



ManageEngine Endpoint Central

Embrace unified endpoint management and security the SaaS way!



Table of Contents

Introduction	3
Company Overview	3
Product Introduction	5
Benefits	8
Associated Services	12
Product Features	13
Data Protection	17
Information Assurance	17
Data Backup, Data Restoration and Disaster Recovery	18
Business continuity statement/plan	19
Using the service	20
Ordering and Invoicing	20
Pricing Overview	20
Availability of Trial Service	20
On-Boarding, Off-Boarding, Service Migration, Scope, etc.	20
Training	21
Implementation Plan	21
Service Management	22
Service Constraints	23
Service Levels	23
Provision of the service	24
Customer Responsibilities	24
Technical Requirements and Client-Side Requirements	25
After-sales Account Management	26
Termination Process	26
Social Value	27
Our experience	33
Testimonials	33



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 organisations 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

Endpoint Central, is a powerful UEM solution that manages devices like servers, desktops, laptops, and mobile devices from a single dashboard and supports OSs like Windows, macOS, Linux, iOS, Android, Windows, tvOS, Chrome OS, and iPadOS. You can perform End-to-End Patch Management, Remote Control, Asset Management, OS Deployment, Mobile Device Management, Configuration Management, and Security Operations, including Vulnerability Management, Browser Management, Application Control, Device Control, Anti-Ransomware, Next-Gen Antivirus, and BitLocker Management.

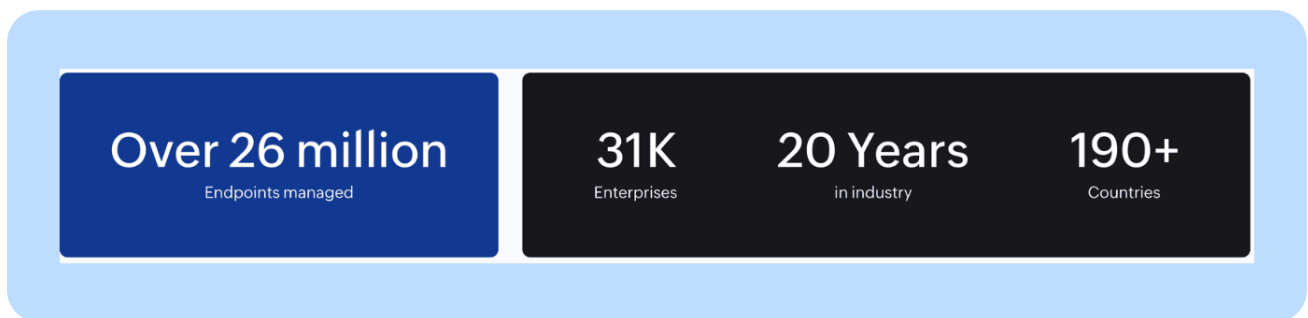


Figure 1: Endpoint Central's global footprint

Endpoint Central from ManageEngine solves the problem of effectively managing and securing endpoints within the public sector. In the current digital landscape, public sector organisations often have a geographically distributed workforce with varying skillsets and knowledge levels. There also exists a challenge to provide the right information, access, devices, and data without compromising security. Endpoint Central unified console streamlines, simplifies and secures your physical infrastructure from desktops and mobile devices to servers and tablets across a diverse range of OSs and platforms. Endpoint Central brings visibility to your device fleet and automates routine IT tasks while securing your network against cyberattacks, which may otherwise cost any public sector organisation both in terms of cost and reputation.

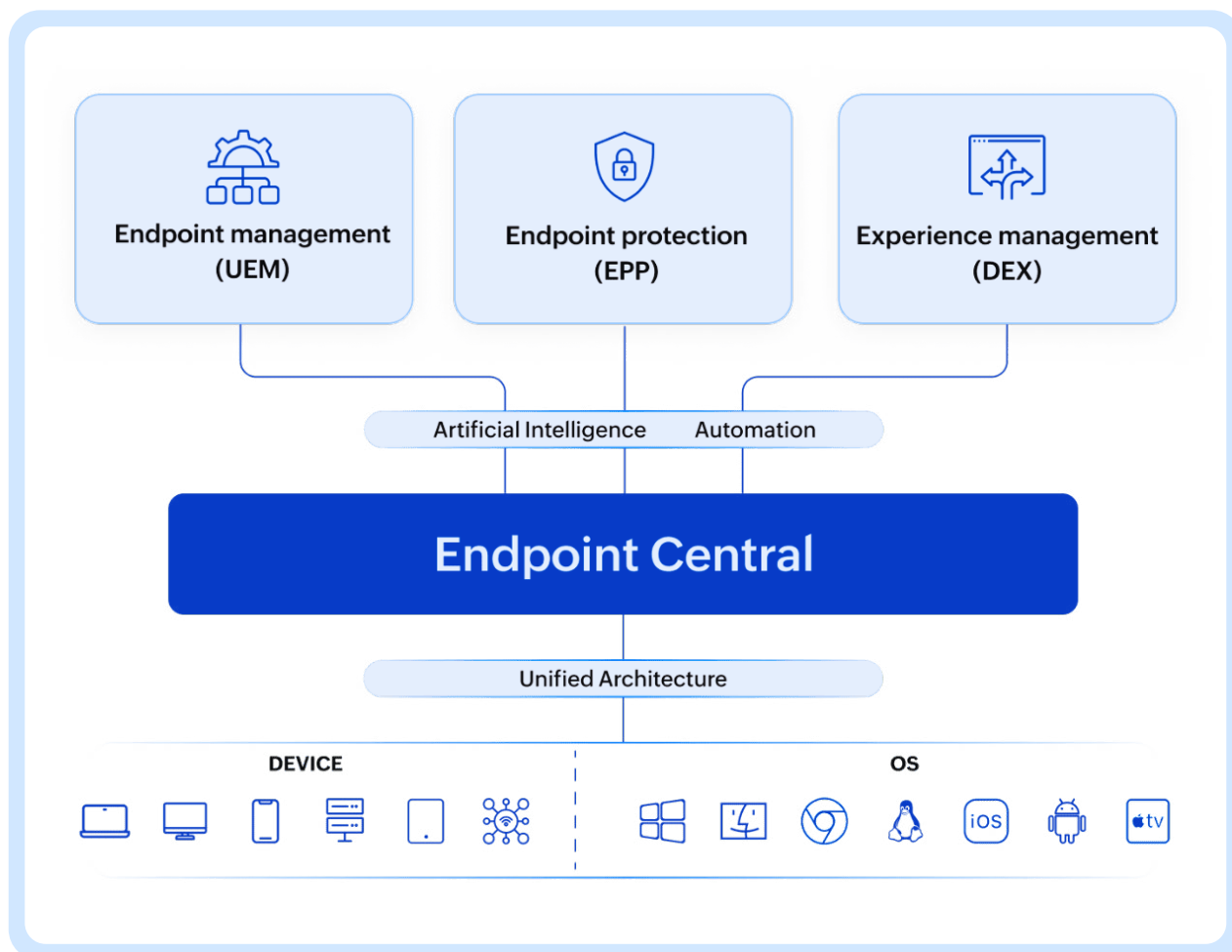


Figure 2: Endpoint Central's core offerings

Who might benefit

Executive & Leadership Stakeholders

- CIO – Chief Information Officer: Responsible for overall IT strategy, technology investments, and ensuring secure, efficient operations.
- CISO – Chief Information Security Officer: Prioritises threat mitigation, incident response, and maintaining a strong cyber-resilience posture.
- CTO – Chief Technology Officer: Focuses on ensuring technology infrastructure is scalable, modern, and aligned with business goals.
- VP / Director of IT: Oversees IT operations and security teams, ensures tools support business continuity and agility.
- Head of Infrastructure & Operations: Seeks stable, automated endpoint operations and minimal downtime across device fleets.

IT Operations & Endpoint Management Teams

- IT Manager / IT Operations Manager: Drives endpoint standardisation, device lifecycle management, and workflow automation.
- Endpoint Management Lead / UEM Lead: Deeply involved in device enrolment, OS updates, compliance, imaging, and policy enforcement.
- System Administrators: Handle patching, software deployment, OS updates, hardware/software inventory, and remote troubleshooting.
- Desktop Engineers / EUC Engineers: Manage end-user devices, application provisioning, and device configuration at scale.
- Workplace / Digital Experience (DEX) Teams: Focus on improving user productivity, device performance, and employee digital experiences.

Security Operations & Cybersecurity Teams

- SOC Manager / SOC Analysts (L1–L3): Need real-time threat detection, event correlation, rapid isolation, and automated remediation.
- Cybersecurity Engineers: Oversee threat prevention, hardening, attack surface reduction, and endpoint defence policies.
- Vulnerability Management Teams: Rely on automated patching, risk-based prioritization, and compliance reporting.
- Incident Response (IR) Teams: Need quick endpoint isolation, forensic data, rollback options, and attack chain visibility.

Compliance, Governance & Risk Teams

- IT Compliance Officers / GRC Teams: Require consistent policy enforcement, audit logs, asset visibility, and configuration compliance.
- Internal Audit Teams: Need proof of patch status, device compliance, and policy adherence.
- Data Protection Officers (DPOs): Concerned with safeguarding personal data and ensuring the organisation complies with privacy rules.

Support & Helpdesk Teams

- Helpdesk Managers & Technicians (L1–L3): Benefit from remote control, device diagnostics, automated scripts, and rapid issue resolution.
- Service Desk Teams: Use endpoint insights to resolve incidents faster and reduce ticket volume.

Benefits



Figure 3: Endpoint Central ROI as per Forrester

According to a Forrester TEI study, ManageEngine Endpoint Central delivers a 442% ROI and \$4.5 million in total benefits over three years. Centralised visibility and policy enforcement contribute to improved security posture and compliance, reducing audit risks and unplanned downtime. With a payback period of less than six months, Endpoint Central consolidates endpoint management operations while providing measurable business value.

1. Gain complete operational visibility for faster, smarter IT decision-making

IT directors often struggle with “Shadow IT” the anxiety caused by unknown devices or unauthorised software lurking on the network, which creates blind spots in budgeting and security.

By illuminating the entire infrastructure, this solution transforms a chaotic mix of unknown assets into a clear, live inventory. This granular visibility empowers leadership to stop guessing and start making data-backed decisions, effectively eliminating wasteful spending on unused licenses and ensuring every IT dollar is accounted for.

2. Strengthen organisational security and reduce breach exposure across all endpoints

With the traditional network perimeter gone, endpoints are the new frontline, and security teams are frequently overwhelmed by the volume of vulnerabilities and sophisticated attacks.

Shifting from a reactive to a proactive posture, the platform enforces strict browser security, BitLocker encryption, and device controls from a central hub. This drastically shrinks the organisation's attack surface, ensuring audit readiness and minimising the business disruptions caused by malware or data leaks.

3. Manage any OS or device seamlessly with broad platform flexibility

The modern workplace is a mix of Windows, macOS, Linux, and mobile devices, often forcing administrators to “console hop” between disparate tools to manage them all.

This solution brings order to the chaos by allowing IT administrators to manage every device—regardless of the operating system—from a single pane of glass. This flexibility future-proofs the organisation, enabling it to support a diverse, multi-OS talent pool without increasing administrative complexity or headcount.

4. Unify IT management and security from the cloud with one lightweight agent

“Agent bloat” creates significant friction; when devices run separate background agents for antivirus, patching, and inventory, performance degrades and employee productivity suffers.

Converging security and management into a single, lightweight agent eliminates the performance drag on end-user devices. This consolidation breaks down the silos between IT Operations and Security teams, allowing them to operate from a unified cloud platform that reduces infrastructure costs and ensures consistent policy enforcement for both on-premise and remote workers.

5. Accelerate time-to-value (TTV) and maximize ROI through streamlined operations

Enterprise software implementations often drag on for months, leaving investments idle and vulnerabilities exposed while the organisation waits for deployment.

Designed for rapid deployment, the system allows organisations to configure policies and see results in days rather than months. This speed ensures immediate operational improvements, enabling the business to realize a quick return on investment while freeing up IT staff to pivot toward high-value digital transformation initiatives.

6. Access real-time IT intelligence with fully customizable reporting

When executives ask critical questions about compliance or asset health, IT teams often lose days manually compiling data from disparate sources, delaying strategic decisions.

IT leaders gain access to a dashboard that translates technical metrics into business insights through drag-and-drop reporting. This transparency elevates IT from a maintenance function to a strategic partner, building trust with stakeholders by providing immediate, verifiable proof of the organisation's technological health.

7. Improve productivity with an intuitive, easy-to-navigate management interface

Complex, archaic interfaces are a primary source of burnout for IT staff, leading to slower response times and an increased likelihood of configuration errors.

An interface built with the human user in mind lowers the barrier to entry for new technicians and reduces friction for veterans. This intuitive design minimises errors and accelerates task execution, ultimately leading to faster resolution times for end-user issues and a more agile IT department.

8. Eliminate manual effort with automated patching for third-party apps

Manually testing and deploying updates for hundreds of third-party applications is a tedious, repetitive cycle that often leads to “patch fatigue” and overlooked vulnerabilities.

Automating the entire patching lifecycle from detection to deployment liberates IT teams from the drudgery of routine maintenance. This not only reclaims valuable man-hours but also closes the critical vulnerability gap between a patch’s release and its installation, significantly hardening the organisation’s security posture.

9. Adapt quickly with a solution configurable to your business requirements

“Agent bloat” creates significant friction; when devices run separate background agents for antivirus, patching, and inventory, performance degrades and employee productivity suffers.

Converging security and management into a single, lightweight agent eliminates the performance drag on end-user devices. This consolidation breaks down the silos between IT Operations and Security teams, allowing them to operate from a unified cloud platform that reduces infrastructure costs and ensures consistent policy enforcement for both on-premise and remote workers.

10. Empower employees with an enterprise self-service portal and app store

Skilled employees often face frustration when they have to wait days for a help desk ticket to be resolved just to install simple, approved software.

Giving employees the power to install approved software through a curated self-service portal transforms the user experience from dependence to autonomy. This self-sufficiency deflects a significant volume of routine help desk tickets, allowing IT support to dedicate their expertise to resolving complex, mission-critical challenges.

Associated Services

Endpoint Central from ManageEngine offers a range of associated services that can be bought alongside the main service. These include:

1. **APIs:** Endpoint Central 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 Endpoint Central. 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 Endpoint Central. This includes regular updates, bug fixes, and technical assistance to address any issues or concerns.
4. **Video Tutorials:** Endpoint Central also maintains a repository of video tutorials and conducts live webinars with our product experts throughout the year for every module and function at <https://www.manageengine.com/products/desktop-central/training.html>
5. **Workshops and User Conferences:** Endpoint Central 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.
6. **Product customisations and feature requests:** Endpoint Central is open to facilitate any customer use-case/feature after careful internal vetting.
7. **Online Documentation:** Endpoint Central provides in-depth help documentation that is hosted online at <https://www.manageengine.com/products/desktop-central/help/>, which provides step by step guidance for administrators, technicians, and end-users. These associated services enhance the functionality and value of Endpoint Central, providing a comprehensive solution for endpoint management and security.

Product Features

1. Automated patch management and vulnerability remediation with compliance scoring

This feature automates the entire lifecycle of patch management, extending beyond just the operating system to include over 1000 third-party applications (like Adobe, Chrome, and Java). It automatically scans endpoints to detect missing patches, tests them for stability, and deploys them. Integrated compliance scoring provides a live “health score” for the network, highlighting high-risk areas immediately.

Use Case: Consider a scenario where a critical “Zero-Day” vulnerability is discovered in a widely used web browser on a Friday afternoon. Instead of the IT team working through the weekend to manually update every machine, the system identifies the vulnerability immediately. It automatically deploys the patch to a test group; once stability is confirmed, it pushes the update to the entire global fleet.

2. Advanced ITAM and unified MDM for enterprise device governance

The Capability: This combines IT Asset Management (ITAM) with Mobile Device Management (MDM) to create a single source of truth for all hardware and software assets. It tracks asset lifecycles, manages software licenses to prevent audits, and secures mobile devices (iOS, Android, etc.) alongside traditional workstations.

Use Case: An organisation has a mix of corporate-issued laptops and employee-owned smartphones (BYOD). When a sales executive leaves/loses a corporate iPad, IT administrators can instantly locate and remotely wipe corporate data from the device without touching the user’s personal photos. Simultaneously, the ITAM system flags the executive’s laptop for return and re-provisioning, ensuring no hardware goes missing during off boarding.

3. Scalable software deployment with enterprise self-service application portal

This feature streamlines software distribution, allowing administrators to create repositories of approved software packages that can be silently installed on thousands of machines simultaneously. It includes a Self-Service Portal where employees can access pre-approved applications without needing admin rights or IT assistance.

Use Case: A Design department expands and hires 20 new designers who all need complex design software immediately. Instead of IT logging into each machine individually, the administrator pushes the software package to the “Design Team” custom group. For optional tools, the designers simply open the Self-Service Portal on their desktop, click “Install” on the required apps, and are productive within minutes without needing to raise any help desk tickets.

4. Endpoint analytics for digital experience and performance optimization

This tool moves beyond simple device lifecycle management to optimise the digital employee experience. It tracks metrics like boot times, application crash rates, and system resource usage to identify why a device feels “slow” to the user, often diagnosing issues before the user complains.

Use Case: Users in the finance department begin complaining that their computers are sluggish during month-end closing. Rather than guessing it’s a network issue, the IT team is able to pinpoint that a recent driver update is causing high memory usage specifically on the finance team’s laptop model. They roll back the driver proactively, restoring performance before the majority of the department is even aware of the problem.

5. DLP enforcement with application allow listing and block listing controls

Data Loss Prevention (DLP) features prevent sensitive data from leaving the organisation via unauthorised channels like USB drives or cloud uploads. This is reinforced by application control, which allows trusted apps to run (allow listing) and bans known malicious or unproductive software (block listing).

Use Case: An employee attempts to copy a folder of sensitive client contracts onto a personal USB drive to work from home. The DLP agent instantly blocks the transfer and displays a policy violation notification. Meanwhile, the application control policy prevents another user from installing an unauthorised peer-to-peer file-sharing application, neutralizing a potential avenue for data exfiltration.

6. Behaviour-driven NGAV and ransomware defence with malware protection

Unlike traditional antivirus that relies on known signatures, Next-Gen Antivirus (NGAV) uses AI and behavioural analysis to detect anomalies. It identifies suspicious activities, such as a process attempting to rapidly encrypt files and kills the process instantly to stop ransomware and malware attacks.

Use Case: A remote employee accidentally opens a sophisticated phishing attachment that contains a new strain of ransomware not yet listed in global virus databases. As the malware attempts to encrypt the user's "Documents" folder, the NGAV detects this abnormal behaviour. It immediately terminates the process, isolates the infected machine from the network to prevent spread, and notifies the security team, stopping the attack in an instant.

7. Unified Endpoint Protection Platform with proactive and pre-emptive threat protection

This feature implements a robust "Defence in Depth" strategy by layering multiple security controls. It moves beyond simple detection to proactive Endpoint Hardening and Security Baselineing. The platform continuously scans endpoints against rigorous industry standards (such as CIS Benchmarks or STIG), identifying dangerous misconfigurations like weak password policies, unnecessary open ports, or default administrative shares. It then acts to remediate these gaps, effectively locking down the OS and reducing the attack surface before a threat even arrives.

Use Case: An organisation defines a strict security baseline to prevent the lateral movement of malware. During a routine automated scan, the platform detects that a specific department's sub-network has "drifted" from this baseline, specifically, several

workstations have re-enabled a vulnerable legacy protocol (like SMBv1) that is frequently exploited by ransomware. The system immediately flags this high-risk deviation and auto-remediates the configuration to meet the standard. By hardening these endpoints instantly, the organisation neutralizes a critical entry point, ensuring the “doors” are locked tight before an adversary even tries the handle.

8. OS imaging, deployment, and provisioning for Windows endpoint fleets

This feature simplifies the process of setting up new computers. Administrators can capture a “Golden Image” of a perfectly configured OS (with all standard apps and settings) and deploy it to bare-metal machines, supporting unicast and multicast to image one or hundreds of devices at once.

Use Case: A company opens a new branch office and receives a shipment of 100 blank desktops. Instead of spending weeks manually setting them up, the IT team uses OS imaging to deploy a standardized Windows image to all 100 machines simultaneously over the network. By the time the new employees arrive on Monday morning, every computer is booted up, domain-joined, and ready to use.

9. Web security with integrated browser-based threat and exploit prevention

Since the browser is the most commonly used application, this feature secures it specifically. It manages browser extensions, filters malicious URLs, and restricts downloads from untrusted sources, effectively placing a shield between the user and the web.

Use Case: A sales representative attempts to boost productivity by installing an unapproved “Grammar Helper” extension found on a public store. Unbeknownst to them, this extension requests permission to “read and change all data on websites you visit”, a tactic often used to scrape sensitive CRM customer details or capture login credentials in the background. The web security module intervenes immediately, enforcing a strict “browser extension allowlist.” The installation is blocked before it can begin, keeping the browser environment sterile and preventing a silent data breach where sensitive corporate data could have been siphoned off unnoticed.

10. Endpoint privilege management with zero-trust access control policies

This implements the principle of “Least Privilege” by removing full local administrator rights from users, a key step in Zero Trust security. However, it allows specific, trusted applications to run with elevated privileges when needed, balancing security with usability.

Use Case: A developer needs to run a specific legacy application that requires administrator rights to function. Giving them full admin access to the laptop would be a security risk. Instead, the IT admin configures a policy that allows only that specific legacy application to “self-elevate” when run by the developer. The developer gets their work done without needing full admin rights, and the rest of the system remains locked down.



Figure 4: Compliance in Endpoint Central

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 centres. 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/products/desktop-central/free-trial.html>

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

On-boarding and off-boarding processes are crucial aspects of Endpoint Central. 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 of Endpoint Central. When users decide to stop using our service, we have an off-boarding process in place to ensure a smooth transition out of Endpoint Central. 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 Endpoint Central 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 for more information.

Implementation Plan

Options for Implementation

Endpoint Central 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 Endpoint Central 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).

Endpoint Central 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. Endpoint Central 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 Endpoint Central, 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 (UKtime), 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: Endpoint Central also offers a paid program called, Premium Support, 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 Premium Support 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.

Onsite Support: Endpoint Central offers professional services for onsite training and implementation.

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 Endpoint Central. 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

Being a cloud solution, Endpoint Central 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. You can find our system requirements from [here](#).

Endpoint Central is compatible with major browsers such as Google Chrome, Microsoft Edge, and Mozilla Firefox browsers. It can be accessed from desktops, laptops, or mobile phones.

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 utilization 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 IoT to measure and optimise energy consumption across our offices. We've also implemented LED lighting, energy-efficient equipment, and IoT 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 IoT 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 impacted 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 Subscription Assistance 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 company Zoho 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 organisation 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.
- In-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

Testimonials

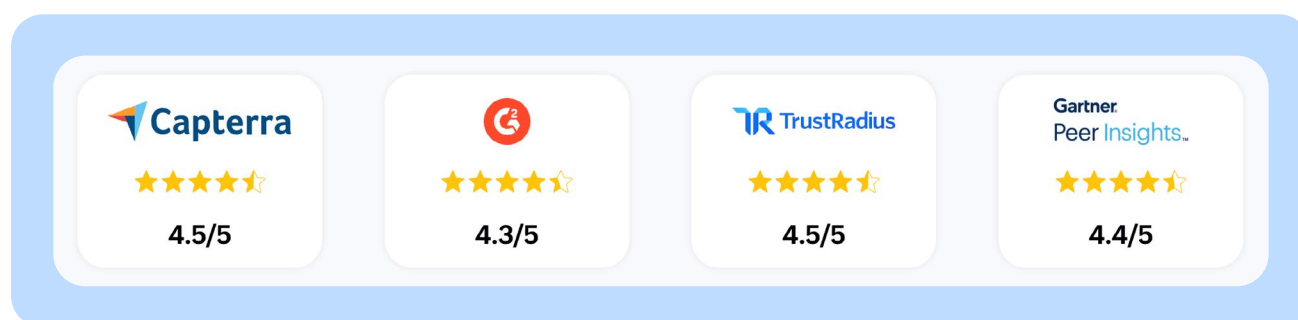


Figure 5: Consolidated list of Endpoint Central reviews

ManageEngine Endpoint Central continues to receive global recognition for its product excellence and innovation. In 2025, it earned several prestigious distinctions, including Gartner's Customer's Choice for Unified Endpoint Management and ISG's Leader recognition for Digital Employee Experience. The solution was also named a GigaOm Fast Mover in Secure Enterprise Browsing, received the AV-Comparatives Approved certification for malware protection, and was awarded Best UEM at the Cyber Security Summit.

In the latest AV-Comparatives Business Main-Test Series 2025, Endpoint Central 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 6: AV-Comparatives Badge for December 2025

Case Studies

1) How Endpoint Central helped Aria Care achieve boosted productivity and strengthened security compliance

Business challenge: Aria Care Group, a leading UK healthcare provider with over 68 care homes and 3,500 employees, struggled with inconsistent patch roll-outs and limited visibility into their distributed IT estate. Relying on legacy tools like Microsoft WSUS made it difficult to verify successful patching, while reactive troubleshooting often required physical device collection and manual intervention. This lack of centralized control resulted in security vulnerabilities, increased operational costs, and significant device downtime across their nationwide locations. To safeguard sensitive health data and streamline operations, Aria Care turned to Endpoint Central for a unified endpoint management strategy.

Major use-cases:

- Automated patch management and audit reporting replaced inefficient manual processes, providing clear visibility into device status and closing security gaps.
- Seamless device encryption and remote troubleshooting ensured the protection of sensitive health data while allowing the IT team to resolve issues instantly from anywhere, reducing on-site visits and costs.

2) How Endpoint Central helped Celtic Manor Resort accomplish centralised IT endpoint management

Business challenge: The Celtic Collection is a group of hotels and resorts offering luxury accommodations, event venues, and golf courses, with seven different locations across the UK, including the iconic Celtic Manor Resort. The business faced concerns over a poor deployment system that was susceptible to data loss. So, the IT team wanted to ensure visibility into all devices connected to the business. To find the right solution to combat IT vulnerabilities,

Celtic Manor resorted to EndpointCentral for unified endpoint management.

Major use-cases:

- Reduced manual hours with the automated patch deployment and approval mechanism.
- Integrated asset management and ticketing system under a single console.

3) How Endpoint Central helped Galbraith LLP accomplish streamlined OS deployment and CE+ compliance

Business challenge: Galbraith LLP, a leading property consultancy with 13 offices, struggled to maintain consistent patching and asset inventory across its distributed network. Their existing OS deployment process was remarkably slow, taking up to 2.5 hours per workstation, which hindered IT productivity. Additionally, the lack of a unified mobile device management platform made it difficult to enforce security policies and protect sensitive data on mobile endpoints, complicating their path toward Cyber Essentials Plus (CE+) certification.

Major use-cases:

- Significant efficiency gains by reducing OS deployment time from 2.5 hours to just 15 minutes per machine using automated imaging.
- Achieved CE+ certification through real-time visibility into endpoint vulnerabilities and automated patch deployment.
- Unified mobile security by implementing granular MDM policies and secure remote data wipe capabilities for lost devices.

You can also find a list of our updated case studies at our page [here](#).

Client List

Endpoint Central has a customer base of 33,000 with a mix of SMBs, enterprises and government organisations across multiple verticals (education, healthcare, finance, IT, manufacturing, defence and more).

You can also find a list of our updated client list at our page [here](#).

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



www.manageengine.com