eSENTIRE

eSentire for Private Equity

RFP FAQ: What PE Sponsors Ask When Selecting an MDR Partner

Private equity firms are building cybersecurity into every stage of the deal lifecycle, from diligence through exit. This FAQ is meant to help PE firms and their advisors evaluate eSentire against other Managed Detection and Response (MDR) providers, with straight answers to the questions we hear most often from sponsors and portfolio companies.

Why eSentire for Private Equity

Q: Why do private equity firms choose eSentire?

eSentire works with more than 50 private equity firms and their portfolio companies, covering investments with over $7 trillion in combined assets under management. We've been in this business since 2001, and today we run what we call Controlled Autonomy SecOps: an operating model that pairs an AI-driven platform with a 24/7 human SOC to find exposures before attackers do, then detect and stop threats in real time. What sets us apart from generalist MDR providers is a delivery model built specifically for PE: each relationship gets a dedicated coverage team, including a PE relationship director and a dedicated onboarding lead, so portfolio companies get consistent, fast coverage instead of being run through a one-size-fits-all process. It's built around how PE firms operate: fast timelines, many companies at once, and a need to show real, measurable progress at diligence and at exit. Our own Threat Response Unit's (TRU) research into this sector shows why that specialization matters: initial access into PE-backed companies is dominated by valid credentials delivered over email 38.9% of intrusions, and browser-delivered malware, 34.4%.

Q: What makes eSentire different from a typical MDR provider?

Most MDR is reactive: wait for an alert, queue it, investigate, respond, hope it doesn't happen again. Our Atlas Platform runs a continuous loop instead: preempt, detect, respond, adapt, repeat, so every incident makes the next one less likely. AI investigates every signal first, at machine speed, while a 24/7 SOC (with an average analyst tenure of 6 years) validates anything high-consequence before it executes. We prevent initial host compromise in 99.99% of cases, and our mean time to contain, 15 minutes, is written into the contract, not just used in marketing. For a PE firm, Atlas also rolls up individual portfolio company data into a single firm-level view, giving the sponsor real visibility into the breadth and depth of the whole portfolio, not just a stack of separate account reports. The noise reduction behind that can be well over 99% , and in one published example, Atlas AI and our TRU team filtered 48,520 signals down to 17 real findings. On average, Atlas AI engages a new signal in under 30 seconds and assembles full threat context in under 5 minutes.

Q: Can we talk to other PE firms already using eSentire?

Yes. Thomas H. Lee Partners, uses eSentire to protect more than 35 portfolio companies, and their Managing Director has spoken publicly about the partnership and what it's meant for how they manage risk across the portfolio. We're glad to arrange reference conversations with current PE clients as part of your evaluation.

Q: How does eSentire compare to other MDR providers we're likely to see in an RFP?

In an evaluation like this, sponsors typically shortlist us against EDR-vendor-led offerings , broader MSSPs, and other security firms. Our PE-dedicated team is built to protect a portfolio: standardized onboarding measured in weeks, portfolio-wide benchmarking, a dedicated relationship team per sponsor, and reporting designed for a fund-level audience (the IC, the board, an insurer, a buyer), not just a single IT team. We're happy to walk through a side-by-side against whichever providers are in your RFP, backed by reference calls with sponsors who've run the same comparison.

Supporting the Deal Lifecycle

Q: How does eSentire support a deal from diligence through exit?

We fit into a firm's usual process at every stage. Before close, we can assess the baseline of a target acquisition's security, before signatures. At close, we help stabilize the environment on Day 0. During the hold period, we provide 24/7 detection and response, plus continuous offensive testing, to mature the security program. Before exit or an IPO, the same assessments and reporting we've used all along double as evidence for buyers that the program is mature and well established.

Q: Can eSentire assess a target company before a deal closes?

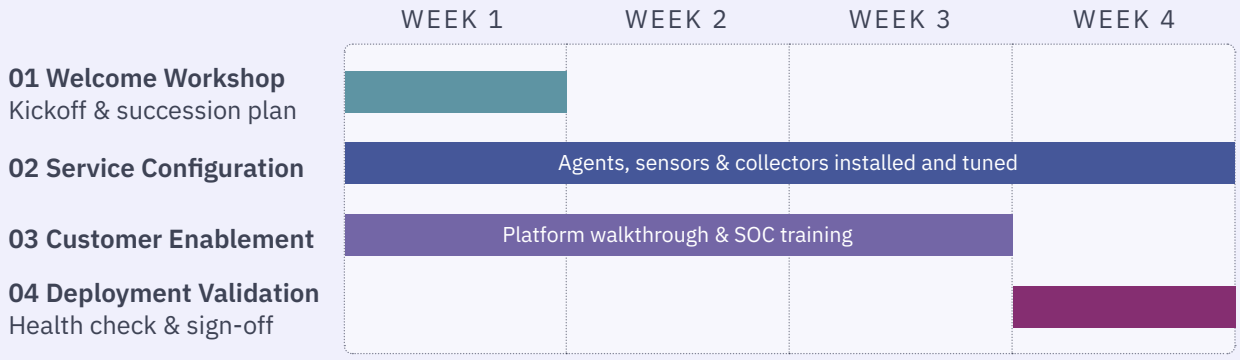
Yes. Before close, we can run a security program assessment against frameworks like NIST CSF, CIS, or ISO, plus a non-intrusive external vulnerability scan and autonomous pentest to simulate an attacker taking aim, as well as a check on the dark web for leaked credentials, exposed services, and any chatter about ransomware groups targeting the company. This greatly helps impact the go or no-go decision and to sets Day 1 priorities for security maturity. Findings are typically shared in hours, not weeks, so they're usable inside the deal timeline instead of arriving after the decision's already been made.

Q: How quickly can a new portfolio company be onboarded?

Deployment averages under 4 weeks from signature to full production, and monitoring starts from the first live signal, not after everything is fully configured. Onboarding runs through four phases: a welcome workshop to set priorities and roles, service configuration and tuning as sensors and collectors come online, customer enablement so your team is comfortable in the platform, and a final deployment validation with a signed-off health report.

eSentire Onboarding — Weeks 1-4

How the four onboarding phases overlap across the first month.



Deployment averages under 4 weeks from signature to full production; monitoring starts from the first live signal.

Q: How does eSentire support cybersecurity diligence for add-on or bolt-on acquisitions during a buy-and-build strategy?

In an evaluation like this, sponsors typically shortlist us against EDR-vendor-led offerings , broader MSSPs, and other security firms. Our PE-dedicated team is built to protect a portfolio: standardized onboarding measured in weeks, portfolio-wide benchmarking, a dedicated relationship team per sponsor, and reporting designed for a fund-level audience (the IC, the board, an insurer, a buyer), not just a single IT team. We're happy to walk through a side-by-side against whichever providers are in your RFP, backed by reference calls with sponsors who've run the same comparison.

Portfolio-Wide Consistency and Visibility

Q: How does eSentire standardize security across a diverse portfolio?

We roll companies out in waves, prioritizing by risk, deal timing, and how complex each environment is, typically 3 to 5 companies at a time using the same playbooks. To hold every company to the same standard, we track a consistent set of KPIs across the whole portfolio: a blended portfolio risk score built from exposure, control maturity, threat activity, and response readiness; coverage health, meaning percentage of telemetry connected and EDR deployment rate; threat and SLA performance, including mean time to detect and time to contain; and benchmarking against portfolio and peer medians. That gives every company, whether it's been with us for years or was acquired last quarter, a comparable scorecard instead of a one-off report.

Q: What visibility does the PE firm get across its portfolio?

Through the Atlas Platform, sponsors get one comparable view across every portfolio company: coverage, open exposures, incidents and time to contain, and control gaps against a common baseline. Reporting is built to be board-ready, with evidence packs sponsors can hand to insurers, auditors, or acquirers. A dedicated Technical Account Manager runs fund-level reviews and supports security diligence on new acquisitions, backed by monthly or quarterly portfolio reviews, so the investment team stays informed without hiring for it.

Q: Do portfolio companies contract directly with eSentire, or does the firm hold one master agreement?

Each portfolio company signs its own contract with eSentire, so there's clear accountability and service tailored to that business. If the PE firm needs specific language built into the portfolio company contracts, such as reporting requirements or standard terms, we can do that. At the same time, the sponsor gets the benefits of scale: portfolio pricing, faster onboarding, a dedicated support team, and shared threat intelligence across the group.

Q: How does eSentire support LP reporting or operational due diligence (ODD) questionnaires about portfolio cybersecurity?

LPs and their ODD consultants are asking GPs more direct questions about portfolio-wide cyber risk, not just individual portfolio company practices. We can provide the sponsor with fund-level summaries, aggregated coverage and maturity metrics, and supporting documentation (assessment history, incident history, control evidence) formatted for inclusion in an ODD response or LPA-related disclosure, without exposing portfolio company-specific detail the sponsor isn't ready to share. This is typically coordinated through the dedicated Technical Account Manager alongside the regular portfolio reviews.

Q: Can eSentire help quantify cyber risk in financial terms for an investment committee or board?

Yes. The blended portfolio risk score already tracked for benchmarking (exposure, control maturity, threat activity, noise reduction, response readiness) can be paired with a financial risk quantification approach to translate technical findings into a dollar range for the IC or board, useful when justifying security spend, comparing a target's residual risk during diligence, or explaining why a control gap matters beyond a checklist. That turns "we found 12 critical vulnerabilities" into a number an IC can act on.

Services and Coverage

Q: What does eSentire's MDR service cover?

Coverage spans network, endpoint, cloud, log, email, browser, identity, and AI, all fused together by AI investigation and backed by a 24/7 SOC. We work with what the portfolio company already runs, including CrowdStrike, SentinelOne, Microsoft Defender, Palo Alto Cortex, Okta, and most major firewall and cloud platforms, so nobody needs to rip out what they've already paid for.

Q: What if a portfolio company already has security tools in place?

That's normal. We're not tied to one vendor; we connect to any technology integration. We can manage a company's existing tools, integrate your SIEM signal (whether that's Splunk, Sumo Logic or other), or fill gaps with our own platform where needed. The goal is consistent protection and comparable reporting across the portfolio, not forcing every company onto the same stack. That matters more in PE than almost anywhere else: a portfolio of 30 companies often means 30 different security stacks, and funding 30 parallel projects just to get comparable coverage is not feasible.

Q: Does eSentire test a portfolio company's defenses before an attacker does?

Yes, and it's built into the platform rather than sold as a separate service. We run continuous offensive testing, including AI-led penetration testing, attack surface discovery, vulnerability scanning, and dark web and digital risk monitoring, so gaps get found and turned directly into detection coverage, or fixes instead of sitting in a PDF report nobody has time to act on.

Q: How does eSentire support incident response and ransomware readiness?

Incident response is included in every managed contract. Beyond that baseline, our Digital Forensics and Incident Response team offers a 24/7 hotline with a threat suppression guarantee, covering remote triage, full recovery, digital forensics, and coordination with legal teams and cyber insurance carriers. We also help portfolio companies prepare before anything happens, through tabletop exercises and incident response plan development.

AI, Governance, and Oversight

Q: How does eSentire balance AI speed with human oversight?

Routine, low-risk actions, like isolating a compromised host, happen automatically at machine speed. Anything high-consequence gets staged for a human analyst to approve first, with full context: what was found, the risk score, and a rollback plan. Every action is explainable, reversible, and logged, which is the kind of governance boards, auditors, and insurers ask about. Each portfolio company also sets its own limits on what's allowed to run autonomously versus what needs a human sign-off.

Q: Does eSentire monitor how portfolio companies use AI tools themselves?

Yes, AIDR is a newer part of the platform. As portfolio companies adopt tools like Claude, Copilot or other AI assistants, we can provide visibility into that usage, tied to identity, so a company knows what data is being used and what's being asked, and can enforce policy on the accounts those tools operate under, without blocking adoption outright.

Q: Does eSentire train its AI models on customer data, and how is data kept separate between portfolio companies?

Each portfolio company's telemetry and findings are logically segregated and used only to protect that company, and, in aggregate and anonymized form, to inform the portfolio-level benchmarking a sponsor sees.

Pricing and Contracts

Q: How is pricing structured?

We package services into three tiers, Atlas Professional, Atlas Enhanced, and Atlas Elite, each adding more coverage and advisory support than the last. Add-ons like AIDR, Vulnerability & Exposure Management, and additional penetration testing are priced separately. Exact pricing depends on company size and scope, and portfolio companies benefit from the sponsor's overall scale through preferred rates, confirmed during scoping.

Q: What contract terms and portfolio incentives are available?

We offer multi-year contract options with volume-based discounts, and portfolio companies benefit from pre-negotiated terms and conditions that streamline legal review. Each company still works out terms suited to its own size and needs, so speed doesn't come at the cost of fit.

Q: Does eSentire work directly with insurance brokers and carriers to streamline underwriting for portfolio companies?

Yes. We regularly work alongside brokers and carriers during underwriting and renewal, providing the evidence a carrier wants to see: control attestations, incident history, and a summary of the monitoring and response capability in place, so a portfolio company doesn't have to translate our reporting into insurer language itself. For a sponsor managing renewals across several portfolio companies at once, that consistency can also support a more coordinated conversation with brokers at the portfolio level.

Compliance, Global Reach, and Exit Readiness

Q: What compliance and regulatory frameworks does eSentire support?

We regularly support companies against NIST CSF, ISO 27001, SOC 2, PCI DSS, HIPAA, GDPR, and CMMC, among others. In practice, that means putting in place the controls (24/7 monitoring, endpoint detection, identity monitoring, log retention, and a documented incident response process) that auditors and regulators want to see as evidence.

Q: Does eSentire help meet SEC cybersecurity requirements for registered investment advisers?

Yes. The SEC's cybersecurity risk management rules for RIAs, investment companies, and business development companies call for formal policies and procedures, 24/7 threat detection and response, and timely disclosure of material incidents. Our MDR and incident response services are built to support exactly those requirements, and we publish a dedicated checklist for GPs and RIAs working through what the rule asks for.

Q: How can we verify eSentire's own security and compliance posture?

eSentire maintains a public Trust Portal where prospects and customers can review our security practices, certifications, and compliance documentation directly, rather than taking our word for it. We're also glad to complete a standard vendor security questionnaire as part of your due diligence process.

Q: Can eSentire support a global or multi-region portfolio?

Yes. eSentire protects over 2,000 organizations in more than 80 countries, with a 24/7 SOC model out of Waterloo, Ontario and Cork, Ireland, support for different time zones and languages per company, and regional data storage options, such as the US, Canada, or EU, to meet local rules.

Q: How does this help with cyber insurance and exit readiness?

Our MDR services are built to meet the requirements insurers typically ask for, which helps portfolio companies get and keep the right coverage. Independent claims research has ranked endpoint detection and response among the most effective controls for reducing claim likelihood, and that's core to what we deploy. At exit, the same assessments and documentation used through the hold period double as proof for buyers that the security program is mature and well run.

Q: If a portfolio company is divested or switches providers, what happens to its data, logs, and historical findings?

The portfolio company owns its data. At offboarding, we support an orderly transition, exporting historical findings, assessment reports, and log data in a usable format for the incoming provider or the acquiring owner, so the security history built up over the hold period isn't lost right when a buyer wants to see it.

This FAQ is a general reference for evaluating eSentire's fit for a private equity portfolio. Exact SLAs, pricing, and scope are confirmed for each portfolio company during scoping and contracting.

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.