WHITEPAPER

MAPPING BEYONDTRUST CAPABILITIES TO CIS CONTROLS 7.1

BeyondTrust

CONTENTS

CIS Controls 7.1

With the volume of cyberattacks growing every day, organizations are increasingly relying on third-parties to help discover, prioritize, categorize, and provide guidance to remediate threats. Once such third party is the Center of Internet Security (CIS).

The latest update, CIS Controls 7.1, was released on April 2, 2019. According to the CIS website, CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

The CIS Controls® and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals.

The five critical tenets of an effective cyber defense system as reflected in the CIS Controls are:

- **Offense informs defense:** Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
- **Prioritization:** Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment. The CIS Implementation Groups discussed below are a great place for organizations to start identifying relevant Sub-Controls.
- **Measurements and Metrics:** Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
- **Continuous diagnostics and mitigation:** Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.
- **Automation:** Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

BeyondTrust has mapped its PAM solutions for privileged password management, endpoint privilege management, and secure remote access into the CIS Controls 7.1. With this mapping, organizations can better optimize the return on their security investments.

BeyondTrust Solution Mapping Key

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges.

Each CIS Control is outlined in the following sections and are mapped to these BeyondTrust solutions:

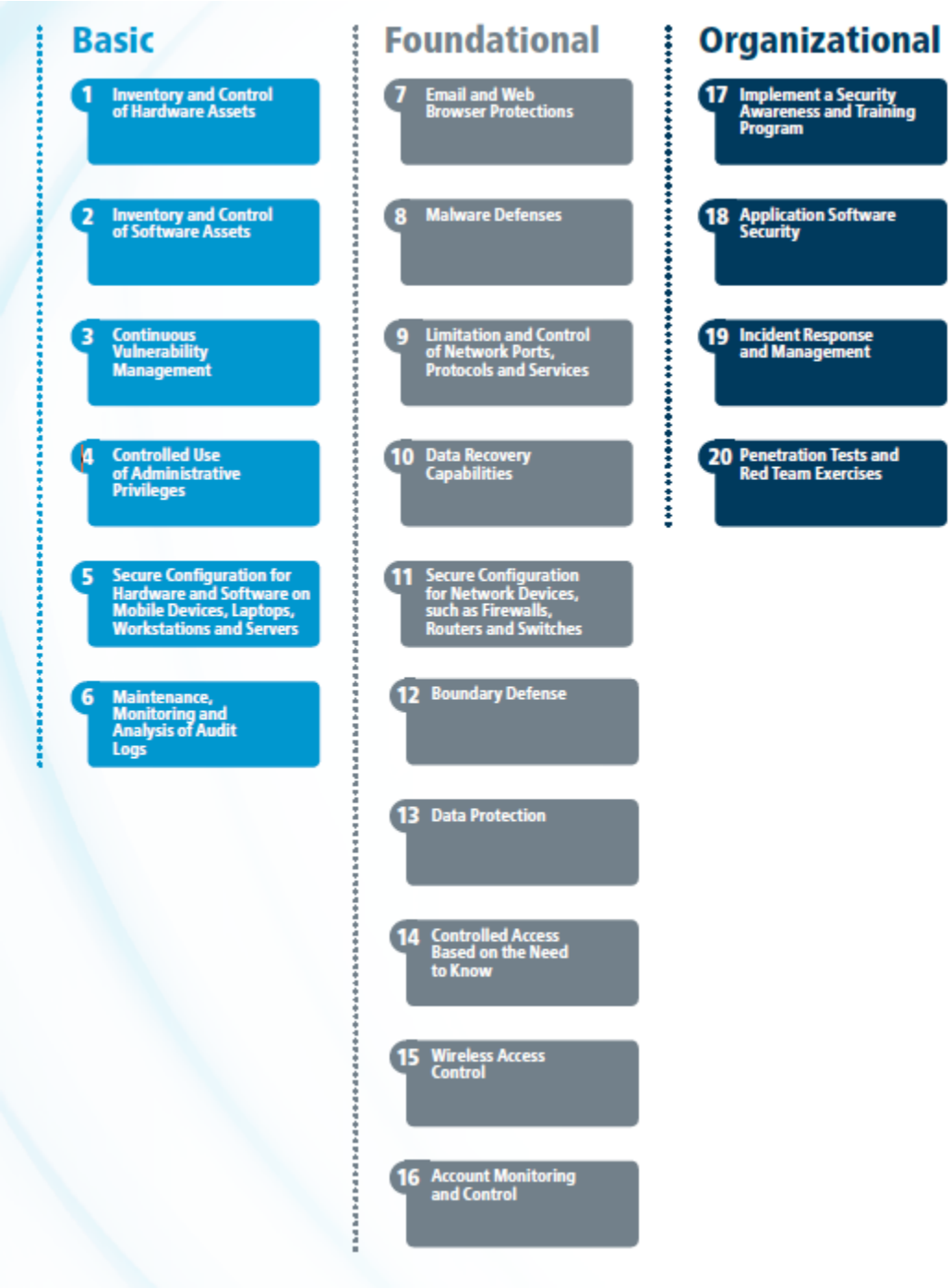
- (PPM) Privileged Password Management - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities.
- (SRA) Secure Remote Access - Apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.
- (EPM) Endpoint Privilege Management - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

These symbols indicate the following:

■ - Broad applicability
O - Partial applicability
n/a - Not applicable

The 20 CIS Controls

Source
www.cisecurity.org/controls



CIS. CIS Controls™ V7.1

Implementation Group 1:

An IG1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of these organizations is to keep the business operational as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. However, there may be some small to medium-sized organizations that are responsible for protecting sensitive data and, therefore, will fall into a higher Group. Sub-Controls selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Sub-Controls will also typically be designed to work in conjunction with small or home office commercial-off-the-Shelf (COTS) hardware and software.

Implementation Group 2:

An IG2 organization employs individuals responsible for managing and protecting IT infrastructure. These organizations support multiple departments with differing risk profiles based on job function and mission. Small organizational units may have regulatory compliance burdens. IG2 organizations often store and process sensitive client or company information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Sub-Controls selected for IG2 help security teams cope with increased operational complexity. Some Sub-Controls will depend on enterprise-grade technology and specialized expertise to properly install and configure.

Implementation Group 3:

An IG3 organization employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. A IG3 organization must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Sub-Controls selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

While this approach provides generalized guidance for prioritizing usage of the CIS Controls, this should not replace an organization's need to understand their own organizational risk posture. Organizations should still seek to conduct their own duty of care analysis and tailor their implementation of the CIS Controls based on what is appropriate and reasonable given their resources, mission, and risks. Using these types of methods, such as those described in CIS RAM, organizations of different Implementation Groups can make risk-informed decisions about which Sub-Controls in their Group they may not want to implement and which higher Group's they should strive for. The intention is to help organizations focus their efforts based on the resources they have available and integrate into any pre-existing risk management process.

Definitions	1	2	3
CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●	●	●
CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.		●	●
CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.			●

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	■	■	■
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	n/a	■	■
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	n/a	■	n/a
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	■	■	■
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	○	■	○

1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	■	■	○
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	n/a	■	n/a
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	■	■	○

2. Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software 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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	■	n/a	■
2.2	Applications	Identify	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	n/a	n/a	n/a

2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	■	n/a	○
2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	■	n/a	○
2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	■	○	■
2.6	Applications	Respond	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	n/a	n/a	■
2.7	Applications	Protect	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	■	■	■
2.8	Applications	Protect	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.	n/a	■	■
2.9	Applications	Protect	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.	○	■	■

2.10	Applications	Protect	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.	■	■	■

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	n/a	n/a	n/a
3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	n/a	n/a	n/a
3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	n/a	n/a	○

3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	n/a	n/a	n/a
3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	n/a	n/a	n/a
3.6	Applications	Respond	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	n/a	n/a	n/a
3.7	Applications	Respond	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	○	n/a	■

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
4.1	Users	Detect	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	■	■	■
4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	■	■	■

4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	■	■	■
4.4	Users	Protect	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	■	■	■
4.5	Users	Protect	Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.	■	■	■
4.6	Users	Protect	Use Dedicated Workstations For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.	■	n/a	■
4.7	Users	Protect	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.	■	■	■
4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	■	■	■

4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	▪	▪	▪

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
5.1	Applications	Protect	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.	n/a	n/a	n/a
5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	n/a	n/a	n/a
5.3	Applications	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	n/a	n/a	n/a

5.4	Applications	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	n/a	n/a	n/a
5.5	Applications	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	n/a	n/a	n/a

6. Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	○	○	○
6.2	Network	Detect	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.	■	■	■
6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	■	■	■

6.4	Network	Detect	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.	■	■	■
6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	■	■	■
6.6	Network	Detect	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	■	■	■
6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	■	■	■
6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	■	■	■

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
7.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	n/a	■	■
7.2	Applications	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	n/a	■	○
7.3	Applications	Protect	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	n/a	■	■
7.4	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	n/a	■	n/a
7.5	Network	Protect	Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	n/a	n/a	n/a

7.6	Network	Detect	Log All URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	■	■	■
7.7	Network	Protect	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	n/a	n/a	n/a
7.8	Network	Protect	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.	n/a	n/a	n/a
7.9	Network	Protect	Block Unnecessary File Types	Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	n/a	n/a	■
7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	n/a	n/a	○

8. Malware Defenses

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 defense, data gathering, and corrective action.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
8.1	Devices	Protect	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	n/a	n/a	■
8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	n/a	n/a	○
8.3	Devices	Protect	Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	n/a	n/a	n/a
8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	n/a	n/a	○
8.5	Devices	Protect	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.	n/a	n/a	n/a

8.6	Devices	Detect	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	n/a	n/a	■
8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	n/a	n/a	n/a
8.8	Devices	Detect	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	■	■	■

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
9.1	Devices	Identify	Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.	■	■	■
9.2	Devices	Protect	Ensure Only Approved Ports, Protocols, and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	■	■	○
9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	■	n/a	■

9.4	Devices	Protect	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	n/a	n/a	n/a
9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	n/a	n/a	n/a

10. Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
10.1	Data	Protect	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.	■	■	n/a
10.2	Data	Protect	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	■	■	n/a
10.3	Data	Protect	Test Data on Backup Media		■	■	n/a
10.4	Data	Protect	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	■	■	n/a

10.5	Data	Protect	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	■	■	n/a

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain documented security configuration standards for all authorized network devices.	n/a	n/a	○
11.2	Network	Identify	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	n/a	■	n/a
11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use, and alert when any deviations are discovered.	n/a	n/a	n/a

11.4	Network	Protect	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.	n/a	n/a	n/a
11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.	■	■	■
11.6	Network	Protect	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.	■	■	■
11.7	Network	Protect	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	■	■	■

12. Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	n/a	n/a	■
12.2	Network	Detect	Scan for Unauthorized Connections Across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	■	n/a	■
12.3	Network	Protect	Deny Communications With Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.	○	■	■
12.4	Network	Protect	Deny Communication Over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	■	■	■
12.5	Network	Detect	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	n/a	n/a	n/a

12.6	Network	Detect	Deploy Network-Based IDS Sensors	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	n/a	n/a	n/a
12.7	Network	Protect	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	n/a	n/a	n/a
12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	n/a	n/a	n/a
12.9	Network	Detect	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	n/a	■	n/a
12.10	Network	Detect	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	n/a	■	n/a
12.11	Users	Protect	Require All Remote Login to Use Multi-Factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	■	■	■

12.12	Devices	Protect	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	▪	▪	o

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
13.1	Data	Identify	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	o	▪	o
13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	▪	▪	n/a
13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	n/a	n/a	n/a

13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	n/a	■	n/a
13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	n/a	n/a	n/a
13.6	Data	Protect	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.	n/a	■	n/a
13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	n/a	n/a	n/a
13.8	Data	Protect	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	n/a	n/a	■
13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	n/a	n/a	n/a

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
14.1	Network	Protect	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	▪	▪	○
14.2	Network	Protect	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	n/a	n/a	n/a
14.3	Network	Protect	Disable Workstation to Workstation Communication	Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro segmentation.	n/a	▪	○
14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	▪	▪	○
14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.	n/a	○	○

14.6	Data	Protect	Protect Information Through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	n/a	■	n/a
14.7	Data	Protect	Enforce Access Control to Data Through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	n/a	■	n/a
14.8	Data	Protect	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	■	■	n/a
14.9	Data	Detect	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	■	■	■

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.	n/a	n/a	n/a
15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	n/a	n/a	n/a
15.3	Network	Detect	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	n/a	n/a	n/a
15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	n/a	n/a	n/a
15.5	Devices	Protect	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	n/a	○	n/a
15.6	Devices	Protect	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.	n/a	n/a	n/a

15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	n/a	■	n/a
15.8	Network	Protect	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which requires mutual, multi-factor authentication.	n/a	n/a	n/a
15.9	Devices	Protect	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.	n/a	n/a	n/a
15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	n/a	n/a	n/a

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
16.1	Users	Identify	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	■	■	■
16.2	Users	Protect	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	■	■	■
16.3	Users	Protect	Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	■	■	■
16.4	Users	Protect	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	■	■	■
16.5	Users	Protect	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	■	■	■
16.6	Users	Identify	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	■	■	■

16.7	Users	Protect	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	■	■	■
16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	■	■	n/a
16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	■	■	n/a
16.10	Users	Protect	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	■	■	n/a
16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	■	■	n/a
16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	■	■	○
16.13	Users	Detect	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.	■	■	○

17. Implement a Security Awareness and Training Program

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
17.1	N/A	N/A	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	○	○	n/a
17.2	N/A	N/A	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	■	■	■
17.3	N/A	N/A	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	n/a	n/a	n/a
17.4	N/A	N/A	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.	n/a	n/a	n/a
17.5	N/A	N/A	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	■	■	■

17.6	N/A	N/A	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.	n/a	n/a	n/a
17.7	N/A	N/A	Train Workforce on Sensitive Data Handling	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.	■	■	■
17.8	N/A	N/A	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	■	■	■
17.9	N/A	N/A	Train Workforce Members on Identifying and Reporting Incidents	Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.	n/a	n/a	n/a

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.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
18.1	N/A	N/A	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.	■	■	■
18.2	N/A	N/A	Ensure That Explicit Error Checking is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	■	■	■
18.3	N/A	N/A	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	■	■	■
18.4	N/A	N/A	Only Use Up-to-Date and Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.	■	■	■
18.5	N/A	N/A	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized, currently accepted, and extensively reviewed encryption algorithms.	■	■	■
18.6	N/A	N/A	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	■	■	■

18.7	N/A	N/A	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	■	■	■
18.8	N/A	N/A	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	■	■	■
18.9	N/A	N/A	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	■	■	■
18.10	N/A	N/A	Deploy Web Application Firewalls	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	■	■	■
18.11	N/A	N/A	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	■	■	■

19. Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
19.1	N/A	N/A	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	n/a	n/a	n/a
19.2	N/A	N/A	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking ad documentation throughout the incident through resolution.	n/a	n/a	n/a
19.3	N/A	N/A	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	n/a	n/a	n/a
19.4	N/A	N/A	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	n/a	n/a	n/a

19.5	N/A	N/A	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.	n/a	n/a	n/a
19.6	N/A	N/A	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.	n/a	n/a	n/a
19.7	N/A	N/A	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	n/a	n/a	n/a
19.8	N/A	N/A	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	n/a	n/a	n/a

20. Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

CIS Sub-Control	Asset Type	Security Function	Title	Description	PPM	SRA	EPM
20.1	N/A	N/A	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	■	■	■
20.2	N/A	N/A	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	■	■	■
20.3	N/A	N/A	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	■	■	■
20.4	N/A	N/A	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	■	■	■
20.5	N/A	N/A	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	■	■	■

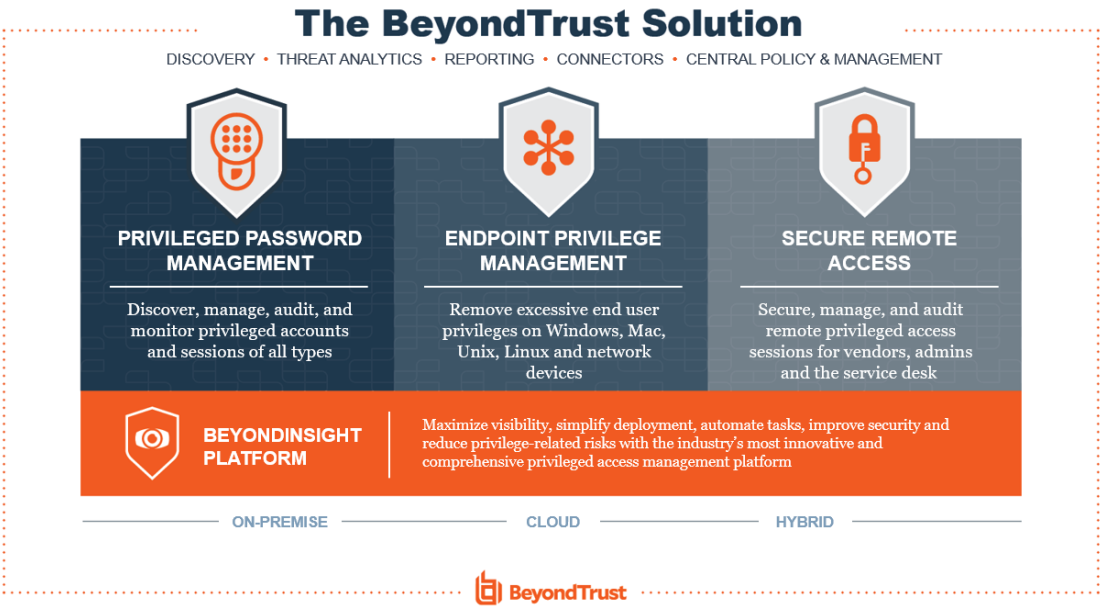
20.6	N/A	N/A	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	■	■	■
20.7	N/A	N/A	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	■	■	■
20.8	N/A	N/A	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes and are removed or restored to normal function after testing is over.	■	■	■

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the 2018 Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.

V2020_04_ENG