The MSP Who Saw It All: How Key Methods Stopped Guessing and Took Control with Huntress Managed SIEM

Key Methods, a top managed service provider (MSP) in Washington state, has earned a solid reputation for keeping security front and center in their business. They manage more than 2,000 endpoints and support nearly 80 clients, providing all with strong solutions to tackle the toughest threats. But as they've learned, when it comes to cybersecurity, it's not just about stopping attacks—it's also about understanding what's really going on behind the scenes.

Prologue | Key Methods' history with Huntress

Key Methods first tried Huntress in 2022. They rolled out Huntress Managed Endpoint Detection and Response (EDR) across all their clients for a month, but they scaled back when no major security issues popped up. Instead, they took a more selective approach, using it only when they spotted something suspicious or during new client onboarding.

Company
Key Methods

Location
Wenatchee, WA

Product
Managed SIEM

About
Founded in 1998 as a small IT support company, Key Methods found their niche in providing professional technology services that let their customers focus on core business competencies without worrying about their IT infrastructure.

In 2002, they shifted their focus to proactively monitor and maintain their clients' computer networks. This new approach of focusing on "up-time" instead of waiting for "things to break" helped them grow. Today, their team consists of nearly 20 employees, serving clients around the Pacific Northwest. They look forward to pursuing their goal to be Washington state's premier IT services company.

HUNTRESS

Incident one | Managed EDR quickly shuts down a threat

In 2023, Huntress Managed EDR came in handy, flagging suspicious activity inside a client's network. This wasn't just any client, however. It was a company handling vast sums of money and a treasure trove of personal data. In other words, a prime target for hackers.

Huntress' Security Operations Center (SOC) stepped in quickly, working hand-in-hand with Key Methods. In no time, endpoints were isolated, access was shut down, and the threat was contained.

Crisis averted.

...or so it seemed.

Post-incident | The decision no MSP wants to make

The real challenge started after the immediate threat was handled. Key Methods was left with critical questions that would inform their next steps.

"All we knew was the attackers had possibly seen things they shouldn't have," says Dan Paquette, Managing Partner at Key Methods.

The entire Key Methods team was on edge, haunted by questions like, "How did the hackers get in?" "What data was compromised?" "Could they still be in the system?"

With little in terms of logs or data to go on, they had to make the call no MSP ever wants to make—shut everything down.

> Managed SIEM provides us with immediate, actionable insights, so we're never left guessing during critical moments.
>
> Dan Paquette
> Managing Partner | Key Methods

HUNTRESS

Before Huntress Managed SIEM | Playing a costly game of guesswork

The impact was huge. The client faced over a week of downtime, more than $75,000 on incident response (IR) and legal fees, and uncertainty about their future.

"It felt like forever to get the client back online," Paquette admits. "There were so many unknowns. We were digging through user logs, piecing together backward forensics, but our records only went back so far."

In the end, it turned out the hacker hadn't actually stolen any data. Using only screenshots and trickery, they'd pulled off a convincing illusion of a full database breach, leaving the client believing the worst. No data was lost, but the financial and operational toll was massive.

This was a wake-up call for Key Methods. They realized they needed more than just the ability to detect and respond to threats. They needed clear, immediate answers, especially when it mattered most.

Incident two | Managed SIEM reveals all

Not long after the incident, Huntress launched Managed Security Information and Event Management (SIEM). Key Methods jumped on board, determined to avoid ever being uncertain again. While still fine-tuning when another mass-isolation event hit, the difference was obvious.

This time, a hacker exploited a vulnerability in a client's firewall. In the past, critical decisions had to be made in real time about whether to call in IR teams, consult legal, or notify cyber insurance. Without solid data, every decision felt like a gamble—overreacting meant wasting time and money, but hesitating could spell disaster.

With Huntress Managed SIEM in place, everything changed. Put simply, there was no more guessing. The system didn't just flag threats—it connected the dots. Every log, every move, every breadcrumb the attacker left behind was laid out clearly.

With new technology and capabilities at their fingertips, Key Methods had complete clarity to act fast and make the right calls.

> "The SOC analyzed every executable across all machines and confidently pinpointed exactly which devices the hackers had compromised. Having access to such precise, actionable information is incredibly powerful."
>
> Dan Paquette
> Managing Partner | Key Methods

HUNTRESS

Unraveling the incident | The Huntress SOC paints a clear picture

The Huntress SOC quickly collaborated with Key Methods, providing clarity within hours. Detailed logs revealed the timeline of events and exactly where the attackers had been.

"Thanks to Managed SIEM, we had critical information fast," says Paquette. "We reviewed the logs and immediately recognized the severity of the issue, allowing us to involve IR and legal teams quickly."

With Managed SIEM's robust logging capabilities, Key Methods easily exported accurate, reliable data to the IR firm. "There was no question about the quality or authenticity of the logs," Paquette notes. This significantly accelerated the investigation and led to a crucial finding: no data had been exfiltrated.

"Smaller MSPs like us usually don't have a SOC," Paquette explains. "With breaches in the past, we had to bring in an external team, install their tools, and wait for results. This time around, Managed SIEM handled it all. We told the SOC what we needed, ran a quick query, and immediately got clear answers like, 'No, that executable wasn't run anywhere else in the organization.'"

With vital insight, Key Methods swiftly shifted their focus to recovery. By isolating affected systems on day one, they could begin restoration efforts right away.

Incident three | Managed SIEM wins the race against downtime

Weeks later, another mass-isolation event unfolded, this time targeting a bustling factory—a place where assembly lines hum, conveyor belts zip, and products are packaged with non-stop precision. A place where every minute of downtime risked thousands of dollars in lost revenue.

Again, an attacker exploited a vulnerability in the client's firewall. But this time, there was no panic.

> When your primary security layers are all unified in one platform, it's easier to build depth with a vendor. And when everything feeds into the same SOC, it's even better.
>
> Dan Paquette
> Managing Partner | Key Methods

HUNTRESS

"We got on the phone with Huntress, and a SOC analyst immediately understood the situation," recalls Paquette. "Within hours, we identified the issue and had already begun restoring operations. This time, legal or IR teams weren't even needed."

Armed with real-time intelligence from the Huntress SOC and Managed SIEM, Key Methods knew the attack's origin with unparalleled speed. The factory was back online the same day.

"The SOC analyzed every executable across all machines and confidently pinpointed exactly which devices the hackers had compromised," Paquette explains. "Having access to such precise, actionable information is incredibly powerful."

What could've been a financially devastating shutdown was a masterclass in resilience.

Why Key Methods is all-in on Huntress

From day one, Huntress Managed SIEM proved its worth by helping Key Methods contain threats faster, reduce downtime, and avoid unnecessary third-party headaches. While hackers rely on staying hidden, Managed SIEM gave Key Methods complete clarity into their malicious ways.

While Managed EDR wasn't initially a priority, it didn't take long for Key Methods to see the power of the entire Huntress platform. Now, they've expanded further to make Managed Identity Threat Detection and Response (ITDR) and Managed Security Awareness Training (SAT) part of their offerings. Instead of treating them as optional extras, they've baked them into their core service plans.

What really sets Huntress apart is the technology, which is purpose-built for the Huntress SOC. This tight integration of proprietary tools and human expertise creates a defense system that radically cuts down on errors, response times, and risks.

When your primary security layers are all unified in one platform, it's easier to build depth with a vendor," says Paquette. "And when everything feeds into the same SOC, it's even better."

The power of Managed SIEM | Achieving true confidence, clarity, and control

For Key Methods, Managed SIEM brought unprecedented clarity, control, and responsiveness to their operations. With Huntress Managed SIEM, they can:

- Respond to incidents in hours instead of days
- Minimize client downtime and significantly cut recovery costs
- Protect clients from escalating threats while avoiding unnecessary legal or forensic complications
- Make decisive, high-stakes calls with confidence because they're armed with clear insights on what happened, how it happened, and what data was affected

"It's all about confidence and clarity," says Paquette. "Managed SIEM provides us with immediate, actionable insights, so we're never left guessing during critical moments."

HUNTRESS

About Huntress

Huntress is the enterprise-grade, people-powered cybersecurity solution for all businesses, not just the 1%. With fully owned technology developed by and for its industry-defining team of security analysts, engineers, and researchers, Huntress elevates underresourced tech teams whether they work within outsourced IT environments or in-house IT and security teams.

The 24/7 industry-leading Huntress Security Operations Center (SOC) covers cyber threats for outsourced IT and in-house teams through remediation with a false-positive rate of less than 1%. With a mission to break down barriers to enterprise-level security and always give back more than it takes, Huntress is often the first to respond to major hacks and threats while protecting its partners and shares tradecraft analysis and threat advisories with the community as they happen.

As long as hackers keep hacking, Huntress keeps hunting.

To learn more, visit huntress.com

HUNTRESS