ManageEngine

Unified Endpoint Management and Security

ZOHO Corp.

(Est. 1996)

Privately held and profitable since inception

WebNMS
A Division of ZOHO Corporation
(1996 -2021)

IoT management framework

ManageEngine
(Est. 2002)

Enterprise IT management solutions

ZOHO
Work. Online
(Est. 2005)

Applications for business, collaboration and productivity

ZOHO SCHOOLS OF LEARNING
CONTEXTUAL · RELEVANT · EXPERIENTIAL
(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

Enterprise service management

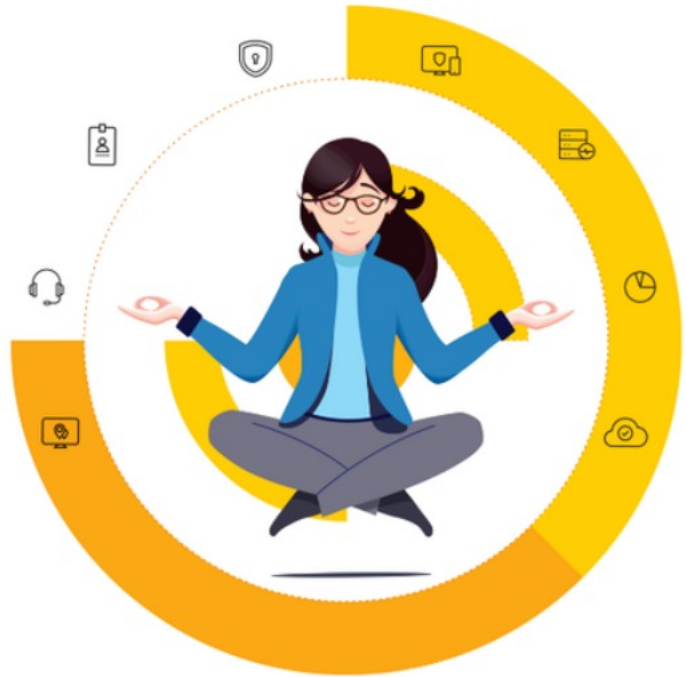
Full-stack ITSM suite
IT asset management with CMDB
Knowledge base with user self-service
Built-in and custom workflows
Orchestration of all IT management functions
Service management for all departments
Reporting and analytics

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 & Exchange management and auditing
AD & Exchange -backup and recovery
SSH and SSL certificate management

Security information and event management

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



Available for

Enterprise IT | Managed service providers (MSPs)

as

Self-hosted on-premises
Self-hosted in public cloud (AWS, Azure)
Zoho Cloud-native

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 & configuration management
Application discovery & dependency mapping
Cloud cost and infrastructure monitoring
End user experience monitoring
AIOps

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

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

Data center compliance certifications

US

Central Washington
SOC 1 TYPE II | SOC 2 TYPE II | HIPAA | PCI DSS
Dallas
SOC 1 TYPE II | SOC 2 TYPE II | SOC 3

India

Chennai
ISO 27001
Mumbai
ISO 27001 | ANSI/TIA ISO 20000-1:2011 | SOC 1 TYPE II | SOC 2 TYPE II

Australia

Sydney
SOC 1 TYPE II | SOC 2 TYPE II | ISO 27001
Melbourne
SOC 1 TYPE II | SOC 2 TYPE II | ISO 27001

Europe

Amsterdam
ISO 27001 | ISO 22301
Dublin
ISO 9001 | ISO 27001

China

Shanghai
ISO 27001 | ISO 22301 | CNAS
Beijing
ISO 9001 | ISO 22301 | ISO 27001

Japan

Tokyo
ISO 27001 | SOC 1 TYPE II
Osaka
ISO 27001 | PCI DSS | SOC 2 TYPE II | SOC 3

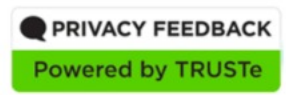
Cloud security and privacy

- Dedicated team assigned to run privacy programs, internal audits, and awareness training for employees
- All cloud services comply with industry standards to ensure data security and privacy
- Privacy and security certifications that ManageEngine's cloud offerings comply with:

Our compliance certifications

SOC 2

GDPR



TRUSTe

ManageEngine

Patch Manager Plus

Product overview

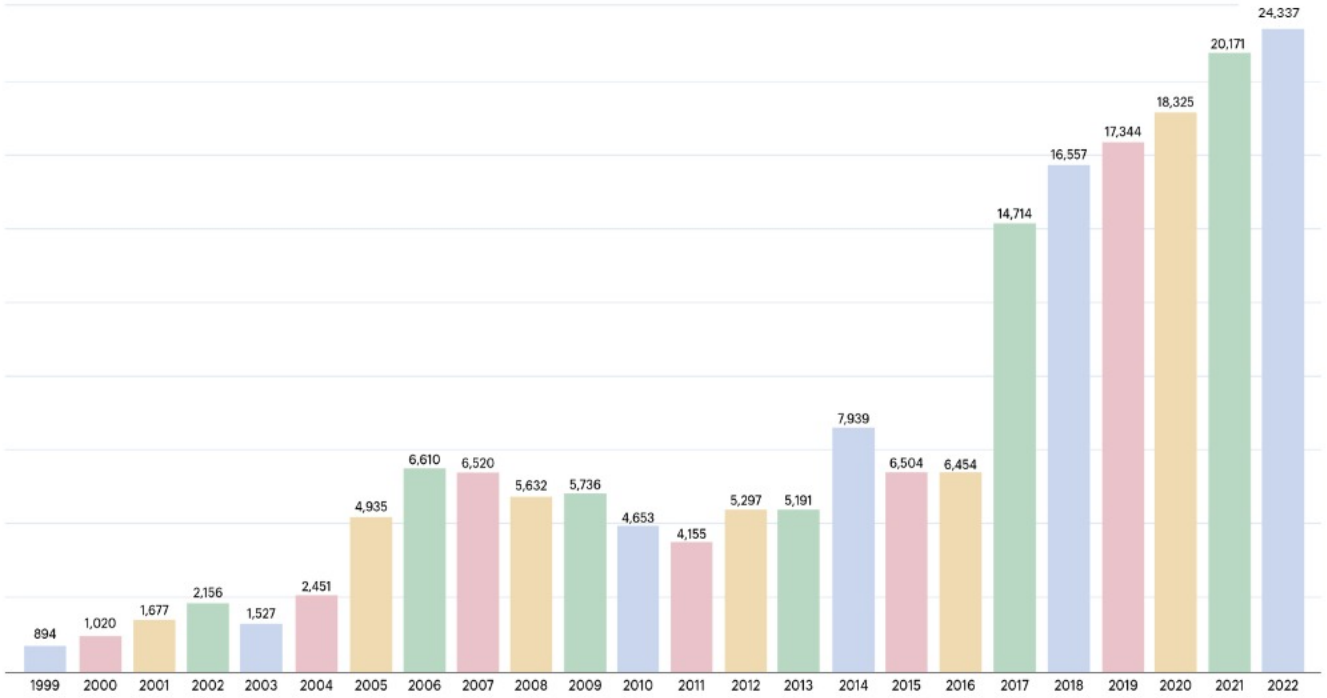
Why do you need to automate patch management?

Old disclosed vulnerabilities on unpatched systems are often the target of cyberattacks

Most of the common vulnerabilities targeted every year were publicly disclosed during the previous years

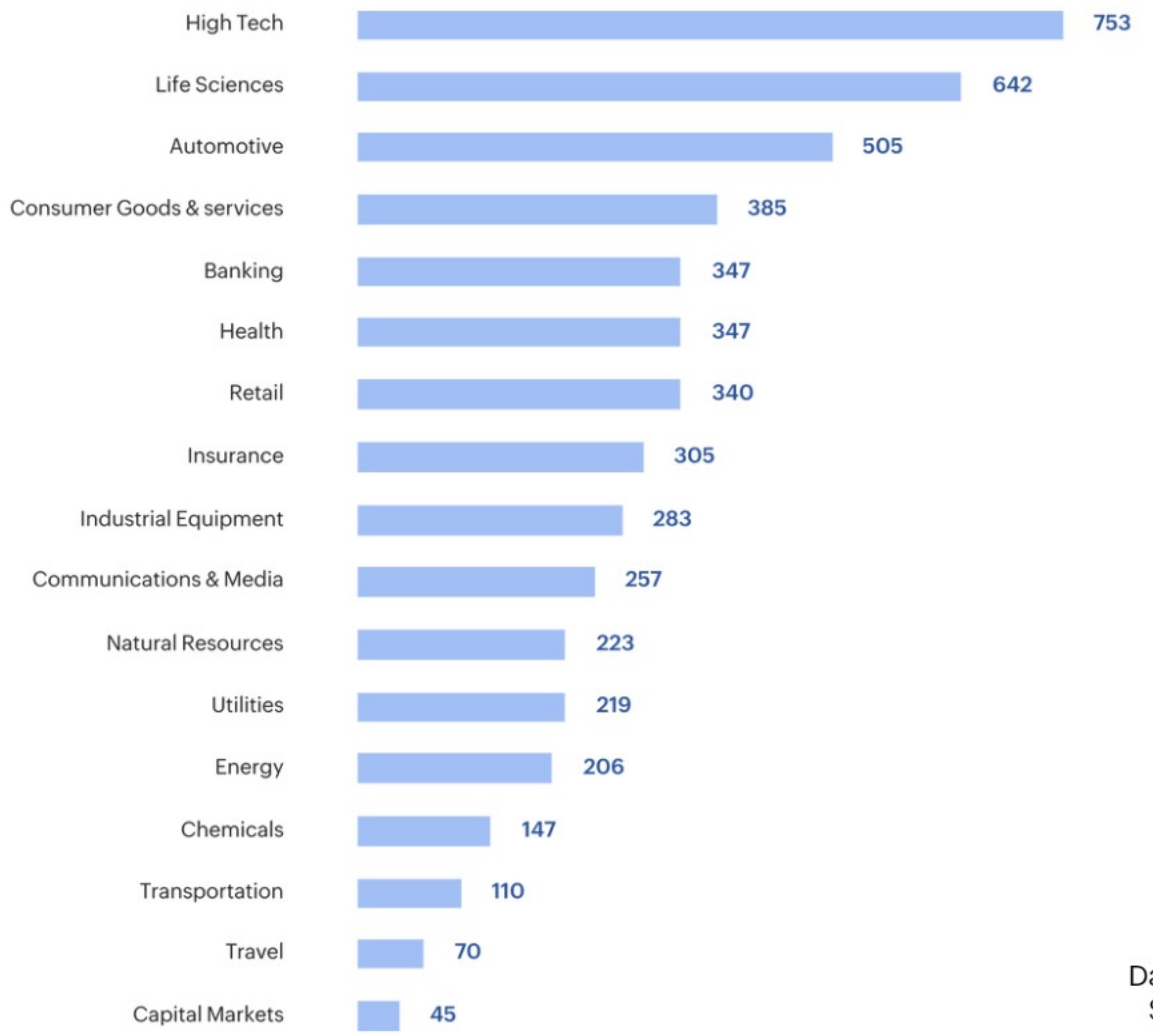
Reasons:

- The number of exploited vulnerabilities is constantly increasing
- A lack of time and resource to patch the ever-increasing number of endpoints in an enterprise



Vulnerability distribution by severity over time, 1999-2022 (Source: NIST)

Negligence in securing your endpoints could cost you greatly



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

Effective patch management = Revenue saved in dealing with cyberattacks

- On average, data breaches cost organizations $3.92 million
- According to a study by Ponemon Institute, 57% of data breaches are attributed to poor patch management

What's worse?

34% of breach victims knew that they were vulnerable before they were breached

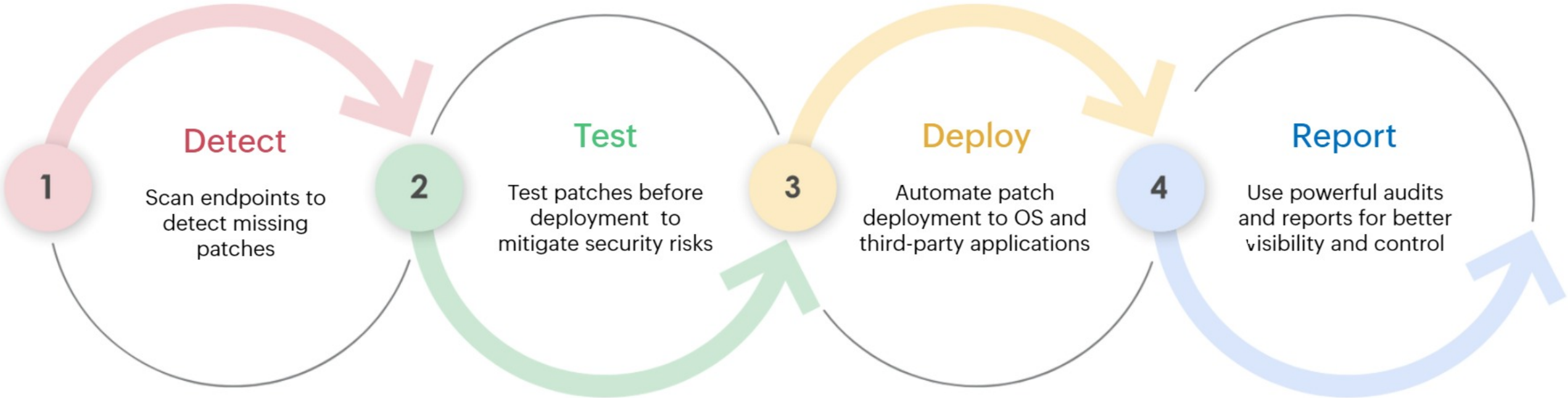
What is Patch Manager Plus?

A single solution for all your patching needs

- Patch Manager Plus provides a single interface from where you can completely automate all your patch management tasks across OS platforms like Windows, macOS, and Linux

- With Patch Manager Plus, you can patch over 1,000 applications, including more than 850 third-party applications, and a wide range of antivirus solutions, drivers, and BIOS

4 steps to taking control of your patching routine



Supports Windows, macOS, and Linux via cloud and on-premises

Highlighted features

- Automated patch management
- Cross-platform and heterogeneous endpoint support
- Flexible deployment policies
- Test and approve patches before bulk deployment
- Decline patches based on enterprise needs
- Reports and compliance audits

Patch Manager Plus features explained

Automated patch management

- Completely automate the entire process of patch management, right from synchronizing the vulnerability database to deploying the missing patches and providing periodic updates on patch deployment status

Benefits:

- Effective use of available time and resources
- Minimal human intervention reduces the possibility of errors in patching
- Helps achieve 100% compliance status
- Brings down the average time to patch, which is currently 102 days after patches are released

Cross-platform and heterogeneous endpoint support

- Deploy patches to over 1,000 applications across Windows, macOS, and Linux endpoints
- Patch 850+ third-party applications
- Secure a variety of endpoints, like laptops, servers, desktops, and workstations
- Deploy patches remotely and in bulk
- Patch roaming users and systems in closed networks, like demilitarized zones

Benefits:

- One solution to patch and secure your heterogeneous enterprise IT environments
- Perfect for current hybrid work environments

Flexible deployment policies

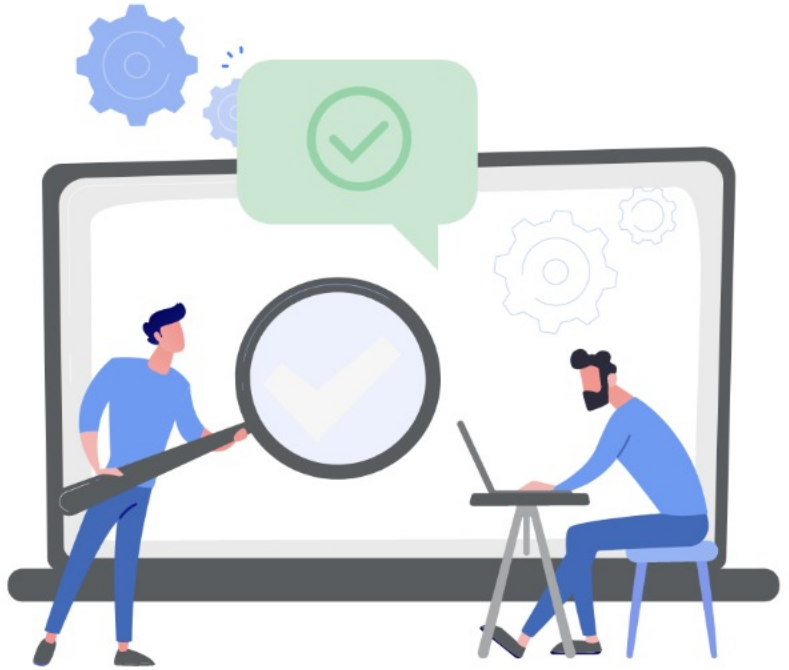
- Customize deployment policies to cater to all your individualized patching requirements
- Wake computers on LAN during non-business hours for patching and shut them down remotely after patching is done
- Create custom groups of machines and deploy to these groups with targeted deployment and patching
- Leverage the pre- and post-deployment settings to further streamline your patching and reboot process

Benefits:

- Completely control when you want your machines to be patched and how you want them rebooted
- Create scripts to perform unique and environment-specific pre- and post-deployment activities

Test and approve patches

- Test patches on a pilot group of systems before deploying them in bulk
- Decline patches that cause issues in the work environment during testing
- Configure the system health policy according to your enterprise needs to achieve a green state in patch management

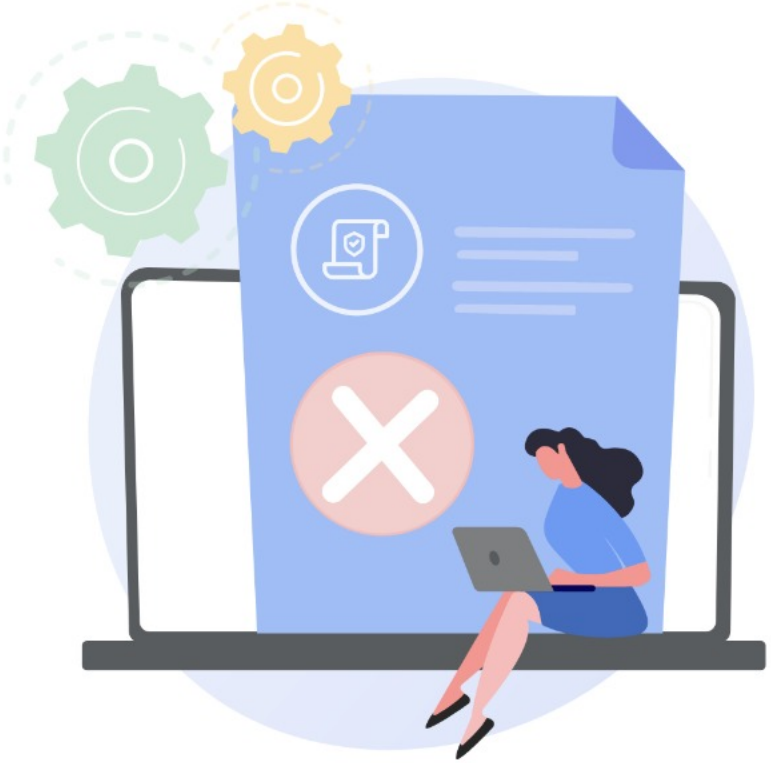


Benefits:

- Avoid environment-specific misbehavior due to patch-application incompatibilities
- Save time by automating the testing process

Decline patches

- Decline patches to specific groups of computers
- Prevent the deployment of patches found problematic during testing
- Decline updates based on patches, applications or families
- Delay the deployment of less critical patches by declining them initially

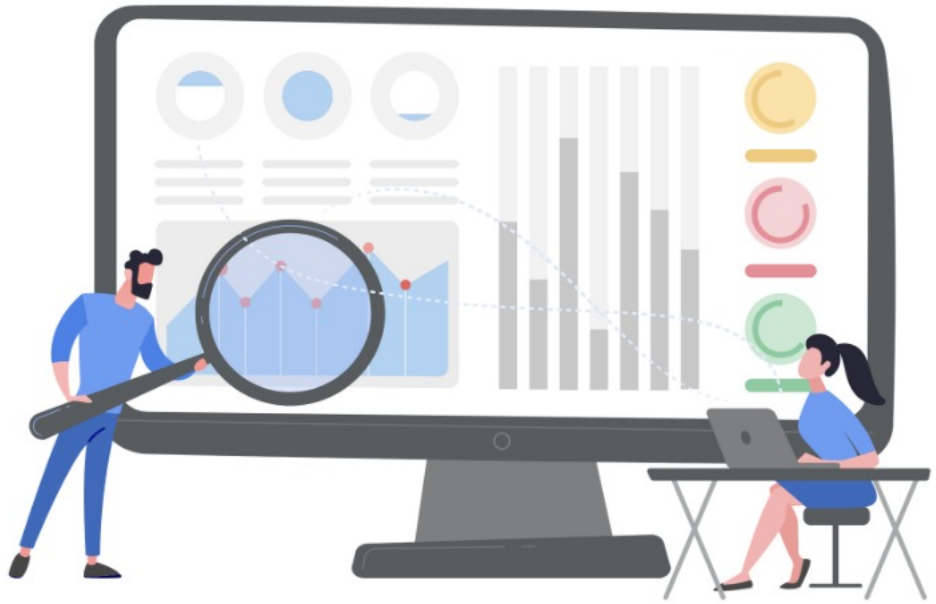


Benefits:

- Avoid legacy applications from getting updated automatically
- Declined patches won't affect the system health policy

Insightful reports

- Use predefined reports to help track the patching process
- Customize query reports
- Audit applications to ensure patch compliance
- Take advantage of at-a-glance patch summary dashboards



Benefits:

- Complete visibility into the entire patching process
- Detailed reports for all your auditing needs

How Patch Manager Plus benefits your organization

- Reduces the capital and effort spent on patch management
- Eliminates 90% of the time spent on patching
- Provides an integrated console
- Supports heterogeneous environments
- Delivers maximum endpoint security
- Flexible and easy to use
- Seamlessly handles remote patch management

To learn more, visit:

www.manageengine.com/patch-management

Try it for free!

www.patch.manageengine.com/free-trial.html

ManageEngine
IT Management, Simplified