20 January 2022

\*\*\*

Security Reference Architectures

REPORT

Document Control

|  |  |
| --- | --- |
| Document Information | |
| **Creation date** | 20/01/2022 |
| **Owner/author** |  |
| **Internal/External audience** | External |
| **Document classification** | Confidential |
| **Design review board reference** | N/A |
| **Template version** | 7.1-SD (July 2020) based on 7.0 (February 2020) |

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History | | | |
| **Version** | **Revision Details** | **Revised By** | **Date** |
| 0.1 | First draft |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Document Review/Approval | | | |
| **Reviewer** | **Position** | **Version** | **Review Date** |
|  |  |  |  |
|  |  |  |  |

[1. EXECUTIVE Summary 6](#_Toc97215467)

[1.1. Document Purpose 6](#_Toc97215468)

[1.2. Intended Audience 6](#_Toc97215469)

[1.3. Project Overview 6](#_Toc97215470)

[2. Security Architecture Components 7](#_Toc97215471)

[2.1. Overview 7](#_Toc97215472)

[2.1.1. Core and User/IoT/OT security Services 7](#_Toc97215473)

[2.2. Core Security Services 9](#_Toc97215474)

[2.2.1. Asset and Device Management 9](#_Toc97215475)

[2.2.1.1. CIS v7 Sections 9](#_Toc97215476)

[2.2.1.2. Hardware Assets 9](#_Toc97215477)

[2.2.1.3. Software Assets 10](#_Toc97215478)

[2.2.2. Vulnerability Management and Patching 11](#_Toc97215479)

[2.2.2.1. CIS v7 Sections 11](#_Toc97215480)

[2.2.2.2. Vulnerability Management and Patching Overview 11](#_Toc97215481)

[2.2.3. Secure Configuration 12](#_Toc97215482)

[2.2.3.1. CIS v7 Sections 12](#_Toc97215483)

[2.2.3.2. Hardware, System, Software (Application), and Network Hardening 12](#_Toc97215484)

[2.2.4. Logging 13](#_Toc97215485)

[2.2.4.1. CIS v7 Sections 13](#_Toc97215486)

[2.2.4.2. SIEM/XDR Overview 13](#_Toc97215487)

[2.2.4.3. Core Capabilities of Next Generation SIEM/XDR 14](#_Toc97215488)

[2.2.4.4. SIEM vs XDR 15](#_Toc97215489)

[2.2.4.5. Event Logging 16](#_Toc97215490)

[2.2.5. Identity Provider and Governance 16](#_Toc97215491)

[2.2.5.1. CIS v7 Sections 16](#_Toc97215492)

[2.2.5.2. Identity and Access Management (IAM) Overview 17](#_Toc97215493)

[2.2.5.3. Least Privileged 18](#_Toc97215494)

[2.2.6. Email Security 18](#_Toc97215495)

[2.2.6.1. CIS v7 Sections 18](#_Toc97215496)

[2.2.6.2. Email Security Overview 19](#_Toc97215497)

[2.3. End USer, Internet of Things/Operational technology Security Services 20](#_Toc97215498)

[2.3.1. Single Sign-On (SSO) 20](#_Toc97215499)

[2.3.1.1. CIS v7 Sections 20](#_Toc97215500)

[2.3.1.2. Single Sign-On Overview 20](#_Toc97215501)

[2.3.1.3. Summary 21](#_Toc97215502)

[2.3.2. Data Loss Prevention (DLP) 21](#_Toc97215503)

[2.3.2.1. CIS v7 Sections 21](#_Toc97215504)

[2.3.2.2. Data Loss Prevention (DLP) Overview 21](#_Toc97215505)

[2.3.3. Key/Password Management 24](#_Toc97215506)

[2.3.3.1. CIS v7 Sections 24](#_Toc97215507)

[2.3.3.2. Application Key Storage 24](#_Toc97215508)

[2.3.3.3. Public Key Infrastructure (PKI) Management 24](#_Toc97215509)

[2.3.3.4. Password Vaults 25](#_Toc97215510)

[2.3.3.5. Hardware Security Module (HSM) and Trusted Platform Module (TPM) 25](#_Toc97215511)

[2.3.4. Web Security 26](#_Toc97215512)

[2.3.4.1. CIS v7 Sections 26](#_Toc97215513)

[2.3.4.2. Overview 26](#_Toc97215514)

[2.3.4.3. Secure Access Service Edge (SASE) 26](#_Toc97215515)

[2.3.4.4. SASE Benefits 27](#_Toc97215516)

[2.3.4.5. Where and What is the Edge? 27](#_Toc97215517)

[2.3.4.6. Secure Web Gateway (SWG) 27](#_Toc97215518)

[2.3.4.7. Cloud Access Security Broker (CASB) 28](#_Toc97215519)

[2.3.4.8. Remote Browser Isolation (RBI) 29](#_Toc97215520)

[2.3.5. DNS Security 29](#_Toc97215521)

[2.3.5.1. CIS v7 Sections 29](#_Toc97215522)

[2.3.5.2. DNS Security Overview 29](#_Toc97215523)

[2.3.6. Network Access Control 30](#_Toc97215524)

[2.3.6.1. CIS v7 Sections 30](#_Toc97215525)

[2.3.6.2. Network Access Control Overview 30](#_Toc97215526)

[2.3.7. Multi-factor, Adaptive (Conditional), and Risk Authentication 31](#_Toc97215527)

[2.3.7.1. CIS v7 Sections 31](#_Toc97215528)

[2.3.7.2. Multi-factor Authentication (MFA) Overview 31](#_Toc97215529)

[2.3.8. Wireless Security 33](#_Toc97215530)

[2.3.8.1. CIS v7 Sections 33](#_Toc97215531)

[2.3.8.2. Wireless Security Overview 33](#_Toc97215532)

[2.3.9. Firewall 34](#_Toc97215533)

[2.3.9.1. CIS v7 Sections 34](#_Toc97215534)

[2.3.9.2. Firewall Capabilities 34](#_Toc97215535)

[2.3.9.3. FIREWALL SECURITY FUNCTIONS 36](#_Toc97215536)

[2.3.9.4. Firewall as a Service (FWaaS) 37](#_Toc97215537)

[2.3.10. Endpoint Security 38](#_Toc97215538)

[2.3.10.1. CIS v7 Sections 38](#_Toc97215539)

[2.3.10.2. Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) Overview 38](#_Toc97215540)

[2.3.10.3. EDR vs MDR 38](#_Toc97215541)

[2.3.10.4. Endpoint Detection and Response 39](#_Toc97215542)

[2.3.10.5. Recommendations 39](#_Toc97215543)

[2.3.11. Encryption 40](#_Toc97215544)

[2.3.11.1. CIS v7 Sections 40](#_Toc97215545)

[2.3.11.2. Encryption at Rest vs Motion 40](#_Toc97215546)

[2.3.12. Virtual Private Network 41](#_Toc97215547)

[2.3.12.1. CIS v7 Sections 41](#_Toc97215548)

[2.3.12.2. Traditional VPN 41](#_Toc97215549)

[2.3.12.3. Zero Trust Network Access (ZTNA) 41](#_Toc97215550)

[3. Personas 42](#_Toc97215551)

[3.1. Security Framework 42](#_Toc97215552)

[3.2. General Head Office Users 43](#_Toc97215553)

[3.2.1.1. Accessing Software as a Service (SaaS) 43](#_Toc97215554)

[3.2.1.2. Accessing General Internet Services 44](#_Toc97215555)

[3.2.1.3. Accessing On-premise, Data Centre or Cloud Services 45](#_Toc97215556)

[3.3. Distribution Centre Staff 46](#_Toc97215557)

[3.4. Retail Store Colleagues 48](#_Toc97215558)

[3.5. Customer Care Staff (PCI) 49](#_Toc97215559)

[3.5.1.1. Accessing Software as a Service (SaaS) 50](#_Toc97215560)

[3.5.1.2. Accessing On-premise, Data Centre or Cloud Services 51](#_Toc97215561)

[3.6. Third Parties (App Support, Payment, etc) 52](#_Toc97215562)

[3.7. SUBSIDIARIES 54](#_Toc97215563)

[3.7.1.1. Accessing Software as a Service (SaaS) 54](#_Toc97215564)

[3.7.1.2. Accessing On-premise, Data Centre or Cloud Services 55](#_Toc97215565)

1. EXECUTIVE Summary

## Document Purpose

## Intended Audience

This Cyber Security Roadmap aims for business and technical decision-makers, technical stakeholders, and some wider business focused stakeholders. Content in this document is most relevant to those in the following or similar roles:

* Technical Architects
* Security Architects
* Security Managers/Directors
* Security Engineers
* IT Managers/Engineers

## Project Overview

\*\*\* seek high-level security reference architecture to illustrate conceptual layers of technology and process intersections accompanied with strategic alignment for the business to functions/ personas within an organisation. This in-turn will demonstrate/inform what best practice ‘good security’ would look like within the business. It must be noted that the security reference architectures are based around users accessing services. Core security services are added to the document that won’t pertain directly to persona security but outline good security practice as a whole.

A security reference model simplifies securing business functions by organising them into a building block. The model incorporates today’s security best practices in addition to:

* Centralised security management for the group and businesses, subsidiaries.
* Business use cases illustrating the surface that fraudsters can attack
* Reference architectures that logically arrange the security capabilities into blueprints

Following the undertaking on a CIS v7 security baseline assessment, gap analysis and discovery workshop the contents of this document and diagrams will represent present state and outlook.

1. Security Architecture Components
   1. Overview

In this ever-evolving world of increased technological dependency, attacks such as phishing, ransomware, and advanced persistent threats are becoming more sophisticated and evasive. Technology adaptations for the purpose of addressing new use-cases, and organizations leveraging a multitude of products that do not interoperate seamlessly, also adds to an increased attack surfaces and cumbersome defences.

Organisations of all sizes/verticals now recognise that the attack surface has increased exponentially. No sole product can successfully secure a business from these risks. A holistic architectural approach that highlights and identifies critical business flows ranging from any source be it human or IoT to any destination be it On-Prem server housing a critical database or SaaS application is more important than ever for mitigation against the risks as well as those not listed.

Predictability accompanied with simplicity is what this document will aim to provide, clear visibility demonstrated through easy-to-read workflow representations that map personas to a technology stack to help elevate the unknown and speed up remediation if ever required. The security architecture components detailed throughout are in-line with industry recognised best practice that will outline technical areas that \*\*\* can use for reference.

* + 1. Core and User/IoT/OT security Services

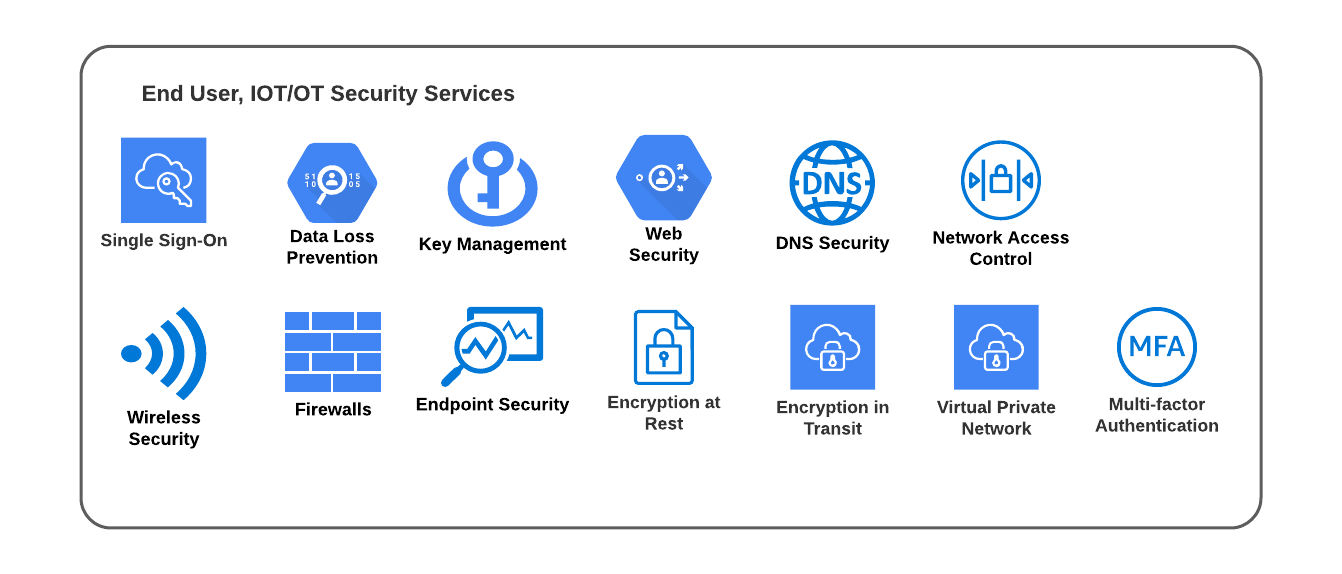
The security services have split into two areas core services and End User, Internet of Things/Operational technology Security Services.

* **Core Security Services:** Security services that represent core functions that would apply to implementation:
  + Asset and Device Management
  + Secure Configuration
  + Vulnerability Management and Patching
  + Logging
  + Identity Provider and Governance
  + Email Security

A picture containing logo

Description automatically generated

* **End User, Internet of Things/Operational technology Security Services:** Security services that are more related to end user, IoT, and OT.
  + Single Sign -On
  + Data Loss Prevention
  + Key/Password Management
  + Web Security
  + DNS Security
  + Network Access Control
  + Multi-factor, Adaptive and Risk Authentication
  + Wireless Security
  + Firewalls
  + Endpoint Security
  + Encryption
  + Virtual Private Network



* 1. Core Security Services
     1. Asset and Device Management

Visibility of assets plays a fundamental role with implementation of any security controls. Without knowing key factors such as what hardware and software assets are present, IT / security teams lack the crucial awareness of their attack surface, they lose the ability to meet security and operational objectives which as a direct result puts the business at risk.

On average, it can take more than a month to create and generate an accurate asset inventory, utilizing a combination of tools that weren’t purpose built for this task, including endpoint management and security tools, network access controls, network scanning, configuration, patch management, and vulnerability assessments.

The securing of assets can be difficult, but there are many ways in which asset inventories can be leveraged to inform or enrich either as a separate source or a centralised database.

* + - 1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 1 | **Inventory and Control of Hardware Assets** | Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. |
| 2 | **Inventory and Control of Software Assets** | Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. |

* + - 1. Hardware Assets

A hardware asset is any device whether used/ stored or owned/in possession of and or used for business purposes for the benefit of an organisation (BYOD). Whether they are connected to the network or not assets holding nonephemeral data/information provide a means of direct access to sensitive data. To mitigate against the associated risk, it is essential for organisations to undertake routine discovery/audit review and record the findings. With an increase of IoT use cases many devices/ appliances that were not traditionally deemed an integral part of the network now are, these vectors act as an easy means of exploit hence it is essential to also include these asset types when undertaking discoveries.

Having a centralised hardware database and processes is critical to implementing holistic security for the business. Using a centralised data is recommended, however using existing technology can be used separately or to inform a central database. Whichever way the business decides to implement hardware asset management the operating model and processes will differ, being more onerous without a centralised solution.

**The following technology elements can be used to manage or inform of hardware assets:**

* **CMDB:** Configuration management database
* **Service Desk:** The service desk solution will have a certain level of hardware asset visibility
* **Device Management:** Data from technologies such as Intune, SCCM, JAMF, and SOTI can be used to inform hardware assets
* **Vulnerability Management:** VM can be provide scanning of the environment, this information can be used to inform any changes or rouge devices in the environment.
* **Active Directory:** Devices in AD can be used, along with DHCP logging.
* **Network Access Control:** Devices connected too and access the network can be logged
* **Endpoint Detection and Response (EDR):** Some EDR solutions provide local scanning of the network and telemetry from the local device that can be utilised.

**Areas for governance to manage hardware assets:**

* Define and review the physical asset processes
* Review tooling/solutions, processes, and infrastructure components to ascertain the correct operating model for hardware asset management. This could be the use of separate tools or a centralised database
  + - 1. Software Assets

A central software asset database will include systems, installed applications and SaaS applications. Also, having a sanctioned list of applications that can be used in the business is recommended that can be updated as the need arises.

Enforcement and visibility of unsanctioned applications, scripts, and libraries is another area that is critical for ensuring security is maintained. Knowing what software is being used will help to identify vulnerabilities in those applications and where ‘Shadow IT’ is being used.

**Technology that can be used to manage or inform software assets used:**

* **Device Management:** Solutions such as Intune/SCCM/JAMF can be used to inform of applications that are installed in the environment.
* **Endpoint Detection and Response (EDR):** EDR solutions come with the ability to provide visibility on installed software on devices and vulnerabilities for the applications.
* **Vulnerability Management:** Authenticated vulnerability scans can show installed software and vulnerabilities, this is very similar functionality to EDR.
* **Cloud Access Security Broker (CASB):** A CASB solution provides visibility coupled with a risk scoring of SaaS applications and can be used to build a database of consumed SaaS.

**Technology that can used to enforce the use of software:**

* **Groups policy objects (GPO):** GPO’s can enforce application controls on Windows devices.
* **Endpoint Detection and Response (EDR):** EDR can allow or deny applications, scripts, and libraries through policies. The policies can be grouped to allow for differing levels of use, depending on the use case.
* **Cloud Access Security Broker (CASB):** A CASB can allow or deny access to specific SaaS applications and/or tenants.
* **Just in time privileged access management:** Privileged access management can allow only certain people access to install software on the device. A reason is required and control over permissions to enforce the installation of software.

**Governance around software asset management:**

* Review asset management technology and operating model on a regular basis
* Review controls that are in place for software asset management
  + 1. Vulnerability Management and Patching
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 3 | **Continuous Vulnerability Management** | Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. |

* + - 1. Vulnerability Management and Patching Overview

Vulnerability management (VM) is one of the most important areas that the business needs to address for reassurance that vulnerabilities are detected and mitigated against in a timely fashion. If critical and high CVSS scored vulnerabilities exist, hackers will find, target, and exploit these known vulnerabilities.

Having robust vulnerability management and pathing process will greatly reduce the attack surface of the organisation. The process consists of:

1. Roles and responsibilities should be clearly defined for all aspects of the VM and patching process. Timescales for patching vulnerabilities based on criticality should be defined along with the timescales for review of patching.
2. Determine all hardware and software assets and utilise all technology solutions that are available. If possible, centralise all vulnerability management data for review.
3. Perform regular vulnerability scanning on all assets, where automation is not available a periodic manual assessment should take place.
4. Prioritise patching for vulnerabilities that are detected, high and critical CVSS scores should be patched at the earliest opportunity. Lower CVSS scores should be address by the usual patching period.
5. Review the patching of vulnerabilities in a timely fashion to ensure all patching has been actioned. If there are system that cannot be patched in a timely fashion due to operations or other factors. Other compensating security controls should be put into place.
6. Review the entire vulnerability and patching process in a regular basis to make improvements where required.

Ensure that all assets are covered in the vulnerability detection and patching process. For areas that do not have an automated scanning process, a periodic manual assessment should take place with audit and review measures in place. This is usually true for OT/IoT and network devices where there may not be vulnerability management automation tooling in place.

Technology and sources for detecting and managing vulnerabilities:

* **Remote Vulnerability Scanning:** Remote vulnerability scanning is useful for discovery and devices that are not able to accommodate local authenticated scans. It is advised that authenticated scans are performed over remote scanning.
* **Authenticated Vulnerability Scanning:** Authenticated vulnerability scanning will produce more information on the system, services, and applications as direct access to the system is available.
* **Endpoint Detection and Response (EDR):** Many EDR vendors provide a packaged vulnerability management solution within their product setthat can be used instead of a ‘pure’ vulnerability management solution. With good management and integration, EDR can be a good VM solution.
* **Security Content Automation Protocol (SCAP):** SCAP has the ability to scan the system for vulnerabilities of the system and installed software.
* **Vendor News feeds:** Vendors provide up to date vulnerability information for their products. Subscription to vendor vulnerability feeds is recommended.
* **Industry Vulnerability Management Data:** NVD, CERT and CVE data is freely available to review for specific systems and software in the business.

**For the governance area the following are recommended:**

* Prioritise vulnerability patching.
* Review patching process on regular basis.
  + 1. Secure Configuration
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 5 | **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers** | Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |
| 11 | **Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** | Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |

* + - 1. Hardware, System, Software (Application), and Network Hardening

System and service hardening for all types of infrastructure components is essential to ensuring that the attack surface is reduced as much as possible. All hardware, systems, software applications, services, and network devices should use security baseline templates.

Baseline templates and tooling can be obtained for a variety of places and technologies:

* **The Centre for Internet Security (CIS) benchmarks**: The CIS benchmarks are the industry standard for securing systems and applications. The benchmarks go through rigorous testing and peer review to ensure the best security hardening. More information can be found here: <https://www.cisecurity.org/cis-benchmarks/>
* **Vendor recommendations**: Vendors publish hardening documentation and security recommendations that should be considered.
* **Security Content Automation Protocol (SCAP):** To guard against security threats, organizations need to continuously monitor computer systems and applications they have been deployed, incorporate security upgrades to software and deploy updates to configurations. The Security Content Automation Protocol (SCAP) pronounced "ess-cap", but most commonly as "skap" comprises several open standards that are widely used to enumerate software flaws and configuration issues related to security. Applications which conduct security monitoring use the standards when measuring systems to find vulnerabilities and offer methods to score those findings to evaluate the possible impact. Most larger vendors do provide SCAP capable scanning and remediation software, another useful source is OpenSCAP: <https://www.open-scap.org/>
* **Security Tooling:** There are some specialised tooling that can be used to continuously monitor and remediate secure configurations. An example of this type of solution is Gytpol: <https://gytpol.com/>
* **Cloud Security Posture Management (CSPM):** A CSPM provides posture assessments in IaaS, PaaS environments.

**With regards to governance the following actions are recommended:**

**Audit:** Audit all elements in the business that will require hardening. A hardware and software inventory can be used to inform of assets. This would include all network devices, operating systems, IOT/OT devices, services, applications, and service accounts.

**Establish a written standard and formalise:** Establish a written standard for all assets that require hardening and formalise the process to implement, test, and deploy.

**Review 3rd party templates:** Where required review any 3rd party hardening templates to ensure best security practices are being observed. Consider using baseline security technology to audit 3rd party managed devices.

**Periodic Review:** A periodic review annually or bi-annually to make any changed required to hardening and/or business processes.

* + 1. Logging
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 6 | **Maintenance, Monitoring and Analysis of Audit Logs** | Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack. |
| 16 | **Activate Audit Logging** | Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them. |

* + - 1. SIEM/XDR Overview

A SIEM system provides a central console for viewing, monitoring, and managing security-related events and log data from across the enterprise. Because it correlates data from multiple sources, a SIEM system can enable an analyst to identify and respond to suspicious behaviour patterns faster and more effectively than is currently possible by looking at data from individual systems. Log data represents the digital fingerprints of all activity that occurs across a networked infrastructure—it can be reviewed to detect security, operations, and regulatory compliance problems.

To be effective, a SIEM must remain relevant in the face of new threats and changes in both the technical and support infrastructures of an organisation. Yet, legacy SIEMS are notorious for being difficult to configure and maintain. The average shelf life for a traditional SIEM is 18 to 24 months. Furthermore, because a conventional SIEM often fails to produce actionable information, the security team may be unable to justify ongoing investment costs such as license renewal, ongoing system management, integration of additional data sources, and continued personnel training.

Modern SIEM solutions should be viewed as the central nervous system, capturing data, and generating information that security teams can use as intelligence to detect potentially malicious activity before any damage is realised whilst providing a safety net that can catch potential threats that might slip through traditional cyber defences.

Because of these issues, demand arose for tools that can provide actionable information while optimising current and future security investments and reducing risk. Next-generation SIEM augments traditional capabilities (automated log management, correlation, pattern recognition and alerting) with emerging and agile technologies (cloud-based analytics; security orchestration, automation, and response [SOAR]; user and entity behaviour analytics [UEBA]; machine learning and artificial intelligence).

* + - 1. Core Capabilities of Next Generation SIEM/XDR

Modern-day SIEM’s still need to provide core functionality to the business, improving on their predecessors’ perceived weaknesses. However, the SIEM forms the foundation of an organisation’s security operations, and as such, should fulfil core operational requirements for security teams. These are mapped to core needs in the table below.

|  |  |
| --- | --- |
| Need | NextGen Capabilities |
| Manage and monitor the modern hybrid infrastructure (e.g., cloud, on-premises, in the hands of users) as a single entity. | • Permit quick integration into an enterprise infrastructure via open architecture  • Meet operational demands of complex, global environments both in terms of performance and maintainability due to scalable architecture |
| Visualize related security events across disparate datasets for accurate incident identification and threat detection. | • Curate standard taxonomy of activities from log and machine data  • Employ real-time visualization tools that help gain insight into the most important, high-risk activities |
| Detect, classify, escalate, and respond to threats in real-time. | • Use scenario- and behaviour-based analytics to capture well-understood scenarios and indicate significant changes in behaviour  • Integrate with and use threat intelligence gathered from commercial, open-source and custom sources |
| Search efficiently against massive amounts of data captured from various sources, quickly homing in on the data most pertinent to forensic investigation. | • Provide precise and rapid access to data through high-performance and centralized searches on both structured and unstructured data  • Rely on high scale indexing and storage of forensic data for months or even years  • Use big data architecture to allow storage of source data in its historical or original form  • Enable search capabilities |
| Manage and improve repetitive workflows, adjusting to changing organisational needs, policies, and systems (e.g., guide incident response more rapidly and accurately after threat detection occurs). | • Support SOAR capabilities  • Provide a flexible framework that allows custom workflow implementation for key organisational use cases (e.g., Secure DevOps, incident response) |
| Represent and manage business risk in terms of organisational compliance and other mandates. | • Measure current status against a regulatory and other policy-based frameworks for risk prioritization and management via a rules engine  • Provide standard (e.g., PCI DSS, HIPAA, SOX) rule sets that are customisable and extensible |

* + - 1. SIEM vs XDR

##### Dictionary Definition of a SIEM

*“Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).”*

* *Gartner*

##### Dictionary Definition of an XDR Tool

*“Extended detection and response (XDR) is defined as an extension of endpoint detection and response (EDR), with the intention of expanding the sources of telemetry beyond the endpoint and streamlining response. The required XDR capabilities can be provided by a single vendor or as a hybrid solution composed of products from multiple vendors.”*

* *Gartner*

Table comparison:

|  |  |  |
| --- | --- | --- |
| Categories | NG-SIEM | Open XDR |
| Deployment | Generally, more complex deployments that require a “tiered” architecture approach. Most Vendors now offer the core components of the SIEM such as detection engines and storage, as cloud-hosted however, so deployments are more simplified. | Exclusively cloud-based and very short deployment timeframes. Only on-premise footprints are normally log collectors. As open XDR tools work within data lakes, a lot of standard integrations or “connectors” are included within the product, which makes onboarding very simple. |
| Design Approach | Designed for “just in case” situations and customised security use cases. | Very much focused on the detection, investigation and response against threats. |
| Data Location | Assumes that all data must be stored within the SIEM platform itself. | Operates on back-end data storage that does not form part of the core architecture of the XDR tool itself. |
| Storage Requirement | Offers infinitely scalable storage for retention requirements. | Although extended to offer up to and over (in some cases) 12 months of storage. XDR solutions typically do not offer longer term retention and storage. |
| Detection Approach | Traditionally focused on correlation-based attributes. Pattern matching across large data sets ingested in to the SIEM. | Offers a more advanced, machine learning based approach to detection. Algorithms that look for anomalous activity and deviations in data. |
| Automation Approach | Very flexible and highly customisable automation and orchestration features. | Often bundle pre-packaged automation into the XDR product, with pre-set playbooks and orchestration actions. |
| Market Space | Typically renders legacy SIEM’s defunct and replaces them. Often newly adopted with a cloud first approach. | Can be used to replace legacy SIEM’s and in more advanced SOC’s, used to augment SIEM’s for a hybrid SOC technology model. Wholly replaces any existing MDR or EDR services. |

* + - 1. Event Logging

Is recommended to implement an Endpoint Detection and Response solution where possible that can provide the most valuable telemetry directly from the endpoint device. This logging along with other types of logging can be captured centrally and analysed using a SIEM or XDR solution. The solution would be dependent on the operating model that the business employs.

Logs to ingest from technology areas:

* Endpoints (EDR)
* Firewalls (IPS, IDS)
* Audit logs from servers and network devices
* Secure Web Gateways and Cloud Access Security Brokers
* Cloud IaaS and PaaS environments
* Identity Providers (AD, AAD)
* Data Prevention Technology
* Email Gateways
  + 1. Identity Provider and Governance
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 4 | **Controlled Use of Administrative Privileges** | The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. |
| 14 | **Controlled Access Based on the Need to Know** | The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. |
| 16 | **Account Monitoring and Control** | Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them. |

* + - 1. Identity and Access Management (IAM) Overview

There are two main areas in which identity and access management should be addressed when implementing security controls in this area. The first being business and processes and the second focusing on technical aspects:

* **Business and Processes:** Focus on high level business requirements, governance, and processes.
* **Technical:** Focus on technical requirements, assets, Role Based Access Control (RBAC) and Discretionary Access Control (DAC) models.

**Business and Processes:**

* **Governance**: A robust governance framework is required to implement policies and procedures for joiners, movers, and leavers.
* **Human Resources (HR):** HR is usually the primary directory for staff in the business were good communication and workflows with other departments
* **Help Desk:** The help desk will provide changes for joiners, movers, and leavers
* **IAM Use Case Definitions:** Define IAM use cases for the business
* **IAM Strategy:** The IAM strategy encompasses all elements with regards to identity and access management and would include all areas outlined in this section.

**Technical:**

* **Assets:** Assets are critical for IAM implementation. Knowing what systems, applications, and those that can be integrated into an IdP is essential. Also, what users need to have access too.
* **Privileged Access Management (PAM):** Privileged Access Management is where any privileged user needs access to a system or application: The main features of a PAM solution:
  + ‘Jump box’ like functionality where administrators must use a session manager to gain access to a system/application
  + Password rotation
  + Session recording
  + Just in time privileged access
  + Local administrative account access
  + Break glass accounts
  + Service account management
  + Database access control
* **Identity Governance and Administration:** An IGA solution is used to automate and manage identity and access management in the business.
* **Single Sign-On (SSO) and Self-service password reset (SSPR):** SSO and SSPR should be considered where required.
* **Analytics, Reporting, and Audit:** Part an IGA of some SSO, identity provider platforms. The analytics and reporting can be used for incident response, and all areas can be used for compliance purposes.
* **Access Control Models and Identity Provider (Directory):** 
  + **Role-based Access Control (RBAC):** RBAC is used in many areas of security where users are grouped into roles. With the advent of the zero-trust model where identity-based security is used pretty much everywhere in the infrastructure today.
  + **Discretionary Access Control (DAC):** DAC is an important piece in identity and access management were managers and business data owners can give access to applications. This type of access control can be used with RBAC and is best implemented using an IGA or workflows in the helpdesk.
  + **Identity Provider (IdP):** The IdP is the ‘engine’ for identity where a directory is used to integrate with other infrastructure components using open standards. The two most popular IdP’s are Active Directory and Azure Active Directory.
    - 1. Least Privileged

The principle of least privilege (PoLP) refers to an information security concept in which a user is given the minimum levels of access – or permissions – needed to perform his/her job functions. It is widely considered to be a cybersecurity best practice and is a fundamental step in protecting privileged access to high-value data and assets. Least privilege extends beyond human access. The model can be applied to applications, systems or connected devices that require privileges or permissions to perform a required task. Least privilege enforcement ensures the non-human tool has the requisite access needed – and nothing more. Effective least privilege enforcement requires a way to centrally manage and secure privileged credentials, along with flexible controls that can balance cybersecurity and compliance requirements with operational and end-user needs.

##### What is Privilege Creep?

When organizations opt to revoke all administrative rights from business users, the IT team will often need to re-grant privileges so that users can perform certain tasks. For example, many legacy and homegrown applications used within enterprise IT environments require privileges to run, as do many commercial off-the-shelf (COTS) applications. For business users to run these authorized and necessary applications, the IT team must give local administrator privileges back to the users. Once privileges are re-granted, they are rarely revoked, and over time, organizations can end up with many of their users holding local administrator rights again. This “privilege creep” reopens the security loophole associated with excessive administrative rights and makes organizations – that likely believe they are well-protected – more vulnerable to threats. By implementing least privilege access controls, organizations can help curb “privilege creep” and ensure human and non-human users only have the minimum levels of access required.

* + 1. Email Security
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 7 | **Email and Web Browser Protections** | Minimize the attack surface and the opportunities for attackers to manipulate human behaviour though their interaction with web browsers and email systems. |
| 12 | **Boundary Defense** | Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. |

* + - 1. Email Security Overview

It is advised that a registry of all email domains is available to ensure that there is visibility for all email transactions in the business. Also, all technology that is used in the business the business should be considered as certain departments like marketing may use specific email distribution systems. If the security controls are put into place this could ‘break’ the functionality of these systems if the email routing is not taken into account.

Email security can split into both inbound and outbound features:

##### Inbound Email

Inbound email scanning is in place using Trend Micro, it is advised that the correct policies are implemented and audited to ensure all capabilities are enabled to satisfy the business control risk and operational levels.

General features:

* **TLS on SMTP**: Transport Layer Security should be enabled to receive emails over a secure channel when available.
* **Malware scanning/Sandboxing**: Inbound malware scanning and sandboxing of files entering the organisation via email.
* **SPF/DKIM/DMARC**: Adhere to inbound DMARC policies and check for SPF and DKIM with appropriate policies in place.
* **Spam Filtering:** Basic spam filters and scoring should be in place.
* **Threat Intelligence** – Threat intelligence should be in use to provide up to date protection against attacks such as phishing.
* **URL replacement/scanning:** Replacement URL’s should be added to egress (exit) through a secure web gateway with inbound scanning to ensure malicious links are removed.
* **File extensions policies:** File extensions should be restricted.

##### Outbound Email

Outbound email security ensures that emails sent by the business cannot be spoofed to other organisations/people. Hackers can use the method of spoofing from domains to try a gain a foothold via email viruses/social engineering. \*\*\* have some domains that use SPF which does give a level of protection. SPF, DKIM, and DMARC should be implemented to give a better level of email integrity and protect against spoofing.

It must be noted that the receiver side of the email transaction also needs to implement these technologies, currently all major email providers and many organisations have adopted SPF, DKIM, and DMARC.

* **Transport Layer Security (TLS):** TLS should be enabled to send emails over a secure channel when available.
* **Sender Policy Framework (SPF):** SPF is used for authorising the sending mail servers (IP/hostname) via a DNS entry for the domain.
* **DomainKeys Identified Mail Standard (DKIM):** DKIM is used by signing the email that is check and verified by the receiver using a DNS entry. This ensures that the
* **Domain-based Message Authentication Reporting and Compliance (DMARC):** DMARC unifies SPF and DKIM by providing policies (set by the sender in DNS) that receiving email services can implement. The policies declare how the email from that domain should be handled if it fails the authorisation test for SPF and DKIM. The policies can be to do nothing, reject or quarantine. Another aspect of DKIM in the reporting, this is useful to request information for domains that have received email from your domain. The information can be used to identify if your domain is being spoofed by outside parties.
* **Data Loss Prevention (DLP):** DLP is a crucial element to emails leaving the organisation. If classification and labelling has been implement, these can be used to restrict sensitive data from leaving the business. Also, there are other technologies that can detect inline sensitive data and restrict as per the company policies.

## End USer, Internet of Things/Operational technology Security Services

* + 1. Single Sign-On (SSO)
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 4 | Controlled Use of Administrative Privileges | The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. |
| 13 | Data Protection | The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. |
| 14 | Controlled Access Based on the Need to Know | The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. |

* + - 1. Single Sign-On Overview

Single sign-on centralises web application/sites security controls by either allowing or preventing authentication. A user will only have access to applications that are presented to them. Role based access (RBAC) control can be used to build out groups of users that need access easing the overall administration and providing better security around access to applications.

The other added benefit is that a user does not have to remember multiple passwords which will streamline the authentication point for the end user.

Most organisations will use their primary identity provider (IdP) along with a single sign-on method: Open ID Connect, OAuth, SAML, Header based, LDAP etc. This enables a central point to manage credentials for users, multi-factor authentication should also be implemented when using SSO.

There is the caveat that the application must support an SSO method, it is advised that the organisations software inventory includes application SSO capability and those that do not.

Integration into the identity access and management (IAM) process should be done where appropriate.

There are two main use cases for SSO:

1. **Application SSO**: Application SSO enables an end user to access enterprise applications with the help of SAML authentication. As the user logs into the system using an identity integrator, the credentials are stored by the identity provider. And, when the user tries to access any application, the service provider (application) requests the identity provider for authenticity of the user and the identity provider validates the user’s identity, granting the end user access to the application.
2. **Privileged SSO**: Privileged Single Sign-On is a type of SSO Authentication focused mainly on privileged users who require access to administrative or super user accounts to connect to any resource or application. The PAM agent stores credentials of such administrative accounts centrally in the vault, and whenever the user tries to access any resource, it passes on those credentials directly from the vault to the resource and validates his/her identity, enabling a secure way for the privileged user to access a wide variety of resources including Windows Machines, Databases, Routers, Switches, Application and more depending on the privileges he/she has been granted.
   * + 1. Summary

* Use SSO on all applications where possible
* Implement MFA with single sign-on
* Use with IAM processes
* Role based access control (RBAC) is recommended
* Utilise the software inventory to ensure all SaaS applications are covered
  + 1. Data Loss Prevention (DLP)
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 13 | **Data Protection** | The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. |

* + - 1. Data Loss Prevention (DLP) Overview

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of [sensitive data](https://test.imperva.com/data-security/compliance-101/sensitive-data/). Organizations use DLP to protect and secure their data and comply with regulations.

The DLP term refers to defending organizations against both data loss and data leakage prevention. Data loss refers to an event in which important data is lost to the enterprise, such as in a [ransomware attack](https://www.imperva.com/learn/application-security/ransomware/). Data loss prevention focuses on preventing illicit transfer of data outside organizational boundaries.

DLP can cover all areas of technology and governance in the business, with this in mind there are many areas of that need to be considered when implementing data loss prevention:

##### Governance

Data Loss Prevention (DLP) should start with governance in the organisation to understand the overall ‘data landscape’. The following areas should be addressed in this area.

* Identify data management and security policies and procedures that already exist in the organisation.
* Data risk assessments.
* Cost of a breach.
* Regulation requirements.
* People: Awareness, Accountability, Responsibility.
* Gap analysis.
* Identify stakeholders
  + Data Owners - The owner of the data asset and is responsible for the asset. They can also influence the classification of data.
  + Data Stewards - Can be known as data champions are responsible for taking care of the data.
  + Data Custodians – Make decisions on onboarding, maintenance, and end-of-life updates of the data assets. Utilise the data lifecycle management process.
  + Data Governance Committee – Develop and maintain data policies and procedures.

##### Content Awareness

Content awareness is used to identify the context or content of data in the organisation:

* **Contextual awareness**: Identify the business context of data within the organisation, some examples:
  + Ownership and permissions.
  + Encryption, file formats and network protocols.
  + User roles and business units.
  + Web services.
  + USB device information.
  + Desktop applications.
* **Content awareness**: What types of content analysis is needed:
  + Rules-Based/Regular expressions – Use rules to identify structured data.
  + Database Fingerprinting – Analyse data from databases.
  + File Matching – Analyse file types.
  + Partial Document Matching – Unstructured data for protecting sensitive documents.
  + Statistical Analysis – Use machine learning to identify policy violations.
  + Categories – Pre-built rules such as credit card numbers, PII.

##### Threats and Risks

Threats and risks to all data should be considered to ascertain the level of controls that are appropriate to the business. A list of examples to identify threats and risks:

* Who has access to critical data.
* Current access rights to critical data.
* Current data controls in place.
* Malicious activity:
  + Access right violation
  + Exploitation
  + Developer’s trust (abuse of privilege)
  + Unsupervised office (Staff screenshot to an external actor)
  + Employee discontent
  + Insider Trading
* Data loss causes:
  + Process: Governance, Data Retention, Data Monitoring, Incorrect Classification, Accelerated change control plan.
  + Technology: Hardware theft, Unencrypted data, Inheriting data, Unnecessary services, Data transfer (USB), Cybercrime (APT).
  + Human error, Insiders.
  + Printable copies.

##### Identification and Data Management

The following items outline the areas that will need to be addressed to ensure effective data identification and management:

* Data management lifecycle. *See next section.*
* Data usage monitoring.
* Identify high-risk data and prioritise accordingly.
* Identify exfiltration methods that are in scope.
* Any examples of root cause analysis for historical data loss.
* Classification classes data based on data risk.
* Risks associated with data types.
  + Customer data
  + PII
  + Transactional data
  + Corporate data
  + Intellectual Property
* Labelling (metadata).
* Tooling (discovery).
* Location of data (Physical and Logical).
* Third-party data access.
* View only access rights.
* DLP Policy Requirements
  + Identify high-level policy requirements.
  + Built-in rules and addition custom rules.

##### Data Movement (Lifecycle)

Finally, identifying data movement in the business will help to identify all the areas where controls could be placed. This is not an exhaustive list but will indicate the primary areas to assess. There are three main areas: Data in motion, Data in use, and Data at rest.

* Data in motion
  + Perimeter.
  + Network monitoring.
  + Internet access control.
  + Third-party exchange – Email, FTP, API.
  + Instant messaging, Social media, Web apps, etc.
  + Remote access.
  + Scanning tools.
  + Encrypted traffic.
* Data in use
  + Privileged user monitoring.
  + Access usage/monitoring.
  + Data sanitation.
  + Test data.
  + Data redaction.
  + Copy/Paste/Save control.
  + Application control.
  + Screenshots.
  + DRM.
  + Email client.
  + Cameras.
* Data at rest
  + Endpoint Security – AV, EDR, etc.
  + Host encryption.
  + Mobile device protection.
  + Network-based access control.
  + Physical media control.
  + Data erasure and wiping.
  + File shares.
  + Databases.
  + Document management systems.
  + Hard copies.
    1. Key/Password Management
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 4 | **Controlled Use of Administrative Privileges** | The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. |
| 14 | **Controlled Access Based on the Need to Know** | The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. |
| 16 | **Account Monitoring and Control** | Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them. |
| 18 | **Application Software Security** | Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. |

* + - 1. Application Key Storage

Keys that are stored in code should not be ‘hard coded’ in files that are used in application. A secrets manager can be used to provide security around keys in code, thus making the application more secure.

Most systems and coding languages provide some method of secure key storage and should be utilised.

* + - 1. Public Key Infrastructure (PKI) Management

PKI management is a term used to encompass a lot of tasks and responsibilities necessary for upholding a fully functional and effective public key infrastructure.

The concept includes PKI certificate management, authorizing public and private keys, and critical decision making regarding private key storage, as well as the misuse or loss of a private key. The role is highly complex, which is why it’s always best to enlist the help of a seasoned professional to protect the privacy of your electronic data.

PKI certificate management involves the generation of PKI certificates, suspending or revoking digital certificates, and managing distribution, renewals, and other PKI best practices that keep your public key infrastructure functioning at an optimal level.

* + - 1. Password Vaults

Password vaults for staff are highly recommended to ensure safe storage, auditing, and access of passwords. If the user has the option to use single sign-on, this would be a preferred method along with multi-factor authentication.

Users that have a requirement to use multiple passwords, a password vault is recommended.

General features provided by password vaults:

* Enforcement of security protocols to reduce risk
* Insight into password behaviour
* Security and login reports for compliance
* Reduce password reuse
* Enforce password rotation

There are two main use cases for password vaults:

* **General Users:** General staff would be under this category.
* **Privileged Users:** Privileged users would be IT staff, and users that have any privileged or administrative access to assets. Note: in some cases, a full privileged access management (PAM) solution includes password vaults.
  + - 1. Hardware Security Module (HSM) and Trusted Platform Module (TPM)

For a higher level of key storage and security a hardware security module could be considered to secure and create key material used for PKI and other types of keys in the business. The trusted platform module comes with most computer hardware today and can be used to secure keys:

* TPMs are primarily used for key storage
* Hardware Security Modules (HSMs) are hardened, tamper resistant hardware devices that that protect cryptography keys used for such functions as encryption, digital signing, and key generation.

HSMs typically have two primary, closely related functions. The first function is hardware enabled / accelerated cryptographic functions including encipherment, decipherment, key generation, PRNG functions, and related signing/signature validation functions.

TPMs are meant to provide a hardware root of trust to enable secure computing by providing a secure key storage enclave with minimal cryptographic functions primarily in the signing and signature verification space. The primary use cases are storage of drive encryption keys and validation of signatures on boot loaders, kernels, and device drivers. Note, much of this can be accomplished without a TPM (secure boot with bios that support Windows WHQL including default Microsoft keys), password-based disk encryption.

* + 1. Web Security
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 7 | **Email and Web Browser Protections** | Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems. |
| 12 | **Boundary Defense** | Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. |

* + - 1. Overview

Web security is critical to ensure users are accessing safe and sanctioned content on the Internet, SaaS applications, IaaS, and PaaS environments. On-premise web applications can also be included and secured depending on the use case, this usually being hybrid or remote workers.

Web security can cover many components and can be deployed in a few ways. The primary recommendation is to use a SASE or SSE model using a security SaaS model as opposed to an on-premise solution.

Main web security components (Note: this is not the full list of SASE elements, only web security):

* Secure Web Gateway (Web proxy)
* Cloud Access Security Broker (CASB)
* Remote Browser Isolation (RBI)
* TLS Decryption
* Threat Prevention
* Anti-Malware

Deployment methods:

* **On-premise:** The on-premise or traditional security web controls where users are ‘back hauled’ through a data centre via VPN, or are in an office where web traffic is ‘pushed’ through a web proxy. An on-premise solution will generally only comprise of a secure web gateway, other features such as CASB are only provided with a SASE solution.
* **Secure Access Service Edge (SASE):** An agent-based solution that can be used for remote or office workers where all web traffic is tunnelled through a ‘secure edge’. It is more dynamic and generally contains more security features than an on-premise solution.
  + - 1. Secure Access Service Edge (SASE)

SASE (pronounced "sassy") is a model put forward by Gartner in August 2019. This newly introduced concept directly responds to a changing landscape, i.e., adoption of SaaS (software-as-a-service) applications, overall increase of internet traffic, remote working, branches offices requiring direct internet access (DIA). Organisations moving away from a centralised ingress/egress point once filtered/analysed all traffic, including Internet-bound, through a single stack of security appliances located on the perimeter. The changes have led to administrators losing vital visibility of an ever-growing attack surface susceptible to exploits.

Demand for a flexible, agile workforce with uninterrupted access irrespective of location has spiked sharply, calling for the functionality of multiple point solutions to provide depth in defence (DiD) with security embedded within all layers rendering the securing of SaaS, PaaS and IaaS using traditional ('back haul') security methods as inefficient.

The need arose for a consolidated approach, with a replicational framework for a validated design capable of providing a robust cloud-driven security solution. Shifting the network security perimeter to the cloud and facilitating centralised management controls for more efficient administration with data and be more user-centric. Using the SASE model allows the organisation to re-think how security architecture is implemented, moving away from a network-centric approach reliant on Layers 1,2,3,4 of the OSI model to one that is associated with identity, device, location, privilege level and UEBA analytics (behaviour) and what authorisation is required. Context is critical and a guide to how deep the SASE implementation needs to be.

Contextual factors include:

* The identity of the user.
* The device being used to request access.
* The location from which access is being attempted.
* Identification of cloud applications.
* The data that is being requested.
* User behaviour.
* Application authorisation.

On top of context, security policies are applied based on the information evaluated; these policies will determine the following:

* The access level of services and types of network services to apply.
* What types of data encryption is used?
* The level of data protection to apply.
* The level of authentication required.
* Does the application require additional security services, such as SWG, DLP and CASB?

All things happen in real-time and continuous risk management throughout a SASE architecture, guaranteeing an increase of security, user experience, and network connectivity improved drastically subject to a satisfactory implementation.

* + - 1. SASE Benefits

As SASE is a single service, it cuts complexity and costs. Adopting OpEx over CapEx, SASE is a SaaS-based solution removing the need for ongoing management of the many on-premise infrastructures.

SASE also enables IT agility, security and reliability, greater visibility and transparency, consistent security enforcement and network performance. Whilst the initial implementation needs detailed planning, the long-term benefits for the organisation outweigh this shift of paradigm.

* + - 1. Where and What is the Edge?

An edge is where the SASE solution is delivered; this is through Point of Presence (PoP), Internet service providers and content delivery networks data centres. The PoP's are a vital backbone; using this connectivity method where PoP's worldwide are leveraged, allowing users and devices to connect into the SASE solution with minimal latency. When combined with the backbone networks that the SASE vendors use enables an enhanced user experience. Most SASE providers will also peer with major cloud providers and SaaS providers, further reducing network latency. \

* + - 1. Secure Web Gateway (SWG)

A secure web gateway ensures that all web traffic (HTTP/HTTPS) is secured by using various technologies; some SASE providers will bundle some of these features into other technology areas of SASE. The SWG is usually deployed as a forward proxy where access is controlled by an agent on a device and/or user authentication.

The core technologies:

**Monitoring & Analytics**: Monitoring and analytics are used for reporting and understanding user behaviour in real-time.

**Threat Prevention**: Protects against malware, advanced threats using sandboxing, threat intelligence, behaviour analytics and machine learning analysis. Files or other malicious content will be blocked or quarantined using these methods.

**Web-Based Applications**: The ability to create policies around what type of application is used, such as Skype, IM, Team, etc.

**URL Filtering**: Filtering URL's use either singular category policies so organisations can block or allow what users can access from the corporate network environment. URL blocklist are also used based on the latest threat intelligence to stop any user from accessing a malicious site.

**TLS Decryption**: TLS session decryption is used to inspect the encrypted traffic so the content can be analysed. Polices can be placed to ensure that specific sites like banking and contain personal information will bypass decryption.

**Data Loss Prevention**: Data loss prevention technologies will be incorporated into the SWG or use external technology.

* + - 1. Cloud Access Security Broker (CASB)

A cloud access security broker delivers security for a data path between a user and a cloud service (SaaS application).

Three methods of deployment for a CASB solution:

Used as a proxy agent where software is installed on an end device to 'steer' traffic to the CASB.

A reverse proxy is put in place between the user and the website that is being accessed; when the user accesses the website, they are redirected to the reverse proxy where the CASB is located. The SaaS applications must have the capability to integrate with the CASB solution for this to work.

Using API integration, this is a so-called 'out of band' security control where the CASB uses an API to detect any behaviours that have taken place in the application using the API. The API method is not real-time hance the 'out of band' term but can use policies to change data within an application if required. For example, a user uploads a malicious file to a file-sharing SaaS application; the file can be deleted if the policy is set.

A unique selling point of a CASB is enhanced visibility within an organisation of cloud applications that are utilised by users, providing the ability to see what is being used allows IT/Security staff to assess if the application is safe, confirms with compliance, highlights licensing requirements, and uncovers shadow IT applications that the organisation has not sanctioned.

The majority of leading CASB solutions provide a risk scoring for cloud applications, allowing administrators to efficiently build security policies based on a known risk score of applications. Administrators can make informed decisions about what applications are benign "safe" to use and those that are not.

Compliance is another example of where a CASB can aid an organisation, designed to ensure safety and privacy of personal and corporate data allowing simplicity and efficiency of complying with regulations set forth.

Data security or data loss prevention is included in all CASB provider solutions. Mitigating sensitive data from interception and exfiltration. A CASB also stops users from using social media and personal applications to send data through unmonitored backdoor channels within an organisation.

Threat prevention is also available in a CASB to stop any malicious data entering or leaving an organisation. User behaviour analytics is used to indicate an attack or data breach. Encryption at rest can be implemented to ensure data is encrypted in cloud applications.

* + - 1. Remote Browser Isolation (RBI)

Also referred to as web isolation or browser isolation is an advanced cybersecurity technique that provides an additional layer of protection for users and organisations. Browser isolation separates browsing activity from endpoint hardware, thereby reducing the device's attack surface.

**Enables safe access to web content**: It isolates users from web apps and delivers a safe rendering of web content—without requiring an endpoint agent on every device.

**Protects sensitive data**: It protects users from targeted attacks hidden in web pages, downloadable web content, and vulnerable plug-ins.

**Removes the threat of data exfiltration**: It eliminates the ability for a webpage to exfiltrate data or compromise a user's machine, even if the browser is outdated, vulnerable, or has unsafe plug-ins installed.

**Allows broader internet policies**: Enables organisations the ability to minimise policy complexity, reduce risk, and implement more open policies for internet access.

* + 1. DNS Security
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 7 | **Email and Web Browser Protections** | Minimize the attack surface and the opportunities for attackers to manipulate human behaviour though their interaction with web browsers and email systems. |
| 8 | **Malware Defences** | Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action. |

* + - 1. DNS Security Overview

DNS queries supersede a three-way-handshake and can block (blackhole) sessions when necessary. Leveraging a list of automated threat feeds of domains both known to be malicious and unknown. Provides granularity to administrators to create organisational policies that can be implemented to block any queries of these domains, thus further protecting the source user from malicious destinations.

Using DNS security is a fast way to implement security policies as the DNS lookup is performed before any data is accessed from the Internet with the added benefit of being port and protocol agnostic. With telemetry in mind, providers have advanced reporting and data analytics associated with a user (via an IdP).

Role based access control is recommended to build out more easily managed policies.

General features provided by DNS Security:

* Blocklist and category DNS blocking for domains
* The ability to stop ransomware, trojans, and other malware without requesting any data from a domain
* Machine learning to block domains that are deemed malicious
* Integration into a directory such as Azure AD to build out user and role-based policies
* Reporting and analytics for users and domain
  + 1. Network Access Control
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 1 | **Inventory and Control of Hardware Assets** | Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. |
| 9 | **Limitation and Control of Network Ports, Protocols, and Services** | Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers. |
| 14 | **Controlled Access Based on the Need to Know** | The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. |
| 15 | **Wireless Access Control** | The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems. |

* + - 1. Network Access Control Overview

Network Access Control (NAC) is a solution that uses a set of protocols to define and implement policies on how to provide secure access to the network by devices when they are initially attempting to access the network.

NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches, and firewalls to work together with back-office servers and end user computing equipment to ensure the information system is operating securely before interoperability is allowed. A basic form of NAC is the [802.1X](https://en.wikipedia.org/wiki/802.1X) standard.

Main features of Network Access Control:

* Mitigation of [zero-day attacks](https://en.wikipedia.org/wiki/Zero_day_attack).
* Authorization, Authentication and Accounting of network connections.
* Encryption of traffic to the wireless and wired network using protocols for 802.1X such as EAP-TLS, EAP-PEAP or EAP-MSCHAP.
* Role-based controls of user, device, application, or security posture post authentication.
* Automation with other tools to define network role based on other information such as known vulnerabilities, jailbreak status etc.
  + The main benefit of NAC solutions is to prevent end-stations that lack antivirus, patches, or host intrusion prevention software from accessing the network and placing other computers at risk of cross-contamination of [computer worms](https://en.wikipedia.org/wiki/Computer_worm).
* Policy enforcement
  + NAC solutions allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, and [network middleboxes](https://en.wikipedia.org/wiki/Middlebox).
* Identity and access management
  + Where conventional IP networks enforce access policies in terms of IP addresses, NAC environments attempt to do so based on authenticated user identities, at least for user end-stations such as laptops and desktop computers.

Ideally all servers should authenticate to the network with certificates and users should use their user identity to authenticate.

The user authentication can be automatic when logging into systems, such as Windows. Additional certificate authentication for corporate devices issued to users should be enforced to determine corporate vs BYOD devices.

Role based access control is highly advised to segment certain groups of users to specific logical VLAN’s that have access to specific services.

* + 1. Multi-factor, Adaptive (Conditional), and Risk Authentication
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 4 | **Controlled Use of Administrative Privileges** | The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. |
| 11 | **Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** | Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |
| 12 | **Boundary Defense** | Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. |
| 16 | **Account Monitoring and Control** | Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them. |

* + - 1. Multi-factor Authentication (MFA) Overview

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

The three main authentication methods that are used to provide additional information:

* **What you know:** such as a password or PIN.
* **What you have**: such as a badge or smartphone.
* **What you are:** such as a biometric like fingerprints or voice recognition.

As MFA integrates machine learning and artificial intelligence (AI), authentication methods become more sophisticated, including:

##### LOCATION-BASED

Location-based MFA usually looks at a user’s IP address and, if possible, their geo location. This information can be used to simply block a user’s access if their location information does not match what is specified on a whitelist or it might be used as an additional form of authentication in addition to other factors such as a password or OTP to confirm that user’s identity.

##### ADAPTIVE (CONDITIONAL) AUTHENTICATION OR RISK-BASED AUTHENTICATION

Another subset of MFA is Adaptive Authentication also referred to as Risk-based Authentication. Adaptive Authentication analyses additional factors by considering context and behavior when authenticating and often uses these values to assign a level of risk associated with the login attempt. For example:

* Where is the user located when trying to access information.
* When are you trying to access company information - During normal working hours or during "off hours".
* What kind of device is used - Is it the same one used yesterday.
* Is the connection via private network or a public network.

The risk level is calculated based upon how these questions are answered and can be used to determine whether a user will be prompted for an additional authentication factor or whether they will even be allowed to log in. Thus, another term used to describe this type of authentication is risk-based authentication.

Standard signals that Conditional Access can look at when making a policy decision include the following signals:

* User or group membership
  + Policies can be targeted to specific users and groups, giving administrators fine-grained control over access.
* IP Location information
  + Organisations can create trusted IP address ranges that can be used when making policy decisions.
  + Administrators can specify entire countries/regions IP ranges to block or allow traffic from.
* Device
  + Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
* Application
  + Users attempting to access specific applications can trigger different Conditional Access policies.
* Real-time and calculated risk detection

Signals integration allows Conditional Access policies to identify risky sign-in behaviour. Policies can then force users to perform password changes or multi-factor authentication

* + 1. Wireless Security
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 15 | **Wireless Access Control** | The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems. |

* + - 1. Wireless Security Overview

##### Authentication and Encryption

Authentication for a wireless LAN should use WPA2. The IEEE 802.11i standard was defined and implemented; the IEEE 802.11i standard is also referred to as WPA2. WPA2 replaced TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which is based on Advanced Encryption Standard (AES); it is common for the WPA2 encryption method to be referred to as AES.

There are three main methods of authentication that are used on today's wireless LANs:

* **Open authentication:** The open authentication method is the simplest of the methods used and only requires that the end device be aware of the Service-Set Identifier (SSID) used on the network, if the SSID is known then the device will be allowed onto the network. The problem with this method is that the SSID is typically broadcast and if it is not, it can be easy to figure out with passive capturing techniques.
* **Shared authentication:** The shared authentication method is commonly used on individual and small business wireless LAN implementations; this method uses a shared key (Pre-Shared Key – PSK) that is given to both sides of the connection; if they match then the device is allowed onto the network.
* **EAP (Extensible Authentication Protocol) authentication:** The third method uses the Extensible Authentication Protocol (EAP) and is the most common method used by enterprises. The EAP method utilizes an authentication server that is queried for authentication using a variety of credential options.

##### Guest SSID’s

Guest SSID’s should be completely segmented for the SSID, LAN, and Internet connectivity (where possible). The Guest SSID’s can use any authentication method and should have a captive portal to agree terms of use and potentially an email address for access.

Logical or physical separation should be in place for LAN at OSI layers either/or 1 (physical),2 (logical), and 3 (IP). A firewall should be in place on the local network to ensure isolation of traffic and an IDS/IPS.

Monitoring and logging of guest Wi-fi activity should be performed to respond to any incidents. At least authentication, IP addresses, and website sites visited should be logged.

An optional secure web gateway (web proxy) can be put in place to restrict certain sites being accessed and for additional logging.

##### Corporate SSID’s

Corporate SSID’s should be using an EAP method to authenticate staff onto the corporate network using the central directory, this is usually Active Directory. Where appropriate logical VLAN’s should be mapped to SSID’s with a firewall to segment more sensitive areas of the business infrastructure.

##### Other Security Features

Some additional security features that should be considered:

* Multi-factor authentication should be considered on more secure SSID’s.
* Rogue Access Point Detection.
* Periodic password Rotation on password only SSID’s.
* Disable wireless access on devices that do not need them.
  + 1. Firewall
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 9 | **Limitation and Control of Network Ports, Protocols, and Services** | Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers. |
| 12 | **Boundary Defense** | Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. |

* + - 1. Firewall Capabilities

To defend against a rapidly expanding threat landscape in-addition to providing a future proofed environment, organisations seeking to acquire a NGFW should seek a solution that supports nine critical Network Firewall Capabilities. However please note from section 3.0. and throughout, subject to objectives set by TGM we will only focus on six of these capabilities.

##### Security Management

Effective architectures still lack robustness without the presents of full visibility. A centralised management console presenting data from multiple sources via a unified display, with the ability to effectively fulfil compliance and auditory controls is a must. The purpose of a unified display is to present operational data in a way that's easier to read and interpret. Ease of use, an efficient UI reduces the man-hours required to complete operational tasks, Threat detection with incident response life-cycle management leveraging automation and orchestration also saves on operational overheads and speeds up remediation. Interoperability with third-party IT and security solutions whether in a data centre, virtualized environment, Cloud should be centrally controlled with consistent policies across the entire security infrastructure (including but not limited to the firewalls).

##### Threat Prevention

One of the most significant capabilities added to enterprise firewalls has been the integration of robust threat prevention. Initially the focus was integration of IPS, but NGFW’s go far beyond that; sandboxing, anti-phishing, anti-virus and anti-bot are all threat prevention techniques. Many vendors use cloud-based analytics and threat intelligence in conjunction with their firewalls. These cloud platforms push and receive malware indicators and threat prevention updates, today’s enterprise firewalls must integrate with third party NAC and analytics systems that dynamically push IoCs, creating a more secure and resilient ecosystem.

##### Inspection and Control

The need for granular inspection and control has grown immensely and could be deemed directly proportional to applications becoming more sophisticated. This in-turn has driven the evolution of traditional FW functions to NGFW (Next Generation Firewall) functionality, able to strengthen security posture by mitigating against the latest known and unknown threats whilst simplifying administrative tasks, operational input and overheads. It is key to pick a firewall that has broad application support, deep (sub-functions within applications), intelligence (able to find an app even if evasion technology is used) able to dynamically apply frequent updates when applications proliferate or change.

##### Identity-Based Inspection and Control

The traditional monolithic approach to access control with network/ protocol-based firewall rules defined on IP addresses and port numbers are less effective at protecting against modern-day threats. There has been a shift to allow for policies shaped around identity access management, dynamic addressing, cloud architectures, and group-based policies. Enterprise Firewalls must support policies based on users or (more importantly) user groups. The most common situation is a group-based policy that leverages an organization’s primary IDP / identity store, typically Active Directory group membership or AAD. Policies such as these are highly effective and reduce human input/ error by automating typical processes (user moves/add/changes) which in turn decreasing the need to manually define configuration changes.

##### Cloud Support

Cloud-first / digital transformation is top priority for many organisations and is an integral means of providing the flexibility, agility and scalability needed to cope with an ever-changing landscape. A few key drivers being the shift such as moving from a CapEx model to OpEx, adoption of SaaS, IaaS and PaaS. Cloud adoption doesn't come without draw backs for example when migrating an existing workload, adoption errors are common alongside the creation of vulnerabilities due to failure to adhere to best practice and human error. The has created a need for security solutions that focus on the gaps, Firewalls must extend security to protect strategic workloads. Both hardware and software-based options to support hybrid cloud environments should be available. The ability to automation and orchestration management is crucial, scalable performance that work in tandem with dynamic workloads accompanied with a consumption model able to facilitate a cost-effective deployment.

##### Scalable Performance with Advanced Security Functions

The wide variety of services supported by next-gen firewalls requires a significant amount of compute and memory resources, which can create performance bottlenecks and affect application availability and user experience. There are multiple approaches to dealing with this consideration, all of which have their advantages/ drawbacks. However, the key requirements associated with the ability to easily scale performance horizontally when required is a must.

##### Encrypted Traffic Inspection

More than 80% of the web traffic generated by the activity of an end-user is encrypted. Unfortunately, at the same time, malware creators can leverage Certification Authority (CA) automation initiatives like encryption to create phishing sites trusted by browsers. As encrypted traffic and threats proliferate, firewalls must be capable of inspecting such traffic both to apply control policies and for threat prevention. It also must be sophisticated enough to support complex policies such as selective decryption so that certain traffic (e.g. employee’s on-line banking or other personal data) can be excluded from decryption to avoid regulatory or liability penalisation.

##### Autonomous Threat Prevention

Threat detection and prevention technology is not restricted to a single network device but rather, it’s a system of interconnected components. In addition to network security enforcement points monitoring network traffic, there are management systems that set policy, feed updates as threats change, collect log data from the enforcement points and analysis engines to find the threats in the billions of events seen daily. Threat response times are lower when infrastructure processes are autonomous and do not need manual control.

##### Security Automation

Security of the network spans more than just the infrastructure and should include identity providers/ stores, communications equipment, databases, web services, network components and most recently IOT (Internet-of-Things) devices, cloud applications/ services and workloads. Security is more robust and consistent when these systems are interconnected, e.g. firewalls connect to Windows Active Directory or IAM (Identity and Access Management) systems to create a stronger and more dynamic user-based security policy. With the shift to cloud and Software-defined Networking (SDN), firewalls have become modular components that can be provisioned, configured, and included in an automated security orchestration and response (SOAR) to threats.

* + - 1. FIREWALL SECURITY FUNCTIONS

This section will provide an agnostic view of key security features organizations can expect to leverage with the use of a Next Generation Firewall/ and or subject to vendor may require the use of additional add-ons.

##### Network Segmentation

Network segmentation defines boundaries between network segments where assets within the group have a common function, risk or role within an organization. For instance, the perimeter gateway segments a company network from the Internet. Potential threats outside the network are prevented, ensuring that an organization’s sensitive data remains inside. Organizations can go further by defining additional internal boundaries within their network, which can provide improved security and access control.

##### Access Control

Access control defines, people, groups and/ or the devices that access resources, network applications and systems which in-turn increases control to deny unsanctioned access and reduce the attack surface. Integrations with Identity and Access Management (IAM) products aid with defining policies for identification of users to ensure user and/or device is authorized to access assets through Role-based Access Control (RBAC) polices.

##### VPN Connectivity

Site to Site and Remote access VPN connections provide secure access to a company’s network. Hub and Spoke, Partial Mesh and Full Mesh deployment types allow for flexible architecture. Remote access VPN connectivity leverage client software installed or alternatively clientless via a web-based client. Privacy and integrity of sensitive information is ensured through multifactor authentication, endpoint compliance scanning, and encryption of all transmitted data.

##### Zero Trust Network Access

Also referred to as [software-defined-perimeter (SDP)](https://www.checkpoint.com/cyber-hub/network-security/what-is-software-defined-perimeter-sdp/) ensures all users only have access and permissions, only the right users and devices have the access they require to perform their duties. This is a different approach in comparison to traditional security solutions, like VPN's that grant a user full access to the target network. ZTNA overcomes common issues such as visibility of network access, security tool sprawl, and unspecific access policies linked to subnets granting complete access to a LAN.

* **Access Control**: Improve visibility into device, user and risks associated with third-party access activity and enable role-based access to applications and data. Identity-based authentication and access control found in ZTNA provide an alternative to IP-based access control, dramatically decreasing an organisation's cyber risk and exposure to cyber threats.
* **Risk and Conditional Access**: Risk-based access and conditional access policies can further enhance the control of resources.

##### Email Security

Email security refers to any processes, products, and services designed to protect your email accounts and email content safe from external threats. Most email service providers have built-in email security features designed to keep you secure, but these may not be enough to stop cybercriminals from accessing information. Data loss prevention (DLP) is a cybersecurity methodology that combines technology and best practices to prevent the exposure of sensitive information outside of an organization, especially regulated data such as personally identifiable information (PII) and compliance related data: HIPAA, SOX, PCI DSS, etc.

##### Intrusion Prevention Systems (IPS/IDS)

IPS technologies can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and exploits of known vulnerabilities. A vulnerability is a weakness for instance in firmware and an exploit is an attack that leverages that vulnerability to gain control. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System can be used in these cases to mitigate against these attacks.

##### Sandboxing

Sandboxing is a cybersecurity practice where you run code or open files in a safe, isolated environment on a host machine that mimics end-user operating environments. Sandboxing observes the files or code as they are opened and looks for malicious behaviour to prevent threats from getting on the network. For example, malware in files such as PDF, Microsoft Word, Excel and PowerPoint can be safely detected and blocked before the files reach an unsuspecting end user.

##### Scalable Network Security

The ability of an architecture to scale appropriately, as increased demand is added to the system. Includes rapid deployment, scaling up or down to meet changes of network security demands within an organisation. By tightly integrating resources in it is possible to fully utilize all capacity of hardware/ software available within a clustering solution.

##### Cloud Network Security

Applications and workloads are no longer exclusively hosted on-premises be it on-site or hosted within a local data centre. Protecting the modern data centre requires greater flexibility and innovation to keep pace with the migration of application workloads to the cloud. Software-defined Networking (SDN) and Software defined Wide Area Network (SD-WAN) solutions enable network security solutions in private, public, hybrid and cloud-hosted Firewall-as-a-Service (FWaaS) deployments.

* + - 1. Firewall as a Service (FWaaS)

FWaaS and be referred to as a cloud-delivered Firewall that provides advanced next-generation Firewall (NGFW) capabilities spanning not only the traditional layers but also highlighting layer 7 of the OSI model, including access controls, URL filtering, advanced threat prevention, intrusion prevention systems (IPS) and DNS security additional functions are as follows:

**Block shadow IT over non-web ports**: Stop use of unapproved SaaS apps.

**Cloud IPS**: A cloud-based intrusion prevention system (IPS)

**DNS security and control**: First line of defence protects users from reaching malicious domains. It optimises DNS resolution to provide a better user experience and cloud application performance, which is especially critical for CDN-based apps. And it provides granular controls to detect and prevent DNS tunnelling.

**Visibility and simplified management**: A cloud-based Firewall delivers real-time visibility, control, and immediate policy enforcement across the platform.

* + 1. Endpoint Security
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 8 | **Malware Defences** | Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action. |

* + - 1. Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) Overview

There are many differences between ‘legacy’ anti-virus and Endpoint Protection/Endpoint Detection and Response, these are outlined in this section of the paper.

An endpoint can be defined as any device on a network. A smartphone, laptop, tablet, or desktop computer; generally, this will be an operating system on which an agent can be installed.

An Endpoint Protection Platform (EPP) therefore describes any security program that aims to protect these devices from cyber threat. Initially, security protection started with Antivirus (AV), which then progressed onto ‘Next-Generation’ Antivirus (NGAV). As security technology improved, the size of the umbrella grew – as technology companies adopted a more holistic approach to endpoint security – and hence Endpoint Protection (EPP) terminology was born. Following this, the Endpoint Protection (NGEP) was phrased. One point that must be made is that AV is not separate from EPP, it is just one element that is used within the umbrella.

Antivirus software is the original endpoint protection. But there’s good reason to differentiate NGAV and EPP (or NGEP) from ‘legacy’ AV; NGAV or NGEP (these terms are pretty much interchangeable) has therefore been developed as a step up from the original ‘legacy’ AV to provide the protection from the advanced malware threats we see today. Traditional AV programs rely on an up-to-date list (database) of virus definitions from which it can recognise “known” threats in malicious files. So firstly, a suspect file needs to be “known” – it also presumes that all threats will be file-based.

Instead of relying on just signature-based detection, the leading Next Gen Endpoint Protection Platforms use behaviour-based monitoring to look for suspicious behaviour – whether in a file, or via an advanced “fileless” attack.

It’s a much more effective means of protection because it doesn’t count on the specific malware code having ever been seen before – it can be an entirely new type of attack and still NGEP will recognise that this code is carrying out unwanted/illegitimate actions that must be prevented. EDR will limit the scope of the infection, then use remediation technologies to remove and/or fix files in the infected system.

Crucially, EDR technologies do a lot of data gathering around incidents to learn more about attack behaviour. That data obviously strengthens the EDR offering, but also pays off in the wider cyber security field.

* + - 1. EDR vs MDR

Endpoint Detection and Response (EDR)

EDR – or Endpoint Detection & Response, is based on the premise that at some point an infection is going to occur. EDR is a different kind of technology.

Gartner defines EDR solutions as having four primary capabilities:

1. Detect security incidents.
2. Contain the incident at the endpoint, such that network traffic or process execution can be remotely controlled.
3. Investigate security incidents.
4. Remediate endpoints to a pre-infection state.

Managed Detection and Response (MDR)

Managed detection and response build on top of EDR where the vendor or a Managed Security Services Provider MSSP provide services around:

* Threat Hunting
* Incident Response or Guided and Active Response
* Periodic reporting
* Deployment assistance
* Onboarding

Whilst all vendors listed in this Options Paper provide an MDR service, these services will differ slightly. Further investigation into any specific vendor offering can be arranged.

* + - 1. Endpoint Detection and Response

Endpoint detection and response refers to a category of tools used to detect and investigate threats on endpoints. EDR tools typically provide detection, investigation, threat hunting, and response capabilities. Endpoint detection and response has become a critical component of any endpoint security solution because there’s simply no better way to detect an intrusion than by monitoring the target environment being attacked, and the telemetry collected by an EDR platform enables full triage and investigation.

EDR security solutions analyse events from laptops, desktop PCs, mobile devices, servers, and even IoT and cloud workloads, to identify suspicious activity. They generate alerts to help security operations analysts uncover, investigate, and remediate issues. EDR tools also collect telemetry data on suspicious activity and may enrich that data with other contextual information from correlated events. Through these functions, EDR is instrumental in shortening response times for incident response teams, and ideally, eliminating threats before damage is done.

If they are well-resourced, they might develop a zero-day attack that takes advantage of unknown app or system vulnerabilities. Fortunately, effective threat prevention tools can stop over 99% of all attacks automatically. They can apply multiple analysis engines, from the reputation of the source and the signer of a file to the byte code distribution to the functions in an executable to block the attack. Since many zero-day attacks use known techniques, the right security tools can stop these zero-day attacks even if they have never seen a specific attack before. However, the most sophisticated and potentially damaging attacks require detection and response. These attacks, such as insider threats, low and slow attacks, and advanced persistent threats, may require manual verification from a security analyst. Oftentimes, the only way to identify these attacks is by analyzing activity over time and across data sources with machine learning.

These advanced attacks rarely can be identified in real time. And oftentimes a security analyst must try to understand the intent of the activity to determine whether or not it’s malicious. So, while few attacks require detection and response, these attacks can be extremely destructive. Security teams need EDR solutions to find, investigate and stop them.

* + - 1. Recommendations

Endpoint Detection and Response (EDR) is recommended for all corporate endpoints. EDR has many features that can be utilised to cover many areas of security controls under on technology:

The features and areas that EDR covers:

**Next Generation Anti-virus (NGAV):** NGAV consists of machine learning and AI to detect unknown malware, behaviour-based indicators of attack (IOA), Exploit blocking, and the use of threat intelligence.

**Endpoint, Detection and Response (EDR):** Continuous event recording for visibility, threat hunting to aid in identifying attacks.

**Device control:** Control USB and devices that can be allowed or denied on an endpoint

**Software application control:** Control which applications are allowed to be used, enforce unsanctioned applications

**Endpoint Firewall Management:** Centralised management of the local firewalls can be useful in building out standard policies across all endpoints

**Vulnerability Scanning:** EDR can provide vulnerability scanning for the system and software installed. This could replace an authenticated vulnerability solution

* + 1. Encryption
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 8 | **Malware Defences** | Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action. |
| 10 | **Data Recovery Capabilities** | The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it. |
| 12 | **Boundary Defense** | Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. |

* + - 1. Encryption at Rest vs Motion

There are two types of data: data in motion and data at rest. Data in motion (or “active data”) is data that you most likely use daily. It is usually stored on a database that’s accessed through apps or programs. Data at rest is stored and is usually protected by a firewall or anti-virus software. Though these methods of protection for data at rest is good, complete safety requires adding an additional layer of defence. This is where [encryption at rest](https://brightlineit.com/encrypting-data-at-rest/) comes to play.

##### Data at Rest

Data encryption is the process of translating one form of data into another form of data that unauthorized users can’t decrypt. For example, you saved a copy of a paid invoice on your server with a customer’s credit card information. By encrypting data at rest, you’re essentially converting your sensitive data into another form of data. This usually happens through an algorithm that can’t be understood by a user who does not have an encryption key to decode it. Only authorized personnel will have access to these files, thus ensuring that your data stays secure.

Examples of data at rest encryption are BitLocker for Windows, hardware encrypted USB drives, and SAN volume encryption.

It is advised where possible that all data at rest should have some form of encryption, especially remote devices, such as laptops and mobile phones. Also, remote storage devices should have encrypted data.

* + 1. Virtual Private Network
       1. CIS v7 Sections

|  |  |  |
| --- | --- | --- |
| CIS Control | Title | Description |
| 12 | **Boundary Defense** | Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. |

* + - 1. Traditional VPN

Traditional on-premise, data centre, and IaaS VPN access is useful in some uses in the business. A VPN client can be used to access services on private networks. However, using the ‘backhaul’ where data has to ingress and egress a single point can impact on the user experience as latency and bandwidth restrictions can be introduced. Multi-factor authentication and the use of an identity provider is highly recommended.

* + - 1. Zero Trust Network Access (ZTNA)

Zero trust network access is usually deployed as part of a SASE solution, which provides

Also referred to as ensures all users only have access and permissions required to fulfil their role. This is a quite different approach in comparison to traditional security solutions, like VPN's that grant a user full access to the target network. ZTNA overcomes common issues such as visibility of network access, security tool sprawl, and unspecific access policies linked to subnets granting complete access to a LAN.

**Access Control**: Improve visibility into device, user and risks associated with third-party access activity and enable role-based access to applications and data. Identity-based authentication and access control found in ZTNA provide an alternative to IP-based access control, dramatically decreasing an organisation's cyber risk and exposure to cyber threats.

**Risk and Conditional Access**: Risk-based access and conditional access policies can further enhance the control of resources.

1. Personas
   1. Security Framework

The security framework has been split into two layers that contains security elements that are used for the mapping of services or assets that are being accessed. All core security elements will be required for each persona.

It must be noted that the security architecture frameworks use identity-based security with a view to having the primary security boundary at the device (if possible). The architectures are also based on an identity accessing a service or services, otherwise known as Zero Trust.

A picture containing logo

Description automatically generated

Application

Description automatically generated

* 1. General Office Users
* Service types – applications: Cloud and on-premise. O365.
* User type – Employee.
* Device types – Corporate (Desktop/Laptop), Mobiles - Intune (Corporate – JAMF, BYOD).
* Connectivity – LAN, VPN, No VPN, Mobile (Public 4G). No back Haul, Wifi.
* Cloud/On premise – Both
* Locations – Office, Home, anywhere for laptops.
  + - 1. Accessing Software as a Service (SaaS)

The user can be located anywhere when leveraging a SASE solution, an agent is required to be installed on the corporate device. The security architecture describes the components required to access Software as a Service applications including Office 365. SaaS applications that are hosted on-premise can be integrated into the Cloud Access Security Broker, Secure Web Gateway or Single Sign-On depending on the capabilities present within the organisations chosen solution.

For BYOD devices the Cloud Access Security Broker, Single Sign-On, Multi-factor authentication, and Key Vault components can be in place but not the Secure Web Gateway. Some OOB (Out of band) Data Loss Prevention can be put in place.

Diagram

Description automatically generated

##### Components

* **Endpoint Security:** The endpoint security using EDR ensures monitoring on the device that could provide some DLP functions and additional security, such as application control, anti-virus/malware. A local firewall should be in place and managed, and control of browsers that can be used on the device. ***Note: this is not available on BYOD devices.***
* **Web Security**:
  + A Secure Web Gateway (SWG) will provide high level control of URL’s, anti-malware, threat intelligence, and sandboxing. Remote Browser Isolation (RBI) can be used for high-risk websites. Policies can also be built using the identity provider integration for either user level or role-based access. ***Note: this is not available on BYOD devices.***
  + The Cloud Access Security Broker (CASB) will control access to the applications based on user or RBAC and provide malware detection/sandboxing. Also, monitoring of sanctioned and unsanctioned applications and risk-based application access. ***Note: BYOD devices will only be able to use a reverse proxy with the CASB***
* **Data Loss Prevention**: DLP is integrated into the CASB both inline and out of band (API). ***Note: Only out of band DLP functions are available for BYOD devices.***
* **Encrypted Data in Transit:** The web security component will ensure encryption in transit. ***Note: this is not available on BYOD devices.***
* **Identity Provider (IdP):** The IdP (AAD) will integrate into the web security and authentication layer: Key Vault, SSO, and MFA
* **Key Vault (optional):** A key vault can be in place with MFA. Note: This may not be needed if SSO is on place.
* **Single Sign-On (SSO):** SSO can be used to allow or deny access to application by integrating into the IdP and using RABC to create group access to applications. Only applications that are assigned to a group can be accessed.
* **Multi-factor, Risk, Conditional Authentication:** Some form of multi-factor authentication should be in place either through SSO or directly with the application. For risk based and conditional access an SSO solution will be needed, in some instances
* **Asset and Device Management:** The CASB can inform the software asset inventory. ***Note: this is not available on BYOD devices.***
  + - 1. Accessing General Internet Services

The security components required for secure Internet access; the design assumes a SASE model approach whereby an agent is installed on the end user corporate device. For BYOD devices, these can use the Secure Web Gateway and DNS Security if they are using a network that is under corporate control. The caveat is that any egress traffic will have the same SWG policies as there is no way to base the policies on identity. Also, DNS security can be implemented issuing a forwarding DNS server by DHCP. For BYOD devices outside of the corporate network there is no way to monitor or control web traffic.

Diagram

Description automatically generated

##### Components

* **Endpoint Security:** The endpoint security using EDR ensures monitoring on the device that could provide some DLP functions and additional security, such as application control, anti-virus/malware. A local firewall should be in place and managed, and control of browsers that can be used on the device. ***Note: this is not available on BYOD devices.***
* **Web Security**:
  + A Secure Web Gateway (SWG) will provide high level control to URL’s, anti-malware, threat intelligence, and sandboxing. Remote Browser Isolation (RBI) can be used for high-risk websites. Policies can also be built using the identity provider integration for either user level or role-based access. ***Note: this is not available on BYOD devices.***
  + As with the SaaS application control, CASB is available for corporate devices.
  + Remote Browser Isolation (RBI) can be used for more risk adverse browsing and higher end user protection.
* **Data Loss Prevention**: DLP can be achieved to certain level with the Secure Web Gateway, this is done by restricting access to specific sites, such as drop box, box ,etc. ***Note: this is not available on BYOD devices.***
* **DNS Security (optional):** DNS Security can be used as an agentless solution for OT and IoT devices as well as an additional security layer for other assets.
* **Encrypted Data in Transit:** The web security component will ensure encryption in transit.
* **Identity Provider (IdP):** The IdP (AAD) will integrate into the secure web gateway and DNS security to provide identity-based policies. ***Note: this is not available on BYOD devices.***
* **Key Vault (optional):** A key vault can be in place with MFA. Note: This may not be needed if SSO is present.
  + - 1. Accessing On-premise, Data Centre or Cloud Services

The security components required to secure access on-premise, data centre, and or a Cloud platform (IaaS, PaaS) service. The Virtual Private Network, Wireless Security, and Network Access Control are optional depending on the way the user is accessing the infrastructure. Diagram

Description automatically generated

##### Components

* **Endpoint Security:** The endpoint security using EDR ensures monitoring on the device that could provide some DLP functions and additional security, such as application control, anti-virus/malware. A local firewall should be in place and managed, and control of browsers that can be used on the device. ***Note: this is not available on BYOD devices.***
* **Virtual Private Network (optional):** For remote users accessing services on-premise, data centre or IaaS networks either a traditional VPN or Zero-Trust Network Access (ZTNA) can be used. The authentication should be provided by a central identity provider and multi-factor authentication. For BYOD devices, clientless VPN can be considered. The caveat is that only certain services such as RDP, SSH and Web applications can be presented.
* **Network Access Control (optional):** For users that are connected to a local corporate LAN, Network Access Control ensures that only authorised devices and staff can gain access to the network.
* **Wireless Security (optional):** The corporate SSID should be logically of physically separated to the LAN and have enterprise 802.1x authentication. For more SSID’s that require a highly level of security, MFA should be implemented.
* **Identity Provider and Multi-factor Authentication**: Active Directory or Azure Active Directory should be used to provide authentication to the various network elements. Role based access control can be implemented to allow access for certain user groups. For example,
* **Firewalls and Network Segmentation:** Network segmentation should be implemented for all zones with the infrastructure:
  + Wireless SSID to VLAN or physical network separation (Layer 1 and 2). Firewall separation at IP and TCP/UDP (OSI Layer 3 and 4).
  + The firewall should use identity-based rules that can be integrated with the identity provider.
  + Intrusion prevention should be in place for more secure areas of the network.
  + Segmentation of the servers, services, and differing service infrastructure.
  + Dynamic access control could be implemented from network access control through to the firewall.
  + Perimeter firewalls should in place for remote users and create network access policies to services.
* **Asset and Device Management:**
  + Software and hardware assets should be known and what users need to access.
  + Device management can deploy certificates to devices that can be used creating policies for all types of network access. Local firewall rules can be deployed for end user devices and servers.
* **On-premise, data centre, and Cloud (IaaS, SaaS) Services:** Identity based access from a central identity provider should be in place to all applications, systems, etc.Robust IAM policies and procedures will be required for applications and systems that do not have the capability to integrate with a directory.
  1. Distribution Centre Staff
* Service types: Applications: on-premise. O365. No public services, private access to apps (GCP) via VPN. Restrict general internet access – Proxy auth required (shared).
* User type: Employee.
* Device types: Shared terminals, mobile devices.
* Connectivity: LAN Only, Corporate Wifi.
* Cloud/On premise: Both.
* Locations: Office/Warehouse.

The distribution centre staff have similar controls to the general head office users, although identity-based access control is not possible. Generic security policies should be implemented for all components.

Diagram

Description automatically generated

##### Components

* **Endpoint Security (if possible):** The endpoint security using EDR ensures monitoring on the device that could provide some DLP functions and additional security, such as application control, anti-virus/malware. A local firewall should be in place and managed, and control of browsers that can be used on the device.
* **Web Security**:
  + A Secure Web Gateway (SWG) will provide high level control to URL’s, anti-malware, threat intelligence, and sandboxing. Remote Browser Isolation (RBI) can be used for high-risk websites. Policies can also be built using the identity provider integration for either user level or role-based access.
  + As with the SaaS application control, the CASB is available to corporate devices.
* **Data Loss Prevention**: DLP is integrated into the CASB both inline and out of band (API). Must be agent based.
* **DNS Security (optional):** DNS Security can be used as an agentless solution for OT and IoT devices as well as an additional security layer for other assets.
* **Network Access Control (optional):** For users that are connected to a local corporate LAN, Network Access Control ensures that only authorised devices and staff can gain access to the network.
* **Wireless Security:** The corporate SSID should be logically of physically separated to the LAN and have enterprise 802.1x authentication. For more SSID’s that require a highly level of security, MFA should be implemented.
* **Identity Provider and Multi-factor Authentication**: Active Directory or Azure Active Directory should be used to provide authentication to the various network elements. Role based access control can be implemented to allow access for certain user groups.
* **Firewalls and Network Segmentation:** Network segmentation should be implemented for all zones with the infrastructure:
  + Wireless SSID to VLAN or physical network separation (Layer 1 and 2). Firewall separation at IP and TCP/UDP (OSI Layer 3 and 4).
  + The firewall should use identity-based rules that can be integrated with the identity provider.
  + Intrusion prevention should be in place for more secure areas of the network.
  + Segmentation of the servers, services, and differing service infrastructure.
  + Dynamic access control could be implemented from network access control through to the firewall.
  + Perimeter firewalls should in place for remote users and create network access policies to services.
* **Asset and Device Management:**
  + Software and hardware assets should be known and what users need to access.
  + Device management can deploy certificates to devices that can be used creating policies for all types of network access. Local firewall rules can be deployed for end user devices and servers.
* **On-premise, data centre, and Cloud (IaaS, SaaS) Services:** Identity based access from a central identity provider should be in place to all applications, systems, etc.Robust IAM policies and procedures will be required for applications and systems that do not have the capability to integrate with a directory.
  1. Retail Store Colleagues
* Service types: Applications: Majority on-premise, some cloud.
* User type: Employee.
* Device types: Mobile devices (Bar code scanners, etc), Desktops (back office), Physical tills.
* Connectivity: Private MPLS.
* Cloud/On premise: Both.
* Locations: Store supervisors have access to O365.

##### Desktops in the back office

The desktops located within store back offices should be treated the same from a security point of view as the General Head Office User detailed within section 3.3.. it assumed that O365 access is performed from the back-office desktops.

##### Mobile Devices and Physical Tills

The assumption is that the mobile devices and physical tills do not have the ability to install an agent.

Diagram

Description automatically generated

##### Components

* **DNS Security:** DNS Security can be used as an agentless solution for OT and IoT devices as well as an additional security layer for other assets.
* **Network Access Control (optional):** For users that are connected to a local corporate LAN, Network Access Control ensures that only authorised devices and staff can gain access to the network. MAC addresses can be used for devices that are allowed on the network but do not have the capability to authenticate.
* **Wireless Security:** The corporate SSID should be logically of physically separated to the LAN and have enterprise 802.1x authentication where possible. If the device wireless network is using password authentication, ideally this should be changed on a semi regular basis (every few months) if operations permit.
* **Firewalls and Network Segmentation:** Network segmentation should be implemented for all zones with the infrastructure:
  + Wireless SSID to VLAN or physical network separation (Layer 1 and 2). Firewall separation at IP and TCP/UDP (OSI Layer 3 and 4).
  + The firewall should use identity-based rules that can be integrated with the identity provider, if possible.
  + Intrusion prevention should be in place for more secure areas of the network.
  + Segmentation of the servers, services, and differing service infrastructure.
  + A firewall should be in place for store connections back to any centralised office, data centre, or cloud environment. Only networks or services that are needed should be allowed through the firewall.
* **Asset and Device Management:**
  + Device management Mobile Application Management MAM should be in place for BYOD devices and Mobile Device Management (MDM) for corporate owned devices.
* **On-premise, data centre, and Cloud (IaaS, SaaS) Services:** Identity based access from a central identity provider should be in place to all applications, systems, etc.Robust IAM policies and procedures will be required for applications and systems that do not have the capability to integrate with a directory.
  1. Customer Care Staff (PCI)
* Service types: Applications: PCI, Cloud and on-premise.
* User type: Employee, Card Translations.
* Device types: Corporate devices only.
* Connectivity: Secure LAN (VLAN), SaaS services, payment gateways, need VPN.
* On premise only.
* Locations: Office.
  + - 1. Accessing Software as a Service (SaaS)

Diagram

Description automatically generated

* **Endpoint Security:** The endpoint security using EDR ensures monitoring on the device that could provide some DLP functions and additional security, such as application control, anti-virus/malware.
  + A local firewall should be in place and managed, and control of browsers that can be used on the device.
  + Endpoint telemetry should be logged to a SIEM or XDR solution along with security analysts in a Security Operations Centre (SOC) to identify any breaches or anomalies as soon as possible.
  + A separate physical machine from normal corporate use should be in place for the end user.
  + Strict application, script, and library whitelisting should be implemented.
* **Encryption at Rest:** All data on the end user device should encrypted, as with data that the SaaS service is providing. In some cases, tokenisation may be required from some data types and use cases.
* **Firewalls**: Segmentation of network traffic for PCI data from standard corporate data is essential. A least privilege principal for firewall rules should be considered.
* **Network Access Control:** For users that are connected to a local corporate LAN, Network Access Control ensures that only authorised devices and staff can gain access to the network. Certificate based authentication for devices should be considered, and users should use the identity provider to authenticate.
* **Network Segementation:** Either logical (VLAN) or physical (Switching)
* **Virtual Private Network:** If a VPN is in use the terminating endpoint should be a secure remote desktop either virtualised or physical that has the same characteristics. A zero-trust network access (ZTNA) solution will provide both the VPN, authentication, and Firewalling features that
* **Web Security:**
  + A Secure Web Gateway (SWG) will provide high level control to URL’s, anti-malware, threat intelligence, and sandboxing. Remote Browser Isolation (RBI) can be used for high-risk websites. Policies can also be built using the identity provider integration for either user level or role-based access.
  + As with the SaaS application control, the CASB will provide additional security access controls.
* **Data Loss Prevention**: DLP is integrated into the CASB both inline and out of band (API).
* **Encryption in Transit:** Encryption in transit is critical for any ingress (VPN) or egress (SaaS application). The SWG and CASB will ensure that all TLS connection encryption methods are of a good standard.
* **Key Vault (optional):** A key vault can be in place with MFA. Note: This may not be needed if SSO is on place.
* **Single Sign-On (SSO):** SSO can be used to allow or deny access to application by integrating into the IdP and using RABC to create group access to applications. Only applications that are assigned to a group can be accessed.
* **Multi-factor Authentication:** Any authentication access should have MFA enabled, this would include VPN/ZTNA, SSO, Key Vault, and SaaS applications.
* **Device Management:** Device management should be in place to control/patch system and applications.
* **Identity Provider:** Identity based access from a central identity provider should be in place to all applications, systems, etc.Robust IAM policies and procedures will be required for applications and systems that do not have the capability to integrate with a directory.
  + - 1. Accessing On-premise, Data Centre or Cloud Services

Diagram

Description automatically generated

##### Components

* **Endpoint Security:** The endpoint security using EDR ensures monitoring on the device that could provide some DLP functions and additional security, such as application control, anti-virus/malware.
  + A local firewall should be in place and managed, and control of browsers that can be used on the device.
  + Endpoint telemetry should be logged to a SIEM or XDR solution along with security analysts in a Security Operations Centre (SOC) to identify any breaches or anomalies as soon as possible.
  + A separate physical machine from normal corporate use should be in place for the end user.
  + Strict application, script, and library whitelisting should be implemented.
* **Encryption at Rest:** All data on the end user device should encrypted, as with data that the SaaS service is providing. In some cases, tokenisation may be required from some data types and use cases.
* **Firewalls**: Segmentation of network traffic for PCI data from standard corporate data is essential. A least privilege principal for firewall rules should be considered.
* **Network Access Control:** For users that are connected to a local corporate LAN, Network Access Control ensures that only authorised devices and staff can gain access to the network. Certificate based authentication for devices should be considered, and users should use the identity provider to authenticate.
* **Network Segementation:** Either logical (VLAN) or physical (Switching).
* **Virtual Private Network:** If a VPN is in use the terminating endpoint should be a secure remote desktop either virtualised or physical that has the same characteristics. A zero-trust network access (ZTNA) solution will provide both the VPN, authentication, and Firewalling features.
* **Key Vault (optional):** A key vault can be in place with MFA.
* **Multi-factor Authentication:** Any authentication access should have MFA enabled, this would include VPN/ZTNA, SSO, Key Vault, and on-premise, systems and applications.
* **Device Management:** Device management should be in place to control/patch system and applications.
* **On-premise, data centre, and Cloud (IaaS, SaaS) Services:** Identity based access from a central identity provider should be in place to all applications, systems, etc.Robust IAM policies and procedures will be required for applications and systems that do not have the capability to integrate with a directory.
  1. Third Parties (App Support, Payment, etc)
* Service types : Applications: Cloud and on-premise.
* User type: Third party: Support functions mainly on-premise.
* Device types: Any, no control present.
* Connectivity: VPN.
* Cloud/On premise: Both
* Locations: Anywhere

Diagram

Description automatically generated

##### Components

* **Firewalls**:
  + Segmentation of network traffic for a third party accessing the corporate environment should be controlled as much as possible.
  + A jump box or reverse proxy should be considered when for third parties that need to access protocols such as SSH, RDP and Web. Remote desktop could be another option for remote access.
  + Internet access should be restricted where possible, a web proxy should be considered to for internet restrictions.
  + Intrusion Prevention (IPS) should be in place to monitor traffic from any remote business.
  + Anti-malware detection should be enabled on the firewall.
* **Network Access Control:** . Note: The network access control would not include technologies such as 802.1x and dynamic VLAN’s.
  + For third parties that are supporting IT infrastructure, out of band management should be considered with VLAN or physical network separation.
  + Firewall policies should be in place to deny access to other areas of the network.
* **Virtual Private Network:**
  + If a VPN is in use the terminating endpoint should be a secure remote desktop either virtualised or physical that has the same characteristics.
  + A zero-trust network access (ZTNA) solution will provide both the VPN, authentication, and firewalling.
* **Single Sign-On (SSO):** For web applications and privileged access to infrastructure components SSO can be used to allow or deny access to application by integrating into the IdP and using RBAC to create group access to applications.
* **Identity Provider:** 
  + Identity based access from a central identity provider should be in place to all applications, systems, etc.Robust IAM policies and procedures will be required for applications and systems that do not have the capability to integrate with a directory.
  + AAA for network infrastructure access should be in place.
  + A privileged access management solution should be considered for third party access control, this could include reverse proxy, session management/recording, and delegated access.
  + Federation to the third party could be considered to improve identity access control.
  1. SUBSIDIARIES
* Service types: Applications: Cloud and on-premise.
* User type: No control of group IT. Access to services centrally.
* Device types: Any.
* Connectivity: VPN/MPLS or direct link. Firewalled preventions present.
* Cloud/On premise: Both.
* Locations: Anywhere.

A recommendation for subsidiaries would be to use central core security services if some group IT is possible to aid in the security posture in the organisation. Examples of services would be vulnerability management, logging, and identity federation.

* + - 1. Accessing Software as a Service (SaaS)

Accessing Software as a Service (SaaS) applications for subsidiaries can be integrated into existing technologies such as SSO, MFA and direct access to SaaS applications using federation. This can improve authentication and authorisation to applications. If federation is not an option a local directory group/OU could be created on the IdP.

Diagram

Description automatically generated

##### Components

* **Web Security:** The Cloud Access Security Broker (CASB) will control access to the applications based on user or RBAC and provide malware detection/sandboxing. Also, monitoring of sanctioned and unsanctioned applications and risk-based application access. Note: Only a reverse proxy can be put into place.
* **Data Loss Prevention**: DLP is integrated into the CASB out of band (API).
* **Single Sign-On (SSO):** SSO can be used to allow or deny access to application by integrating into the IdP and using RBAC to create group access to applications. Only applications that are assigned to a group/user can be accessed.
* **Multi-factor, Risk, Conditional Authentication:** Some form of multi-factor authentication should be in place either through SSO or directly with the application. For risk based and conditional access an SSO solution will be needed, in some instances
* **Identity Provider:** 
  + Federation to the subsidiary could be considered to improve identity access control.
  + An OU or group can be created in the IdP directory for SSO or SAML, OAuth integration directly into the SaaS application.
    - 1. Accessing On-premise, Data Centre or Cloud Services

Diagram

Description automatically generated

##### Components

* **Firewalls**:
  + Segmentation of network traffic for the subsidiary accessing the corporate environment should be controlled as much as possible.
  + Internet access should be restricted where possible, a web proxy should be considered to for internet restrictions.
  + Identity based firewall policies could be used to enable specific access to networks, protocols and applications.
  + Intrusion Prevention (IPS) should be in place to monitor traffic from any remote business.
  + Anti-malware detection should be enabled on the firewall.
* **Network Access Control:** Note: The network access control would not include technologies such as 802.1x and dynamic VLAN’s.
  + Firewall policies should be in place to deny access to other areas of the network
* **Virtual Private Network:**
  + If a VPN is in use the terminating endpoint should be a secure remote desktop either virtualised or physical that has the same characteristics.
  + A zero-trust network access (ZTNA) solution will provide both the VPN, authentication, and firewalling.
* **Single Sign-On (SSO):** For web applications and privileged access to infrastructure components SSO can be used to allow or deny access to application by integrating into the IdP and using RBAC to create group access to applications.
* **Multi-factor, Risk, Conditional Authentication:** Some form of multi-factor authentication should be in place either through SSO or directly with the application. For risk based and conditional access an SSO solution will be needed, in some instances
* **Identity Provider:** 
  + Identity based access from a central identity provider should be in place to all applications, systems, etc.Robust IAM policies and procedures will be required for applications and systems that do not have the capability to integrate with a directory.
  + AAA for network infrastructure access should be in place.
  + A privileged access management solution should be considered for third party access control, this could include reverse proxy, session management/recording, and delegated access.
  + Federation to the third party could be considered to improve identity access control.

Thank You