ManageEngine
Endpoint Central

Datasheet

A single pane of glass for complete Endpoint Management and Security

Today's challenge

The way businesses operate has been redefined by the rapid rise in the number and diversity of endpoints used in enterprises. This also leads to various forms of cyberattacks and insider threats. With devices varying in form and function, more and more enterprises these days are looking for a unified endpoint management (UEM) model that will provide a single software platform for managing and securing a wide range of enterprise devices, including servers, desktops, laptops, smartphones, tablets, and IoT devices.

The solution

Endpoint Central is a unified endpoint management and security solution that manages and secures servers, desktops, and mobile devices from a single console. It automates the entire endpoint lifecycle, reducing IT costs, boosting efficiency, and improving productivity. With built-in security measures against vulnerabilities, data leaks, and browser threats, along with DEX capabilities for proactive monitoring and issue resolution, it ensures optimal performance and a seamless digital workplace.

Use Endpoint Central to

- Automate regular endpoint management activities.
- Standardize OS and application configurations across your network.
- Secure endpoints from a wide range of threats.
- Troubleshoot day-to-day problems.
- Audit your IT assets.
- Proactively monitor and enhance digital employee experience

Highlights

Supported operating systems

Linux
macOS
ChromeOS
Windows
iOS
Android
Windows Phone
tvOS

Recognized by

IDC FORRESTER Gartner

Over **20 Years** of expertise.

Trusted by over **34K** IT professionals.

Managing over **28M** endpoints.

Product support for **20** languages.

Used across **190+** countries

Patch Management

- Automate patching for over 1000 Windows, Mac, Linux, and third-party apps.
- Proactively detect and deploy missing patches.
- Test and approve patches before deployment to mitigate security risks.
- Deploy critical zero-day patches.
- Disable auto-updates and decline patches as needed.
- Obtain reports on system health status as well as system vulnerability.

Software Deployment

- Install or uninstall MSI and EXE-based applications.
- Schedule software deployments and perform pre and post-deployment activities.
- Allow users to install software themselves using the self-service portal.
- Utilize over 10000 predefined templates to deploy applications.
- Create a repository of packages and reuse them any number of times to install or uninstall software.
- Install software as a specific user using the Run As option.

Vulnerability Management

- Improve your security posture with integrated threat and vulnerability management by instantly detecting and remediating vulnerabilities.
- Enhance security by deploying security policies and mitigating system misconfigurations.
- Leverage ManageEngine's exclusive partnership with the Centre for Internet Security (CIS) to ensure compliance with CIS benchmarks.
- Swiftly spot zero-day vulnerabilities and deploy mitigation scripts as workarounds before the patches arrive.
- Audit and eliminate high-risk software such as end of life software, remote desktop sharing software, and peer to peer software to stay safe from data breaches.
- Audit active ports to discover anomalies as a part of vulnerability management.

Asset Management

- Track all hardware and software in your network live.
- Ensure software license compliance.
- Block executables and uninstall prohibited software.
- Analyze software usage statistics and reduce costs associated with unused software using software metering.
- Receive notifications for specific events such as detection of new software, non-compliance due to under-licensing, and prohibited software.
- Gain over 20 pre-defined reports for hardware, software, inventory, and license compliance.

Mobile Application Management

- Create your own enterprise app repository containing only IT-approved in-house and commercial apps.
- Silently install, update, and remove corporate apps from devices while also managing app licenses and preconfiguring app permissions.
- Ensure devices run only trusted corporate apps, blacklist malicious/vulnerable apps, and prevent users from uninstalling corporate apps.

System tools

- Monitor and analyze remotely managed systems by viewing the task details and processes that are running on them.
- Remotely boot up a machine instantly using Wake-on-LAN, or schedule boot-ups.

  Publish announcements company-wide or just to technicians.
- Schedule disk defragmentation, check disks, and disk cleanup for local or remote workstations.

Mobile Device Management

- Automate bulk enrollment and authentication of BYOD and corporate devices.
- Control OS updates and troubleshoot remote mobile devices.
- Gain complete visibility into your organization's mobile assets through predefined and customizable reports.

Application Control

- Discover all installed applications and executables, and categorize them as enterprise approved or unapproved based on their digital signatures.
- Flexible regulation that provides multiple modes to efficiently establish a zero trust environment.
- Hassle-free application control that allows users to request access to applications.
- Adopt a Zero Trust approach by enabling Strict Mode to prohibit even unmanaged applications, automatically.

Data Leakage Prevention

- Monitor and regulate your enterprise data movement from a centralized console to combat insider attacks and data loss.
- Scan and categorize enterprise's critical data as per compliance and regulatory standards.
- Regulate data transfer attempts via cloud uploads, E-mail exchanges, printers, and other peripheral devices.
- Receive instant alerts for policy breach attempts and remediate false positive events.

Browser Security

- Lockdown enterprise browsers and harden the browser settings to prevent browser-based attacks.
- Gain a comprehensive view of multiple browsers being used across the network.
- Enforce browser security configurations such as STIG and CIS compliances.
- Implement a safe browsing experience by detecting and removing harmful plug-ins.
- Allow enterprise-approved websites and block unwanted web apps to increase productivity and security.

Mobile Security Management

- Configure and enforce corporate security policies affecting Wi-Fi, VPN, email, and more.
- Prevent unauthorized access to corporate email, and securely distribute, save, and view content.
- Enforce device-level encryption; isolate personal and corporate workspaces on BYOD devices; and locate, lock, and wipe misplaced devices.

Reports

- Utilize over 200 out-of-the-box Active Directory reports on users, computers, groups, OUs, and domains.
- Lower utility bills with effective power management, and view system uptime reports.
- Obtain up-to-date user logon details with user logon reports.
- View reports on patches, configurations, and events for auditing.

Configurations

- Standardize desktop, computer, application, and security settings with baseline configurations for your entire organization.
- Use over 40 configurations for users and computers, or create templates for frequently used configurations.
- Choose from over 180 scripts in the script repository.
- Restrict and control the usage of USB devices like printers, CD drives, portable devices, bluetooth devices, modems, and other peripherals in the network, both at the user and computer level.
- Go green with effective power management by applying power schemes, shutting down inactive computers, and viewing system uptime reports.
- Configure browser, firewall, and security policies; achieve access control for files, folders, and the registry using permissions management.
- Set alerts for password expiration and low system drive space.

Peripheral Device Control

- Effectively regulate and restrict the entry of more than 15 types of peripheral devices from a centralized console along with automatic detection of active ports.
- Role-based file access and transfer control with file transfer limit to secure your enterprise-critical data.
- Grant temporary access for peripheral devices to specific endpoints for a defined time frame.
- Be proactive by mirroring the data in a secure location when USB devices access your critical enterprise data, thus preventing data loss.
- Adhere to device compliance standards by preventing data loss through peripheral devices and get insights from comprehensive device audit reports.

Endpoint Privilege Management

- Remove unnecessary admin rights and run business-critical applications with restricted privileges to prevent attacks based on privilege elevation or credential compromise.
- Maintain the least privilege model without compromising productivity by enabling application-specific privilege elevation.
- Handle interim user needs by enabling privileged temporary access to applications that are automatically revoked after a set period.

Ransomware Protection

- Reactive protection for heightened endpoint security by gatekeeping ransomware.
- Multi-patented and machine learning-assisted behavior analysis instantly detects any ransomware attempting to intrude on your network.
- Provides detailed analysis of all intrusion attempts.
- Offers seamless rollback to ensure your data is recovered with one click.

Digital Employee Experience (DEX)

- Continuously monitor endpoint health with real-time telemetry on CPU, memory, disk, battery, warranty, GPU, and application crashes.
- Detect and prioritize issues proactively through configurable alerts, severity tagging, and smart alert grouping to reduce noise.
- Diagnose root causes quickly using contextual diagnostics that link failures to device versions, app versions, models, services etc
- Automate remediation at scale with pre-built scripts, workflows, and a no-code builder for silent or consent-based fixes.
- Benchmark and improve performance using device-level experience scores, trend dashboards, and baseline comparisons.
- Leverage a pre-built action library of data collectors, scripts, and workflows, for organization-specific actions.

*Available as an add-on

Remote Control

- Leverage secure remote control to meet various compliance regulations, including HIPAA and PCI DSS.
- Troubleshoot remote desktops seamlessly with collaboration between multiple users.
- Integrated video, call, chat; and options for transferring files between machines.
- Record entire remote control sessions for auditing purposes.
- Lock end users' keyboards and mice, and black-out their screens to ensure confidentiality during remote sessions.
- Take advantage of 128-bit AES encryption protocols during remote control operations.

OS Deployment

- Automatically capture the image of a computer, whether it's live or shut down, using intelligent online and offline imaging techniques.
- Store these images in a centralized repository and perform OS deployment on the go.
- Customize captured images by using deployment templates for different roles and departments within your organization.
- Perform hassle-free deployment across different types of hardware.
- Execute post-deployment activities like installing applications, configuring computer settings, and more.

BitLocker Management

- Secure your computer's data by automating encryption for select drives or the entire hard drive.
- Identify the TPM-installed computers for enhanced PIN security along with passphrase authentication.
- Retrieve your computer's data using the recovery key in case of faulty hardware and reset the password for the computers removed from the network.
- Employ data encryption policies and stay compliant with data protection guidelines like FISMA, HIPAA, and PCI-DSS.

Next-Gen Antivirus

- Real-time AI-assisted malware detection enforces protection against evolving threats.
- Comprehensive incident forensics with detailed reports align with MITRE Tactics, Techniques, and Procedures (TTPs).
- In-depth insights into attack methods, pathways, and kill-chain analysis.
- Immediate intrusion mitigation, including ransomware protection, ensures swift intrusion neutralization.
- Threat mitigation with minimal disruptions to your network's operations ensures business continuity.
- One-click file recovery allows users to easily restore compromised files to their original state with a simple click.

Endpoint Detection and Response

- Continuously monitor endpoints using AI-powered behavioral analytics and memory scanning.
- Proactively hunt threats across your environment with forensic timelines, and process-level telemetry.
- Accelerate investigations with Zia AI-driven root cause analysis that traces every threat back to its origin, within minutes.
- Execute rapid response actions such as isolating a device, terminating processes, and containing the attack — then remediating the same endpoint from the same console, without needing physical access.

Secure Private Access with Zero Trust

- Enable zero trust-based, identity-driven access to internal applications without VPN or any implicit trust.
- Grant access only to the specific application a user is authorized to reach, eliminating lateral movement risks.
- Enforce granular access policies evaluated per request, based on user identity, device health, and context instead of a one-time login check.
- Connect users to internal apps through secure, encrypted tunnels routed directly to the application without exposing the corporate network.
- Native to Endpoint Central — no new agent to deploy. Private Access uses the same agent already on your endpoints, effective from day one.

© 2026 Zoho Corp. All rights reserved.

ManageEngine
Endpoint Central