

ManageEngine



Desktop
Management



Mobile Device
Management



OS
Deployment



Device and App
Management

Patch
Management



Advanced Remote
Control



Enterprise
Browser
Security



Vulnerability Man-
agement



Endpoint Management & Security Solutions

One-stop solution for all your **endpoint management needs**

Automated patch management

- Automate patching for Windows, macOS, Linux, and third-party applications
- Patch servers, OSs, desktops, laptops, legacy applications, and drivers
- Break bandwidth bottlenecks by empowering computers to download patches directly from the vendor's website
- Deploy patches from mobile devices to stay secured on the go

Manage up to
50
endpoints for free



Available for MSP / Available on cloud and on-premises

Simplified, tailor-made software deployment

- Silently install and uninstall free and commercial software
- Implement a self-service portal for Windows and macOS
- Leverage over 7,000 software templates for Windows, macOS, and Linux
- Stay atop critical software updates by automating the template updates

Real-time IT asset management

- Manage software licenses and hardware warranties
- Be notified of every hardware and software change
- Gauge the usage of every application, & make informed decisions about license purchases
- Periodically keep tabs on the types of files present in your network

Advanced remote control and system tools

- Record and audit remote sessions; leverage integrated chat, voice, and video calls
- Use the remote command prompt, registry, device manager, and task manager
- Leverage power-saving schemes, and remotely reboot, lock, shut down, & wake computers
- Get past the traditional file transfer protocols with two-way file transfers across endpoints

Secure endpoints from a central console

- Keep an eye on USB device usage, and fortify your browsers against web-based threats
- Blacklist unauthorized applications and malicious executables
- Fetch details on BitLocker encryption and FileVault
- Keep privilege elevation attacks at bay by getting a bird's-eye view of the granted administrative privileges

Amp up productivity with integrations

- Integrates with ServiceDesk Plus, ServiceNow, Jira, Zendesk, Spiceworks, and other help desk software
- Integrates with Asset Explorer, Browser Security Plus, and Analytics Plus for augmented IT administration
- Available in AWS marketplace and Azure marketplace; APIs available for third-party integration

Image and deploy OS

- Utilize simplified, centralized imaging techniques
- Automate the collection of drivers from imaged machines
- Leverage hassle-free deployment across dissimilar hardware
- Carry out OS deployment for remote offices around the globe

Mobile device management

- Manage endpoints running Android, iOS, iPadOS, macOS, Windows, tvOS, and Chrome OS
- Silently install store and in-house apps; access corporate data using authorized apps
- Track the location of mobile devices, and create a geo-fence to impose restrictions

Endpoint management for MSPs

- Enjoy remote monitoring and management software specifically built for managed service providers (MSPs)
- Manage clients' servers, desktops, laptops, mobile devices, and tablets from a central location

Empower your workforce with the enhanced **powers of mobility**

End-to-end device management

- Leverage automated out-of-the-box enrollment and authentication for BYOD and corporate devices with integrated directory services
- Enforce corporate policies and preconfigure device settings like Wi-Fi, VPN and certificates
- Remotely control devices, and chat with users to troubleshoot devices in real time

Seamless app management

- Build a repository of enterprise-approved store and in-house apps, and prevent installation of malicious and unapproved apps
- Silently install, delete, or update apps, and test enterprise apps before deploying them in your production environment
- Predefine app permissions and configurations while distributing apps to devices

Prevent corporate data theft

- Containerize corporate data, enforce encryption, and proactively secure stolen and misplaced devices using Lost Mode, Firmware Password, etc.
- Associate security policies with corporate Office 365 apps, even when accessed from unmanaged devices, or completely restrict access from unauthorized devices
- Create a geo-fence to automatically locate, lock, or wipe non-compliant devices remotely

Configure and secure corporate email access

- Allow only managed devices to access enterprise-approved email apps and accounts
- Integrate with email platforms such as Office 365, Exchange Online, Azure, and Lotus
- Ensure users share and view email attachments securely using authorized apps only

Manage up to
25
mobile devices for free



Available for MSP / Available on cloud and on-premises

Securely distribute, save, and view content

- Segregate your corporate documents and securely distribute them to devices
- Access corporate documents using trusted apps, and prevent backups via third-party cloud services
- Automate the updating and deletion of documents from a central point

Lock down devices to kiosk mode

- Lock devices to a single app to use them for point-of-sale (POS), digital signage, etc.
- Whitelist a set of apps that devices can run
- Prevent users from modifying admin-defined settings by restricting basic device functionalities, physical buttons, etc.

Control device OS updates

- Automate and schedule OS deployment during non-work hours to avoid affecting productivity
- Test and approve OS updates for enterprise app compatibility
- Restrict users from manual ad hoc updating to unapproved OS versions

One-click integrations

- Integrates with ServiceDesk Plus, Spiceworks, Jira, ServiceNow, Zendesk, Zoho Creator, and Zoho CRM
- Available on AWS and Azure marketplaces
- APIs available for third-party integration

Patch **Windows, macOS, Linux**, and **third-party** applications

Patch over 1,000 applications

- Deploy patches to Windows, macOS, and Linux platforms
- Patch more than 300 third-party applications like the Adobe suite and Java
- Patch computers across LAN, WAN, roaming users, and closed networks (DMZ)

Automate patch management

- Automate patching for desktops, servers, workstations, drivers, and more
- Detect, download, and deploy missing patches to vulnerable systems
- Automatically test and approve patches before deployment


Granular control over patch deployment

- Configure deployment policies to install patches during non-business hours
- Decline patches to specific groups or departments
- Wake devices before deployment, reboot after installation, and perform remote shutdown

Compliance and reporting

- Leverage PCI-compliant patching, auditing, and reports
- Report on missing patches and vulnerable systems
- Customize query reports, dashboards, and views

Manage up to
25
endpoints for free




Available on cloud & on-premises

Automate third-party patching using **Microsoft SCCM**

Patch more than 300 third-party applications

- Customize and automate the deployment of patches to SCCM
- View complete data on SCCM deployment using deployment reports
- Streamline third-party patching in SCCM with our native plug-in

Supports patching for over
300
third-party apps



Create desired third-party applications in SCCM and Microsoft Intune

- Customize the deployment of applications using scripts
- Select from a large repository of third-party applications

Manage SCCM client systems with ease

- Perform a wide range of client management actions with 25 of the most essential admin tools
- Carry out on-demand client actions, client troubleshooting, and system management operations

Third-party update catalogs

- Simplify third-party patching with update catalogs for SCCM 1806 and above
- Get updates for third-party apps within the SCCM console

Provision **OSs on multiple workstations** as quickly as provisioning one device.

Adaptive imaging techniques

- Perform online and offline disk imaging
- Image disks irrespective of disk style, size, and driver type
- Image the OS based on disk partitions, and shrink these partitions as needed
- Automatically collect drivers from the imaged machine
- Migrate user profiles right when upgrading the operating system

Automate OS imaging
and deployment for
Windows



One master image for every make and model

- Deploy images across dissimilar hardware
- Utilize flexible boot options such as using a USB device, ISO media, or a PXE server
- Leverage advanced deployment options, such as deployment using a unique authentication passcode, unicast or multicast deployment, and scheduled deployment
- Perform post-deployment activities such as application installation

Flexible deployment templates

- Customize a standard image to meet your organization's needs
- Utilize unallocated disk space while deploying the OS
- Rename the machine and provide a unique security identifier (SID) post deployment

Access and troubleshoot **Windows, macOS, and Linux** computers anytime

Granular control over network computers

- Utilize HIPAA, PCI, and trade practice compliant remote control
- Collaborate with other technicians while troubleshooting
- Automatically reconnect to remote sessions after reboot
- Seamlessly access computers that are connected to multiple monitors

Troubleshoot up to
10
computers for free



Available on cloud and
on-premises

Hassle-free troubleshooting

- Leverage voice, video, and text chats to get more background information
- Instantly wake computers on LAN before troubleshooting
- Fetch idle computers and remotely shut them down to cut production costs

Tweak computer settings without leaving your desk

- Instantly access the command prompt and registry using systems account
- Send and receive file and folders right away
- Manage processes, services, start-up programs, and more

Secure, comprehensive remote assistance

- Get the end user's stamp of approval before every session
- Track and audit remote sessions by recording them
- Monitor users by shadowing sessions
- Tackle user-level access control and management

Multi-browser management has never been so easy

Comprehensive browser management

- Obtain better visibility by tracking the browsers, plug-ins, and extensions across your network
- Prevent web-based cyberattacks and data leaks by enforcing security policies
- Keep tabs on the web applications and websites users visit

Ensure and enforce compliance

- Enforce browser compliance with CIS and STIG standards
- Create your own compliance standard to be followed in your organization
- Deploy policies to ensure computers comply with mandated standards

Mitigate web-based threats

- Detect and remediate computers that have harmful plug-ins or extensions
- Provide and revoke access to URLs, plug-ins, and extensions based on users' roles
- Restrict downloads to trusted websites

Stay ahead of zero-day attacks

- Detect computers running infected plug-ins
- Run multiple versions of Java plug-ins side-by-side on a single machine
- Render legacy websites and applications in legacy browsers, even when opened with modern browsers



Prioritization-driven threat and vulnerability management with built-in patching

Vulnerability management

- Detect vulnerabilities in real time and assess their risk based on CVSS score, severity, age, impact type, exploit disclosure, patch availability, and asset criticality to prioritize your response
- Gain visibility into publicly disclosed and zero-day vulnerabilities with a dedicated tab, and utilize workarounds to mitigate them before the fixes arrive
- Analyze vulnerability trends, see which vulnerabilities matter most, and track remediation efforts with dashboards

Security configuration management

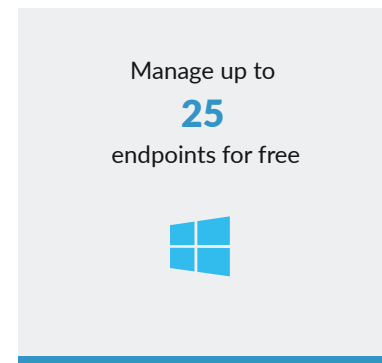
- Identify misconfigurations in operating systems, applications, browsers, and web servers, and bring them back to compliance
- Audit your firewalls, antivirus and BitLocker status, and open ports for malicious activity
- Prevent brute-force attempts by enforcing complex password, account lockout, and secure logon policies

Swift remediation with built-in automated patching

- Automatically correlate vulnerability intelligence and patch management
- Automate and customize the scanning, testing, and deployment of patches for Windows, macOS, Linux, and over 350 third-party applications

High-risk software audit

- Look out for legacy software that has or is about to reach its end of life (EOL)
- Sniff out and remove peer-to-peer and remote desktop sharing software



Data Loss Prevention solution for USB and peripheral devices

Authorize only what you trust

- Instantly discover newly connected devices and classify them as whitelisted or blacklisted
- Curate your trusted devices list by adding devices based on their device instance paths
- Trust a group of similar devices simply by utilizing wildcard patterns
- Secure your network perimeter by allowing only BitLocker-encrypted devices

Manage the actions of
17
types of peripheral devices



Granular device and file action control policies

- Designate file access permissions—like allow, block, or read-only—for individual devices or based on device type
- Manage exactly which files can be copied to or from USB devices, and regulate file transfers based on file size and extension
- Grant third-party devices temporary access to boost productivity without compromising security

Monitor device activity, and record events

- Continuously track data transfers and other user interactions with USB devices
- Maintain logs containing salient details on all device and file actions
- Receive email notifications whenever a user tries to connect a restricted device
- Automatically retain shadow copies of vital information transferred via USB devices for swift recovery in case of emergencies

Intuitive reports for easy analysis

- Gain actionable insights on important events through the dashboard
- Perform audits and schedule reports to stay up-to-date on device trends and user patterns

Application control with an integrated privilege management solution

Trust-centric control and malware prevention

- Discover all running applications and executables, and categorize them as authorized or unauthorized based on their digital signatures
- Create Zero Trust based application whitelists targeted to users or devices
- Blacklist all malicious executables to prevent malware intrusions, advanced persistent threats, and zero-day attacks

Manage up to
25
devices for free



Customizable control capabilities

- Build application whitelists and blacklists based on rules like vendor, product name, verified executables, and hash values of executables
- Personalize the implementation of your application control solution utilizing either Audit Mode or Strict Mode
- Authorize or prohibit greylisted applications by moving them to new or existing whitelists and blacklists

Endpoint privilege management

- Establish the principle of least privilege by maintaining all employees as standard users
- Allow chosen users to run business-critical applications as administrators to maintain productivity

Dashboards and reports

- Gain real-time insights into your entire application environment from the dynamic, graphics-rich dashboard
- Arrive at informed decisions by leveraging an intuitive set of predefined reports

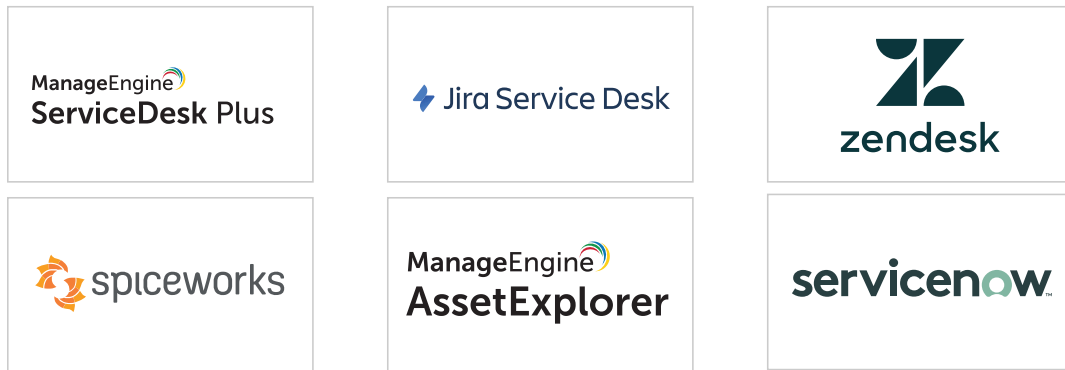
Reviews



Recognized by



Integrations



Available on



Available as **Mobile App**



Over 30,000 customers across the globe

Managing over 8 million endpoints worldwide



ENDPOINT MANAGEMENT

Desktop Central

Automate patch and software deployment, IT asset management, advanced remote control, mobile device management, imaging and deploying OS, audit-ready IT reports.

Mobile Device Manager Plus

Quick onboarding, App Management, Containerization, Email Management, Profile Management, Security Management, Geofencing & Reports.

Desktop Central MSP

Remote monitoring and management (RMM) software for MSPs to automate endpoint management and security for clients' network from a central location.

Mobile Device Manager Plus MSP

Customer Segmentation, Asset Management, Remote Troubleshoot, OS Update Management, App Lock, Compliance Management.

OS Deployer

OS imaging and deployment software for local, and remote offices.

Remote Access Plus

Advanced remote control and over 12 diagnostic tools to troubleshoot Windows, Mac, and Linux computers.

ENDPOINT SECURITY

Patch Manager Plus

Automated patch management for Windows, Mac, Linux, and 3rd party apps.

Patch Connect Plus

Integrates with Microsoft SCCM to patch third-party applications.

Browser Security Plus

Deploy security configurations to browsers, manage add-ons, isolate sites and prevent all browser-based threats.

Vulnerability Manager Plus

A single interface to detect and remediate misconfigurations and vulnerabilities, harden web servers & eliminate risky software.

Device Control Plus

Device detection and monitoring, port auditing, device whitelisting and blacklisting, File access control, File tracing, File shadowing and Temporary device access.

Application Control Plus

Endpoint privilege management, application discovery, whitelisting, and blacklisting of applications at granular levels.