RAPID7

THE FIRST 24 HOURS OF A CYBERATTACK

How Rapid7 MDR Stopped an Active Exploit Before It Spread

IT DOESN'T TAKE LONG TO LOSE CONTROL

Cyberattacks have evolved. No longer the domain of lone hackers or isolated breaches, today's threat landscape is dominated by coordinated, persistent, and often automated campaigns. Attackers now operate with the speed and scale of a modern enterprise, leveraging zero-day vulnerabilities, stolen credentials, and AI-driven reconnaissance to compromise systems before teams can react.

Organizations are up against overwhelming volumes of alerts, fragmented visibility across hybrid environments, and increasing pressure to protect operations with limited resources. Detection alone is no longer enough. Speed, context, and coordinated response are now non-negotiable.

This is where managed detection and response (MDR) comes in. This is where Rapid7 leads. With 24/7 expert-driven detection, automated triage, and real-time response, Rapid7 MDR helps security teams act faster, respond smarter, and stop threats before they spread.

In the following pages, we explore a real-world case that brings best-in-class MDR to life. We'll show you that being outnumbered never has to mean you're outmatched.

We'll explore:

- What actually happens in the first 24 hours of a real-world cyberattack
- How Rapid7 MDR detects and responds in minutes, not hours
- The critical role of agentic AI, Active Response, and expert investigation
- How to evaluate your team's readiness against emerging threats

CVE-2025-53770: AN EXPLOIT IN THE WILD

In July 2025, a previously unknown vulnerability in Microsoft SharePoint was weaponized in the wild. The flaw, assigned CVE-2025-53770, enabled unauthenticated attackers to deploy a malicious file through a crafted POST request to `/ToolPane.aspx.` Once written to disk as `spinstall0.aspx`, this file was used to extract and store cryptographic keys from the server. These keys, when retrieved via a follow-up GET request, allowed attackers to forge authentication tokens and execute arbitrary commands without needing to exploit the original vector again.

Rapid7 MDR identified the attack within minutes of its emergence in customer environments. What followed was a textbook example of what effective detection and response looks like when every second counts.

With Rapid7 MDR, the investigation started before the attacker had time to move laterally.

Hour 0: Exploit detected. Response begins.

A crafted web request triggered unusual activity on a customer's SharePoint server. Rapid7's behavioral detection system picked up a suspicious chain of processes: w3wp.exe spawning cmd.exe, followed by powershell.exe with an encoded command to create spinstall.aspx. This isn't normal behavior for SharePoint.

The alert was generated automatically and triaged by Rapid7's agentic AI, which acted as a smart investigator. It assembled relevant telemetry, correlated the process chain against threat models and campaign intelligence, and built a contextual case around the activity. Within minutes of the original activity, a SOC analyst received a complete summary outlining what was happening, where, and why it mattered. This enabled Rapid7 MDR to begin response procedures while most teams would still be sorting through logs.

Detection wasn't delayed. It was active.
Response wasn't reactive. It had already begun.

> The moment we saw that PowerShell chain, we knew it wasn't normal behavior for SharePoint. The encoded command told us exactly what they were after, and we moved fast to cut them off before they got what they came for."
>
> **Senior Manager, Detection & Response Services**

Hour 1 to 2: Escalation and containment

Recognizing the risk of token forgery, Rapid7 analysts moved quickly. Using Active Response, they isolated the affected server, severing the attacker's access. Attempts to access or extract keys were stopped in their tracks.

Containment wasn't debated. It was executed.

Hour 2 to 6: Deep investigation and forensic validation

With the immediate threat contained and no initial signs of broader attacker activity, the SOC team focused on confirming the threat had not extended beyond the original compromise. Using Velociraptor, Rapid7's open-source digital forensics and incident response (DFIR) tool, they conducted a targeted review of the affected environment.

Rather than sweeping for unknowns, the goal was to confirm that the observed activity – the POST request, encoded PowerShell command, and occasional GET request – represented the full extent of the attack. As part of this review, memory and logs were checked for any additional persistence mechanisms or malware variants, particularly those aligned with ToolShell's known objectives.

Analysts identified credential access probes and failed privilege escalations, confirming no credential reuse and no lateral movement. One attacker. One endpoint. One early detection.

This was no longer just about stopping an active exploit. It was about ensuring the threat had truly gone no further.

Hour 6 to 12: Remediation and readiness

Once the forensic validation confirmed the threat had not spread, the Rapid7 SOC team shifted into focused remediation. With Velociraptor already running in the environment, analysts immediately leveraged the tool to remove the malicious file and any associated scripts, registry changes, or scheduled tasks. Artifact removal was surgical, targeted and verified without causing disruption to the broader environment.

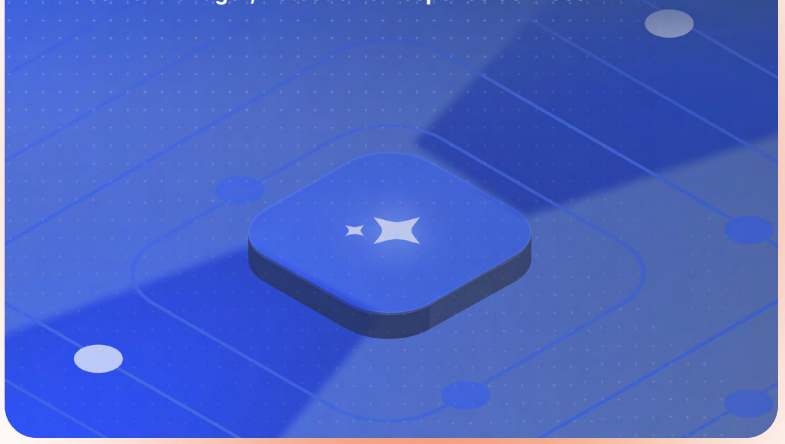
Analysts also conducted a final check for any signs of persistence that may have evaded first-pass detection. Known ToolShell behaviors were used as a guide to ensure the attacker had no lingering footholds.

Meanwhile, Rapid7's Intelligence Hub was updated with telemetry from the event. This triggered internal watchlists and campaign correlation across the MDR customer base, allowing analysts to flag similar behaviors elsewhere.

By this point, the environment was no longer in recovery. It was returning to readiness. Systems were cleared, reviewed, and placed back under full monitoring coverage. The attacker was gone, and confidence was restored.

With MDR, containment isn't the finish line, it's the foundation for full assurance.

> "Everything about this one was fast from the detection, to the triage, to the response. But what stood out was how tightly everything came together. AI gave us the context, intel narrowed the scope, and from there, it was just about staying ahead of the attacker."
>
> **Senior Manager, Detection & Response Services**



Hour 12 to 24: Reporting, hunting, and assurance

With containment and remediation complete, the Rapid7 team turned to communication, clarity, and validation. A detailed incident report was delivered to the customer before the 24-hour mark. It included a step-by-step forensic timeline, confirmed root cause, and a comprehensive breakdown of all remediation actions taken. Importantly, it also documented what didn't happen: no data loss, no lateral movement, and no persistence.

Simultaneously, indicators of compromise (IOCs) from this incident were fed into Rapid7's Intelligence Hub and shared back with the customer for cross-environment hunting. The Rapid7 MDR threat hunting team proactively searched for signs of similar activity across adjacent systems and user accounts, verifying that the attacker's reach had been contained to a single host.

This was not just closure, it was confidence. One alert. One response. One attacker's playbook, neutralized. One team ending their day with answers - not aftermath.

WHAT MADE THE DIFFERENCE

When every second mattered, Rapid7 MDR didn't just detect. It decided. It acted. And it delivered.

Why customers stayed ahead in this attack:

- **Early behavioral detection** flagged subtle process anomalies before traditional signature-based tools could react.
- **AI-driven triage** sifted through alert noise and assembled the full picture in minutes, not hours.
- **Named analyst oversight** brought human insight to machine speed.
- **Threat intelligence enrichment** ensured the SOC team wasn't flying blind, they knew what they were up against.
- **Active containment** shut down the attacker's window of opportunity before they could escalate.
- **Velociraptor-powered forensics** ensured surgical cleanup without business disruption.
- **Clear, timely reporting** gave the customer confidence and closure.

The bottom line? Rapid7 MDR combined precision, speed, and partnership to turn a zero-day crisis into a contained event.

Command is... Outnumbered. Never outmatched.

STRATEGIC TAKEAWAYS FOR SECURITY LEADERS

This eBook is more than a timeline, it's a practical tool to help teams strengthen readiness and response.

- **Start the conversation.** Use this example to align your team on what readiness looks like in practice.
- **Test your readiness.** How would your current team handle this same attack?
- **Know your window.** The difference between a close call and a breach is now measured in minutes, not days.
- **Realize value up front.** With unlimited data ingestion and incident response, there are no surprises - your coverage scales with the threat.

ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

Request a demo →

You don't get to choose when the next zero-day hits. But you can choose who's in your corner when it does.

Explore Rapid7 MDR. See how it performs when every second matters.

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at **rapid7.com**