ManageEngine

Malware Protection Plus

AI-driven malware protection that detects threats, prevents breaches and adapts to the evolving threat landscape

Table of Contents

Introduction

Company Overview

History: Formerly known as AdventNet Inc., Zoho Corporation started its operations in 1996 delivering web-based network management tools for telecom service providers. In 2002, the company diversified into IT management solutions for small, medium, and large enterprises. In 2005 with cloud taking off the company forayed into business SaaS with the introduction of Zoho Writer. By 2009, as the product portfolio became vast and diverse, the company was rechristened Zoho Corporation, which now serves as the umbrella firm for four distinct divisions: ManageEngine, Zoho.com, Qntrl, and TrainerCentral.

About our Company: ManageEngine is the enterprise IT management division of Zoho Corporation. We offer comprehensive on-premises and cloud-native IT and security operations management solutions for global organisations and managed service providers. With a powerful, flexible, and AI-powered digital enterprise management platform, we help businesses get their work done from anywhere and everywhere better, safer, and faster.

Established and emerging enterprises organisations-rely on ManageEngine's real-time IT management tools to ensure the optimal performance of their IT infrastructure, including networks, servers, applications, endpoints and more. ManageEngine has 18 data centres, 20 offices and 200+ channel partners worldwide to help organisations tightly align their business to IT.

ManageEngine's solutions include tools for Identity and Access Management, Enterprise Service Management, Endpoint Management and Security, IT Operations Management, Security Information and Event Management, Advanced IT Analytics, and Low-code app development.

Our Global Market: ManageEngine's solutions are industry-agnostic, designed to support organizations of all sizes across diverse sectors. In the UK, our customer base spans a wide range of industries, with strong adoption across BFSI, Healthcare, Government and Public Sector, Manufacturing, Education, IT & Technology, and

Hospitality, among others. This broad presence reflects the flexibility and scalability of our portfolio in addressing varied IT management and security needs.

Our Values & Goals

Simplicity without compromise

We aim to simplify IT management without sacrificing functionality. Our solutions are designed to be intuitive, easy to deploy, and straightforward to manage eliminating unnecessary complexity and reliance on third-party services.

Customer-led innovation

Customer needs drive our product strategy. Backed by a strong in-house R&D team, we continuously develop solutions that address real-world IT challenges, guided by direct feedback and hands-on usage.

Transparency and long-term value

We follow a transparent pricing model with no hidden costs. Our solutions are built to scale with organisations of all sizes, ensuring sustained value as business requirements evolve.

Empowering business-aligned IT

We focus on enabling strong alignment between IT and business objectives through continuous innovation, contextual integrations, and forward-looking solutions that support long-term growth.

Product Introduction

Malware Protection Plus is a modern next-generation antivirus and endpoint protection solution designed to safeguard enterprise devices against today's most complex and fast-evolving cyberthreats. It provides a multi-layered security framework that combines AI-powered malware detection, behavioral analytics, exploit prevention, endpoint isolation, and fileless attack defense.

Through a lightweight agent and a centralized management console, Malware Protection Plus continuously monitors endpoints, analyzes suspicious behavior, and blocks threats before they can disrupt operations.

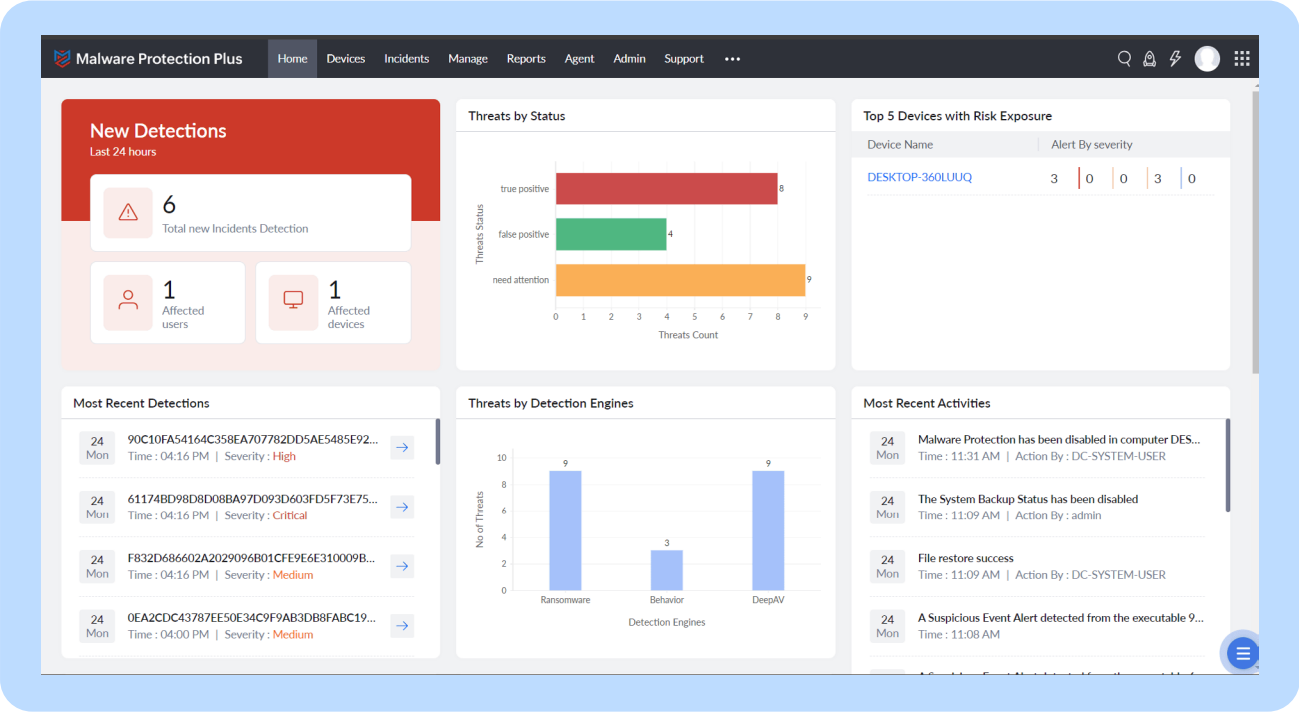

Figure 1: Screenshot of service console

Its deep-learning–based detection engine identifies known, unknown, and zero-day threats, while its integrated EDR capabilities provide attack-chain forensics, MITRE-mapped insights, and automated remediation workflows.

With Malware Protection Plus, IT and SecOps teams can detect malware, prevent ransomware, stop fileless attacks, investigate incidents, isolate compromised endpoints, roll back malicious changes, and restore affected systems quickly from a single, intuitive platform designed for operational efficiency and scalable security.

How it helps

Enterprises today face a threat landscape where traditional signature-based antivirus alone is no longer sufficient. Attackers routinely use obfuscation, fileless techniques, legitimate system tools, and zero-day exploits to bypass legacy defenses. This makes endpoint protection one of the most critical layers in an organization's security posture.

Malware Protection Plus addresses these challenges by combining next-generation antivirus, behavioral detection, and EDR into a single cohesive solution. Its machine-learning models detect emerging and previously unseen threats, while its behavioral engine identifies malicious actions in real time, even when devices are offline. For ransomware events, the solution stops encryption attempts, preserves clean copies of critical data, and allows swift point-in-time recovery to minimize downtime.

Security teams gain complete visibility into endpoint activity through MITRE-aligned attack-chain forensics, enabling faster investigations and clearer root-cause analysis. Automated cleanup, rollback actions, and instant endpoint isolation ensure incidents are contained quickly without manual intervention.

By consolidating protection, detection, response, and recovery into one platform, Malware Protection Plus empowers organisations to strengthen cyber resilience, reduce operational complexity, and maintain secure, compliant, disruption-free endpoints across their entire workforce.

Who might benefit

Executive & Strategic Leadership

- Chief Information Security Officer (CISO): Gains stronger threat prevention, faster incident response, and improved cyber resilience across the organisation.
- Chief Information Officer (CIO): Benefits from reduced operational complexity, centralized management, and improved compliance.
- Chief Technology Officer (CTO): Ensures technology environments remain secure, stable, and aligned with transformation initiatives.
- Head of Risk & Compliance: Gains visibility into endpoint risks, attack paths, and audit-ready reporting.

Security & Threat Management Teams

- Security Operations Center (SOC) Managers & Analysts (L1–L3) using EDR telemetry, MITRE-mapped detections, isolation controls, and forensic insights for faster investigations.
- Threat Hunters & Incident Responders leveraging behavioral analytics, attack-chain reconstruction, and anomaly insights for proactive hunting.
- Cybersecurity Engineers working with SIEM, SOAR, and other detection systems to strengthen defensive architecture.
- IT Infrastructure & Endpoint Management Teams: IT Administrators / System Administrators benefit from unified agent management, low resource usage, and simplified ransomware recovery.
- Endpoint Engineering Teams seeking to gain consistent protection across laptops, desktops, and servers without performance impact.
- IT Operations Managers wanting to achieve streamlined remediation workflows and reduced device downtime.
- Helpdesk & Desktop Support Technicians relying on automated cleanup, rollback, and infection containment to resolve issues faster.

Compliance, Governance & Audit Functions

- Internal Audit Teams: Gain complete visibility into endpoint events and attack-chain forensics.
- Data Protection Officers (DPOs): Reduce risk of data breaches, exfiltration, or regulatory violations.
- Governance, Risk & Compliance (GRC) Teams: Benefit from strong device-level controls and clear reporting for regulatory adherence.

Business-Critical Operational Roles

- Heads of Remote & Hybrid Workforce Management: Ensure distributed employees remain protected—even offline.
- Business Continuity & Disaster Recovery Leaders: Gain faster endpoint recovery in the event of cyber incidents.

Benefits

1. Stop advanced attacks with multi-layered detection and zero-day defense.

Modern cyberthreats rarely rely on a single technique. They blend malware, fileless attacks and phishing payloads. Multi-layered detection counters this by combining signature-based scanning, behavioral analytics, threat hunting and zero-day defense. This ensures threats are intercepted even before they are fully understood or weaponised. The outcome is a dramatically reduced risk of breach, fewer successful intrusions, and a security posture resilient enough to withstand modern attack chains.

2. Ensure rapid recovery with built-in backup and fast point-in-time restoration.

When systems are compromised or data becomes corrupted, the organisation's resilience hinges on how quickly operations can be restored. By capturing consistent point-in-time snapshots directly from the endpoint, the solution enables fast and precise restoration of critical files and configurations without relying on external cloud infrastructure or complex automation layers. This allows IT teams to recover quickly from ransomware damage, accidental deletion, or system failures while maintaining complete control over where data resides and how it is restored.

3. Protect administrative environments with secure, policy-driven role-based access controls.

Within modern IT and SecOps teams, unrestricted or loosely managed console permissions can expose organisations to configuration drift, accidental missteps, or malicious insider activity. Role-based access controls establish a structured, least-privilege model where each administrator receives only the permissions required for their function. This creates a more controlled, audit-ready operational environment where sensitive administrative actions are protected, tracked, and aligned with organisational governance standards.

4. Simplify IT operations using one lightweight, unified endpoint agent.

Traditional security stacks often rely on multiple bulky agents that compete for resources, slow devices, and flood networks with constant updates. A lightweight, unified agent eliminates this burden by consolidating essential protections into a single, efficient footprint that runs quietly without taxing CPU, memory, or storage. Its minimal bandwidth consumption ensures that even remote workers on unstable or low-speed connections remain fully protected without experiencing performance degradation.

5. Detect sophisticated online threats before they impact business continuity.

Many attacks begin with subtle early signals- malicious URLs, phishing attempts, unusual behavior or anomalous content downloads. Proactive detection monitors these indicators and blocks threats before they reach endpoints. This prevents business-impacting incidents such as credential theft, ransomware staging, and data exfiltration. The organisation experiences fewer interruptions, avoids costly remediation, and maintains uninterrupted business operations.

6. Centralize visibility and control through a single, intuitive management console

Managing security from multiple disconnected tools leads to blind spots, inconsistent configurations, and slower incident response. A single management console brings all endpoint data, alerts, statuses, and controls into one unified view. IT gains immediate clarity on threats, compliance, and device health, allowing for faster decisions, tighter governance, and a more predictable security environment.

7. Accelerate threat response and forensics using VirusTotal intelligence and MITRE-mapped detections.

By correlating events with VirusTotal intelligence and aligning detection patterns with the MITRE ATT&CK framework, IT teams gain deep contextual insight into how threats behave and where they originate. This dramatically shortens investigation time and enables analysts to respond with precision instead of guesswork. The result is faster containment, improved root-cause analysis, and stronger long-term defence against recurring attack vectors.

8. Reduce security complexity by replacing legacy antivirus with AI-powered protection.

Traditional antivirus tools struggle against modern, rapidly evolving threats. AI-powered protection learns from vast threat datasets and adapts in real time, eliminating dependence on outdated signature updates. This upgrade reduces operational friction, lowers false positives, and enhances overall detection accuracy. Organisations benefit from a more efficient, cost-effective security stack that future-proofs their endpoint protection strategy.

9. Strengthen cyber resilience with ML-based behavioral detection and exploit prevention.

Attackers increasingly bypass traditional defenses by using fileless techniques, memory exploits, and living-off-the-land tools that leave no obvious signatures behind. Behavioral detection monitors how processes, scripts, and applications behave in real time, identifying suspicious patterns such as privilege escalation, unauthorized memory access, or abnormal script execution. Paired with exploit prevention, it stops attacks at the technique level before they can take root, cutting off ransomware spread and data exfiltration attempts. This combination empowers organisations to maintain operational continuity even against highly adaptive threats, ensuring that systems remain stable, breaches are contained early, and cyber resilience becomes a built-in strength rather than a reactive effort.

Figure 2: Benefits of the solution

Associated Services

Malware Protection Plus offers a range of associated services that can bebought alongside the main service. These include:

1. APIs: Malware Protection Plus provides APIs that allow for integration with other systems and applications, enabling seamless data exchange and automation.

2.Professional Services: ManageEngine offers professional services to assist with the implementation, customisation, and optimisation of Malware Protection Plus. Our team of experts can provide guidance and support to ensure a smooth deployment and maximise the value of the service

3.Maintenance and Support: We provide ongoing maintenance and support services to ensure the smooth operation of the service. This includes regular updates,bug fixes, and technical assistance to address any issues or concerns.

4.Workshops and User Conferences: ManageEngine conducts workshops where users are given a deep-dive on the product based on business challenges and use-cases along with an opportunity to avail a product associate certification.

5.Product customisations and feature requests: Malware Protection Plus is open to facilitate any customer use-case/feature after careful internal vetting.

6.Online Documentation: Malware Protection Plus provides in-depth help documentation that is hosted online at https://www.manageengine.com/malware-protection/help/mp-overview.html, which provides step by step guidance for security analysts, administrators, technicians, and end-users. These associated services enhance the functionality and value of Malware Protection Plus, providing a comprehensive solution for endpoint based next-gen antivirus.

Product Features

1. ML-powered malware detection with deep learning for advanced endpoint protection

Machine learning-powered detection uses deep neural networks to identify malicious files based on patterns, behaviors, and attributes that are too subtle for signature-based antivirus tools to catch. Instead of relying solely on known threat indicators, the model generalizes from millions of data points to identify suspicious activity even when dealing with new or modified strains of malware. This strengthens protection against rapidly evolving threats, polymorphic malware variants, and sophisticated adversaries. Organisations benefit from a dramatically reduced likelihood of infection, especially in scenarios where attackers attempt to bypass traditional security with custom payloads or rapidly shifting malware families.

2. Proactive ransomware defense with tamper-proof backups and single-click recovery

Ransomware defense begins long before a payload begins encrypting data. By monitoring suspicious encryption behavior, process anomalies, and unauthorized file modifications, the system can intervene early in the attack chain. If files are compromised, tamper-proof local backups allow IT teams to restore data instantly with a single recovery action, bypassing ransom demands entirely. This eliminates the long restoration cycles associated with external backup systems and empowers teams to quickly return devices to a usable state. Organisations maintain business continuity, avoid costly downtime, and eliminate the financial and operational leverage attackers often gain during ransomware incidents.

3. Fileless attack prevention through memory scanning and behavioral analytics

Fileless attacks operate directly in memory, leveraging legitimate tools and system processes to evade disk-based scanning. Preventing these attacks requires constant

visibility into process behavior, script execution, and memory operations. By combining memory scanning with exploit prevention and behavioral analysis, the system detects unusual process injections, unauthorized PowerShell or WMI activity, and exploit attempts targeting applications or the OS. This stops adversaries who rely on stealthy techniques such as living-off-the-land binaries, making it extremely difficult for attackers to remain hidden. The result is stronger protection for systems frequently targeted by advanced, evasive threat actors.

4. Zero-day threat detection using anomaly modeling and pre-execution file inspection

Zero-day threats exploit unknown vulnerabilities or use previously unseen malware strains that traditional tools cannot detect. Anomaly-based models evaluate files and executable behavior before they run, analyzing intent to determine whether a program is safe. This pre-execution inspection ensures threats are stopped before they ever start, significantly reducing the risk of compromise on endpoints that handle untrusted downloads, email attachments, or files from removable storage. Organisations gain the confidence that even undisclosed vulnerabilities or emerging attack techniques cannot easily bypass their defenses.

5. Endpoint isolation to contain lateral movement and block active cyberattacks

When a device shows signs of compromise, seconds matter. Endpoint isolation allows IT or SecOps to cut off all network communication from the affected machine while still maintaining a secure channel for investigation and remediation. This stops attackers from moving laterally through the network, harvesting credentials, or spreading malware to other devices. In high-risk environments such as finance, healthcare, or manufacturing, this containment mechanism prevents widespread disruptions and keeps the blast radius of an attack extremely small. It ensures that incidents remain localized and manageable.

6. Autonomous remediation with rollback, backup restoration, and malware cleanup automation

Autonomous remediation handles the full cleanup process from start to finish. If malware modifies system files or registry settings, the agent automatically reverts them to a known good state using forensic snapshots. If important data is altered or encrypted, local backups can be restored immediately without requiring IT to manually intervene. Malicious artefacts are removed, processes terminated, and system integrity restored. This automation significantly reduces the workload on security teams, shortens mean time to remediation, and ensures compromised systems return to normal operation quickly, even when incidents occur outside standard support hours.

7. Attack-chain forensics mapped to MITRE TTPs for complete endpoint visibility

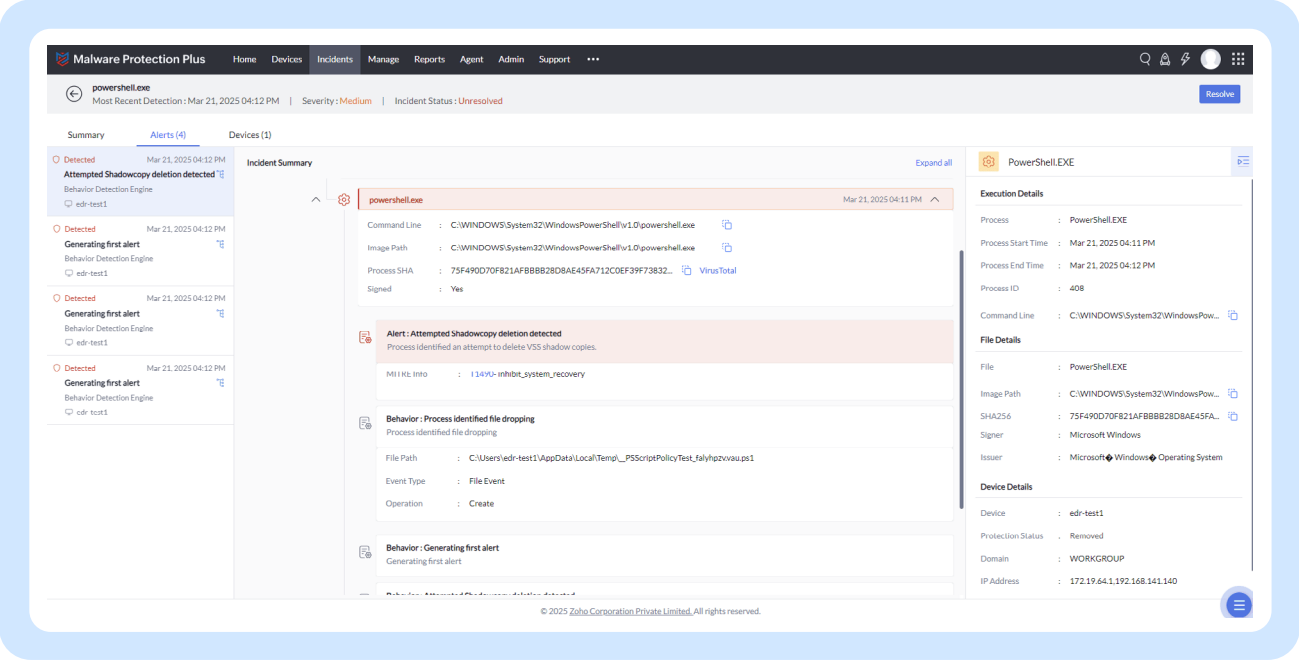

Figure 3: Behavior detection alerts tree

Understanding how an attacker moved through a system is critical for preventing repeat incidents. By mapping events and behaviors to MITRE ATT&CK IDs, the system provides a clear, structured narrative of how a threat entered, what actions it attempted, and which components were affected. This allows analysts to quickly identify root causes, evaluate the scope of compromise, and improve security controls. For organisations with compliance requirements or audit needs, this forensic clarity strengthens reporting and helps build a long-term defensive strategy grounded in real attacker behavior.

8. On-device behavioral detection providing continuous protection even during offline operation

Devices are not always connected to the corporate network, yet attackers can strike anywhere, during travel, offsite operations, or in remote field environments. On-device behavioral detection eliminates dependency on cloud lookups by analyzing processes, scripts, and system actions directly on the endpoint. Even without internet access, the agent can block suspicious behavior, stop exploit attempts, and contain threats. This ensures that users working offline, in low-bandwidth areas, or on isolated networks remain fully protected, closing a critical gap in modern endpoint defense.

9. Centralized web console with role-based access and reporting

A single, centralized console provides IT and security teams with real-time visibility into all endpoints, alerts, and security events. Role-based access ensures administrators receive only the permissions needed for their responsibilities, reducing internal risk and improving operational governance. This centralization streamlines day-to-day operations, accelerates incident response, and enhances organisational oversight.

10. Data exfiltration prevention by analyzing abnormal data flows and user behavior

Data exfiltration often happens quietly through unusual file transfers, suspicious uploads, or misuse of legitimate applications. By monitoring data flow patterns, network usage, and user actions, the system identifies and blocks attempts to move sensitive information off the endpoint. Behavioral analytics detect anomalies such as large file

movements, unauthorized cloud uploads, or atypical after-hours activity. This protects intellectual property, customer information, and regulated data from leaking, whether due to compromised accounts, malicious insiders, or advanced attackers.

Data Protection

Information Assurance

ManageEngine adheres to industry-leading security standards and has implemented robust security measures to protect sensitive information. ManageEngine follows best practices and complies with relevant policies and standards. ManageEngine has a strong commitment to information security and employs processes and facilities to safely manage data. The service prioritises data protection, confidentiality, and integrity, ensuring that organisations can trust their identity management processes. By implementing ManageEngine solution, organisations can have confidence in the security of their identity-related information and mitigate the risk of unauthorised access or data breaches.

As part of the development team's training, they are briefed about the various networking protocols that are used in the product and are encouraged to use only secure communication protocols such as HTTPS and TLS in their code.

- To ensure access to critical information by the development team, measures such as strong passwords, controlled access to test machines, and network segmentation are implemented.
- All the data collected through online forms has a field to obtain consent for collecting and processing data from the prospect.
- Marketing team members are strictly asked to check if a prospect has given consent to receive marketing communications before sending marketing emails.
- Support and pre-sales engineers who communicate directly with customers are trained to maintain privacy of customer information.
- Dedicated guidelines on handling customer data has been given to the members of the team in light of regulations such as GDPR.
- The customer data is stored in databases that can be accessed only by authorised employees.

Data Backup, Data Restoration and Disaster Recovery

ManageEngine runs incremental backups everyday and weekly full backups of our databases using Zoho Admin Console (ZAC) for ManageEngine's Data Centres (DC). Backup data in the DC is stored in the same location and encrypted using AES-256 bit algorithm. We store them in tar.gz format. All backed up data are retained for a period of three months. If a customer requests for data recovery within the retention period, we will restore their data and provide secure access to it. The timeline for data restoration depends on the size of the data and the complexity involved.

To ensure the safety of the backed-up data, we use a redundant array of independent disks (RAID) in the backup servers. All backups are scheduled and tracked regularly. In case of a failure, a re-run is initiated and is fixed immediately. The integrity and validation checks of the full backups are done automatically by the ZAC tool.

From your end, we strongly recommend scheduling regular backups of your data by exporting them from the respective Zoho services and storing it locally in your infrastructure.

Business continuity statement/plan

Application data is stored on resilient storage that is replicated across data centrs. Data in the primary DC is replicated in the secondary in near real time. In case of failure of the primary DC, the secondary DC takes over and the operations are carried on smoothly with minimal or no loss of time. Both the centres are equipped with multiple ISPs.

We have power back-up, temperature control systems, and fire-prevention systems as physical measures to ensure business continuity. These measures help us achieve resilience.

In addition to the redundancy of data, we have a business continuity plan for our major operations, such as support and infrastructure management.

Privacy by Design

Every change and new feature is governed by a change management policy to ensure all application changes are authorised before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our code analyser tools, vulnerability scanners, and manual review processes.

Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection, cross site scripting and application layer DOS attacks.

Our privacy commitment: Zoho has never sold your information to someone else for advertising, or made money by showing you other people's ads, and we never will. This has been our approach for almost 25 years, and we remain committed to it. This policy tells you what information we collect from you, what we do with it, who can access it, and what you can do about it.

More information on our privacy policy can be found at https://www.manageengine.com/privacy.html

Using the service

Ordering and Invoicing

Paid subscription can be availed from ManageEngine by contacting our team to discuss your requirements in detail. They will guide you through the ordering process and provide any necessary assistance in completing the Order Form (Call-off contract). We accept payment via Visa, MasterCard, American Express, and PayPal. We also accept payment via bank transfer or check transfer for yearly subscriptions. We strive to make the ordering and invoicing process as smooth as possible, ensuring that you have a clear understanding of the fees and payment terms.

Pricing Overview

Pricing is based on endpoint/server count and number of technicians. Refer Pricing document for more details.

Availability of Trial Service

We offer an all-inclusive, free, 30-day trial for all users. Once the trial period has lapsed,the product with all of its features will be free for 25 endpoints only. Please refer to our Free Trial page: https://www.manageengine.com/malware-protection/free-trial.html

On-Boarding, Off-Boarding, Service Migration, Scope, etc.

On-boarding and off-boarding processes are crucial aspects of Malware Protection Plus. On availing our premium support service, we assign a dedicated point of contact who will provide assistance throughout the on-boarding phase. They will be available to answer any questions, provide guidance, and ensure a seamless on-boarding experience as per the customer's requirements. During the on-boarding process, we provide comprehensive documentation that guides users through the setup and configuration. When users decide to stop using our service, we have an off-boarding process in place to ensure a smooth transition out of Malware Protection Plus. We understand that circumstances may change, and we aim to make the off-boarding process as hassle-free as possible. Our dedicated point of contact will work closely with the user to understand their reasons for discontinuing the service and provide any necessary assistance.

Training

We offer training sessions to familiarise users with the features and functionalities of our service. These training sessions can be conducted remotely or on-site, depending on the user's preference and requirements.

Onsite Training: Whether it's training for a few employees, a team, or your entire organisation, we offer convenient and exhaustive training on Malware Protection Plus at a location of your choice.

Online Training: If you prefer to learn at your own pace, we provide a paid online option offering comprehensive training from experts — all from the convenience of your office or home. All you need is an internet connection, and the training will be delivered over the web. Please refer to our Pricing sheet and SFIA rate card for more information.

Implementation Plan

Options for Implementation

Malware Protection Plus implementation takes several steps to ensure smooth deployment and integration with the existing infrastructure.

• Requirement discussion.
• Allocation of resources and timeline.
• Assessment of the organisations existing IT infrastructure, like endpoint count,architecture.
• Formulating an implementation plan with timelines and prerequisites.
• Initial configuration and integrations.
• Conducting tests based on various use cases.
• Extending the implementation to other groups in the production environment.
• Post-implementation monitoring and health checks.

Service Management

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. Likewise, we track and close the incidents with appropriate corrective actions. Whenever applicable, we will identify, collect, acquire and provide you with necessary evidence in the form of application and audit logs regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations.

We respond to the security or privacy incidents you report to us through incidents@zohocorp.com, with high priority. For general incidents, we will notify users through our blogs, forums, and social media. For incidents specific to an individual user or an organisation, we will notify the concerned party through email (using their primary email address of the Organisation administrator registered with us).

Malware Protection Plus offers robust service levels to ensure optimal performance, availability,and support for our customers. Our goal is to provide a reliable and responsive service that meets the specific needs of our customers while ensuring compliance with industry standards and best practices.

Workflow adopted in handling customer requests:

• Questions received from customers through live chat and web-forms will be created as tickets in Zoho Desk.
• The tickets will be assigned manually by agents or admin users.
• Customers will be provided with a valid first response via email/phone call within the defined SLA.
• The ticket is processed further based on the customer's response.
• Based on the ticket category, the ticket is assisted at various levels. Upon providing a resolution and receiving the customers confirmation for the same, the ticket will be closed.

Service Constraints

Our team will work with you to understand your needs and provide the necessary information to ensure a successful implementation of the solution while addressing any potential constraints that may arise. We guarantee high availability of our service with minimal downtime. Our product is designed for scalability to accommodate the growing needs of all organisations. Our support team comprises well-trained professionals who operate 24/5 to deliver top-quality service. In the event of feature deprecation, we will announce in advance an improvised hotfix or new feature upgrade. Communication will be done through the publication of release notes, help documents, technical guides, and more. Malware Protection Plus provides administrators with the flexibility to personalise the settings of their console according to their preference. It allows users to customise their display settings, port details, and also enable support access for the support team to debug their issues.

Service Levels

At Malware Protection Plus, we believe every customer is important and is the reason for our existence. We also realise that our success lies in keeping our customers happy. We adhere to industry standards and best practices to ensure the highest level of service management. Further, we handle service constraints and incidents through a dedicated service desk, where customers can seek support and make requests. Our support team is managed by experienced professionals who ensure smooth operations and timely progress.

Classic Support: This customer support program is included within the subscription,wherein customers can contact our product specialists through chat and email. ManageEngine's dedicated team of product specialists are available 9 am to 5 pm (UK time), from Monday to Friday, for responding to customer enquiries within eight hours. ManageEngine classifies support inquiries into three severity levels, depending on the nature of the reported issue.

The response and resolution times for these severity levels are as follows:

Severity Level 1: Response time: 6 hours
Severity Level 2: Response time: 15 hours
Severity Level 3: Response time: 24 hours

Premium Support: ManageEngine also offers a paid program called PremiumSupport with 24x5 support for high-impact, urgent issues during non-business hours.Our customer support executives will respond within 3 hours, and the resolution timelines for every ticket depend on the priority and nature of the customer's enquiry. Dedicated account managers and escalation teams will keep track of issues to expedite resolution while providing timely updates to customers. Customer will get access to a customer portal to track their incidents and interact with ManageEngine. The PremiumSupport program is priced at 20% of the subscription cost.We request you to refer to our Terms and Conditions document and our support page for additional information.

Provision of the service

Customer Responsibilities

- Choose a unique, strong password and safeguard your login information.
- Use multi-factor authentication.
- Use the latest browser versions, mobile OS updates, and updated mobile applications to ensure they are patched against vulnerabilities and benefit from the latest security features.
- Exercise appropriate caution when sharing data from our cloud environment.
- Classify your information as personal or sensitive and label it accordingly.

- Monitor devices linked to your account, active web sessions, and third-party access to detect any unusual activity. Manage roles and privileges carefully to maintain control over your account.
- Stay alert to phishing and malware threats by watching for unfamiliar emails, websites, and links that may attempt to exploit your sensitive information by impersonating Zoho or other trusted services.

Additionally, you may be required to actively participate in the implementation process by providing relevant information and collaborating with our team. Understanding and fulfilling these responsibilities is essential for a smooth and successful onboarding experience with Malware Protection Plus. Our team will guide you throughout the process and provide all necessary support to help you meet these obligations.

Customers are also responsible for: (i) providing accurate, current, and complete information related to their access and use of the on-demand services; (ii) ensuring authorised users comply with the agreement, documentation, and invoice; (iii) maintaining the accuracy, quality, and legality of customer data; (iv) ensuring the customer data is lawfully acquired and used; (v) taking commercially reasonable steps to prevent unauthorised access to or use of the on-demand services; (vi) using the on-demand services in accordance with the agreement, documentation, and invoice; (vii) overseeing all activities that occur under the customer's account; (viii) complying with all applicable laws and regulations; and (ix) adhering to the terms governing the use of non-on-demand services.

Technical Requirements and Client-Side Requirements

Malware Protection Plus has no specific technical requirements or client-side requirements that users should be aware of. However, in the event of bandwidth constraints, we recommend using distribution servers for bandwidth optimisation.

Malware Protection Plus is compatible with major browsers such as Google Chrome, MicrosoftEdge, and Mozilla Firefox browsers. It can be accessed from desktops and laptops.

After-sales Account Management

- We offer customer support via email and chat to address queries, troubleshoot issues, and provide guidance.
- We keep customers informed about the latest product updates, enhancements, changes/planned downtime, and new features.
- We manage license renewals and communicate with customers regarding upcoming renewals.
- We provide information about licensing options, upgrades, and any relevant promotions or discounts.
- We gather customer feedback to understand their satisfaction with ManageEngine products, using surveys and feedback mechanisms to identify areas for improvement and address customer concerns.
- We provide customers with information about complementary products that could enhance their IT management capabilities.
- We maintain regular communication with customers through newsletters, announcements and product updates, ensuring that customers are informed about relevant events, workshops, webinars, and training sessions.
- We conduct periodic account reviews to assess customers' usage of ManageEngine products, discussing any challenges or opportunities for improvement and providing recommendations accordingly via health checks.
- We also implement customer success programs to proactively engage with customers, ensuring they achieve their goals with ManageEngine solutions and providing best practices, use cases, and success stories to inspire effective utilisation of the products.

Termination Process

You have the right to terminate your user account for convenience or if Zoho Corporation Limited breaches its obligations under our Terms and in such event, you will be refunded the subscription fee for the unused portion of the subscription period. Termination of user account will include denial of access to all Services, deletion of information in your user account such as your e-mail address and password and deletion of all data in your user account in accordance with our deletion cycle.

Social Value

Fighting Climate Change

ManageEngine and its parent company Zoho Corp have committed to working towards achieving Net-zero by 2050. Some initiatives for this:

- Green data centres: We've partnered with Equinix to host our UK data centres in London and Manchester. Equinix is also committed to sustainability and is compliant with the Climate Neutral Data Centre Pact, ISO 14001, LEED, etc.
- Energy initiatives at Zoho UK's workspace at Bletchley - The energy supply for the UK office is derived from renewable sources, accounting for 21% of total power consumption. LED retrofits have been implemented to enhance energy efficiency throughout the building.
- Renewable energy: We've built a 5 megawatt on-grid solar energy farm at Abinimangalam near Trichy, India. This farm offsets the electricity consumption of our Chennai headquarters and data centre. Designed with a focus on energy efficiency, data centres that support Zoho UK are powered by renewable energy.
- Further, these data centres are progressing towards integrating with a solar grid to reduce environmental impacts.
- Green Energy Procurement - All purchased energy for the data centres is sourced from green energy providers. This enables us to minimise the carbon footprint associated with our operations.
- Emissions - The United Kingdom has committed to achieving carbon neutrality by
- 2050. Supporting this pledge, we have taken steps to monitor greenhouse gas (GHG) emissions from our operations and implement measures to mitigate them. We account for Scope 2 and Scope 3 emissions and exclude Scope 1 emissions as our work does not involve fuel combustion within operational boundaries.

Globally, emissions need to be cut down by 45% by 2030, in order to achieve net-zero by 2050. 60% of fossil fuels (coal, oil, and gas reserves) need to be replaced by efficient energy sources to achieve net-zero.

- E-mobility: We've switched completely to electric vehicles for movement within the campus.

- Energy efficient operations: We use loT to measure and optimise energy consumption across our offices. We've also implemented LED lighting, energy-efficient equipment, and loT based energy management to reduce our energy consumption and greenhouse gas emissions.

- Recycling and waste reduction: All the waste generated on campus is segregated at source. Food waste is processed in our own biogas plant, which generates the electricity used to run the plant. All other waste is sent to the recycling vendors for recycling it.

- Minimising water usage: We use an in-house sewage treatment plant to treat wastewater for reuse for flushing, gardening and cooling tanks. We've also implemented loT sensors to detect water leakage, rain-detecting sprinklers systems, and smart water management, to monitor and reduce our water usage and wastage.

- Sustainable procurement: We encourage sourcing materials from suppliers who have environment friendly practices. We also recycle obsolete gadgets by sending them to an e-waste recycling unit.

- Reduced paper use: We've reduced paper use at work. Most our documents are now digitally maintained, reducing our print-related environment impact.

- Reducing business travel: We've reduced our business travel. Many Events and meetings are conducted online using our in-house meeting tools.

COVID-19 Recovery

- During the COVID-19 pandemic, ManageEngine and its parent company Zoho Corp. worked to minimise the impact of COVID on our customers, other business, and our local community.

- Supporting remote work: At the start of the pandemic, ManageEngine and its parent company Zoho Corp. created and distributed a Secure Remote Access Toolkit to help organisations quickly adapt to and work securely during the pandemic. This toolkit was made free for the first 100 days.

- Discounts and waivers: To assist organisations impacted by the pandemic, ManageEngine and its parent company Zoho Corp offered free licenses of flagship products and offered discounts and waivers on licenses on a case-by-case basis.

- Food to the underprivileged: While most of our employees worked from home, we kept the kitchen at our Chennai headquarters running with a skeletal staff to provide food to underprivileged people in the local area, many of whom were im pacted due to a loss of employment during the lockdown.

- Infrastructure support: We converted one of our office buildings into a temporary COVID-19 ward to accommodate citizens who were required to quarantine.

- We ran Covid vaccination camps for our employees. their dependents and the support staff who worked in Zoho.

- ManageEngine Site24x7 introduced the Small Business Emergency SubscriptionAssistance Program (ESAP) during Covid-19. ESAP gives our small business customers a chance to use Site24x7 and other Zoho products free for three months.

Tackling Economic Inequality

ManageEngine and its parent company Zoho Corp. has always aimed to tackle economic inequality and give back to the community. This is reflected in the following:

- Transnational localism: Coined by our CEO, transnational localism is the philosophy that underpins our staffing and office location plans. Instead of focusing on crowded urban centres, we've been opening spoke offices in smaller towns and villages. The goal is to improve local infrastructure, boost the economy of these smaller towns and villages, and provide more employment opportunity.

- Local hiring: As part of our philosophy of transnational localism, we believe in hiring locally for each spoke office. This helps promote local talent and bring high-paying jobs back to the villages and towns where we are based.

- Zoho Schools of Learning: Started in 2004, Zoho Schools of Learning (formerly Zoho University) provides training and employment for high school students and those holding or pursuing diplomas. Those inducted into Zoho Schools are trained by industry experts in the fields of their choice - technology, business, or design. The students are also trained in social skills. The course is completely free, and students are paid a monthly stipend throughout its duration. Graduates from this program are automatically inducted into Zoho Corp.

Equal Opportunity

- As part of our efforts to tackle inequality, ManageEngine and its parent company Zoho Corp. have made efforts to provide equal opportunities and tackle workforce inequality.

- Helping women restart their careers: Zoho Schools of Learning has begun a program called Marupadi. Aimed at helping women restart their tech careers after a break, Marupadi is a 3-month program comprising a mix of lectures, experiential learning and internships. At the end of the program, the candidates who've successfully completed training get to sit for exclusive face-to-face interviews for jobs at Zoho Corp.

- Diversity and inclusion in hiring: All roles at ManageEngine and its parent companyZoho Corp. are open to all people irrespective of gender, sex, race, ability, or religion.We hire solely based on skill and have a diverse team.

- We eschew discrimination on any grounds, including age, colour, disability, ethnicity, family or marital status, gender identity or expression, language, national origin, physical and mental ability, political affiliation, race, religion, sexual orientation, socio-economic status, and other unique characteristics that define our associates.Instead, we espouse, fairness, striving to ensure that a merit-based approach allows wage parity among associates with comparable experiences and responsibilities, irrespective of their gender.

- Accessible campus: Our campus has been designed to be accessible to all, including differently abled colleagues. The layout design includes ramps and lifts in every building, allowing ease of mobility and access to all.

- On-campus crèche and day care: We support new parents within the organization by providing them with on-campus crèche, day-care and play school.

- Apart from the usual shuttle facilities, special cab service covering a certain distance is given for women during their third trimester.

Wellbeing

ManageEngine and its parent company Zoho Corp. in UK adheres to industry standards in remuneration, ensuring that compensation is equitable across genders. Recognising the diverse needs of our people, we provide essential support such as parental leave, aligning with our efforts to build an organisation that values and cares for every individual.

- Free on-campus medical services: We have trained medical practitioners and a dedicated medical clinic available on all days of the week. Employees can freely avail their services for any medical requirements. The cost of consultation is borne completely by the company. This is for all employees based out of India.

- Hazard Management Framework: The Hazard Identification & Risk Assessment (HIRA) Framework is followed rigorously at the premises. Under this, regular assessments are conducted to identify workplace hazards and evaluate social risks.

- n-house mental health counselling: We provide in-house counselling to our employees for free via our team of trained and qualified therapists.

- Free medical camps: We organise free medical check-ups for our employees on an annual basis.

- Blood donation camps: We organise regular blood donation camps in association with various blood banks.
- We have open house sessions conducted by the CEO periodically where employees can raise any concerns. Team level open house sessions (from operations teams) are done every week.
- Day Care facilities provided for employees' children.
- Continuous Improvement: The compliance monitoring framework involves ongoing reviews and enhancements of occupational health programs, guided by feedback, data analysis, and emerging best practices. We foster a culture of continuous improvement, encouraging employee engagement, and incorporating insights from incidents or near misses.

Employee Engagement

With respect to employee engagement, we prioritise transparent communication and foster a supportive work environment. Our talent acquisition process emphasises diversity and inclusion with the aim of building a talent pool that offers the richness of diverse skills, experiences, and cultural perspectives.

The onboarding for new employees begins with the Security and Privacy Awareness (SPA) quiz. This short assessment ensures that our employees possess a basic understanding of our compliance regulations and ethical practices. Subsequently, they undergo a comprehensive departmental training spread over 3-4 weeks. This immersive program is designed to equip new joiners with the necessary understanding and skills to excel in their role. In addition, they can access learning resources through our Zoho Learn platform. This online portal houses a range of materials, including product tutorials, system guides, and best practices, enabling them to enhance knowledge and expertise.

Employee retention is an area of focus which we address by implementing programs tailored for professional development, mentorship, and work-life balance. In turn, these contribute to a dynamic, inclusive, and fulfilling work culture. Further, we make sure to communicate career growth opportunities, enabling employees to feel valued and motivated. By emphasising continuous progress and adapting to evolving employee needs, we work to build an organisation remains a place where talent flourishes over the long term.

Governance

ManageEngine and its parent company Zoho Corp.'s operations in the UK are underpinned by ethical governance, which require every employee to demonstrate integrity in business conduct, while also ensuring the company's compliance with legal and regulatory requirements. Business integrity is not only the foundation on which Zoho UK's reputation is being built, it also enhances our capacity to forge enduring stakeholder relationships that enable us to create shared value in the long term.The following section outlines our policy framework comprising the Code of Ethics, Modern-Slavery and Anti-Bribery Policies.

Policy Framework Code of Ethics

The Code of Ethics is a set of guidelines for ethical behaviour characterised by integrity, respect, and responsibility. It is applicable to all workforce of ManageEngine and its parent company Zoho Corp. in the UK, including employees, consultants, and interns. The Code of Ethics emphasises the following for workplace and business conduct:

- Fairness: We foster a diverse and inclusive work environment, promoting equal opportunities for all, thereby embracing the values of Equality Act 2010.
- Respect: Harassment is eschewed, and a clear reporting mechanism has been put in place to register concerns.
- Ethical Sourcing: Zoho UK stands against forced labor, slavery, and human trafficking, and promotes ethical procurement practices.
- Privacy: Responsible handling of personal information, acknowledging resource limitations.

Our experience

In the latest AV-Comparatives Business Main-Test Series 2025, Malware Protection Plus earned the Approved Business Product certification by delivering balanced, real-world performance.

1. Real-World Protection Test: Achieved a protection rate of 97.4%, comfortably above the 90% threshold needed for certification, helping block live threats in practical, everyday scenarios.

2. Performance Test: Kept system impact low with a score of 3.0, so everyday work stays smooth and devices remain responsive.
3. False Positives: Registered zero false positives on business software, ensuring essential applications keep running without unnecessary interruptions.

Figure 4: Proven by AV-Comparatives

As a trusted standard for businesses, AV-Comparatives validates malware protection solutions that truly perform through rigorous real-world testing, thereby helping businesses identify the right solution and facilitate informed decision-making that aligns with their cybersecurity needs.

Contact Details

Company Name:ManageEngine, a division of Zoho Corporation

Primary Contact:gcloud@manageengine.com

Address:Suite 1.09, Challenge House, Sherwood Dr, Bletchley,Milton Keynes MK3 6DPUK

Toll Free:0800 028 6590

ManageEngine

www.manageengine.com