Kaseya®

EBOOK

Finding signal in the noise with Kaseya SIEM

Table of contents

Introduction

Cyberthreats are evolving faster than most security operations can keep up. For MSPs protecting dozens, sometimes hundreds of client ecosystems across endpoints, cloud applications, identities and networks, the stakes are even higher.

The reality is that most MSPs don't have the resources for 24/7 security operations coverage. Instead, they piece together security using different tools, each covering a specific function. Endpoint protection platforms, firewalls, cloud security tools, identity monitoring solutions — the list keeps growing.

And with every new tool comes more data, more alerts and more "signals."

On the surface, that might sound like a good thing. More visibility should mean better security, right? However, in practice, it creates the opposite effect.

Security tools generate an overwhelming volume of alerts, many of them low-priority, redundant or outright false positives. Instead of clarity, MSPs are faced with noise. Critical threats are buried under thousands of daily notifications, and security teams are left sifting through alerts, trying to determine what actually matters. This is the reality of alert fatigue, and it's one of the biggest barriers to effective threat detection today.

At the same time, some MSPs turn to fully managed security solutions to escape the noise, only to find themselves limited by rigid platforms that don't allow for meaningful customization or control.

Turning raw signals into meaningful, actionable investigations is where most security operations break down. Knowing which alerts to trust, which patterns to follow and which incidents require immediate action is no longer something traditional tooling alone can solve.

That's where **Kaseya SIEM** comes in.

This eBook explores how MSPs can move beyond alert overload and start finding true signal in the noise. We'll look at why conventional security stacks fall short, what it takes to transform signals into investigations and how Kaseya SIEM is changing the game, helping MSPs surface real threats faster, reduce noise and operate with greater confidence and efficiency.

Why MSPs are overwhelmed by their own security stack

They want stronger security outcomes:

- More integrations across tools and platforms
- More visibility into client environments
- More comprehensive detection coverage

At the same time, they're trying to reduce the operational burden:

- Fewer alerts to sift through
- Less noise from false positives
- Less time spent on manual investigations

These priorities may seem compatible, but in reality, they create tension.

Because every step taken to improve visibility and coverage, i.e., adding a new tool, integrating another data source, expanding telemetry, also increases the volume of signals flowing into the system.

In simple terms, security visibility has exploded. MSPs today are ingesting data from everywhere:

- Endpoint activity across hundreds or thousands of devices
- Network logs from firewalls, routers and switches
- Cloud and SaaS activity spanning identities, access and user behavior

Each source adds valuable context but also complexity. This results in more alerts than teams can handle.

IT technicians are left dealing with:

- Too many alerts to realistically triage
- Not enough time to investigate each one properly
- Alerts that lack context, making them easy to misinterpret or ignore

This is where the real risk begins, as the signals that actually matter are buried in that noise.

Take ransomware as an example. Most ransomware attacks don't appear out of nowhere. In fact, they generate signals well before the final impact. A typical attack sequence includes:

- Initial access into the environment
- Privilege escalation to gain deeper control
- Lateral movement across systems
- Data staging in preparation for exfiltration
- Encryption activity that triggers the visible breach

Each of these steps produces alerts across different tools and systems. When you look at these alerts individually, they may seem low priority or routine. But together, they form a clear pattern of compromise.

In a noisy environment, that pattern often goes unnoticed. Alerts remain disconnected, context is missed and by the time the real threat is identified, the damage is already done.

This is the main challenge MSPs face today. It's not a lack of signals but the inability to turn those signals into clear, actionable answers.

The investigation burden

Every security alert demands an answer. IT teams must determine whether it's malicious, normal behavior or requires immediate action.

However, in a high-volume environment, answering that question across hundreds or thousands of alerts quickly becomes unsustainable.

Most alerts don't provide enough context to guide decision-making. As a result, analysts are forced into manual investigation workflows:

- Pivoting across multiple tools to gather additional data
- Reconstructing timelines to understand what happened before and after the alert
- Relying heavily on individual experience to separate real threats from benign activity

This is where alert fatigue truly begins — not just from the volume of alerts, but from the effort required to make sense of each one. And the problem is compounded by a common misconception: that more coverage automatically leads to better security.

However, that's not entirely true. Coverage without prioritization creates more noise, not more protection. Having alerts is not the same as having insight.

Effective security requires three things working together:

- Signal: Identifying meaningful activity
- Context: Understanding what that activity means
- Prioritization: Knowing what matters most, right now

Without context, these signals are incomplete. And when every alert feels uncertain, everything starts to feel urgent. This is the real issue.

It's not that security teams are dealing with too many false positives. It's that they're dealing with too much unprocessed signal. Until that signal is enriched, connected and prioritized, the investigation burden will continue to grow, slowing response times and allowing real threats to slip through.

What you should do today

Solving the signal-to-noise problem starts with making smarter use of the tools and data you already have.

Here's where to focus first.

1. **Ensure deep activity logging is in place**
   You can't investigate what you can't see. When evaluating or configuring your tools, prioritize depth over surface-level visibility. Look for solutions that capture rich, behavioral data, not just basic alerts. The more detailed your telemetry, the easier it becomes to reconstruct events, validate threats and build meaningful context around suspicious activity.

2. **Tune your environment continuously**
   Noise often comes from your own environment. Regular hygiene goes a long way in reducing unnecessary alerts:

   - Remove outdated users, devices and inactive agents
   - Stay on top of patching to eliminate known vulnerabilities
   - Enforce strong authentication controls such as MFA and hardware keys

A cleaner environment produces cleaner signals and fewer distractions for your team.

3. **Teach your systems what "normal" looks like**
   Not every alert needs investigation. By defining expected behavior, you can reduce repeat noise and focus only on what deviates from the baseline. Use suppressions, filters and policy tuning to eliminate known-good activity. Over time, this helps your systems and your analysts spend less time on the predictable and more time on the unknown.

4. **Interrogate your data with AI**
   AI can analyze patterns across vast datasets, correlate signals from different sources and surface relationships that would be nearly impossible to detect manually. Instead of chasing individual alerts, you start asking better questions and getting faster, more actionable answers.

5. **Act fast on high-confidence threats**
   When indicators of compromise (IOCs) are clear and validated, speed matters. Use automated response actions to immediately isolate systems, disable accounts or block malicious activity. This reduces dwell time and limits impact without requiring constant manual intervention.

These steps not only reduce noise but alsoshift your security posture from reactive and overwhelmed to focused and controlled.

How AI changes security investigation

For most MSPs, investigations are still driven by manual effort. An alert comes in, an analyst pivots across tools, gathers fragments of data and tries to piece together what happened. It's slow, repetitive and heavily dependent on individual expertise.

AI speeds up and improves the effectiveness of security investigations.

Instead of forcing analysts to chase signals, AI brings the signals together, accelerating investigations from the very first alert. It continuously analyzes data across endpoints, networks and identities, automatically surfacing what matters most:

- Related alerts that would otherwise appear disconnected
- Anomalous hosts behaving outside their normal patterns
- Behavioral trends that indicate potential compromise
- Likely attack paths based on observed activity

The result is a fundamental shift in workflow. Analysts start with context instead of grappling with isolated alerts. And that means moving from detection to investigation to conclusion much faster than traditional approaches allow.

Take endpoint activity as an example.

Over time, AI can analyze how systems and users typically behave, building a baseline of what "normal" looks like. From there, it can surface:

- Abnormal behavior patterns that deviate from the baseline
- Suspicious activity concentrated on specific hosts
- Groups of alerts that are actually part of the same incident
- Summarized investigations that highlight what happened and why it matters

Instead of sifting through raw data, analysts are presented with a clearer narrative, which drives real outcomes, such as stronger signal with less noise and faster, more confident response.

The impact becomes even more apparent in real-world attack scenarios, such as ransomware.

Let's consider the ransomware scenario discussed above. In traditional workflows, the signals of an attack appear separately:

- Initial access via phishing
- Privilege escalation
- Lateral movement onto the endpoint.

Each step generates alerts, but they often live in different tools, timelines and contexts. Connecting them requires time, effort and experience. Unfortunately, in most cases, that connection happens too late.

AI changes this by automatically linking those signals. It connects events across the attack chain into a single investigation path, revealing the full scope of activity as it unfolds. What once looked like isolated, low-priority alerts now becomes a clear pattern of compromise.

And that means threats surface earlier — before they escalate into full-blown incidents. AI helps you see more, understand faster and act sooner.

Cut through the noise with Kaseya SIEM

Kaseya SIEM is designed to help MSPs like you take control of overwhelming signal volume by combining intelligent filtering, behavioral analysis and automated response. The goal is simple: less noise, more clarity and faster action.

Reducing SaaS and cloud noise

Cloud and SaaS environments generate constant activity, resulting in a flood of alerts. Without proper tuning, even low-risk or expected behavior can quickly overwhelm analysts.

Kaseya's SIEM gives you the controls to refine what matters:

Suppression rules to eliminate repetitive, low-value alerts

PowerFilters to fine-tune detection logic based on your environment

Custom alert severity to downgrade non-critical activity

IOC-based elevation to promote truly suspicious signals into high-priority alerts

They reduce alert noise across cloud and SaaS environments, so your team can focus on high-value investigations.

Reducing endpoint noise

Endpoint signals are some of the most valuable IOCs, but they also require careful tuning to be effective.

Kaseya provides three critical tools to help MSPs separate signal from noise:

- Exclusions
- Alert suppressions
- Automation policies

Together, these allow you to teach the system what matters and what doesn't.

Exclusions:
Removing known benign activity

Not all activity is a threat. Exclusions help eliminate repeated alerts triggered by trusted processes and tools, such as backup agents, RMM scripts, internal automation tools and patch management workflows.

By removing known safe behavior, you get cleaner, more relevant alerts and reduced analyst fatigue.

Alert suppressions:
Eliminating repetitive noise

Some alerts are valid but not actionable every time they appear. Suppressions help reduce repetitive alerts from recurring administrative scripts, expected system behaviors or known operational patterns while maintaining visibility and protection. This allows your technicians to spend less time revisiting the same signals and more time focusing on new or potentially risky signals.

Policy-based automation:
Respond faster, every time

When a threat is clear, speed is critical. Automation policies ensure a consistent, immediate response without relying on manual intervention.

With Kaseya SIEM, you can automatically contain compromised hosts, terminate malicious processes and quarantine suspicious files.

These policies enable you to:

- Respond faster to high-confidence threats
- Reduce manual workload
- Standardize response across all client environment

Kaseya SIEM not only reduces noise but also transforms how you operate. It brings together endpoint, identity, cloud and network data from over 60 sources into one connected platform. It includes your own custom automated response capabilities, 24/7 SOC support and global high-confidence automated response rules created and continuously updated by Kaseya security engineers.
By combining intelligent filtering, behavioral context and automated response, Kaseya SIEM helps you move from reactive alert handling to proactive threat management.

The AI-powered interrogation chatbot in Kaseya SIEM lets you ask natural language questions such as, “What critical events happened today?” or “Is it normal for User XYZ to use Linux?” With this intelligent tool, you get instant answers, allowing you to take the right action based on the severity of the alert.

Ready to see Kaseya SIEM in action?
Discover how you can cut through the noise, accelerate investigations and surface real threats faster.

Get a demo today

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