Kaseya 365
Endpoint

EBOOK

The MSP guide to reducing endpoint tool sprawl

Table of contents

Introduction

Every MSP wants to grow, but it's hard to move forward when your tools keep pulling you back. You might have one system for monitoring, another for security and a third for backup, which means you're constantly switching between them to keep everything in sync.

You probably hesitate to take on new clients because your team is already stretched thin. Hiring more technicians isn't always an option, and even if it were, more people wouldn't fix the problem of disconnected tools. What you need is a unified solution that brings everything together and makes your team more efficient.

This guide shows why a unified platform is essential for solving the problems modern MSPs face. Once your core tools connect under one platform, processes run faster, automation works seamlessly and your team can finally focus on service and growth instead of tool management.

How a fragmented stack holds MSPs back

If you're thinking about adding another point solution to your stack, it's worth understanding the challenges that come with disconnected tools.

Tool sprawl creates complexity and slows growth

Imagine you add a new RMM to close a monitoring gap. It does the job — improves visibility and helps you stay on top of endpoints. But then you notice it doesn't cover security. So, you bring in another tool for protection. A few months later, backup becomes a concern, and you add one more. Before long, you're managing a mix of platforms that don't talk to each other. What started as a simple fix slowly turns into a stack that's expensive to manage and difficult to scale. The hidden cost of tool sprawl is that each point solution solves one problem but creates two new ones.

A unified platform takes a different approach. It connects core functions like monitoring, security and backup in one system, reducing complexity while giving you the visibility and automation needed to grow efficiently.

Gaps between security and backup increase risk

Now imagine your security and backup tools are separate. One protects your clients from threats, while the other restores data when something goes wrong. But when those systems don't communicate, things slip through the cracks. A ransomware attack might be contained, but your backups could still be exposed — or worse, outdated.

Switching between tools during an incident can be detrimental. It might be too late by the time you piece everything together. MSPs know their clients are watching security more closely than ever. In Kaseya's 2025 MSP Benchmark Report, 76% said security is the number one challenge their clients face this year. It's also one of the biggest profit drivers — MSPs who had advanced security services on their roster earned 15% or more in margins compared to those who didn't. Can you really win in this high growth area with fragmented tools?

That's where unified tools make the difference. They strengthen protection and make it easier to deliver security effectively. When monitoring, backup and security work together, response times improve, visibility increases and SLAs are easier to meet. You're not just defending clients but building confidence and delivering a higher standard of service.

Disconnected systems drain your margins

Investing in a new tool is useful, but the costs also add up. Each license, vendor fee and integration pulls a little more from your margins. Before long, you're spending more time and money managing tools than growing your business. Efficiency drops, budgets tighten and hiring more technicians stops being an option.

A unified platform changes the math. Kaseya 365 Endpoint unifies monitoring, security, backup and automation for the cost of one product. It frees up the budget for new services, winning new clients or investing back in the team.

Pros and cons of standalone solutions

Standalone tools can deliver strong results in one area, but they rarely work well together. Each has its strengths, but the gaps between them often create bigger challenges than they solve.

Tools	Pro	Con
RMM	Enables device monitoring, patching and remote management.	Offers limited security context. Technicians still depend on separate tools to detect and contain threats, creating blind spots and slower response times.
EDR	Detects and responds to advanced endpoint threats in real time.	Operates independently, generating large volumes of alerts without correlation to monitoring or patch data. This leads to alert fatigue and inconsistent resolution.
AV	Blocks known malware and basic threats.	Lacks visibility into emerging or zero-day attacks. MSPs must rely on additional tools for detection, analysis and recovery, increasing both cost and complexity.
Backup	Provides data recovery and business continuity.	Backup only ensures that a copy of the data exists. It protects information, not operations, leaving technicians to bridge the gap manually during an incident.
MDR/ SOC	Offers continuous threat detection and incident response support by cybersecurity experts.	Without integration with RMM or backup systems, response actions remain manual and slow, reducing the overall effectiveness of the service.

Why unified platforms outperform standalone tools

Unified platforms replace scattered systems with one connected environment that runs lean, smart and fast, helping teams deliver more value with less effort.

A single pane of glass simplifies management

A unified platform gives you one place to manage everything. With Kaseya 365 Endpoint, RMM, EDR, MDR, AV and backup all live on the same platform, creating a clear picture of each client's environment. You can move through tasks without switching tools or waiting for data to sync.

If a client reports slow performance, you can open the dashboard and see what's happening immediately. System health, security activity and recent backups appear together, making it easy to pinpoint the cause and fix the issue before it affects productivity.

For MSPs managing hundreds of endpoints, this kind of visibility changes daily operations. It's easier to see what matters, respond quickly and keep clients confident that their systems are protected and performing as they should.

Comprehensive security and ransomware detection builds trust

A unified platform delivers complete protection across every stage of a threat. Detection, containment, remediation and recovery all work together, reducing the gaps that threats like ransomware often exploit.

Kaseya 365 Endpoint brings together advanced security solutions — EDR, AV and integrated endpoint backup — to create a single, coordinated defense. The Pro version of Kaseya 365 Endpoint goes even further with MDR, adding a 24/7 security team that monitors, analyzes and responds to incidents in real time.

This kind of coordination is nearly impossible to maintain with separate tools. When detection and backup operate in different silos, valuable time is lost switching between systems or confirming recovery points. Clients notice the difference in stability, quick response and consistent protection. This confidence builds trust and strengthens long-term relationships.

Automation and faster response improve efficiency

When every solution works within the same platform, automation becomes seamless. With Kaseya 365 Endpoint, patching, threat response and backup scheduling all operate through connected workflows. Each action triggers the next automatically, without the need to jump between tools or re-enter data.

This coordination turns routine maintenance into a continuous process. Patches can be applied, verified and logged automatically. If a threat is detected, containment begins right away, and backup verification runs in the background to confirm data integrity. Nothing is left waiting for a manual step.

The result is a faster, proactive response. For example, if a device shows signs of compromise, the system can isolate it, roll back recent changes, and start recovery in minutes. Technicians can focus on analysis and communication instead of chasing alerts or repeating tasks.

By reducing manual effort and reaction time, automation allows MSPs to deliver stronger, more reliable service. Problems are handled before clients even notice, which keeps operations smooth and trust high.

Reduced cost and vendor sprawl boosts margins

Managing multiple vendors and tools can quietly drain both time and profit. Each product brings its own contract, renewal cycle and integration work. Before long, MSPs are spending more on overlapping capabilities than on business growth. Licensing fees stack up, and so does the effort needed to keep everything working together.

Kaseya 365 Endpoint simplifies that entire model. It combines the essentials into one platform with a single contract, which means fewer renewals to track, lower overall costs and less administrative overhead. The pricing structure is straightforward — four essential capabilities for the cost of one — so margins stay healthy.

This consolidation frees up both budget and bandwidth. MSPs can focus resources on expanding services, improving customer experience and investing in their team instead of juggling vendors and chasing renewals. With everything unified, operations stay lean, predictable and profitable.

Standalone tools vs. unified endpoint platform

Here's how individual point solutions compare to a unified platform. The table below highlights the key differences in capability, efficiency and value.

Capability	RMM	EDR	AV	Backup	Unified platform
Device management	Strong monitoring and patching, but limited integration with security tools	Minimal management capability	None	None	Complete endpoint visibility and control across monitoring, patching and security
Threat detection	Relies on external tools for detection	Detects advanced threats but lacks operational context	Detects known malware only	None	Unified detection across all endpoints with shared intelligence and automated alerts
Data recovery	Manual recovery through backup tools	Requires separate backup integration	None	Reliable data copies, but no live system insight	Instant recovery connected to live monitoring and threat response
Automated remediation	Manual or script-based fixes	Responds to incidents but requires manual correlation	Limited to basic quarantine	Restores data only after incident	End-to-end automation from detection to resolution within one workflow
Ransomware resilience	Detects system anomalies, but cannot isolate threats	Can flag encryption activity but needs manual backup sync	Detects after infection	estores data but with downtime	uto-isolation, detection and fast restore with minimal disruption
Cost efficiency	Multiple licenses and vendor contracts	Separate licensing and maintenance costs	Adds incremental cost	Additional tool and storage expenses	Single platform, single contract, lower operational and licensing cost
User productivity	Constant switching between tools	Complex incident correlation	Limited visibility	Reactive recovery	One console, less noise, faster work, higher technician output

Business impact of a unified solution for MSPs

Unified platforms reshape how MSPs operate. The benefits are clear across performance, profit, and client relationships.

- **Stronger margins:** Fewer vendors mean less overhead and simpler billing. One platform with bundled pricing keeps costs predictable and frees budget for growth.
- **Operational efficiency:** Automation connects patching, detection, response and recovery. Technicians handle fewer manual tasks and spend more time delivering value to clients.
- **Customer trust and retention:** When monitoring, security and backup work together, reliability improves. Clients see consistent performance and stronger protection, which builds lasting trust.
- **Ransomware readiness:** Integrated security, backup and recovery ensure quick data restoration. MSPs can minimize downtime and protect clients from costly disruptions.
- **Scalability:** Unified workflows standardize delivery across clients. Service quality stays consistent even as the business grows.

How to evaluate solutions

As you assess your options, focus on what truly drives performance for your MSPs. Ask questions that reveal long-term value, not short-term fixes.

Does it reduce the noise or add to it?

A good platform cuts through alert fatigue and tool clutter. It should simplify your day, not add more dashboards to manage.

Can it turn data into action?

Visibility matters, but insight matters more. The right platform connects performance, security and backup data so you can act quickly and confidently.

Is it built for speed when things go wrong?

Incidents happen. What matters is how fast you detect, contain and recover. Look for built-in response and recovery that keeps clients online.

Does it make your team more capable without growing your headcount?

The best platforms multiply your team's impact. Automation, smart workflows and clear visibility help technicians manage more clients without burnout.

How quickly can new technicians get productive?

Look for solutions that simplify onboarding so new technicians can start contributing in hours, not weeks.

Can it scale without friction?

Growth shouldn't mean reinventing your processes. A unified solution should make adding new clients and endpoints as easy as managing existing ones.

Does it strengthen client trust?

Every interaction shapes your reputation. Reliable protection, faster response, and consistent service create the kind of confidence that keeps clients loyal.

Why Kaseya 365 Endpoint

Running an MSP is easier when everything works together. Kaseya 365 Endpoint gives you one platform to manage, secure and back up every endpoint, and the difference shows up across your entire business.

1

Work smarter, not harder

With RMM, EDR, MDR, AV, and backup in one place, your technicians don't lose time switching tools or chasing alerts. Every action — from monitoring to recovery — happens in a single view, keeping your team focused and productive.

2

Stay ahead of ransomware

Threats move fast, but Kaseya 365 Endpoint moves faster. It detects and isolates attacks automatically, and restores data in moments, helping you keep clients online and confident that their systems are safe.

3

Protect your margins

One contract covers everything. Four essential capabilities for the cost of one mean less vendor management, fewer renewals and healthier profit margins that scale as you grow.

4

Future ready

With continuous updates, AI insights and built-in automation, the platform evolves alongside your business. Thus, you stay competitive without rebuilding your stack every year.

Customers testimonials

Here's what some of our customers have to say:

> "Kaseya 365 has been an absolute revelation. We went from having no SOC solution, no effective EDR solution, to suddenly having a whole swath of products that we could offer to our customers."
>
> **Phil Callow, Founder of Ark ICT Solutions**

> "Consolidating everything into one pane of glass reduced our tech burden by at least 30%. I was purchasing three separate systems, which cost over 140% more than the single Kaseya 365 license."
>
> **Ian Dunstan, Managing Director at Cobalt**

> "For the past 10 years, we've been looking for that magical single pane of glass, a solution where we don't have to go to six different screens to do one thing. We're finally getting it with Kaseya 365."
>
> **Roman Shain, Chief Solutions Architect at Nero Consulting**

Win the fight against tool sprawl with Kaseya 365 Endpoint

MSPs achieve more when their tools work together. Growth, profitability and service quality all depend on how well you can manage, protect and recover every endpoint from one place. Kaseya 365 Endpoint makes it effortless. Experience how our modern unified platform can help your business grow with less effort and more impact.

Kaseya®

Kaseya is the leading global provider of AI-powered IT management and cybersecurity software. Kaseya delivers a unified technology platform to manage infrastructure, secure endpoints, back up critical data, and streamline operations for more than 40,000 MSP and SMB customers around the globe. To learn more, visit www.kaseya.com.

kaseya.com