Data Sheet

eSENTIRE

MDR for Private Equity

24/7 Threat Detection and Response for Every Company You Own

Portfolio companies rarely have the security depth of the firms that acquire them. Small teams, no red team capability, limited tooling, and management measured on growth. That gap does not stay contained to one company. A breach surfaces at the fund level. It affects deal valuation. It draws scrutiny from insurers and acquirers.

eSentire MDR delivers 24/7 threat detection and response for 50+ private equity firms and hundreds of their portfolio companies. We standardize security posture across the portfolio, protect deal value, and produce the compliance evidence insurers and acquirers demand.

THE EXPOSURE IS MEASURABLE

THIN TEAMS, HEAVILY TARGETED

86%

Intrusion ratio for VC and PE backed companies, among the highest of any sector eSentire tracks.

eSentire Private Equity Threat Report

THE COST OF BEING A TARGET

$2.1M

Average financial impact of a single security incident at a portfolio company.

Kroll, Feb 2026

BREACHES HAPPEN DURING THE DEAL

26%

Of PE firms report a reduced deal or exit valuation tied to a portfolio company breach.

Kroll, Feb 2026

Security That Understands Private Equity

eSentire provides AI-driven tools, SOC, and expertise built for the speed and scale of private equity.

Immediate Portfolio Protection

- Deployed at close or pre-close, so coverage starts when ownership does
- Runs on the portfolio company's existing stack from day one, with no rip-and-replace
- 24/7 monitoring live from the moment you take ownership, powered by Atlas AI
- Environment context captured at onboarding and held in Atlas, so investigations start with it
- Security baselines set with the management team in the first weeks

Works With the Existing Stack

- Multi-signal ingestion across endpoint, identity, cloud, network, AI, and email
- Visibility into AI and agent usage across portfolio companies, powered by Atlas AIDR
- Supporting SentinelOne, CrowdStrike, Microsoft, Palo Alto
- Vulnerability data ingested from Qualys, Tenable, Rapid7, and/or Wiz
- Existing licenses keep working, which protects capital already spent
- Same service level whether the portfolio company has 50 employees or 5,000

Cyber Insurance & Compliance Readiness

- MDR service meets cyber insurance underwriting requirements
- Continuous compliance evidence for SOC 2, PCI DSS, and HIPAA portfolio companies
- Audit-ready reporting for boards, investors, and acquirers
- AI usage across the portfolio company, closing a gap insurers and auditors are starting to ask about
- Incident response included in MDR
- Digital forensics available as a specialist add-on when incident needs legal-grade evidence

THE FIRM-LEVEL VIEW

Every Portfolio Company Protected. One Place to See All of It.

MDR is table stakes. Every portfolio company needs it. Report at the fund level and get answers without going from company to company.

1

One Comparable Risk View

Each portfolio company is measured the same way, so you can rank them against each other and see which assets need investment. Coverage, open exposures, and control gaps roll up into a portfolio view that stays current as you buy and sell.

2

Reporting Built for Your Board

Reporting is built around what the firm has to show, including:

- Coverage by portfolio company and service tier
- Open critical exposures by asset
- Incidents detected and time to contain
- Control gaps against your security baseline
- Evidence packs for insurers, auditors, and acquirers

3

A Dedicated Team for the Firm

A Technical Account Manager (TAM) works with the organization, separate from the SOC analysts protecting each portfolio company. They run fund-level reviews, support security diligence on new acquisitions, and coordinate onboarding at close.

Why Private Equity Firms Choose eSentire

"The only way we can sleep at night is to have a partner like eSentire at our side."

Mark Benaquista, Managing Director, Thomas H. Lee Partners

See the full Thomas H. Lee Partners story, including portfolio coverage details and MDR service specifics, in the eSentire MDR for Private Equity datasheet.

2,000+ organizations in **80+** countries | **50+** PE Firms protected plus hundreds of their portfolio companies

25 years of SOC expertise | **MDR Leader**, 2026 IDC MarketScape (Midmarket) and Forrester Wave for MDR

FEATURED CASE STUDY

Thomas H. Lee Partners

35+ portfolio companies

$35B equity capital

4 industry verticals

"We want our management teams to focus on things that are going to move the needle and help the company grow, generate revenue [...] So we bring eSentire in either at close or even sometimes prior to close."

Mark Benaquista, Managing Director

The Challenge

Two people responsible for 35 portfolio companies. No standardized security posture. No in-house security expertise at the portfolio company level. A high-value M&A target with active threat actor interest.

The Outcome

eSentire MDR and CTEM deployed across the portfolio. Standardized threat detection and response at every portfolio company. Unified Managing Director reporting. Portfolio management teams focused on growth while eSentire handles security 24/7.

OUR PORTFOLIO OF SERVICES FOR PRIVATE EQUITY FIRMS

Preempt → Detect → Respond → Adapt → Repeat

One operating model across every portfolio company, delivered by AI operatives and human analysts working, 24/7.

PREEMPT

Autonomous Offensive Security & CTEM

- Recurring adversarial validation that runs continuously
- Attack simulation using real adversary TTPs
- Vulnerability scanning to correlate against existing vulnerabilities across Qualys, Tenable, Rapid7, and Wiz
- External attack surface management (EASM)
- Covers the five-stage CTEM lifecycle
- Security program maturity assessments for pre-close diligence

DETECT

Managed Detection & Response

- 24/7 SOC staffed by human analysts, and AI Operatives, with unlimited threat hunting
- Multi-signal ingestion from any vendor and any stack
- Machine-speed detection and triage, with human review reserved for anything that crosses a high-consequence threshold
- Atlas AIDR extends detection to AI itself, tracking usage, data and agents across each portfolio company
- Threat intelligence from eSentire's Threat Response Unit (TRU) applied to every portfolio company
- Full audit trail for every investigation and action

RESPOND

Controlled Autonomous Response

- AI operative teams: Investigator, Critic, Reporter
- Machine-speed containment with a human on the loop
- Policy-bounded action inside the authority limits each portfolio company set
- Tier-3 analyst validation before any high-consequence action is taken
- Every decision explainable, reversible, and auditable
- Incident response included in every managed contract, with portfolio-wide coverage

Standardize security across your portfolio before the next deal closes.

A dedicated PE team, with same-day response.

Reilly Parker
Director, Private Equity Sales
reilly.parker@esentire.com

Kerry Albert
Principal Solutions Architect
kerry.albert@esentire.com

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSENTIRE

eSentire is a leader in Controlled Autonomy SecOps, protecting 2,000+ organizations across 35+ industries around the world. Founded in 2001, the company's Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire's Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit www.esentire.com and follow @eSentire.