



DATASHEET

MDR for Microsoft

Leverage your microsoft investment for superior security outcomes

Our Managed Detection and Response (MDR) service leverages the full capabilities of the Microsoft Security Suite to provide comprehensive, proactive security for your organization. Acting as an extension of your team, our experts ensure continuous monitoring, threat detection, and rapid response to keep your business secure.

Binary Defense experts work closely with your security team to craft a personalized Managed Detection and Response strategy centered on your Microsoft security investments, maximizing the value of your existing tools, reducing blind spots, and enhancing your overall security operations and posture alert triage, and threat detection backed by real intelligence, so only high fidelity alerts made it to the internal team.

Personalized Detection

We manage and continuously fine-tune the detection strategy to ensure high-fidelity detections that evolve with your specific needs.

Reduce Alert Fatigue

Prioritize critical threats, minimize false positives, and keep your team focused by reducing noise.

24x7 Eyes-On-Glass

Ensure continuous protection with 24x7x365 monitoring, detection, and responding to threats anytime, day or night.

20+Years

of combined experience with Microsoft environments

5+Years

specializing in Microsoft Sentinel

How Binary Defense Enhances Your Microsoft Security Investments

Monitoring for Microsoft	Our analysts serve as an extension of your team, offering 24/7/365 expert monitoring with an attacker's mindset. This allows your team to focus on critical tasks when time is of the essence. We maintain an average response time of 12 minutes and 30-minute SLAs for critical alerts, so your team can act swiftly when it matters most.
Detections & Tuning for Microsoft	To achieve full optimization, continuous tuning and application of your detection strategy are essential. Guided by our expert detection engineers, this process minimizes false positives, enabling your team to concentrate exclusively on critical threats.
Implement Microsoft Security	Our expert detection engineers collaborate with your security team to implement your Microsoft Sentinel from the ground up within your environment. This process includes identifying and integrating critical log sources, developing a personalized detection strategy, performing the initial tuning, and ensuring that your Microsoft Sentinel alerts seamlessly flow into the BD Platform.
Management of Microsoft Security	Our expert detection engineers collaborate with your security team to implement your Microsoft Sentinel from the ground up within your environment. This process includes identifying and integrating critical log sources, developing a personalized detection strategy, performing the initial tuning, and ensuring that your Microsoft Sentinel alerts seamlessly flow into the BD Platform.

Microsoft's Enterprise Cloud Investment Fund (ECIF)

Being on Microsoft's Enterprise Cloud Investment Fund (ECIF) means Binary Defense can offer your business enhanced cybersecurity solutions with the added benefit of tapping into Microsoft's funding, which can help reduce costs, accelerate project timelines, and provide access to advanced resources.

[Click here](#) to contact us to discuss how you can utilize [Microsoft ECIF Program Funds](#).

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our [blog](#) for the latest insights, or follow us on [LinkedIn](#).

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com



BINARY DEFENSE