DATASHEET

Binary Defense Overview

Agentic MDR. Human command. AI speed.

Who We Are:

Binary Defense delivers Agentic MDR grounded in offensive security expertise and an attacker's mindset. Human instinct and AI speed work as one, helping organizations detect threats earlier, investigate with greater depth, and respond decisively across endpoints, networks, identity, and cloud.

At the center of that capability is NightBeacon our AI SOC platform built inside our own live MDR operation, not in a lab. NightBeacon turns raw alerts into evidence-backed investigations. The result is faster triage, deeper context, and analysts focused on decisions not data processing.

NightBeacon keeps humans in command. Analyst judgment drives every escalation and response action. AI accelerates the work; people own the outcomes.

Core Services:

Six capabilities. One tactical team.

1 Managed Detection & Response (MDR)

Our core service delivers 24x7x365 monitoring across endpoint, cloud, network, identity, and other log sources. U.S.-based SOC analysts triage every alert, investigate with full context, and coordinate response backed by NightBeaconAI that handles the first 80% of repetitive triage so analysts focus on decisions that matter.

NightBeacon includes Threat Intelligence, Threat Emulation, IOC Queries and Threat Hunts, and Threat Research all feeding into a Detection, Investigation, Response pipeline. Analysis-On-Demand gives you Tier 3 analyst access for forensics and malware analysis when you need it.

2 Turnkey MDR

Subset delivery method of MDR

Binary Defense delivers Turnkey MDR by fully managing your SIEM and security operations end to end. We take care of implementation, detection engineering, continuous tuning, and 24x7 monitoring so your security program produces real results without adding operational burden. Our analysts and engineers handle deployment, threat-informed detection strategy, ongoing tuning, and 24x7 coverage protecting you against the latest emerging threats.

3 Platform Management

Subset delivery method of MDR

Already invested in a SIEM or XDR platform? We layer onto it. Binary Defense handles implementation, detection engineering, continuous tuning, and 24x7 SOC monitoring across platforms like Sentinel, Palo Alto Networks Cortex XSIAM, Google SecOps, Sumo Logic, and more.

Your team keeps access and ownership. We bring the expertise, the coverage, and the 24x7 eyes — you keep the visibility and control. The SIEM or XDR platform you already paid for starts working the way you expected it to.

4 Managed Threat Hunting

Attackers who know what they're doing don't trigger alerts. They move slowly, blend into normal traffic, and wait. Managed Threat Hunting puts our analysts on offense, actively searching your environment for the activity your detections aren't designed to catch.

Our threat hunters develop and execute hunts using current threat intelligence, known adversary TTPs, and observed attack patterns specific to your environment. This is an ongoing service, not a one-time engagement. Hunts run across your in-scope SIEM and EDR platforms without requiring your team to define hypotheses or manage the process. When threat hunters find something, you get context and recommended next steps.

5 Digital Risk Protection (DRPS)

Continuous monitoring of the open and dark web for threats targeting your brand, credentials, and data. When we find brand spoofing, leaked credentials, or threat actor chatter about your organization, we act not just alert.

6 Phishing Response

Full-scope phishing investigation and detection building. When a suspicious email lands, our analysts investigate end-to-end: headers, payloads, infrastructure, and downstream impact. We build custom detections to catch the next variant before it lands.

Supported Platforms:

We work with what you have.

While not exhaustive, these are the key technologies we frequently integrate with and support. Our platform works alongside the tools your team already relies on delivering stronger outcomes without disruption.

	Implementation	Detections	Tuning	Management	SOC Monitoring	Managed Threat Hunting
SIEMS						
Sentinel	✓	✓	✓	✓	✓	✓
Palo Alto Networks Cortex XSIAM	✓	✓	✓	✓	✓	✓
Splunk		✓	✓	✓	✓	✓
Sumo Logic	✓	✓	✓	✓	✓	✓
Google SecOps	✓	✓	✓	✓	✓	✓
CrowdStrike NG						✓
ExtraHop			✓	✓	✓	
Add-On						
Cribl		✓	✓	✓		
EDRs						
BDVision	✓		✓	✓	✓	
CrowdStrike		✓	✓		✓	
Sentinel One		✓	✓		✓	✓
Microsoft Defender		✓	✓		✓	✓
Palo Alto Networks Cortex XDR	✓	✓	✓	✓	✓	✓

Table Definition Key

Implementation
Deployment of a SIEM within a customer environment from the ground up. Includes identifying and onboarding log sources, integrating SIEM alerts into the Binary Defense environment, and performing initial tuning to ensure optimal visibility and performance.

Detections & Tuning
Continuous refinement and application of Binary Defense's threat-informed detection strategy to enhance alert fidelity and minimize false positives.

Management
Ongoing administration of the SIEM or EDR platform, including updates, upgrades, health checks, troubleshooting, and coordination with third-party vendors. Includes continuous tuning and applying Binary Defense's threat-informed detection strategy.

SOC Monitoring
Binary Defense's 24x7x365 monitoring service, where SOC analysts provide real-time analysis and response for all SIEM and EDR alerts to detect and mitigate threats promptly.

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