DATASHEET

MDR for Private Equity

Defending Data. Protecting People. Powering Confident Investments.

Private Equity firms run on precision, speed, and certainty, but cybersecurity gaps across portfolio companies introduce risks that can stall deals, disrupt value creation, or weaken an exit. Binary Defense helps PE firms outmaneuver attackers with an MDR solution built on human insight, adaptive technology, and an attacker's mindset. Our analysts work in NightBeacon CMD, the AI-driven SOC workbench behind our MDR, which correlates related alarms into one verdict-ready Situation so investigation starts with roughly 80% of the work already done, in every portfolio company we cover.

Delivering Value at Scale

Our MDR solution helps:

- Accelerate diligence and onboarding during M&A
- Improve exit readiness with measurable security maturity
- Standardize security tools and detection quality to reduce overall operating expenses
- Run every portfolio company on one operating model, one workbench, one standard of evidence

PE Firm Challenges

Private Equity firms rarely start at the same security baseline. Many often struggle with:

- Underfunded Security: We scale your coverage, expertise, and capacity instantly.
- Disparate Security Tools That Limit Visibility: NightBeacon CMD unifies your stack across 130+ connectors spanning 19 categories, so alarms from every portfolio company surface as one correlated Situation instead of scattered alerts across a dozen consoles.
- Underfunded or Overextended Internal Teams: We act as an extension of your team giving you access to cross-platform expertise and knowledge transfer.
- Untapped Capabilities: We turn existing security investments into high performance defenses. Detection content is authored and versioned in NightBeacon CMD, then deployed into the SIEM each company already owns, in its native query language across 19 platforms. No rip and replace.
- Expanding Attack Surface: With our Digital Risk Protection Services we can defend every edge internal, external, and executive, no matter how fast your portfolio grows.

How We Do It

- Attacker's Mindset Drives Defense In-depth: We think like adversaries, to stop them before impact events occur.
- Human Insight + Adaptive Tech = Stronger Defense: Your environment gets expert-led, always on protection.
- Alarms Detect, Situations Are the Work: An alarm is a unit of detection. Treat it as the unit of work and one adversary shows up as three unrelated rows. NightBeacon CMD correlates related alarms into one Situation before anyone opens a ticket.
- NightBeaconAI Makes Analysts Faster: It never becomes a black box that replaces them. AI does the analysis at machine speed, our analysts own every decision.
- Threat-Informed Detection Engineering: We align detections to real adversary behaviors, ensuring your program continuously adapts to threats rather than static signatures.
- Detection-as-Code: We build, test, and deploy detections using engineering grade processes that ensure consistency, auditability, and rapid iteration across your entire portfolio.
- You Bring Your Security Tools, We Amplify Their Impact: No rip and replace, no black box.
- White-Glove MDR Solution: We build our MDR solution around what's best for you.

How Our SOC Runs CMD

> Binary Defense runs NightBeacon CMD in its own 24x7x365 SOC, with U.S.-based analysts in the driver's seat, owning every decision. Managed Detection and Response clients get machine-speed analysis and human-owned outcomes, across every company in the portfolio.

HOW WE DELIVER MDR

Our analysts own every decision

We run NightBeacon CMD inside our own 24x7x365 SOC. NightBeaconAI does the analysis at machine speed; our analysts own every decision and stand behind every outcome. Nothing reaches you without a human reviewing it, and high-impact actions are always analyst-approved.

Built inside a live SOC

NightBeaconAI is trained on years of real analyst decisions across a large, diverse client base. It sharpens every shift, operational signal a tool-only vendor cannot copy. Your event content is never used for training, and connectors are read-only by default.

Detections run in your SIEM

Detection content is authored and versioned in NightBeacon CMD, then deployed into each portfolio company's own SIEM in its native query language across 19 platforms. When a rule fires, the alarm returns tied to the exact rule that raised it, so noise and outcomes score per rule.

WHAT PE CLIENTS GET

Faster detection and response

Related alarms auto-correlate into one verdict-ready Situation before an analyst opens a ticket, so our SOC decides in minutes, not after 20 to 40 minutes of manual context assembly.

One standard across the portfolio

A company acquired last month reports the same way as one you have held for five years. Same Situations, same evidence trail, same MITRE ATT&CK mapping, same coverage reporting.

Glass box, not black box

Every verdict carries its reasoning, down to the evidence that moved it. Every AI-generated field is marked, a second model reviews the first, and your analyst can disagree with either. Findings you can defend to a board, an LP, an auditor, or a cyber insurer.

~80%	~46%	24x7x365	130+
Of the investigation pre-built before an analyst engages	Faster Situation summarization for the client write-up	U.S.-based analysts who own every decision	Connectors unifying your whole stack

Why PE Firms Need a Different Kind of MDR Provider

1. Security Risk During M&A, Integrations, and Transitions

Mergers and acquisitions bring massive changes to security tools, teams, and visibility, the perfect window for attackers. Binary Defense locks it down from all sides:

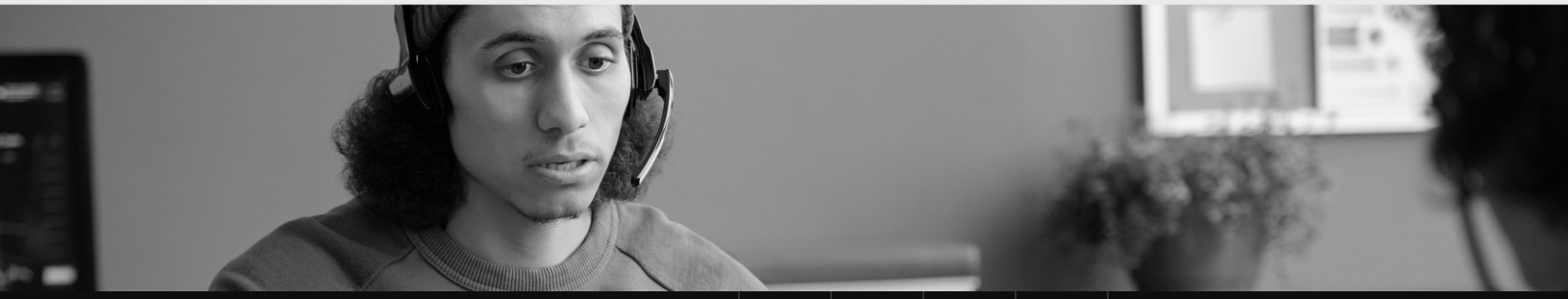
- 24/7 monitoring and real-time response across both environments so threats don't get lost in the noise.
- During integration, both environments onboard into NightBeacon CMD. Once they are consolidated under one organization, alarms from either side correlate into a single Situation, so cross-environment activity reads as one story instead of two unrelated queues.
- Threat-Informed Detection Engineering ensures we deploy detections built specifically for M&A related attacker TTPs like lateral movement, credential abuse, domain pivoting, and account takeover attempts.
- Proactive threat hunting to uncover hidden risks like dormant malware, legacy access, or misconfigurations before they become active threats.
- Our hunters use the Agent in NightBeacon CMD to run a hypothesis, a MITRE technique, or an IOC sweep across every connected platform in parallel, so a newly acquired environment gets swept in hours, not quarters.
- Digital Risk Protection to monitor external attack surface expansion, leaked credentials, executive targeting, and increased exposure during M&A.

*We help you stay in control and ahead of the threats, from start to finish.

2. Limited Internal Resources with Varying Expertise

With limited manpower, internal teams are overloaded and risk missing critical threats. New CISOs often inherit outdated or underdeveloped programs that demand immediate uplift. Binary Defense becomes the extension of their team by:

- Delivering 24/7 coverage from experienced analysts and solution engineers, and threat hunters.
- Handing them a short list of Situations instead of an alarm flood. Related alarms auto-correlate before an analyst opens a ticket, so our SOC decides in minutes rather than after 20 to 40 minutes of manual context assembly.
- Implementing Threat-Informed Detection Engineering to give teams clarity and assurance about which adversary behaviors matter most.
- Providing detection level transparency so teams understand why detections triggered and how they map to real threat actor behaviors, with the full evidence chain visible in the Situation.
- Offering comprehensive forensic expertise and advisory support across SIEM, EDR, cloud, and identity.
- Answering "is this malicious?" in house. Deep Scan detonates unknown files in an isolated sandbox, extracts the IOCs, and sweeps other hosts for what it finds.



3. Alert Fatigue & Wasted Resources

Inherited security tools often produce noise instead of actionable insights. Binary Defense MDR solution shifts programs from alert fatigue to meaningful detections by:

- Deploying detections that create real signal, not isolated events with no context.
- Correlating a hundred alarms into one Situation, so the queue is bounded by real events rather than alarm volume.
- Using Detection-as-Code to continuously refine, tune, and version control detections across environments.
- Removing noisy or low value detections through continuous tuning, scored per rule in NightBeacon CMD so tuning follows the data instead of a hunch.
- Letting the 24/7 SOC filter out noise, escalating only what matters.
- Making the quiet legible. When the queue clears, the Peace-of-Mind panel reports alarms in, auto-resolved, escalated, false-positive rate, and confidence health.

*This gives leaders clarity and increases operational efficiencies across the portfolio.

Binary Defense delivers a purpose built MDR solution that gives private equity firms the confidence to move fast, invest boldly, and operate securely, no matter how complex or rapidly changing their portfolio becomes. Our SOC runs NightBeacon CMD. You get decisions, not a queue.

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

FORRESTER
WAVE STRONG PERFORMER 2025
Managed Detection And Response Services

BINARY DEFENSE