



**ManageEngine**

 **Unified Endpoint Management and Security**

# ZOHO Corp.

(Est. 1996)

*Privately held and profitable since inception*



 **WebNMS**  
A Division of ZOHCO Corporation  
(1996 -2021)

IoT management framework

**ManageEngine**  
(Est. 2002)

Enterprise IT management solutions

 **Work. Online**  
(Est. 2005)

Applications for business, collaboration and productivity

 **ZOHO SCHOOLS OF LEARNING**  
(Est. 2005)

Technology and soft-skills training for local students

**Qntrl**  
(Est. 2021)

Workflow orchestration software

**Trainer Central**  
(Est. 2021)

An all-in-one training platform

# Bringing IT together



ManageEngine crafts comprehensive IT management software for your business needs

Available for  
Enterprise IT | Managed service providers (MSPs)  
as  
Self-hosted on-premises  
Self-hosted in public cloud (AWS, Azure)  
Zoho Cloud-native

## Enterprise service management

- Full-stack ITSM suite
- IT asset management with a CMDB
- Knowledge base with user self-service
- Built-in and custom workflows
- Orchestration of all IT management functions
- Service management for all departments
- Reporting and analytics

## Identity and access management

- Identity governance and administration
- Privileged identity and access management
- AD and Azure AD management and auditing
- SSO for on-premises and cloud apps, with MFA
- Password self-service and sync
- Microsoft 365 and Exchange management and auditing
- AD and Exchange backup and recovery
- SSH and SSL certificate management

## Unified endpoint management and security

- Desktop and mobile device management
- Patch management
- Endpoint device security
- OS and software deployment
- Remote monitoring and management
- Web browser security
- Monitoring and control of peripheral devices
- Endpoint data loss prevention

## IT operations management

- Network, server, and application performance monitoring
- Bandwidth monitoring with traffic analysis
- Network change and configuration management
- Application discovery and dependency mapping
- Cloud cost and infrastructure monitoring
- End-user experience monitoring
- DNS management
- AIOps

## Security information and event management

- Unified SIEM for cloud and on-premises
- AI-driven user and entity behavior analytics
- Firewall log analytics
- Data leak prevention and risk assessment
- Regulatory and privacy compliance

## Advanced IT analytics

- Self-service IT analytics
- Data visualization and business intelligence for IT
- Hundreds of built-in reports and dashboards
- Instant, flexible report creation
- Out-of-the-box support for multiple data sources

## Low-code app development

- Custom solution builder



## ManageEngine:

A bootstrapped, private, and profitable company

**20+**

years in the  
industry

**280,000+**

Organizations across the  
globe trust ManageEngine

**120+**

products and free tools for  
IT management

---

**4,500+**

ManageEngine  
employees

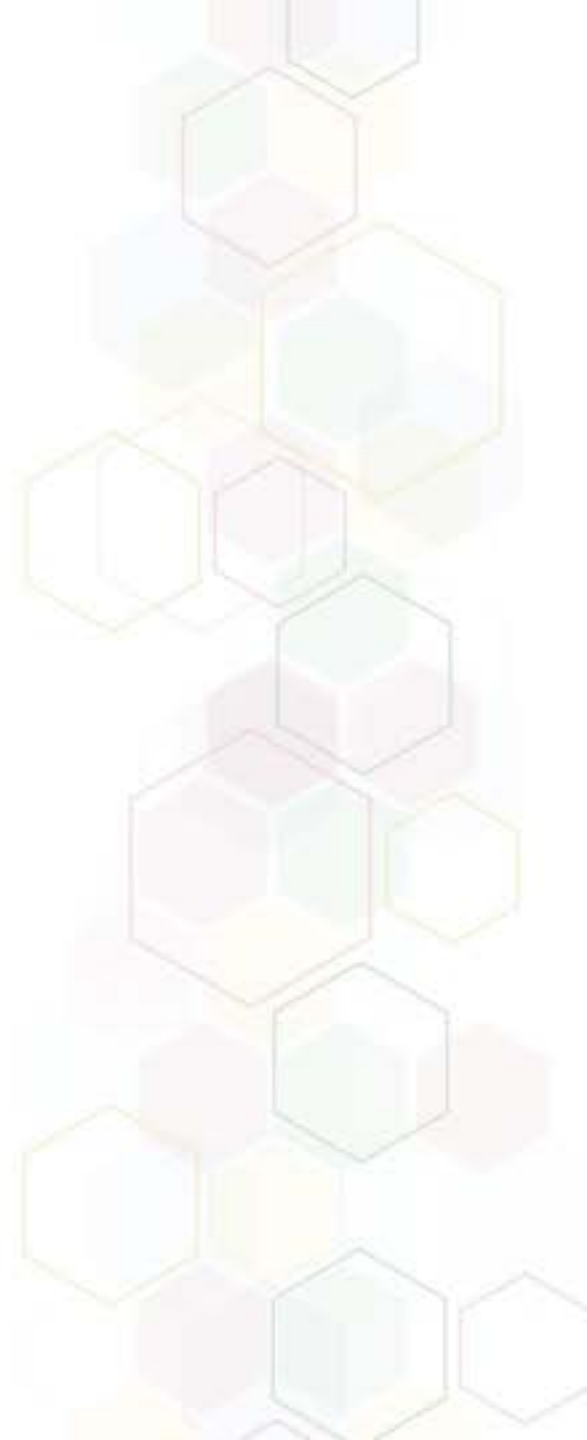
**190**

countries

ManageEngine 

# Vulnerability Manager Plus

Product overview

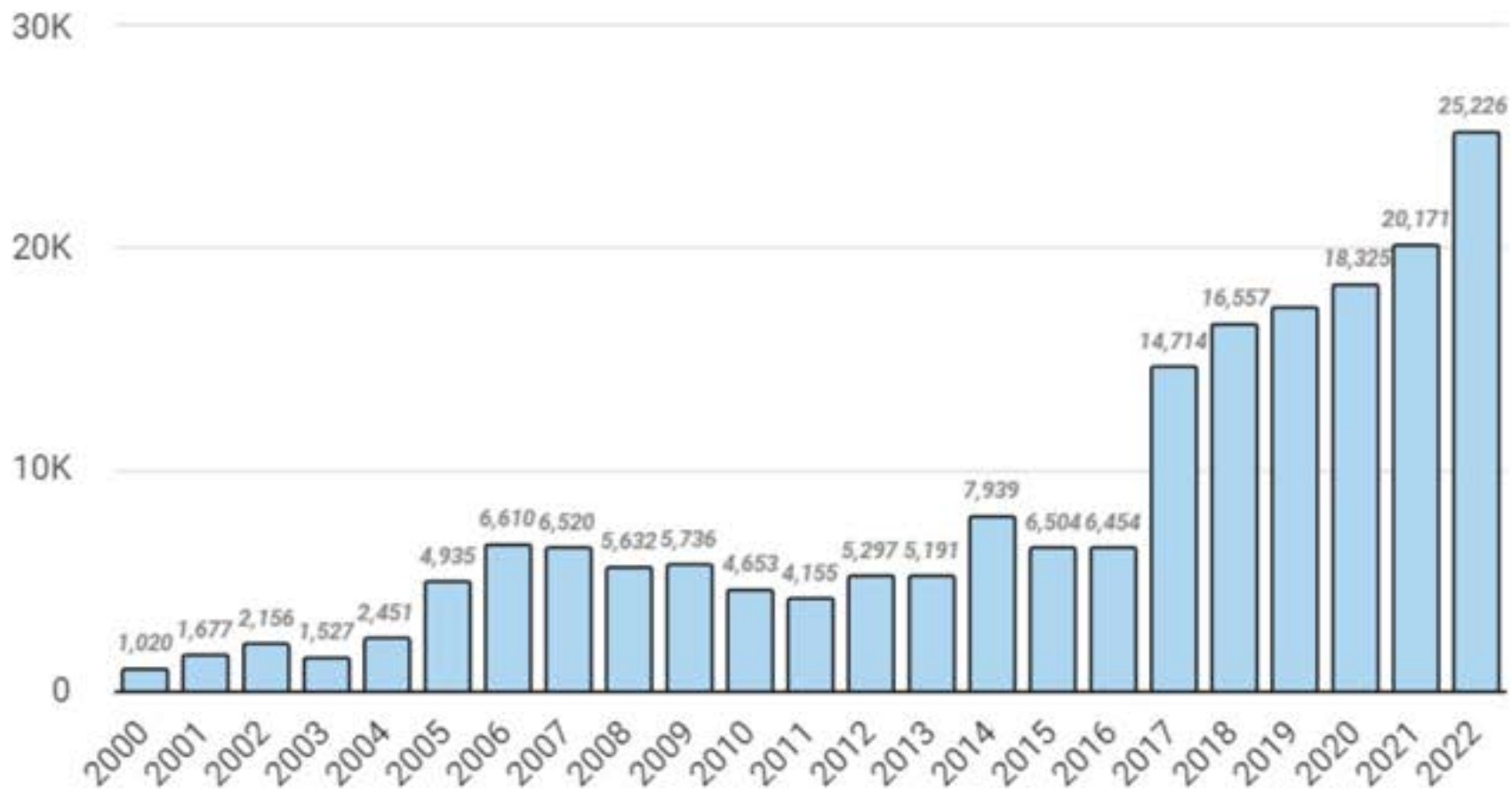




**Why do you need a vulnerability management solution?**

# Vulnerabilities are always on the rise

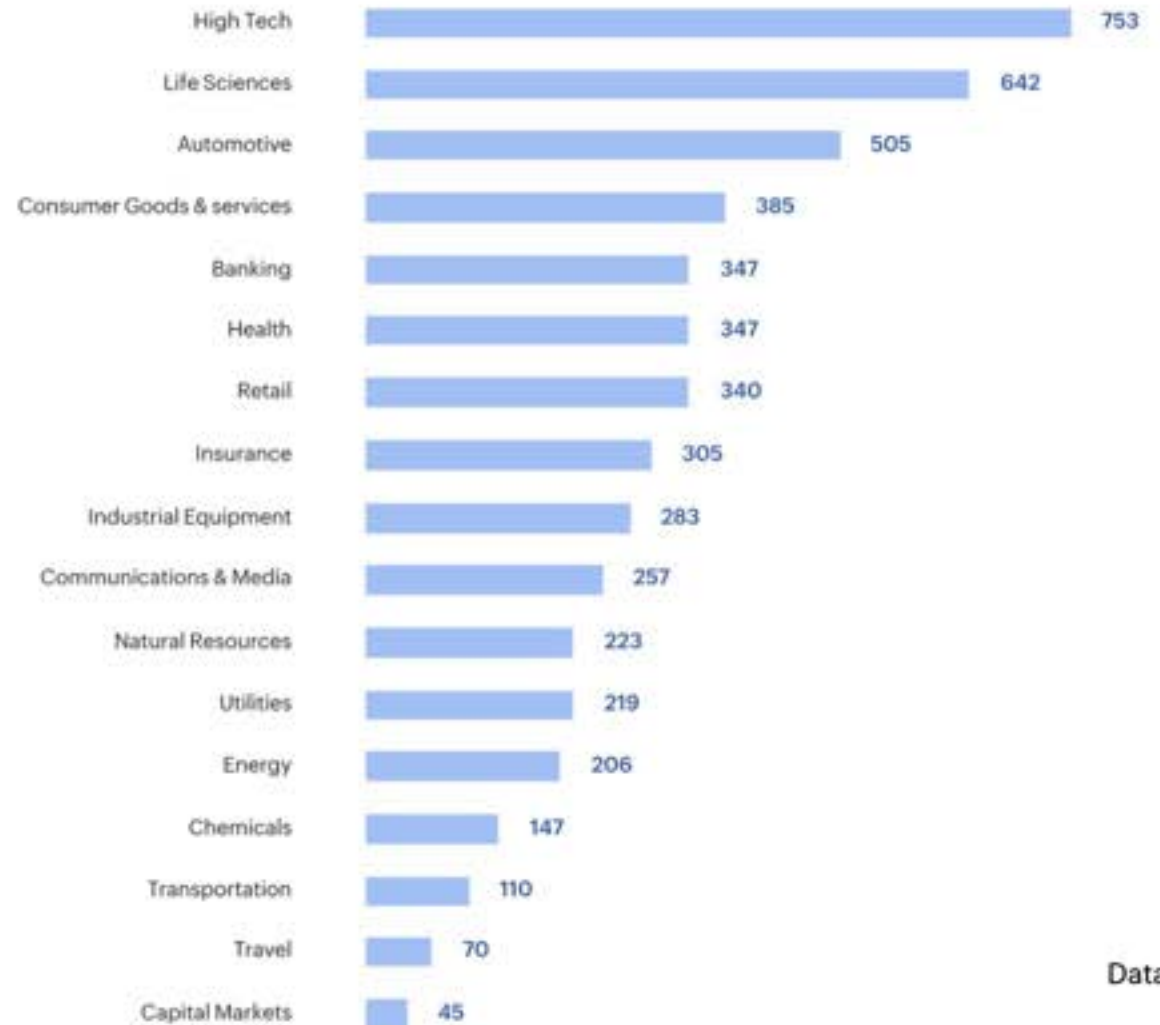
## Vulnerabilities by the year



Newly Identified and Cumulative Vulnerabilities Per Year, 1988-2020 (Source: [NIST](#))

# Negligence in securing your endpoints could cost you greatly

**\$5.2Tr**



Data in \$Bn

Expected foregone revenue cumulative over the next 5 years. Calculations over a sample of 4,700 global public companies - Source : Accenture research





**What is Vulnerability Manager Plus?**

## Prioritization-focused threat and vulnerability management software offering built-in patching for enterprises

- It is a multi-OS solution for delivering comprehensive visibility, assessment, remediation, reporting of vulnerabilities, misconfigurations, and other security loopholes across the enterprise network from a centralized console.



# 4 steps to taking control of your vulnerability management routine



# Supports Windows, Linux, and Mac



**Windows**



**Linux**



**Mac\***

\*Only patch management is supported for macOS.

# Highlighted features

- Comprehensive vulnerability assessment
- Security configuration management
- Automated patch management
- Compliance with CIS benchmarks
- Insightful reports





**Vulnerability Manager Plus features explained**

## Comprehensive vulnerability assessment & detection

Identify and assess real risks from a plethora of vulnerabilities spread across your OSEs, network devices and third-party applications

### Capabilities:

- ❖ Identify vulnerabilities along with their context, such as CVSS and severity scores, to ascertain priority, urgency, impact, and patch availability
- ❖ Know whether exploit code has been publicly disclosed for a vulnerability
- ❖ Keep tabs on how long a vulnerability has resided in your network
- ❖ Leverage a dedicated tab on publicly disclosed and zero-day vulnerabilities, and utilize work-arounds to mitigate them before the fixes arrive



# Security configuration management

Keep track of configuration drifts and deploy secure configurations to eliminate security loopholes.

## Capabilities:

- ❖ Identify misconfigurations in operating systems, applications, and browsers, and bring them back under compliance
- ❖ Audit your firewalls, antivirus, and BitLocker status
- ❖ Prevent brute-force attempts by enforcing complex password, account lockout, and secure logon policies
- ❖ Manage and alter security configurations by sharing permissions, modifying user account controls, and disabling legacy protocols to reduce your attack surface without interrupting business operations





# Automated patch management

Seamlessly download, test and deploy patches to multiple Operating Systems and 850+ 3rd-party applications.

## Capabilities:

- ❖ Automatically correlate vulnerability intelligence and patch management
- ❖ Automate patching for Windows, macOS, Linux, and over 300 third-party applications
- ❖ Customize deployment policies for hassle-free deployment
- ❖ Test and approve patches before rolling them out to production environment and decline patches to specific groups based on user requirements



# Compliance with CIS benchmarks

Leverage out-of-the-box policies to comply with over 75 CIS benchmarks.

## Capabilities:

- ❖ Helps audit and maintain compliance with over 75 CIS benchmarks.
- ❖ Automate audits on assets against multiple CIS benchmarks at once
- ❖ Gain detailed remediation for every violation.



# Web server hardening

Detect and remediate expired SSL, inappropriate web root directory access and other web server flaws.

## Capabilities:

- ❖ Continuously monitor your web servers for default and insecure configurations
- ❖ Analyze web server misconfigurations based on context, and gain security recommendations
- ❖ Ensure SSL certificates are configured and HTTPS is enabled to secure the communication between clients and servers
- ❖ Verify whether the server root directory permissions are restricted to prevent unauthorized access



# Audit high-risk software and active ports

Manage high-risk software and audit port activity in your network as a part of vulnerability management.

## Capabilities:

- ❖ Stay vigilant of legacy software that has or is about to reach end of life
- ❖ Obtain real-time information on peer-to-peer software and remote sharing tools that are deemed unsafe, and eliminate them with just a single click
- ❖ Gain continuous visibility over the active ports and sniff out instances where a port has been activated by malicious executables



# Insightful reports

Enterprises can arrive at informed decisions by leveraging dynamic, graphics-rich dashboard and intuitive set of predefined reports.

## Types of reports:

- ❖ Executive reports
- ❖ More than 10 pre-defined reports
- ❖ Schedule reports
- ❖ Custom query reports



# How does Vulnerability Manager Plus benefit your organization?

- Early identification of imminently exploitable threats that require little to no user intervention
- Reducing the effort spent in vulnerability management with a central console and insightful dashboards
- Eliminating the need for investing in separate patch management tools
- Avoiding hefty fines by conforming to cybersecurity compliance and regulations

**To learn more, visit:**

<https://mnge.it/vuln-mgmt>



---

**Try it for free!**

<https://mnge.it/vmp-download>

