IT NATION™ SECURE

hosted by CONNECTWISE®

Identity & Access Management – What is it, How it Maps to CIS Controls, and How to Profit

Presented by: Michael Roth, CEO of Evo Security

IT NATION™ SECURE

Agenda

1. What is IAM
2. IAM for Enterprise
3. IAM for MSPs
4. CIS Control Mapping
5. How to Profit

About Me

- Engineer
- Private Equity
- Cybersecurity

What is Identity and Access Management (IAM)?

Identity Management (IdP)

Validate You are Who You Say You are

"Logging into Stuff"

MFA, SSO, Directory Services, User & Endpoint & Device Management, Provisioning, Integrations

Privileged Access Management (PAM)

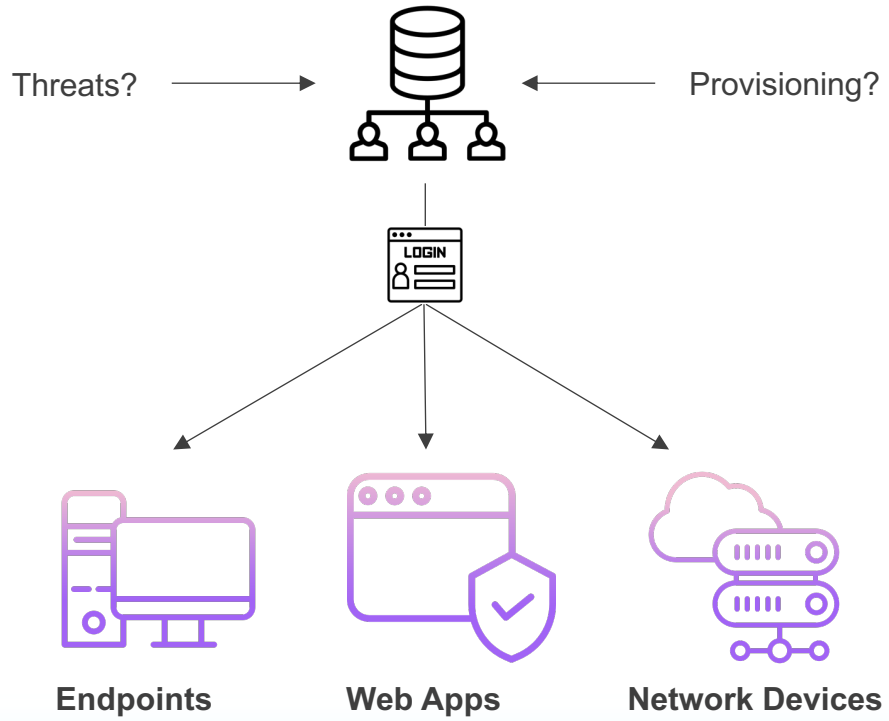
Apply Least Access Possible Once Inside

"Gaining Access to Stuff"

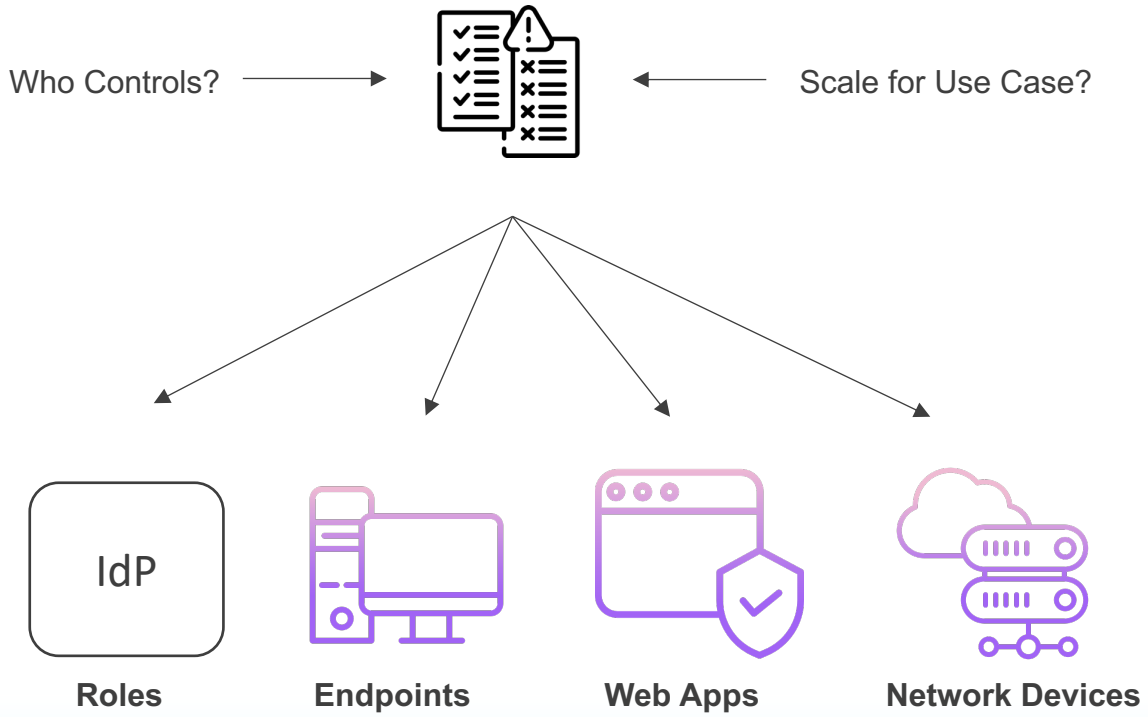
Roles, Groups, Policies, Credential Vaults, Endpoints Activities, Folders, Processes

What is IAM?

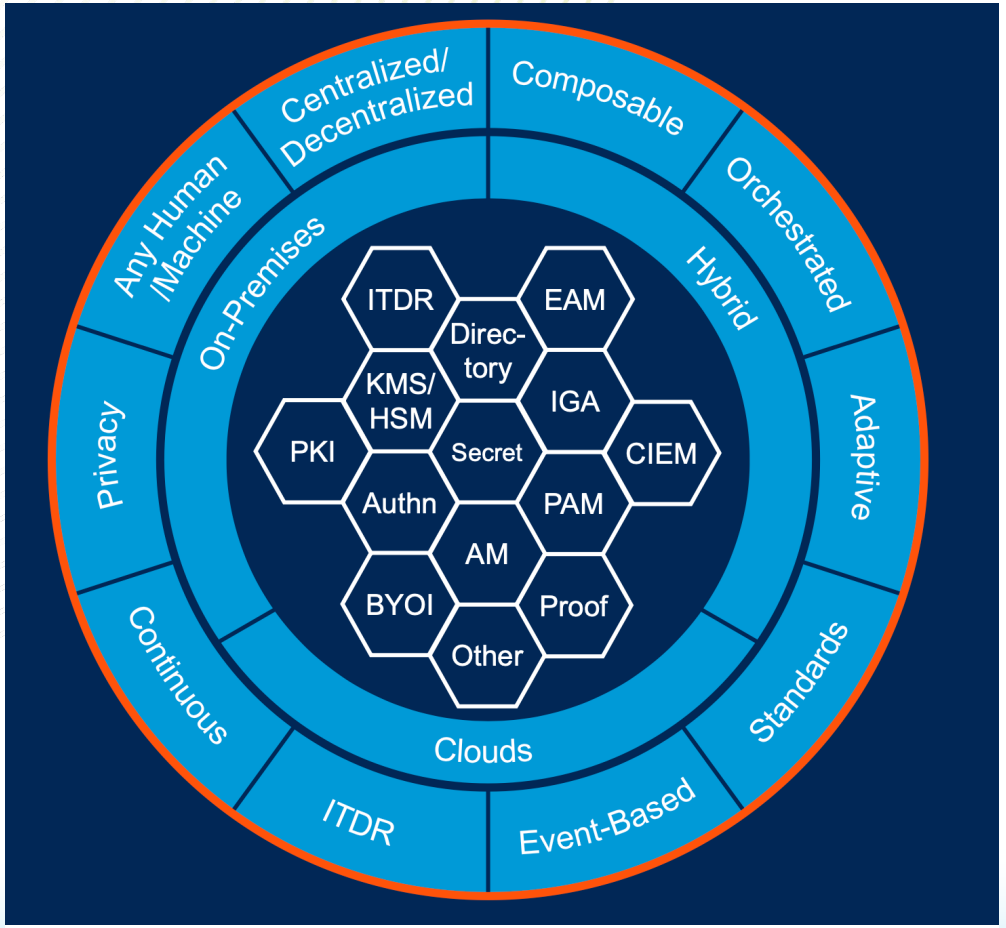
Identity Management (IdP)



Privileged Access Management (PAM)

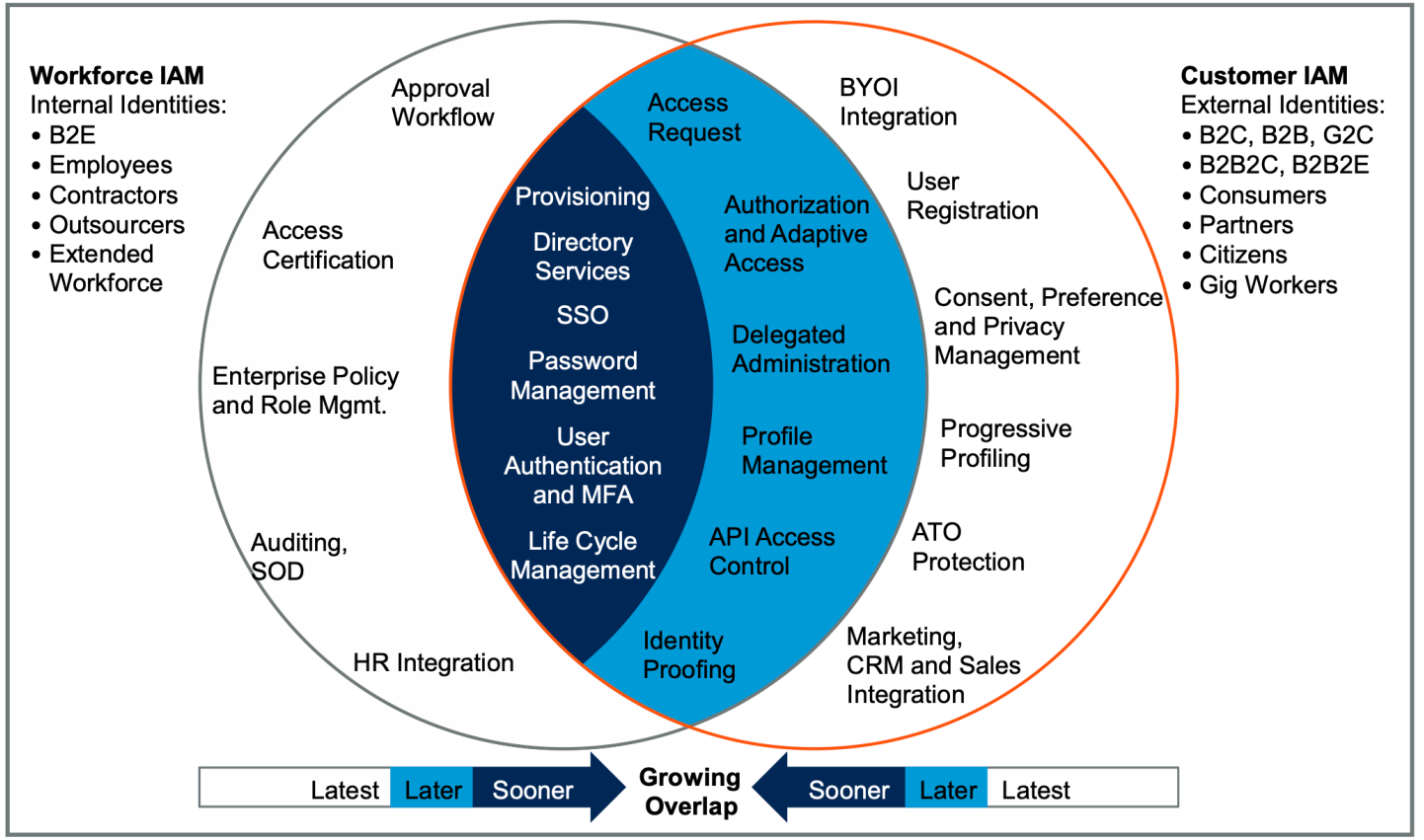


IAM for Large Enterprise



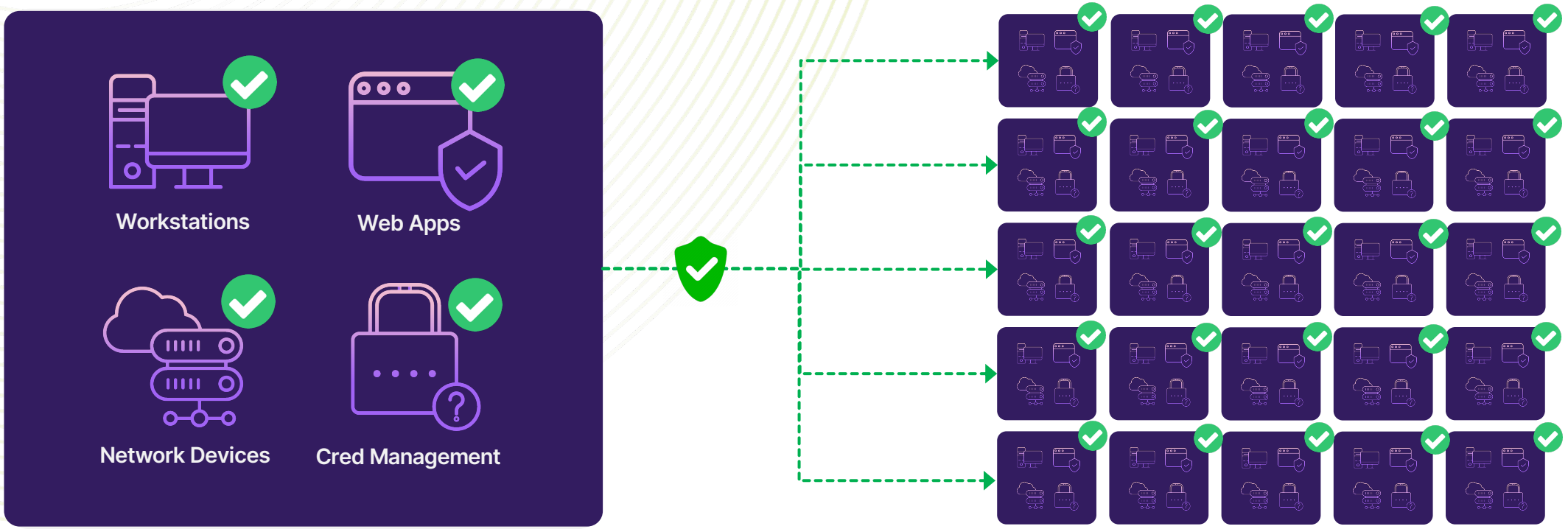
Source: Gartner

IAM for Medium Enterprise



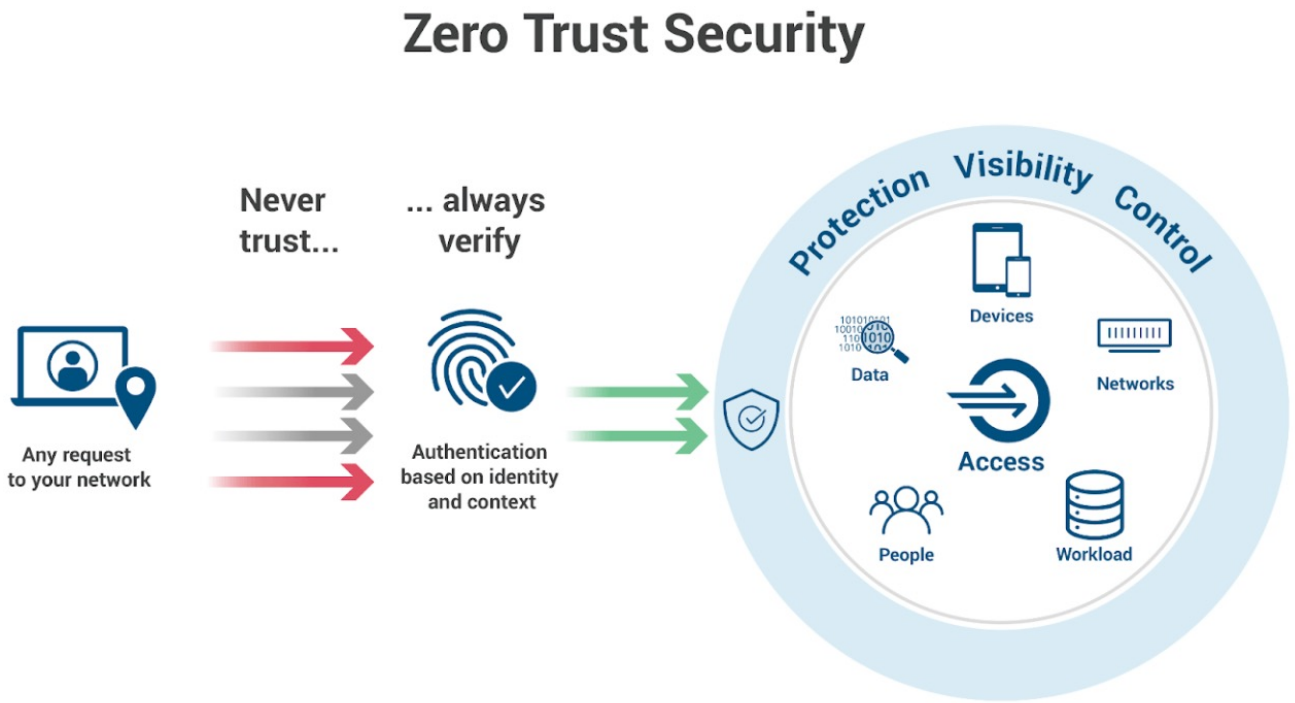
Source: Gartner

IAM for MSPs and their Customers

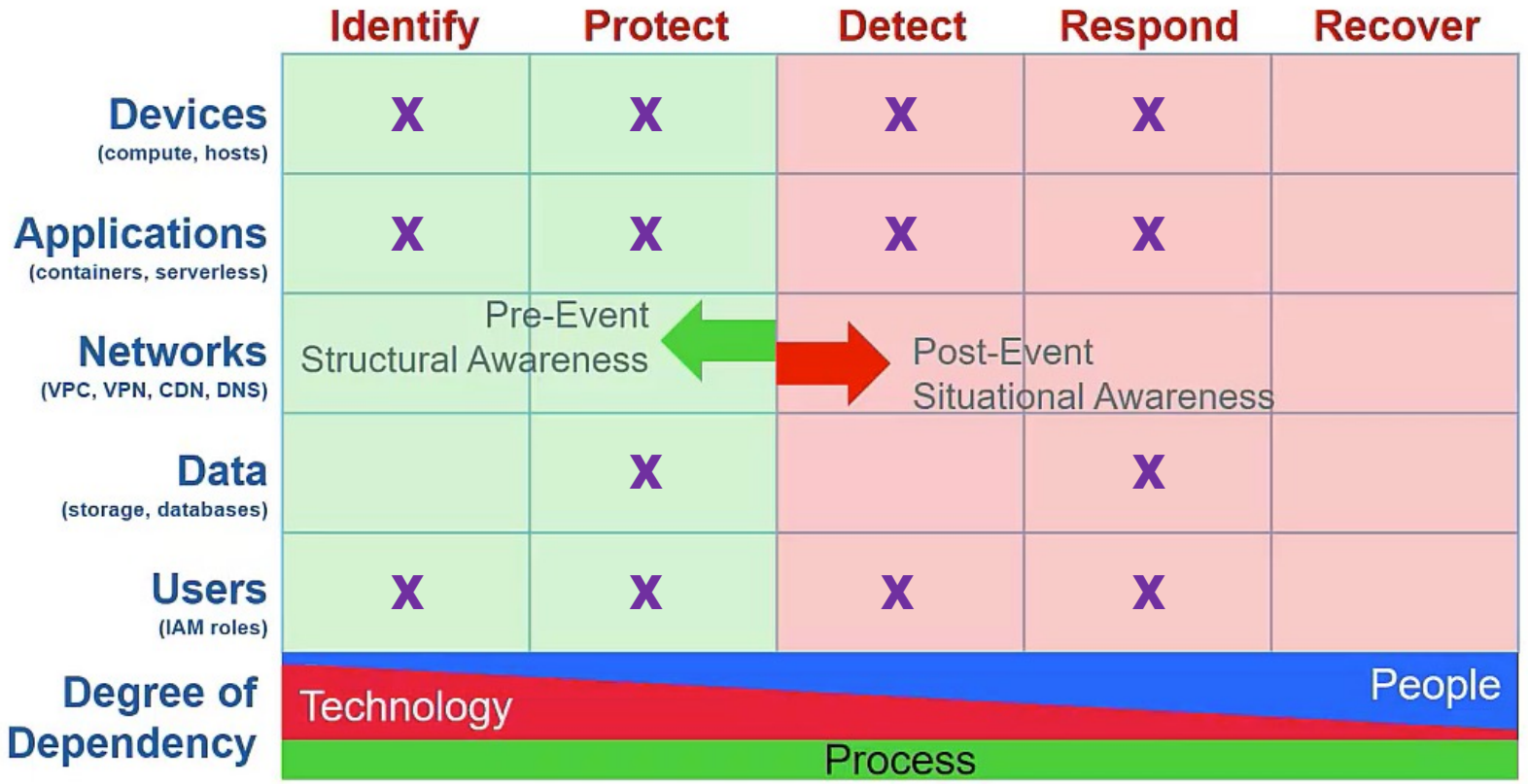


Secure the MSP — **Establish Secure Admin Elevation** — **Secure the MSP Customer**

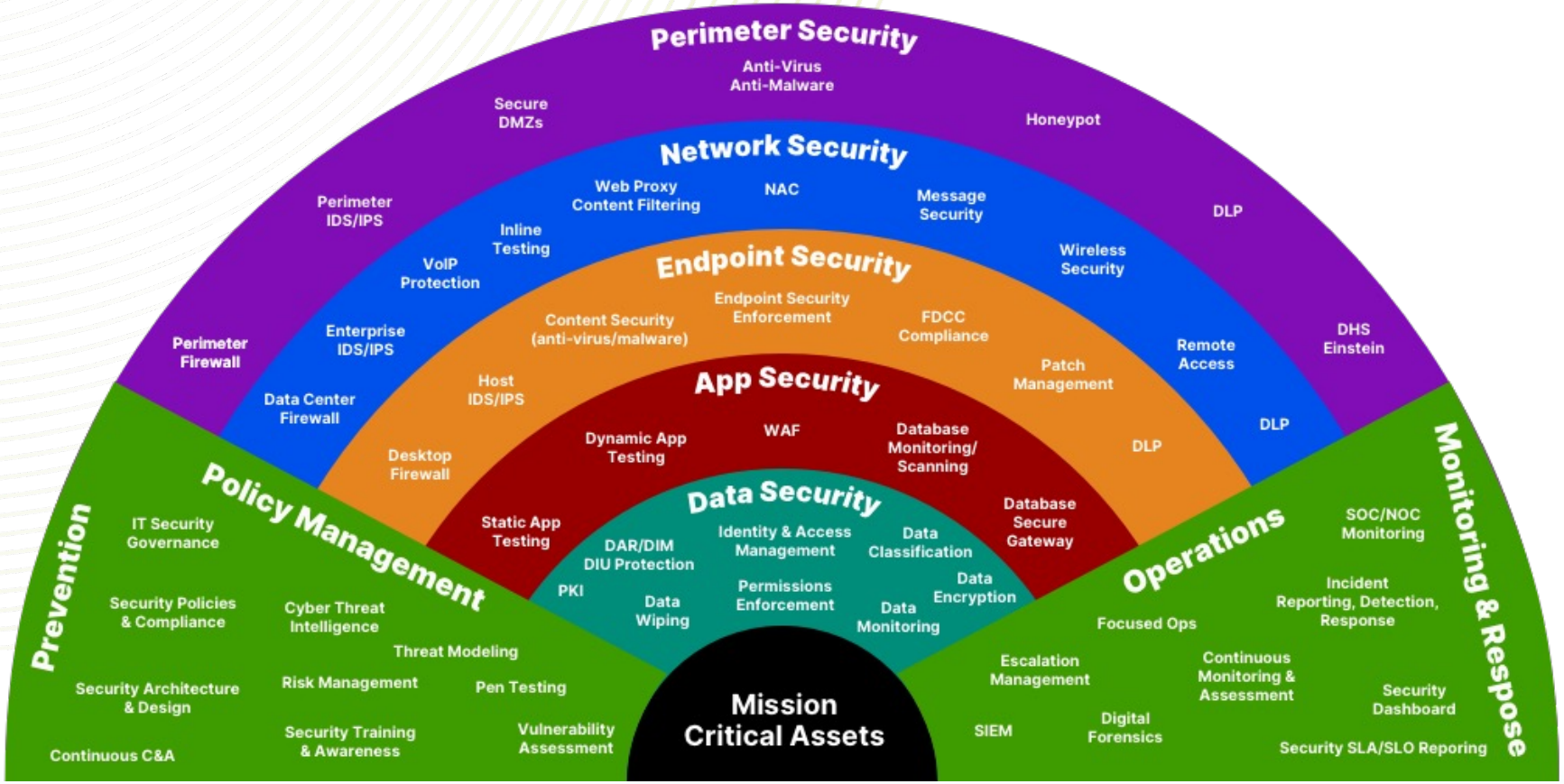
IAM and Zero Trust



IAM and Cyber Defense Matrix



IAM and Defense in Depth



What are CIS Controls

The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture.

Version 8

- 18 Controls
- 153 Safeguards
- 3 Implementation Groups
  - IG1 – Essential Cyber Hygiene
  - IG2 – Increased Operational Complexity
  - IG3 – Protection from Sophisticated Adversaries

https://www.cisecurity.org/controls/cis-controls-navigator/

IAM and CIS Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	
1				**Inventory and Control of Enterprise Assets**	***Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.***				**IAM**
1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x	Yes
1	1.2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	x	x	x	Yes
1	1.3	Devices	Detect	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		x	x	No
1	1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		x	x	No
1	1.5	Devices	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			x	No

IAM and CIS Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	
2				**Inventory and Control of Software Assets**	***Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.***				
2	2.1	Applications	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	x	x	x	Maybe
2	2.2	Applications	Identify	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	x	x	x	Yes
2	2.3	Applications	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	x	x	x	Yes
2	2.4	Applications	Detect	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		x	x	Maybe
2	2.5	Applications	Protect	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		x	x	Yes
2	2.6	Applications	Protect	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		x	x	Yes
2	2.7	Applications	Protect	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			x	Yes

IAM and CIS Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	
3				Data Protection	*Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.*				
3	3.1	Data	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	No
3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	x	x	x	No
3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	x	x	x	Yes
3	3.4	Data	Protect	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	x	x	x	No
3	3.5	Data	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	x	x	x	No
3	3.6	Devices	Protect	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	x	x	x	No
3	3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	No
3	3.8	Data	Identify	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	No
3	3.9	Data	Protect	Encrypt Data on Removable Media	Encrypt data on removable media.		x	x	No
3	3.10	Data	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		x	x	No
3	3.11	Data	Protect	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		x	x	No
3	3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		x	x	No
3	3.13	Data	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			x	No
3	3.14	Data	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			x	No

IAM and CIS Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	
4				**Secure Configuration of Enterprise Assets and Software**	***Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).***				
4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Maybe
4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Maybe
4	4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	x	x	x	Yes
4	4.4	Devices	Protect	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	x	x	x	Maybe
4	4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	x	x	x	No
4	4.6	Network	Protect	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	x	x	x	No
4	4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	x	x	x	Yes
4	4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		x	x	No
4	4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		x	x	No
4	4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		x	x	Yes
4	4.11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.		x	x	Maybe
4	4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.			x	Maybe

IAM and CIS Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	
5				**Account Management**	***Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.***				
5	5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	x	x	x	Yes
5	5.2	Users	Protect	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	x	x	x	Yes
5	5.3	Users	Respond	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	x	x	x	Yes
5	5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	x	x	x	Yes
5	5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		x	x	Yes
5	5.6	Users	Protect	Centralize Account Management	Centralize account management through a directory or identity service.		x	x	Yes

IAM and CIS Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	
6				**Access Control Management**	***Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.***				
6	6.1	Users	Protect	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	x	x	x	Yes
6	6.2	Users	Protect	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	x	x	x	Yes
6	6.3	Users	Protect	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	x	x	x	Yes
6	6.4	Users	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	x	x	x	Yes
6	6.5	Users	Protect	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	x	x	x	Yes
6	6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		x	x	Yes
6	6.7	Users	Protect	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		x	x	Yes
6	6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x	Yes

IAM and CIS Controls Summary

Identity Management (IdP)

Validate You are Who You Say You are

"Logging into Stuff"

MFA, SSO, Directory Services, User & Endpoint & Device Management, Provisioning, Integrations

CIS Controls 1, 2, 5, 6

Privileged Access Management (PAM)

Apply Least Access Possible Once Inside

"Gaining Access to Stuff"

Roles, Groups, Policies, Credential Vaults, Endpoints Activities, Folders, Processes

CIS Control 3, 4, 6

How to Launch Your IAM Journey

1. What does your MSP need?
2. What Customers are most likely to need IAM now?
3. What Customers are mostly likely to need IAM later?
4. Build a practical rollout plan
5. Find an IAM partner that makes sense for your needs

How to Profit from IAM

1. Build a Program!
2. Add to your existing “Security Package”
3. Resell for $3 - $5/user/month
4. Build in incentives to get your customers started
5. Have your IAM company provide sales materials and talk track
6. ***Consolidate tooling***

Don't forget to fill out your

SESSION SURVEY