BINARY DEFENSE

DATASHEET

MDR Core

The Right Partner is the Best Defense

Binary Defense provides a Managed Detection and Response service that detects and isolates threats early in the attack lifecycle. Expert security analysts in the Binary Defense Security Operations Center leverages an attackers-mindset, monitoring your environments for security events 24×7×365, acting as an extension of your security teams. When a security event occurs, Binary Defense analysts' triage, disposition, and prioritize the event. Analysts conduct full kill chain analysis and supply tactical and strategic mitigation recommendations to your security team with the goal of increasing your organization's security posture against the latest adversary threats.

SOC Built for Defense-in-Depth

The Binary Defense SOC acts as an early warning system for your organization - responsible for monitoring the security of your organization, detecting and investigating threats, and responding to security incidents. Trained and qualified across a variety of technologies and techniques, they continuously monitor your infrastructure for suspicious activity or anomalies that could indicate a threat to your systems or users.

- 24×7×365 monitoring, detection, analysis, and response capability by operate as an extension of your team
- Event triage, notification, kill-chain analysis, tactical mitigations, documentation, and reporting
- Helps you find threats faster, more consistently, and more accurately across your diverse attack surface before they can harm your organization
- Cuts through the endless alerts to determine what's a threat to your organization and what is just noise or false positives by enriching security alerts with context and collaborating with you in that process
- Analysis on Demand for level 2-3 forensics and attack reconstruction
- Threat Intel On Demand includes 1 inquiry per quarter offering actionable insights into a specific threat or set of threats that your organization may be concerned about, helping you stayahead of potential risks.
- Continuous Analytical Threat Hunting that's based on known IOCs and static signatures to make your environment more resilient to attacks
- Provides guided responses, delivering actionable advice on the best way to contain and remediate a specific threat. Organizations are advised on activities

Binary Defense brings unsurpassed technical chops...

Forrester Wave: Managed Detection and Response 2023

FORRESTER®
WAVE STRONG PERFORMER 2023
Managed Detection And Response

Why Security Teams Trust Binary Defense for MDR

Detection Strategy

A comprehensive detection strategy is key to detecting threats early in their attack. That's why our Detection Strategy is focused on understanding the adversary's TTPs (tactics, techniques, and procedures) to detect and isolate attacks at multiple stages on the attack chain.

Answers, Not Alerts

Our Security Analysts analyze any alarms generated and only send alerts requiring further action. Any alerts that are sent to you for review will contain additional context- who, what, why, how - about the alert so that your team is able to quickly understand what is going on.

Metrics that Matter

We provide a comprehensive suite of advanced metrics and reporting to enable accurate measurement of threat, risk, impact, and effectiveness - including incident volume metrics, tactical trends, noteworthy incident reviews, and threat intelligence updates.

Open-XDR Strategy

Our Open XDR strategy allows us to ingest telemetry and logs from near-endless sources, providing security visibility across your full environment. By leveraging your existing tools, this strategy not only hardens your security posture but helps drive ROI on those existing tool investments.

Tradecraft Expertise

We bring a set of Standard Operating Procedures personalized to your environment - this includes our incident handling procedures, response playbooks, and escalation processes. Analysts are highly trained to detect anomalous behaviors and specialize in the Cyber Kill Chain framework for investigations into security events in your environment. When a security event occurs, not only do the analysts analyze the event, but they also synthesize the attack to ensure that key indicators of compromise are identified across the entire kill chain. This analysis is provided back to your security team through detailed tactical and strategic recommendations to increase your security posture.

Threat Intelligence and Collective Defense™

Our Threat Intelligence team is collecting, processing, and then disseminating tactical, operational, and strategic Threat Intelligence to our clients.Additionally, with Collective Defense™ when one of our clients is attacked, we defend that client, leveraging the newly acquired threat intelligence to protect and defend the rest of the portfolio. You will benefit from proactive communications, situational awareness, threat context, mitigation strategies, and operationalized threat intelligence.

> **I haven't seen another product that combines the visibility that Binary Defense MDR offers with the response times of the SOC."**
>
> **Mike Saunders, Principal Consultant in Information Security**

Our Approach to Managed Detection and Response

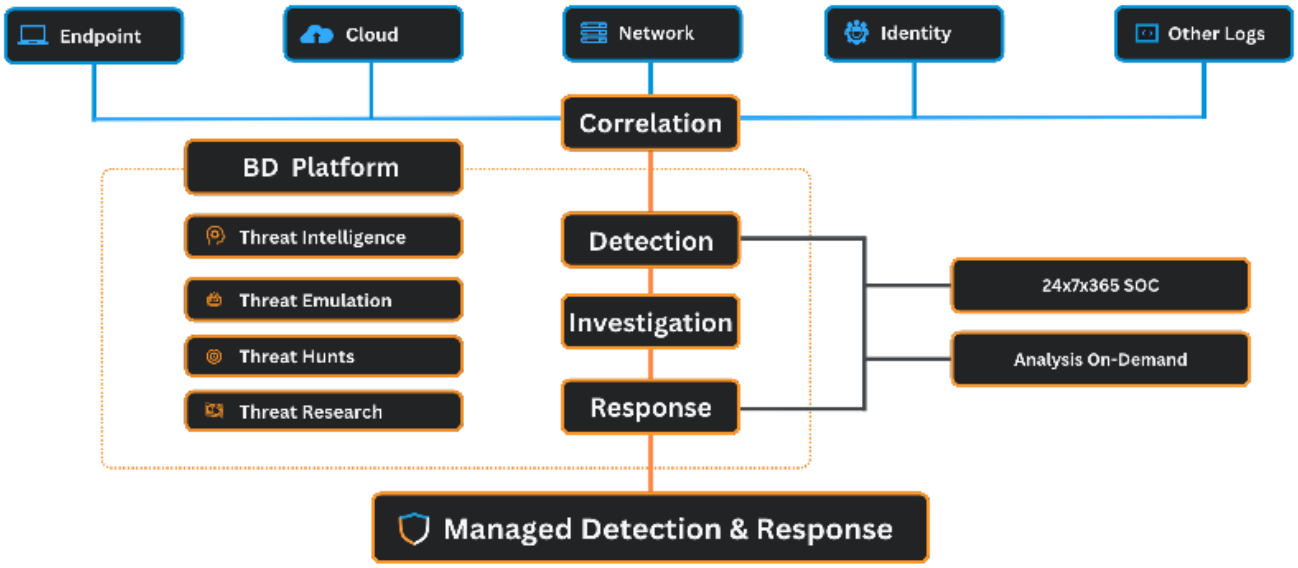
Binary Defense's Managed Detection and Response is built around three important pillars - **People, Process, and Technology**

Open XDR Strategy
enriches your security investments to deliver maximum ROI and increase security maturity

Security Orchestration and Automation
enables deep integration while allowing you to retain full ownership of data

Ability to Scale Your Security Program
as your business grows

Flexible Engagement Models
focused on driving security objectives



About Binary Defense

Binary Defense is on a mission to Make 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.

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