Citizens Bank®

Cloud Security Reference Architecture

Security Engineering & Architecture (SEA)

Author: Chris Elomaa

Contributors: Eric Parker, Ram Eati, Garrett Bontempo, Peter Gries, Charles Fletcher, Chris Choquette, Ginny Palmer, Mark Thompson, Randy Simmons, Ben Jackson, Jed Tanner, Fernando Calle, John Hart, Sabrina Viscomi

2/1/2021 - v1.10

Use of Cloud Service Providers (CSPs)

Cloud Service Providers (CSPs) provide a cloud services platform offering computing power, database storage, content delivery, and other functionality to help businesses scale and grow.

Some of the benefits offered by CSPs include:

- Speed to innovate / Speed to market
- Fail fast (and cheap)
- Consumption based model – pay only for what you use
- Scalability
- Next generation tools and services
- Simplicity of automation
- Resiliency and Redundancy – built-in

Establishing Security in the Cloud Environment

The many benefits of CSPs makes them an attractive solution and the use of them will only continue to grow. While many CSPs offer native security capabilities, it is important to understand the risk exposure associated with CSPs and ensure CFG takes the appropriate measures in augmenting those capabilities to secure the cloud environment.

CFG Cloud Strategy

Cloud First

Prioritize delivering IT services using the cloud computing model. Use traditional technology delivery model as an exception. (CFG has also adopted a SaaS First guiding principle.)

Hybrid Cloud

Adopt hybrid cloud services from both a service model and a deployment model perspective.

Risk Based Adoption

Use risk as a key factor to determine the type of cloud (Public, Private, SaaS, etc.) that should be adopted to meet a particular business need.

Multi-Vendor Cloud

Source cloud services from a variety of providers whenever feasible to avoid vendor lock in and take advantage of SaaS model.

Cloud Service Models*

- IaaS
  - the cloud service model in which the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
- PaaS
  - the cloud service model in which the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- SaaS
  - the cloud service model in which the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

* Definitions from Cloud Security Minimum Requirement(MR)

Cloud Deployment Models*

- Public
  - the cloud computing deployment model in which the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. (typically multi-tenant)
- Private
  - the cloud computing deployment model in which the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on-premise or off-premise. (typically single-tenant)
- Hybrid
  - the cloud computing deployment model in which the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

* Definitions from Cloud Security Minimum Requirement(MR)

Cloud Service & Deployment Models

Four major cloud service deployment models exist today and are utilized by CFG based on balancing business needs with risk exposure.

	CFG Managed
	Cloud Service Provider (CSP) Managed

Security Controls

Data Center	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Application	Application	Application	Application
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
▪ Traditional on-premises data centers resources. ▪ CSP on-premises private cloud implementations have begun such as Oracle (ExaCC) for Oracle RDBMS database hosting and PolyCloud.	▪ Public CSP resources are compartmentalized into Private CFG accounts / subscriptions utilizing services such as AWS Virtual Private Cloud (VPC) or Azure Virtual Networks (vNet).	▪ Public CSP resources are compartmentalized into Private CFG accounts / subscriptions utilizing services such as AWS Virtual Private Cloud (VPC) or Azure Virtual Networks (vNet).	▪ CSP can be either Public (multi-tenant) shared code base with global release upgrade SLA's or Private (single-tenant) CFG specific code base conforming to CSP release upgrade SLA's

Cloud: Historical - High Level Milestone Map

Capabilities built

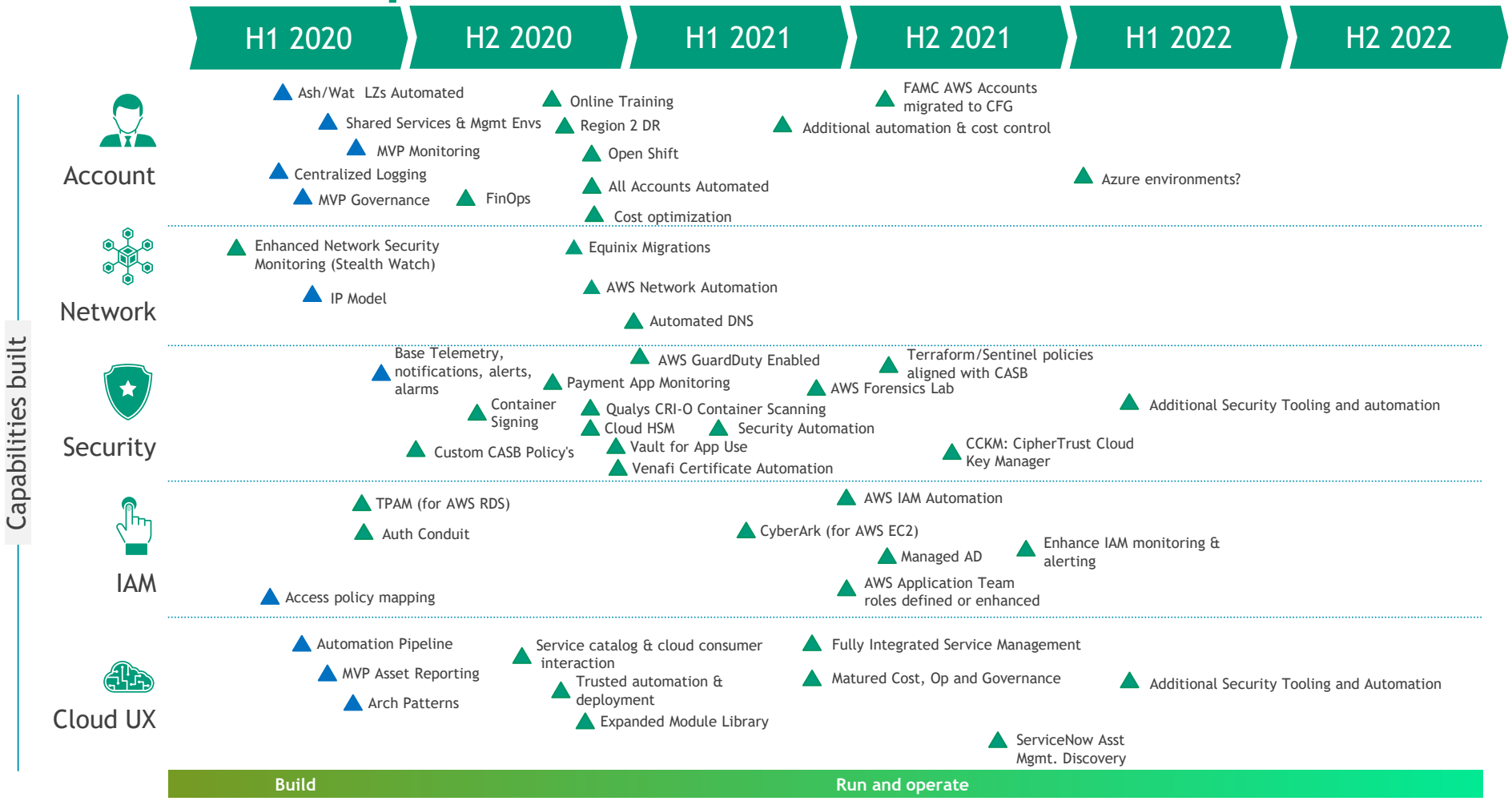
	2017	2018	2019
Account	Create Cloud Strategy Perform Limited Application Cloud Affinity Assessment Select Planning Execution Partner Define Target Operating Model Build Business Case for Phase 2 Build PoC Cloud Foundation	Build public cloud foundation, AWS account structure and env's Establish contract with AWS and other public cloud ecosystem vendors Up-skill talent on AWS/cloud technologies Implement Innovation Lab Establish base Cloud Operating Model and Goverannce	Productionalize AWS Onboard additional applications. Execute JIT app migrations Cloud Cost Management Apptio integration for Cloud transparency Closure of open cloud risks.
Network	Establish IPSec VPN Tunnels to AWS	Establish AT&T NetBond AWS connectivity VPC Design Security Group Model	Next Gen FW (Palo Alto) Enhanced Load Balancing (f5) AWS Transit Gateway
Security	Establish mVision Integration - POC	CASB (mVision) OS Image Hardening Logging & Monitoring (Splunk) Vulnerability Mgmt.(Qualys) Key Mgmt.(Gemalto)	Database Logging & Monitoring (jSonar) HashiCorp Vault (Secrets) Security Requirements (SD Elements)
IAM	Establish Okta Integration - POC	CFG Federated Identity to AWS (Okta) AWS CSP Authorization (SailPoint) AWS Organizations	AWS account mapping AWS CSP base roles defined
Cloud UX	Establish ServiceNow CMP Integration - POC		

Build | Run and operate

△ Completed

Note: activities in H2-2021 through H2-2022, would focus on operating and maintaining the landing zone, thus not separately represented here

Cloud: Current and Future State - High Level Milestone Map



- Functionalities built for Ashburn / Watertown, would need additional build for future app migration
- New functionalities to be built for future app migration

Note: activities in H2-2021 through H2-2022, would focus on operating and maintaining the landing zone, thus not separately represented here

Risk Management Practices

CFG has taken various steps to appropriately secure the cloud environment including the development and continued refinement of policies, standards, and patterns, establishment and regular testing of cloud controls, monthly reporting of cloud security metrics, and issue remediation.

POLICY

- Cloud Security Minimum Requirement(MR)
  - A minimum requirement under the Cybersecurity Policy.
  - Based on Cloud Security Alliance and The Open Group.
  - First published 2017 and revised annually.
  - Update to Procurement Master Software and Services Agreement (MSSA) in Q4 2018.

STANDARDS

- Configuration Standards
  - CFG Hardening Guidelines based on CIS Benchmarks, STIG and vendor best practices.
  - Configuration validation performed by Qualys and McAfee MVISION (CASB).
- Cloud Services Patterns and Standards
  - In-flight list: Being managed by Cloud Consortium.

CONTROLS

- CASB Related Controls
  - BLCID-0020314: Security capabilities are enabled in the cloud monitoring tool when technically feasible, for cloud service providers, associated CFG managed applications, and newly integrated clouds services to identify potential security threats, unauthorized activity, and malicious traffic.
  - BLCID-0020315: The SEA team ensures platform operational integrity for the successful delivery of security event data to application stakeholders and systems. Additionally, the SEA team provides SIEM integration, AWS Security Compliance reports, and support for ad-hoc information requests.

Risk Management Practices (cont.)

METRICS	▪ Cloud Access Security Broker (CASB) Metrics ▪ Cloud Security Dashboard
ISSUE REMEDIATION	▪ Open Issues ❑ OR-01972 CASB Monitoring - Enhancements to CASB monitoring are needed to more effectively identify potential security threats. ❑ OR-01974 AWS monitoring - Enhancements to AWS monitoring are needed to more effectively identify potential security threats. ▪ Closed Issues ❑ OR-08437 Skyhigh CASB Solution is not integrated with Sailpoint for User Entitlement Reviews

Governance Implementation

CFG has established governance practices within existing organizational processes to ensure cloud service providers (CSPs) are appropriately assessed prior to being brought onboard and continuously assessed going forward to ensure compliance with CFG policies and standards.

	Process Owner	Governance Process	Details
Within CS&R	Cyber Security	Information Security Business Impact Assessment (ISBIA)	▪ Validates CSP against Cloud Security Alliance (CSA) – Consensus Assessments Initiative Questionnaire (CAIQ). ▪ Validates Solution Design against CFG - Cloud Security MR.
	SEA (Cyber Storefront)	Security Requirements	▪ Leverage SD Elements to add security requirements early in lifecycle and populated in Jira Town/Neighborhood/PODs
Outside of CS&R	Third Party Vendor Assessment	Vendor Classification Profile (VCP)	▪ Risk scoring in GRC updated in Q1 2019 with Cloud questions such as Service Model (SaaS, PaaS, IaaS), Deployment Models (Public, Private, Hybrid), Single Tenant / Multi Tenant, 4th party (identify where SaaS vendors services run from AWS, Azure, etc.).
		Vendor Assurance	▪ Onsite visit or paper based assessments incorporating cloud specific controls from Cloud Security Alliance (CSA) - Cloud Controls Matrix (CCM).
	Procurement	Master Software and Services Agreement (MSSA)	▪ Exhibit B – Section 1.g : Added Cloud Security MR specific content not already contained elsewhere in the MSSA.
	Enterprise Architecture	Architecture Review Board (ARB)	▪ Ensure that solution architecture and designs are in alignment with policy and standards (e.g. authentication, multiple geographic regions defined if required, single or multi tenancy design impacts).

Cloud Security Principles

- Identity and Access Management least privileged roles and polices
- Encryption-at-rest with Customer Managed Keys (CMK) based on Data Classification
- Encryption-in-motion with CFG Managed certificates
- Database Logging and Monitoring for GLBA/SOX/Payment systems
- CFG Hardening Standard deployments and monitoring
- Service governance for IaaS/PaaS (AWS Organizations, Azure Mgmt Groups)
- CSP logging and monitoring for all IaaS/PaaS API and network traffic flows
- Integration with enterprise security system
- Integration with enterprise Information Technology Service Management (ITSM)

Cloud Security: Tools in the Toolbox

- Okta
  - Federated integration with CFG Active Directory providing Single Sign On and Multi Factor Authentication capabilities.
- mVision
  - Cloud Access Security Broker (CASB) providing Shadow IT, Configuration Audit, DLP and User Activity monitoring for select cloud services
- Qualys
  - Threat and Vulnerability Mgmt providing Port Scanning, host based scanning, IaaS CSP integrations and container/registry security
- Splunk
  - Cloud and on-prem logging and monitoring
- SailPoint
  - Centralized access requests, provisioning / de-provisioning, and access review certifications
- Azure Active Directory
  - Selective sync of CFG Active Directory objects
- Stealth Watch
  - Security analysis and threat detection for network activity through VPC flow log analysis.
- ForcePoint
  - Web proxy providing filter and DLP inspection based on
- Active Roles Server (ARS)
  - Management of Active Directory objects and select cloud provider objects
- Active Directory
  - Enterprise directory store containing CFG user credentials / entitlements, groups, and computer objects
- Key Management
  - KeySecure appliance on-prem and in the cloud
  - AWS Cloud HSM
- Venafi
  - End to end Certificate Mgmt and integration with Certificate Authorities
- HashiCorp – TerraForm, Vault, Consul
  - Terraform Sentinel for Infrastructure as Code (IaC) policy enforcement
  - Vault for dynamic secrets management
  - Microsoft PKI
- ServiceNow
  - Information Technology Service Management (ITSM)
  - IaaS/PaaS Asset Mgmt, Cloud Mgmt Platform planned (H2'2020)
- CyberArk
  - Strategic - Enterprise password vault for privileged identities with check-out/check-workflow and password rotation
- TPAM
  - Legacy - Enterprise password vault for privileged identities with check-out/check-workflow and password rotation

Scope for AWS

Design and build the foundational elements of public cloud in AWS as part of Digital transformation.

- Enabling approximately twenty AWS services in landing zones.
- Create environments for Production, P-1 (QA / Pre-prod), and P-2 (Dev/SIT) as well as the supporting accounts – Shared Services, Security Services, Logging, SSO.
- Establish the base network connectivity to AWS.
- Ensure appropriate cloud security by implementing or integrating with key security tools: Okta, Splunk, mVision, Gemalto, and Sailpoint.
- Enable use of containers, automated provisioning, and "Infrastructure as Code (IaC)".
- Establish new governance and processes as required to support cloud enablement.
- Establish appropriate operating model to support use of public cloud at AWS.
- Establish processes and tooling to provide cost transparency for AWS cloud usage (Apptio).
- Integrate with the Cloud Management Platform (CMP).
- Provide training to appropriate teams to support AWS cloud (as needed).

How Security ties into the AWS effort

Core capabilities such as identity and access control, vulnerability management, data encryption, etc., will be used to further secure AWS within the CFG environment.

How CFG is Securing AWS*?

- Authentication with Okta enabling Single Sign On, and authorization through Okta integration to Active Directory (AD) groups managed by SailPoint.
- Configuration Audit with McAfee MVision (CASB).
- Data-at-rest encryption using keys generated and managed by AWS Cloud HSM and Gemalto KeySecure.
- Data-in-motion encryption using certificates issued centrally from Venafi.
- Logging and Monitoring information collected by Splunk Cloud for security analytics.
- Compliance with CFG Hardening Standards including installation of required OS agent and Qualys executed Threat and Vulnerability Management scans.
- Standard templates to consistently automate the configuration of AWS objects in Hashicorp Terraform with Sentinel policies
- Protection through the appropriate cloud based boundary devices (Palo Alto firewalls, f5, NACL, SG).
- Encryption and management of connectivity between AWS and CFG through CFG on premise firewalls.
- Capture of current and historical configurations for all CFG Accounts.

* Integration exceptions and mitigations are captured in the Cloud Security Dashboard

Scope for Microsoft – Desktop Transformation Program (DTP)

Design and build the foundational elements of public cloud in Microsoft as part of Desktop Transformation Program.

- Enable o365 for Exchange, SharePoint and OneDrive running on Windows 10
- Secure o365 with Microsoft Security and Compliance Add-ons
  - Azure Active Directory (P2), Customer Lockbox, Azure ATP, o365 ATP, Customer Key, Azure Information Protection (P2), Advanced e-Discovery, Security and Compliance Center, Exchange Online Protection, Advanced Message Encryption
- Enabling Azure services supporting o365 deployment.
  - Management Groups, RBAC, Policy, KeyVault, Security Center, Log Analytics, Monitor, Advisor, Service Trust
- Create Azure KeyVault subscriptions for Production and P-1 (QA)
- Establish CFG network connectivity to o365 via ForcePoint (Tenant Restrictions) and Firewalls.
- Ensure appropriate cloud security by implementing or integrating with key CFG security tools: Okta, Splunk, mVision, Gemalto, Symantec DLP, Remediant, CyberArk, ForcePoint, and Sailpoint/ARS.
- Establish new governance and processes as required to support o365.
- Establish appropriate operating model to support use of o365 and supporting Azure services.

How Security ties into the Microsoft effort

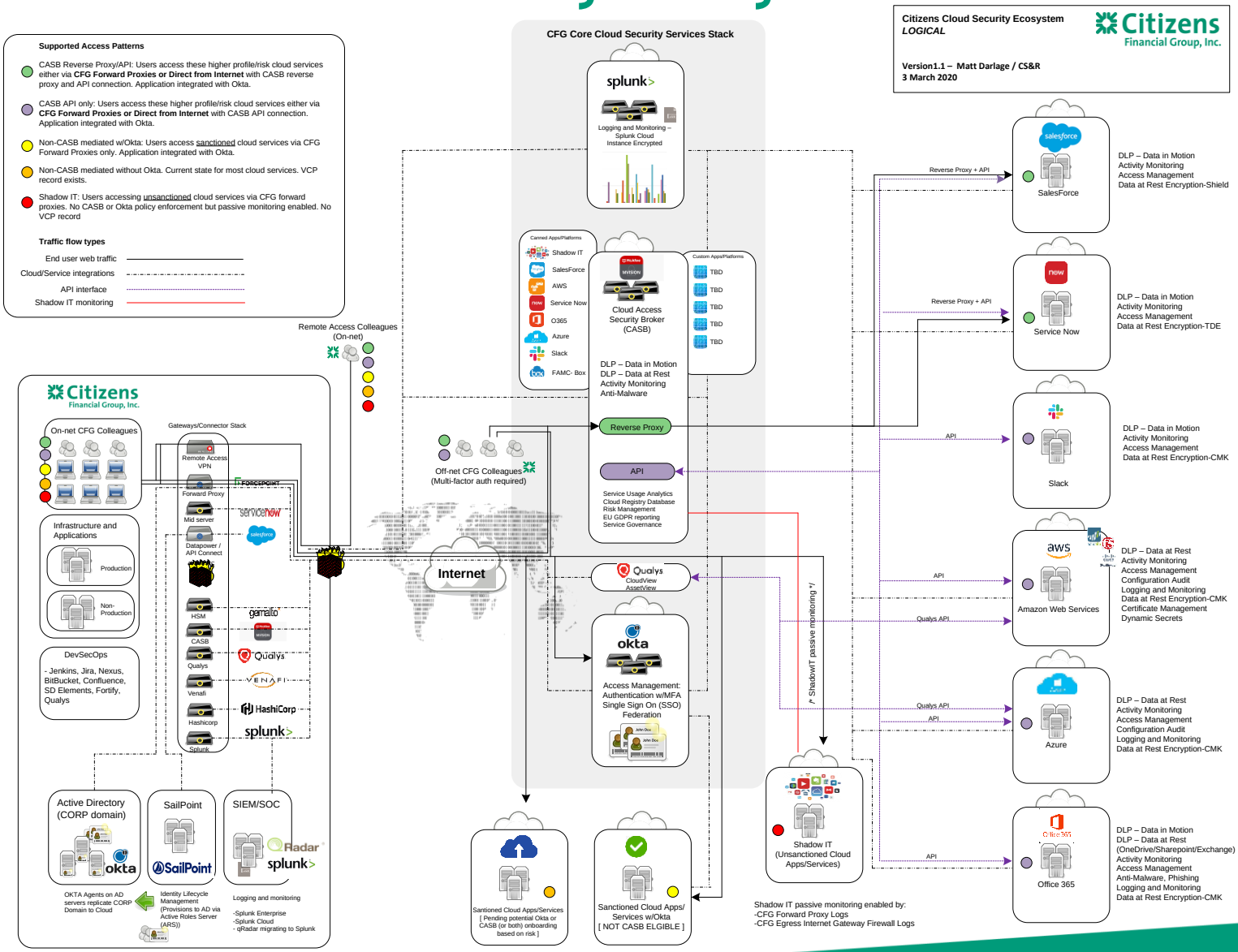
Core capabilities such as identity and access control, vulnerability management, data encryption, etc., will be used to further secure Microsoft within the CFG environment.

How CFG is Securing Microsoft*?

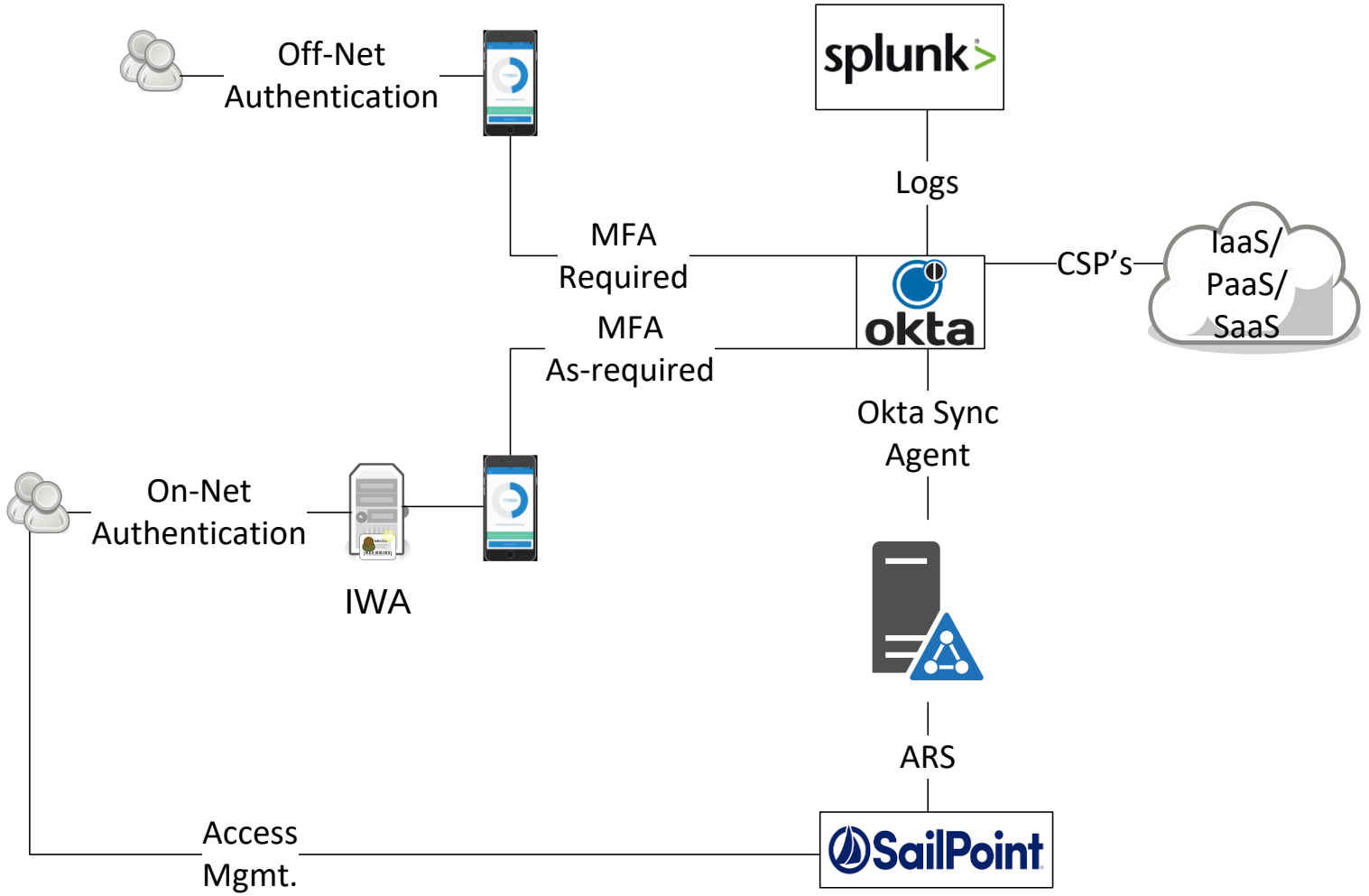
- Authentication with Okta enabling Single Sign On, and authorization through Okta integration to Active Directory (AD) groups managed by SailPoint.
- Azure Configuration Audit with McAfee mVision (CASB).
- DLP controls implemented with Symantec DLP (email), mVision (SharePoint, OneDrive) and Azure Information Protection (Data Classification and Tagging)
- Data-at-rest encryption through Gemalto HSM and KeyVault for Exchange, Sharepoint, OneDrive and based on Data Classification. Data-in-motion encryption using certificates issued centrally from Venafi.
- Logging and Monitoring information collected by Splunk Cloud for security analytics.
- Compliance with CFG Hardening Standards including installation of required OS agent and Qualys executed Threat and Vulnerability Management scans.
- Encryption and management of connectivity between Microsoft and CFG through CFG on premise firewalls and ForcePoint web proxy.
- Windows 10 local administration access managed with Remediant for self service/on-demand privileged access
- MFA required for all administrative accounts via Okta (Verify/RSA) and secondary AD accounts
- Approved mobile devices managed either with BlackBerry or Microsoft Intune

* Integration exceptions and mitigations are captured in the Cloud Security Dashboard

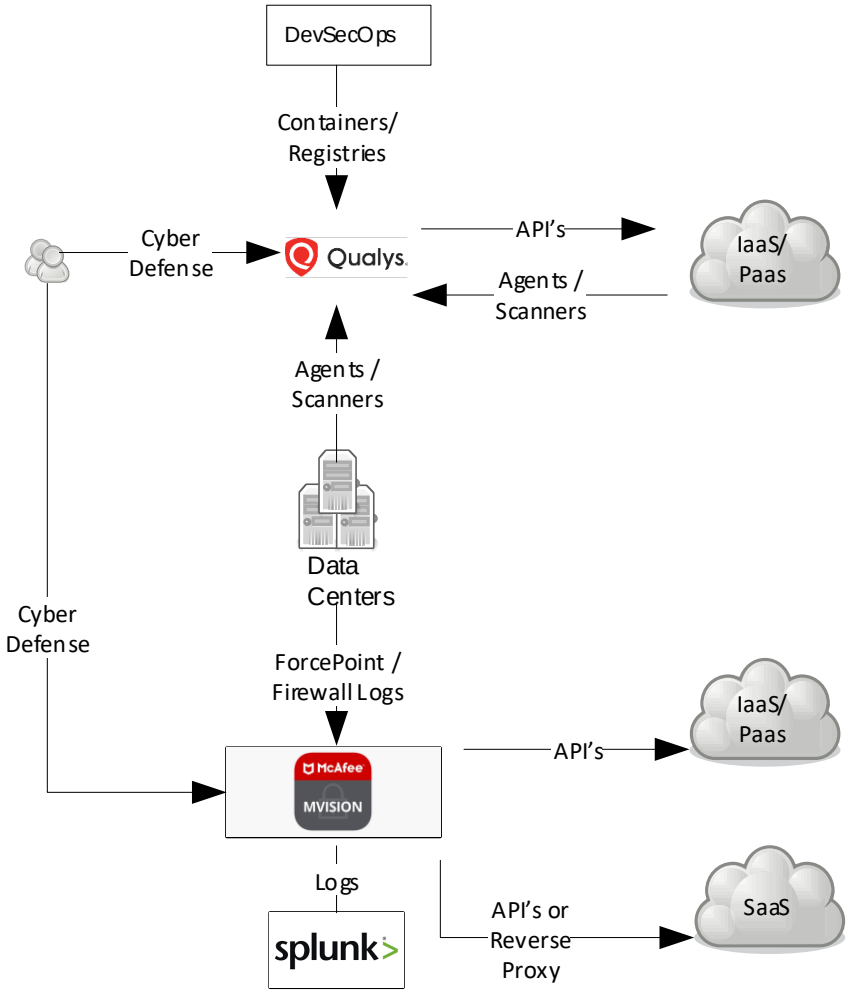
Citizens Cloud Security Ecosystem



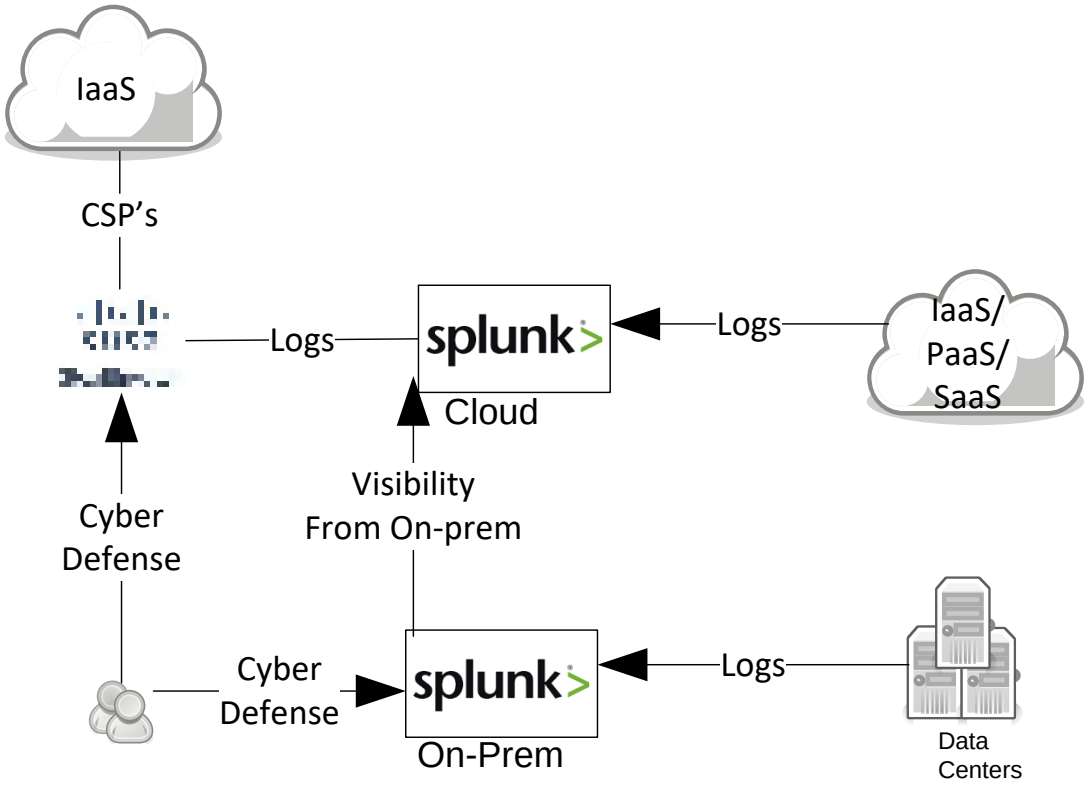
Logical Architecture: Identity & Access Control



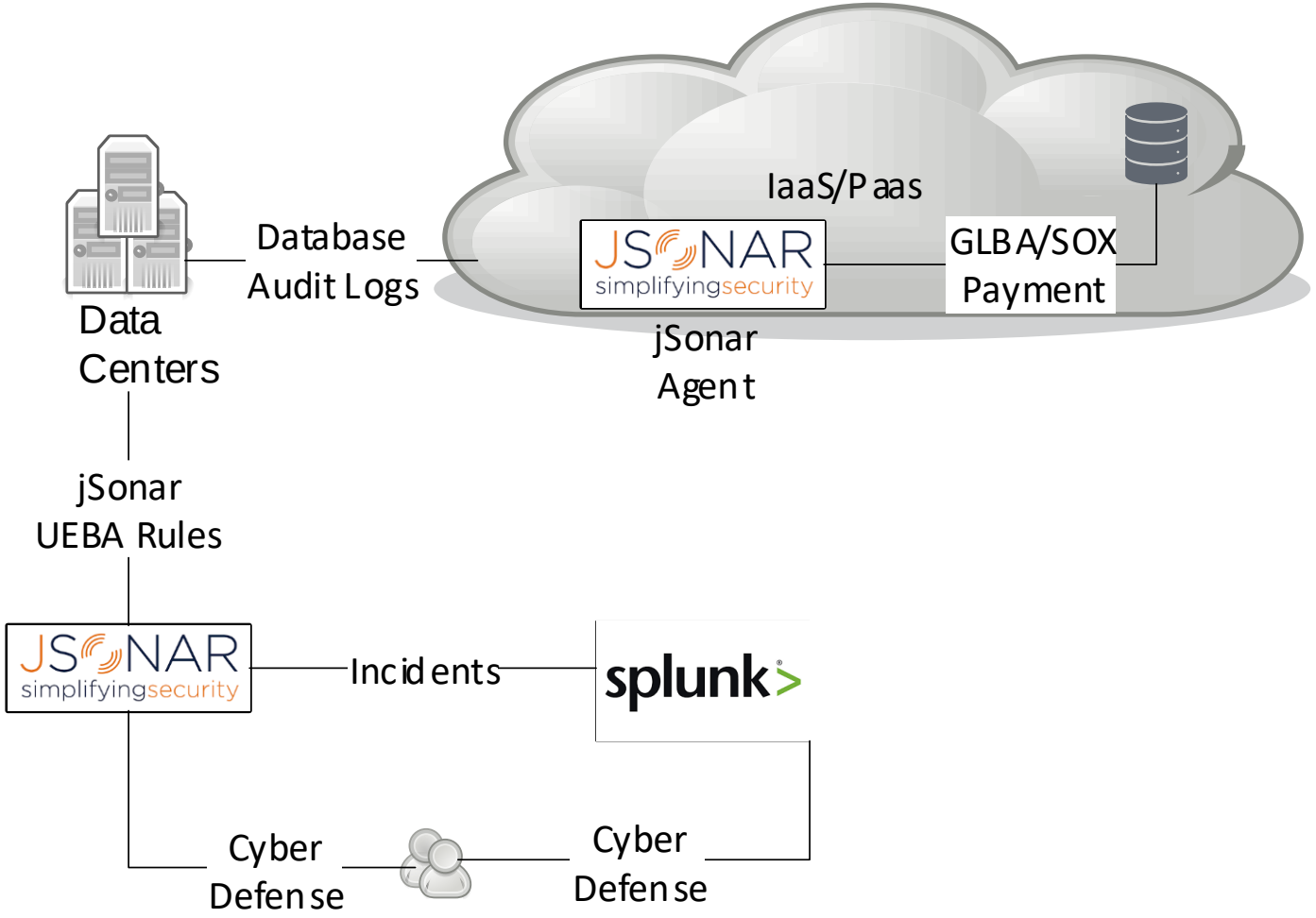
Logical Architecture: Vulnerability Management



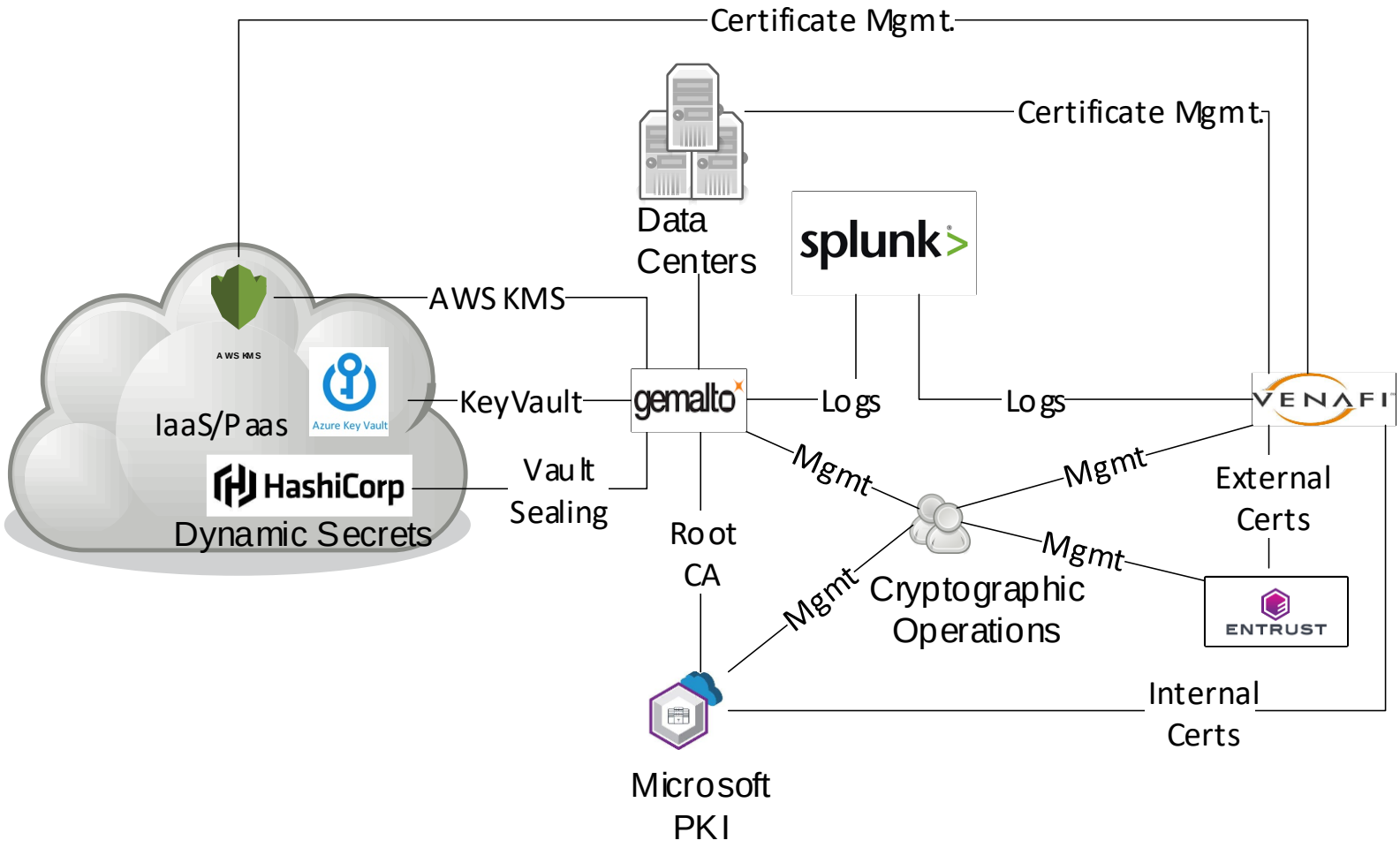
Logical Architecture: Security Visibility / SIEM



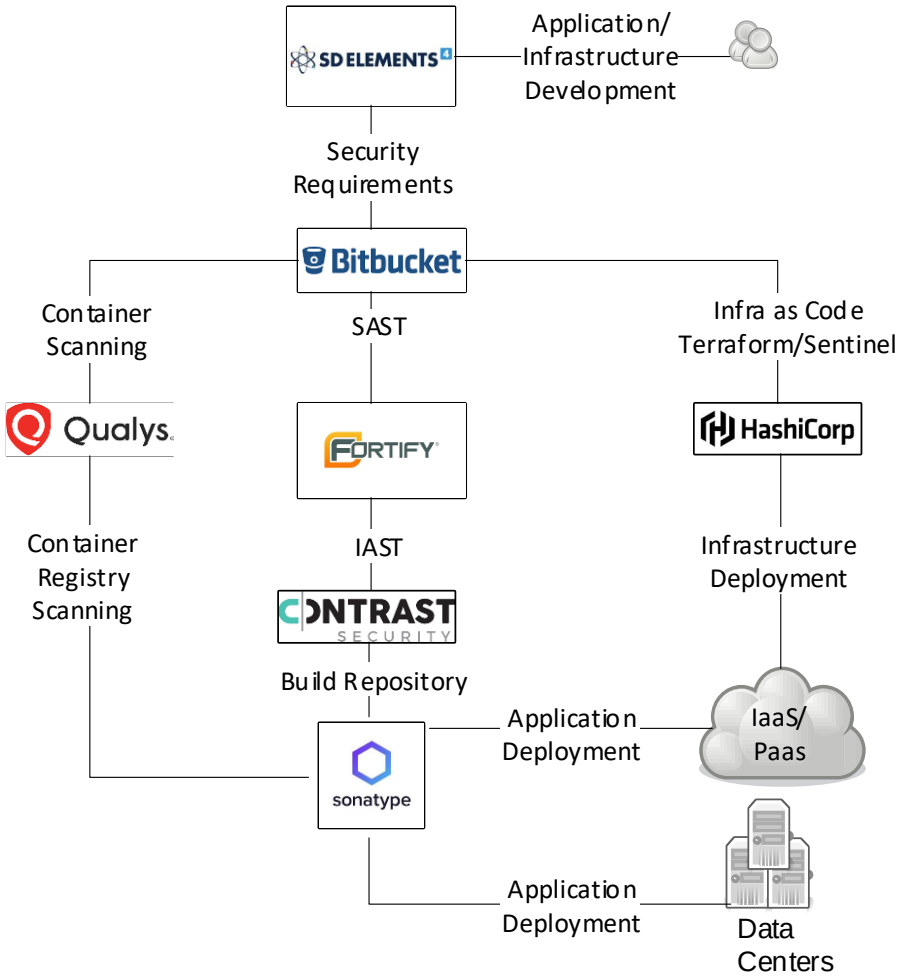
Logical Architecture: Database Logging & Monitoring



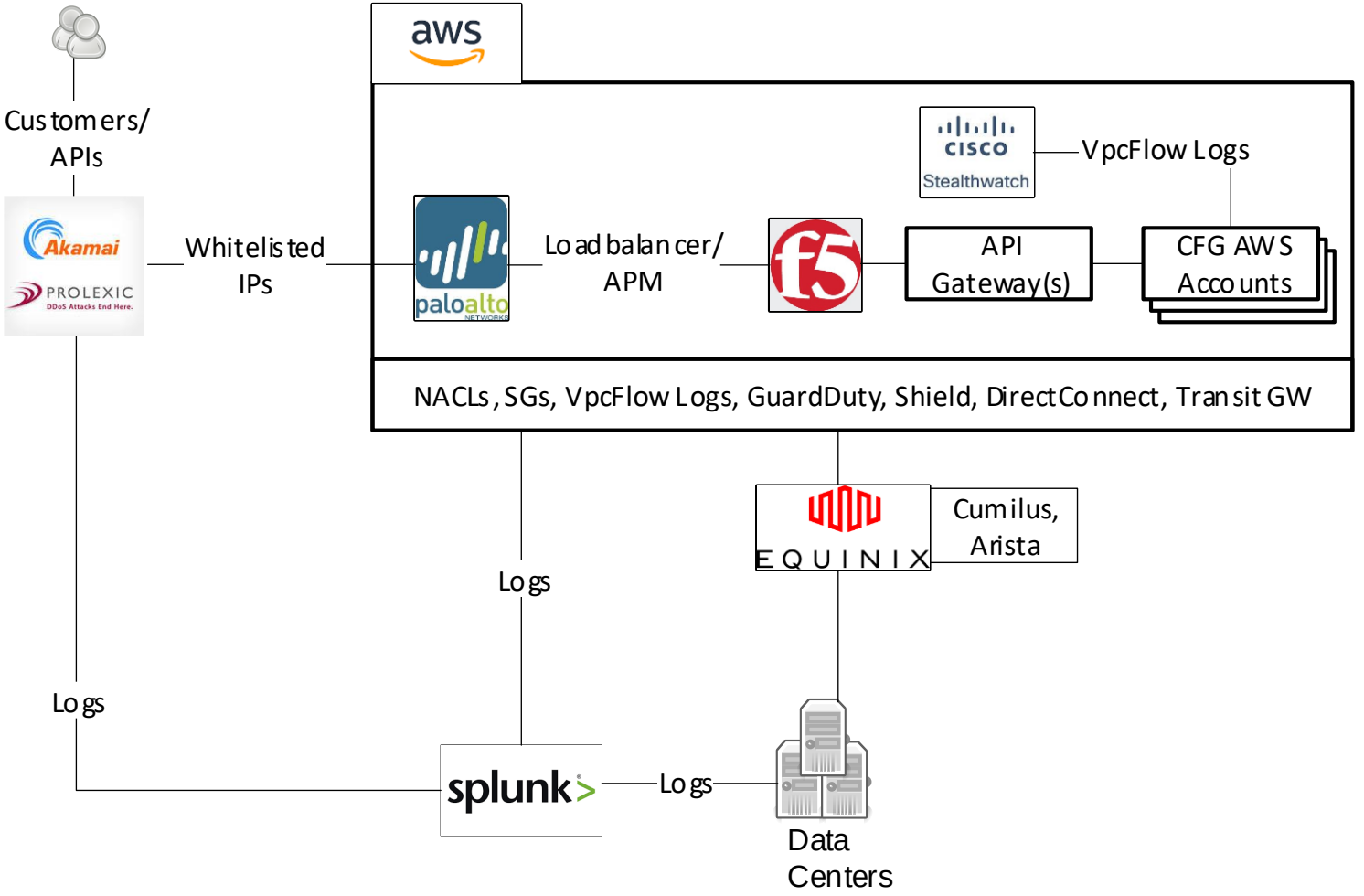
Logical Architecture: Cryptography Management



Logical Architecture: DevSecOps Pipeline



Logical Architecture: Network Security



Core Security Capability:
Identity & Access Control

CS&R Pillar(s)	Identity & Access Management
Solution(s)	Okta / Sailpoint / ARS/ AD /TPAM

Capability Benefits	▪ Single point of authentication and access control for eligible cloud-based applications. ▪ Allows more rapid movement to cloud using CFG identities. ▪ Conforms to standard CFG Identity and Access Management processes. ▪ Governance for approved services. ▪ Common architecture for both Console and CLI access.

	AWS	Comments	Azure	Comments
Colleague authentication integration with Okta Single Sign On and Multi Factor Authentication.	✓	AWS roles and policies managed by CFG IAM team implemented with least privilege.	✓	Microsoft roles and policies managed by CFG IAM team implemented with least privilege.
Okta enforces conditional access rules and MFA policies as required.	✓		✓	
Okta integration to CFG Active Directory for single source of identity.	✓		✓	
SailPoint managed authorization by way of access requests, provisioning, de-provisioning, and access review certifications.	✓		✓	
Privileged Identity Management	✓	TPAM, all ids with Okta and MFA	✓	TPAM, secondary administrative accounts with Okta and MFA
Centralized Account / Subscription Management	✓	All CFG Accounts are joined through AWS Organizations enabling service control policies governing approved AWS services.	✓	All CFG Subscriptions are joined through Azure Management Groups enabling policies governing approved Microsoft services and regions.
Digital App Implications	✓	Digital App for risk based authentication – Transmit Security, Threat Matrix, and Okta for customer authorization.	N/A	

Core Security Capability:
Vulnerability Management

CS&R Pillar(s)	Security Engineering & Architecture; Cyber Defense
Solution(s)	MVISION CASB; Qualys

Capability Benefits	▪ Security monitoring and handling connectivity to high risk cloud services. ▪ Facilitates increased data protection for cloud access from CFG. ▪ Conforms to standard CFG Cyber Defense processes. ▪ Enforces CFG Hardening Standards. ▪ Weekly reviews of MVISION Configuration Audit results.

	AWS	Comments	Azure	Comments
MVISION Integration • User Activity and Anomaly monitoring and alerting. • Configuration audit based on CIS Benchmark. • DLP Scanning	✓	DLP scanning of s3 buckets.	✓	DLP for SharePoint and OneDrive.
Qualys Asset View and Cloud View integration into all CFG Accounts	✓	Discovery of AWS objects to feed Qualys Virtual Scanner.	✓	Trinity subscriptions only, no other subscriptions have servers at this time.
Qualys Virtual Scanner	✓	Scans all AWS:EC2 instances and AWS:RDS databases.	✓	Trinity subscriptions only, no other subscriptions have servers at this time.
Qualys Agent	✓	Installed on all Linux and Windows EC2 instances as well as all other standard CFG required agents.	✓	Trinity subscriptions only, no other subscriptions have servers at this time.
Qualys Container Scanning	✓	Vulnerability scanning of Docker Containers and Registry.	N/A	

Core Security Capability:
Security Visibility / SIEM

CS&R Pillar(s)	Security Engineering & Architecture; Cyber Defense
Solution(s)	Splunk Cloud, GuardDuty

Capability Benefits	▪ Centralized logging and analytics. ▪ Enables enhanced visibility and correlation of events across multiple cloud platforms and on premises log sources. ▪ Aligns to enterprise logging and monitoring strategy. ▪ Conforms to standard CFG Cyber Defense processes.

	AWS	Comments	Azure	Comments
In Application Logging	✓	Dedicated AWS logging account receives activities from all CFG AWS Accounts including: AWS:CloudTrail, AWS:VPCFlowLogs, AWS:ELB access logs, AWS:s3 access logs. AWS logging account persists logs to AWS:s3 bucket for long term storage.	✓	
Splunk Cloud Log Ingestion	✓	Splunk Cloud consumes log sources from dedicated AWS logging account AWS: Firehose.	✓	Microsoft Audit and Service logs pulled into Splunk Cloud using the Splunk Add-Ons for Microsoft Cloud Services and Office 365.
Splunk Cloud Dashboards to Visualize Relevant Activity	✓		✓	
Splunk Cloud alerts are generated to the CFG SOC based on pre-defined monitoring activities	✓		✓	Several Microsoft Integrated security services are enabled including ATP, AIP, CAS.
GuardDuty Monitoring	✓	Provides an additional threat detection capability for AWS accounts	N/A	
Network Behavior and Threat Detection	✓	AWS Stealthwatch, Digital, EDO, Innovation Lab, Network, Shared Services accounts monitored	✓	Several Microsoft Integrated security services are enabled including ATP, AIP, CAS.
Additional Log Sources – Digital App	✓	Okta, Akamai and Palo Alto firewalls.	N/A	

Core Security Capability:
Database Logging & Monitoring

CS&R Pillar(s)	Security Engineering & Architecture; Cyber Defense
Solution(s)	JSonar

Capability Benefits	▪ Specific to GLBA / SOX / Payment databases. ▪ Logging and Monitoring to detect account abuse and insider threat ▪ Native integration with Cloud Platforms ▪ Operational Intelligence for Risk Reduction Controls

	AWS	Comments	Azure	Comments
JSonar Implementation with Log Forwarding to Splunk	✓	Supported databases	N/A	

Core Security Capability:
Cryptography Management

CS&R Pillar(s)	Security Engineering & Architecture
Solution(s)	Gemalto, AWS Cloud HSM

Capability Benefits

- Cryptographic key material managed by CFG not cloud service provider.
- Data-at-Rest and Data-in-Motion encrypted securing sensitive content.
- Aligns to enterprise cryptography strategy.
- Conforms to standard CFG Cryptographic Operations Management processes.
- TDE Encryption required for eligible and supported GLBA / SOX / Payment databases.

	AWS	Comments	Azure	Comments
Encryption Implementation	✓	AWS: Key Management Service (KMS) implemented with external Customer Managed Keys (CMK). AWS: Cloud HSM	✓	Azure Key Vault implemented with external Customer Managed Keys (CMK).
Data-at-Rest Encryption	✓	AWS:KMS used for Allowed CFG Services: AWS:s3, AWS:EBS, AWS:EFS, AWS:RDS, AWS:CloudTrail, AWS:VPC Flow Logs.	✓	Azure Key Vault used for Allowed CFG Services: Customer Key – Exchange, SharePoint and OneDrive, and AIP (BYOK) – Documents classified as Restricted and email classified as Confidential or greater.
Key Material generated within CFG on-premises Gemalto HSMs	✓		✓	
TDE Encryption	✓	AWS Native TDE with KMS is supported for RDS Oracle, RDS Microsoft SQL, and DynamoDB; Gemalto Keysecure has been deployed in AWS to support TDE for Non-RDS databases.	N/A	

Core Security Capability:
DevSecOps Pipeline

CS&R Pillar(s)	Cyber Defense
Solution(s)	Hashicorp, SD Elements, Fortify, Qualys Container & Registry Scanning, Contrast

Capability Benefits	▪ Reduces manual changes and adds another layer of auditing capabilities. ▪ Ensures consistency in deployments with reusable Terraform modules. ▪ Sentinel runs policy compliance checks before changes are executed. ▪ Enables appropriate teams to approve code changes and policy changes (e.g. VpcEndpoint, s3 bucket, KMS and IAM policies). ▪ Security requirements introduced at the beginning of the development process.

	AWS	Comments	Azure	Comments
Hashicorp Terraform used to script infrastructure as code changes with Sentinel validating policy compliance	✓	In use for Digital and Cloud Engineering	N/A	
Hashicorp Vault used for Secrets Management	✓	In use for Digital	N/A	
Hashicorp Consul	✓	Service Registry and Discovery for Digital	N/A	
SonaType	✓	Used for artifact management and Open Source Library Compliance for Digital	N/A	
SD Elements adding security requirements in Jira Boards	✓		N/A	
IAST: Contrast integrated real-time application monitoring resident within application and identifies vulnerabilities as part of normal functional and QA testing processes	✓	In Use for FAMC, planned for CFG starting 2021	N/A	
Qualys Container scanning validating that the containers, registries and runtimes are in compliance with Application Security Guidelines	✓	In Use for Digital, Enterprise DevSecOps Prod Nexus Registry and OpenShift runtimes	N/A	
SAST: Fortify code scans validating application code is in compliance with Application Security Guidelines	✓	In Use for Digital, Enterprise DevSecOps, FAMC	N/A	

Core Security Capability:
Network Security

CS&R Pillar(s)	Security Engineering & Architecture
Solution(s)	AWS Security Groups, NACLs, Access Policies, Prolexic

Capability Benefits	▪ Current capabilities provide visibility into the VPCs, which have network infrastructure. Compliance scanning and threat detection is provided through several different tools and services including McAfee MVISION Cloud Security, Cisco Stealthwatch, and Splunk.

	AWS	Comments	Azure	Comments
DDoS Protection	✓	Akamai (specific to onboarded applications); AWS Shield, Prolexic	N/A	
VPC Flow Log ingestion into Splunk	✓	All VPC	N/A	
Network Filtering	✓	NACLs, Palo Alto, F5, AWS Security Groups	N/A	
Application Routing	✓	ALBs, ELBs, NLBs, F5, Zuul, API Connect	N/A	
Software Defined Networks (SDNs)	✓	RedHat – Calico Digital – Flannel Eqinix – Cumilus, Arista	N/A	
Private Cloud Gateway Services	✓	Netbond, Equinix, DirectConnect	N/A	

APPENDIX

ARB: Cloud Security Links

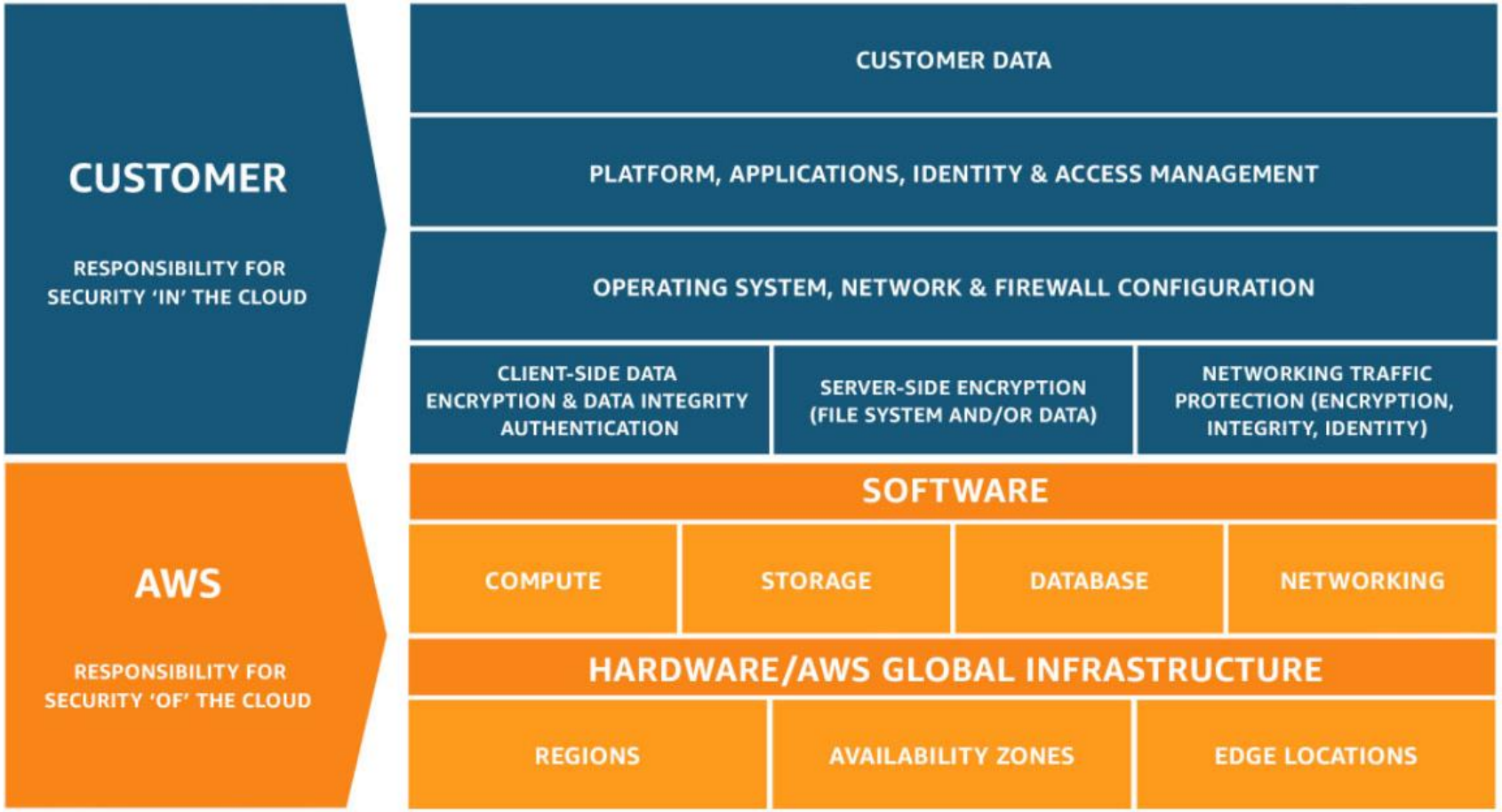
- ARB – Link to Solution Approaches and Designs for supporting Cloud Security tools
  - Okta – PV6114
  - mVision – PV5900
  - Splunk Cloud – PV5945
  - Gemalto, Venafi – PV6113
  - SailPoint/ARS – PV1335
  - Active Directory – PV2770, PV5346, PV6178
  - ForcePoint – PV5366
  - API Connect/DataPower - PV5805
  - Cloud Transformation Program/HashiCorp – PV5945
  - Desktop Transformation Program – PV5938

* Definitions from Cloud Security Minimum Requirement(MR)

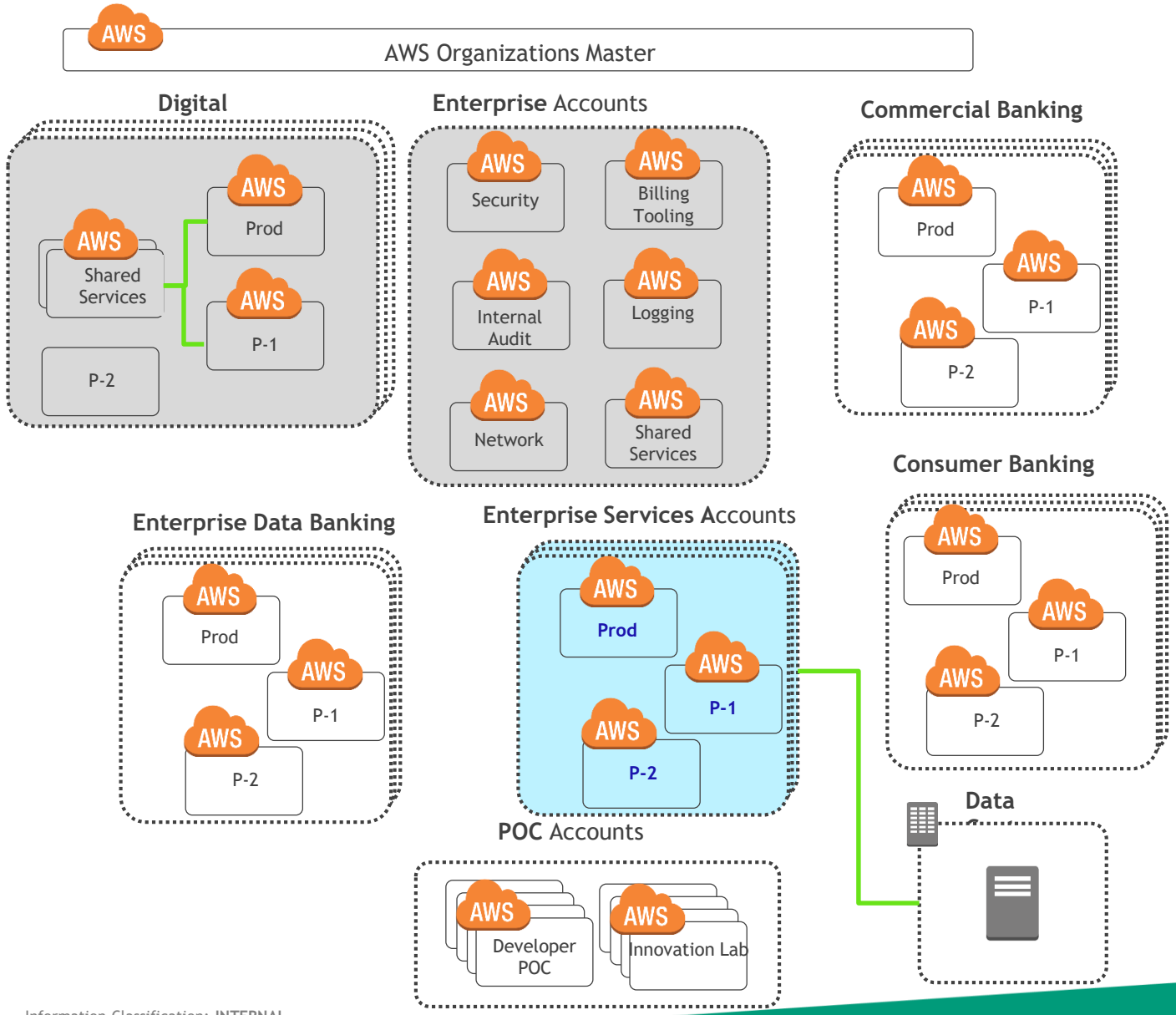
Amazon – Cloud Service Provider

AWS Shared Security Model

As stated on the previous slides and illustrated below, CFG, as Customer of AWS, has a responsibility to further enhance the security capabilities around AWS.



AWS - Enterprise Account Approach



Orgs: Account management

Logging: Centralized logs

Security: AWS Config Rules, security tools

Shared services: Directory, DNS, limit monitoring

Billing Tooling: Cost monitoring

POC: Experiments needing CFG Connectivity

Innovation Lab: Experiments needing internet (No CFG)

Enterprise Services: Account for Common enterprise tools that do not need connectivity to all Accounts.

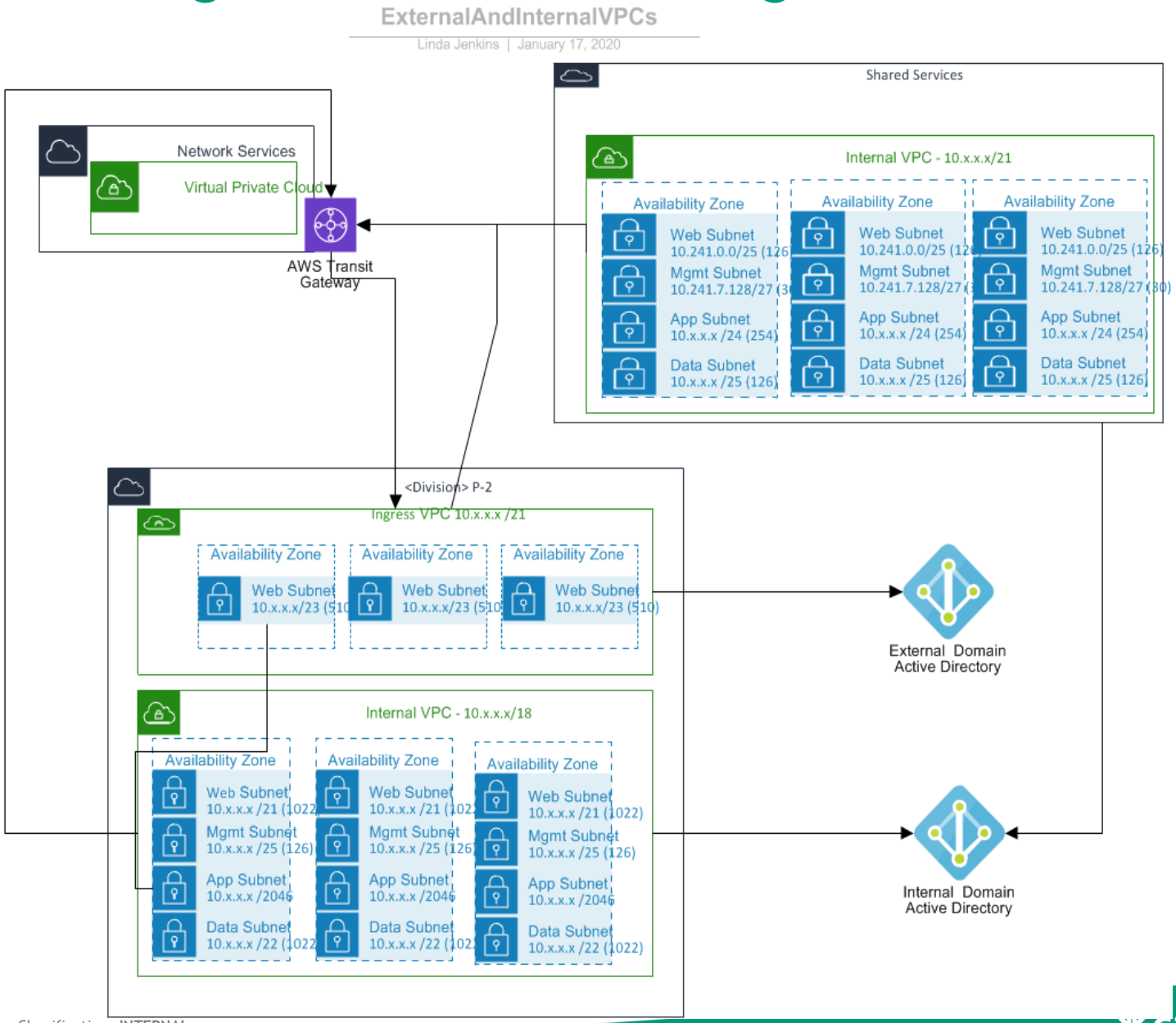
(Confluence, Jira, Bitbucket)

P-2: 2 levels below Prod (dev, SIT, iterative QA) Most permissive

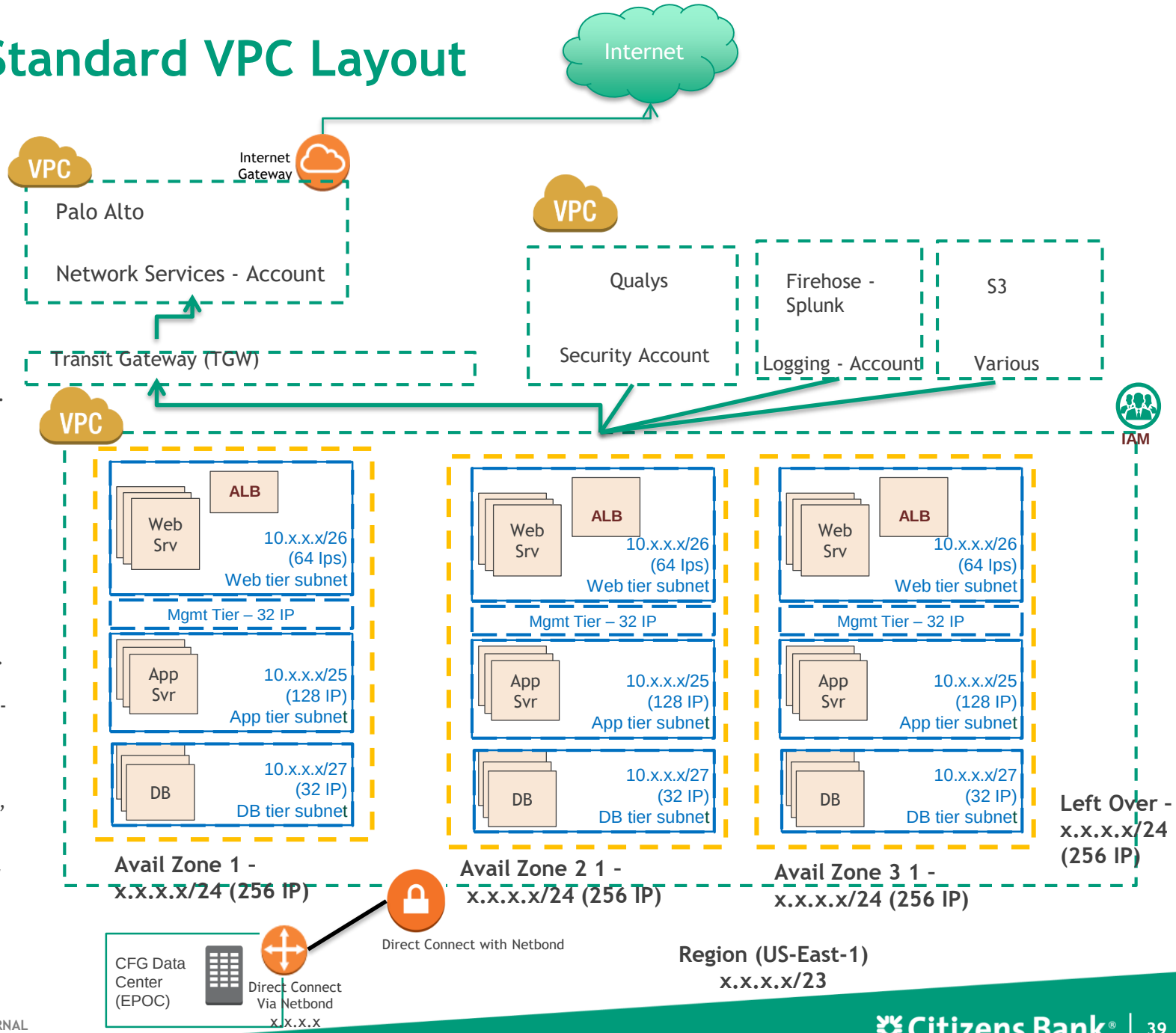
P-1: 1 Level below Prod QA, UAT, Staging

Prod: Production

AWS - High Level Network Design



AWS - Standard VPC Layout



Notes:

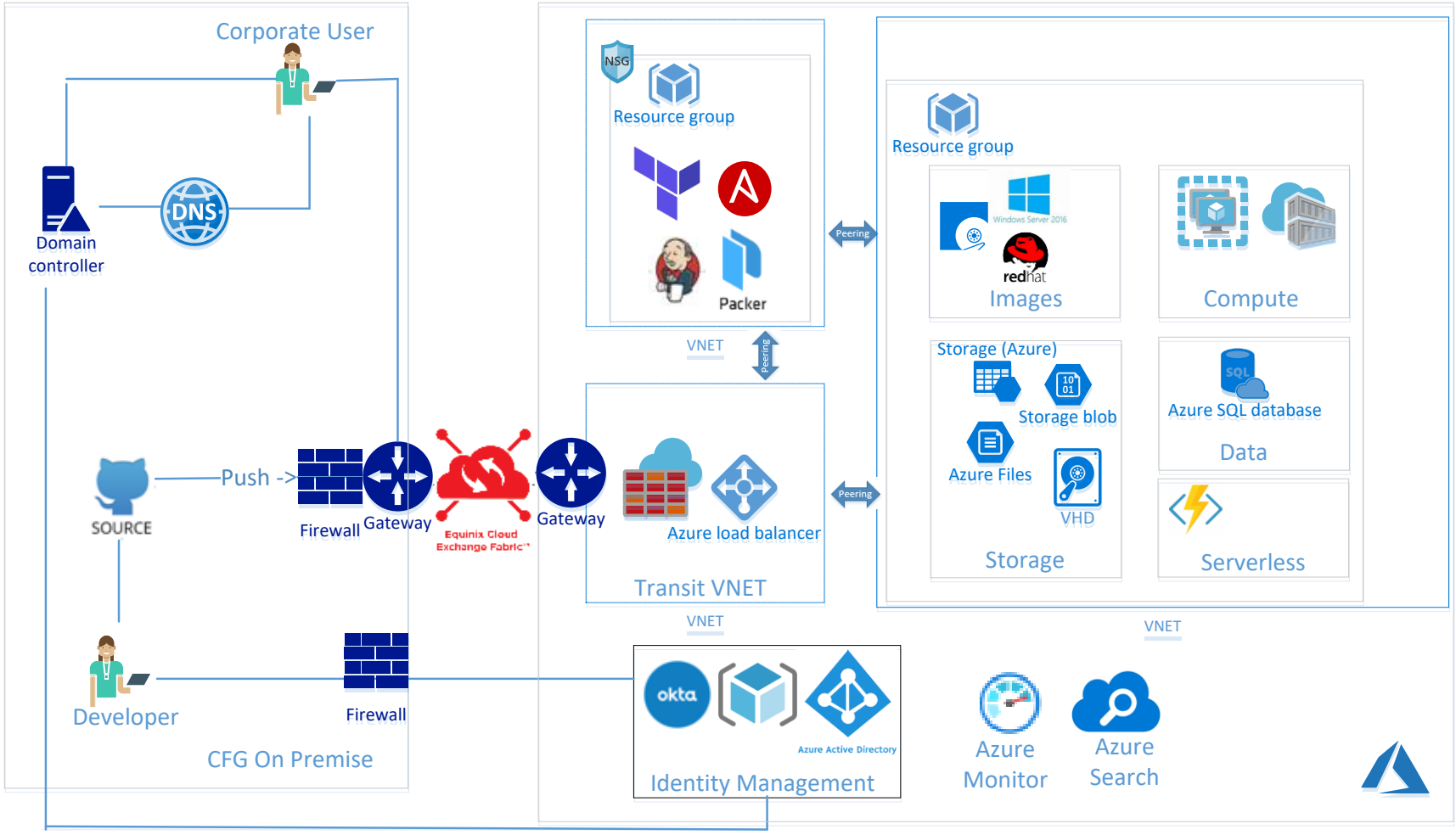
- CIDR Bloc – 1024 IPs.
- No Inbound Internet Access - Internal AD access
- Inbound Internet access -External
- **Web** = DMZ – Connectivity from External/Untrusted
- **App** = No Data - Connectivity from Trusted Servers (i.e. Data Center/AWS)
- **Data** = Data Stores - No Connectivity to CFG or Internet
- **Mgmt** – Bastion Hosts, Tools Servers, Operational Tools
- Subnet size can change but quantity (4) and type (App, Web) remain standard.

Microsoft - Cloud Service Provider

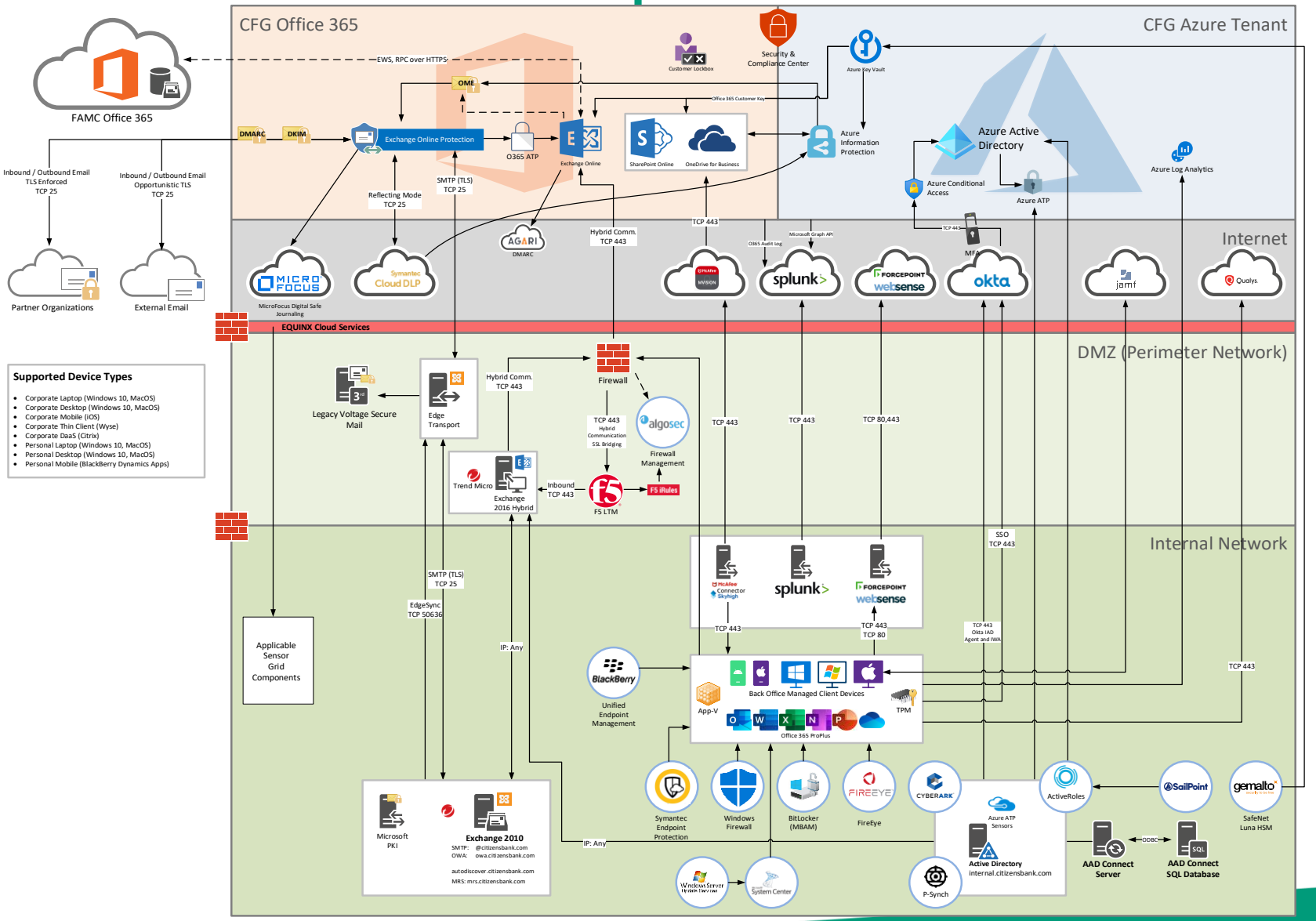
Microsoft Shared Security Model

As stated on the previous slides and illustrated below, CFG, as Customer of Microsoft, has a responsibility to further enhance the security capabilities around Microsoft.

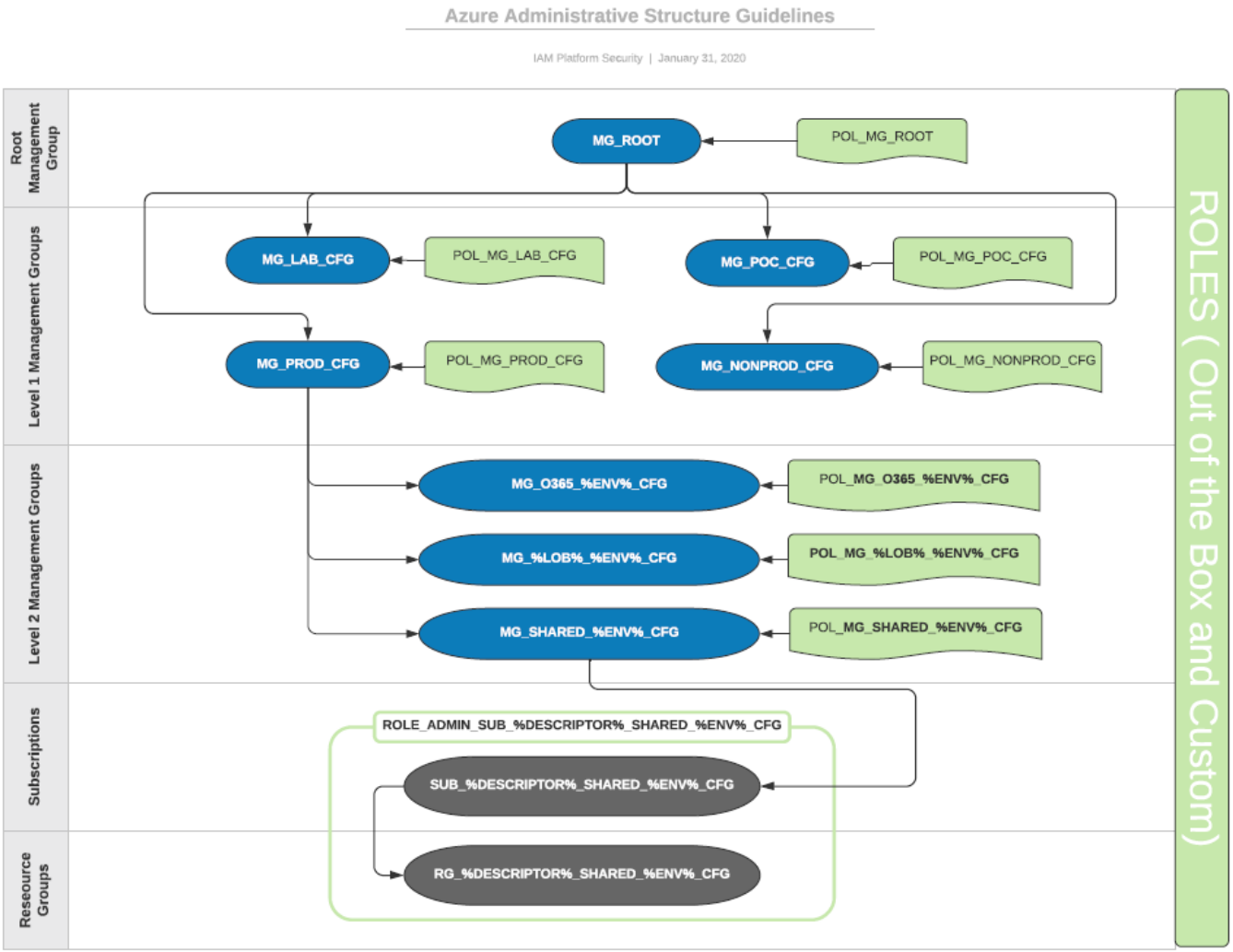
Microsoft - Azure Conceptual Architecture



Microsoft - o365 Conceptual Architecture



Microsoft – Management Group Model



DETAILS

MG = Management Groups
POL = Policy
SUB = Subscriptions
RG = Resource Group

Level 1 Management Groups

LAB: Sandbox for any possible implementation, including new Azure services or any application that may or may not be implemented in the future.Broad permissions for everyone.Liberal usage policy.

POC: As name indicates, this is where one would implement POC versions of any service or app for consideration.

NONPROD: Dev, Test and QA versions of services and apps that are going to be (or have been) implemented in PROD. %ENV% indicates specific environment.

PROD: Production versions of service and apps for use in the bank

Level 2 Management Groups

SHARED: Shared container would include any subscription that is needed by multiple LOBs or the entire company.

%LOB%: Dedicated LOB would include subscriptions designated to a single LOB.

%ENV%": P, P-1 , P-2

Roles

Controls user permissions at different levels in Azure.Can be applied to Management Groups, Subscriptions, Resources and Resource Groups.

Scope: Model serves as guideline for internaldev, internalqa, and internal AAD forests