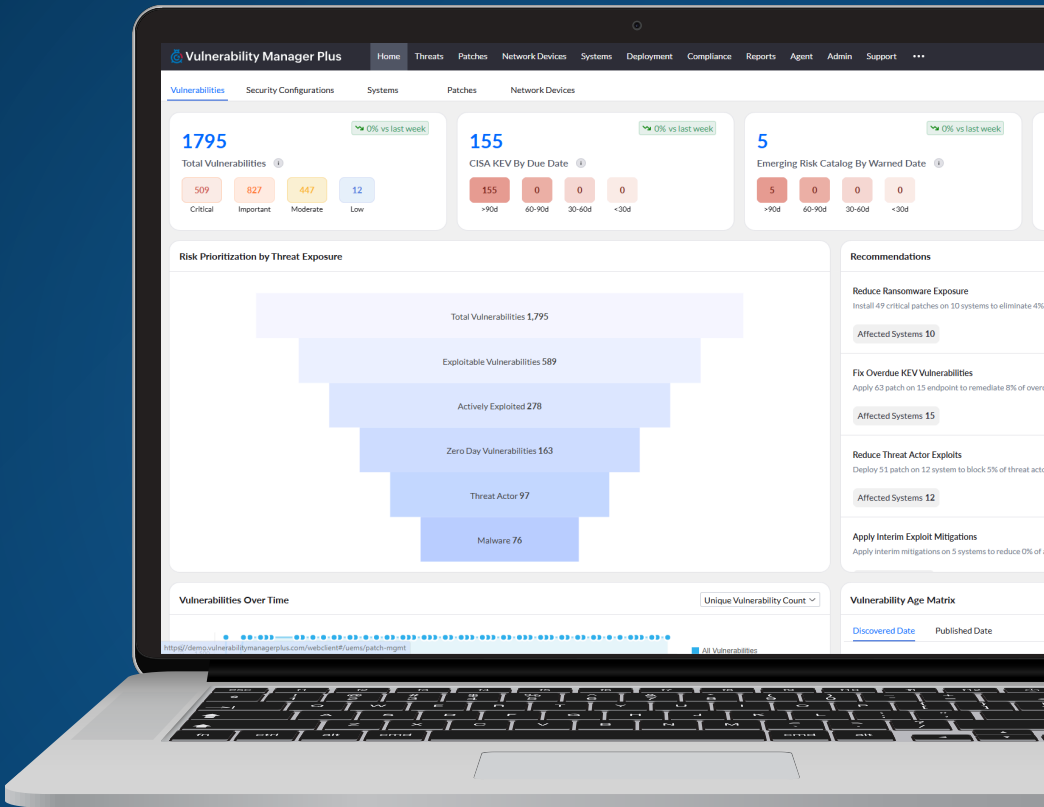


Minimize your attack surface with proactive exposure management

ManageEngine Vulnerability Manager Plus is a comprehensive exposure management solution that builds a strong cybersecurity foundation, helping security teams proactively identify, prioritize, and remediate known and unknown vulnerabilities. With built-in patching and compliance auditing, it delivers complete visibility and control across desktops, laptops, servers, VMs, DMZ servers, and network devices.



Challenge

The risk is accelerating

The CVE database has grown to over 375,000 recorded vulnerabilities, making it the largest repository of security flaws to date. This surge highlights how rapidly the attack surface is expanding, giving threat actors more ways to impede organizations than ever before.

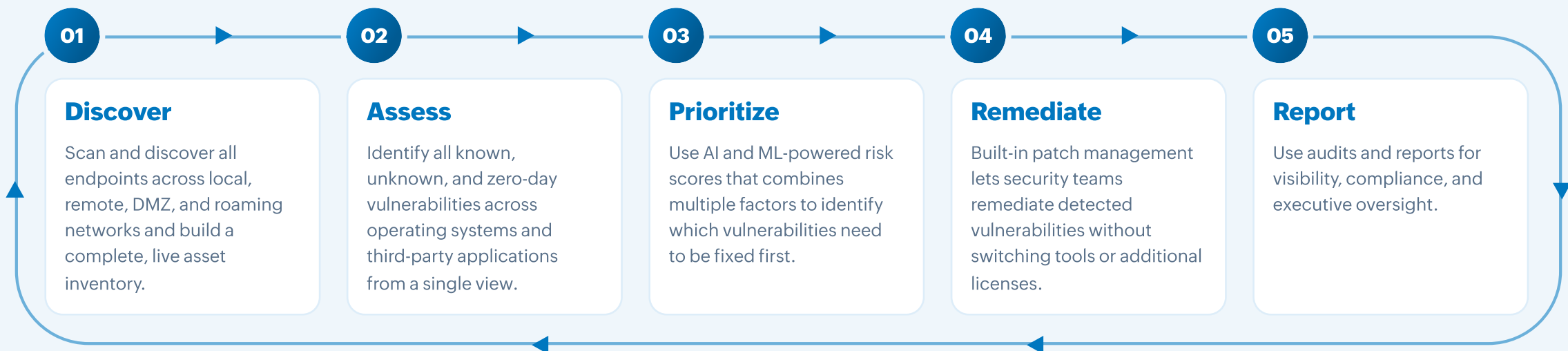
With hundreds of new vulnerabilities emerging every day, implementing an exposure management solution is no longer a debate; it's imperative. Keeping your attack surface protected starts with exposure management as a foundational layer for a resilient cybersecurity posture.

Solution

Close the gap between detection and remediation

ManageEngine Vulnerability Manager Plus delivers continuous discovery, AI-powered risk prioritization, and built-in patching from a single console, so security teams act on what matters and not on everything at once.

The Vulnerability Manager Plus lifecycle



135+
countries served

7+
years in the industry

4500+
organizations worldwide

2M+
endpoints secured

Trusted by



Key Benefits



Built-in patching with no additional cost



AI/ML-based risk prioritization



Proactive defense against zero-day threats



Audit ready compliance, always



Multi-OS coverage



Emerging threats, flagged early

How Vulnerability Manager Plus reduces your attack surface

Asset discovery, vulnerability assessment, and AI-powered risk prioritization

- Discover every endpoint and asset across your network, whether roaming, in local or remote offices, or in a DMZ, through automated or on-demand scans.
- Get complete visibility into all vulnerabilities (known, unknown, zero-day, or exploited) in a single window as well as a dedicated view for zero-day threats.
- Prioritize and remediate vulnerabilities based on AI and ML-based risk scores, **vulnerability age**, **CVSS severity**, **active attack trends**, Exploit Prediction Scoring System (EPSS) scores, and more to ensure the most critical ones are addressed first.

Security configuration management

- Identify misconfigurations in OSs, applications, and web servers and restore compliance.
- Audit your firewalls, antivirus software, and BitLocker status.
- Prevent brute-force attempts by enforcing complex password policies, account lockout policies, and secure logon policies.
- Ensure memory protection settings, such as Structured Exception Handling Overwrite Protection, Data Execution Prevention, and Address Space Layout Randomization, are enabled.
- Manage share permissions, modify user account controls, and disable legacy protocols to reduce your attack surface.
- Safely alter security configurations without interrupting business operations by reviewing critical deployment warnings.

Built-in automated patch management

- Automate patching for Windows, macOS, Linux, and over 1,500 third-party applications.
- Customize patch deployment policies for hassle-free installation.
- Automatically test, approve, and deploy stable patches to endpoints.
- Decline patches to specific endpoint groups based on their performance.

Web server hardening

- Continuously monitor your web servers for default and unsecure configurations.
- Analyze web server misconfigurations based on the context and view resolutions to fix them.
- Ensure SSL certificates are configured and HTTPS is enabled for secure client-server communication.
- Verify whether the server root directory permissions are restricted to prevent unauthorized access.

High-risk software, port, and antivirus auditing

- Stay vigilant about legacy software that has reached or is about to reach its end of life.
- View real-time information on P2P software and remote sharing tools and eliminate them with just a click.
- Gain continuous visibility over the active ports in your environment, helping you identify those that can pose risks.
- Identify systems that have outdated or disabled antivirus solutions and rectify them to improve your organization's security posture.

Compliance auditing

- Audit and maintain compliance with over 130+ CIS Benchmarks, NIST SP 800-171 and 800-53, and the United Kingdom's Cyber Essentials.
- Customize compliance benchmark rules to align with your organization's security policies and operational requirements.
- Automate audits on multiple groups of endpoints for multiple benchmarks at once.
- View detailed remediation guidance for every violation.

Network device vulnerability management *

- Maintain a consolidated inventory of all network devices across your local and remote offices.
- Run the appropriate firmware detection commands on each device to identify firmware versions and associated vulnerabilities.
- Gain complete visibility into all firmware vulnerabilities present on your managed devices.
- Group devices by the OS, vendor, or similar attributes to streamline and target patch deployment.
- Deploy the right firmware patches efficiently to reduce risks and remediate vulnerabilities faster.

System Quarantine Policy

- Configure system compliance conditions based on factors such as OS patches, software, services, vulnerabilities, registry and file checks, file versions, and file paths.
- Audit your network regularly to identify non-compliant systems and notify end users about the non compliance status.
- Isolate non-compliant systems from the network and auto-restore access once compliant.

*Only available on the on-premises platform

Pricing

Free edition Complete vulnerability management for 20 workstations, five servers, and two network devices	On-premises Professional edition Starts at \$695 per year for 100 endpoints Enterprise edition Starts at \$1,195 per year for 100 endpoints	Cloud Professional edition Starts at \$895 per year for 100 endpoints Enterprise edition Starts at \$1,545 per year for 100 endpoints
---	--	--