ManageEngine

ManageEngine's guide to complying with the Cyber Essentials scheme

Table of Contents:

Disclaimer

 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 Cyber Essentials compliance in your organisation. Fully complying with the Cyber Essentials 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 parts of Cyber Essentials compliance. Coupled with other appropriate solutions, processes, and people, ManageEngine's solutions help organisations implement the Cyber Essentials. This Material is provided for informational purposes only and should not be considered as legal advice for implementing Cyber Essentials requirements.

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.

Prelude

The Internet is everywhere, and data is inherent in it. In these times of rapid technological evolution, leaning towards cyber hygiene practices is a must to safeguard data. Organisations today are well aware of the damage that could follow a cyberattack. As a risk mitigation strategy, countries across the world have defined regulations and laws that could serve as defences against cyberattacks. A notable certification is the United Kingdom's Cyber Essentials scheme, which has existed for over 10 years. It consists of five technical controls: firewalls, secure configuration, security update management, user access control, and malware protection to guard your organisation's cyber health. The Cyber Essentials scheme is overseen by the National Cyber Security Centre (NCSC), the UK's appointed technical authority, to safeguard critical assets and resources. Complying with it is regarded as a preemptive approach to deflect the most common cyberattacks and gain maximum protection.

What is the Cyber Essentials scheme?

Cyber Essentials is a government-backed certification scheme formulated by the United Kingdom and run by the National Cyber Security Centre (NCSC), the UK's appointed technical authority that provides controls and guidelines to safeguard critical assets and resources. It is considered a minimum cybersecurity standard requirement for all organisations. The purpose of this scheme is to ensure that businesses, devices, and data are protected against common cyberattacks. It applies to companies of all sizes that handle customer data and is mandatory for tendering any central government contracts in the UK.

With updates like the 2025 "Willow" version, it now includes stricter guidelines for remote working, cloud usage, and MFA multi-factor authentication. Achieving Cyber Essentials certification not only strengthens an organisation's security posture but also boosts trust among customers and partners, and often forms part of broader compliance and procurement requirements.

Purpose of the Cyber Essentials scheme

The objectives of the Cyber Essentials scheme are to:

- Identify and implement basic security controls that prevent 80% of common cyberattacks.
- Establish and promote basic cyber hygiene practices among organisations.
- Keep organisations informed about the most common cybersecurity risks.
- Build resilience and lower the rate of insurance claims caused by cyber incidents.

Levels of Cyber Essentials certification

There are two levels under which organisations can be certified:

Level 1: Cyber Essentials

Organisations are required to self-evaluate based on five basic security controls established by the scheme. This can be achieved by completing the self-assessment questionnaire that should be reviewed and attested to by a board member or individual of an equivalent position in the organisation. An independent assessor will verify the questionnaire, and the certification will be awarded based on completing the requirements. The pricing structure of this basic level assessment will vary depending on the size of the organisation.

Level 2: Cyber Essentials Plus

The level 2 assessment is the Cyber Essentials Plus certification that offers a higher level of assurance as it includes a thorough on-site or remote technical audit by an authorised body. Before commencing the test, obtaining written permission from the applicant organisation is essential. Compliance with the security controls is verified by the performance of internal and external vulnerability assessments and a random sampling of systems accessible to internet users. It is necessary to confirm that the scope included in the Cyber Essentials Plus certification is aligned with the one mentioned in the self-assessment certification.

Additionally, when the assessment scope does not involve the “whole organisation,” subsets must be effectively segregated. Compared to the level 1 assessment, Cyber Essentials Plus reflects increased pricing due to its complexity and the time required to complete it. Both certifications can be obtained from any authorised body in the IASME Consortium listings, the NCSC’s official Cyber Essentials delivery partner.

Cyber Essentials 2025 updates

The changes to the Cyber Essentials scheme for the year 2025 are as follows:

1. The term plugins has been updated to extensions. The definition of software has been updated to include extensions instead of plugins, aligning with modern terminology used in browsers and applications.

2. The assessment scope now explicitly includes remote working alongside home working. Not just home working, but any BYOD home and remote devices, routers, and corporate VPN connections used outside of office environments are also under scope for consideration.

3. Starting from 28 April 2025, the “Willow” question set will replace “Montpellier.” All applications filed on or after 28 April 2025 will follow the “Willow” framework.

4. The definition of vulnerability fix is newly added, and the line items include patches, updates, registry fixes, configuration changes, scripts, or any other vendor-approved mechanism to address known vulnerabilities. This was previously limited or referred to as “software updates known as patches or security updates.”

5. Passwordless authentication is a newly added definition that includes, but is not limited to, biometric data, physical devices such as security keys or tokens, one-time codes, QR codes, and push notifications.

6. Apart from password-based and MFA requirements, guidance is provided on passwordless authentication methods under the user access control.

7. Security updates, whether applied automatically, manually, or via third-party tools, are implemented on time. Updates must comply with the new definition of a vulnerability fix.

Organisations seeking certification on or after 28 April 2025 should follow the document's latest version (v3.2). Applications initiated before 28 April 2025 will continue to be governed by the version (v3.1) effective from April 2023.

Cyber Essentials 2023 updates

Clarifications on the technical requirements and other necessary guidance are listed below:

1. Applicants are now only required to list the make and OS for all user devices except firewalls and routers, as cited in the self-assessment question set.

2. The definition of software has been updated to cover only router and firewall firmware.

3. End-user devices that the organisation loans to third parties are now in scope for the assessment.

4. Where default settings are not configurable on specific devices, applicants are now allowed to use the vendor's default settings.

5. The malware protection mechanism should not be signature-based or sandboxed. Instructions on applying relevant antimalware measures have been documented.

6. Guidance is now available on asset management as a core security function and its impact on applicants in alignment with the five technical controls.

7. There is now guidance on the importance of the Zero Trust model in the evolving network architecture landscape.

8. The technical controls have been reordered to accommodate changes in the layout of the self-assessment question set.

9. Revisions have been made to the Cyber Essentials Plus illustrative test specification, considering amendments to malware protection mechanisms.

Here is further clarification on devices not owned by organisations and what is in and out of scope concerning third-parties:

	Owned by your organisation	Owned by a third party	BYOD
Employee	✅	**N/A**	✅
Volunteer	✅	**N/A**	✅
Trustee	✅	**N/A**	✅
University research assitant	✅	**N/A**	✅
Student	✅	**N/A**	❌
MSP adminstrator	✅	❌	❌
Third party contractor	✅	❌	❌
Customer	✅	❌	❌

✅ In scope ❌ Out of scope

User devices connected to the organisation's data should be configured appropriately, even if they are out of the scope of the assessment.

The updated technical requirements and question set are effective April 24, 2023. Applications received on or after this date must align with the revisions of 2022 and 2023.

Cyber Essentials 2022 updates

Here are the major changes brought into this scheme that will be considered for compliance from January 2023 on:

New additions to the scope for assessment under the Cyber Essentials certifications:

- Home working devices
- Cloud services (IaaS, PaaS, and SaaS)
- Thin clients
- End-user devices
- All servers
- Under BYOD: User-owned devices that access organisational data or services
- Subsets to be considered along with the whole of the IT infrastructure used for business (subsets are a part of the organisation with a separate network defined by a firewall or a VLAN)
- Wireless devices within the organisation that use the internet to communicate with other devices and are vulnerable to direct internet attacks

The devices that remote workers use, both personal and company-owned, need to meet all the technical control requirements under Cyber Essentials.

Devices should be unlocked using a password, a PIN with a minimum of six characters, or biometric authentication. A process has also been established to change passwords for suspicious activities.

MFA is also extended to cloud services due to the rising number of attacks in this segment.

Depending on the cloud services, some of the technical controls can be met either by the organisation seeking certification or by the cloud service provider.

However, the implementation of technical control will differ based on cloud service design. The table below shows who would typically be expected to implement each control for the Cyber Essentials certification:

Requirements	Applicant			Cloud provider		
	lass	PasS	SasS	lass	PasS	SasS
Firewalls	✓	✓	✗	✓	✓	✓
Secure configuration	✓	✓	✓	✓	✓	✓
Security update management	✓	✓	✗	✓	✓	✓
User access control	✓	✓	✓	✗	✗	✗
Malware protection	✓	✓	✗	✓	✓	✓

Separate accounts are needed to perform IT admin tasks and minimise risks to privileged accounts.

Cyber Essentials has adopted a tiered pricing structure based on the enterprise size determined by the employee count.

Scope overview

The scope boundary includes either all the devices and software in the organisation's IT infrastructure (for maximum protection) or a well-defined subset for the assessment. The scope boundary has to be clearly defined and agreed upon with the certification body before the assessment commences.

All in-scope devices and software are subject to the requirements if any of the mentioned conditions are met:

- Can accept incoming network connections from untrusted internet-connected hosts
- Can establish user-initiated outbound connections to devices via the internet
- Control the flow of data between any of the above devices and the internet

Administrators can configure device discovery, user roles, and group policies with ManageEngine's Endpoint Central. User access is governed through role-based administration, ensuring users only manage or access devices within their assigned scope. This setup allows clear demarcation of managed assets based on network, location, department, or user privileges.

Asset management and Cyber Essentials

Managing assets is a fundamental requirement for staying aligned with technical controls. Adequate information on the asset management life cycle and overall visibility of the assets in the organisation facilitate effective decision-making and pave the way for better cybersecurity.

Bring your own device (BYOD)

User-owned personal devices for accessing organisational data and services are in scope. The NCSC also issues platform guides in scenarios where users allow traditional full-device management. However, the security risks and challenges, such as protecting corporate data, end-user privacy, complying with the company policies, and meeting support and contractual obligations, emphasise the need to position the relevant technical controls in place.

Home and remote working

Corporate or BYOD home or remote working devices that are used for the organisation's business are in scope for assessment.

Wireless devices

Wireless devices, including wireless access points, are in scope for assessment if internet communication is possible with other devices. Similarly, such devices will be excluded from the cases if there is no possibility of attack via the internet or if they are part of an ISP router located remotely or at home.

Cloud services

Organisational data and services hosted on cloud services are in scope for assessment. Cloud services considered include infrastructure as a service, platform as a service, and software as a service. The implementation of controls might vary between the applicant and the cloud service provider on a case-by-case basis. Please refer to the table explained under the “Cyber Essentials 2022 updates.” When implementing controls on behalf of the applicant, cloud providers must ensure that they are in line with the applicant’s contractual clauses or necessary documents referenced by contracts, like security or privacy statements.

Accounts used by third parties and managed infrastructure

Organisation-owned accounts are under the scope even when such accounts are used by third parties or managed infrastructure. If the organisation opts for externally managed services, technical controls should still be met and demonstrated in the assessment.

Devices used by third parties

End-user devices owned by an organisation and loaned to a third party are part of the scope. Organisations are responsible for configuring devices that are not under the assessment scope but actively interact with organisational data and services. For clarification on devices not owned by an organisation, please refer to the “Cyber Essentials 2023 updates.”

Web applications

All publicly available commercial web applications are covered in the scope of improving security posture. In-house developed, bespoke, and custom components of web applications are not under consideration. Regular testing of applications and assessing through commercially best security standards are advised to minimise vulnerabilities.

Backing up data

Backing up data, whether local or automatic, is not a technical requirement under the scheme, but a comprehensive backup solution is recommended.

Zero Trust architecture

With organisations' increasing adoption of Zero Trust architecture models, the implementation of technical controls will not restrict or prevent the usage of Zero Trust architecture, as defined by the NCSC guidance.

The five technical controls of the scheme

The security control requirements for the certifications are specified under five broad themes discussed below:

Firewalls: Use a firewall to ensure that all your systems, networks, and devices are protected against incoming threats.

Secure configuration: Prioritise security settings for all your systems and devices over ease of use.

Security update management: Deploy patches or security updates periodically to protect your systems and applications against cybersecurity vulnerabilities.

User access control: Provide employees with the access rights they need to fulfill their roles only.

Malware protection: Enforce measures like application allowlisting and restricting access to unsecure websites to avoid malware attacks.

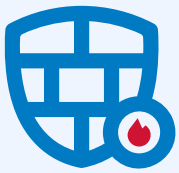
Security control 1: Firewalls

Applicable to boundary firewalls, desktop computers, laptops, routers, servers, IaaS, PaaS, and SaaS

Establish a baseline security standard to restrict unsecured and unnecessary internet access to networks. Secure all your internet-enabled devices with a firewall to distinguish between wanted and unwanted traffic. Implement hardware or software-based firewalls or data flow policies in cloud services to control and monitor web traffic, preventing malicious content from entering your networks and devices. But how do you determine if your firewall functionality is conducive to delivering the expected protection to your networks and devices?

Hygiene measures required to keep firewalls or network devices with firewall functionality at utmost protection include switching to strong and unique passwords, tracking inbound firewall rules approval and documentation, removing or disabling unnecessary firewall rules, preventing and gating access to the administrative interface through MFA, and IP allowlisting, blocking unauthenticated inbound connections by default.

How can ManageEngine help?



Firewall Analyzer

This software analyses the usage of firewall rules and fine-tunes them for maximum effectiveness. With this solution, you can view audit log information to track all the activities of the firewall users and receive notifications from its custom alert profile in case of anomalous activities in the network. The firewall security log reports help security admins analyse and visualise threat scenarios and strategise accordingly.

Security control 2: Secure configuration

Applicable to servers, desktop computers, laptops, tablets, mobile phones, thin clients, IaaS, PaaS, and SaaS

Default configurations are often set to enable ease of use in computers and network devices. However, such standardised processes also make threat entries possible. Publicly known preset admin accounts and credentials or access without MFA, preinstalled unnecessary applications or services, and pre-enabled user accounts that are unnecessary are all mediums through which an attacker might make their entry.

With the application of secure technical controls, vulnerabilities can be minimised. In the case of computers and network devices, organisations must necessarily remove or disable user accounts, software, or an unauthorised auto-run feature during file execution that could potentially bring malware risks. Also includes regular password resets to offboard default or guessable passwords, appropriate user authentication methods, and device locking controls for physical user handling.

Digital or physical credentials are a must for authenticating any device that demands a user's physical presence to access its services. Device locking controls, like biometric tests, PINs, or passwords, should be protected against brute-force attacks by either of the following methods:

- Permit no more than 10 device unlock attempts in 5 minutes.
- Do not permit another device unlock attempt after 10 failed attempts.

The vendor's default settings can be used when the above configuration is unlikely. Where the intention is only to unlock a device, a minimum password or PIN of at least six characters would suffice. However, if the device unlocking credentials involve authentication, guidance under user access control must be applied.

How can ManageEngine help?

Password Manager Pro

Store, access, and share passwords securely using the solution's centralised vault. Automate required periodic password resets while using critical systems and provide real-time alerts on password access. Password Manager Pro's role-based access control feature helps ensure that only authorised personnel can access the resources and passwords stored in its vault.

PAM360

Enable MFA and access control workflows that leverage the solution's just-in-time privileged access. This ensures that only authorised users can remotely access sensitive data for a specific period. Perform periodic password resets for cloud solutions. Centrally store IaaS infrastructure access keys and privileged user credentials, and log in to SaaS applications in a single click.

Endpoint Central

Implement application allowlisting and application sandboxing to permit only authorised applications to run, thereby preventing malware intrusions, threats, and Zero Day attacks. With a well-organised script repository that is written and tested by Endpoint Central, organisations can streamline their configuration processes, enhance automation, and ensure consistency across endpoints. Scan the network for vulnerabilities and audit on a regular basis, disable default settings, encrypt data, and set strong passwords and ensure account lockout policies.

Log360

Log360 and Log360 Cloud detect configuration drift and flag security misconfigurations through audit trail analysis. The capabilities include identifying the use of default configurations (for example, accounts with default credentials, unencrypted protocols) and insecure services by parsing logs from OS, AD, and network devices.

AD360

Strengthen security with a granular password policy for all accounts and fortify your infrastructure using over 19 MFA methods, including passwordless options and conditional access. Mitigate brute-force attacks by configuring account lockout policies based on invalid login attempts. Reduce the attack surface by automatically identifying and removing stale or inactive user accounts.

Security control 3: Security update management

Applicable to servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, IaaS, PaaS, SaaS

[Vulnerability fixes previously limited to only patches or security updates, now include patches, updates, registry fixes, configuration changes, scripts, or any other mechanism approved by the vendor to fix a known vulnerability]

Any software is prone to vulnerabilities, which could open opportunities for security compromise when left unattended. Product vendors extend support for vulnerabilities on a timely or immediate basis. In some cases, vendors might roll out a single update to fix multiple issues with differing levels of security. As a cautionary measure, such updates must be installed within 14 days of their release. Having the right vulnerability management tools in place is pivotal to boosting security.

Software requirements for in-scope devices:

1. All software must be licensed and supported by the vendor.
2. Unsupported software must be removed from devices or excluded from the assessment scope.
3. Automatic updates should be enabled wherever feasible.
4. Security updates must be applied within 14 days of release if they address:

- Vulnerabilities classified by the vendor as critical or high risk
- Vulnerabilities with a CVSS v3 base score of 7.0 or above
- Vulnerabilities where the vendor provides a fix but does not specify the severity

Note: For Cyber Essentials purposes, vulnerabilities are considered critical or high risk if they:

- Have a CVSS v3 base score of 7.0 or higher (or)
- Are designated as critical or high risk by the vendor, regardless of CVSS score

How can ManageEngine help?

Endpoint Central

Automate the entire patch testing and deployment process to shield your network from security threats. This unified endpoint management and security solution also detects vulnerabilities through periodic scans, instantly mitigates them using patches or alternative fixes, and is capable of much more.

Patch Manager Plus

Secure your systems and applications by enabling automated patch deployment for OSs and third-party applications. Test patches before deployment to eliminate security risks. Gain visibility into the patch status of endpoints with real-time audits and reporting. The solution also helps patch remote endpoints in a work-from-home setup.

Vulnerability Manager Plus

Scan and detect firewall misconfigurations, web server misconfigurations, and vulnerabilities in your local and remote office endpoints. Ensure that your network systems initially grant the least privileges and utilise complex passwords and memory protection. The solution also helps you comply with the Security Technical Implementation Guide and the Center for Internet Security guidelines.

Network Configuration Manager

Network Configuration Manager integrates with NIST and other vendor sources to fetch the latest vulnerability data daily. It automatically updates its vulnerability database and identifies at-risk devices. Further, it lists the CVE ID, base score, severity level, and direct links to relevant patch information. Configlets also make simultaneous firmware upgrades across multiple devices possible.

Security control 4: User access control

Applicable to servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS, and SaaS

Ensure that user accounts are accessed only by authorised individuals, and the scope extends to devices and information essential to fulfilling their roles. This approach significantly limits the leak of sensitive information. Establishing a strong user life cycle management process, removing or turning off special access privileges when no longer needed, enabling password authentication, implementing MFA, and maintaining separate accounts for administrative purposes are some of the essential requirements as suggested by the NCSC. Most importantly, in case of an account or password compromise, a protocol to change or reset passwords must be in place. Organisations are encouraged to implement appropriate access controls based on their risk profile and practical use cases.

Password-based authentication

Below is a list of protective measures to consider regarding password management. A user is expected to include at least one method under each scenario.

1. To shield the users from a simple brute force attack, implementing MFA, throttling the rate of attempts to not more than 10 guesses in five minutes, and locking devices after 10 unsuccessful login attempts.

2. To manage quality passwords, enabling MFA, using at least 12 characters as a minimum with no maximum limit, or eight minimum characters with no maximum limit, and blocking commonly used passwords with a predefined list of password combinations.

3. Restrict users from maintaining common passwords, keeping up with secure password storage, password creation with three random words, and no strict rules on password expiry and complexity.

Multi-factor authentication

Apart from using a single password, MFA enables a user to have more than one credential and a password to access a particular device or information. Consider this as an extra layer of security to protect corporate data. Some of the additional factors that could be used for this purpose include:

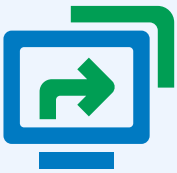
- A trusted device (key-based credential and a local user verification)
- An application (authenticator app or a push-based authentication app)
- A physically separate token (hardware-based code generators)
- A known or trusted account (single-use codes sent to registered email or contact number)

While accessing online services, it is recommended that you prefer the ones that are supported by multiple MFA methods, contextually authenticated, and supported by corporate single sign-on (SSO) practices.

Passwordless authentication

Passwordless authentication is an alternative to traditional passwords for verifying user identities. This is considered a more secure approach where reliance is placed on mediums like biometric authentication, security keys or tokens, one-time codes, and push notifications.

How can ManageEngine help?



Access Manager Plus

Regulate access to remote systems through secure channels from a unified console. Scrutinise access requests and approve them on a case-by-case basis by establishing a request-release workflow. Provide temporary role-based access to third parties, record privileged user sessions, shadow user sessions, and revoke access instantly upon detecting any anomalous activities.

PAM360

Identify and automatically onboard privileged accounts separately into secure vaults to provide role-based access permissions, policy-based conditional access based on real-time risk assessment, Zero Trust protection, and encryption. Consolidate and securely store all passwords in the centralised password vault. Closely monitor privileged accounts to detect any unusual activities with the help of PAM360's anomaly detection capabilities.

Endpoint Central

Supports local user account management and rolls out regular reports on inactive users and accounts. With a well-organised script repository that is written and tested by Endpoint Central, organisations can streamline their configuration processes, enhance automation, and ensure consistency across endpoints. This unified endpoint management solution also detects vulnerabilities through periodic scans, instantly mitigates them using patches or alternative fixes, and is capable of much more.

Application Control Plus

Implement application allowlisting and application sandboxing to permit only authorised applications to run, thereby preventing malware intrusions, threats, and Zero Day attacks.

Log360

Log360 and Log360 Cloud provides exhaustive auditing of user access events (for example, logon and logoff, privilege use, group membership changes). It helps track and report inappropriate or unauthorised access and privilege escalation activities, fulfilling the control's requirement for monitoring access boundaries and misuse.

AD360

Manage the entire identity life cycle, from automated provisioning and deprovisioning of accounts and access. Enforce the principle of least privilege with granular role-based access control and remove or disable special access privileges when no longer required. Secure every access point with adaptive MFA, including passwordless authentication methods such as FIDO2 Passkeys, biometric data, email verification, QR code verification, and more, while maintaining strong password policies where required. Delegate administrative tasks through secure workflows without elevating native permissions, and continuously audit all access changes to ensure complete policy compliance. Manage the access permissions for critical file servers and clean up unused user accounts and empty security groups to avoid unauthorised access.

Network Configuration Manager

Network Configuration Manager grants admins the benefit of assigning roles and scopes to operators. Only the assigned scope of devices will be accessible to operators. The admins can delete users if they are no longer needed. Admins will be notified of the configuration changes made to assigned devices. Upon their acceptance, the configuration will be taken towards the product. This creates a secure environment and restricts unauthorised changes from going out.

Security control 5: Malware protection

Applicable to servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS, and SaaS

When malware takes control of the systems in the network, potential impacts include loss of the organisation's data, system malfunctioning, and continued destabilisation. The cause is associated with malicious actions like installing unauthorised software, downloading, including those from application stores, and email attachments.

Implement a malware protection mechanism on all devices in scope as a fundamental security measure. While most software has it built-in, third-party providers are also preferable. Some standard practices that can safeguard your organisation from malware:

- Enable antimalware and keep it aligned with vendor recommendations.
- Block access to malicious websites and malicious code executables.
- Execute application allowlisting on devices.

Antimalware, whether built-in or purchased from a third party, should always be updated and configured in accordance with Cyber Essentials requirements.

How can ManageEngine help?

Malware Protection Plus

Identify and mitigate real-time threats with a dedicated antimalware engine and AI and ML behaviour assistance. Strengthen defences through automatic signature updates and policy-based scanning. Identify, isolate, and remove infected malware to stop malware from spreading to critical assets and counter in-memory and fileless threats. Restore infected endpoints to their original state by quarantining and reducing downtime in operations.

Endpoint Central

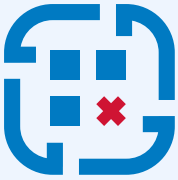
Implement application allowlisting and application sandboxing to permit only authorised applications to run, thereby preventing malware intrusions, threats, and Zero Day attacks. Maintain a least privilege model and enable application-specific privilege elevation to enhance security. Blocklist unknown or unauthorised applications and threats from an executable level control to reduce attack possibilities. With the next-gen antivirus feature, proactively detect, prevent, and mitigate malware threats.

Ransomware Protection Plus

Identify ransomware attacks at a 99.9% accuracy rate with advanced detection capabilities and isolate infected devices to stop ransomware spread. Halt malicious processes to counter in-memory and fileless threats. Quickly rollback and restore files and systems to their original state with a patented single click recovery technology.

Log360

Instantly notify the IT personnel upon detecting anomalous activities in the system using Log360 Cloud's predefined alert profiles. Block access to malicious websites and applications by performing regular web content filtering. Mitigate external threats by detecting known attack patterns, like denial-of-service, distributed denial-of-service, SQL injection, and ransomware attacks, with the Log360 Cloud's real-time event log correlation engine.



Application Control Plus

Implement application allowlisting and application sandboxing to permit only authorised applications to run, thereby preventing malware intrusions, threats, and Zero Day attacks.

Certifications and regulations that apply to ManageEngine products

ManageEngine solutions comply with a number of standards and certifications, including:

Trusted by

ManageEngine solutions:

Identity and access management

Manage, govern, and secure digital identities and privileged access

Unified service management

Design, automate, deliver, and manage IT and business services

Unified endpoint management and security

Manage and secure desktops, servers, laptops, mobile devices, and web browsers

IT operations management and observability

Monitor and manage your network, servers, and applications

Security information and event management

Secure your network from cyberattacks and ensure compliance

Advanced IT analytics

Visualise IT data and gain actionable insights into IT operations

Low-code app development

Build powerful custom applications rapidly and launch them on-premises

IT management for MSPs

Grow your MSP business with scalable and secure IT management solutions

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, 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. 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.

To learn more,
visit www.manageengine.com.