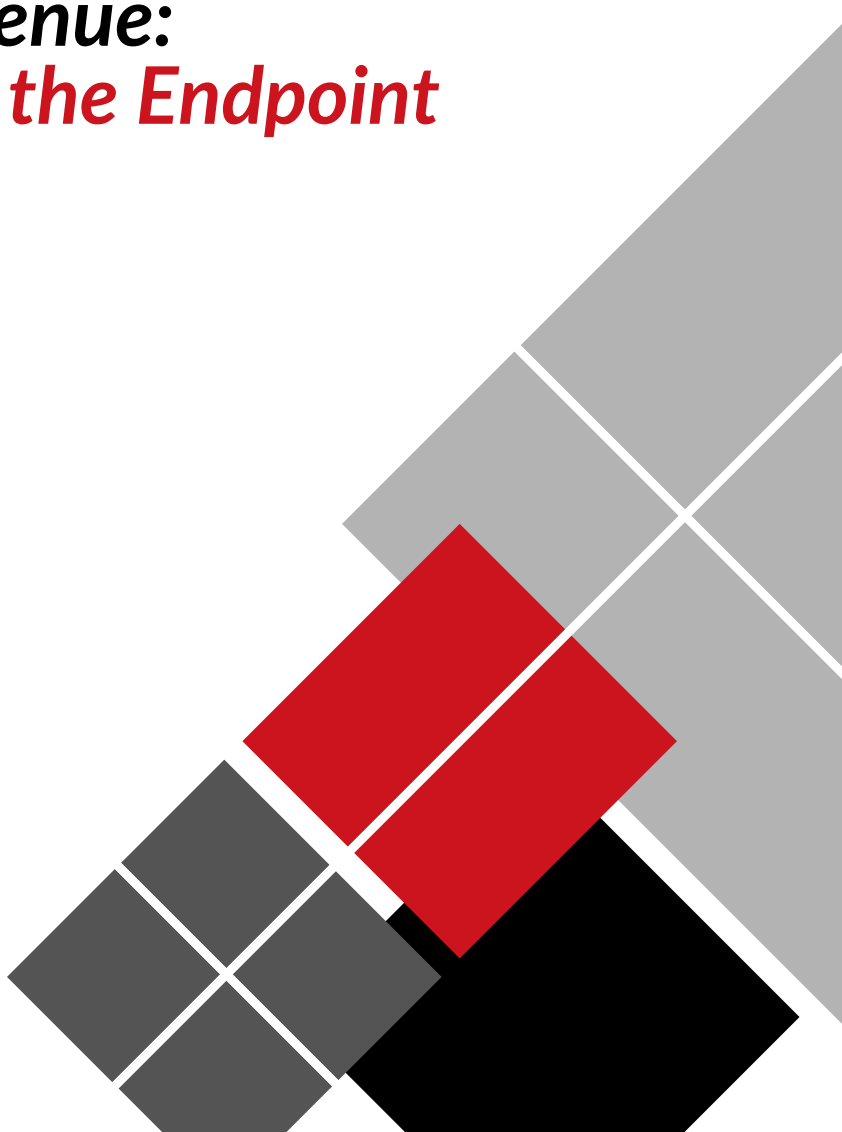
CHANNEL MASTERED
Research | Strategy | Consulting | Content

Kaseya 365 Endpoint

From Risk to Revenue:
How MSPs Close the Endpoint Security Gap



Kaseya®

Introduction

Today's managed service providers have their hands full keeping up with increasingly sophisticated security threats from attackers with access to cutting-edge artificial intelligence. To make matters worse, rising operational costs are putting pressure on profitability.

This report takes a close look at why gaps created by piecemeal legacy tool-based approaches to endpoint security and management are not only weakening protection for end users, but reducing operational efficiency and eroding MSP margins as well. It also shows why the answer to these challenges is embracing a security model that integrates threat prevention, detection, response, and recovery into a single, consolidated endpoint solution.

Finally, it explains how Kaseya 365 Endpoint, powered by Kaseya Intelligence, turns this model from theory into practice by consolidating core security, backup, management, and automation capabilities in a unified, AI-powered offering that helps MSPs eliminate security blind spots, respond more quickly to threats, and protect margins as they grow.

Fundamental Changes in the Endpoint Threat Landscape

Artificial intelligence has dramatically changed the variety and seriousness of endpoint threats. Many of the attacks themselves aren't significantly different. Threat actors continue to rely on phishing and other unpatched assets along with social engineering techniques as primary attack vectors, for example. But AI has made these intrusions more dangerous and harder to detect by helping threat actors find vulnerabilities more easily, eliminate telltale spelling and grammatical mistakes, tailor business email compromise attacks to specific individuals, and even generate convincing "deepfake" videos impersonating customers and corporate executives.

Traditional Threats	AI-Accelerated Threats
Manual phishing emails with obvious errors	AI-crafted phishing with perfect grammar & targeting
Slow vulnerability scanning & exploitation	Automated discovery cuts exploit time in half by 2027
Generic ransomware attacks	Deepfake social engineering & precision BEC attacks
Weeks from intrusion to encryption	Hours from intrusion to encryption

Furthermore, malicious hackers are using automation to shorten the time from intrusion to encryption. Gartner, for example, predicts that AI agents will cut the time attackers need to exploit account exposures in half by 2027. This time crunch requires significantly faster detection and response to limit damage.

To further complicate matters, MSPs must follow audit trails and reporting requirements associated with each of these events. That's all overhead that drives up costs, not to mention the likelihood of customer churn after an incident.

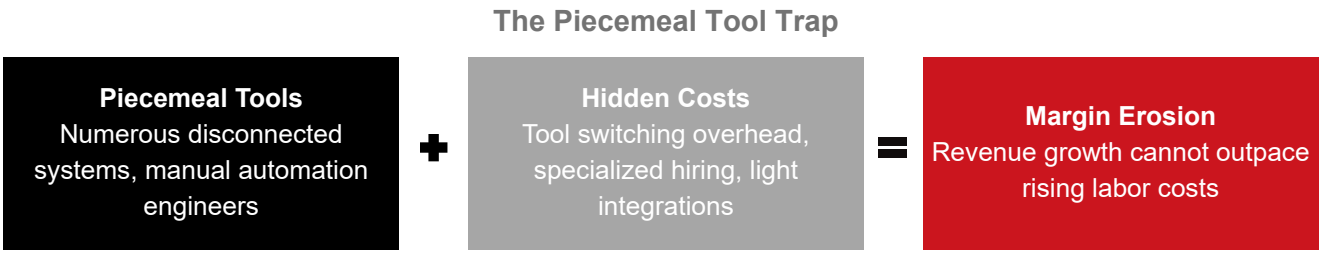
If threat actors are moving faster, then so too must MSPs, and they must do so in a manner that protects margins. That's a job stand-alone legacy tools can't handle. To keep customers safe and make real money doing it, MSPs need a comprehensive, integrated, automated, and connected endpoint strategy that combines prevention, detection, and response through security tools with recoverability through a dedicated backup solution, and incorporates AI to identify, isolate, and remediate threats swiftly.

How Endpoint Security Gaps Financially Impact MSPs

Security is only as strong as its weakest link. In today's threat environment, MSPs need effective, integrated visibility, patching, detection, response, and backup technologies to protect users and data.

Yet integrations between discrete backup and security solutions rarely go far enough. While some systems may exchange data, they typically do so via 'light' connections rather than deep, two-way coordination between platforms. The result is a lack of true alignment between tools — such as the ability to maintain a remote session to a device even when it has been isolated.

Integrating traditional layered tools also requires MSPs to make substantial investments, typically by hiring specialized automation engineers — highly skilled technicians who are expensive to retain and often paid solely to build connections between security and data protection solutions.



Unified security solutions with deeply integrated components both eliminate that waste and allow MSPs to move fast when an incident impacts a client’s normal operations. They also empower businesses to continue operating with minimal disruption once a threat is isolated at the endpoint while the MSP carries out recovery and audit activities through integrated tools and workflows.

But closing endpoint security gaps requires more than integration alone. In a threat environment characterized by sophisticated, fast-moving threats, deeply embedded AI technology capable of monitoring signals, correlating data, and taking rapid, automated action across security, backup, and management is essential too.

Modernizing Your Endpoint Security Strategy

The key to success for MSPs in today's cybersecurity landscape is to evolve their security strategy toward a model that improves outcomes without increasing cost or complexity. This starts with integration, then focuses on automation.

Integration allows security, backup, and RMM solutions to collaboratively prevent, detect, respond to, and recover from attacks. Automation reduces exposure by continuously patching systems, enforcing security policies, maintaining compliance, and remediating issues without human intervention.

A highly integrated, automated MSP infrastructure is also more efficient, allowing technicians to support roughly 1,000 endpoints each, compared to approximately 200-220 in a more traditional model, without sacrificing security, reliability, or control. More endpoints per engineer means higher revenue per engineer, allowing MSPs to grow profits faster than they grow headcount.

Technician Capacity: Legacy vs Modern Integrated and Automated Approach

LEGACY MODEL	MODERN APPROACH
200	**1,000**
Endpoints per engineer	**Endpoints per engineer**
Traditional piecemeal tool approach	Kaseya 365 Endpoint Integrated approach

How Integration and Automation Fight Ransomware

When ransomware strikes environments equipped with traditional resilience tools, defenders must shut systems down immediately and manually isolate infected machines. Then they must endure the painstaking process of recovering from backups, all while the customer's business is partially or fully offline. That results in downtime and slow recovery that can be a huge cost to the organization.

The traditional response to ransomware is reactive and can further disrupt business operations. A more modern approach is proactive: It incorporates integration, automation, and continuous validation to keep attacks from spreading, and increases the likelihood of a fast recovery.

In a Modern Integrated and Automated Approach:

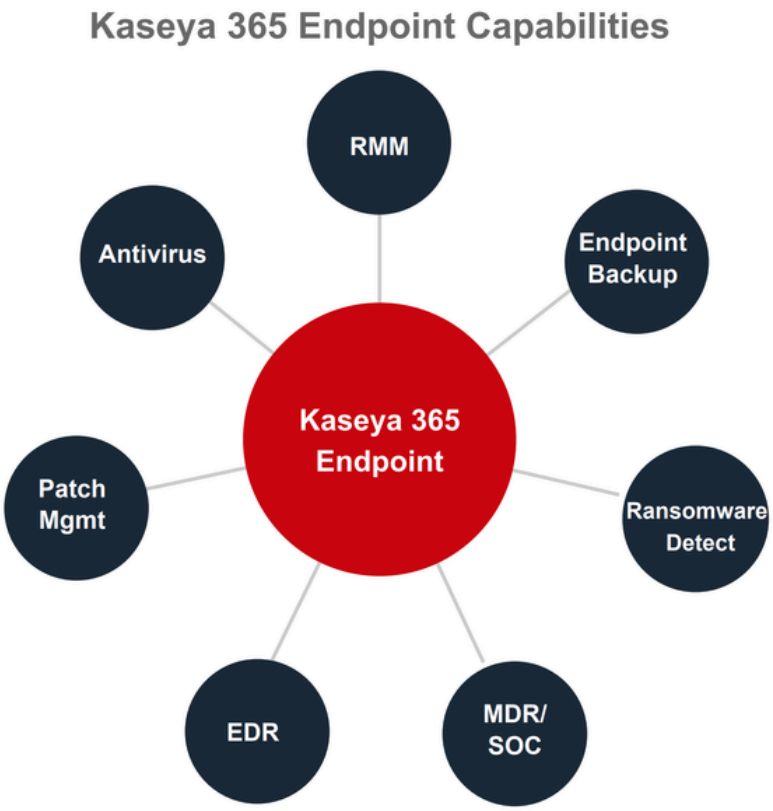
- Remote monitoring and management can reduce the number of ransomware attack vectors.
- EDR and antivirus can detect threats sooner.
- Automation allows you to react more quickly.
- Managed detection and response adds expert-led support and speedier, technology-driven response.
- Trusted backups ensure recovery after an attack.

Moving Toward a More Resilient, Profitable Model

Making the move toward a modern endpoint protection model begins with two key steps:

1. Ensuring that laptops, desktops, mobile phones, and other devices have standardized configurations, consistent security policies, and uniform update processes. This both lowers overhead by ensuring everything can be managed the same way and enables scalable growth by simplifying technician onboarding and training.

2. Reducing tool sprawl. The average MSP uses between 40 and 50 systems to deliver services. Having fewer overlapping systems doing similar jobs makes automation easier and produces an immediate bump in efficiency.



This is where Kaseya 365 Endpoint, powered by Kaseya Intelligence, comes in. A unified solution, Kaseya 365 Endpoint gives MSPs and internal IT teams RMM, antivirus, patch management, endpoint detection and response, and managed detection and response with 24/7 SOC, ransomware detection, and endpoint backup in a single subscription.

Each component is highly effective on its own; together, they eliminate visibility gaps that weaken customer security and enhance operational effectiveness. Better yet, Kaseya 365 Endpoint significantly reduces total costs — equivalent protection from disparate tools can cost three to four times more.

Beyond Kaseya 365 Endpoint: The Complete Platform Family

Just as the tools in Kaseya 365 Endpoint work cohesively, so too do the solutions in the Kaseya 365 family:

- Kaseya 365 User protects businesses from their employees' risky behavior, such as using weak passwords, falling for phishing lures, and installing unauthorized software.
- Kaseya 365 Ops unifies documentation, ticket management, and technician time logging by integrating multiple Kaseya IT operations and business management solutions.

Kaseya 365 Endpoint	Kaseya 365 User	Kaseya 365 Ops
Manage, secure, and backup every network device and endpoint	Prevent, respond, and recover every user from security threats	Orchestrate, optimize, and demonstrate smart and efficient IT operations

Together, Kaseya 365 Endpoint, Ops, and User form a unified offering that secures business users, protects their devices, and streamlines how IT teams detect, manage, and respond to security threats while ensuring ongoing operational efficiency.

They also address margin compression. An MSP's revenue growth won't keep pace with rising costs unless they scale efficiently by managing more with less. Kaseya 365 Endpoint and its sister Kaseya 365 offerings make this goal achievable. The Kaseya 365 framework helps MSPs add endpoints, users, and services faster than they add costs by increasing endpoint capacity through automation and integrated tooling.

MSPs must respond more quickly to more sophisticated attacks. Slow reaction to security events can lead directly to real business damage and loss of customers. The Kaseya 365 family spares IT teams that fate by helping them detect and respond to threats quickly and consistently.

Conclusion

Cyberattacks are growing more complex. The only way for MSPs to keep their customers safe is to streamline how they detect, assess, and resolve issues — starting at the endpoint — so engineers don't need to switch among disparate tools when a security crisis arrives. If technicians can move quickly from alert to resolution within a single workflow, MSPs can shorten response times and limit potential damage.

Kaseya 365 Endpoint, powered by Kaseya Intelligence, makes that single workflow possible by turning what are ordinarily a collection of point products into a cohesive, AI-equipped security and IT management solution offering a meaningful strategic business advantage. Aligning endpoint security, user protection, and operational workflows into an integrated and automated system helps MSPs reduce customer risk, improve efficiency, and protect margins amid a threat landscape that grows more and more complex every day.

Key Takeaways for MSPs

- Piecemeal security tools create dangerous gaps and drive up operational costs significantly.
- AI-powered threats require faster detection and response — legacy tools cannot keep pace.
- Integrated automation enables 1,000 endpoints per engineer vs. 200–220 in legacy models.
- Kaseya 365 Endpoint consolidates 7 critical capabilities into one unified, AI-powered platform.
- Equivalent protection from disparate tools costs 3–4x more with lower efficacy.

Start strengthening your endpoint protection today.

Request a Kaseya 365 Endpoint Demo

About Kaseya 365 Endpoint

Kaseya 365 Endpoint is a unified solution that gives MSPs RMM, antivirus, patch management, EDR, MDR with 24/7 SOC, ransomware detection, and endpoint backup in a single subscription — powered by Kaseya Intelligence AI.

www.kaseya.com

About Channel Mastered

Our team of multi-award-winning MSP experts help vendors build successful channel programs that drive growth and revenue with services ranging from research and analysis of the latest channel trends to channel assessment and optimization to partner recruitment and enablement.

www.channelmastered.com