

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



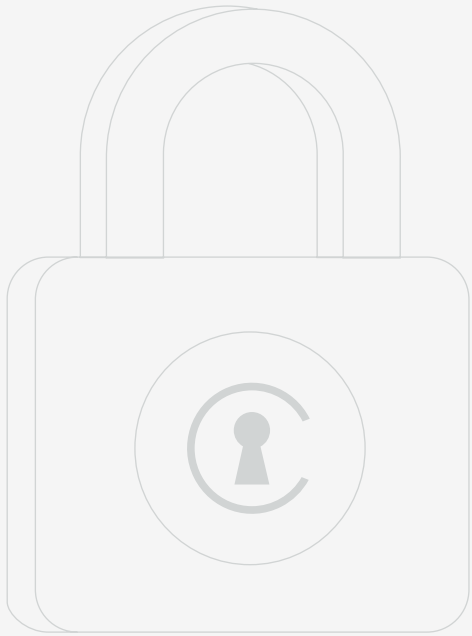
# Table of contents

<b>A brief introduction to the CIS Controls®</b> .....	4
<b>The structure of the CIS Controls®</b> .....	6
<b>The role of ManageEngine solutions</b> .....	8
<b>ManageEngine products mapped to Controls</b> .....	8
<b>Control 1: Inventory and Control of Enterprise Assets</b> .....	
9	
<b>Control 2: Inventory and Control of Software Assets</b> .....	11
<b>Control 3: Data Protection</b> .....	14
<b>Control 4: Secure Configuration of Enterprise Assets and Software</b> .....	16
<b>Control 5: Account Management</b> .....	19
<b>Control 6: Access Control Management</b> .....	21
<b>Control 7: Continuous Vulnerability Management</b> .....	23
<b>Control 8: Audit Log Management</b> .....	25
<b>Control 9: Email and Web Browser Protections</b> .....	28
<b>Control 10: Malware Defenses</b> .....	29
<b>Control 11: Data Recovery</b> .....	30
<b>Control 12: Network Infrastructure Management</b> .....	31
<b>Control 13: Network Monitoring and Defense</b> .....	32
<b>Control 14: Security Awareness and Skills Training</b> .....	36
<b>Control 15: Service Provider Management</b> .....	38
<b>Control 16: Application Software Security</b> .....	39
<b>Control 17: Incident Response Management</b> .....	40
<b>Control 18: Penetration Testing</b> .....	41
<b>ManageEngine products and the Safeguards they support</b> .....	42
<b>ManageEngine products that will help you with the implementation process</b> .....	43
<b>ManageEngine's suite of IT management solutions</b> .....	47

## Disclaimer

Copyright © Zoho Corporation Pvt. Ltd. All rights reserved. This material and its contents (“Material”) are intended, among other things, to present a general overview of how you can use ManageEngine’s products and services to implement the CIS Controls in your organization. Fully complying with the [CIS Controls](#) requires a variety of solutions, processes, people, and technologies. The solutions mentioned in this Material are some of the ways in which IT management tools can help with some of the CIS Controls. Coupled with other appropriate solutions, processes, and people, ManageEngine’s solutions help organizations implement the CIS Controls. This Material is provided for informational purpose only and should not be considered as legal advice for implementing the CIS Controls. ManageEngine makes no warranties, express, implied, or statutory, and assumes no responsibility or liability as to the information in this Material.

You may not copy, reproduce, distribute, publish, display, perform, modify, create derivative works, transmit, or in any way exploit the Material without ManageEngine’s express written permission. The ManageEngine logo and all other ManageEngine marks are registered trademarks of Zoho Corporation Pvt. Ltd. Any other names of software products or companies referred to in this Material and not expressly mentioned herein are the trademarks of their respective owners. Names and characters used in this Material are either the products of the author’s imagination or used in a fictitious manner. Any resemblance to actual persons, living or dead, is purely coincidental.



## A brief introduction to the CIS Controls®

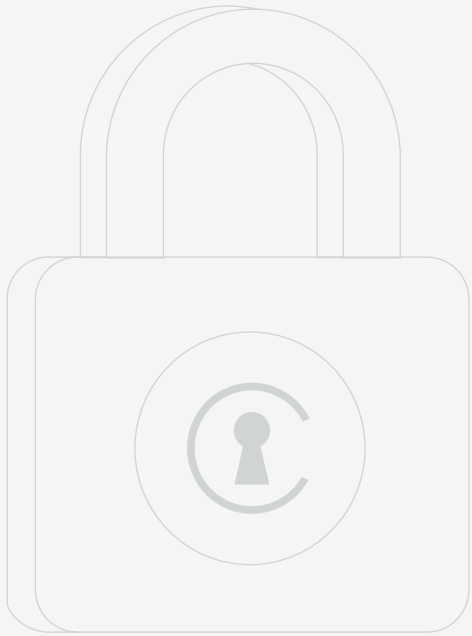
The CIS Controls are a prescriptive, prioritized, and simplified set of cybersecurity best practices and defensive actions that help support compliance in this multi-framework era.

The CIS Controls were formulated by a group of IT experts at the Center for Internet Security (CIS) using information gathered from actual attacks and their effective defenses. They are comprised of 18 cyberdefense recommendations surrounding organizational internet security. Organizations around the world leverage the CIS Controls to get clear guidance on how to achieve the objectives described by multiple legal, regulatory, and policy frameworks. Based on your organization's cybersecurity maturity, risk exposure, and availability of security resources, you can plan and prioritize the implementation of various Controls.

In the latest version, v8, the CIS Controls are split into Implementation Groups (IGs). IGs are self-assessed categories aimed at helping enterprises prioritize the implementation of the CIS Controls.

Implementing all of the CIS Controls is the definition of an effective cybersecurity program. Effectively implementing IG1 represents basic cyberhygiene for any organization. The CIS Controls map to most major compliance frameworks, including the NIST Cybersecurity Framework, NIST 800-53, ISO 27000 series, and regulations such as PCI DSS, HIPAA, NERC CIP, and FISMA.





## CIS Controls

**Control 1: Inventory and Control of Enterprise Assets**

**Control 2: Inventory and Control of Software Assets**

**Control 3: Data Protection**

**Control 4: Secure Configuration of Enterprise Assets and Software**

**Control 5: Account Management**

**Control 6: Access Control Management**

**Control 7: Continuous Vulnerability Management**

**Control 8: Audit Log Management**

**Control 9: Email and Web Browser Protections**

**Control 10: Malware Defenses**

**Control 11: Data Recovery**

**Control 12: Network Infrastructure Management**

**Control 13: Network Monitoring and Defense**

**Control 14: Security Awareness and Skills Training**

**Control 15: Service Provider Management**

**Control 16: Application Software Security**

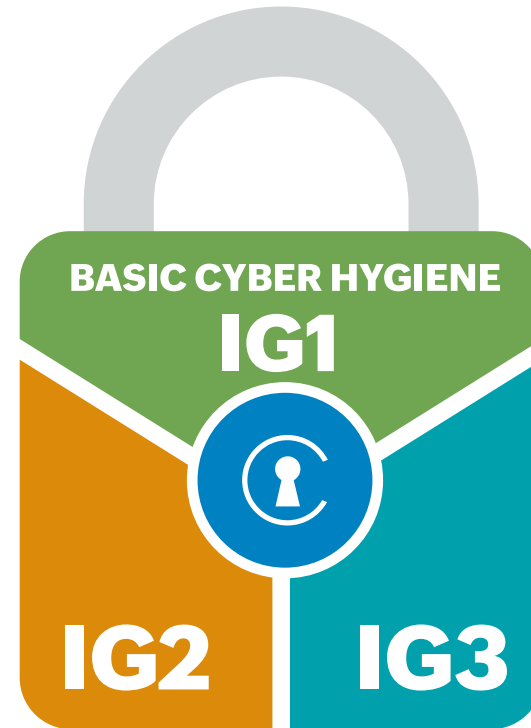
**Control 17: Incident Response Management**

**Control 18: Penetration Testing**

## The structure of the CIS Controls®

The latest version of the CIS Controls, Version 8, comprises a set of 18 cyberdefense recommendations. Version 8, an extension of Version 7, consists of IGs, the new recommended guidance for prioritizing implementation of the Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. They are based on the risk profile of an enterprise and the resources available to the organization to implement the CIS Controls.

Each IG identifies a set of Safeguards (previously referred to as CIS Sub-Controls) that the enterprise needs to implement. There are a total of 153 Safeguards in CIS Controls Version 8. Every enterprise should start with IG1. IG2 builds upon IG1, and IG3 is comprised of all the Controls and Safeguards.





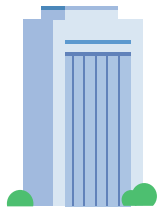
### **Implementation Group 1**

IG1 focuses on basic cyberhygiene. It is comprised of the foundational set of cyberdefense Safeguards that every enterprise should apply to guard against the most common attacks. Small to medium-sized organizations with limited cybersecurity expertise and low-sensitivity data will need to implement the cyberdefense Safeguards that typically fall under the IG1 category.



### **Implementation Group 2**

Organizations with moderate resources (employing individuals responsible for managing and protecting IT infrastructures) and greater risk exposure from handling more sensitive assets and data will need to implement the IG2 Controls along with IG1. These Controls focus on helping security teams manage sensitive client or company information.



### **Implementation Group 3**

Mature organizations with significant resources (employing security experts who specialize in the different facets of cybersecurity) and high risk exposure from handling critical assets and data need to implement the Safeguards under the IG3 category along with IG1 and IG2. Safeguards selected for IG3 abate targeted attacks from sophisticated adversaries and reduce the impact of zero-day attacks.

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.

## **The role of ManageEngine solutions**

ManageEngine's suite of IT management solutions that focus on security and risk management 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 IG Safeguards they help meet. To learn more about this, please reach out to us at [me-consultants@manageengine.com](mailto:me-consultants@manageengine.com)



## Control 1: Inventory and Control of Enterprise Assets

Actively manage all enterprise assets connected to your infrastructure physically, virtually, or remotely, or those within cloud environments, to accurately determine the totality of assets that need to be monitored and protected. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
1.1	Devices	<b>Identify</b>	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	X	X	X	<p><b>AssetExplorer</b> AssetExplorer helps you identify and manage assets in your network. It scans your infrastructure to deliver complete inventory data.</p> <p><b>ServiceDesk Plus</b> If you would like incident management along with asset inventory, you should look at ServiceDesk Plus, which has a built-in asset module.</p> <p><b>Endpoint Central</b> Endpoint Central offers patch management along with inventory management. This inventory is for specific OSs, like Windows, macOS, and Linux.</p>

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
1.2	Devices	<b>Respond</b>	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	X	X	X	<b>OpUtils</b> Handle rogue device detection and prevention with powerful switch port management capabilities, and gain control over who or what is connecting to your network.
1.3	Devices	<b>Detect</b>	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		X	X	<b>OpUtils</b> OpUtils periodically scans routers, switches, and gateway servers to discover the devices in your network.
1.4	Devices	<b>Identify</b>	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		X	X	<b>OpUtils</b> OpUtils' DHCP monitoring tool integrates with IP, switch port, and DHCP management solutions. Having all these features in one console enables you to easily discover and monitor devices connected to your network.
1.5	Devices	<b>Detect</b>	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			X	<b>OpUtils</b> Scan for devices connected to your network and block the switch port when you find an unauthorized device that's connected.

## Control 2: Inventory and Control of Software Assets

Actively manage all software in your network to ensure that only authorized software is installed and executed and that unauthorized and unmanaged software is found and prevented from being installed or executed.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
2.1	Applications	<b>Identify</b>	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	X	X	X	<b>AssetExplorer, ServiceDesk Plus, Endpoint Central</b> All three solutions can scan for software inventory, collecting information such as the vendor and the install date. You can add additional fields to assets or software to note custom details like business process. This can also be achieved using the CMDB of AssetExplorer or ServiceDesk Plus.
2.2	Applications	<b>Identify</b>	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	X	X	X	<b>Endpoint Central, Application Control Plus</b> Whitelist applications and remove any unauthorized software. If software is unsupported but necessary for the fulfillment of your enterprise's mission, it can be documented as an exception.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
2.3	Applications	<b>Respond</b>	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	X	X	X	<b>Application Control Plus, Endpoint Central</b> Use application blacklisting to instantly block applications that might hamper either the security or productivity of your enterprise.
2.4	Applications	<b>Detect</b>	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		X	X	<b>AssetExplorer</b> Scan your network for assets, including installed software, using AssetExplorer.  <b>ServiceDesk Plus</b> ServiceDesk Plus has asset management capabilities along with ITIL functions.  <b>Endpoint Central</b> Carry out patch management for Windows, macOS, and Linux devices with Endpoint Central. The product's inventory feature includes a software inventory.
2.5	Applications	<b>Protect</b>	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		X	X	<b>Application Control Plus, Endpoint Central</b> Whitelist applications and remove any unauthorized software.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
2.6	Applications	<b>Protect</b>	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		X	X	<b>Application Control Plus, Endpoint Central</b> View all executable files of the running processes, including those that don't have a valid digital certificate. 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 instantly removed from the application whitelist. This policy is perfect if you want to run only extremely specific executables.
2.7	Applications	<b>Protect</b>	Allow list Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			X	<b>Application Control Plus, Endpoint Central</b> Whitelist applications not just by vendor or product name but also using a verified executable and file hash.

## Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
3.1	Data	<b>Identify</b>	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	<b>DataSecurity Plus</b> With the help of DataSecurity Plus' Risk Analysis module, you can locate risky content such as PII or ePHI and maintain an inventory of the personal data you store. Scan for passport numbers, email addresses, credit card numbers, and over 50 other types of personal data with preconfigured and customizable data discovery policies. Automate the classification of files containing PII or ePHI to better understand which files need elevated data security measures.
3.2	Data	<b>Identify</b>	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	X	X	X	<b>PAM360</b> Store, manage, and share many types of sensitive data, such as digital certificates, license keys, files, documents, and photocopies. During retrieval, a link to the file is provided for it to be saved locally to the disk.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.		X	X	<b>PAM360, DataSecurity Plus</b> Protect access permissions for local and remote file systems, databases, and applications. Audit file servers via DataSecurity Plus. Manage passwords for databases, applications, and other resources with PAM360.
3.9	Data	Protect	Encrypt Data on Removable Media	Encrypt data on removable media.		X	X	<b>Device Control Plus</b> While we don't offer a solution for encrypting data on removable devices, you can use Device Control Plus to allow only BitLocker-encrypted USB devices to access organizational data in order to view information or perform specific file actions.
3.13	Data	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			X	<b>DataSecurity Plus</b> Discover and classify data. Delete or quarantine files, and stop USB data transfers. Spot instances of anomalous user behavior, and prevent files from being exfiltrated via external storage devices or via email (Outlook).
3.14	Data	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			X	<b>DataSecurity Plus</b> Audit file or folder changes, like creation, movement, deletion, and permission changes.

## Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets and software.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
4.1	Applications	<b>Protect</b>	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	<b>Endpoint Central</b> Endpoint Central's many computer security configurations aid in hardening the security of your endpoints. It offers configurations for certificate distribution; firewall settings, permission management; securing USBs; setting up environmental variables, registry settings, shortcuts, and Wi-Fi settings; power management; group management; managing desktops' display settings and file/folder operations (copy, move, delete); and displaying legal notices and other announcements.
4.2	Network	<b>Protect</b>	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	<b>Network Configuration Manager, OpManager Plus</b> Schedule device configuration backups, track user activity, and spot changes by comparing configuration versions, all from a centralized web GUI.



Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	X	X	X	<b>Endpoint Central</b> With Endpoint Central for desktop operating system and mobile devices you can turn off the display, lock the screen after a specified period of inactivity.
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	X	X	X	<b>PAM360</b> Scan your network and discover critical assets to automatically onboard privileged accounts into a secure vault that offers central management.
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		X	X	<b>Endpoint Central</b> Add the list of software that is prohibited in your company to look for those applications during the regular scan cycles.
4.10	Devices	Respond	Enforce Automatic Device Lock-out on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		X	X	<b>Mobile Device Manager Plus, Endpoint Central</b> Apply policies for passcodes, device auto-lock, and other security features to protect corporate data on enterprise devices.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
4.11	Devices	<b>Protect</b>	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.		X	X	<b>Mobile Device Manager Plus, Endpoint Central</b> Perform remote wipe functionalities on Windows laptops, desktops, and tablets. Windows, Android, and iOS devices are also supported.
4.12	Devices	<b>Protect</b>	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.			X	<b>Mobile Device Manager Plus, Endpoint Central</b> Create containers to segregate enterprise data from personal data, which is especially important for corporate devices.

## Control 5: Account Management

Use processes and tools to assign and manage authorization to handle the credentials of user accounts, including administrator accounts, as well as service accounts associated with enterprise assets and software.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
5.1	Users	<b>Identify</b>	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	X	X	X	<b>PAM360</b> Automatically scan and discover critical accounts for Windows, Solaris, macOS, Linux, Active Directory, VMware, and a host of network devices and databases, and onboard those privileged accounts into a centralized, secure repository. Set time frames for accessing accounts and password discovery attempt limits. Upon discovery, randomize resource passwords in accordance with preconfigured password policies.
5.2	Users	<b>Protect</b>	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	X	X	X	<b>PAM360</b> Automate the process of scheduled password rotation to eliminate manual password change procedures.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
5.3	Users	<b>Respond</b>	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	X	X	X	<b>ADManager Plus</b> Manage and clean up inactive or unused user and computer accounts in bulk, right from ADManager Plus' reports. Once you generate the inactive users or computers report, you can select the desired objects from the report and delete, disable, or move them to a different OU, or even enable the disabled ones, using the management options right within the report.
5.5	Users	<b>Identify</b>	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		X	X	<b>PAM360</b> Auto-discover all your service accounts and manage them. When discovering Windows accounts, PAM360 will also automatically fetch the service accounts associated with services present in the domain members.
5.6	Users	<b>Protect</b>	Centralize Account Management	Centralize account management through a directory or identity service.		X	X	<b>PAM360</b> Consolidate account credentials in one place with our centralized password vault. Add credentials to the vault directly, import them from a CSV, or leverage the automated scanning process.

## Control 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
6.1	Users	<b>Protect</b>	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	X	X	X	<b>PAM360</b> Grant users access to resources by creating user and resource groups.
6.2	Users	<b>Protect</b>	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	X	X	X	<b>PAM360</b> When you remove a user from a user group in PAM360—for instance, because their role changed or they were terminated—their privilege also gets revoked.
6.3	Users	<b>Protect</b>	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	X	X	X	<b>ADSelfService Plus</b> Secure multiple points of access to your organization's sensitive resources using endpoint MFA.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
6.4	Users	<b>Protect</b>	Require MFA for Remote Network Access	Require MFA for remote network access.	X	X	X	<b>PAM360</b> Offer access to network resources within PAM360.
6.5	Users	<b>Protect</b>	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	X	X	X	<b>PAM360</b> Require MFA for logging in to PAM360; this acts as a secondary layer of security.
6.7	Users	<b>Protect</b>	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		X	X	<b>ADSelfService Plus</b> Eliminate the need for multiple user IDs and passwords, streamline the login experience for users, and improve security with single sign-on. ADSelfService Plus uses Active Directory credentials to verify users' identities, and OU and group-based policies to controls access to various cloud applications. Users have to remember only their Windows username and password to access all their enterprise applications.
6.8	Data	<b>Protect</b>	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			X	<b>PAM360</b> By default, PAM360 has six predefined roles that come with a specific set of permissions. If you'd like to create custom roles, you can do that as well.

## Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within your enterprise's infrastructure to remediate flaws and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
7.1	Applications	<b>Protect</b>	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	<b>Vulnerability Manager Plus</b> Scan your network's endpoints for vulnerabilities.
7.2	Applications	<b>Respond</b>	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	X	X	X	<b>Vulnerability Manager Plus, Endpoint Central</b> Identify vulnerabilities on specific OSs, web servers, and databases and fetch the patch the vendor has provided for the vulnerability.
7.3	Applications	<b>Protect</b>	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	X	X	X	<b>Endpoint Central, Patch Manager Plus, Vulnerability Manager Plus</b> Carry out patch management for Windows, macOS, and Linux devices as well as third-party patching.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
7.4	Applications	<b>Protect</b>	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	X	X	X	<b>Endpoint Central, Patch Manager Plus, Vulnerability Manager Plus</b> Automate patch management for Windows, Mac, Linux and third party applications. Apart from security fixes, ensure new features or enhancements for existing applications are updated.
7.5	Applications	<b>Identify</b>	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		X	X	<b>Vulnerability Manager Plus, Endpoint Central</b> Maintain uninterrupted visibility into endpoints across your entire global hybrid IT with our advanced, multipurpose agents. From scanning threats and vulnerabilities to deploying remediations, everything is carried out seamlessly with the help of our lightweight, remote agents.
7.6	Applications	<b>Identify</b>	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	X	X	X	<b>Vulnerability Manager Plus, Endpoint Central</b> Scan devices in your network for software vulnerabilities, zero-day vulnerabilities, system misconfigurations, high-risk software, and web server misconfigurations.



Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
7.7	Applications	<b>Respond</b>	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		X	X	<b>Vulnerability Manager Plus, Endpoint Central</b> Identify vulnerabilities and remediate them by applying the patches provided by the respective vendor.

## Control 8: Audit Log Management

Collect, alert on, review, and retain audit logs of events that could help you detect, understand, or recover from an attack.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
8.1	Net-work	<b>Protect</b>	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	<b>Log360</b> Collect, review, and retain audit logs for enterprise assets.
8.2	Network	<b>Detect</b>	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	X	X	X	<b>Log360</b> Collect logs from various sources in your infrastructure: Windows infrastructure, databases like Oracle Database and MySQL, firewalls, IDSs and IPSs, hypervisors (Microsoft and VMware), Linux and Unix systems, routers and switches, vulnerability scanners, web servers, servers, workstations, cloud platforms, and other applications.
8.3	Network	<b>Protect</b>	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	X	X	X	<b>OpManager Plus</b> Use OpManager Plus to make sure you have enough space to accommodate the collected logs. You can also set thresholds.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
8.5	Network	<b>Detect</b>	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		X	X	<b>Log360</b> Log data collected by Log360 includes event source, date, username, timestamp, source address, and destination address.
8.6	Network	<b>Detect</b>	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.		X	X	<b>ADAudit Plus, Log360</b> Run out-of-the-box reports on your domain, DNS changes, and added, removed, or modified DNS nodes.
8.7	Network	<b>Detect</b>	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.		X	X	<b>Firewall Analyzer, OpManager Plus</b> View the top allowed and denied URLs as part of the web usage reports, with source and destination details.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
8.9	Network	<b>Detect</b>	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.		X	X	<b>Log360</b> Audit Active Directory changes, network device logs, Exchange Server, Exchange Online, Azure Active Directory, and your public cloud infrastructure from a single console.
8.11	Network	<b>Detect</b>	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		X	X	<b>Log360</b> Continuously monitor user and device activity. UEBA learns about every user and creates a baseline of regular activities for each user and entity.  Any activity that deviates from this baseline gets flagged as an anomaly and will generate an alert.

## Control 9: Email and Web Browser Protections

Improve protection and detection of threats from email and web vectors because these are opportunities for attackers to manipulate human behavior through direct engagement.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
9.1	Applications	<b>Protect</b>	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	X	X	X	<b>Browser Security Plus, Endpoint Central</b> Manage browsers, add-ons, extensions, and plug-ins.
9.3	Network	<b>Protect</b>	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		X	X	<b>Browser Security Plus, Endpoint Central</b> Group unapproved websites and restrict access to websites and web applications. Deny access to websites that are not needed in your organization.
9.4	Applications	<b>Protect</b>	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		X	X	<b>Browser Security Plus, Endpoint Central</b> Disable Chrome extensions and only grant access to IT-approved extensions.

## Control 10: Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
10.3	Devices	<b>Protect</b>	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	X	X	X	<b>Device Control Plus, Endpoint Central</b> Disable auto-play.
10.7	Devices	<b>Detect</b>	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.		X	X	<b>Log360</b> Log360 UEBA maintains a risk score for each and every user and entity profile. Whenever an activity log for a user/entity differs from its baseline, the risk score of that particular profile increases. An increased risk score of a profile helps the IT admin look into the matter immediately to prevent any security breach. Based on the risk score, IT administrators can modify the organization's anti-malware software to suit their specific needs.

## Control 11: Data Recovery

Establish and maintain data recovery practices sufficient for restoring in-scope enterprise assets to a pre-incident, trusted state.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
11.3	Data	<b>Protect</b>	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	X	X	X	<b>RecoveryManager Plus</b> Back up Active Directory, Azure AD, Microsoft 365, Google Workspace, and Exchange environments from a single console.

## Control 12: Network Infrastructure Management

Establish, implement, and actively manage network devices to prevent attackers from exploiting vulnerable network services and access points.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
12.1	Network	<b>Protect</b>	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	X	X	X	<b>Network Configuration, Manager, OpManager Plus</b> Determine whether the software on your networking devices is up-to-date. Generate reports on EOS and EOL devices.
12.2	Network	<b>Protect</b>	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		X	X	<b>PAM360</b> Take care of least privilege permission management.
12.4	Network	<b>Identify</b>	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	<b>AssetExplorer, ServiceDesk Plus</b> The CMDB offers a relationship map that is uniquely designed to provide the ability to understand the dependencies between CIs. A CI can either be a physical entity or a virtual one.



## Control 13: Network Monitoring and Defense

Create processes and select appropriate tools to establish and maintain comprehensive network monitoring and defense against security threats across your enterprise's network infrastructure and user base.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
13.1	Network	<b>Detect</b>	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		X	X	<b>ADAudit Plus</b> Collect security event logs from your Windows infrastructure and generate compliance reports based on those details.
13.2	Devices	<b>Detect</b>	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.		X	X	<b>Device Control Plus</b> With the help of Device Control Plus, you can prevent unauthorized removable devices from connecting to your network.  <b>OpUtils</b> Using OpUtils, you can block unauthorized devices from connecting to your network.  <b>DataSecurity Plus</b> With DataSecurity Plus, you can detect and prevent data leaks through USBs and email (Outlook).

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
13.3	Network	<b>Detect</b>	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		X	X	<b>EventLog Analyzer</b> Monitor the logs from your IDS or IPS and extract the information they provide to further secure your network.
13.4	Network	<b>Protect</b>	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.		X	X	<b>NetFlow Analyzer</b> Monitor traffic between two specific sites, which are created based on IP address or IP network. Site-to-site traffic monitoring helps you understand the network traffic behavior between any two user-defined sites and filter traffic that is not necessary for your organization.
13.5	Devices	<b>Protect</b>	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		X	X	<b>Endpoint Central, PAM360</b> Using PAM360, provide the minimum access permissions for assets remotely connected to enterprise resources. Make sure your endpoints are running up-to-date operating system versions and applications via Endpoint Central's patch management, software deployment, and Windows configurations.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
13.6	Network	<b>Detect</b>	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		X	X	<b>NetFlow Analyzer, OpManager Plus</b> Collect logs from your networking devices and generate reports on the top talkers in your network as well as the top source destination, port, and protocol used.
13.7	Devices	<b>Protect</b>	Deploy a Host-Based Intrusion Prevention Solution	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.			X	<b>Device Control Plus</b> With the help of Device Control Plus, you can prevent unauthorized removable devices from connecting to your network.  <b>OpUtils</b> Using OpUtils, you can block unauthorized devices from connecting to your network.  <b>DataSecurity Plus</b> With DataSecurity Plus, you can detect and prevent data leaks through USBs and email (Outlook).

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
13.8	Network	<b>Protect</b>	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			X	<b>NetFlow Analyzer</b> NetFlow Analyzer's Advanced Security Analytics module is a network-flow-based security analytics and anomaly detection tool that helps in detecting intrusions using a Continuous Stream Mining Engine. With the help of the collected flows, you can classify anomalies like bad source destination, suspect flows, and denial-of-service attacks.

## Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to make employees more security-conscious and ensure they have the proper skills to reduce cybersecurity risks to your enterprise.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
14.3	N/A	Protect	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	X	X	X	<b>ADSelfService Plus, PAM360</b> With ADSelfService Plus, you can establish MFA for Windows, macOS, and Linux systems. For enterprise applications and databases, you can achieve this via PAM360.
14.4	N/A	Protect	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	X	X	X	<b>Endpoint Central</b> Manage and optimize the power consumption of computer hardware to save money and energy.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
14.5	N/A	<b>Protect</b>	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	X	X	X	<b>DataSecurity Plus</b> Report on the creation, deletion, overwriting, and renaming of files and folders.
14.7	N/A	<b>Protect</b>	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	X	X	X	<b>Mobile Device Manager Plus, Endpoint Central</b> Manage OS updates for iOS, Android, and Chrome OS devices. You can update immediately, delay deployment, or schedule the update.

## Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for your enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
15.7	Data	<b>Protect</b>	Securely Decommission Service Providers	Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.			X	<b>ADManager Plus</b> Decommission users and file servers without the hassle of dealing with complex custom scripts.

## Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact your enterprise.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	<p>Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p> <p>Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.</p>		X	X	<p><b>Vulnerability Manager Plus, Endpoint Central</b> Scan systems for vulnerabilities and get information on each vulnerability's severity. Identify and deploy the patches available for the vulnerability from the vendor.</p>



## Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Safe guard	Asset type	Security function	Control title	Control description	Implementation Groups			How ManageEngine products can help
					IG1	IG2	IG3	
17.9	N/A	Recover	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			X	<b>ServiceDesk Plus</b> With the help of ServiceDesk Plus' Enterprise Service Management, you can create a portal for your IT security team to handle incidents with unique notifications, SLAs, and escalation procedures. This will not interfere with your regular IT management process.

## Control 18: Penetration Testing

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.

## ManageEngine products and the Safeguards they support



ManageEngine products	CIS Controls v8 Safeguards
<b>ADAudit Plus</b>	8.6, 8.12
<b>ADManager Plus</b>	5.3, 15.7
<b>ADSelfService Plus</b>	6.3, 6.7, 14.3
<b>Application Control Plus</b>	2.2, 2.3, 2.5, 2.6, 2.7
<b>AssetExplorer</b>	1.1, 2.1, 2.4, 12.4
<b>Browser Security Plus</b>	9.1, 9.3, 9.4
<b>DataSecurity Plus</b>	3.1, 3.13, 3.14, 13.2, 13.7, 14.5
<b>Endpoint Central</b>	1.1, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 4.1, 4.3, 4.8, 4.10, 4.11, 4.12, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 9.1, 9.3, 9.4, 10.3, 10.4, 13.5, 14.4, 14.7, 16.2
<b>Device Control Plus</b>	3.9, 10.3, 10.4, 13.2, 13.7
<b>EventLog Analyzer</b>	13.3
<b>Firewall Analyzer</b>	8.7
<b>Log360</b>	8.1, 8.2, 8.5, 8.6, 8.9, 8.11, 8.12, 10.7, 13.1, 13.3
<b>Mobile Device Manager Plus</b>	4.10, 4.11, 4.12, 14.7
<b>NetFlow Analyzer</b>	13.4, 13.6, 13.8
<b>Network Configuration Manager</b>	4.2, 12.1
<b>OpManager Plus</b>	4.2, 8.3, 8.7, 12.1, 13.6
<b>OpUtils</b>	1.2, 1.3, 1.4, 1.5, 13.2, 13.7
<b>PAM360</b>	3.2, 3.3, 4.7, 5.1, 5.2, 5.5, 5.6, 6.1, 6.2, 6.4, 6.5, 6.8, 12.2, 13.5, 14.3
<b>Patch Manager Plus</b>	7.3, 7.4
<b>RecoveryManager Plus</b>	11.3
<b>ServiceDesk Plus</b>	17.9
<b>Vulnerability Manager Plus</b>	7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 16.2

## ManageEngine products that will help you with the implementation process



**Endpoint Central**



**Log360**



**OpManager**



**ServiceDesk Plus**



**PAM360**












**AD360**

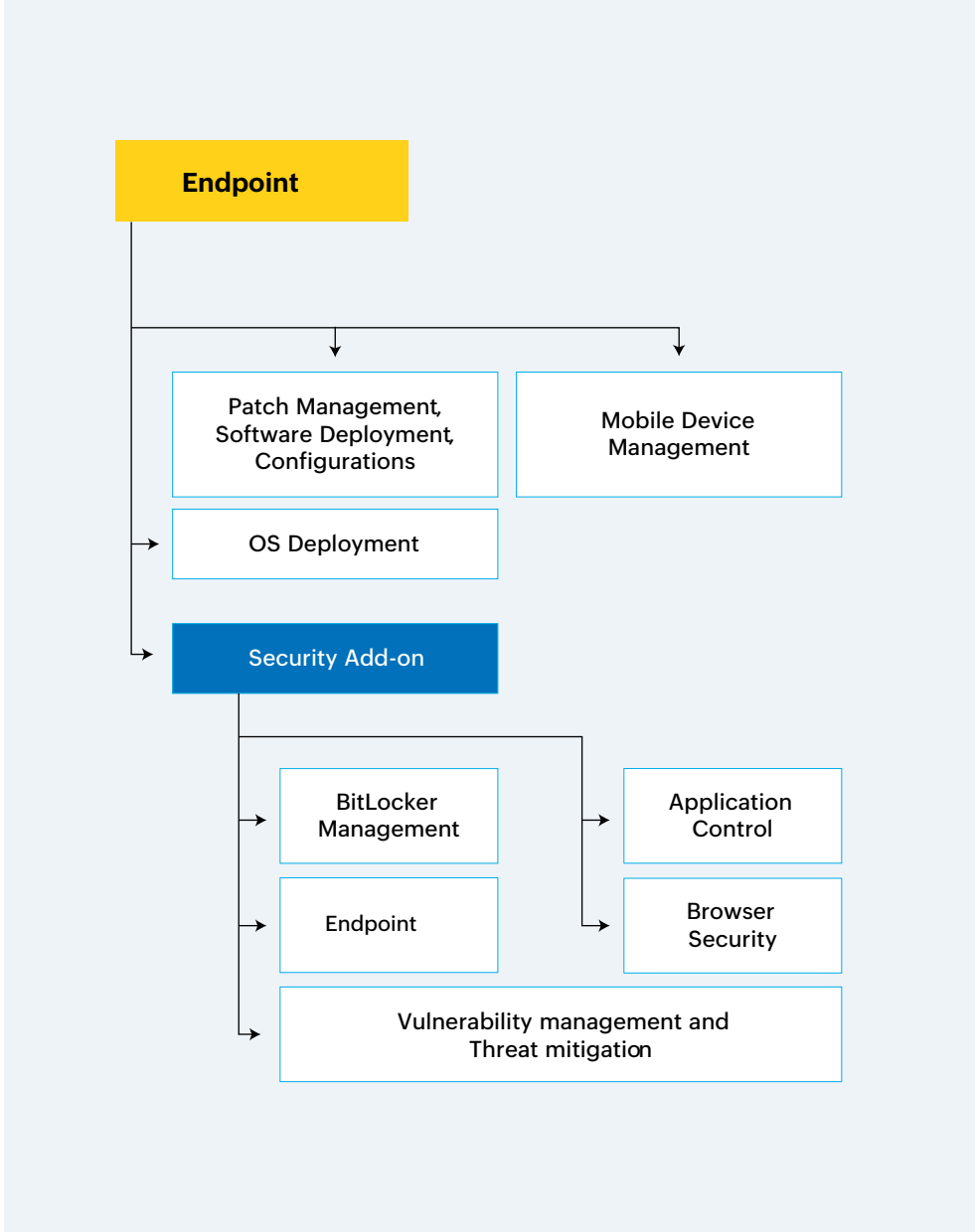



**Data Security Plus**

**18 controls | 24 products | 6 solutions | 1 vendor**


**Here is the complete list of ManageEngine products that will help your organization meet the CIS Con-**


- 
**ADAudit Plus:** Real-time Active Directory, file, and Windows server change auditing
  
- 
**ADManager Plus:** Active Directory, Microsoft 365, and Exchange management and reporting
  
- 
**ADSelfService Plus:** Password self-service, endpoint MFA, conditional access, and enterprise SSO
  
- 
**Application Control Plus:** Software discovery and endpoint privilege management
  
- 
**AssetExplorer:** IT asset management with an integrated CMDB
  
- 
**Browser Security Plus:** Browser security and management
  
- 
**DataSecurity Plus:** File auditing, data leak prevention, and data risk assessment
  
- 
**Device Control Plus:** Data loss prevention for peripheral devices
  
- 
**Endpoint Central:** Unified endpoint management and security





 **EventLog Analyzer:** Comprehensive log and IT compliance management

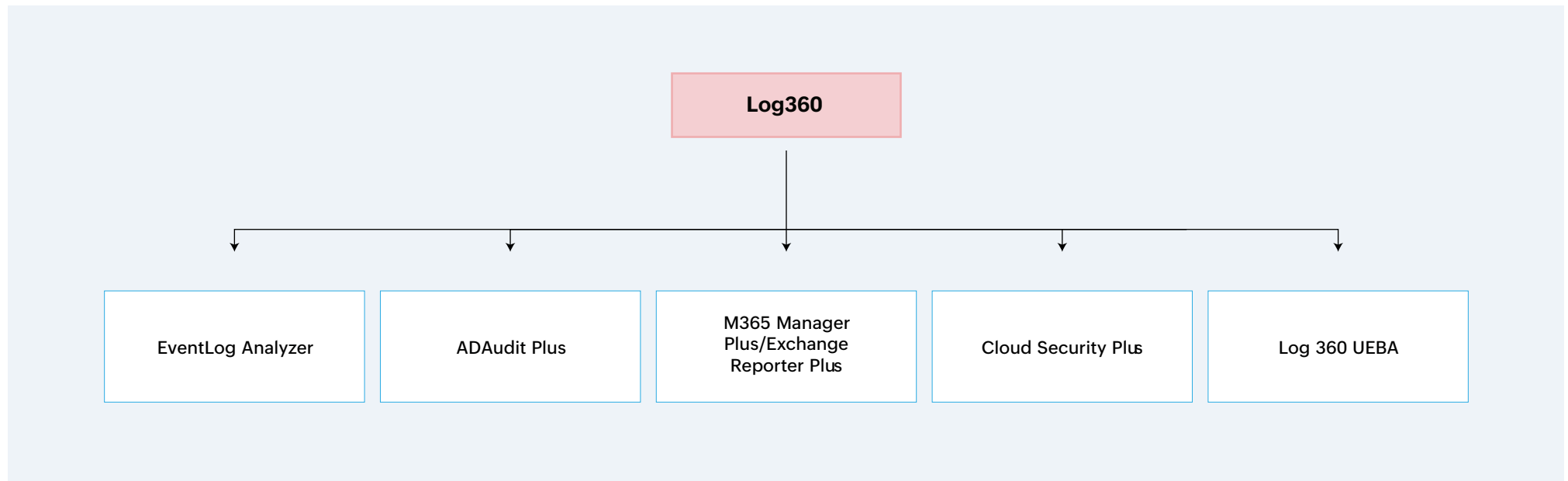
 **Mobile Device Manager Plus:** Comprehensive mobile device management










 **Firewall Analyzer:** Firewall rule, configuration, and log management

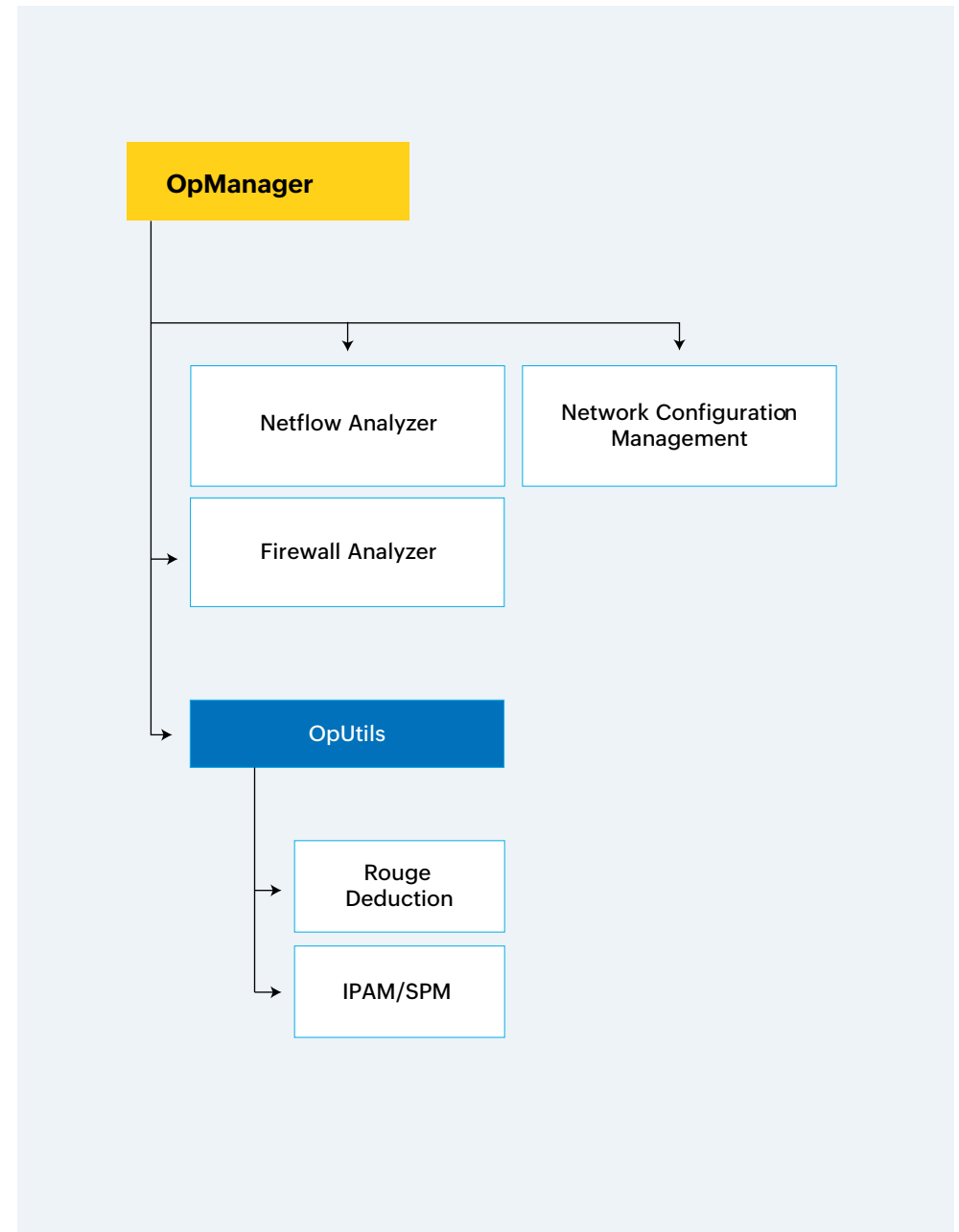
 **NetFlow Analyzer:** Bandwidth monitoring and traffic analysis

 **Log360:** Integrated SIEM with advanced threat analytics and ML-driven UEBA

 **Network Configuration Manager:** Network change and configuration management



-  **OpManager Plus:** Unified network, server, and application management
-  **OpUtils:** IP address and switch port management
-  **OS Deployer:** OS imaging and deployment
-  **PAM360:** Complete privileged access security for enterprises
-  **Password Manager Pro:** Privileged password management
-  **Patch Manager Plus:** Automated multi-OS patch management
-  **RecoveryManager Plus:** Active Directory, Microsoft 365, and Exchange backup and recovery
-  **ServiceDesk Plus:** Full-stack service management for enterprises
-  **Vulnerability Manager Plus:** Prioritization-focused enterprise vulnerability management





# Bringing IT together

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

## **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 & Exchange management and auditing
- AD & Exchange -backup and recovery
- SSH and SSL certificate management

## **Enterprise 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
- Service management for all departments
- Reporting and analytics

## **Unified endpoint management and security**

---

- Desktop and mobile device management
- Patch management Endpoint device security
- OS and software deployment
- Remote monitoring and management
- Web browser security
- Monitoring and control of peripheral devices
- Endpoint data loss prevention

## **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



## **Security information and event manage-**

---

- Unified SIEM for cloud and on-premises
- AI driven user and entity behavior analytics
- Firewall log analytics
- Data leakage prevention and risk assessment
- Regulatory and privacy compliance

## **Advanced 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 120 products and free tools—to manage all of your IT operations, from networks and servers to applications, your service desk, AD, security, desktops, and mobile devices.


Since 2002, 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 280,000 companies around the world, including nine of every 10 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 future opportunities.



# ManageEngine

[www.manageengine.com](http://www.manageengine.com)

 [ManageEngine](#)

 [ManageEngine](#)

 [ManageEngine/](#)