You've patched more systems than ever this year.

You're still exposed like never before.

Automated Patch Management, Built to Scale



ManageEngine
Patch Manager Plus

Your patching program is broken.
We're here to fix it.

Complete visibility from Week 1 and live by Week 4. ***Here's why your team isn't already there →***

01

Runs lean

Full coverage without adding headcount.

02

Centralized console

Every OS, plus 1100+ third-party applications.

03

Fully automated

Detect, test, stage, and deploy automatically.

04

Audit-ready by default

Compliance evidence generated, not assembled.



Exploitation often begins before the patch even exists.



⚠ AI further shrinks the runway.

⚠ A single Patch Tuesday disclosed **974 vulnerabilities** at once, more than any team can manually triage.

*Source: 2026 Verizon DBIR, Mandiant M-Trends 2026

Where do organizations struggle?

01 **Pricing black box**

Some vendors require a sales call just to understand the cost.

02 **Third-party coverage gaps**

Browsers, Java, Adobe, Zoom, drivers. Most tools stop at the OS.

03 **Invisible endpoints**

Remote and hybrid devices often go unpatched and uncounted.

04 **Disconnected tools**

Separate systems for on-premises, cloud, and reporting that don't talk.

05 **Compliance scramble**

Audit prep means manually assembling evidence instead of pulling a report.



Now put this in numbers →

What this costs you today

6+ hrs

/ week
Per IT team spent on manual security patching.

Nearly a full workday, every week.

Source: IDC

$1 Million

Additional cost for AI-driven attacks, above the global average for malicious data breach costs.

Source: IBM 2026

$5-10k

/ month
Levied by card brands through acquiring banks for PCI DSS non-compliance.

PCI DSS Requirement 6.3.3 gives one month from release to install critical security patches.

Source: PCI DSS Guide

Higher insurance premiums

Patch management is a standard control and insurers underwrite on this specifically.

Vague answers also affect terms and whether claims are honored.

What we do for you

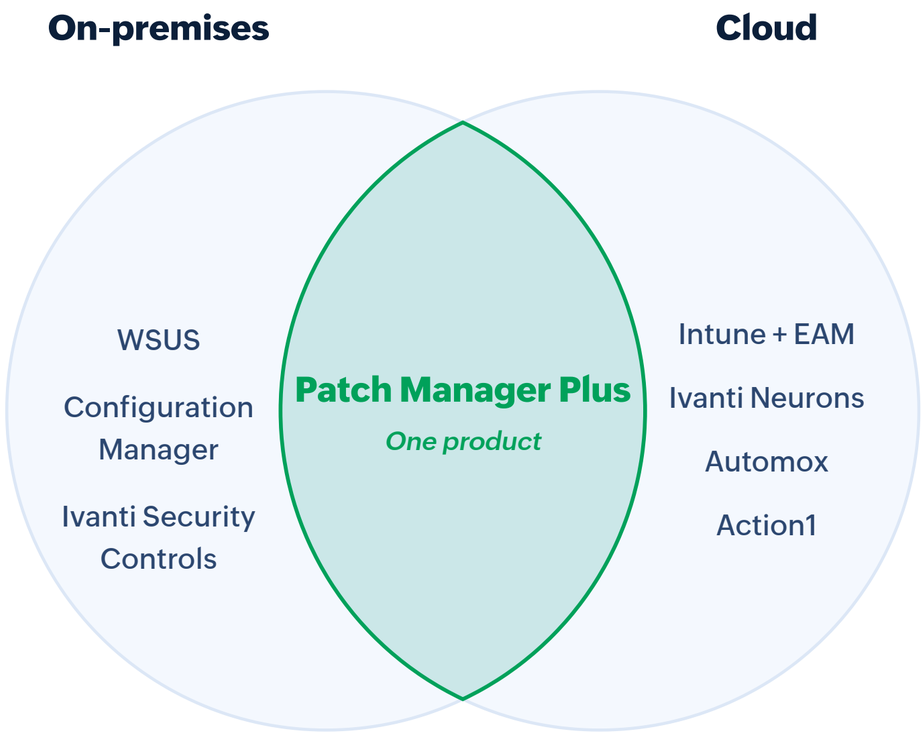
FOR YOUR IT TEAM

“We already have Intune / SCCM / WSUS”	WSUS is deprecated. SCCM and Intune leave a third-patching gap. Patch Manager Plus can work in tandem or replace them to close the gap.
“Won't automation risk an outage?”	Automation here means validation happens before deployment, not instead of it. Every patch is tested, staged, and reversible before it reaches production.
“Setup and agent rollout is a project in itself”	ManageEngine handles implementation, configuration, and training as part of onboarding. You don't have to worry about a DIY rollout.

FOR THE C-SUITE

“We have extensive compliance and audit needs”	Pre-built, audit-ready reports mapped to your framework—HIPAA, PCI DSS, SOX, GDPR, ISO 27001—no manual report-building required.
“Another agent expands our attack surface”	Patch Manager Plus is ISO 27001 and SOC 2 Type II certified, encrypted end-to-end, and least-privilege by design.
“We're concerned about tool sprawl”	Patch Manager Plus likely replaces two or three partial tools you're already stitching together, rather than adding a fourth.

Why Patch Manager Plus?



- Published, transparent pricing
- Highest verified third-party app coverage
- One product covering both deployment models
- Windows, macOS, and Linux in the same console
- Compliance-ready reporting out of the box
- Implementation support included

*Product names and deployment models from each vendor's current documentation, checked August 2026.

1 month average time to implement
12 months to ROI*

W1

Week 1

Discovery

Every endpoint detected and inventoried, including remote and roaming machines.

W2

Week 2

Baseline

Your 'before' number. The business case starts here.

W3

Week 3

Pilot

Validate safety and efficiency on a test group first.

W4

Week 4

Rollout

Staged expansion across the full fleet.

M2+

Month 2+

Steady state

The cycle runs itself. Your team only has to review exceptions.



Windows, macOS, Linux, and 1100+ third-party applications. On-premises or cloud, regardless of where the endpoint sits.

*Source: G2, averages based on real user reviews.

Pricing at a glance

FREE

No cost

Up to 20 workstations, 5 servers, and 1 technician

Best fit: a single department or IT team testing out automated patching with full capability.

PROFESSIONAL

$245/year

For 50 computers and 1 technician

Best fit: a single-site organization on one LAN, with a single tech or lean IT team.

TOP PICK

ENTERPRISE

$345/year

For 50 computers and 1 technician

Best fit: multi-site or remote workforces on a WAN. Same lean team, more infrastructure to cover.

ENTERPRISE

What Enterprise adds over Professional

- ✓ Automated test and approve
- ✓ Patch download scheduling
- ✓ Driver and BIOS updates
- ✓ Distribution server for bandwidth optimization
- ✓ Antivirus definition updates
- ✓ Scheduled remote shutdown and Wake-on-LAN

Add-ons available across all editions: failover server, secure gateway server, multi-language support. Cloud and on-premises deployment available. Servers and additional technicians licensed separately.

From leaders who've already made this call

> Our IT Security team automated vulnerability scan of servers and computers. They are reporting vulnerability details every week. Now, we must update servers and computers before vulnerability scan to take vulnerability score very low. This product helped us to automate patch deployments in our corporate network.

HI **Head of IT**

> We used to use WSUS which required constant fixing/uninstall/reinstall. It was a total waste of time. We installed Patch Manager Plus and once setup it found many patches which WSUS didn't find and updated them without an issue. Many other features as remote control was very nice. It has saved us with the ability to connect to servers when RDC would not connect.

CB **CIO, Banking**

> Overall experience was good from the purchasing process, cost, implementation, and configuration. It simply does what it was designed to do. Easy to install and configure. We purchased Patch Manager Plus to create internal/external efficiencies and improve our compliance and risk management.

ID **IT Director**



What's next? Let's talk.

RECOMMENDED

Demo

30 minutes, walked through against your environment and compliance requirements.

Best if you want to understand fit before moving forward.

Get Quote

Pricing for your endpoint count, technician count, edition and deployment model.

Best if you already know the direction and just need a number.

Free Trial

30 days, full functionality, on your own endpoints.

Best if you want internal buy-in before the budget conversation.

Your team just got hours back.
Ready to automate the entire stack?

Tell me more → | manageengine.com/patch-management

