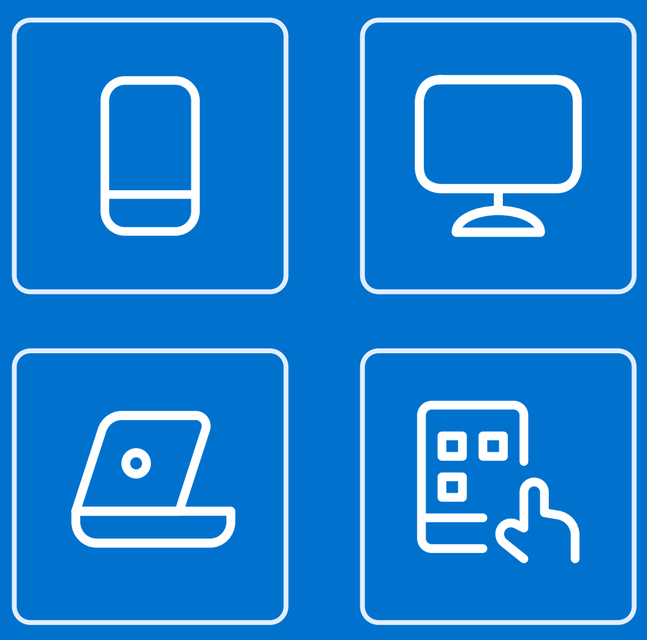
Smarter Endpoint Management for a Complex IT World

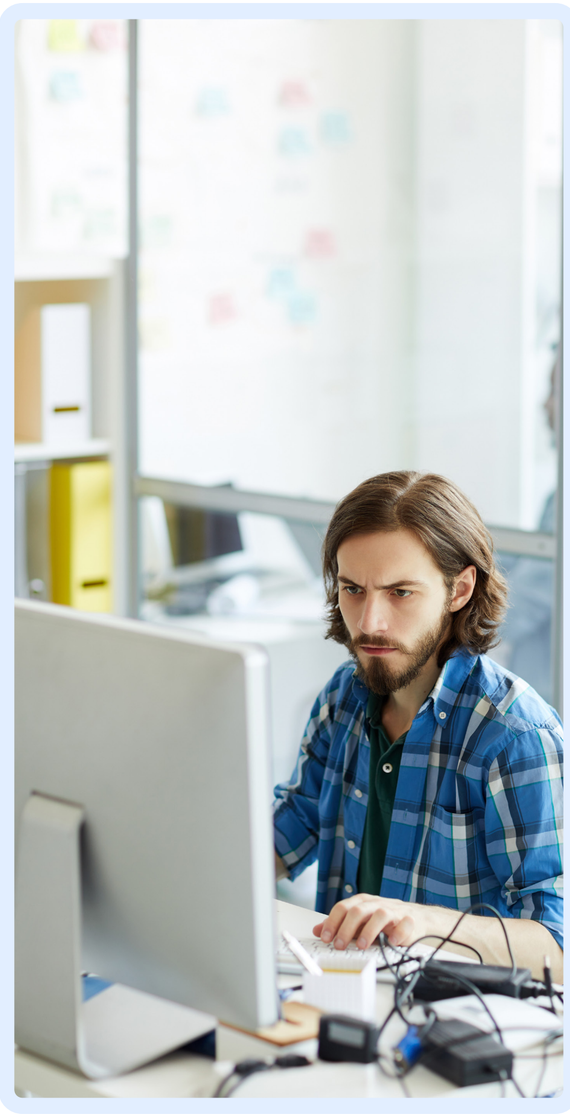
How automation, visibility, and security tools help IT teams stay ahead of risk and focus on what matters most.



splashtop®

Why Endpoint Management Must Evolve

For IT leaders, MSPs, and security-conscious organizations, managing endpoints has never been more urgent—or more complex. As many as 67% of organizations still rely on ad-hoc or manual processes for patching and software updates.[1]
But patching is only part of the challenge.



IT teams also struggle with:

- Incomplete visibility into hardware and software inventory
- Manual, repetitive tasks that eat away at limited resources
- Slow troubleshooting when remote users or hybrid teams run into issues
- Compliance pressures that demand audit-ready reporting
- Fragmented tools that create silos instead of efficiency

These pain points add up to greater security risk, operational inefficiency, and user frustration.

What IT needs now is a smarter approach that automates routine work, brings essential functions together, and gives teams the speed and confidence to act.

That approach is **Autonomous Endpoint Management (AEM)**. By combining patch automation, inventory, scripting, remote control, troubleshooting, alerts, remediation, and endpoint security into one unified platform, AEM enables IT to move from reactive firefighting to proactive, strategic enablement. In the pages ahead, we'll explore why traditional strategies are failing, how AEM changes the game, and what steps IT teams can take to begin the shift.

67%

of organizations still rely on ad-hoc or manual processes for patching and software updates.[1]

By 2028

50%

50% of midsize enterprises will not have implemented modernized ERP with AI capabilities, thus losing a competitive advantage.[2]

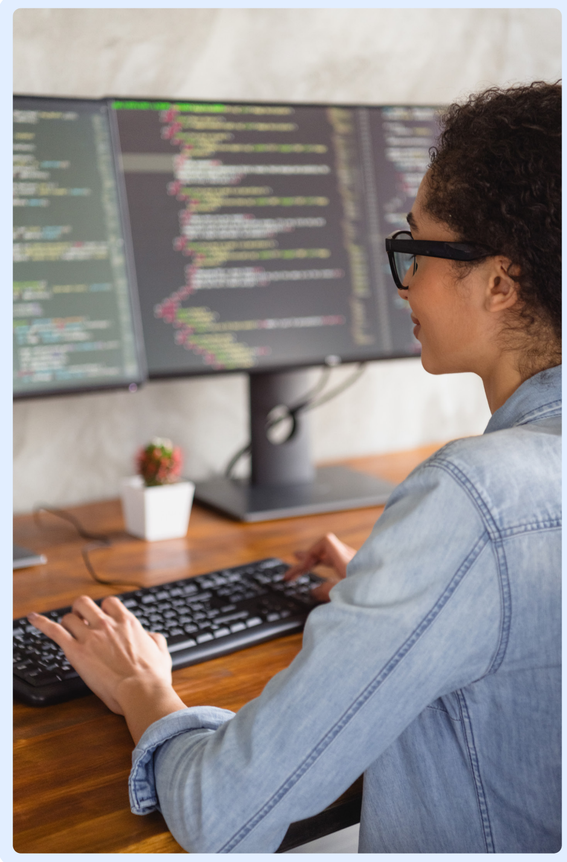
splashtop®

A New Model for IT: Autonomous Endpoint Management

The old model of IT operations, built on manual oversight, reactive support, and fragmented tooling, is no longer sustainable. As environments grow more complex, IT needs more than just additional tools. It needs a smarter framework.

AEM shifts IT from reactive management to automated, policy-driven systems that safeguard security, compliance, and performance while removing manual bottlenecks.

Gartner® predicts that by 2029, over 50% of organizations will adopt AEM capabilities within advanced endpoint management and DEX tools to significantly reduce human effort, an increase from nearly zero in 2024.[3] This rapid trajectory signals more than a trend—it marks a structural change in how IT environments will be managed in the coming years.



Over

50%

of organizations will adopt AEM capabilities within advanced endpoint management and DEX tools.[3]

The Role of AI in the Future of AEM

AI will increasingly shape the next generation of endpoint management and will be used to analyze endpoint data, optimize patch timing, and predict failures before they happen. These advancements are not yet widespread, but they represent the direction the industry is headed.

Robust AEM solutions already deliver the automation, visibility, and control that form the foundation for this evolution. By consolidating key capabilities into one platform, these solutions position IT teams to take advantage of AI-driven enhancements as they mature.

Beyond Patching: The Full Spectrum of AEM

While patch automation is a critical foundation, true AEM extends far beyond keeping systems up to date. A comprehensive AEM approach integrates multiple layers of capability, simplifying IT operations and reducing the risks created by fragmented or manual workflows.

splashtop®

Key features of a mature AEM model may include:

Cross-platform, real-time patching that closes the gap between operating systems and ensures critical updates are applied without long exposure windows to vulnerabilities.

Comprehensive inventory and visibility across hardware, software, and configurations, giving IT leaders confidence that no device or application is overlooked.

Policy-driven automation and scripting that standardize repetitive fixes, enforce security baselines, and scale responses across diverse environments.

Integrated remote troubleshooting tools that resolve issues quickly, particularly for hybrid or distributed workforces where delays are costly.

Proactive alerts and remediation workflows that detect anomalies early and trigger corrective action before disruptions occur.

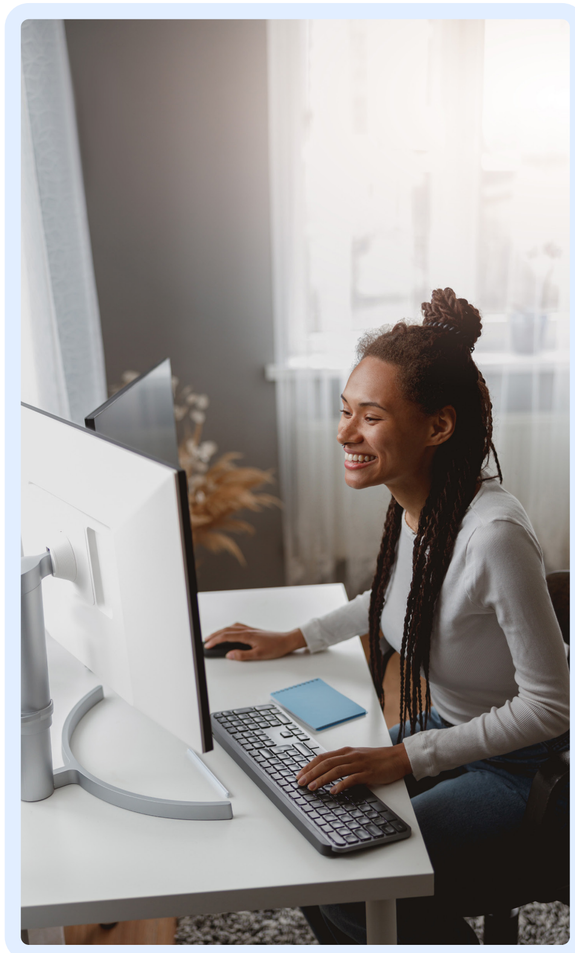
Centralized security and compliance management with dashboards surfacing critical vulnerabilities and prioritizing action needed, audit-ready reporting, and policy enforcement to meet regulatory or internal requirements.

Taken together, these capabilities illustrate how AEM can evolve from “just patching faster” into a unified framework that strengthens security, reduces operational complexity, and frees IT teams to focus on more strategic initiatives. While not every platform delivers all of these capabilities today, this spectrum represents the direction endpoint management is moving toward: consolidation, intelligence, and resilience.

splashtop®

The Benefits of Moving to Policy-Driven Automated Patching

AEM isn't just about faster patching. By consolidating multiple capabilities into one platform, AEM helps IT teams improve efficiency, strengthen security, and reduce the burden of manual processes. The result is more time for strategic work and less time spent firefighting.



Faster Patch Turnaround

Manual patching often introduces delays due to scheduling conflicts, testing bottlenecks, or resource limitations. With automation in place, teams can roll out critical updates much faster, minimizing the window of exposure to known vulnerabilities. Automation also allows IT teams to dramatically accelerate patch cycles.

IT professionals using Splashtop AEM report the same impact in their day-to-day operations. By simplifying installation, reducing repetitive manual tasks, and introducing new features for automated patch management, Splashtop makes it easier for small IT teams to stay on top of updates without sacrificing speed or quality. Gartner estimates that with Autonomous Endpoint Management, patching cycle times can improve from 55–94 days to 6–13 days.[4]

Gartner estimates that with Autonomous Endpoint Management, patching cycle times can improve from 55–94 days to 6–13 days.[4]

Complete Inventory Visibility

You can't protect what you can't see. Many IT teams struggle with incomplete visibility into hardware, software, and device configurations. AEM provides real-time inventory reporting across distributed environments, giving IT leaders a clear view of every endpoint. This visibility simplifies compliance, reduces blind spots, and ensures updates reach every device.

"[Splashtop] is simple to use, and I can quickly and easily handle multiple help requests at a time. Installing on my network was quick and painless. I use it every day, throughout the day. I also love the new features for endpoint management that allow me to keep up with patch management."

Rebecca C.
IT Liaison
Avery Eye Clinic

Automation and Scripting for Scale

Routine tasks like reboots, software updates, and configuration changes can overwhelm small IT teams. AEM enables policy-based automation and custom scripting, so teams can standardize responses to common issues and run fixes across hundreds of endpoints simultaneously. This reduces repetitive work and allows IT to focus on higher-value initiatives.

splashtop®

Faster Troubleshooting with Remote Control

When users run into problems, time is critical. Traditional troubleshooting often requires multiple touchpoints—or worse, waiting for on-site support. With AEM, IT teams can use remote control and integrated troubleshooting tools to diagnose and fix issues instantly, reducing downtime and improving user satisfaction.

Proactive Alerts and Remediation

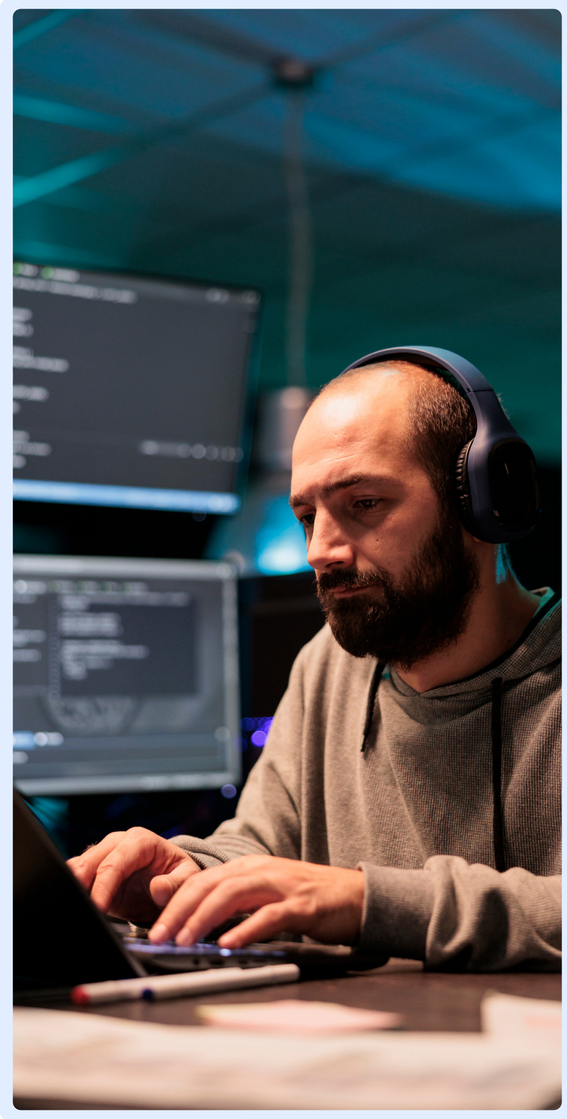
Most endpoint problems don't appear out of nowhere; they build up over time. AEM includes alerts and automated remediation workflows that allow IT to detect and respond to issues before they escalate. Whether it's a failed patch, a device running out of storage, or a service crash, automated responses keep systems running smoothly without requiring constant oversight.

Stronger Endpoint Security and Compliance

Distributed environments make it harder to enforce security standards consistently. AEM provides centralized controls that help IT enforce security policies, track vulnerabilities, and generate audit-ready reports. By combining patch automation with compliance visibility, IT leaders can reduce risk and demonstrate accountability with confidence.

The real power of AEM lies in how these capabilities work together. Instead of managing separate tools for patching, inventory, remote support, and compliance, AEM unifies everything into one platform. IT teams gain speed, visibility, and control, all while reducing complexity and cost.

For instance, organizations like pb2 Architecture + Engineering have seen the difference when replacing costly, complex tools with one unified platform that strengthens security, streamlines monitoring, and simplifies remote access.



"Where other solutions proved costly and lacked the user-friendliness and features required to support our growing hybrid workforce, Splashtop more than delivered with simplicity, excellent performance and a comprehensive feature set. From our designers who are securely remoting into their work computers, to our IT team who support devices, monitor systems and keep them compliant, Splashtop has provided unmatched value compared to alternatives."

pb2 Architecture + Engineering

splashtop®

Manual vs. Autonomous: A Workflow Comparison

Traditional endpoint management relies heavily on manual processes, fragmented tools, and reactive responses. AEM replaces these inefficiencies with real-time visibility, automation, and unified control.

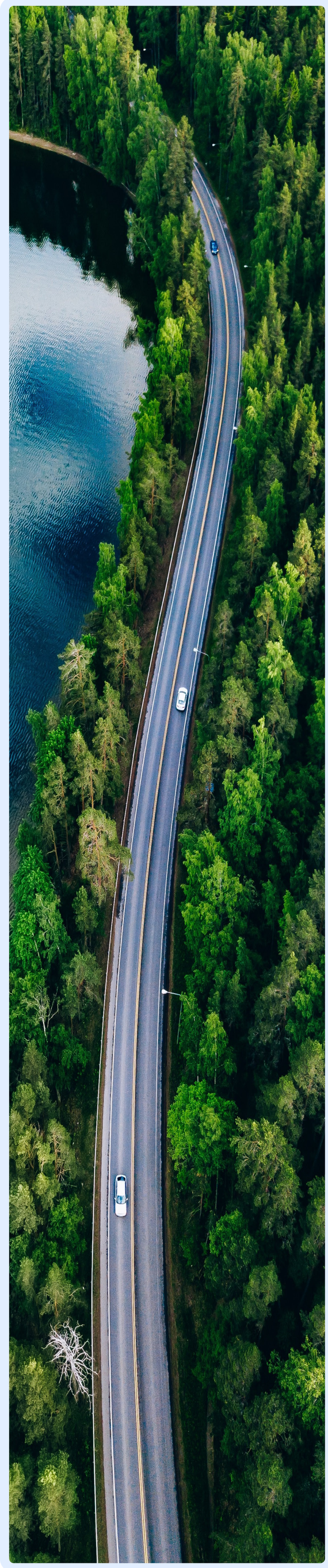
The table below highlights how the right AEM solution can transform everyday IT workflows:

Step	Manual Workflow	Autonomous Workflow (AEM)
Update Detection	IT manually checks for vendor updates or CVEs across OS and third-party apps.	The system automatically surfaces CVEs and detects available OS and app updates across all endpoints.
Remediation Planning	IT scripts fixes or creates custom deployment workflows from scratch.	Admins configure patching and remediation policies by device type, group, or severity level.
Testing	Limited manual testing on a few machines; often skipped due to time constraints.	Patches and scripts can be staged to designated device groups (e.g., pilot/test group first).
Deployment	Static schedule; often delayed due to approvals or resource constraints.	Scheduled or on-demand deployment and reboots triggered automatically by policy or admin approval.
Validation	Teams wait to hear about issues via helpdesk tickets or user complaints.	Deployment status, success rates, and error logs are reported in real time.
Remediation Adjustments	Manual rollback or patch removal if issues surface late.	Admins can stop, postpone, or reconfigure future deployments instantly based on outcomes.
Inventory Visibility	IT runs periodic audits, often incomplete or outdated.	Real-time hardware/software inventory ensures every endpoint is accounted for and up to date.
Scripting & Automation	Manual scripting required, run device by device; error-prone and time-consuming.	Policy-based automation and reusable scripts can be executed across hundreds of endpoints at once.
Troubleshooting	IT remotes into devices individually, often after long delays or escalations.	Integrated remote control and troubleshooting tools enable instant issue resolution from anywhere.
Alerts & Remediation	IT reacts only after an issue is reported by users.	Automated alerts flag issues early; remediation policies resolve common problems before users notice.
Security & Compliance	Compliance reports are compiled manually, taking days or weeks.	Centralized dashboards provide audit-ready reports, security policy enforcement, and CVE insights.

splashtop®

Roadmap for Building Toward an Autonomous Endpoint Future

Moving to AEM does not require an overnight transformation. Even if your team still relies heavily on manual processes today, you can modernize step by step. By layering in automation gradually, IT can reduce risk, build confidence, and prove value at every stage. Here's a practical roadmap to guide the journey:



1. Start with Visibility

Begin by auditing your current patching tools, schedules, and approval workflows. Identify where manual processes are introducing risks, delays, or blind spots.

Visibility also extends to inventory. This means knowing exactly what hardware and software are deployed across distributed environments and device types. A complete picture allows IT teams to better target updates, spot vulnerabilities, and prepare for compliance audits.

2. Set Operational Guardrails

Define clear criteria for when and how updates or fixes should be applied, whether by device type, severity level, or business impact. Establish approval steps or automation boundaries that align with your team's risk tolerance. For example, you might choose to allow automated patch deployment but require approval before scripts or configuration changes are rolled out.

3. Create Pilot Workflows

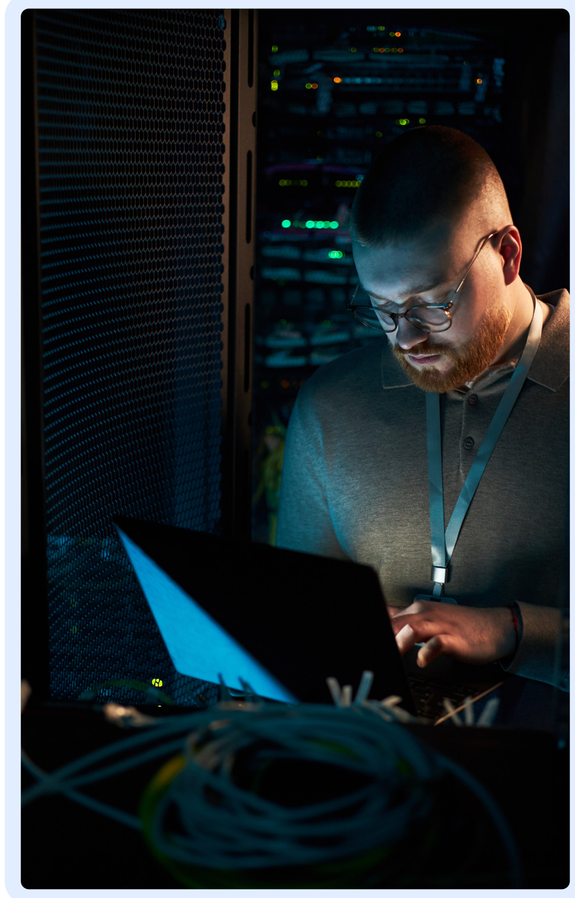
Start small by testing automation with a limited set of endpoints. For example:

- Deploying critical patches to a pilot group first
- Running a scripted fix across non-production machines
- Using alerts to track storage, CPU usage, or service crashes

Pilot workflows allow IT to validate stability, measure outcomes, and build trust in automation.

splashtop®

4. Monitor Outcomes in Real Time



Replace reliance on helpdesk tickets with dashboard-level visibility. Track update success rates, script execution, and device health in real time. Alerts can notify you when systems fall out of compliance or when a remediation policy has been triggered.

This feedback loop gives IT confidence that automation is working as intended and provides data for continuous improvement.

5. Expand with Confidence

Once pilot workflows prove effective, scale your automation policies to more endpoints, departments, or geographies. Adjust timing, frequency, or automation levels based on results and team capacity.

At this stage, scripting and automation can help standardize fixes across large fleets, while remote troubleshooting tools provide fast support for distributed users.

6. Build Beyond Patching

The ultimate goal is to move from patch automation to full-spectrum AEM. This means extending automation into:

- Configuration management
- Remote remediation and troubleshooting
- Policy enforcement through scripting
- Automated alerts and proactive remediation
- Security monitoring and compliance reporting

With patching as the foundation, IT teams can expand into a unified model where visibility, automation, troubleshooting, and security work together seamlessly.

Why This Roadmap Works

By breaking the journey into manageable steps, IT teams avoid the pitfalls of big bang change. Instead, they build trust in automation gradually while delivering measurable improvements at each phase.

splashtop®

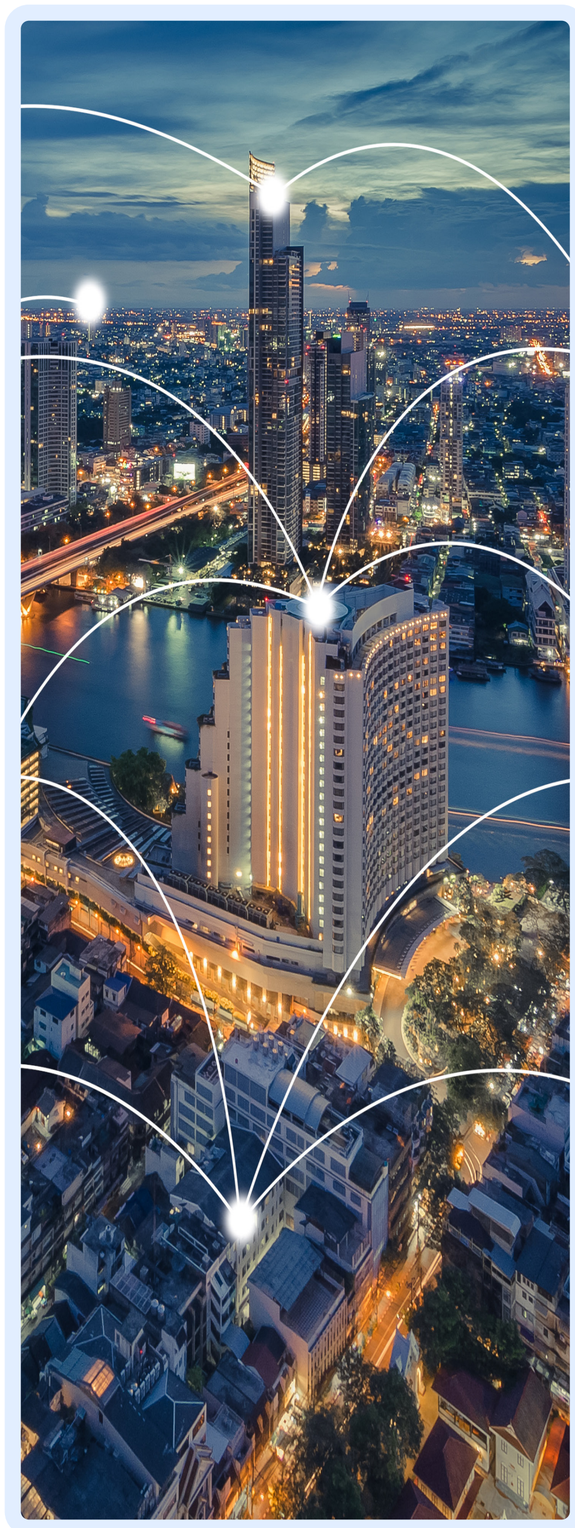
From Reactive to Autonomous

The pace of IT operations is accelerating, and manual patching with fragmented endpoint strategies can no longer keep up. AEM offers a smarter path forward by replacing reactive workflows with automated, policy-driven systems that reduce risk, improve reliability, and elevate IT's strategic impact by transforming IT from a reactive support function into a proactive enabler of business success.

Unlike traditional tools that leave gaps or delays, Splashtop AEM delivers real-time patching across Windows and macOS, policy-based automation that adapts to changing conditions, and compliance-ready reporting that closes the audit gap. The result is a unified solution that simplifies compliance, strengthens security, and accelerates resolution—without the inefficiencies of juggling multiple tools.

Show your team how Splashtop AEM can close gaps and automate patching in real time.

Book Your Live Demo



Sources

1. Splashtop, Endpoint Management Survey, 2025.
2. Gartner, Predicts 2026: Strategic Predictions for Midsize Enterprise CIOs, Alexander Buschek, Joseph Provenza, Paul Furtado, Vikram Siddharth, 16 October 2025
3. Gartner, Gartner Market Guide for Endpoint Management Tools, Tom Cipolla, Lina Al Dana, Sunil Kumar, 13 January 2025.
4. Gartner, Innovation Insight: Autonomous Endpoint Management, Tom Cipolla, Dan Wilson, 15 January 2025.

Disclosures

splashtop®