Kaseya 365
Endpoint

EBOOK

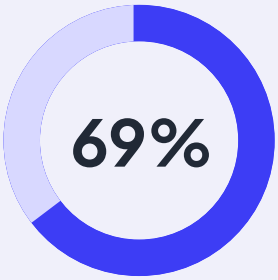
Work smarter: The IT pro's shortcut to efficiency

Fragmented tools: The quiet thief of time

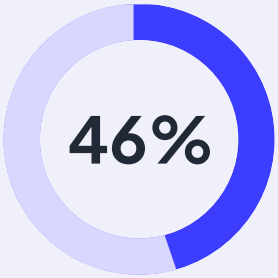
Every time you switch platforms, re-enter data or go digging for details that should have been at your fingertips, you lose precious minutes that soon turn into hours. It's estimated that **15% to 25% of an IT professional's day** is spent just navigating between fragmented systems — patching in one tool, endpoint monitoring in another and ticketing in a third. There's no straight line from issue to resolution.

Over time, this disconnect becomes a steady drain on your time, energy and resources. What starts as a small inefficiency turns into late nights, missed weekends and a quiet erosion of personal time, all in the name of staying afloat. It doesn't just hinder productivity — it slowly wears people down.

According to the **2024 Future of IT Survey Report,**



of IT professionals have worked through holidays or weekends, and



reported having pulled all-nighters to keep up.

These aren't isolated incidents — they are warning signs of a deeper issue. That's why **unifying toolsets and automating repeatable work** is critical to building an IT operation that works for the people running it.

What fragmented tools look like in real life

Here's a look at common IT challenges caused by disconnected systems, and the time and effort they waste:

Duplicate work across platforms

You patch a system in one tool but manually update it in another.

Incomplete visibility

Different tools track different data, and nothing gives you the full picture.

Slower response times

Alerts come from one system, but the resolution happens in another.

Inconsistent policies and settings

Security, patching and monitoring settings vary between tools, making compliance difficult.

Constant firefighting

Your team stays reactive because monitoring, patching and security aren't in sync.

High security risk

Missed alerts, unpatched devices and shadow IT slip through the cracks when tools aren't connected.

Poor reporting and analytics

Pulling reports from disconnected tools takes time, doesn't tell the full story and hinders decision-making.

Lackluster automation

Disjointed workflows and poor automation lead to more manual work.

Wasted time and budget

Overlapping licenses and tool fatigue waste time and money without better results.

Practical fixes that pay off fast

IT teams waste about **eight hours a week** tracking down issues across disconnected tools. The best way to reclaim your time is by removing the friction that slows you down in the first place. That starts with smarter systems and fewer silos. Here are practical ways to simplify your setup and save hours each week:

If you can do only one thing, conduct a system audit to identify redundancies and gaps to determine what to prioritize.

1

Start with a system audit

Map out all the tools you use for patching, monitoring, antivirus (AV), backup and ticketing. Identify which ones overlap, lack integration or require duplicate steps.

2

Consolidate overlapping tools

If two tools do 80% of the same thing, ask yourself if you really need both. Look for solutions that combine multiple functions, such as patching, AV, backup and automation, within one interface.

3

Automate where it makes the most impact

Start with high-volume, low-complexity tasks like patching, password resets and software updates. These are often the first to be repeated and the easiest to automate.

4

Document and templatize everything

Turn repeatable tasks into templates and SOPs (standard operating procedures) so nothing starts from scratch. This reduces mistakes and saves time during handoffs.

Why IT teams need to embrace automation

If juggling disconnected tools slows things down, doing everything manually only makes it worse. Fragmented systems are already eating up time, but when every task also needs to be done by hand, the workday becomes a series of repeat steps that never seem to end.

Automation is not only the biggest time saver but also allows for speed and consistency at scale. The **2024 Future of IT Survey Report** found that **40% of organizations are prioritizing investments in automation, while another 37% are investing in AI and machine learning**, recognizing the long-term value of letting technology handle what no longer needs to be manual.

Whether it's patching, backups, software installs or ticket creation, **automating the most repeated tasks** helps IT teams regain time, reduce stress and shift from constantly reacting to improving how things run.

6 automations that save you the most time

Here are six tasks you can automate to make your work easier and more efficient:

01 Automate patch deployment

Set up policy-based patching to scan, approve and deploy updates automatically. No more switching tools or missing critical fixes.

Why it matters: Keeps every device secure and up to date without the manual work.

02 Software deployment by device group

Automatically send apps to specific device groups, like HR or engineering, instead of installing them one by one.

Why it matters: Saves time and ensures every department gets exactly what it needs, fast.

03 Auto-ticket creation from monitoring alerts

Connect your monitoring and ticketing tools so alerts trigger tickets with key details already filled in.

Why it matters: Eliminates manual entry and helps your team respond faster.

04 Automated threat detection and response

Use EDR tools to automatically detect suspicious behavior, isolate affected devices and trigger alerts or remediation steps.

Why it matters: Stops threats early and reduces response time even if no one's watching the dashboard.

05 Scheduled backups with automatic verification

Run backups on a schedule and include auto-checks like file tests or screenshots to confirm success.

Why it matters: Confirms backups are working without manual checks, so you're always ready to restore.

06 Self-service password reset

Let users reset their passwords securely from a login screen or portal without contacting IT.

Why it matters: Reduces ticket volume and gets users back to work faster.

The value of a unified endpoint management system

A **unified endpoint management system** brings all your critical IT functions into one place, so you can respond faster, reduce manual work and gain full visibility without switching between tools. Instead of spending your day connecting the dots, you're free to focus on what actually moves things forward.

A complete endpoint management solution gives you:

Full visibility

See device health, patch status and backup activity in one dashboard — no flipping through tabs.

Real-time response

If an endpoint goes offline, get alerted instantly and auto-create a ticket without lifting a finger.

Unified security

Protect every endpoint with consistent, layered defenses — antivirus, EDR, backup and patching — all managed from one platform. No blind spots. No loose ends.

Easy scalability

Add 50 devices and apply policies in minutes — no extra setup or tools needed.

Built-in automation

Automate repetitive tasks like patching, ticket creation and software installs to save hours every week.

Fewer platforms, lower costs

Replace five tools with one and cut down on licenses, vendor calls and training time.

Your fix-it checklist for disconnected IT

Once you have a unified endpoint management platform in place, it becomes much easier to fix the common problems caused by disconnected systems.

Duplicate work across platforms

- [ ] Standardize patching, backup and software deployment under one unified tool.

Incomplete visibility

- [ ] Use a single dashboard to view endpoint health, backup status and security coverage.

Slower response times

- [ ] Automate alert-to-ticket workflows to avoid delays in resolving issues.

Inconsistent policies and settings

- [ ] Apply universal policies across all devices from a central platform.

Constant firefighting

- [ ] Enable real-time monitoring and scheduled patching to prevent common issues.

High-security risk

- [ ] Unify AV, EDR and patch management to close gaps and catch threats early.

Poor reporting and analytics

- [ ] Generate reports from one platform that include security, backup and device status.

Difficult automation

- [ ] Use built-in, no-code automation tools to streamline repetitive tasks.

Wasted time and budget

- [ ] Eliminate redundant tools and consolidate licensing into one cost-effective platform.

The all-in-one platform that actually is

If there's a solution that truly delivers unified IT management, it's **Kaseya 365 Endpoint**. This platform brings together monitoring, backup, security and automation in one place. With Kaseya 365 Endpoint, you skip the whole integration headache and go straight to a lean, efficient setup.

Starting at just a few dollars per month, you're not just improving productivity, you're boosting profitability as well.

RMM at the core

At the heart of Kaseya 365 Endpoint is powerful remote monitoring and management (RMM) solutions. You can choose between Datto RMM or VSA 10, both tightly integrated with advanced AV, EDR and backup solutions.

It's not just RMM, but RMM connected to everything you need. You can automate entire workflows, from patching to threat response, using a built-in library of 20 **automation groups** and countless pre-built routines. The result? Up to a 75% boost in efficiency.

What you get with Kaseya 365 Endpoint

It's a system that grows with you and makes the everyday parts of IT easier to manage.

RMM

Monitor, manage and automate all your endpoints from a single platform.

AV/AM

Protect every device with built-in AV that runs in the background and blocks known threats before they spread.

EDR

Detect suspicious behavior, isolate affected systems, and respond fast without manual intervention.

DNS filtering

Block access to harmful or unauthorized websites at the network level to prevent risky activity before it starts.

Ransomware detection

Spot early signs of ransomware attacks and shut them down before they cause damage.

Endpoint rollback

Quickly restore infected or broken endpoints to a previous healthy state with minimal disruption.

Advanced software management

Deploy, patch, and manage software across devices automatically. No more one-by-one installs.

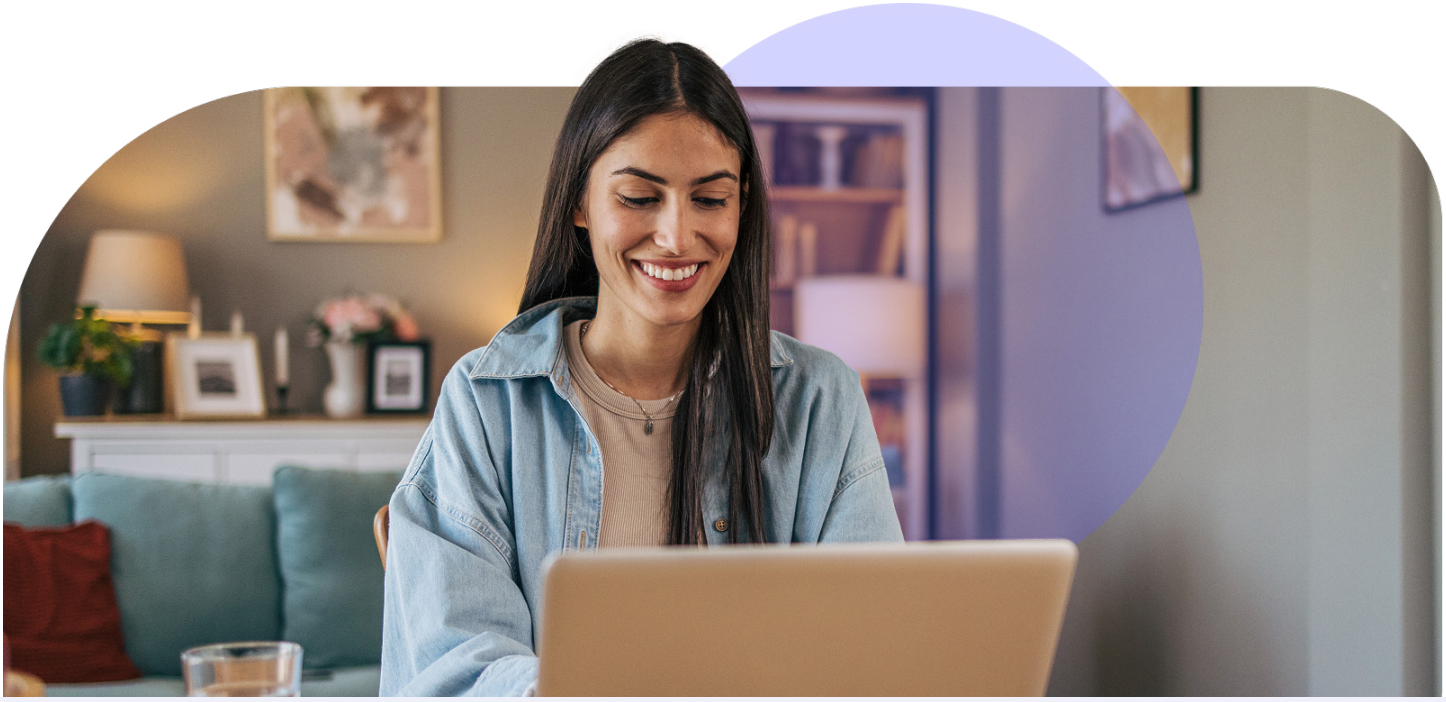
Endpoint backup

Schedule reliable backups with built-in verification so you know your data is protected and restorable.

Here’s what comes next

We’ve explored the real problems caused by fragmented IT tools — from wasted time and inconsistent policies to security gaps and reactive firefighting. We’ve also shown you how to fix them with practical strategies, smart automations and a leaner approach to managing your environment.

If you’re looking for a way to put these solutions into action without stitching together different platforms, it’s time to see what Kaseya 365 Endpoint can do. With powerful RMM at the core, it helps you streamline operations, reduce costs and keep your systems running and your business growing.



See how easy unified IT can be.

Book a demo

Kaseya®

©2025 Kaseya Limited. All rights reserved. Kaseya and the Kaseya logo are among the trademarks or registered trademarks owned by or licensed to Kaseya Limited. All other marks are the property of their respective owners.