ManageEngine

ManageEngine's guide to implementing the **CIS Controls®** in your organization

Table of contents

Table of contents

Disclaimer

A brief introduction to the CIS Controls®

The CIS Controls are a prescriptive, prioritized set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks. These controls help organizations strengthen their cyberdefense and help support compliance in a multi-framework era. The CIS Controls map to most major compliance frameworks, including the NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, and ISO 27000 series, and regulations such as PCI DSS, HIPAA, NERC CIP, and FISMA. They therefore provide specific guidance and a clear pathway for organizations to achieve the goals and objectives described by multiple legal, regulatory, and policy frameworks.

The structure of the CIS Controls®

The CIS Controls comprise a set of 20 cyberdefense recommendations split into three distinct categories—basic, foundational, and organizational—and these 20 controls are further divided into Sub-Controls. The CIS Controls are not a one-size-fits-all solution; based on your organization's cybersecurity maturity, you can plan and prioritize the implementation of various controls.

Basic CIS Controls (1-6)

These are general purpose security controls that should be implemented by every organization to ensure essential cyberdefense readiness.

Foundational CIS Controls (7-16)

These are controls that organizations should implement to counter more specific technical threats.

Organizational CIS Controls (17-20)

These controls are less focused on technical aspects but more focused on people and processes involved in cybersecurity. They operate at the highest level and are key practices that must be adopted by the organization internally to ensure long-term security maturity.

CIS Controls

Basic	Foundational	Organizational
Inventory and Control of Hardware Assets	Email and Web Browser Protections	Implement a Security Awareness and Training Program
Inventory and Control of Software Assets	Malware Defenses	Application Software Security
Continuous Vulnerability Management	Limitation and Control of Network Ports, Protocols and Services	Incident Response and Management
Controlled Use of Administrative Privileges	Data Recovery Capabilities	Penetration Tests and Red Team Exercises
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	
Maintenance, Monitoring and Analysis of Audit Logs	Boundary Defense	
	Data Protection	
	Controlled Access Based on the Need to Know	
	Wireless Access Control	
	Account Monitoring and Control	

The CIS Implementation Groups

In addition to the basic, foundational, and organizational controls, in the latest version of the CIS Controls, V7.1, the controls are prioritized into Implementation Groups (IGs). Each IG identifies which Sub-Controls are reasonable for an organization to implement based on their risk profile and their available resources.

Organizations are encouraged to self-assess and classify themselves as belonging to one of three IGs to prioritize the CIS Controls for a better cybersecurity posture. Organizations should start by implementing the Sub-Controls in IG1, followed by IG2 and then IG3. Implementation of IG1 should be considered among the very first things to be done as part of a cybersecurity program. CIS refers to IG1 as "Cyber Hygiene"—the essential protections that must be put in place to defend against common attacks.

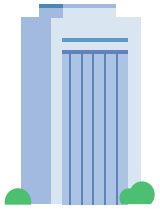
To know more about the CIS Controls and Sub-Controls, please visit their CIS Controls Navigator web page.

IG1

Organizations with limited resources where the sensitivity of data is low will need to implement the Sub-Controls that typically fall into the IG1 category.

IG2

Organizations with moderate resources and greater risk exposure for handling more sensitive assets and data will need to implement the IG2 controls along with IG1. These Sub-Controls focus on helping security teams manage sensitive client or company information.



IG3

Mature organizations with significant resources and high risk exposure for handling critical assets and data need to implement the Sub-Controls under the IG3 category along with IG1 and IG2. The Sub-Controls that help reduce the impact of targeted attacks from sophisticated adversaries typically fall into IG3.

Definitions	1	2	3
IMPLEMENTATION GROUP 1 **An organization with limited resources and risk exposure** CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low with typically fall under IG1. IG1 represents basic cyber hygiene for all organizations including those in IG2 and IG3.	●		
IMPLEMENTATION GROUP 2 **An organization with moderate resources and greater risk exposure** CIS Sub-Controls (safeguards) focused on helping organizations handling more sensitive assets and data. IG2 safeguards should also be followed by organizations in IG3	●	●	
IMPLEMENTATION GROUP 3 **A mature organization with significant resources and high risk exposure** CIS Sub-Controls (safeguards) are necessary for organizations that handle critical assets and data. IG3 encompasses safeguards in IG1 and IG3	●	●	●

"The majority of cyber breaches occur when basic security controls have not been implemented and managed. Implementation Group 1 of the CIS Controls are effective against the Top 5 attacks as described by the Verizon Data Breach Report."

– Curtis Dukes, executive vice president of the Security Best Practices & Automation Group at CIS

The role of ManageEngine solutions

ManageEngine's suite of IT management solutions will help you meet the discrete CIS Control requirements and will in turn aid your organization in carefully planning and developing a best-in-class security program to achieve better cyberhygiene.

ManageEngine products mapped to Controls

We have mapped our products to the CIS Sub-Controls they help meet.

BASIC
CIS CONTROLS

CONTROL 1

Inventory and Control of Hardware Assets

Actively track and manage all hardware devices connected to your network. Maintain an up-to-date inventory of all your technology assets, and have an authentication system in place to ensure that unauthorized devices are prevented from gaining access to your network.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Desktop Central** and **AssetExplorer:** Connect to your Active Directory (AD) environment and scan for inventory details in your infrastructure.		IG2	IG3
1.2	Devices	Identify	Use a Passive Asset Discovery Too	Utilize a passive discovery tool to identify devices connected to the or-ganization's network and automatically update the organization's hardware asset inventory.	**OpUtils:** Periodically scans the network to detect new systems or devices. You can mark systems and devices as trusted, guest, and rogue. Using this tool, you can also block the switch port of rogue devices.			IG3
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.	**OpUtils:** Monitor DHCP scopes to find the available IP address count with the help of the DHCP Scope Monitor. When the available IP address count falls below a certain number,the results are shown in red.		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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 assets, whether connected to the organization's network or not.	**Desktop Central** and **AssetExplorer:** Connect to your AD environment and scan for inventory details in your infrastructure.	IG1	IG2	IG3
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.	**Desktop Central** and **AssetExplorer:** Connect to your AD environment and scan for inventory details in your infrastructure.		IG2	IG3
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.	**OpUtils:** Detect unauthorized devices by conducting manual or automatic scans of your network. You can also mark an IP address as trusted, block a rogue device, and manipulate the ports on your switches to prevent unauthorized devices from accessing your network.	IG1	IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**OpUtils:** Utilize port-level access to shut down or enable an interface connection on a switch port. You can manage the devices connected on a port; however, this action has to be done manually to restrict the devices that can connect to your network. You will have to select the devices (single or multiple) at once to restrict their connection to your network. When adding trusted devices, you can upload a CSV file or configure the product to fetch that information from AD.		IG2	IG3
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.	**Desktop Central:** Scan network computers to obtain inventory data. You can authenticate hardware assets using specific asset certificate details.			IG3

CONTROL 2

Inventory and Control of Software Assets

Have a software inventory system in place to actively track and manage all software running in your network. Utilize application whitelisting to ensure that only authorized software is installed and executed and unauthorized software is blocked.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Desktop Central:** Manage the authorized software in your enterprise.	IG1	IG2	IG3
2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to auto-mate the documentation of all software on business systems.	**Desktop Central:** Scan systems for any software that is installed.		IG2	IG3
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.	**Desktop Central:** Scan systems for software information.		IG2	IG3
2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset invento-ry so all devices and associated software are tracked from a single location.	**Desktop Central:** Get the complete list of software installed on each computer.			IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
2.6	Applications	Respond	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	**Desktop Central:** Schedule an inventory scan, and remove software that is marked as prohibited.	IG1	IG2	IG3
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.	**Application Control Plus:** Scan systems to identify the software installed in your network. You can whitelist apps and allow only those programs to run on managed devices.			IG3
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.	**Application Control Plus:** Build the most secure policy based on the hash value of the executable file. All executable files of the running processes, including those that don't have a valid digital certificate, will be displayed. You can choose all the files that you wish to whitelist; after that, even the smallest change to the file, such as a revision of the file's version, will change its hash value, meaning the file will be removed instantly from the application whitelist.			IG3
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.	**Desktop Central:** Generate reports to identify systems that run business operations.			IG3

CONTROL 3

Continuous Vulnerability Management

Continuously scan your assets to identify potential vulnerabilities and remediate them in a timely manner. Strengthen your network security by ensuring that the software and operating systems used in your organization are running the most recent security updates.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
3.1	Applica-tions	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automati-cally scan all systems on the network on a weekly or more frequent basis to iden-tify all potential vulnerabilities on the organization's systems.	**Vulnerability Manager Plus:** Scan systems for OS vulnerabilities, third-party vulnerabilities, and zero-day vulnerabilities, and reme-diate the vulnerability if the vendor has released a patch for it.		IG2	IG3
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.	**Vulnerability Manager Plus:** The product's agent-based model con-tacts the server every 90 minutes for updates.		IG2	IG3
3.4	Applications	Protect	Deploy Automated Op-erating System Patch Manage-ment Tools	Deploy automated software update tools in order to ensure that the oper-ating systems are running the most recent security updates provided by the software vendor.	**Desktop Central:** Carry out patching multiple ways. The product identifies missing patches in systems and auto-mates patching.	IG1	IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Desktop Central:** The product supports more than 250 third-party applications for patch management.	IG1	IG2	IG3
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.	**Vulnerability Manager Plus:** Vulnerable systems are removed from the vulnerability database only when the vulnerability is fixed. Once the remediation is successful, the product will mark the system as healthy.		IG2	IG3
3.7	Applications	Respond	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	**Vulnerability Manager Plus:** The product categorizes vulnerabilities based on severity and exploit status, and you can deploy patches based on this information.		IG2	IG3

CONTROL 4

Controlled Use of Administrative Privileges

Monitor access controls and user behavior of privileged accounts to prevent unauthorized access to critical systems.

Ensure that only authorized individuals have elevated privileges to avoid misuse of administrative privileges.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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	**Desktop Central:** Get reports on Domain Admin users. **ADManager Plus:** Get reports on all groups in AD and their members. **Password Manager Pro:** Discover resources in your infrastructure and identify the local accounts in your systems.		IG2	IG3
4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	**Desktop Central:** Change passwords for local accounts.	IG1	IG2	IG3
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.	**Password Manager Pro:** Set a unique password for local accounts, or allow the product to create a password by itself.		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**ADAudit Plus:** Receive an alert whenever there is a permission change in AD.		IG2	IG3
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.	**ADAudit Plus:** Access default reports on successful and failed logons.		IG2	IG3

CONTROL 5

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish and maintain security configurations based on your organization's approved configuration standards. Define a rigorous configuration management system that monitors and alerts on misconfigurations and implement a change control process to prevent attackers from exploiting vulnerable services and settings.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved con-figuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	**OS Deployer:** Create an image from an existing system and use it as a template to image other systems (Windows only). The product offers multiple ways to image a system online or offline.		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**OS Deployer:** Change the image repository location to a secured path.		IG2	IG3
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.	**Desktop Central:** Automatically enforce and redeploy configuration settings at every system startup or logon.		IG2	IG3
5.5	Applications	Protect	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.	**Desktop Central:** Get automated alerts when a deployed configuration fails.		IG2	IG3

CONTROL 6

Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events to detect anomalies. Keep log records to understand the details of attacks in order to respond to security incidents effectively.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Desktop Central:** Use a Windows configuration to set a time server for all the systems that Desktop Central manages.		IG2	IG3
6.2	Network	Detect	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.	**EventLog Analyzer:** Get logon reports for workstations, servers, databases, and networking devices like routers and switches.	IG1	IG2	IG3
6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date,user, timestamp, source addresses, destination addresses, and other useful elements.	**EventLog Analyzer:** Get detailed reports on all the elements mentioned in the Control description.		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	**Log360:** Collect logs from various sources and manage them in a single console. (AD logs collected in ADAudit Plus and network logs collected in EventLog Analyzer can be accessed via a single console in Log360.)		IG2	IG3
6.6	Network	Detect	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis.	**Log360:** This product offers comprehensive security information and event management (SIEM).		IG2	IG3
6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	**Log360:** Analyze logs from different sources, including firewalls, routers, workstations, databases, and file servers, with the help of the product's user and entity behavior analytics (UEBA) feature. Any deviation from normal behavior is classified as a time, count, or pattern anomaly. Receive actionable insights via risk scores, anomaly trends, and intuitive reports.		IG2	IG3

FOUNDATIONAL
CIS CONTROLS

CONTROL 7

Email and Web Browser Protections

Secure and manage web browsers and email systems against web-based threats to minimize your attack surface. Disable unauthorized browsers and email client plug-ins, and ensure that users will be able to access only trusted websites by maintaining network-based URL filters.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Browser Security Plus:** Get reports on computers with outdated browsers. Turn on auto-updates for Internet Explorer and Chrome. **Desktop Central:** Install the latest browser versions with the help of the product's software deployment feature.	IG1	IG2	IG3
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.	**Browser Security Plus:** Allow or prevent users from installing extensions and plug-ins.		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Browser Security Plus:** Enable or disable JavaScript on the target machines.		IG2	IG3
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.	**Browser Security Plus:** Whitelist websites in Internet Explorer so that users will be able to access only the trusted websites that have already been configured.		IG2	IG3
7.6	Network	Detect	Log All URL Requests	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.	**Firewall Analyzer:** Collect logs from firewalls, and log the URLs accessed by users (requires a supported firewall).		IG2	IG3
7.7	Network	Protect	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	**Browser Security Plus:** Block access to malicious domains.	IG1	IG2	IG3

CONTROL 8

Malware Defenses

Control the installation and execution of malicious code at multiple points in your enterprise to prevent attacks. Configure and deploy anti-malware software and leverage automation to enable your organization to rapidly update its defenses and take corrective action in time of attack.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Desktop Central:** Push out antivirus updates.	IG1	IG2	IG3
8.3	Devices	Detect	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) and 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.	**Vulnerability Manager Plus:** Identify whether systems in the network have DEP and ASLR enabled		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Media	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	**ADAudit Plus:** Audit removable devices that are plugged into systems, and identify which files have been read, modified, or copied and pasted. **Desktop Central:** Block devices from connecting to your network systems. **Device Control Plus:** Set read-only permissions to the removable devices that connect to systems.	IG1	IG2	IG3
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.	**EventLog Analyzer:** Collect logs from anti-malware systems, and get a holistic view of all the logs collected.		IG2	IG3

CONTROL 9

Limitation and Control of Network Ports, Protocols and Services

Track and control activity across ports, protocols, and services on network devices to reduce the scope of attacks through service vulnerabilities.

Leverage host-based firewalls to ensure only appropriate traffic is permitted access.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Vulnerability Manager Plus:** Get the list of all open ports on each system, as well as the applications that are installed on it.		IG2	IG3
9.2	Devices	Protect	Ensure Only Approved	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	**Desktop Central:** Create configurations to set firewall rules and enable or disable ports.		IG2	IG3
9.3	Devices	Protect	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.	**Vulnerability Manager Plus:** Get all the information you need regarding ports in use across your network systems in a single console with the port audit feature.		IG2	IG3

CONTROL 10

Data Recovery Capabilities

Set up processes and tools to ensure that your organization's critical information is properly backed up, and have a trustworthy data recovery system in place for data restoration to overcome attacks that jeopardize critical data.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
10.1	Data	Protect	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.	**RecoveryManager Plus:** Configure a schedule for backing up Active Directory, Microsoft 365, and on-premises Exchange.	IG1	IG2	IG3
10.2	Protect	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.	**RecoveryManager Plus:** Back up and restore critical systems like domain controllers and Exchange servers when needed.	IG1	IG2	IG3

CONTROL 11

Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Establish, implement, and manage the security configuration of network devices to prevent attackers from taking advantage of vulnerable default settings. Have a strict configuration management and control process in place to ensure that configurations are not exploitable.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain documented security configuration standards for all authorized network devices.	**Network Configuration Manager:** Automatically back up network configurations on a scheduled basis.		IG2	IG3
11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.	**Network Configuration Manager:** Create a baseline configuration for your network and compare it with the current running configurations on your network devices.		IG2	IG3
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.	**Network Configuration Manager:** Ensure your devices have the latest OS updates installed.	IG1	IG2	IG3

CONTROL 12

Boundary Defense

Detect, prevent, and control the flow of information across your network boundaries to prevent attackers from gaining access by bypassing boundary systems. Configure perimeter monitoring, deny unauthorized access, and deploy intrusion detection systems to strengthen boundary defenses.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	**OpUtils:** Get the list of all the subnets in your infrastructure by scanning routers.	IG1	IG2	IG3
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.	**OpUtils:** Receive an alert whenever a new device connects to your network. The network device sends a syslog message to OpUtils to raise the alert.		IG2	IG3
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.	**OpUtils:** Block a switch port upon receiving an alert about communications with known malicious or unused IP addresses, or about access through a suspicious IP address.		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**NetFlow Analyzer:** Monitor flows (NetFlow, JFlow, sFlow, IPFIX, and Netstream) through network boundaries.		IG2	IG3
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.	**EventLog Analyzer:** Generate reports on unusual attacks, targeted systems, and attack trends.		IG2	IG3
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.	**EventLog Analyzer:** This product supports devices from Cisco, Juniper, SonicWall, Barracuda, Palo Alto Networks, WatchGuard, NetScreen, Fortinet, and Check Point. Once configured, EventLog Analyzer automatically collects IDS/IPS logs from these devices and stores them in a central location. The product's predefined reports help cover various aspects of your network and offer insight into your network's overall security standing. Once you identify malicious traffic, you can block it using firewall policies.			IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	**NetFlow Analyzer:** Capture information on flows with the help of a device that has the ability to export flows.		IG2	IG3
12.11	Users	Protect	Require All Remote Log-ins 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.	**Password Manager Pro:** Scan resources in your network, and provide access to users who require it. Disable the users' access when no longer needed. Multi-factor authentication (MFA) is available for logging in to the tool.		IG2	IG3
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.	**Desktop Central:** Manage devices in your WAN to ensure policies are set correctly in your systems			IG3

CONTROL 13

Data Protection

Identify and segregate sensitive data and implement a combination of processes, including encryption, data infiltration protection schemes, and data loss prevention techniques, to ensure the privacy and integrity of sensitive data.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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	**DataSecurity Plus:** Audit the sensitive information that is created, modified, deleted, copied and pasted, or stored in your file servers.	IG1	IG2	IG3
13.6	Data	Protect	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.	**Mobile Device Manager Plus:** Protect enterprise data that is stored in users' mobile devices through containerization.	IG1	IG2	IG3
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.	**Desktop Central** and **Device Control Plus:** Allow specific USB devices to connect to your network.		IG2	IG3
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.	**Device Control Plus:** Allow users to only read information from an external medium.			IG3

CONTROL 14

Controlled Access Based on the Need to Know

Track, control, and secure access to critical assets, such as information, resources, and systems. Allow access to critical information based on a need-to-know basis, and establish detailed logging of servers in order to track access and investigate incidents in which data has been improperly accessed.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Desktop Central:** Provide specific users with access to files and folders. **Password Manager Pro:** Provide specific users with access to systems, databases, applications, and network devices.	IG1	IG2	IG3
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).	**ADAudit Plus:** Collect information on files that have been accessed, modified, or deleted.			IG3

CONTROL 15

Wireless Access Control

Track, control, and secure your wireless local area networks, access points, and wireless client systems to prevent attackers from tampering with your perimeter defenses. Implement a wireless intrusion detection system and conduct vulnerability scanning on wireless client machines to detect exploitable vulnerabilities.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**AssetExplorer:** Scan your network through SNMP and get an inventory of access points in the network.		IG2	IG3
15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Net-work	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	**OpUtils:** Scan your network to identify newly added systems, such as access points. Once a device is detected, you can set custom alerts for specific actions.		IG2	IG3
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.	**OpUtils:** Raise custom alerts for unauthorized access.		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
15.4	Devices	Devices	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	**Desktop Central:** Enable and disable wireless adapters.			IG3
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.	**Desktop Central:** Enable and disable wireless adapters.			IG3
15.9	Devices	Protect	Disable Wireless Peripheral Ac-cess to Devices	Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.	**Desktop Central:** Create a registry setting to disable Bluetooth and NFC on systems.			IG3

CONTROL 16

Account Monitoring and Control

Actively manage the entire life cycle of your systems and application accounts, from their creation, use, and dormancy to deletion, to prevent attackers from exploiting legitimate but inactive user accounts.

Mapping the Sub-Controls to ManageEngine products

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Password Manager Pro:** The solution acts as a central console for infrastructure resources, including systems, applications, networking devices, databases, and websites. Provide access to users, and allow users to access resources from that same portal.		IG2	IG3
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.	**Password Manager Pro:** Enable MFA.		IG2	IG3
16.4	Users	Protect	Encrypt or Hash All Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	**Password Manager Pro:** The database used is encrypted via AES-256		IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
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.	**Password Manager Pro:** Run Password Manager Pro on HTTPS to ensure that no one can eavesdrop while privileged passwords are being shared.		IG2	IG3
16.6	Users	Identify	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	**Password Manager Pro:** Build an inventory of all the accounts discovered in your network.		IG2	IG3
16.7	User	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.	**Password Manager Pro:** Enable and disable users' access when required by using the solution as the central point of contact for all access.		IG2	IG3
16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	**Password Manager Pro:** Disable accounts if needed.	IG1	IG2	IG3

Sub -Control	Asset type	Security function	Control title	Control description	ManageEngine products	Implementation Groups		
						1	2	3
16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	**ADManager Plus:** Configure a workflow to disable an account (AD user) after a configured period of time. **Password Manager Pro:** Rotate the password once the session is completed by the user.	IG1	IG2	IG3
16.10	Users	Protect	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	**ADManager Plus:** Ensure that all accounts have an expiration date. Generate reports for accounts that never expire. Modify accounts in bulk to change their configuration.		IG2	IG3
16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	**Desktop Central:** Lock computers after a period of inactivity with the product's out-of-the-box configuration.	IG1	IG2	IG3
16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	**ADAudit Plus:** Generate alerts for attempts to access deactivated accounts.		IG2	IG3
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.	**Log360:** Understand user behavior with the help of UEBA.			IG3

ORGANIZATIONAL CIS CONTROLS

Unlike the basic and foundational controls, these are practices that your organization should adopt internally to ensure good cyberhygiene.

CONTROL 17

Implement a Security Awareness and Training Program

Implement an integrated plan to educate employees on the specific skills and abilities that they should possess to support the defense of the enterprise according to their functional role in the organization.

CONTROL 18

Application Software Security

Regularly test all your in-house and acquired software for vulnerabilities. Have an effective program to address security throughout the entire life cycle of in-house software, from establishing requirements, training, tools, and testing, and have strict security evaluation criteria while purchasing third-party software.

CONTROL 19

Incident Response and Management

Develop and implement a defined incident management system in your organization to discover attacks quickly, effectively contain the damage, revoke the attacker's access to your network, and restore operations swiftly.

CONTROL 20

Penetration Tests and Red Team Exercises

Periodically assess your organization's readiness to defend against attacks by conducting penetration tests. Simulate the objectives and actions of an attacker with the help of red teams to inspect your current security posture and get valuable insights about the efficacy of your defenses.

The CIS-ManageEngine checklist

We have mapped our products to the corresponding CIS Sub-Controls they support to make it easier for you to identify the right ManageEngine product to meet each Control.

ManageEngine products	Supported Sub-Controls
Desktop Central	1.1, 1.4, 1.5, 1.8, 2.1, 2.3, 2.4, 2.5, 2.6, 2.10, 3.4, 3.5, 4.1, 4.2, 5.4, 5.5, 6.1, 7.1, 8.2, 8.4, 9.2, 12.12, 13.7, 14.6, 15.4, 15.5, 15.9. 16.11
Application Control Plus	2.7, 2.8
Vulnerability Manager Plus	3.1, 3.2, 3.6, 3.7, 8.3, 9.1, 9.3
OS Deployer	5.2, 5.3
Browser Security Plus	7.1, 7.2, 7.3, 7.4, 7.7
Device Control Plus	8.4, 13.7, 13.8
Mobile Device Manager Plus	13.6
AssetExplorer	1.1, 15.1
OpUtils	1.2, 1.3, 1.6, 1.7, 12.1, 12.2, 12.3, 15.1, 15.2
ADManager Plus	4.1, 8.4, 16.9, 16.10
Password Manager Pro	4.1, 4.4, 4.5, 12.11, 14.6, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9
ADAudit Plus	4.8, 4.9, 14.9, 16.12
DataSecurity Plus	13.3
EventLog Analyzer	6.1, 6.2, 8.6, 8.7, 12.6, 12.7
Log360	6.5, 6.6, 6.7, 16.13
RecoveryManager Plus	10.1, 10.2
Firewall Analyzer	7.6
Network Configuration Manager	11.1, 11.3, 11.4, 11.5
NetFlow Analyzer	12.5, 12.8, 13.5

ManageEngine products that will help you with the implementation process

Here is the complete list of ManageEngine products that will help your organization meet the CIS Controls.

Desktop Central: Integrated desktop and mobile device management (On-premises | Cloud | MSP)

Application Control Plus: Application control and endpoint privilege management (On-premises)

Vulnerability Manager Plus: Integrated threat and vulnerability management (On-premises)

OS Deployer: OS imaging and deployment (On-premises)

Browser Security Plus: Browser security and management (On-premises)

Device Control Plus: Data leak prevention for removable devices (On-premises)

Mobile Device Manager Plus: Comprehensive mobile device management (On-premises | Cloud | MSP)

AssetExplorer: ITAM with built-in CMDB (On-premises)

OpUtils: IP address and switch port management (On-premises)

ADManager Plus: AD, Microsoft 365, and Exchange management and reporting (On-premises)

Password Manager Pro: Privileged account management (On-premises | MSP)

ADAudit Plus: AD auditing and reporting (On-premises)

DataSecurity Plus: File auditing, data loss prevention, and data risk assessment (On-premises)

EventLog Analyzer: Log management, IT auditing, and compliance management (On-premises)

Log360: Comprehensive SIEM with advanced threat mitigation and ML-driven UEBA (On-premises | Cloud)

RecoveryManager Plus: AD, Microsoft 365, and Exchange backup and recovery (On-premises)

Firewall Analyzer: Firewall rule, configuration, and log management (On-premises)

Network Configuration Manager: Network change and configuration management (On-premises)

NetFlow Analyzer: Bandwidth monitoring and traffic analysis (On-premises)

Implementation Group and Sub-Control mapping

We have mapped the various CIS Sub-Controls with their respective Implementation Group—IG1, IG2, and IG3—for your better understanding. Visit the CIS Controls Navigator web page for more details.

Implementation Group	Corresponding CIS Sub-Controls
IG1	1.4, 1.6, 2.1, 2.2, 2.6, 3.4, 3.5, 4.2, 4.3, 5.1, 6.2, 7.1, 7.7, 8.2, 8.4, 8.5, 9.4, 10.1, 10.2, 10.4, 10.5, 11.4, 12.1, 12.4, 13.1, 13.2, 13.6, 14.6, 15.7, 15.10, 16.8, 16.9, 16.11, 17.3, 17.5, 17.6, 17.7, 17.8, 17.9, 19.1, 19.3, 19.5, 19.6
IG2	1.1, 1.3, 1.4, 1.5, 1.6, 1.7, 2.1, 2.2, 2.3, 2.4, 2.6, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7, 4.8, 4.9, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.1, 9.2, 9.3, 9.4, 10.1, 10.2, 10.3, 10.4, 10.5, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.8, 12.11, 13.1, 13.2, 13.4, 13.6, 13.7, 14.1, 14.2,14.3, 14.4, 14.6, 15.1, 15.2, 15.3, 15.6, 15.7, 15.9, 15.10, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11, 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7. 20.1, 20.2, 20.4, 20.5, 20.6, 20.8
IG3	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.1, 9.2, 9.3, 9.4, 9.5, 10.1, 10.2, 10.3, 10.4, 10.5, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9, 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9, 15.10, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11, 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8, 20.1, 20.2, 20.3, 20.4, 20.5, 20.6, 20.7, 20.8

Bringing IT together

ManageEngine crafts comprehensive IT management software for all your business needs.

IT service management

- Full-stack ITSM suite
- IT asset management with CMDB
- Knowledge base with user self-service
- Built-in and custom workflows
- Orchestration of all IT management functions
- Reporting and analytics
- Service management for all departments

Identity and access management

- Identity governance and administration
- Privileged identity and access management
- AD and Azure AD management and auditing
- SSO for on-premises and cloud apps, with MFA
- Password self-service and sync
- Microsoft 365 and Exchange management and auditing
- AD and Exchange backup and recovery
- Password self-service and sync

Unified endpoint management

- Desktop management
- Mobile device management
- Patch management
- OS and software deployment
- Remote desktop support
- Web browser security
- Monitoring and control over peripheral devices
- Endpoint privilege management and application control

IT security management

- Unified SIEM for cloud and on-premises
- AI-driven UEBA
- Firewall log analytics
- SSH key and SSL certificate management
- Endpoint device security
- Data leakage prevention and risk assessment
- Regulatory and privacy compliance

IT operations management

- Network, server, and application performance monitoring
- Bandwidth monitoring with traffic analysis
- Network change and configuration management
- Application discovery and dependency mapping
- Cloud cost and infrastructure monitoring
- End-user experience monitoring
- AIOps

IT analytics

- Self-service IT analytics
- Data visualization and business intelligence for IT
- Hundreds of built-in reports and dashboards
- Instant, flexible report creation
- Out-of-the-box support for multiple data sources

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need — more than 90 products and free tools — to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2001, IT teams like yours have turned to us for affordable,feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over 180,000 companies around the world, including nine of every ten Fortune 100 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

Over 180,000 organizations trust ManageEngine with their IT.

ManageEngine

www.manageengine.com

ManageEngine ManageEngine ManageEngine/