eSENTIRE

ATLAS PLATFORM

Private Equity

One Security Program From Term Sheet to Exit

A portfolio company's risk does not freeze the day a deal closes. It changes as the company grows, and gets tested hardest right before exit, when there is the least room left to fix what diligence missed the first time. Most security programs cover one moment in that timeline: a checklist at close, an annual pen test, a report nobody is funded to act on.

Atlas is eSentire's Controlled Autonomy SecOps platform. It runs one continuous operating model, adversarial testing, 24/7 detection, and machine-speed response, at every portfolio company, from the day a target is identified to the day the fund exits. The program does not reset at each stage. It carries forward.

A TIMELINE THAT NEVER PAUSES

80%
Of PE firms suffered disruption at a portfolio company during the hold period, not just around the deal.
Kroll, Cyber Risk at Scale, 2026

-7 days
Mean time to exploit a new vulnerability. Exploitation now routinely precedes the patch.
Mandiant M-Trends 2026

22 seconds
Median time from initial access to ransomware deployment.
Mandiant M-Trends 2026

One Platform Across Every Stage of the Deal

Atlas runs the same operating model at every portfolio company, mapped to the stage of ownership it is in.

1

PREEMPT
Pre-Close

- Security maturity assessment of the target
- Attack surface mapping before the deal closes
- Findings carry forward into Day One instead of staying in a data room

2

DETECT
Day One

- 24/7 detection live on the existing stack, no rip-and-replace
- Diligence findings become the starting context for monitoring
- Coverage starts when ownership does

3

PREEMPT + DETECT + RESPOND
Hold Period

- Continuous adversarial testing replaces the annual pen test
- Every offensive finding updates detection content automatically
- Machine-speed containment while leadership focuses on growth

4

ADAPT
Exit Ready

- One evidence trail since pre-close, not a report built for the occasion
- Testing, detection, and response history ready for buyer diligence
- The next owner inherits a documented program, not a blank slate

ONE OPERATING MODEL, NOT THREE VENDORS

Preempt → Detect → Respond → Adapt → Repeat

Most security programs buy offense and defense separately. A pen testing firm hands over a report, a separate MDR vendor watches for threats with no knowledge of what that report found. Atlas runs both inside one platform, so every offensive finding becomes defensive coverage automatically.

Preempt

Atlas Preempt tests the environment the way an attacker would: continuous adversarial validation, not an annual snapshot. A pen test gives you a moment in time. Atlas Preempt gives you a feed.

Detect

Every exposure Preempt finds becomes detection content inside Atlas Detect. Atlas watches every signal 24/7 and escalates what it finds to the SOC for validation.

Respond

Confirmed threats are contained at machine speed. Routine actions execute automatically; anything high-consequence is staged for a human analyst to approve first.

Adapt

Every response feeds back into the next round of testing, so the environment retested next week is not the same one that was tested the week before.

43x

Deeper investigation than manual triage

95%

Alignment with senior analyst conclusions

200+

New threat protections added to Atlas daily

BUILT FOR THE MIDDLE GROUND

AI Speed, Human Accountability

Two approaches fail private equity in different ways. Human-speed programs cannot match adversaries who now move from access to ransomware in seconds. Fully autonomous AI systems move fast but remove the judgment a risk committee, an auditor, and a cyber insurer all expect to see. Atlas is built for the space between: agentic AI that runs at machine speed, with every consequential action staged for a human to explain, reverse, or approve.

AI GUARDRAILS

Controlled Autonomy, Built for Portfolio Accountability

Atlas does not act outside the authority envelopes you define. For PE firms, this means each portfolio company controls its own autonomy boundaries: routine containment executes automatically, high-consequence actions require human approval, and every decision is logged, explained, and reversible for board and insurer reporting.

1

Policy-Bounded Authority

Each portfolio company defines what Atlas can probe, act on, and how aggressively. Atlas executes within that envelope, never outside it.

2

Explainability

Every automated action produces a human-readable rationale. Boards, auditors, and cyber insurers see exactly what happened and why.

3

Reversibility

Automated actions can be undone, so a contained host or suspended account is never a one-way door.

4

Staged Approval

High-consequence actions are staged with full investigation context for human sign-off before execution. Confidence without black boxes.

ONE SIGNAL GRAPH, EVERY PORTFOLIO COMPANY

The Same Platform, However Many Companies You Own

Every portfolio company runs on the same underlying platform, so a firm's view of its portfolio is not thirty separate MDR relationships stitched together after the fact. Findings, detections, and response actions live in one continuously updated system from the moment a company is onboarded.

Comparable by Design

Every portfolio company is measured against the same baseline from day one, whether it joined the fund last month or five years ago.

Current as You Buy and Sell

Add a company at close and its data starts flowing immediately. Exit a company and its history stays documented for the buyer's diligence team.

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

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.