the service and is not part of the standard operation of service that occurs in the systems. The goal of incident management will be to restore the service as soon as possible so that production systems can perform the business services as expected.

The primary goal of the Incident/Trouble Ticket Management will be to attend the complaints by business users and restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Incidents/Trouble Ticket will be properly logged and prioritized accurately routed & tracked and timely resolved and communicated.

Incident Ticket Management at High level is:

Record

The sources of Trouble Ticket will be Email, Direct dial-in number and web/chat. Service Desk team will record these Trouble Tickets in the Ticket management tool. The Knowledge Management tools and historical information on Trouble Tickets will help the service desk resolve issues faster. The service desk teams will be well trained to classify the Trouble Ticket appropriately. Based on the type of Trouble Ticket and its business impact they will assign the severity of the Trouble Ticket. They will be also equipped with standard set of questionnaires required to be asked to the business users.

Track

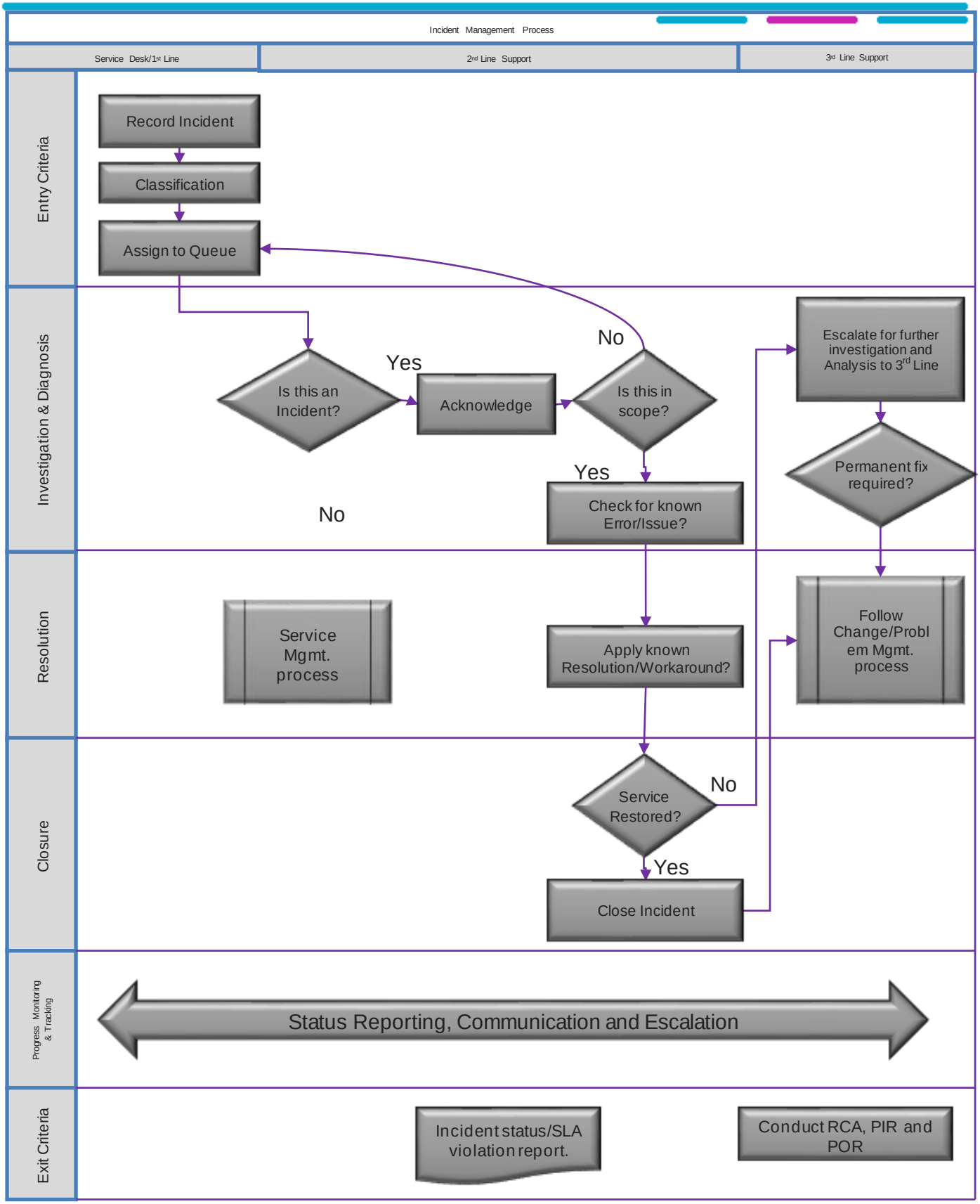
Service Desk teams will escalate the Trouble Tickets which cannot be resolved on call and assigns them for further analysis and resolution. The Service Desks will make sure that the Trouble Ticket SLA is met and will be tracked to be resolved and closed.

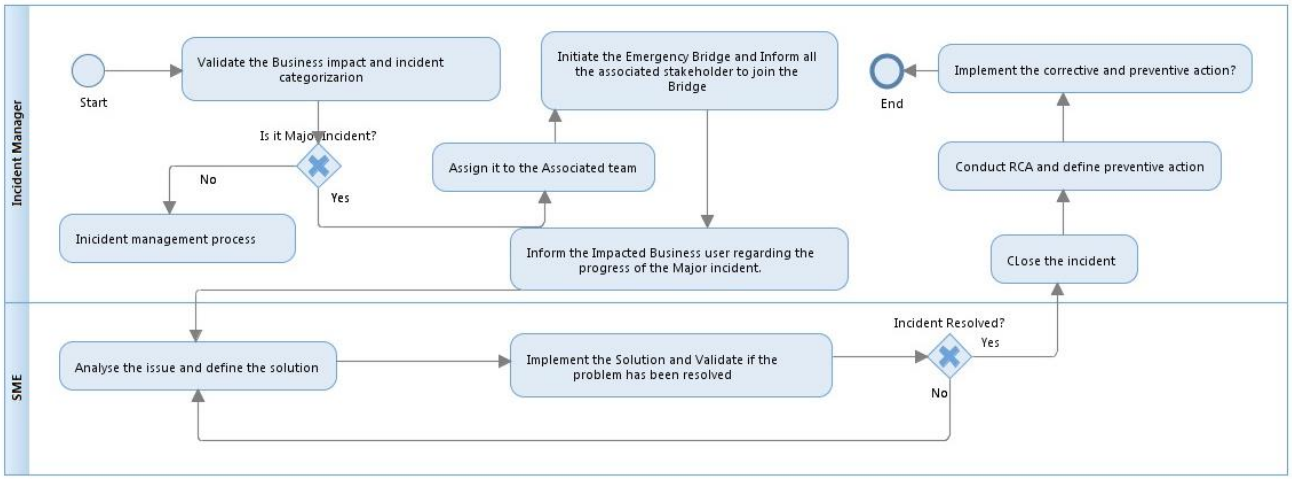
Resolve

The resolution of the Trouble Ticket will be on the call itself or may be escalated, and once it will be resolved Service Desk team will make sure that the resolution information is logged in properly and can be used for root-cause-analysis. They will also ensure the Knowledge base and Historical data will be updated with the findings of new Trouble Tickets if they would have any deviation in handling for future resolutions.

Communicate

The most important aspect of Trouble Ticket Management will be communicating back to the business user. The communication is key when the Trouble Ticket will not be able to get resolved in given SLA framework and is also important when it will be resolved and closed. Escalation within the Service Desk ecosystem is also part of this communication and will be required to seek the attention from higher stake holder to avoid further damage to the business flow.





Key Activities:

Incident identification

The incident will be identified through System event and alarm set in the system. These alarms are proposed to be directly integrated with Incident management tool or event management tool to system health analysis. The system disruption or irregularity/abnormality might be identified by business user and logged with service desk for further analysis and resolution.

Incident logging

End Users will report the Incidents and Service requests to Service Desk. Service Desk agent will record the Incident in the ticketing tool. All incidents will be fully logged and date/time stamped, regardless of whether they are raised through a Service Desk telephone call or whether automatically detected through an event alert.

Incident categorization

Incident categorization guidelines will be present with the help desk and support team for correct incident categorization. All incidents are proposed to be initially categorized based on the type of issue encountered, later the categorization may be changed after identifying the root case. The service desk team governed by customer or DU ensures the incidents will be correctly categorized before incident closure.

Incident prioritization

Prioritization is proposed to be determined by taking into account both the urgency of the incident and the level of impact it is causing. An indication of impact will be often the number of users being affected. The urgency is proposed to be determined based on the crucial are the business services impacted. The correct urgency and impact levels will be used to determine the priority of the incident. The incident periodization guidelines will be defined and agreed with the business user as part of the SLA Agreement activity.

Initial diagnosis

The Service Desk Analyst will carry out initial diagnosis, typically while the user is still on the telephone – if the call is raised in this way – to try to discover the full symptoms of the incident and to determine exactly what has gone wrong and how to correct it. It is at this stage that diagnostic scripts and known error information can be most valuable in allowing earlier and accurate diagnosis. The event and alarms on the other hand will be monitored by the support team for proactive issue identification.

Incident escalation

The incident lifecycle is proposed to be managed and owned by the service desk team (Governed by DU). It will be the ownership of the service desk team to intervene with the support team and ensure the incident will be brought to closure. If required, the service desk will loop in the functional support team or the senior management to ensure timely closure of incident.

Functional escalation: - The service desk team will maintain the details of the functional team based on the subject matter expertise known as functional Escalation Matrix.

Hierarchic escalation: - Untimely resolution incident need senior management intervention and it will be responsibility of the service desk team to ensure timely intervention of the senior management.

Investigation and Diagnosis

DU proposed support groups involved with the incident handling will investigate and diagnose the issue encountered in the system and all such activities will be documented in the incident log for future analysis and reference.

This investigation will likely include activities like:

- Establishing what is the issue or being sought by the user.
- Understanding the chronological order of events and activities which led to the problem.
- Confirming the full impact of the incident, including the number and range of users affected
- Identifying any events that could have triggered the incident i.e., Job Runs, Triggers through other integrated system etc.

Resolution and Recovery

The support team will identify the cause of the problem and resolves the issue, Once the issue will be resolved test will be conducted to validate the issue do not reoccur. Once the issue will be resolved the incident logs will be updated for cause of the problem and the solution and step by step action taken. If any special process will be followed to resolve. the issue the Incident team will update the SOP and knowledge base.

Incident Closure

The Service Desk team will validate that the incident is fully resolved and that the users are satisfied and willing to agree the incident can be closed. Incident closure will involve:

- Closure categorization.
- User satisfaction survey.
- Incident documentation.
- Ongoing or recurring problem?
- Formal closure.

11.7.8 Problem Management

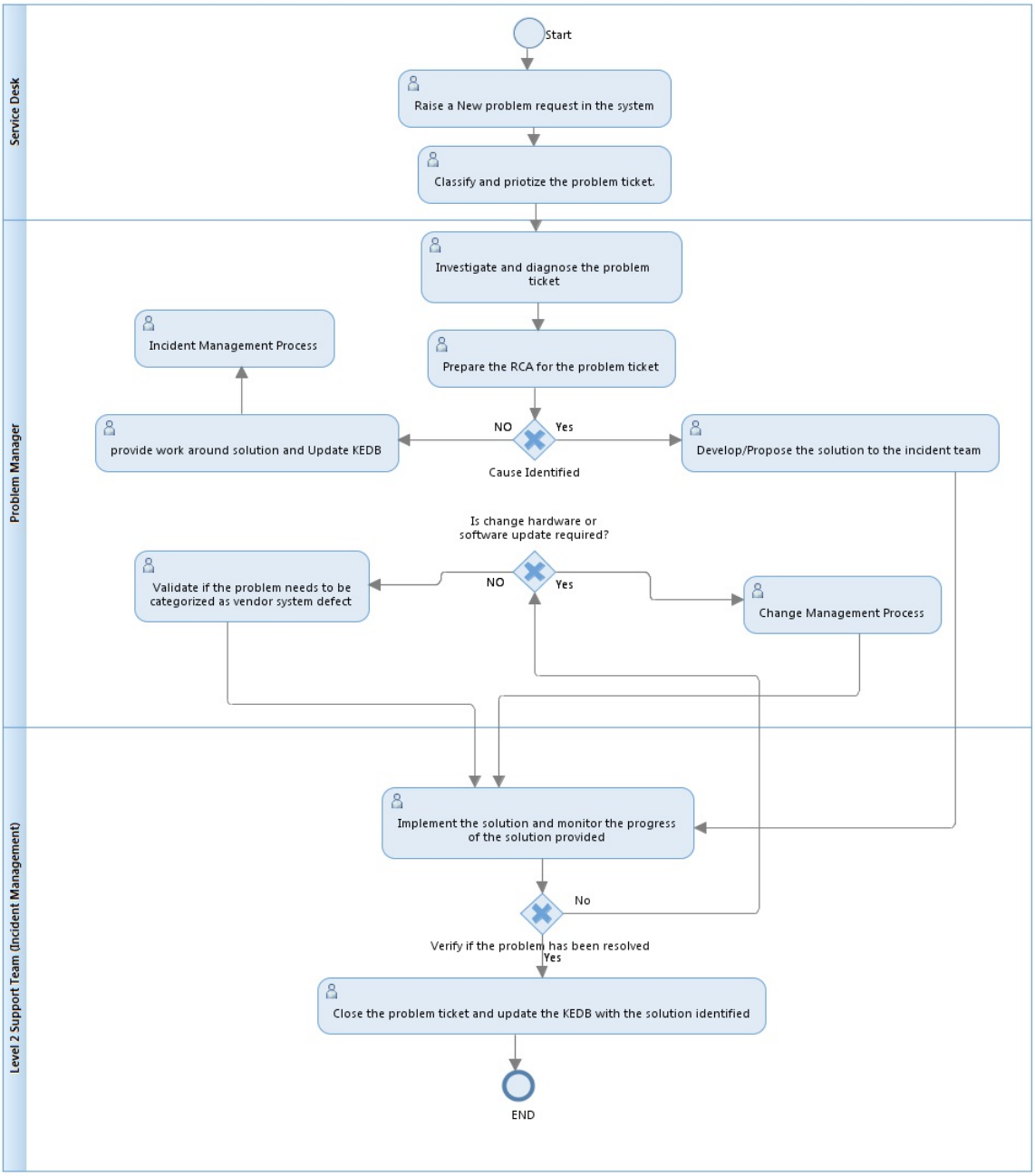
A problem is known cause of one or more Incidents generally identified as part of multiple occurrences of the similar incidents. The basic purpose of Problem Management will be to provide solution to the problem (work around or code fix) and find its root cause to prevent its reoccurrence. This will help to minimize the adverse impact of incidents and problems on business. The problems might be caused by errors

within the IT environment. The root cause analysis will be important as activity to know the reasons and proactively address them. It will help either eliminate the incident, reduce the number of occurrences and severity of incidents. It also will involve reporting the finding and changes into Knowledge Base for the first line and second line of the help desk.

The aim of problem management will be to prevent the repetitive incidents from occurring and to minimize the impact of the incidents that could not be prevented. Problem Management will include the activities required to diagnose the root cause of incidents and to determine the resolution to those problems. Problems will be further categorized as

- Reactive Problem Management: Issues which will be encountered in the live environment disrupting the business service fall under reactive problem management. Such issues will be handled with utmost urgency and priority. Reactive Problem Management will include trend analysis, problem analysis, identification and recording, Problem classification and Problem investigation, diagnosis and elimination of the problem by work around or code fix.
- Proactive Problem Management: Issues which will be identified as part of proactive monitoring and trend analysis will be categorized as proactive problem management. Proactive Problem Management will include Error Control and Problem Control. `

11.7.9 Problem Management Process:



- Problem Classification:
  - The steps involved in Problem classification will be, at a minimum determine:
    - category
    - impact

- urgency
- priority

- Problems will be categorized into related groups or domains (for example, hardware, software, and support software, whatever is appropriate)
- These groups will match the organizational responsibilities, or the User and Customer base, and are the basis for allocating Problems to support staff.
- Identification of a new Problem will be followed by an objective analysis of its impact (that is, its effect on the business)
- DU will be able to design a customized impact system in relation to customer's business needs. The further inclusion of a simple priority rating, subordinate to impact, will provide a total control mechanism.

- Problem Investigation:
  - Available Work-around for the Incidents related to the Problem, as registered in the Incident record database.
  - Activities including updating recommended Work-around in the Problem record, to support Incident control.
  - Showing the cause to be a fault in a registered CI should automatically change the status of the Problem into a Known Error. At this point the error control system and procedures should take over.
- Key Activities:
  - Proactively involve with various teams in Problem Management.
  - Perform trend analysis of incidents and invoke problem management process in case of repetitive incidents, major incidents, and/or known errors. Raise problem records and assign severity based on the impact to the services.

- Perform analysis of the problem and wherever possible devise efficient workarounds to restore service and minimize impact on business operations.
- Perform root cause analysis on Application specific faults/trends and, where appropriate raise a Problem record to thoroughly investigate and devise a permanent fix. Where this permanent fix requires a code change a Change Request will be raised and the fix will follow the Change Management process.
- RCA Methodology used across DU for Problem management:
    - Chronological analysis
    - Pain Value Analysis
    - Brainstorming
    - Ishikawa Diagrams
    - Pareto Analysis
    - Five Why
- Seek confirmation from the customer on the fix implemented and obtain signoff.
- Document and maintain Post Implementation review documents and Root Cause Analysis documents in Known Error Database for future reference and to prevent reoccurrence of the problem.
- Keep the problem raiser informed in timely manner and close problem record through Help Desk upon confirmation from the reporter on the resolution of the problem.
- Update SOP and Knowledge base for workaround solution and problem resolution steps.

- Key KPIs:
    - The total number of problems recorded in the period.
    - The percentage of problems resolved within SLA targets.

- The number and percentage of problems that exceeded their target resolution times.
- The backlog of outstanding problems and the trend.
- The average cost of handling a problem.
- The number of Known Errors added to the KEDB.
- The percentage accuracy of the KEDB.
- The percentage of Major Problem Reviews completed successfully and on time.

11.7.10 Service Request Management

Many times, business users have ad-hock requirement for purpose of analysis or bulk activities. The business situation demands that ad hoc activity. These requests will be handled in service request management. The business user will need to enter the service request in the service request management tool with details required as per the templates defined. In some service requests it might need approval from their managers in case it involves sensitive data. The service request also will be validated at service desk and in case it is not valid and/or incomplete, it will be reverted back to business user. The requirement will be many types based on predefined processes and workflows.

The term 'Service Request' are generic request for many varying types of business demands that will be placed by business users. Many of these will be actually small changes – low risk, frequently occurring, low cost. The SR will be categorized based on the type of SR as follows:

- Operational Requests (ORQs): ORQs will be generally operational tasks that can be fulfilled based on the pre-documented processes in Standard Operating Procedures (SOP). They will be required within timescale that is defined.
- Information Requests (Query Management): Raised by users for information, information requests need to be completed within the timeframe as agreed for the requests.

Typical Service Request Business Needs will be

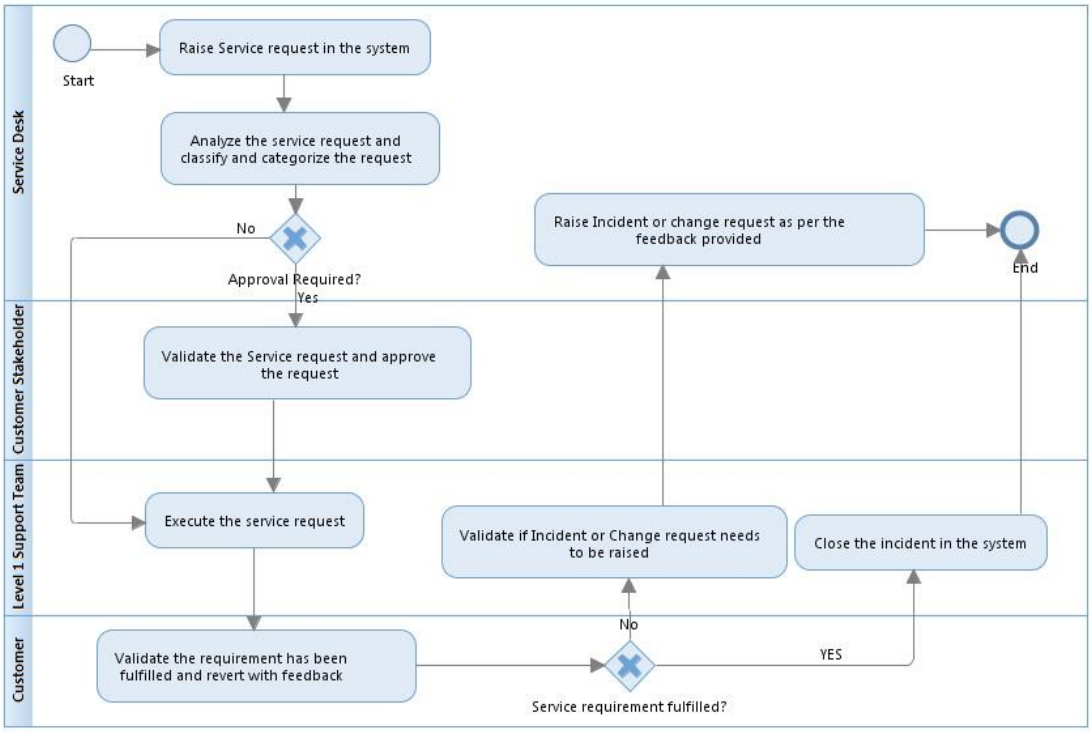
- Provide a single point of contact to handle the customer query and service requests from the business users, and other business departments, to facilitate the users to accomplish business tasks.
- Execute mass requests (offline/online) and monitor.
- Gather customer's information and related requirement details information; clearly understand what customer's actual request is for and the expectation.
- Acknowledge, categorize the receipt of service requests.
- Respond to users in time and handle the simple and duplicate issues using knowledge base or FAQs guide.
- Provide advice, guidance or an existing solution for non-technical issues or known errors of technical issues.
- Plan and allocate necessary resources (Front office, Back office, or management level) to be able to execute the requests.
- Inform the request owner when and how the request will be executed.
- Monitor the request handling progress and keep the information updated.
- Facilitate fulfilment of service requests within agreed business priorities and agreed service levels.
- Report the request handling result to request owner.
- Get the satisfaction comments and close the request process in time.

The objectives of the Request Fulfilment process will include:

- To provide a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists.
- To provide information to users and customers about the availability of services and the procedure for obtaining them.

- To source and deliver the components of requested standard services (e.g., licenses and software media)
- To assist with general information, complaints, or comments.

- Request Management Process:



- User will raise a SR in reporting tool.
- Based on the categorization, SRs shall be forwarded to the relevant services team
- The services team will work on fulfilment of the SR.
- The resolution of SR will be communicated to the customer through support tool.

- Key KPIs:
  - The total number of Service Requests.
  - Breakdown of service requests at each stage.
  - The size of current backlog of outstanding Service Requests.
  - The mean elapsed time for handling each type of Service Request.

- The number and percentage of Service Requests completed within agreed target times.
- The average cost per type of Service Request.
- Level of client satisfaction with the handling of Service Requests.

11.7.11 Event Management

An event can be defined as any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events will be typically notifications created by an IT service, Configuration Item (CI) or monitoring tool. These events will be programmed to communicate operational information as well as warnings and exceptions; they can be used as a basis for automating many routine Operations Management activities.

The goal of Event Management will be to detect and analyse events and determine the appropriate process for dealing with the events. This will include categorizing opened tickets, automating processes, comparing performance/behaviour against Service Level Agreements, and creating the basis of service improvement and reporting.

- Informational: These will be events that should be logged for potential future analysis including confirming if the service is operating as expected.
- Warning: During service design, thresholds will be identified that help gauge the status of a system. When the threshold is reached, predefined parties, or notification groups, will be alerted that the threshold has been reached.
- Exception: This branch will be reserved for configuration items (hardware, software, or service) that are operating abnormally or have failed. Abnormal behaviour criteria will be defined during service design to better understand what types of scenarios trigger what types of exception handling.

These categories, in a way, will be further expanded by some monitoring tools to be more alarm specific. IT NOC will use these alarm categories in analysing an event, or as a hint of the nature of the alarm.

- Key Activities:
    - Communicate operational information as well as warnings and exceptions to the support group configured.
    - Automating many routine Operations Management activities minimizing the efforts and improving the turnaround time
    - Dynamically balancing the demand for a service resource across multiple devices to enhance system performance.
    - Environmental condition monitoring
    - Software license monitoring for usage to ensure optimum/legal license utilization and allocation.
    - Security intrusion detection.
- Events that Signify Regular Operations will be
    - Notification that a scheduled workload has completed.
    - A user has logged in to use an application.
    - An e-mail has reached its intended recipient.
    - Events that signify an exception
    - A user attempts to log on to an application with the incorrect password.
    - An unusual situation has occurred in a business process that may indicate an exception requiring further business investigation.
    - A device's CPU is above the acceptable utilization rate.
    - A PC scan reveals the installation of unauthorized software.
    - Events that signify unusual, but not exceptional, operation. These are an indication that the situation may require closer monitoring.
- Key Metrics:

- Number and percentage of events that required human intervention and whether this was performed.
- Number and percentage of events that resulted in incidents or changes.
- Number and percentage of events caused by existing problems or Known Errors. This may result in a change to the priority of work on that problem or Known Error
- Number and percentage of repeated or duplicated events. This will help in the tuning of the Correlation Engine to eliminate unnecessary event generation and can also be used to assist in the design of better event generation functionality in new services.
- Number and percentage of events indicating performance issues.
- Number and percentage of events indicating potential availability issues.
- Number and percentage of each type of event per platform or application
- Number and ratio of events compared with the number of incidents.

11.7.12 Change Management

The objective of the Change Management process is to ensure that changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Key Benefits will be:

- Standard methods and procedures are used for efficient and prompt handling of all changes.
- All changes to service assets and configuration items are recorded in the Configuration Management System
- Overall business risk is optimized.
- Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption, and re-work.

- Respond to the business and IT requests for change that will align the services with the business needs.

11.7.13 Change Management Process:

- Change Initiation: This activity is responsible for raising various changes, either reactively to resolve problems or proactively to meet business requirements.
- Change Authorization: All changes will be filtered, reviewed, and approved. This would be done by the customer's team.
- Change Implementation: Approved changes shall be implemented by the Operations Team along with L3, Delivery Teams, and 3rd Party Suppliers on case-to-case basis.

11.7.14 The Key Attributes of Change Management Process:

Define Events

The following events may impact the number of tickets or effort per ticket, and therefore impact effort hour/FTE estimates. Scope and effort hours will be re-baselined through change management process when these events occur, and adjustments will be made monthly.

Examples

- New infra. commissioning and de-commissioning.
- New user/site rollout.
- Changes to Architecture, Infrastructure, Network, SSO Enablement, Security, Documentation, and Performance Releases.
- New releases to existing applications.

11.7.15 Define Parameters

The following parameters will help freeze the extent of the change requested to the scope of the engagement. The following list is meant to be indicative only:

- Technology requirements

- Effort and Cost
- SLAs
- Any special activities (batch processing, regular restarts, etc.)

Define Process

DU will work with the Customer Assigned Manager to leverage standard Change Management process. However, DU proposes to leverage the following best practices to evolve as an effective and transparent process:

- Setting up of a Change Advisory Board (CAB) to determine and prioritize scope change requests from various business groups.
- Standardizing the Change Request (CR) form.
- Monthly re-baselining to reflect approved scope change requests.

People

The success of Change Management will depend on its close interaction with various processes in organization. Therefore, people involved in the Change Management activities will have adequate domain knowledge, inter-personal skills, and appropriate rights to perform the functions.

The CAB team will have wide representation of those who would be affected by the Change.

Processes

DU's methodology will address all types of changes that may occur during the engagement. At the time of project inception, the DU Project Manager and Customer Program Manager will agree on a process that elaborates how Change Requests must be communicated, collated, and evaluated. This will be documented as part of the standard Project Plan. The DU Project Manager will identify a group that will perform Change Management activities.

Change requests will be recorded, evaluated, and tracked. All the change requests will be controlled and monitored by the project's Configuration Management team, the status of which will be reported on a regular basis. Change and Version Management will be coordinated along with management's requirement. The configuration management activities will be audited at project milestones and before delivery.

The Change Request Process will define how the change requests are recorded, analysed and either accepted or rejected. All accepted changes will result in changes to the relevant documents, code, project plan, estimates and resource plan. All the changes will be reviewed and approved as per the Quality Plan.

As part of change management process, DU will do a bi-annual review with the customer on the changes to the infrastructure portfolio and if that materially impacts the cost of delivery of the Manged services. On mutual agreement, the costs may be revised downwards or upwards.

Request Change

The Customer Project Manager will communicate the changes to the DU Team through the Change Control Form. Changes will then propose to be approved as per the standard evaluation process and thereby prioritized.

Evaluate Change

The change requests will be assessed and evaluated in terms of the effort, time and cost and its impact on the current project schedule. The customer will have the option to reject, defer or approve this change. On approval, the change will be incorporated as part of the project scope while in the case of a denial; the change request would be closed.

Implement Change

Based on Customer's approval of the changes and the resulting time and cost implications, the change implementation will be affected by the Project Manager. Post implementation of the change,

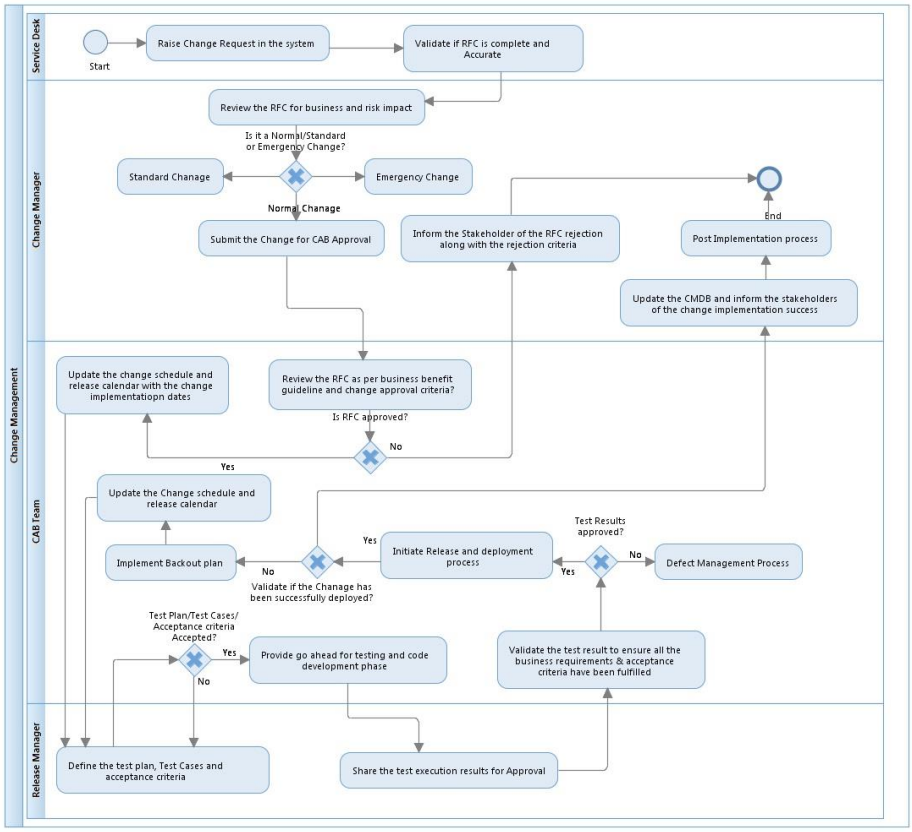
it will be then reviewed to ensure that it has been implemented in line with the business users' expectations and needs.

Another aspect of Change Management relates to change in scope of the original contract in terms of expansion and contraction based upon Customer's requirements. When such requirements will arise, DU's Service Delivery Manager will assess the impact of the change on the contract, and will negotiate with Customer Manager to finalize the adjustments that need to be made to handle the changes.

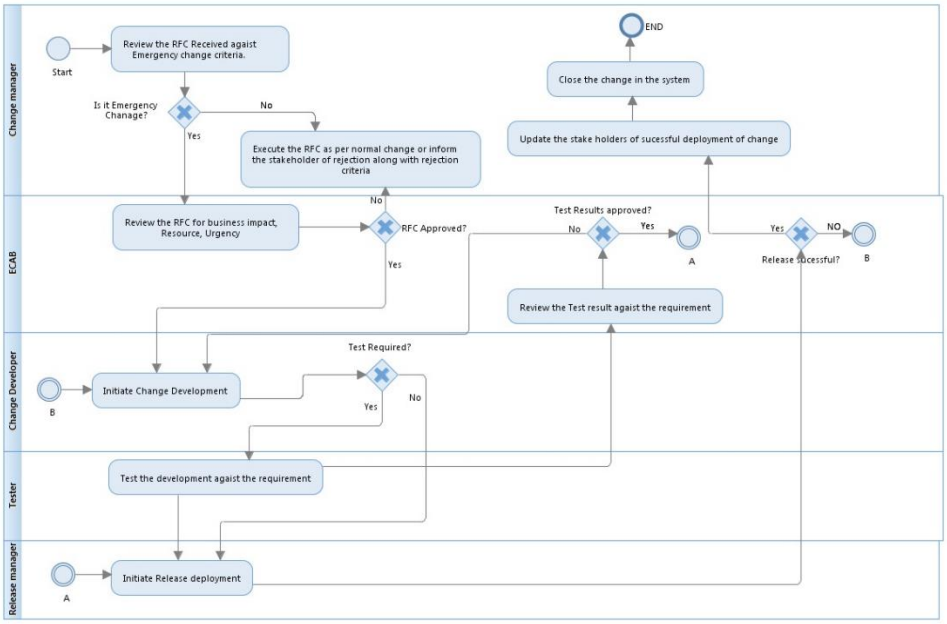
DU will follow the following processes aligned to Customer processes for Change Management:

- Change Management Process.
- Emergency Change Management Process.
- Types of Changes:
  - Standard changes will be changes with no or low service impact or risk and with low complexity these changes will be preapproved changes and need not go through the CAB approval every time.
  - Normal changes will be changes with a medium or high service impact or risk and with potentially high complexity. These changes will go through the CAB process.
  - An emergency change will be a change that, if not implemented immediately, leaves the organization open to high risk. This priority will be reserved for those changes that, if not implemented quickly, can seriously affect Service Levels or result in large costs to the business.
  - All changes will be tracked by the change management tool. All Change Requests will be initiated, authorized, and closed (after the implementation) in the tool so as to ease management and reporting of the changes.

11.7.16 Normal Change Management Process:



11.7.17 Emergency Change Management Process:



Key Activities:

- Planning and controlling changes to the IT architecture and business Services.
- Change and release schedule based on the business objectives.
- Change decision making and change authorization before the change development phase and change deployment on the production environment.
- Ensuring there are remediation plans as part of the deployment plan.
- Management reporting to check the quality of the changes moving to production.
- Understanding the impact of change.
- Derive Service Improvement Based on the changes implemented and services impacted.
- Approve change based on the value addition and service and Business impact.
- Assess and evaluate the change:
    - Establish the appropriate level of change authority.
    - Establish relevant areas of interest.
    - Assess and evaluate the business justification, impact, cost, benefits and risk of changes.
    - Request independent evaluation of a change.
- Authorize the change:
    - Obtain authorization/rejection.
    - Communicate the decision with all stakeholders, in particular the initiator of the Request for Change.
- Coordinate and communicate change implementation plan with the stakeholders and business users.
- Review and close change.
    - Collate the change documentation, for example, baselines and evaluation reports.
    - Review the change(s) and change documentation.
    - Close the change document when all actions are completed.

CAB Agenda:

- Failed changes, unauthorized, backed-out changes, or changes applied without reference to the CAB by incident management, problem management or Change Management
- RFCs to be assessed by CAB members – in structured and priority order.
- RFCs that have been assessed by CAB members.
- Scheduling of changes and update of change schedule (CS) and PSO
- Change reviews.
- The Change Management process, including any amendments made to it during the period under discussion, as well as proposed changes.
- Change Management wins/accomplishments for the period under discussion, i.e., a review of the business benefits accrued by way of the Change Management process
- Outstanding changes and changes in progress
- Advance notice of RFCs expected for review at next CAB.
- Review of unauthorized changes detected through Configuration Management.

- Key Outputs:
  - Rejected RFCs
  - Approved RFCs
  - Change to the services, service or infrastructure resulting from approved RFCs.
  - New, changed or disposed assets or configuration items, e.g., baseline, service package, release package.
  - Change schedule.
  - Revised PSO
  - Authorized change plans
  - Change decisions and actions.
  - Change documents and records.
  - Change Management reports.

- The Key Performance Indicators for Change Management:

- The number of changes implemented to services which met the customer's agreed requirements, for example, quality/cost/time (expressed as a percentage of all changes)
- The benefits of change expressed as 'value of improvements made' + 'negative impacts prevented or terminated' compared with the costs of the change process.
- Reduction in the number of disruptions to services, defects and re-work caused by inaccurate specification, poor or incomplete impact assessment.
- Reduction in the number of unauthorized changes
- Reduction in the backlog of change requests
- Reduction in the number and percentage of unplanned changes and emergency fixes
- Change success rate (percentage of changes deemed successful at review/number of RFCs approved)
- Reduction in the number of changes where remediation is invoked.
- Reduction in the number of failed changes
- Average time to implement based on urgency/priority/change type.
- Incidents attributable to changes
- Percentage accuracy in change estimate.

11.7.18 Tools and Integration – Optional

This section outlines DU's structured implementation plan for the ManageEngine tooling stack that will support DNS Cybersecurity, Internet Security, Observability, and Managed Services operations. The plan ensures seamless integration between ITSM, ITOM, PAM, Patch Management, Analytics, and Automation, with full alignment to DESC's governance, security, and operational frameworks.

Component	Proposed Product	Quantity / Licensing
ITSM	ServiceDesk Plus Enterprise (Arabic/English)	40 Technicians, 1000 Assets
ITOM	OpManager Plus Enterprise	600 Elements (50 Network, 300 Server, 250 Storage) + 20 Users
Analytics	Analytics Plus	5 Users, 10 Viewers, 10 Guests

Privileged Access Management	PAM360	10 Administrators + Unlimited Operators
Server Patching & UEM	Endpoint Central UEM	300 Servers + 10 Technicians
Automation	Automation Platform	2 Bots, 5 Integration Use Cases

11.7.19 Implementation Strategy Overview

1. Centralized Architecture: All tools deployed on-prem within DESC's datacenter with HA where supported (OpManager, Analytics).
2. Integration with DNS Cybersecurity & Observability Platform: SNMP, syslog, API, and Webhook-based links between platforms for incidents, alerts, metrics, and automation triggers.
3. Security-by-Design: All deployments will follow DESC's PDPL, ISR, NESA, and internal compliance requirements.
4. Phased Rollout: Stabilize → Integrate → Optimize → Automate → Enhance Analytics.
5. Tight ITIL Alignment: Powers incident, request, change, asset, SLA, and knowledge processes.

Integration	Purpose
DESC ITSM → ServiceDesk	Auto-ticketing, incident enrichment
DNS Security Platform → DESC ITSM	Telemetry, alerts, behavioural anomalies
DNS Platform → ServiceDesk	High severity incident tickets
DESC PAM (If any)	Privileged activity notifications
Endpoint Central → Analytics Plus	Patch/Risk dashboards
Automation Platform → ITSM	Trigger workflows, auto remediations
DESC ITSM → SIEM/SOC	Logs, traps, performance metrics
DESC Exec	SLA, insights, trend dashboards

11.7.20 Detailed Tools Implementation Plan

1. **Phase 1 – Foundation Setup**
    - Environment Preparation

- Validate infrastructure, OS baselines, network connectivity, DNS entries, certificates, service accounts, and storage allocations for all tool components.
- Establish Production and Staging environments for ServiceDesk Plus, OpManager Plus, Endpoint Central, PAM360, Analytics Plus, and Automation Platform.
- Configure MSSQL databases where applicable and apply DESC security hardening guidelines.

- Core Installations
- Initial Integrations
- Enable central authentication using RBAC/MFA through DESC identity provider (AD/IdP).
- Establish secured communication paths, API whitelisting, vault access policies, and service connectors.

2. **Phase 2 – Configuration of Monitoring, Discovery & Asset Management (Weeks 4–8)**
   - DESC OpManager Plus (optional) in case we are not using DESC existing fault management system
     - Configure discovery profiles using SNMP, SSH, WMI, Telnet, and API-based methods.
     - Discover and classify up to 600 elements (servers, network devices, storage, DNS components).
     - Apply monitoring templates for health, availability, CPU/memory, interfaces, processes, logs, and application services.
     - Enable NetFlow/sFlow/IPFIX collectors for bandwidth and traffic analytics.
     - Configure thresholds, alert routes, suppression windows, and maintenance schedules.
   - DESC ServiceDesk Plus - (optional) in case we are not using DESC existing ITSM management system
     - Populate asset information via OpManager sync.
     - Build CMDB with server, network, and service CI relationships.
     - Configure incident, service request, change, and problem workflows aligned to DESC RACI and severity matrix.
   - Endpoint Central
     - Onboard the servers and VMs and networking devices
     - Configure patch scanning cycles, approval workflows, pilot testing groups, and automated rollout windows.
   - Deliverable for Phase 2
     - Unified asset visibility across monitoring, CMDB, and patch management.

- Baseline monitoring dashboards and configured alerting.

3. **Phase 3 – Security & Operational Controls**
   - PAM360
     - Vault privileged credentials for DNS, observability, Linux/Windows, network, and database systems.
     - Configure password rotation policies, session recording, and approval workflows.
     - Integrate PAM360 with OpManager and Automation Platform to provide secure credential access for tasks and polling.
   - Endpoint Central – Security Baselines
     - Implement CIS-aligned configuration audits.
     - Enable vulnerability assessment scans and risk scoring.
     - Configure patching across Windows/Linux/third-party applications.
   - ServiceDesk Plus – ITIL Enablement
     - Configure SLAs, escalation rules, templates, and change/release approval paths.
     - Build knowledge base articles for DNS, observability, and SOC workflows.
   - Deliverable for Phase 3
     - Privileged access governance and hardened configuration baselines.

4. **Phase 4 – Reporting & Analytics Enablement**
   - Integrate data sources:
     - DESC ITSM (tickets, SLA, asset data)
     - DESC ITSM (events, performance data)
     - Endpoint Central (patch/vulnerability)
     - DESC PAM (session logs & audits)
     - Automation workflows and activity logs
   - Build consolidated dashboards for:
     - SLA compliance
     - MTTR, MTBF, incident trends
     - Patch compliance & vulnerabilities
     - Device health & performance
     - Privileged access usage

- Configure scheduled monthly/quarterly reports for DESC governance.
  - Deliverable for Phase 4
- Unified reporting layer with SOC, observability, and ITSM dashboards.

5. **Phase 5 – Automation & Orchestration Enablement**
   - Automation Platform
   - Deploy platform with HA and two automation bots.
   - Configure up to five vetted use cases (conservative approach):
     - Incident enrichment and ticket field auto-population
     - Routine server/service health checks
     - DNS security policy rule updates (approval-based)
     - Automated certificate expiry notifications
     - Controlled remediation workflows (restart services, clear caches, etc.)
   - Integrate with:
     - DESC ITSM for ticket-triggered automation
     - DESC ITSM for auto-remediation triggers
     - DESC PAM for secure credential retrieval
     - DNS/Observability systems for API-driven approved actions
   - Deliverable for Phase 5
   - Controlled and auditable automation workflows with rollback and approval gates.

6. **Phase 6 – Stabilization, Validation & Knowledge Transfer**
   - Stabilization & Hardening
     - Tune alerts and dashboards based on 4–6 weeks of telemetry.
     - Optimize patch approvals, monitoring templates, automation rules, and CMDB relationships.
   - Operational Validation
     - Conduct end-to-end scenarios:
       - Device failure → DESC ITSM alert → ticket → L1/L2 workflows
       - Patch compliance workflow validation
       - PAM session recording and audit validation
       - SLA reporting demonstration via Analytics Plus

- Automation bot dry runs and fallback validation

- Knowledge Transfer
  - System admin training for all tools.
  - Operation runbooks, SOPs, backup procedures, and maintenance guides.
  - Handover of credentials, architecture diagrams, and configuration documentation.
- Final Deliverables
  - Production-ready ManageEngine suite fully integrated with DESC DNS Cybersecurity & Observability ecosystem.
  - Approved runbooks, SOPs, playbooks, dashboards, and KT artifacts.

11.7.21 Emiratization Plan

Our commitment is to ensure a smooth and sustainable transition through focused Emiratization. We have established a set of clear, progressive targets for the minimum required Emirati national headcount across all roles **within on-site operations and management.** These targets drive the significant increase in Emirati nationals throughout the Operate and Transfer (O&T) phase, culminating in a fully capable and locally-staffed team at the point of handover.

Phase	Duration	Minimum Emirati Headcount Percentage
Year 1	Operation Start to End of Year 1	40%
Year 2	End of Year 1 to End of Year 2	60%
At Handover	End of Year 2 to Contract Completion	70%

11.7.22 Knowledge Transfer Plan

DU managed services team shall work with DESC & our technical teams to understand the newly built DNS cybersecurity and Observability platform & chalk out a transition plan for effective knowledge transfer which will make DU ready to take on day to day operations on its own. The objective of the transition for this engagement is to execute transition of requisite knowledge and documentation of the acquired knowledge for the resources not joining DU for a seamless operations post transition with minimum or no disturbance to operations.

- Current Delivery Commitments and delivery roadmaps taken into consideration to align the transition activities accordingly and assure business continuity.
- Resource Mobilization: Structured ramp-up including availability of key resources and Timely backfilling of resigned resource through DU
- Governance and Setup Service Delivery Operations
- Gap Analysis to ensure all the areas and activities are thoroughly analyzed during Due-Diligence to identify gaps in skill sets, resources, knowledge areas, process, and tools.
- Best Practices and Learning Implementing the industry and transition best practices and learning from previous successful transitions

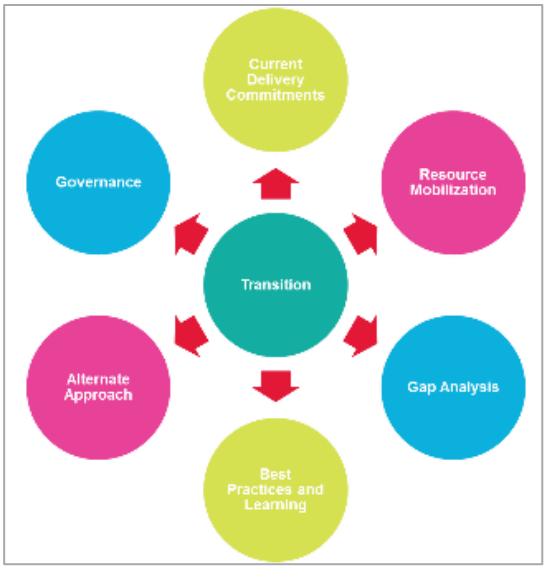


Figure 2- Transition Strategy Key Considerations

DU shall use Service Transition Tool kits which will ensure a seamless transfer of operations to DU for DNS cybersecurity and Observability platform. Our home grown tools like Transition modeler, Information gathering templates, Transition dashboard, Service operation modeler and Gap assessment kit helps us to understand the existing environments & chalk out a transition plan for effective knowledge transfer. DU will undertake a due diligence exercise to fine tune the transition plan which will be agreed with DESC before execution.

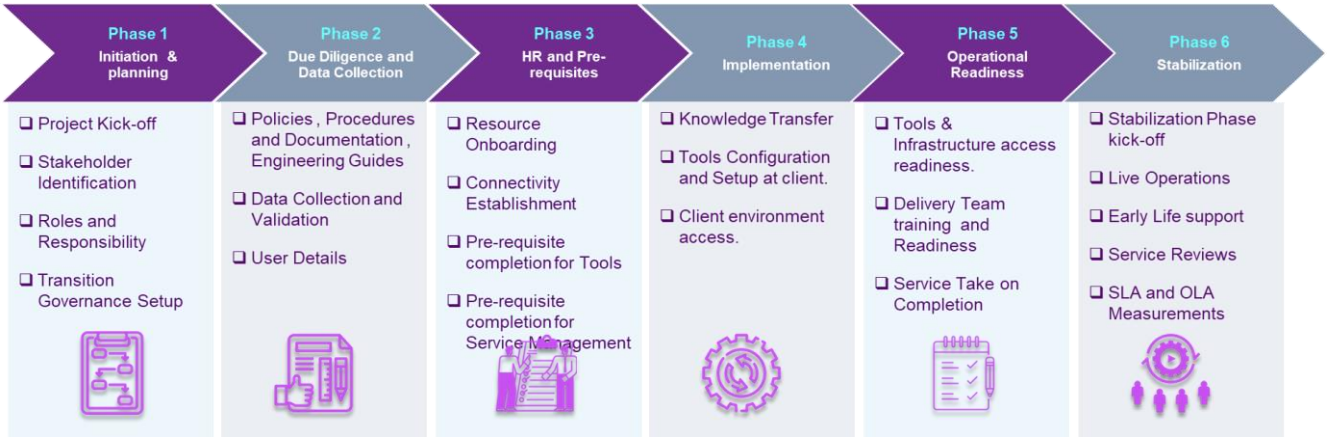
DU proposes a 2 month transition plan before the completion and acceptance of Phase 3 (the "Service Commencement Date"), which is restricted to DESC – Dubai Premises. The high level transition plan showcasing the key phases are mentioned in subsequent section. The transition plan will be updated post due diligence in discussions with DESC.

11.7.23 Summary of required handover and knowledge transfer:

- Develop a detailed transition plan, with tasks, schedules, deliverables in alignment with DESC's stakeholders and availability considerations
- Complete knowledge transfer to acquire relevant subject matter expertise on infrastructure & proposed DNS cybersecurity and Observability platform support services in scope, processes and other dimensions
- Perform the required set of transition activities to prove readiness and obtain sign-off to commence service delivery in a de-risked fashion
- Provide regular reports on transition progress, and adjust transition plans in accordance with potentially conflicting priorities, as required
- Provide best practices in quality process and integrate DESC processes with DU service delivery solution, in conjunction and with approval of DESC
- Develop detailed documentation for all in-scope infrastructure and DNS Internet Security and Observability platform support services as well as required support processes, business process flows, infrastructure technology architecture, interfaces, performance considerations and metrics, roles and responsibilities, process documentation, etc.
- Detail documentation of the infrastructure landscape which includes servers, storage, database, application, Networks, SOC, DNS Internet Security and Observability platform roles and responsibilities, processes etc.
- Detailed documentation of DNS Internet Security and Observability platform including design documents, change request history, configurations, software requirement specifications and understanding of configuration management and release management processes and takeover of source code wherever available.

The proposed transition plan introduces the high-level timelines, approach and methodology to have an effective and fast implementation of DU's service delivery organization. The service delivery date starts

after the preliminary due diligence has been completed and agreed to by DESC, and Du. DESC, Du will finalize the detailed time schedule for delivering the complete set of services during the contract signing.



The pre-transition period, spanning from MOU/LOI issued to contract signature, is needed to complete Due Diligence & Deal-Shaping tasks and to plan Transition detailed processes, activities and responsibilities. DESC and Du will mutually confirm on a start date for this phase.

To perform the Transition in an effective and timely manner, DESC, and Du will work in close cooperation, with involvement and support from both parties, to establish the Tri-party governance model for both Pre-Transition and Transition phases and carefully identify and plan Transition activities. The Pre-Transition phase will start with a detailed due diligence and an audit of current operating model and service-related activities, which will capture the current list of tasks and their respective status.

DESC's organization in scope will be jointly audited with respect to operating models, processes, procedures, interfaces and organizational structure, as well as systems, tools, databases and applications currently in use and deemed necessary for DU's service delivery. After that Du and DESC will define and approve:

- Organizational structure
- Roles and responsibilities
- Transition approach, activities and due dates
- Entry criteria and exit criteria for each activity
- Transition deliverables and milestones

Main activities to be carried out by DU Transition team during this phase are:

- Due Diligence
- Technical solution design enhancement
- Transition plan finalization
- Contingency plan definition and agreement
- Communications and Knowledge Transfer planning

11.7.24 Transformation Roadmap

DU will drive a structured, controlled transformation program throughout the 24-month Operate phase. The intent is to enhance stability, improve visibility, increase operational efficiency, and gradually introduce automation and AI-driven capabilities without creating operational risk.

The transformation roadmap is built around four workstreams defined in the RFP, but executed with measured progression, ensuring that each initiative is validated, documented, and approved by DESC before rollout.

Transformation Principles

1. Stability First: No changes will be made that may impact platform reliability without CAB approval, controlled testing, and fallback readiness.
2. Incremental Adoption: AI, automation, and analytics will be introduced in phased cycles—observe, validate, then automate.
3. Compliance-Driven: All upgrades and optimizations will remain aligned with DESC ISR, NIST 800-53, ISO 27001, PDPL, and internal governance standards.
4. Value Without Disruption: Improvements will be targeted to reduce operational noise, improve MTTR, and enhance visibility with minimal change impact.
5. Platform-Specific Enhancements Only: No broad enterprise-IT transformations; strictly limited to the DNS, Internet Security, and Observability scope.

Transformation Workstreams

1. Workstream 1: Observability & Visibility Enhancement

Goal: Improve telemetry quality, event correlation, and operational awareness in a controlled manner.

Conservative Activities:

- Baseline tuning of existing dashboards and golden signals
- Introduce standardized alert logic to reduce false positives
- Progressive onboarding of new log sources only after data quality validation
- Implement noise reduction rules (dedupe, suppression windows)
- Gradual enhancement of topology mapping and service health indicators
- Build operational playbooks based on real patterns rather than assumptions

Expected Outcomes:

- Lower noise and fatigue
- Better root cause insight
- More consistent S1/S2 detection
- Improved DR drill readiness

2. Workstream 2: Automation and Runbook Optimization

Goal: Automate only high-confidence, repetitive workflows after observing live operations for 6–9 months.

Conservative Activities:

- Identify top 5–10 repeatable actions with low risk (unlock, restarts, log checks, certificate reminders)
- Convert manual runbooks into structured decision trees
- Introduce human-in-the-loop automation before any full automation
- Enforce approvals for all security policy changes and DNS blocks
- Implement gradual rollout: Test → Limited Use → Full Adoption

Expected Outcomes:

- Controlled reduction of MTTR

- Lower manual workload for L1
- Fewer repetitive escalations to L2/L3
- Secure and verifiable automation adoption

3. Workstream 3: Experience & Process Maturity

Goal: Strengthen ITIL practices and governance without major operational restructuring.

Conservative Activities:

- Refine incident, problem, change, and request flows
- Introduce quality gates for RCA, incident timelines, and evidence logs
- Improve shift handover templates
- Build a consolidated knowledge base over time (top 20 → top 50 → top 100 articles)
- Establish structured communications and stakeholder updates

Expected Outcomes:

- More predictable operations
- Better RCA and SLA compliance
- Smoother shift transitions
- Stronger governance and audit readiness

4. Workstream 4: Threat Detection & AI/ML Uplift

Goal: Introduce AI-driven detection and correlation gradually, focusing only on validated, low-risk use cases.

Conservative Activities:

- Phase 1 (Months 1–9):
  - Apply existing AI/ML models for anomaly detection
  - Validate behaviour deviations in DNS, query patterns, and resolver behaviour
  - Tune thresholds to avoid over alerting
  - Build baselines before enabling automated remediation

- Phase 2 (Months 10–18):
  - Introduce correlation logic for DNS + Internet traffic anomalies
  - Integrate curated global threat intel feeds
  - Produce predictive indicators based on long-term trends
  - Begin testing automated containment for well-defined threat categories
- Phase 3 (Months 18–24):
  - Enable limited autonomous workflows for known, low-complexity threats
  - Introduce visual analytics dashboards with investigative overlays
  - Enhance co-relation engines using tagged historical data

Expected Outcomes:

- Higher detection accuracy
- Safer adoption of machine-learning use cases
- Predictive insights without operational risk
- Gradual progression toward semi-autonomous response

Transformation Roadmap (Conservative Timeline)

Period	Focus Area	Key Deliverables
Months 1–3	Stabilization	Noise reduction, config hygiene, dashboard clean-up, baseline tuning
Months 4–6	Observability uplift	Topology maps, alert tuning, correlation improvements, KB Wave 1
Months 7–9	Initial automation	Identify low-risk automations, human-in-loop runbooks, test environment
Months 10–12	AI/ML baseline	ML validation, DNS behavioural profiling, intel feed integration
Months 13–18	Maturity uplift	Advanced dashboards, problem management maturity, limited auto-correlation

Months 19–24	Predictive analytics & controlled automation	Selected autonomous workflows, predictive threat dashboards, process optimization

This roadmap remains fully adjustable and subject to DESC approval at each quarterly review.

11.7.25 Transition Out Plan

DU will ensure an organized, transparent, and risk-free transition of services to DESC or to a Replacement Service Provider at the end of the contract period. The Exit and Service Closure Plan will comply fully with DESC's BOT framework, the RACI responsibilities, and all Closeout & Transition requirements defined in the RFP.

The plan below replaces earlier content and aligns with the expectations for a six-month structured transition period, including a minimum 90-day dual-run, complete documentation handover, secure decommissioning, and full transfer of intellectual property.

Exit Planning and Governance

- DU will prepare a detailed Exit and Service Transition Plan within the first year of the contract.
    - The plan will be reviewed annually with DESC. It will remain a living document throughout the contract lifecycle.
    - Exit planning will be governed through the existing Program Steering Committee, with formal checkpoints during the last two quarters of the contract.
- DU acknowledges its Responsible and Accountable role (per RACI 1.8 mentioned in RFP) for:
    - Preparing and maintaining the Exit Plan
    - Coordinating all exit activities
    - Executing provider deliverables handover
    - Ensuring secure data destruction and decommissioning
    - Providing all exit evidence, artefacts, and compliance documentation

DESC will supervise, approve, and validate all transition outcomes.

Transition-Out Timeline (6-Month Structure)

1. First 2 Months: Audit, Validation, and Preparation
    - Comprehensive inventory and configuration audit Documentation freeze and reconciliation
    - Validation of dashboards, runbooks, SOPs, architecture diagrams
    - Export readiness of monitoring feeds, DNS policies, detection rules, AI pipelines
    - Exit risk assessment and mitigation planning
    - Tool license and subscription review
    - Identification of dependencies (HSM keys, certificates, integrations)

2. Next 2 Months: Initial Knowledge Transfer and Artefact Packaging
    - Knowledge Transfer sessions for all service towers (SOC L1, L2/3 Infra, AI/ML, Observability, Automation, ITIL processes)
    - Packaging of deliverables:
        - Configurations
        - Automation scripts
        - API integrations
        - AI/ML models, training datasets, feature stores, drift logs
        - Correlation engines and threat models
        - DNS policy sets
        - Observability dashboards:
            - Export of all logs, SLA/QBR history, DR/BCP reports
            - Pre-handover testing of tool access and export processes
3. Last 2 Months: Active Transition, Dual-Run, and Handover
    - Reverse-Transition based on shadowing and reverse-shadowing
    - Joint execution of operational runbooks and workflows
    - Transfer of all credentials, RBAC roles, tool access, and certificates
    - Secure data wipe on DU systems after verification
    - Export of last-mile SLA, MTTR, operational and performance reports

- Delivery of final compliance reports (ISO, ISR, PDPL, DPIA)
- Joint Exit Readiness Review and formal sign-off

11.7.26 Roles and Responsibilities

Du	DESC	Incoming MSP (Ifa applicable)
• **Responsible and Accountable for exit planning, execution, handover, and secure decommissioning** • **Provide all deliverables, artefacts, and KT** • **Ensure zero service disruption throughout transition**	• Oversee progress and validate delivered artefacts • Approve acceptance gates and final sign-off	• participate in KT, validation, shadowing • Accept operational responsibility upon transition completion

11.7.27 Governance and Reporting

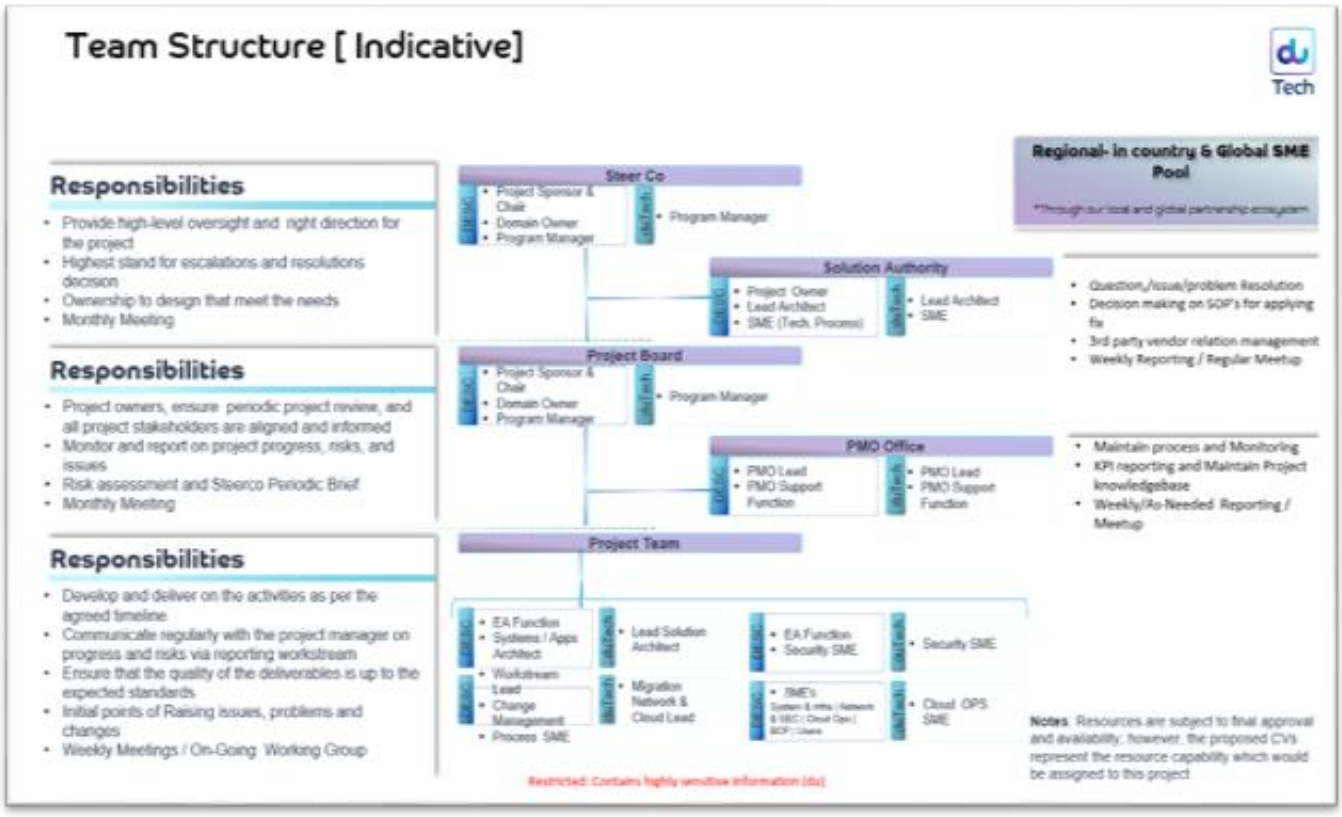
The governance model is an accountability framework and management model that helps to facilitate proper information sharing and define what must be done by each party. The aims of a proper governance model include but not limited to:

- Drive interactions between the two parties.
- Establish feedback mechanisms.
- Encourage communication and desirable behaviour.
- Ensure sufficient management attention to key issues and topics.
- Streamline the decision-making process.

The accountability framework is typically made up of well-defined roles & responsibilities reflecting decision rights among the participants in the IT Operations. In a managed services environment, clarity and communication of decision rights is important. If it is left unaddressed, assumptions from either party will probably be made that can lead to conflicts and unmatched expectations. The decision rights, once defined,

are executed through a management model and the results will be monitored and reviewed through periodic reporting. In a managed services environment, both components are important.

The tri-party management model provides a framework through which decision rights are executed and reporting can occur. Besides, an effective reporting framework is to ensure the visibility of the project performance, it also enable a feedback route for continuous review and alignment of services with predefined targets, and ensure the result satisfy the DESC's expectations.



11.7.28 Reports and Data Exports

DU ensures clear measurable and reportable service levels are established for each IT Service through Service Level Management. Service level metrics are reviewed and analysed to identify areas for improvement. Service levels require adjustments are highlighted to meet the changing business requirements of DESC.

DUs Service Level Management provides a point of regular communication between the Service Delivery team and the client. Service Review Reports will be developed, and regular Service Review Meetings will

be conducted by our appointed Service Delivery Manager to discuss or highlight issues, challenges, and additional requests that surfaced in the delivery of our Managed Services of DESC, based upon and subject to the capabilities of existing and proposed solution tools.

Report Type	Report Name	Description	Frequency
Executive Reports	Executive Service Summary	• Summary of performance of contracted services • All relevant issues needing executive decisions	Quarterly
Service Reports	SLA Report	• Transparency of SLA status and violations • Input to penalty calculations	Monthly
	Management Report: Service Status	• Report consisting of the following statistics: TTR (time to repair) Critical incidents Open trouble tickets and age Closed trouble tickets SLA status, violation Security-related incidents Trends (provisioned services, including historic data)	Monthly
	Management report for critical (by case)	• Report on every critical/high ticket (priority 1 and 2) • Report to include: Cause of incident, description of removal steps/repair actions, Proposed action to prevent a recurrence	On-demand
	Open Service Requests Report	• List of open services or pricing requests per region/globally • Current status of every service request and target time to deliver the request	Monthly
	Service Delivery Time Report	• Actual vs. Standard Average Lead Time to deliver each Service	Monthly, Quarterly, Yearly
	Incident Report	• Categorized reporting on incidents, including: Nature of incident Estimated time to resolution Potential short-term alternatives	Monthly
	Risk Report	• Operational risk status • Status of countermeasures	Quarterly

	Production Status Report	• Reporting on problems, outages, and production impacts	Daily
	Change Report	• Status of changes • Change implementation timelines	Weekly
	Security Report	• Reporting on all security relevant issues	Monthly

11.7.29 Risk Register and Mitigation

Risk Management is a key success factor in delivering the project. Risk is defined as the degree of uncertainty relating to the achievement of the planned outputs or the possibility of an unplanned or unsatisfactory outcome. The word 'possibility' implies a probability level; while the word 'unsatisfactory' implies a measure of 'loss' to someone. Risk must be managed by applying a conscientious effort to their reduction or elimination. Not all risks need to be eliminated entirely; often it is sufficient to reduce the project's exposure to a level that is acceptable to the project and at other times it could be desirable to increase the project's exposure to certain risks. Risk Management costs time and effort, but the rewards can be significant.

Risk Management will be practiced at all levels in the project using the suggested process and documentation as set out in this document. The Project team will apply a risk management approach based on the following principles.

- All team members assist in identifying risks.
- Each identified risk is primarily evaluated in terms of its various probabilities (rated on a scale of Low, Medium and High) of occurrence and its resulting impact (rated on a scale of Low, Medium and High), by the originator.
- Mitigation strategies are devised for all risks, by the team.
- All risks will be categorized.
- All risks are entered into the project risk register by the Project Manager.
- The risk exposures are calculated for all risks of a high probability and high impact nature, medium probability and high impact nature and high probability and medium impact nature. Other specific

risks may be quantified at the discretion of the Project Manager and the Project Sponsor. These resultant exposures are used to prioritize risks response.

- All risks with an exposure of 100% will escalated to the Project Sponsor.
- All team members will assist in suggesting solutions to optimize the risk portfolio.
- Individual comprehensive mitigation plans will be developed for the highest priority (H,H, M.H, H.M) risks to manage their outcome.
- Plans consist of specific actions to be taken by specific individuals within specific time frames.
- Progress is monitored and adjusted as and when necessary.
- As actions are performed, the risk exposure changes, so the priorities continually change.

DU shall align to the below depicted risk management framework, which encompasses people, process, technology and environment risks

Risk Identification:

DU shall proactively identify and document specific risks that could likely occur and adversely affect the objective and timelines of transition and EDGE operations.

Access & Analysis:

Based on the risks identified, DU shall assess, analyze and document the following:

- The underlying cause that would lead to risk materialising
- Risk controls – contingency/ mitigation and action plans required to reduce or mitigate the occurrence and effects of the risk

Mitigation Plan:

DU shall propose best practices and industry standards as mitigation plan / action plan for the identified risk which shall be reviewed and mutually agreed.

Mitigation can be a project by itself which may have associated timelines, efforts and cost.

Implement:

Mutually agreed mitigation shall be implemented with appropriate planning and consensus

Measure, Control, Monitor:

DU shall establish processes for monitoring and reporting on the occurrence of risks

DU shall control the risks on an ongoing basis by preventing and mitigating the identified risks aligned to mutually agreed mitigation/action plan

DU shall on a quarterly basis evaluate its risk management processes and on a monthly basis the individual Risks and Risk Controls in scope of the risk management processes in order to identify, document and implement improvements to the Risk Controls.

DU Risk Matrix:

Probability of Impact	Trivial	Very Low	Very Low	Very Low	Low	Low
	Minor	Very Low	Very Low	Low	Low	Medium
	Moderate	Very Low	Low	Low	Medium	Medium
	Major	Low	Medium	Medium	High	Very High
	Extreme	Medium	Medium	High	Very High	Catastrophic
Impact = Probability of Impact X Likelihood of Occurrence		Rare	Unlikely	Moderate	Likely	Very Likely
		Likelihood of Occurrence				

DU shall adhere to RAID log to track risks and issues to mitigate during transition and the risks and issues that are not mitigated during transition shall be handed over to BAU operations for mitigation

11.7.30 Service Levels and KPIs

11.7.30.1 Minimum Service Levels and KPIs

Service Level Agreements are a critical element of any managed services agreement, whereby the Service Levels are designed to support the business.

The key objectives of Service Level Management are to:

- Manage the delivery of services within agreed Service Level definitions.
- Manage exceptions.
- Negotiate changes to Service Levels in accordance with contractual requirements and changing business needs.
- Minimize the impact of service delivery issues on the DESC's business.
- Provide service level reporting to the DESC.

DU has followed DESC's defined convention and severity levels to define the business impact of an incident on DNS cybersecurity and observability platform. The use of these severity levels allows DU to

rank the customer's service request in the ticketing system based on the criticality of the issue with the following severity level definitions being used by DU:

Severity	Description	Typical Examples
S1 – Critical	Full system failure with national impact, no workaround	DNS outage, SOC alert blackout, DR site failure
S2 – Major	Partial degradation, multi-user or multi-component impact	One PoP down, delayed dashboards, detection lag
S3 – Minor	Limited degradation, workaround exists	Report latency, minor correlation delay
S4 – Informational	Cosmetic or advisory	Feature requests, non-blocking UI issues

DU is proposing to the suite of SLAs as requested by DESC in RFP that have been tailored around the specific scope of the services, are aligned to industry and market SLAs, whilst ensuring they address the business needs of DESC. These SLA's will address the Service Management requirements, speed to react and speed to resolve the IT environment.

#	Metric	Target	Severity	Remarks
1	DNS Uptime	≥ 99.999%	S1	Mission-critical metric
2	Dashboard/API Availability	≥ 99.98%	S2	Includes management UI
3	Data Center Uptime	≥ 99.982%	S1	Aligned to Tier-3
4	Geo-replication Latency	≤ 500 ms	S2	Round-up rule applied
5	DR Drill Success Rate	100% quarterly	S1	Mandatory test
6	Threat Detection Latency	≤ 60 sec	S1	Key AI detection SLA
7	Mitigation Time	≤ 5 min	S1	Detection-to-containment

8	Log Delivery Latency	≤ 15 min	S2	Source-to-central ingestion
9	RCA Submission (S1)	≤ 5 business days	S1	Full RCA (CAPA included)
10	RCA Submission (S2)	≤ 7 business days	S2	As above
11	Ticket Response (S1)	≤ 15 min	S1	Time from incident to ticket
12	Ticket Response (S2)	≤ 30 min	S2	
13	Ticket Response (S3)	≤ 4 hours	S3	
14	MTTR (S1)	≤ 4 hours	S1	Mean Time to Restore
15	MTTR (S2)	≤ 12 hours	S2	
16	Threat Detection Accuracy	≥95% DNS, ≥90% Traffic	All	AI/ML model precision metric
17	Packet Loss	≤ 0.01%	All	Measured end-to-end

11.7.30.2 SLA Exclusions

DU shall be excused from responsibility to meet a designated Service Level to the extent and for the time period that the failure to meet such designated Service Level was due to:

1. Problems or incidents where the 'Time to Repair' is deponent on a 3rd party vendor. The 'Time to Repair' will be excluded from the SLA measurement.
2. Problems or incidents where the 'Time to Restore' is required to perform a restore of a system or device. The 'Time to Restore will be excluded from the SLA measurement.
3. Problems determined to be caused by the actions or inaction of DESC.
4. Planned outages such as scheduled maintenance or other scheduled outages.
5. Problems where the provision of services was dependent on third party Service providers or third-party products not provided by DU.
6. Performance or non-performance by DESC third-party vendors and suppliers in accordance with DESC contracts.

7. Any software defects/bugs where the software vendor/publisher has not supplied DU with a patch to fix the defect/bug.
8. DESC prioritization of available resources provided by DU.
9. Hardware failures in Customer provided hardware.
10. Circumstances that constitute a force majeure event

11.7.31 Implementation Plan and Timelines

The Operate phase is implemented not only to maintain system stability, but also to transform DESC's DNS cybersecurity, and Observability ecosystem into a proactive, AI-enabled, automated, and intelligence-driven environment. The overall implementation plan focuses on continuous uplift across people, processes, and technology while ensuring uninterrupted service delivery and the transformation program will run in parallel with steady-state operations, with clear milestones and measurable outcomes.

The implementation plan is designed to ensure full lifecycle management, continuous protection, operational excellence, and service assurance across all components of the DNS, Security and Observability ecosystem deployed across DESC.

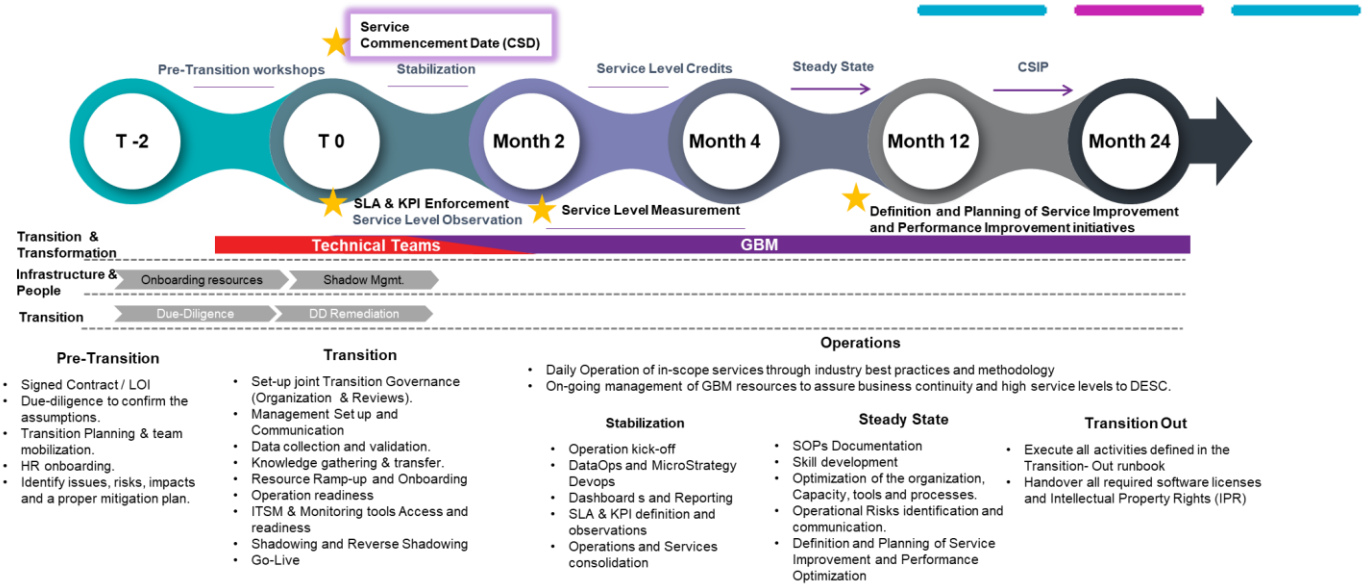


Figure 3- Indicative Transformation Roadmap

Note | *The above plan and respective phases are indicative in nature and the actual plan shall be co-developed and mutually agreed between du and DESC post award of the contract*

- Transition-In: The engagement begins with a Transition-In phase where DU takes operational ownership of the DNS cybersecurity and Observability platform environment in a controlled and transparent way. This includes knowledge transfer from the technology teams, validation of the existing platform setup, establishing monitoring baselines, and confirming the incident, change, and escalation processes. The objective is to ensure service continuity while DU assumes responsibility with minimal disruption to ongoing operations.
- Operate: Once the environment is stabilized, the Operate phase becomes the core of the service. DU will provide day-to-day operational management across the infrastructure, network components, platform services, and backup operations as outlined in the RFP. Activities include proactive monitoring, incident and problem management, preventive maintenance, backup and restore operations, performance tuning, capacity reviews, and coordination with DESC technical teams. The goal is to maintain high availability, improve platform reliability, and keep the environment secure and compliant.
- Transform: DU will lead a structured and carefully managed transformation program over the 24-month Operate phase. The program aims to strengthen stability, improve transparency, boost

operational efficiency, and progressively implement automation and AI-driven capabilities, all while minimizing operational risk.

- Transition-out: As the contract moves toward closure, the Transition-Out phase ensures a well-organized handover to DESC or to a future service provider. This includes updated documentation, structured knowledge transfer, and resolution of outstanding operational items.

The overall intent is to deliver consistent service throughout the 24-month period while helping DESC

11.7.32 Assumptions, Exclusions and Dependencies

11.7.32.1 Assumptions -

1. DESC will provide all necessary & appropriate information, documentation templates, standards, and guides as evidence to DU on commencement of this project.
2. The project delivery completion timelines mentioned here are tentative and the exact timelines would be defined as part of the project commencement plan from DU.
3. All deliverables will be in English language only.
4. Availability of DESC key stakeholders (if required) during the project execution phase for gathering information, support, resolution of reported findings, etc.
5. Deliverables submitted shall be reviewed and approved by the DESC designated representative within five business days. Any deliverable not responded within 5 days will be deemed accepted and approved by default.
6. DESC will provide and arrange for meeting spaces within its facility for all required vendor meetings.
7. Timely availability of Infrastructure credentials or timely availability of a person with access to necessary infrastructure components or equivalents.
8. DU shall liaise with the OEM for problem resolution for any reported Incident, however customer shall own overall third-party contracts, tools, and OEM support contracts for customer's IT infrastructure.

9. If while performing Services, support personnel require access to other vendor's products that are part of DESC system, DESC will be responsible for acquiring all such products and the appropriate license rights necessary for DU to access such products on DESC's behalf.

11.7.32.2 DESC Dependencies

The following activities are the responsibility of DESC, which will be required to enable DU to complete their responsibilities and the Statement of Work(s). DESC will fulfil these responsibilities at no charge to DU.

- Provide du access privileges to the in-scope devices and DESC personnel, where the services are to be performed for the purposes of knowledge transfer, information gathering, and confirmation of the adequacy of operational support procedures. Provide orientation to DU support staff and provide them with training, as required.
- Comply with all copyright restrictions, copyrighted materials provided to do for-training purposes.
- du envisions its resources operating out of DESC premises during Implementation and Operations phases wherein office infrastructure (such as Workplace/Laptops, Desk Phone, VPN Access etc.) will be provided by DESC for these resources.
- Provide, for all resources performing Support Services at DESC site, a safe and healthful workspace (e.g., a workspace that is free from recognized hazards that are causing, or likely to cause, death or serious physical harm, a workspace that has proper ventilation, sound levels acceptable for resources performing Services in the workspace, and ergonomically correct workstations, etc.).
- Required data transfer speed and network bandwidth, even during peak working hours.
- DESC will provide full support and cooperation from their onsite and collaborative resources to assist du resources in delivering the support model effectively.
- Allow access by vendor maintenance personnel or du to DESC designated Locations for purposes of problem diagnosis / resolution.
- Be responsible for any costs (labour, travel, shipping, storing h/w spares and hot swappable devices etc.) associated with the provision of maintenance services which is not covered as part of this proposal.

- Define and provide to du, DESC security policy and procedures, including access controls and backup and restore requirements.
- Be responsible for the physical security at DESC locations, including physical security for in scope devices.
- Be responsible for the identification and interpretation of any applicable laws, regulations, and statutes that affect DESC existing network infrastructure that du will have access to during this project. It is DESC responsibility to assure that the systems and programs meet the requirements of those laws, regulations and statutes.
- Notify du of personnel changes that may impact management processes, approvals or other support responsibilities. du responsibilities are limited to within the framework of proposed solution/manpower
- All IT security policies and procedures will be shared with du during kick-off. Any new policy implementation may result in invoking of the change management process.
- Obtain any approvals and enable access necessary for du to access and use your resources and systems to the extent necessary for du to provide the Services.
- Make suitable staff, information, and materials available as du reasonably requires. du will not be liable for any damage or delay arising from inaccurate, incomplete, or otherwise defective information and materials supplied by or on behalf of the DESC.
- Be responsible for agreements with, management of, and the input and work of third parties whose work may affect du ability to provide the Services. Except to the extent du specifically agrees otherwise in this Service Description, DESC is solely responsible for any third-party hardware, software or communications equipment used in connection with the Services.
- Be responsible for the management of DESC personnel, the management of third-party suppliers whose products, work, or information may affect du ability to, or be required by du to, provide the Services, third party hardware, software, or communications equipment used in connection with the Services.

- Safeguard the integrity and security of software and data used in the Services from access by unauthorized personnel; and ensure that DU is not exposed in performance of the Services to any United Arab Emirates regulated data (whether HIPAA or FFIEC or other), or any other Personally Identifiable Information (PII) originating from and regulated by any country outside the United Arab Emirates.
- Be responsible for the review and evaluation of any du recommendations as well as all final decisions and implementations.
- Provide all necessary security badges and clearance for access. DESC will be responsible for ensuring that it has appropriate backup, security and virus-checking procedures in place for any computer facilities DESC provides or which may be affected by the Services.
- Provide all information and materials reasonably required to enable DU to provide the Services. DESC agrees that all information disclosed or to be disclosed to DU is and will be true, accurate and not misleading in any material respect. du will not be responsible for any loss, damage, delay, or deficiency arising from inaccurate, incomplete, or otherwise defective information or materials supplied by the DESC or their representative.
- Ensure DESC has appropriate agreements in place with third parties to enable du to perform the Services under this SOW, where DESC is using or providing du with third party information, support or materials for a project including but not limited to, where DESC is employing other suppliers, whose work may affect du' ability to provide the Services. Unless specifically agreed to otherwise in writing.
- Unless otherwise expressly stated in this SOW, be responsible for ensuring its own compliance with all laws and regulations, including but not limited to, those pertaining to product safety and regulatory compliance for 3rd party products including those recommended by DU. DESC is solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws, rules and regulations that may affect DESC 's business and

any actions DESC may need to take to comply with such laws. DU makes no representations or warranties with respect to product safety or regulatory compliance of 3rd party products.

- Obtain any necessary consents and take any other actions required by applicable laws, including but not limited to data privacy laws, prior to disclosing any of its employee information or other personal information or data to du. DESC also agrees that with respect to data that is transferred or hosted outside of the United Arab Emirates, DESC is responsible for ensuring that all such data transmitted outside of the United Arab Emirates adheres to the laws and regulations governing such data.
- Before making available to do any facilities, software, hardware or other resources required by du, obtain any licenses or approvals related to these resources that may be necessary for DU to perform the Services and develop Materials. du will be relieved of its obligations that are adversely affected by DESC failure to promptly obtain such licenses or approvals. DESC agrees to reimburse DU for any reasonable costs and other amounts, including costs of litigation and settlements, that DU may incur from DESC failure to obtain these licenses or approvals.

11.7.32.3 Exclusions

1. IT Service Desk for End Users
2. End user laptop, desktop and deskside field support
3. Existing Infrastructure, Network and platform support
4. Design or redesign of IT Policies, firewall or security policy blueprint.
5. Performing any application architecture consultancy
6. Support for any IT assets, technologies or tools not listed in this document.
7. Any Implementation activities, Data acquisition, augmentation or cleansing.
8. Any Services not specifically identified within this scope of Services

11.8 Final Project Ownership Transfer and Exit Fee

Upon the successful completion of the contractual obligations and final sign-off, the ownership of all project deliverables, accumulated data, operational models, and documented intellectual property (IP) created specifically under this contract will be transferred entirely to the DESC

To facilitate this crucial final transition—which involves comprehensive handover documentation, knowledge transfer sessions, and the final administrative release of all project assets—**a mandatory Project Exit and Transfer Fee will be levied**. This ensures a clean, documented, and complete transition of the managerial and professional project ownership to DESC

12. Hardware Support and Maintenance

Refer the attachment : Du Response - RFQ 762640 - 12.0 Hardware support maintenance

13. Project Responsibilities

13.1 Du Responsibilities

1. Providing a single point of contact, the Du Project Manager, to whom all DU communications may be addressed and who has the authority to act on all aspects of the services.
2. Designating a backup when the primary PM is not available.
3. Undertaking to guarantee continuous supply of any relevant resource required to fulfil their obligations under this SOW.
4. Du & DESC jointly review and execute a Milestone/Service Completion Certificate upon completion of the milestones.
5. Participating in regularly scheduled project review meetings or conference calls.
6. Notifying the DESC PM of any requested schedule changes within five (5) business day of any scheduled activity. DU will use reasonable efforts to accommodate schedule changes and/or cancellations made after this time.
7. Providing a single point of contact "Project Manager" who will be responsible to track the project progress and technical leader to discuss pure technical issues or challenges till handover to service operation.
8. Providing a single point of contact, the DU Project Manager (DU PM), for all project issues within the scope of the project.
9. Supply of relevant DU resource required to fulfil their obligations under this SOW.

10. Providing DESC with a list of designated du resources with roles and responsibilities, for this project.
11. Providing a Project Management Plan (PMP). PMP refers to a document that acts as the baseline document, against which the Project Manager can manage deliverables, assess progress, and manage change management issues and ongoing viability questions.
12. Providing a Project Schedule highlighting all deliverables and appropriate milestones, outlining the planned events of the project and milestones.
13. Co-ordinating and managing all implementation activities under defined SOW.
14. Participating in regularly scheduled project review meetings or conference calls, if required. Within five (3) business days, providing Du the details of personnel requiring access to Du/DESC premises.
15. Delivering a monthly project status report to the DESC
16. Acting as the focal point for Change Management Procedure under this SOW

13.2 Assumptions

1. DU may choose to utilize qualified subcontractors.
2. Single point of contact for Technical Lead and Project management will be maintained by both DU and DESC
3. Key stakeholders and decision-makers are available for project discussions, approvals, and feedback throughout the project timeline.
4. During the execution of this project any addition or extension of current scope changes affecting the project schedule and efforts will incur additional charges.
5. Internal Downtime approvals and change management process should be carried out by DESC.
6. Du will provide the Service provider connectivity for the Managed Services Resources to connect to Datacenters for Management and Monitoring.
7. Any changes or parts required extra other than the mentioned BOQ due to scope changes will be considered as additional and will be charged accordingly to DESC

8. Change Management & Approvals – Any major changes to scope, design, or timeline will follow a formal approval process.
9. ITSM, Service Desk and Help desk involved in the project is expected to be provided by DESC. If not the same shall be required to be added in the technical and commercial proposal at addition cost.

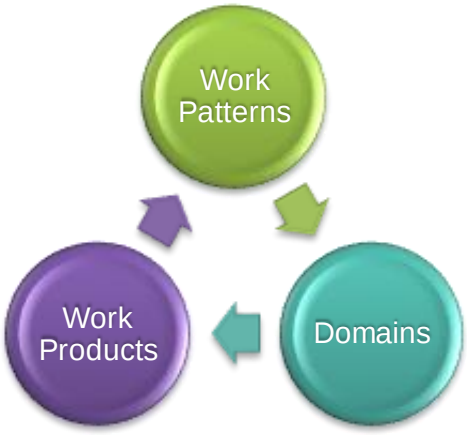
13.3 DESC Responsibilities.

1. The scope of delivering of the 10Gig links carrying tapped/mirrored Internet traffic will fall under the sole responsibility of the two service providers / DESC with each providing 2x10 Gig links each DC.
2. After the Phase-1 when the Data Lake and SIEM would be fully functional and ready to ingest the logs, we are expecting both the service providers (du and E&) to provide us the DNS security logs from their respective PDNS platforms. These logs could be carried over L3 MPLS links as shown in the below network diagram. The delivery scope of these links would be exclusively under the responsibility of the services providers / DESC.
3. DESC would be responsible to provide the GIN network connectivity in both the datacenters for the DNS traffic and the private connectivity to DESC network.
4. The Onsite facility to operate and manage the entire solution not limiting but includes physical access to the resources , laptop , local internet connectivity, phone connections, monitoring screens and seating spaces for the resource would be sole responsibility of DESC.
5. Any third-party software licenses outside of SOW, will be under the DESC responsibility.
6. All the correspondence and communication with the service providers (du and E&) would be governed and coordinated by DESC directly. DESC would be instructing both the service providers (du and E&) for the entire scope which is supposed to be fulfilled by each of the service providers directly.

7. All the correspondence and communication with the service providers (du and E&) would be governed and coordinated by DESC directly.
8. DESC would be instructing both the service providers (du and E&) for the entire scope which is supposed to be fulfilled by each of the service providers directly. A binding directive to UAE service providers (du and Etisalat/E&) to enable Protective DNS security on all DNS traffic from Dubai-based government departments and entities.
9. Service providers, as incumbent public DNS providers, will filter malicious queries and provide copies of DNS traffic logs (request/response) to DESC from their respective networks.
10. DESC will issue a directive to UAE service providers (du and Etisalat/E&) to provide copies of Internet traffic from all Dubai-based government departments and entities, captured at two distinct network positions with detailed operational specifications for the below in Phase 2.
    a. Internet Core Capture
    b. Access Switch Mirroring
11. DESC shall liaise with both service provider to implement DNS traffic redirection at respective service providers.
12. IP Address Provision: DESC will provide service providers with the Anycast IP address of the PDNS stack (e.g., a single routable IPv4/IPv6 address, to be finalized by the bidder), which will serve as the new destination for all government DNS queries.
13. Government Entity Identification: DESC will supply an updated list of government departments and entities, including their public IP prefixes (e.g., IPv4 or IPv6 blocks) and known source subnets, to ensure accurate traffic scoping and filtering by providers.
14. Redirection Validation: DESC will collaborate with service providers to conduct pre-deployment testing, sending test DNS queries from government subnets (e.g., via nslookup or dig) to verify redirection to the PDNS IP, confirming no traffic reaches original provider DNS resolvers' post-cutover.

15. Timeline Coordination: DESC will establish a cutover window (e.g., 48-hour period) with providers, ensuring minimal disruption to government DNS services, and provide a 24/7 escalation contact for real-time issue resolution during redirection.

13.4 Project Management Approach



DU adopts the IBM Worldwide Project Management Method (WWPMM) which an implementation of the Project Management Institute (PMI) PMBOK framework that defines how projects are managed throughout delivery. The methods that comprise WWPMM are based on decades of experience derived from many different types of projects in a variety of constituencies.

It is the project manager's responsibility to tailor the project management (PM) methods, within the constraints of the PM policy, to suit each particular project.

- **PM Domains** provide detailed guidance on how specific types of project management activities are carried out.
- **PM Work Patterns** are a series of steps designed to meet particular project management goals or in response to particular project management situations.
- **PM Work Products** are the verifiable outcomes that are used to manage projects. Under every PM Domain there's a tailored set of outcomes of work products.

13.4.1 PM Domains

- Change management
- Communications management

- Deliverables management
- Event management
- Human resource management
- Project definition
- Quality management
- Risk management
- Supplier management
- Tracking and control
- Technical environment management
- Work plan management

13.4.2 PM Work Patterns Groups

- Defining
- Planning
- Starting
- Monitoring
- Handling exceptions
- Handling deliveries
- Closing

13.5 Risk Management Approach

Risk Management is a key success factor in delivering the project. Risk is defined as the degree of uncertainty relating to the achievement of the planned outputs or the possibility of an unplanned or unsatisfactory outcome. The word 'possibility' implies a probability level; while the word 'unsatisfactory' implies a measure of 'loss' to someone. Risk must be managed by applying a conscientious effort to their reduction or elimination. Not all risks need to be eliminated entirely; often it is sufficient to reduce the project's exposure to a level that is acceptable to the project and at other times it could be desirable to increase the project's exposure to certain risks. Risk Management costs time and effort, but the rewards can be significant.

Risk Management will be practiced at all levels in the project using the suggested process and documentation as set out in this document. The Project team will apply a risk management approach based on the following principles.

- All team members assist in identifying risks.
- Each identified risk is primarily evaluated in terms of its various probabilities (rated on a scale of Low, Medium and High) of occurrence and its resulting impact (rated on a scale of Low, Medium and High), by the originator.
- Mitigation strategies are devised for all risks, by the team.
- All risks will be categorized.
- All risks are entered into the project risk register by the Project Manager.
- The risk exposures are calculated for all risks of a high probability and high impact nature, medium probability and high impact nature and high probability and medium impact nature. Other specific risks may be quantified at the discretion of the Project Manager and the Project Sponsor. These resultant exposures are used to prioritize risks response.
- All risks with an exposure of 100% will escalated to the Project Sponsor.
- All team members will assist in suggesting solutions to optimize the risk portfolio.
- Individual comprehensive mitigation plans will be developed for the highest priority (H,H, M.H, H.M) risks to manage their outcome.
- Plans consist of specific actions to be taken by specific individuals within specific time frames.
- Progress is monitored and adjusted as and when necessary.
- As actions are performed, the risk exposure changes, so the priorities continually change.

13.6 Issues Management Approach

The Issue Management process (in WWPMM it's known as Event Management) is fundamental to the successful delivery of the project/ project. The Issue Management process ensures that each issue/problem identified within the project environment is documented, prioritized and resolved within an appropriate timescale.

Event management domain includes the processes used to:

- Resolve the issues that arise during the course of the project.
- Analyze particular situations that are causing concern.
- Handle compliance incidents.
- Manage the completion of actions.

13.6.1 Change, Scope, Time and Cost Management Approach

All scope changes will be reflected in the updated project plan. Re-baseline will only occur after the Sponsor has approved changes.

The Change register will form Part of the Project Library. Change Requests Forms will be managed and kept by the project Manager who will maintain the Change Register.

13.6.2 Communications and Control Approach

Sharing information regarding progress, issues and risks are considered crucial for the successful delivery of this project. All team members are expected to communicate project progress, issues and risks in a timely fashion using the Enterprise Project Management solution (DU EPM Solution) and communications to external stakeholder are expected to be carried out through the project manager.

13.6.3 Meetings:

The following meetings will be setup for this project:

- "Project Team meeting "meeting in which the discussion will be focused on the following topics: daily progress for each sub-project against schedule, open issues update, open project risks, scheduled leave by project team members...etc. This meeting will be scheduled in a weekly basis and will involve project manager from DESC and du.
- "Project Management meeting" meeting in which the discussion will be focused on the following topics: project progress against schedule, open issues update, open project risks. This meeting will be scheduled in a bi-weekly basis and will involve parties from Project Manager and Customer.
- "Project Steering Committee" meeting in which the discussion will be focused on the following topics: high level progress of the project, high Priority open issues, open project risks with high

probability & impact. This meeting will be scheduled in a Monthly basis and should involve executives from Customer and stakeholders.

Meeting minutes will be sent after every meeting to all attendees with all decisions made.

If no comments are received on the minutes of meetings within two days, then minutes of meetings will be considered approved.

Outside of the standing weekly meetings, project team members may call for a meeting to discuss project related matters or issues.

13.7 Quality Management Approach

It remains the responsibility of DU to lay down the quality measuring criteria for the entire project. However, as this information is not available at this stage, Project quality is based on Customer understanding of the quality requirements. Should the criteria to be supplied by DU invalidate the assumption made at this time, project scope time and cost could be adversely affected.

The quality process will include some or all of the following activities: -

- Peer review on deliverables (DU)
- Quality reviews on documents and implementation services (du and DESC).
- Quality walkthroughs (du and DESC).
- User Acceptance Testing (du and DESC).).

Document Review and Acceptance

For all documents requiring review the following rules shall apply.

- Before work is started on any document, the Project Sponsor or his delegate shall approve the template of that document.
- Documents shall be handed to Customer accompanied by a delivery letter/note by which Customer's Project Manager shall accept the delivery.
- A four working day period is allocated for Customer & project stakeholders to review the document.
- A review meeting, to be arranged by the client Project Manager, is to be set up on the fifth working day after the document has been delivered if requested by project sponsor.

- The project sponsor comments will be delivered to Project Management during that session.
- Approval of any document will only be considered valid after it has been signed by the Project Sponsor.

Acceptance and Authorization

- All due dates for delivery of deliverables and for project authorizations shall be clearly indicated on the sub project schedules.
- No formalized notification of the delivery or of the authorization requirement will be issued.
- Should the due dates be required to change, the Project Manager shall formally notify Customer of the required change as part of the weekly project Consultant Meeting.
- All Deliverables will be delivered with a formal delivery notification, which must be signed by Customer Project Manager in acceptance of the delivery.
- All required project authorization points shall be indicated on the sub-Project Plans.
- The specific authorization will be expected on the day reflected by the project plan.
- Only the Project Sponsor is able to provide project authorization.

13.8 Document Management Approach

13.8.1 General

A general project documentation procedure is hereby issued to all parties and stakeholders on the project. The project team will ensure that all documents are regularized according to this procedure. Within the Project team, the Project Manager will be the document custodian for all version releases and updates.

The Project Manager will control the Project Document Number series. Every document shall therefore conform to this template. Hard Copy handling and Soft Copy handling shall be as detailed below. All project documentation shall be in English. All Project Communication shall be in English only.

13.8.2 Document number structure

The following structure beginning with the prefix (Project Code) "PROJ-CODE" with the '-' slash separator shall be maintained.

This Prefix must then be followed by the abbreviation of the document name, e.g. Scope of Work (SOW), followed by slash.

The creation date shall then form part of the document number in the format (YYYY)(MM)(DD).

13.8.3 Revision Control

- The revision control shall be achieved by applying the following rules;
- Each Time the Document is revised/changed it shall be given a new revision number. This number shall appear in the footer of each page of the document.
- The revision number shall comprise of as a minimum three numeric digits separated by a full stop (.) between the first and second digit.
- The first digit shall reflect the status of the document. Digit 1 = yet to be approved. Digit >1 = approved

13.8.4 Handling

- All documents must, directly after the table of content, include a table of the document's history that shows all the changes done to the document, a table listing all reviewers and the dates of their reviews and a table to indicate the distribution of the document.
- Until Handover, all documents shall be under the control of the Project Manager.
- The Project Library shall consist of an electronic copy of the documents located on the Project server at the DU premises.
- All documents shall be presented to the Project Manager in the form of an electronic copy, or in the case of a document bearing signatures, in the form of both the original signed document and an electronic copy thereof.
- The Project Manager shall be given read and write access to the Project Library. All other project Participants shall only be given read access to this library.

13.8.5 Hard Copies

With the exception of the latest hard copy of signed documents in the folders with the DU project manager, all hard copies of any project documentation are regarded as obsolete and are to be used for reference purposes only.

13.8.6 Electronic Copies

- With the exception of the Latest Electronic Copy of any document in the Project Library all other copies shall be regarded as obsolete and for reference purposes only.
- Any Documents not yet appearing on the Project library will not be considered for contractual, planning or any other purposes. All Contractors shall comply with this procedure. Al documents on the Library shall be named by the document reference number followed by the date of insertion into the library in the format YYMMDD.

13.8.7 Project Management Deliverables

- Project Plans (Communications, Quality, Risk, Change and Scope) management plans
- Weekly status report and meeting minutes
- Project closure report

13.9 Project Implementation Timelines

Task Name	Duration	Start	Finish	Resource Names
DNS & Internet Security & Observability	735 days	Thu 1/1/26	Wed 10/25/28	
Sign Contract	1 day	Thu 1/1/26	Thu 1/1/26	
Issue LPO	1 day	Thu 1/1/26	Thu 1/1/26	
Phase 0: NETWORK AND SECURITY INFRASTRUCTURE DEPLOYMENT	60 days	Fri 1/2/26	Thu 3/26/26	
Delivery Lead Time	3 mons	Fri 1/2/26	Thu 3/26/26	
Datacenter Infrastructure	3 mons	Fri 1/2/26	Thu 3/26/26	DU
Network Fabric Deployment	3 mons	Fri 1/2/26	Thu 3/26/26	DU
Perimeter Security Infrastructure	3 mons	Fri 1/2/26	Thu 3/26/26	DU
Phase 1: DNS SECURITY ENFORCEMENT AND DATA INGESTION FOUNDATION	60 days	Wed 4/1/26	Tue 6/23/26	
DNS Security Directive	3 mons	Wed 4/1/26	Tue 6/23/26	DESC
Data Aggregation/Ingestion Layer	3 mons	Wed 4/1/26	Tue 6/23/26	DU
Data Lake Deployment	3 mons	Wed 4/1/26	Tue 6/23/26	DU
Threat Intelligence Platform	3 mons	Wed 4/1/26	Tue 6/23/26	Du

Analytics and Monitoring Stack	3 mons	Wed 4/1/26	Tue 6/23/26	DU
Phase 2: INTERNET TRAFFIC COLLECTION, INGESTION OF LARGE DATA SETS IN DATA LAKE AND ENHANCED ANALYTICS USING INTERNET ORIENTED SECURITY USE CASES	60 days	Wed 7/1/26	Tue 9/22/26	
Internet Traffic Capture Directive	3 mons	Wed 7/1/26	Tue 9/22/26	DESC
Data Aggregation/Ingestion Layer Enhancement	3 mons	Wed 7/1/26	Tue 9/22/26	DU
Data Lake Expansion	3 mons	Wed 7/1/26	Tue 9/22/26	DU
Analytics and Monitoring Stack Enhancement	3 mons	Wed 7/1/26	Tue 9/22/26	DU
Threat Intelligence Platform Enhancement	3 mons	Wed 7/1/26	Tue 9/22/26	Du
Phase 3: PROTECTIVE DNS STACK IMPLEMENTATION	60 days	Thu 10/1/26	Wed 12/23/26	
Protective DNS Stack Implementation	3 mons	Thu 10/1/26	Wed 12/23/26	DU
DNS Traffic Redirection Directive	3 mons	Thu 10/1/26	Wed 12/23/26	DESC
DNS Traffic Redirection Implementation	3 mons	Thu 10/1/26	Wed 12/23/26	Service Provider Du & Etisalat

Operate & maintain	540 days	Thu 10/1/26	Wed 10/25/28	
Perform daily operations, maintenance, and management tasks	27 mons	Thu 10/1/26	Wed 10/25/28	DU

13.10 Delivery Lead Times

13.10.1 Hardware

- Infrastructure, Network & Security - 8 Weeks

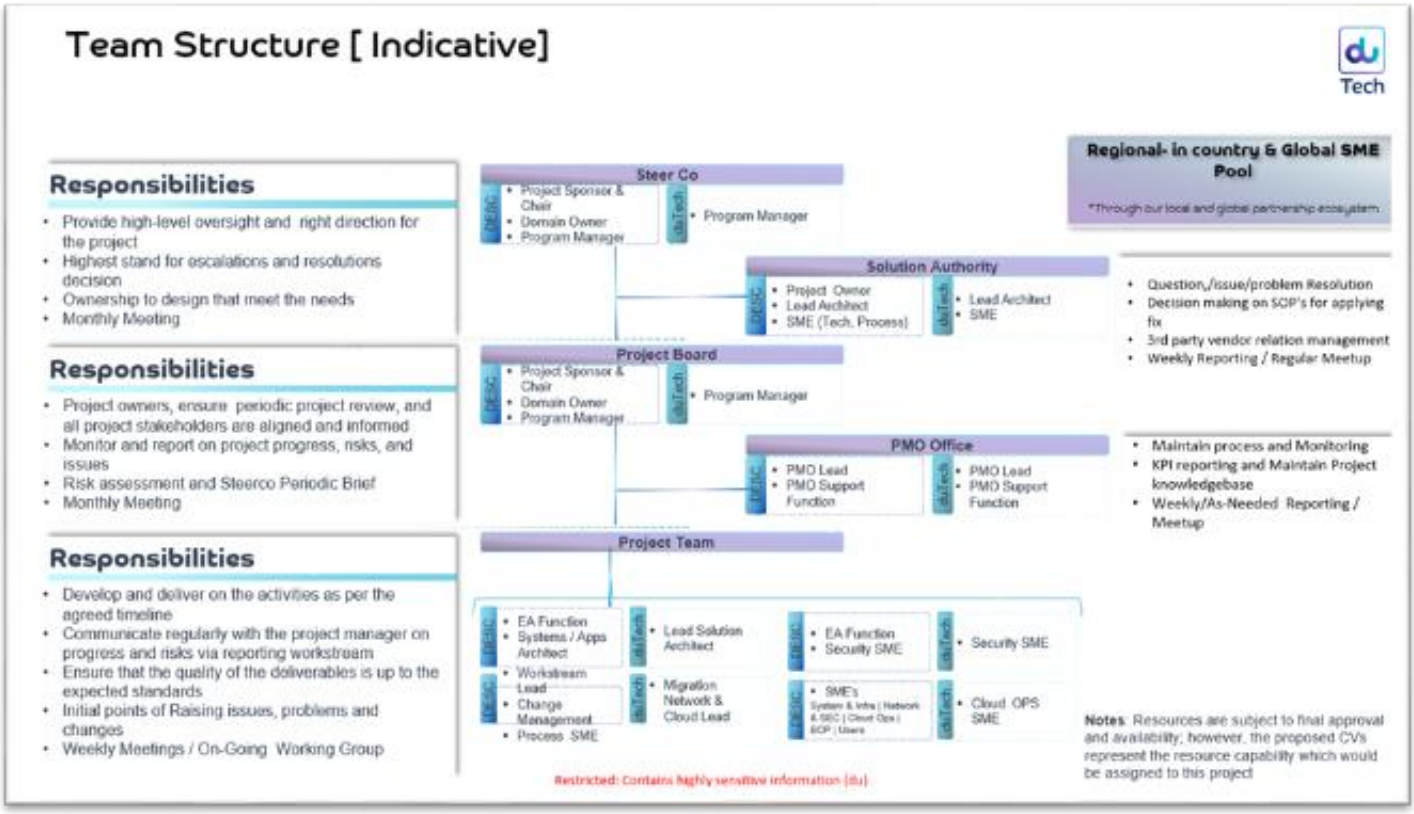
13.10.2 Software

- Software Licenses - 2 Weeks

13.10.3 Team Mobilization

- Resource Mobilization - 4 Weeks

13.11 Project Team Structure

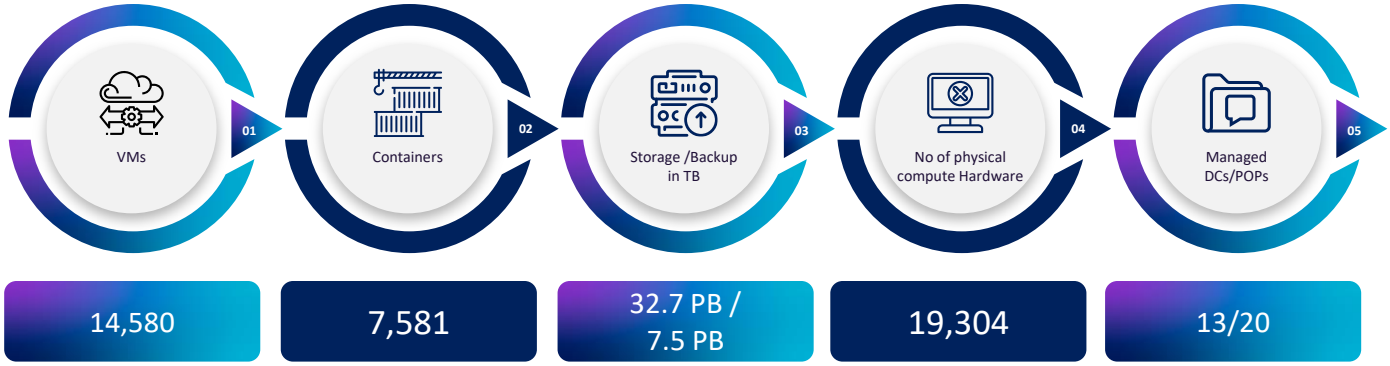


13.12 Resource Profiles

S.No	Resource Roles	Resource CV's
1.	L1 Analyst (SOC Operator)	Du Response - RFQ 762640 - 13.11 Resource Profiles
2.	SOC Shift Lead	Du Response - RFQ 762640 - 13.11 Resource Profiles
3.	Automation Engineer	Du Response - RFQ 762640 - 13.11 Resource Profiles
4.	Process Compliance Manager	Du Response - RFQ 762640 - 13.11 Resource Profiles
5.	SDM	Du Response - RFQ 762640 - 13.11 Resource Profiles
6.	Service Performance Lead	Du Response - RFQ 762640 - 13.11 Resource Profiles
7.	Administrator - Network System Cloud	Du Response - RFQ 762640 - 13.11 Resource Profiles
8.	Threat Detection Hunter	Du Response - RFQ 762640 - 13.11 Resource Profiles
9.	ITSM Engineer	Du Response - RFQ 762640 - 13.11 Resource Profiles

14. Customer References

Trusted by 130+ customers, du delivers seamless cloud management across platforms like FedNet, Dubai Pulse, and Enterprise Cloud—powering the digital backbone of the UAE



References/Case Studies # 1: Commercial Bank of Dubai

du, with its strategic partner HPE, builds cloud and as-a-service solutions to form the foundation of its private cloud environment. These critical solutions are hosted within du's state-of-the-art Tier III-certified data centers, leveraging du's robust connectivity, hosting, and advanced network security services. The Commercial Bank of Dubai's private cloud contract with du (and HPE) is a strategic move

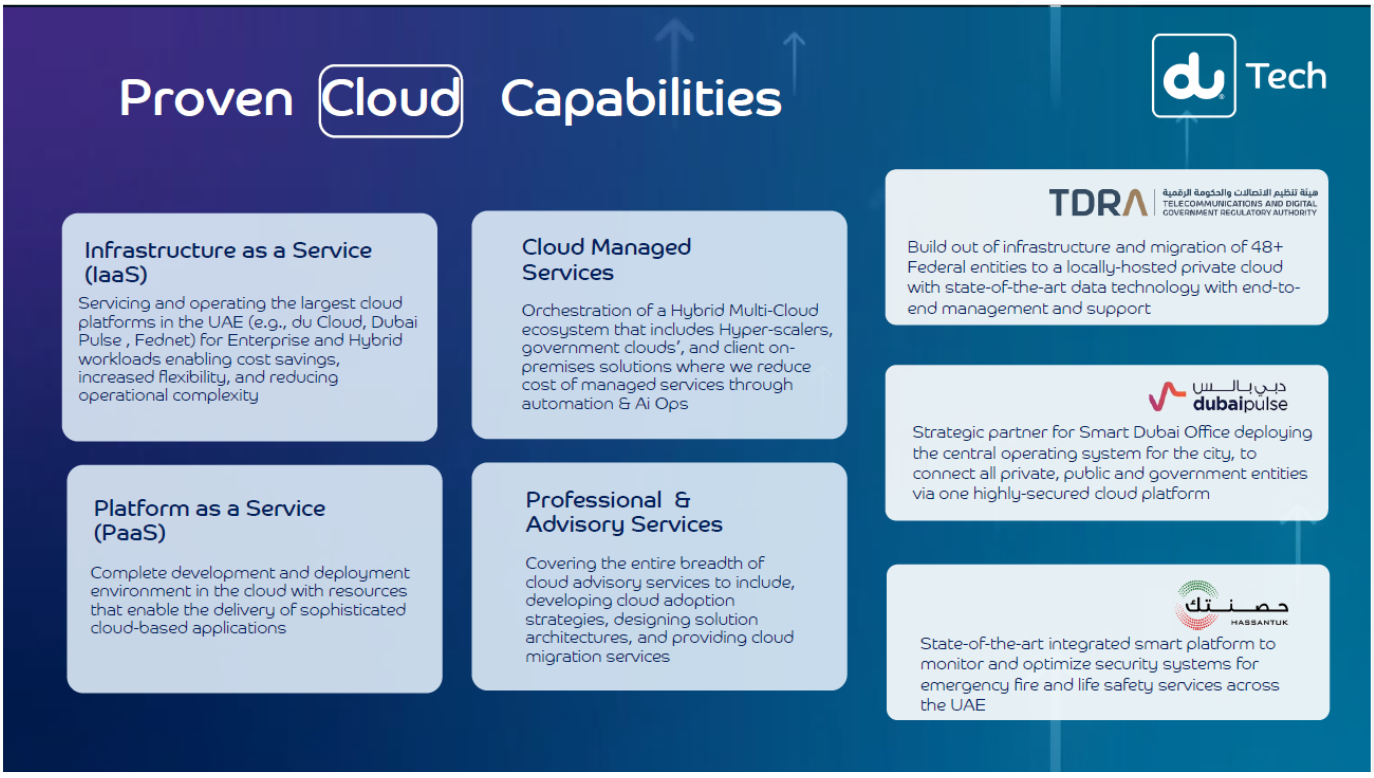
to modernize its IT infrastructure, enhance digital services, and ensure robust security and compliance through a hybrid cloud model, ultimately aiming to improve customer experience and operational efficiency. Commercial Bank of Dubai (CBD), one of the leading national banks in the UAE, forms a strategic collaboration with du, from Emirates Integrated Telecommunications Company (EITC), and Hewlett Packard Enterprise (HPE) to significantly accelerate its hybrid cloud journey and enhance its digital banking services. The collaboration aimed to establish a more efficient and automated self-service IT operational model for CBD, which is a key component of the bank's ambitious five-year strategy. This will lead to enhanced responsiveness, greater visibility, and improved control over IT operations, while minimizing complexities and manual processes. 1600+ Workloads

Project duration – DC Exit planned from 12 to 18 Months from the date of initiation.

Specific role and responsibilities. DU has been appointed as the prime partner and has assumed responsibility for building and managing CBD Sovereign Private Cloud platform and its operations.

- The platform is hosted in du Data Centers which are certified with optimum uptime - Uptime Tier 3+ 99.9 | ISO 27001 (Infra & IT Security) | PCI DSS (payment Data Security) | OHSAS 18001 (Health & Safety) | ISO 22301 (BS continuity management) | ISO 9001(Quality management) | ISO 14001(Environmental management).
- CBD aimed to attain accreditation and compliance such as s, SOC 1 Type I and SOC 2 Type II, ISO 27017, PCI DSS, NESA, which are the basis for compliance to Central Bank Policy and Regulations and DR-BCP guidelines.
- It provides a unified, automated control plane across both CBD's private and public cloud environments, ensuring seamless management of core banking applications and workloads
- The private cloud infrastructure, combined with du's comprehensive data center solutions and managed services, has bolster CBD's security posture, safeguarding sensitive financial information and customer data in full compliance with regulatory standards.
- The new environment is designed to incorporate advanced AI capabilities and tailored services, enabling CBD to rapidly develop and deploy AI-driven solutions that meet evolving business needs and customer expectations
- The new stack facilitates task automation, drives innovation, and optimizes operational efficiency, contributing to a more agile and resilient banking infrastructure.
- The solution is supported by HPE Services for migration, Zerto for VM migration and cyber resilience, and HPE Aruba Networking's intelligent edge solutions (including Wi-Fi 6E and Network Access Control) for secure and efficient connectivity.

Reference 2 & 3 : TDRA and Dubai Pulse



Other Customers

15. Technical Attachments and Annexures :

- Attachment - Du Response - RFQ 762640 - 8.6 - Technical Data Sheet
- Attachment - Du Response - RFQ 762640 - 12.0 Hardware support maintenance
- Attachment - 13.8 Project plan
- Attachment - Du Response - RFQ 762640 - 13.11 Resource Profiles

16. Company Profile

16.1 Company Profile EITC (du)

EITC is an integrated telecom & ICT service provider, dedicated to providing customers the best in choice quality and innovative services. Based in UAE, our commitment to the country extends beyond mere communications services as we strive to contribute towards a positive national transformation in both the Emirates' people and environment.

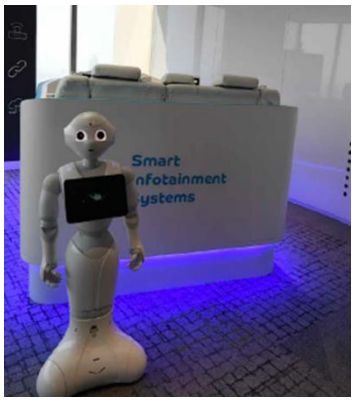
du is dedicated to provide customers the best in choice, quality, innovation and pricing. Based in the UAE, our commitment to the country extends beyond mere communications services as we strive to contribute towards a positive national transformation in both the Emirates' people and environment. We're pretty versatile. Our services include fixed and mobile telephony, broadband connectivity and IPTV services, which we offer to individuals, homes and businesses. We have been in to ICT Services area serving enterprise customers for their raising IT requirements adapting continues change in the IT Environments.

The du tech Division is a new division rising from the integration of Enterprise Telco and ICT Solutions. The ongoing desire for greater efficiencies plus the competitive advantage of offering one full suite of telco and ICT solutions for our clients were the motivation behind this organizational realignment in 2020. Our focus during the year is on advances in the areas of Enterprise Networks, Cloud services, Data Security, Data Centre Services, Managed Services, Smart City Services, Internet of Things (IoT), Data Science, Blockchain, Platform as a Service, and Artificial Intelligence (AI). We've also created the Idea Hub at our head office to showcase solutions to our clients and gather learnings, and continue to build partnerships with global tech companies to maintain our obligation to provide UAE business with best-in-class solutions.

We have established and grown a wide range of successful and evolving partnerships between Enterprise ICT Solutions and the UAE government and private sector. However, our contribution to the UAE Society is even broader than this. The following initiatives are just some examples of the desire and capability of EITC to enhance its growing stature as a national asset.

- **Dubai Pulse** is already being referred to as the new digital backbone of Dubai. We have been appointed as the strategic partner with Smart Dubai Office and have assumed responsibility for building its operating system, the aforementioned Dubai Pulse. Simply, it will connect all private, public and government entities in one unbreachable, secure location. It is so-named because at one touch, any information about Dubai can be obtained. This technological coupling of city services, IoT, cloud services and Big Data

- **Dubai Silicon Park** is the first Smart District in the UAE. To achieve such a distinction, the integration process to marry technology to every aspect of business and personal life in an advanced, yet eco-friendly community was both ambitious and incalculable a few years ago. We are the master systems integrator for the district, ensuring that Dubai Silicon Park is a functioning, fault-free model of a boldly-envisioned future for the UAE.
- **National Customer Relationship Management (NCRM) Platform:** NCRM is another initiative in which du is playing a major role with the TRA. It consists of creating a CRM platform that will integrate all federal authorities in the UAE. This will act as a one stop platform for all federal entities.
- **Hassantuk** is a cutting-edge building safety solution protecting lives and properties across the UAE through the Alarm Receiving Centre (ARC) operators who verify if an alarm is genuine or false in less than 120 seconds. This ensures that any emergency services respond to genuine fire and life safety events and are not dispatched to false or maintenance alarms. Ministry of Interior initiative to enhance public safety and life safety operations awarded to Injazat and sub-contracted to eitc to cover buildings across UAE.
- **Our digital transformation journey began by looking at ourselves:** EITC launched a dedicated Digital Lifestyle & Innovation Division in 2018, which is a key driver and enabler of the holistic digital transformation that began in 2017 and will continue to set the pace of change moving forward.

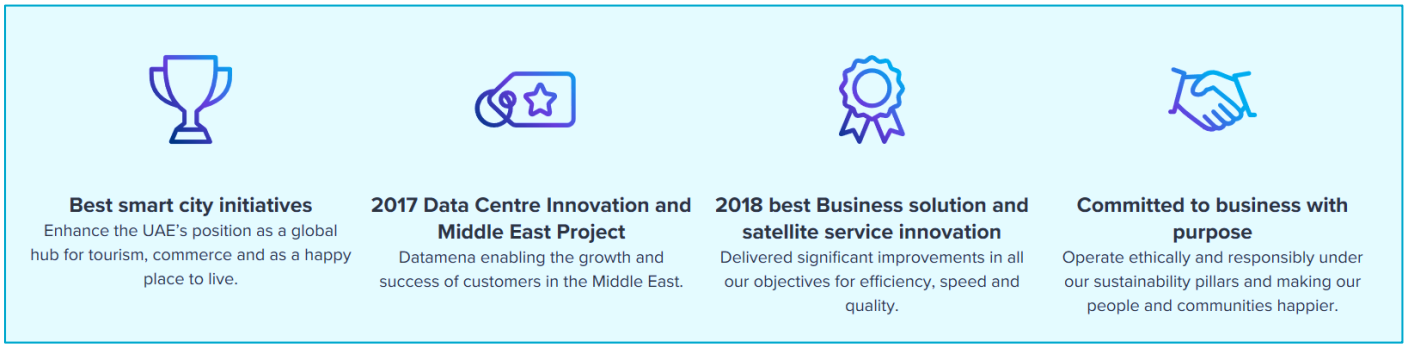


- We are using **robotics** to automate around 200 processes across the entire organisation, enabling a more efficient way of working.
- **WiFi UAE,** a nationwide free Wi-Fi project designed to boost the take-up of e-government services, is being rolled out by EITC – an official Dubai Smart City Platform WiFi provider. EITC's 'freemium' proposition enables Government's Dubai Smart City Platform services whilst catering for user expectations and different use cases. Currently EITC supports over 200 hotspots, including significant locations such as malls, transportation systems and key public sites, both indoors and outdoors.
- **Datamena connectivity hub and an exchange marketplace** for service providers that simplifies business for carriers, operators and content providers by consolidating infrastructure and reducing IP costs. Today Datamena acts as a growth accelerator for digital businesses both in the UAE and the Gulf region.
- **Blockchain Platform as a Service (BPaaS):** Playing a leading role to meet and support the UAE Blockchain Strategy, du has launched an initiative to build the first Blockchain Platform as a Service (BPaaS) in the UAE, to improve the everyday life of the citizens of Dubai and acknowledge the Government of Dubai's pioneering blockchain vision. Document attestation facilitates and automates governmental entities' processing of attesting documents and Patient Safety validates medicines and vaccines before use.

- The roll-out of 5G and expansion of IoT are assisting us to realise the dream of Dubai as a single organism whose every, and only, function is to serve its citizens. The transformation of Dubai to a community where buildings, car parks, hospitals, street lights, roads, even bus schedules are infused with smart technology – ensuring safety, convenience, economy and environmental benefits stands as one of the proudest achievements in our 12-year history.

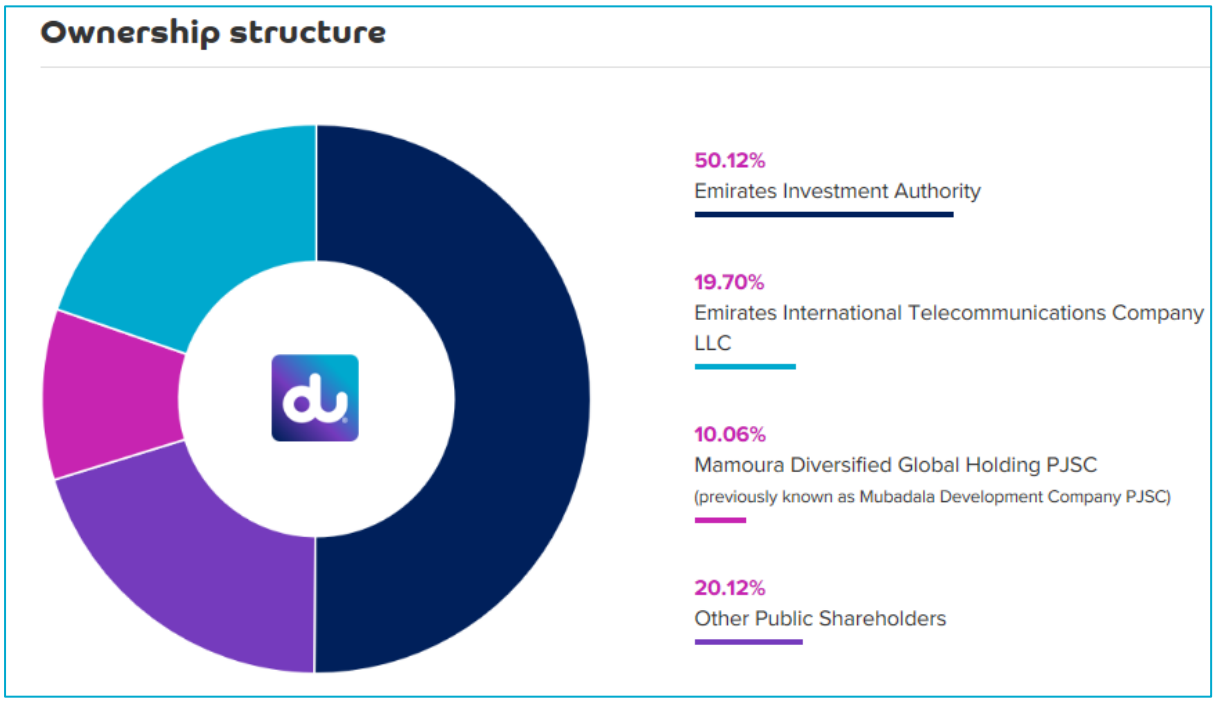
We are proud of the recognition and acknowledgment we've received from the local and regional telecommunications industry, our partners and our clients.

With our total revenue of AED 12.5 Billion and 2000+ employees on-board we are committed to continuously provide the services to the delight of our customers.



16.2 Ownership & Organization Structure

du is owned by stable and strong local entities with well-known and strong presence in UAE business market. Such strong stability of ownership differentiates du from other smaller competitors in the market, and ensures reliability. du is owned by the following entities:



16.3 Company General Data

S no	Data	Details
1.0	Full Name & Address	Emirates Integrated Telecommunications Company PJSC. Dubai Hills Business Park, P.O.Box 502666, Dubai, U.A.E.
1.1	Website	http://www.du.ae
1.2	Office Telephone No	+971 (4) 4346898
1.3	Email Address	supplier.management@du.ae
1.4	Office Fax No	+971 (4) 360 4440
2	**About Us**	
2.1	The total number of years the vendor has been in business and, if applicable, the number of years under the present business name.	Emirates Integrated Telecommunications Company opened for business in 2006 and commercially rebranded as du in February 2007.
2.2	Financial strength and maturity of the Bidder	All du financial reports, including profit/loss, assets/liabilities, and other means of financial reporting are available for public in the following link: https://www.du.ae/about-us/investor-relations/reports Financial highlights for the last 5 years is provided in below figure from du's Annual report 2024.

Table 1: Company General Data

16.4 Financial report

Our vision

To enhance your life, anytime, anywhere.

Our mission

We want to delight our customers, be the employer of choice for the best talent, create optimal value for our shareholders through business excellence and innovation, and proudly contribute to the transformation of our community.
We work to deliver our vision by using our talent, skills and energies to connect, inspire and reward all we touch, every day.

Our values

We are Confident, Friendly, Honest, and Surprising, and our values guide our actions.

From inception of our business in 2006, we have worked hard to enhance and expand our services in an industry that is at the heart of economic and social transformation. Our aim is to bring people and businesses together in what we do best, by offering mobile and fixed services, broadband connectivity and IPTV services to people, homes and businesses all over the UAE. We are building telecommunication company by taking connectivity to the next level to fit the future and the people need because our customer will always be our main focus. Therefore, we are providing carrier services, a data hub, internet exchange facilities and satellite service for broadcasters.

Below is the link for 2024 financial report;

https://www.du.ae/about-us/investor-relations/disclosures-and-reports

وتحيا بها الحياة

add life to life