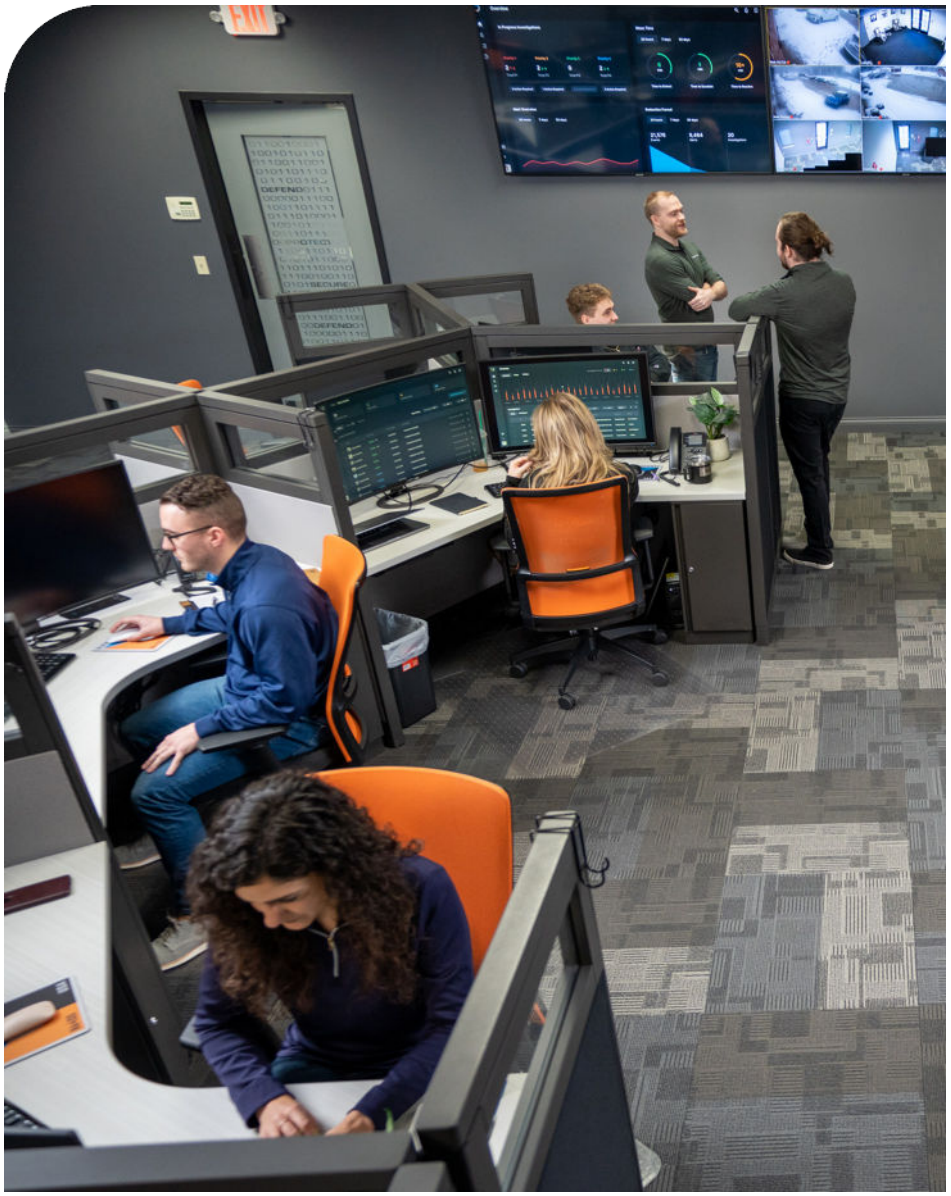


BINARY DEFENSE™

Managed Detection & Response

The Binary Defense Managed Detection & Response solution combines Threat Intelligence, Technology, and Analyst Tradecraft with industry-leading processes to provide a results-driven service that addresses the most pressing security challenges facing organizations today.

The Right Partner is the Best Defense

Binary Defense provides a Managed Detection & Response service that detects and isolates threats early in the attack lifecycle. Expert security analysts in the Binary Defense Security Operations Center leverage an attackers-mindset, monitoring your environments for security events 24x7x365, 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 & 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, 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.

- 24x7x365 monitoring, detection, analysis, and response capability
- Event triage, notification, kill-chain analysis, tactical mitigations, documentation, and reporting
- Analysis on Demand for level 2-3 forensics and attack reconstruction
- Operate as an extension of your team

"Compared with other vendors, Binary Defense demonstrates conclusive proof of superior capabilities in detecting intruder activities"

Forrester Wave: Managed Detection and Response 2021

FORRESTER®
WAVE LEADER 2021
Managed Detection And Response

“The Binary Defense SOC is first class and does a thorough job with analysis, whitelisting and alerting us of potential problems. Over a short period of time, the SOC learnt our environments (3 distinct locations, 2 in the US and one overseas), closes alerts they’re familiar with and only escalates what’s absolutely necessary.”

- CEO of Software Development Firm (Gartner Peer Insights)

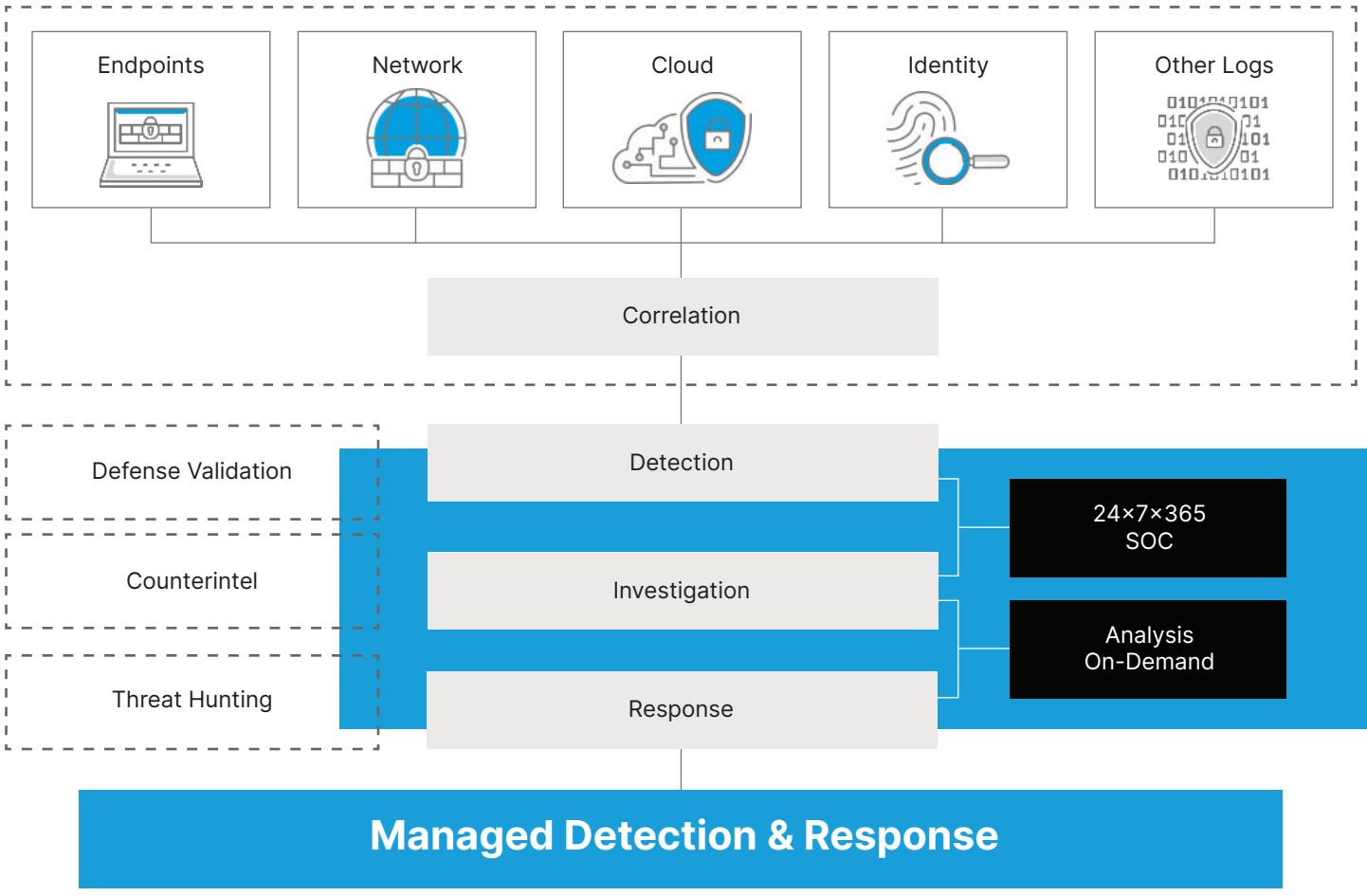
Why Security Teams Trust Binary Defense for Managed Detection & Response

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.
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 specialized in the Cyber Kill Chain framework for investigations into security events in your environment. When a security event occurs not only do the Analysts do the analysis of the event, but 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.
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.
Threat Intelligence & Collective Defense™	Our Threat Intelligence team is collecting, processing, 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.
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.

Our Approach to Managed Detection & Response

Our Managed Detection & 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
- Flexible engagement models focused on driving security objectives
- Ability to scale your security program as your business grows
- Security orchestration and automation enables deep integration while allowing you to retain full ownership of data



BINARY DEFENSE™

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