

ACTION  
GUIDE

# **The Guide for IT Admins: Work Smarter Instead of Doing Everything Yourself**

## More endpoints. The same number of hands.

Device fleets are growing — driven by remote work, BYOD, new locations, and increasing employee numbers. But IT teams are staying the same size. That means **every admin is responsible for more endpoints than ever before, under greater pressure and with the same resources.**

This action guide outlines five practical levers IT teams can use to keep growing infrastructure manageable — without adding headcount and without compromising security or stability.

- **76%** of companies report an IT/tech talent shortage.<sup>1</sup>
- **87%** of technology leaders struggle to find qualified candidates.<sup>2</sup>
- **More than 50%** of organizations will use AEM capabilities in advanced endpoint management and DEX tools by 2029.<sup>3</sup>

<sup>1</sup>Der Spiegel (2023) | Fachkräftemangel im IT-Sektor erreicht Rekordhoch

<sup>2</sup>Robert Half Inc.(2025) | Robert Half Research Reveals Key Priorities and Challenges Facing Today's Technology Leaders

<sup>3</sup>Gartner, Inc. (2025) | Market Guide for Endpoint Management Tools

## Lever 01: Maintain Full Visibility — Across Every Device, Everywhere

Scaling starts with visibility. If you don't know how many devices are active on the network, which ones are outdated, or which are running without a management agent, you can't scale efficiently — no matter how strong your team is.

As the number of devices grows, complexity increases significantly. Remote devices, cloud workloads, field-service laptops, and hybrid environments all need to be identified, assessed, and managed. Centralized endpoint monitoring creates the foundation for managing significantly more devices with a comparable level of effort.

### **The problem**

Distributed device fleets with remote devices and cloud workloads create blind spots — admins can't manage what they can't see.

### **The lever**

Centralized real-time monitoring of all endpoints — regardless of location, operating system, or connection type — provides an immediate basis for action.

### **Why visibility scales**

An admin with complete endpoint visibility can manage significantly more devices efficiently because the system automatically prioritizes anomalies, outdated software, and risks. Without visibility, manual effort increases with every additional device type and every new location.

**What complete visibility delivers in practice:**

- Comprehensive inventory of all endpoints — physical, virtual, mobile, and remote
- Immediate detection of unmanaged or outdated devices on the network
- Transparency into software licenses and actual usage as a basis for more targeted investments
- Network analysis for early identification of connectivity issues
- The foundation for all other scaling levers

## Lever 02: Problems Don't Scale — If You Solve Them Early Enough

Reactive IT management is a resource drain: every ticket, every outage, every escalation consumes time that becomes increasingly scarce as infrastructure grows. Teams that operate proactively can manage the same number of devices with significantly less effort.

**Reactive IT – The cost**

Downtime costs companies money, time, and reputation. Even short outages can severely disrupt operational processes and rapidly increase ticket volumes.

**Proactive IT – The advantage**

Proactive management identifies issues before they escalate — through continuous monitoring, automated anomaly detection, and prioritized recommendations for action. The result: fewer tickets, fewer outages, and more time for strategic work.

**Proactive measures with a direct scaling effect:**

- Continuous AI-powered monitoring automatically detects anomalies — no manual polling required
- Endpoint Risk Analytics prioritizes risks by criticality — no manual sorting through large alert lists
- Guided workflows walk teams through remediation steps — even as device counts grow, processes remain consistent
- Automated incident detection reduces unnecessary escalations

## Lever 03: Automation — The Co-Admin That Never Takes Vacation

Anyone who wants to scale without hiring must remove repetitive tasks from the manual queue. Automation is not a convenience feature — it's a realistic response to growing endpoint numbers with a constant headcount.

Patch management, software rollouts, compliance checks, reporting — all of these can be automated without sacrificing control. The key difference: meaningful automation provides full transparency into every executed action and allows admins to intervene at any time.

- **USD 1.76 million** in average savings through security AI and automation, according to IBM 2024.<sup>4</sup>
- **Up to 40%** lower ticket volumes through automation.<sup>5</sup>
- **Up to 30%** faster resolution times and lower operational costs through automation.<sup>6</sup>

<sup>4</sup>Security Insider (2024) | Datenlecks verursachen neue Rekordschäden

<sup>5</sup>baramundi software GmbH (2026) | Referenz Schnaithmann

<sup>6</sup>Gartner, Inc. (2025) | Gartner Predicts Agentic AI Will Autonomously Resolve 80% of Common Customer Service Issues Without Human Intervention by 2029

## The principle: Automation as a multiplier

Automation doesn't just improve an admin's efficiency — it multiplies it. What a team can manually achieve for a few dozen devices can be extended to much larger fleets through automation, without effort increasing at the same rate.

### Automation areas with the greatest scaling impact:

- **Patch management:** Automated deployment and prioritization of updates based on criticality — across all devices simultaneously
- **Software rollouts:** Standardized deployments without manual individual installations
- **Compliance monitoring:** Continuous verification of all endpoints against defined policies
- **Reporting:** Automatically generated reports — no more manual compilation

## Lever 04: The Right Tools — Focus Instead of Feature Overload

Many companies suffer from tool sprawl: dozens of standalone solutions for monitoring, patching, security, inventory management, and reporting that integrate poorly and create more effort than they save.

The opposite of complexity is not simplicity — it's focus. The best tools for IT teams are not feature monsters, but platforms that do exactly what teams need every day: reliably, quickly, and without a steep learning curve.

On top of that comes budget pressure: many IT teams today must work with limited resources and don't want to pay for expensive enterprise suites whose full feature sets they never actually use. That's why time-to-value, transparency, and clearly defined use cases matter more than maximum feature depth.

### **What slows IT teams down**

- Too many specialized tools without integration
- High licensing costs for unused features
- Long onboarding and training times
- Fragmented data without a unified dashboard

### **What IT teams need**

- A consolidated platform with a clear focus
- Fast time-to-value
- Intuitive usability
- A cloud-native architecture that is quickly ready to use without complex infrastructure

### **The principle:**

#### **Everything you need. Nothing you don't.**

Modern endpoint management platforms should be browser-based, instantly ready to use without complex installation processes, and focused on the functions that truly matter in the day-to-day work of modern IT teams. Less overengineering, more focus.

### Checklist: What Matters When Choosing a Tool

☑ **Fast time-to-value**

Is the tool ready to use immediately, without weeks-long implementation projects?

☑ **Consolidation**

Does it replace multiple standalone tools — or just add another one?

☑ **Intuitive usability**

Can new team members become productive quickly without days of training?

☑ **Scalability**

Does the tool scale with the number of devices without increasing costs exponentially?

☑ **Transparent pricing**

Are the licensing model and feature scope clear and aligned with actual needs?

## Lever 05: AI-Powered Decision-Making — Less Guessing, More Action

Artificial intelligence is no longer a future topic in IT management — it is already delivering practical value today. The benefit doesn't lie in flashy AI demos, but in everyday operations: better prioritization, faster diagnosis, and clear recommendations for action.

The real value of AI in endpoint management lies in connecting data with action. Analyzing raw data from thousands of endpoints overwhelms any human admin. AI systems can process these massive amounts of data in real time — and derive concrete, prioritized action steps from them.

## Gartner forecast on Autonomous Endpoint Management

By 2029, more than 50% of organizations will rely on Autonomous Endpoint Management (AEM) capabilities — up from nearly zero percent in 2024. Gartner describes AEM as “the most significant advancement in endpoint management in more than a decade”.

*Source: Gartner, Market Guide for Endpoint Management Tools, Tom Cipolla et al., January 2025*

### What AI can specifically deliver in endpoint management:

- **Anomaly detection:** AI identifies unusual device behavior patterns earlier than any manual check
- **Prioritization:** Not every alert is equally critical — AI scoring helps teams address the most important issues first
- **Action recommendations:** Instead of raw data, the system provides concrete next steps — even for less experienced admins
- **Predictive maintenance:** Device issues are identified before they result in failures
- **User context:** Combining telemetry data with end-user feedback creates a complete picture of the actual situation

### Important: AI as support — not replacement

Well-designed AI systems in IT management actively support admins — they do not replace them. The tool “thinks along” and provides recommendations, but the admin always remains in control of the final decision. Intelligence lives in the tool, decision-making power stays with people.



Experience It in Practice Now

## All 5 levers in a single platform

The **baramundi Proactive Hub** combines endpoint analytics, AI-powered insights, automated patch management, and guided workflows in a cloud-native platform. Browser-based, instantly ready to use — and built on more than 25 years of endpoint management experience.

- Complete real-time endpoint visibility — with no installation effort
- AI-powered analytics with concrete action points — not just raw data
- Proactive monitoring and Endpoint Risk Analytics
- Automated software and patch management
- Intuitive to use — valuable immediately, even without deep expertise
- Scales with the number of devices — not with headcount

Try it free for 3 months

## Any questions?

**Feel free to make an appointment with us.**

In a personal meeting, we will explain how baramundi software can help you achieve greater digital independence with its unified endpoint management solution.



### **About baramundi software GmbH**

baramundi software develops unified endpoint management for the central administration of PCs, mobile devices, and servers. It automates software distribution, simplifies patch management, and creates transparency in the network. baramundi thus makes a significant contribution to IT security and frees up resources.



## CONTACT US

+49 821 5 67 08 - 380  
request@baramundi.com  
www.baramundi.com



**baramundi software GmbH**  
Forschungsallee 3  
86159 Augsburg

+ 43 19 28 01 36 00 10  
request@baramundi.com  
www.baramundi.com



+41 77 280 49 79  
request@baramundi.com  
www.baramundi.com



+39 340 8861886  
request-italia@baramundi.com  
www.baramundi.com



+48 735 91 44 54  
request@baramundi.com  
www.baramundi.com



+44 2071 93 28 77  
request@baramundi.com  
www.baramundi.com



+1 508-861-7561  
requestUSA@baramundi.com  
www.baramundi.com



**baramundi software USA, Inc.**  
30 Speen St, Suite 501  
Framingham, MA 01701, USA

+49 821 5 67 08 - 390  
request@baramundi.com  
www.baramundi.com

