

DATASHEET

Corporate Overview



Making the World a Safer Place by combining threat Intelligence, technology, and analyst tradecraft with industry-leading processes to provide results-driven cybersecurity services that address the most pressing security challenges facing organizations today.

The Right Partner is the Best Defense

We understand that your company's needs, capabilities, and vulnerabilities are unique; we apply an attacker's mindset and develop a personalized approach. At the core of our approach is client partnership. Security professionals know that in the face of the unknown, they must have absolute confidence that their partners have the right technology, proven operations, and committed people to give them the solution they need in real-time.

Reduce Risk and Mature Security Operations with Binary Defense

Reduce Risk

- ◆ Strategic recommendations to harden security posture during regular security assessments and after-security events.
- ◆ Detection engineers who leverage Detection-as-Code by treating each detection as an engineered threat model built from intelligence, validated through evidence, and tuned for impact.
- ◆ Hypothesis-Driven Threat Hunting team proactively detecting anomalies.
- ◆ Breach response capabilities such as in-depth investigation, malware reverse engineering, digital forensics, etc.

Commitment to Success

- ◆ Weekly or bi-weekly tactical meetings focused on service delivery topics and concerns.
- ◆ Monthly metric review, where we deliver a comprehensive suite of advanced metrics and reporting to enable accurate measurement of threat, risk, impact, and effectiveness.
- ◆ Quarterly strategic meeting to review performance for the past period and demonstrate how Binary Defense is contributing to your security goals. In-depth Technical training provided to clients' security teams by our Security Leaders.
- ◆ Daily newsletter of articles and analysis of latest threats.

24x7x365 Security Experts

- ◆ 24x7x365 Security Operations Center (SOC) monitoring, triaging, and responding to threats.
- ◆ Detection Engineering Team that leverages external and internal threat intelligence, while implementing a Detection-as-Code model.
- ◆ Threat Hunting Team that reduces blind spots and builds custom queries to counter advanced, evasive threats to your business using hypothesis-based Threat Hunting techniques.
- ◆ Counterintelligence Team comprised of experts formerly with the FBI, military, government, and private sector that gather information and conduct operations to identify threats to an organization.

Improve Security Posture

- ◆ Threat-Informed Detection Engineering (TIDE) reframes detection engineering through an evidence-based lens. Engineers begin each detection with a hypothesis, gather supporting evidence from available telemetry, design an experiment to validate it, and only then deploy the logic into production. Giving you signals instead of noise.
- ◆ Standard operating procedures customized to your environment – including incident handling procedures, response playbooks, and escalation processes.
- ◆ BD Platform giving you a centralized hub to ingest telemetry and logs from near-endless sources, providing security visibility across your full environment.

Our Enterprise Defense Portfolio

Managed Detection and Response (MDR):

Our Managed Detection and Response service detects and isolates threats early in the attack lifecycle. Expert security analysts in the Binary Defense Security Operations Center (SOC) apply an attacker-first mindset powered by Threat-Informed Detection Engineering (TIDE) and continuous IOC-driven threat hunting. Acting as an extension of your security team, they monitor your environment 24x7x365 to rapidly detect and respond to security incidents. When a security event occurs, analysts provide triage, disposition, prioritization, and MITRE ATT&CK analysis to provide tactical and strategic recommendations.

BDVision MDR Agent:

BDVision stops threats before they succeed with a detection engine built on behavioral analysis, deception technology, and real-time disruption without impacting legitimate business operations. Stay one step ahead of evasive threats by detecting and monitoring techniques attackers use to bypass traditional defenses. Strengthen your defenses by creating traps that waste attackers' resources while revealing their strategies to strengthen your defenses.

Analysis On Demand (AoD):

AoD provides your team with on-demand, in-depth analysis and investigation within your environment by senior (T3) analysts with extensive experience in forensics and malware reverse engineering.

Threat Intel On Demand:

The Binary Defense Threat Intelligence service is exclusively designed for Managed Detection and Response clients. The service offers actionable insights into a specific threat or set of threats that your organization may be concerned about, helping you stay ahead of potential risks.



Additional Services

Hypothesis-Based Threat Hunting:

Binary Defense's Threat Hunting utilizes a human-driven, technology-enabled approach to detect patterns of threat actor behavior. Our team leverages their expertise and evidence-based hypotheses to proactively detect quiet attackers through custom hunting queries tuned to your unique environment. We provide timely threat intelligence, malware reverse engineering, and insights from threat activity discovered to reduce blind spots across your environment.

Phishing Response Services:

Our Phishing Response service performs full-scope human-led investigations of phishing events in your environment and uses the intelligence gained to improve detection and enhance your existing security controls. We combine threat Intelligence, technology, and analyst tradecraft to reduce the risk of malicious emails reaching your employee's mailboxes.

Digital Risk Protection (DRPS):

We use a human-driven, technology-assisted approach to search the surface web, dark web, deep web, and social media for threat indicators against your business. Our team will provide actionable reporting that helps you stay informed and prepared in the areas that matter most to you. Your organization will benefit from daily intelligence briefings, helping you stay up-to-date on the latest threats targeting your attack surface.

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