RAPID7

24×7 MANAGED SOC FOR YOUR MICROSOFT ENVIRONMENT

POWERED BY RAPID7

Microsoft. They're powerful, reliable and form the backbone of your security and technology stack. But over time, that stack can start to feel a little heavy. Sentinel costs creep higher, alerts pile up, and teams stretched a little too thin to keep up with the day-to-day workload. It's a familiar challenge across many agencies: high expectations, limited resources, and a growing list of threats.

That's where Rapid7 comes in. With our Managed Extended Detection and Response (MXDR) service, we provide 24x7 SOC support for key Microsoft security products. This enables organisations to strengthen their security defenses by combining existing Microsoft telemetry with Rapid7's comprehensive coverage, extensive security ecosystem, and deep expertise in MXDR. The result is enhanced security outcomes through continuous monitoring and proactive threat response.

By seamlessly integrating with key Microsoft event sources—such as Microsoft O365, Defender for Cloud, Defender for Endpoint, Defender for Vulnerability Management, Defender for Identity, and Entra Identity—Rapid7's MXDR enhances detection, visibility, and response capabilities across the technologies you rely on, all without the need for additional infrastructure or complex configurations. This integration empowers security teams to uncover hidden threats and respond to incidents more quickly, leveraging Microsoft's event data to deliver 24x7, comprehensive coverage across your entire Microsoft security stack.

THE MICROSOFT CHALLENGE

We understand Microsoft is likely deeply embedded in your environment, and for good reason. It brings powerful tools and wide coverage. But it can also bring a few challenges if not kept in check:

As usage scales, especially with Microsoft Sentinel, costs can begin to grow. Ingestion charges that appeared manageable at first can quickly become a major line item, stretching already tight budgets. What initially appears to be a smart investment can turn into an unpredictable financial burden.

Then there's the fragmentation challenges. According to a 2024 Gartner survey, organisations use an average of 45 cybersecurity tools. And indeed, multiple security tools across your environment are commonplace, each doing their job. But not always in unison. Alerts come in from all directions and stitching them together into a clear and coherent picture requires time and resources most teams simply don't have a luxury of. That disconnection makes it tough to see the full story; and even harder to act on it quickly.

Add to that pressures of limited internal capacity. Many government agencies run lean security teams, and the sheer volume of threats can overwhelm even the most capable professionals – there's a limit to everyone's capacity. So, then it becomes an issue beyond efficiency, to one of risk. The longer it takes to detect and investigate a threat, the greater the potential impact.

Replacing your entire security stack isn't the answer. Instead, it's about making what you have work smarter for your team, not harder and having conversations about more headcount that budgets don't allow for.

It's about reducing the complexity, managing the cost, and getting proactive about response.

THE RAPID7 APPROACH

Rapid7's MXDR service was designed with environments like yours in mind. We work with Microsoft, not around them, to give you more visibility, more control, and better outcomes.

Here's how:

- **24x7 triage and response:** Our team goes beyond collecting alerts, instead we actively investigate them. We look at context, reduce false positives, and take action when it matters.
- **Cost control:** With unlimited data ingestion and uncapped incident response we shift to a predictable, fixed-cost model that keeps your spend in check.
- **Joined-up visibility:** We bring your entire environment, on-premises, cloud and hybrid, into one overarching picture so you can spot issues before they become incidents.
- **Security expertise on tap:** With us, you get a global SOC team embedded in your environment, working as an extension of your own.

This is about giving your team the support it needs, the visibility your leadership wants, and the flexibility your environment demands.

> **"ORGANISATIONS USE AN AVERAGE OF 45 CYBERSECURITY TOOLS.**

BUILT FOR GOVERNMENT

Public sector agencies work in high-stakes, highly scrutinised environments. We get that, which is why our approach is designed to fit your reality:

- **We work where you work:** Whether it's Microsoft Defender, Sentinel, Azure AD, or third-party tools, we integrate natively and operate across your full tech stack.
- **Proven success:** Rapid7 is a recognised leader in MDR and MXDR, supporting government departments and enterprises around the world. Our SOCs run 24x7, and our analysts are skilled at navigating complex, hybrid security environments.
- **Built for Government:** We understand procurement cycles, budget pressures, and security compliance obligations unique to public sector agencies. Our services align to those needs and scale to fit your environment.
- **Security without complexity:** We do the heavy lifting, from triaging incidents to delivering insights that matter. This means your team can focus on strategic priorities, not alert fatigue.
- **Dedicated local and global expertise:** Local support and understanding is critical. Hence our Australian team works hand-in-hand with our global resources, so you're supported by people who understand your environment and your context, as well as wider insights from experienced hands.

We help remove the noise and complexity to deliver clarity, action, and outcomes so you can stay focused on your mission.

READY TO STRENGTHEN WHAT YOU ALREADY HAVE?

Improving your security posture doesn't have to mean starting over. You don't have to rip out what you've built or make massive changes to get better outcomes.

You just need the right support. With Rapid7, you can:

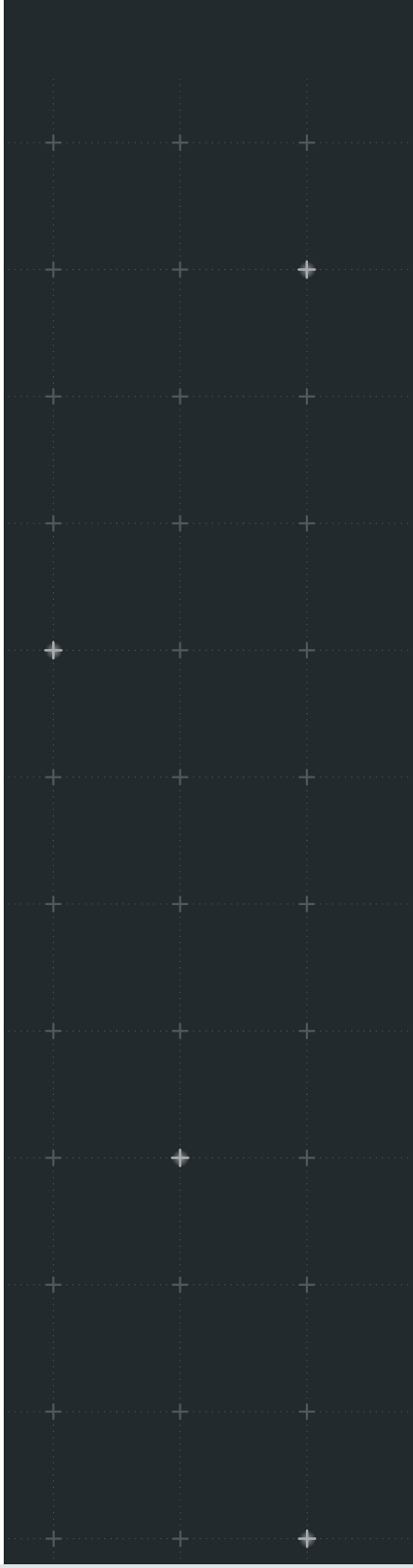
- Reduce costs without sacrificing capability.
- Gain visibility and control without overwhelming your team.
- Get 24x7 detection and response without hiring a whole new SOC.

Book a meeting with us today to discover how we can help make your Microsoft environment work harder, smarter, and more efficiently so your teams can focus on bringing about the value they were brought on board to deliver.

> **WE DELIVER CLARITY, ACTION AND OUTCOMES.**

ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organisations 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 optimise 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.



RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact