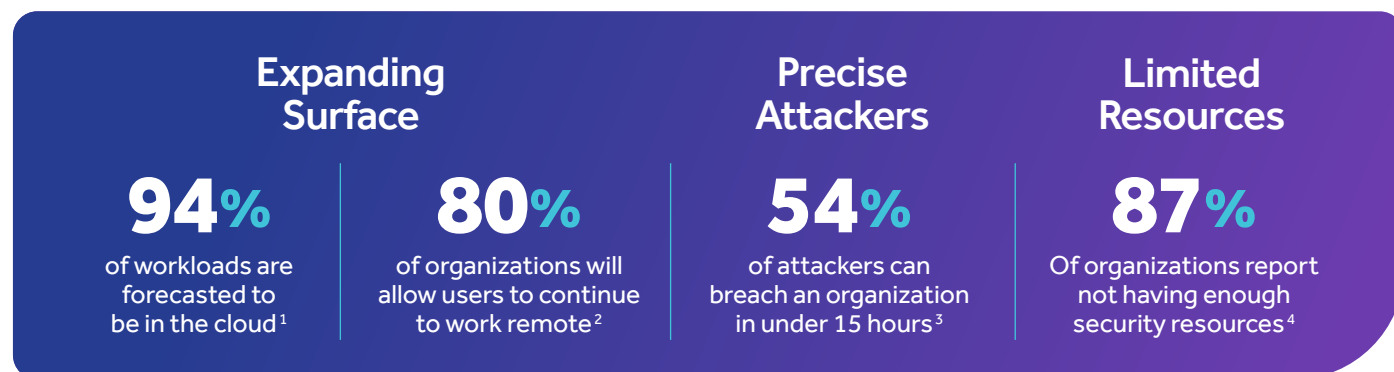


24/7 Managed Detection and Response For Private Equity Firms

Securing Private Equity Firms and their Portfolio Companies with Managed Detection and Response Services that Scale

Cloud adoption, business applications and remote users are expanding at an exponential rate as your firm continues to scale and invest in additional companies. It's unrealistic for your security team to keep pace with your digital transformation requirements and the growing attack surface you're faced with.



Operating with increasing speed and precision, attackers are forcing all organizations to implement preventative controls with advanced detection and response capabilities. eSentire's Managed Detection and Response service has been specifically designed to rapidly identify and contain advanced threats.

Introducing eSentire

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry - financial services. Over the last two decades we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers, hundreds of cyber experts, and 1500+ customers, across 80+ countries, we have demonstrated the ability to Own the R in MDR with a Mean Time to Contain of 15 minutes. While many companies focus on detection, we recognize that there is no end to cyber risk. Preventative technologies will be bypassed and defenses will fail. That's why eSentire prioritizes Response. Our MDR is really MDR³ - Response, Remediation and Results.

We proudly protect over 100 Private Equity firms and their portfolio companies. We would welcome the opportunity to outline how we can help defend your firm, and develop a custom security offering for your entire portfolio to subscribe to.

¹ CISCO Global Cloud Index, ² Gartner HR Survey 2020, ³ Nuix Black Report, ⁴ 451 Research

How eSentire Managed Detection and Response Can Help

With eSentire you should expect detection in seconds, and containment in minutes. Our difference drives your results.

Multi-Signal Ingestion - At eSentire, we believe a multi-signal approach is paramount to protecting your complete attack surface. Whether your environment is in the cloud, on-premises or somewhere in between we have the visibility to see what others MDR providers will miss. As part of eSentire MDR we normalize and correlate data to monitor your entire attack surface, enabling effective investigation and unparalleled response capabilities. Our multi-signal coverage includes network, endpoint, log, cloud, vulnerability scans and behavioral sources.

SOC as a Service with 24/7 Threat Hunting - Our global 24/7 SOC's are staffed with Elite Threat Hunters and experienced Cyber Analysts with CISSP and OSCP accreditations. Because the eSentire Atlas XDR Cloud Platform leverages automation, orchestration and machine learning to filter out high fidelity threats, our SOC teams can focus on responding to high priority security events. They drive human-led investigations to hunt and contain known and unknown threats. Our SOC as a Service is supported by eSentire's industry renowned Threat Response Unit (TRU), delivering threat analysis, intelligence and tactical threat response.

Security That Scales with Atlas XDR Platform - Our scalable, distributed XDR Cloud Platform ingests and analyzes massive amounts of data from signals across our customer base. We offer reliability, redundancy and flexibility to scale with your growing data and business needs. Atlas XDR filters out high fidelity threats, recognizing malicious IOCs and IPs that can be automatically disrupted and contained. That way, our SOC and Elite Threat Hunters spend their time on higher priority security events. If an orchestrated response isn't possible, Atlas XDR equips our cyber experts with the insights and tools they need to perform deep investigation and execute manual containment, when required, in minutes.

Proactive Security Network Effects - Atlas XDR leverages patented artificial intelligence and scalable machine learning to process all the threat signals across our global client base, making the eSentire proactive Security Network Effects possible. When Atlas XDR detects a threat it automatically responds, and pushes new detection and containment knowledge to every eSentire client. Plus, eSentire Atlas is always learning, and improving. There are 12,000+ indicators recognized across our eSentire Atlas XDR Platform and we add 400 on average every day to continue to harden your defenses. When you consider our growing network of Private Equity firms, that means you are benefiting from hundreds of industry-specific investigations and threat hunts every day.

Unmatched Experience and Expertise - When you engage with us, you are part of Team eSentire from Day 1, which means you're joining forces with experienced cybersecurity veterans, Elite Threat Hunters, and industry-renowned threat research experts. We help fill your cyber skills gap and act as a true extension of your team. We all have a role to play in keeping your business secure. Team eSentire includes:

- **Cyber Risk Advisor** - Your named security advisor who prioritizes your business risk reduction and drives results for your security program. .
- **24/7 SOC Cyber Analysts and Elite Threat Hunters** - Cyber experts who monitor your environment around the clock to hunt, contain and respond to threats. Available live anytime and every time you need it most.
- **Threat Response Unit Experts** - Industry-renowned experts who drive original research, threat intelligence and threat analysis to embolden eSentire response capabilities and tools.

How We Deliver

Our team doesn't drown you in alerts, we go beyond other MDR providers to drive results. We support your cyber program with a combination of cutting-edge machine learning XDR technology, 24/7 Threat Hunting expertise and security operations leadership to mitigate your business risk, enable security at scale and drive your cyber program forward.

eSentire Atlas XDR Cloud Platform: The industry's most advanced XDR Cloud Platform offers unmatched visibility, and employs patented machine learning to detect and respond to the most elusive threats in real time. Atlas cuts the noise to our SOC and your team by automatically disrupting 3M+ threats per day, stopping breaches before they disrupt your business. Our platform learns with each detection, correlating and amplifying data across our global customer base hundreds of times each day to deliver proactive security network effects that harden your defenses.

24/7 Security Expertise: Filtering suspicious activity requires human intuition. Our Security Operations Centers are staffed 24/7 with Cyber Analysts and Elite Threat Hunters who provide rapid investigation and response. Plus as part of Team eSentire you're supported by a named Cyber Risk Advisor from Day 1.

Security Operations Leadership: Effective and efficient analysis, investigation, escalation and response refined over a two-decade history of delivering managed detection and response services to high value targets.

eSentire MDR features include:

- | | |
|--|---|
| ✓ 24/7 Always-on Monitoring | ✓ 5 Machine Learning patents for threat detection and data transfer |
| ✓ 24/7 Live SOC Cyber Analyst Support | ✓ Detection of unknown attacks using behavioral analytics |
| ✓ 24/7 Threat Hunting | ✓ Rapid human-led investigations |
| ✓ 24/7 Threat Disruption and Containment Support | ✓ Threat containment and remediation |
| ✓ Mean Time to Contain: 15 minutes | ✓ Detailed escalations with analysis and security recommendations |
| ✓ Machine Learning XDR Cloud Platform | ✓ eSentire Insight Portal access and real-time visualizations |
| ✓ Multi-signal Coverage and Visibility | ✓ Threat Advisories, Threat Research and Thought Leadership |
| ✓ Automated Detections with Signatures, IOCs and IPs | ✓ Operational Reporting and Peer Coverage Comparisons |
| ✓ Security Network Effects | ✓ Named Cyber Risk Advisor |
| ✓ Detections mapped to MITRE ATT&CK Framework | ✓ Business Reviews and Strategic Continuous Improvement planning |

Why Multi-Signal Matters

eSentire MDR means multi-signal telemetry and complete response. We provide comprehensive visibility across your layered attack surface, delivering rapid correlation, deep investigations, and multiple points of contextual awareness & response. Our signal sources and coverage include:



Network - Block malicious IPs, brute force attacks, active intrusions and unauthorized scans



Endpoint - Host isolation to protect other assets from ransomware, trojans and more



Email - Social engineering and phishing investigation, control and retroactive deletion



Identity - Stops compromised user and insider threats with cloud active directory response



Log - Critical visibility and context from your existing security controls and network infrastructure



Cloud - Configuration escalations, policy & posture management across multi-cloud environments



Managed Vulnerability Service - Configuration escalations, policy & posture management across multi-cloud environments

Customer Success

eSentire has a long track record of providing complete, continuous protection that benefits our customers. We have a 92 percent customer retention rate and are proud to confirm our Net Promoter Score of 73. We also track overall project and service satisfaction scores. Our most recent annual customer satisfaction scores demonstrate our commitment to service excellence and continuous improvement in everything we do. Highlights include:

100%

deployment
satisfaction

99%

ongoing operations and
tuning satisfaction

99%

threat detection and
response satisfaction

98%

Security Operations
Center Satisfaction

97%

Overall improvement in
Security Posture

98%

Better protection from
potential business disruption

We believe in transparency and expert level innovation in everything we do. As an eSentire customer you can expect:

- ◆ Regular Threat Advisories on urgent industry activities and emerging threats
- ◆ Thought Leadership including original research, white papers, reports and more to share our security perspective
- ◆ Peer Led Conversations and Events including webinars, in person roundtables and regular fireside chats to drive collaboration and information sharing across our customer base
- ◆ Operational reporting sharing critical insights, and driving security roadmap planning

Additional eSentire Security Services

In addition to Managed Detection and Response, eSentire offers comprehensive security services to support your firm and portfolio companies end-to-end as we stop breaches, simplify security and minimize your business risk.

Additional services include:

- ◆ **Managed Vulnerability Services** - Continuously assess and accurately identify vulnerabilities across your organization's traditional and dynamic IT assets including mobile devices, IoT and virtual machines with a cloud-based scanning cadence. We prioritize and remediate the vulnerabilities in your business-critical assets, whether on-premises or in the cloud.
- ◆ **Managed Risk Services** - Strategic services including Security Assessments, Managed Phishing and Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.
- ◆ **Digital Forensics and Incident Response** - Battle-tested Incident Commander level expertise driving incident response, remediation, recovery, and root cause analysis. Emergency IR services and Incident Response retainer offering available.
- ◆ **Virtual CISO** - Industry certified professionals with decades of experience form the C level to technical implementation roles. Our vCISO team members can be dedicated to your organization to provide security assessments, security strategy, executive briefings, quarterly health checks and drive continuous security maturity.

We can customize a package for your portfolio companies to create a baseline of security requirements that each acquisition should adhere to.

eSentire in Action



"It's to the point where one of the first things my managing partners say after we close a deal is - when are we going to bring in eSentire?"

CIO, Private Equity

- ◆ North American PE Firm focused on manufacturing and industrial services
- ◆ Partnership began with eSentire providing MDR services to just the firm
- ◆ A serious breach at one of their portfolio companies led to rollout of eSentire services across the portfolio
- ◆ eSentire is typically heavily involved in the 100 day post-acquisition plan, mitigating cyber risk during the transition period
- ◆ Enables the firm to be "consistently proactive" about security across their portfolio companies
- ◆ For exiting portfolio companies, all MDR services are transferrable

Why Private Equity Firms Choose eSentire

There is no end to Cyber Risk so go into battle with the best...

- ◆ **Recognized** - The Authority in Managed Detection and Response
- ◆ **Simple** - We absorb the complexity of cybersecurity so you can prioritize your operations
- ◆ **Scalable** - Industry's most powerful machine learning XDR Cloud Platform can ingest data at the pace and scale of your business
- ◆ **Precise** - We're on the cutting-edge of attacker Tactics, Techniques and Procedures mitigating your risk of being breached
- ◆ **Fast** - Extreme time to value as you will be fully operational within weeks
- ◆ **Responsive** - We own the R in MDR to provide extensive response capabilities and threat hunting around the clock
- ◆ **Cost-Effective** - 24/7 threat protection, detection and response at a fraction of the cost of DIY security programs
- ◆ **Complete** - Multi Signal Coverage and comprehensive security services support
- ◆ **Team** - Cyber Risk Advisor + SOC Cyber Analyst and Elite Threat Hunters on guard for your business 24/7

- ◆ **Results** - Your firm and portfolio companies can expect:
 - ~50% reduction in threat detection and response total cost of ownership (TCO)
 - +50% additional coverage on top of commodity threat intelligence, leveraging proprietary technology and our Private Equity network of customers
 - 99% reduction in threat detection and containment times from global averages

Certified



Mapped



Awarded



\$6.5T+

Total ALUM

1500+

Customers in 80+ Countries

20.5M

Daily Signals Ingested

3M

Daily Atlas XDR
Automated Disruptions

6000

Daily Human-led
Investigations

700

Daily Escalations

400

Daily Threat Containments

15min

Mean Time to Contain

Ready to get Started? Connect With Team eSentire

Reilly Parker

Strategic Sales Manager, Private Equity

Email: Reilly.Parker@esentire.com

Mobile: 925.918.2620

Kerry Albert

Sr. Solutions Engineer

Email: kerry.albert@esentire.com

Mobile: 240.483.9636

Grace Carter

Account Executive, Private Equity

Email: grace.carter@esentire.com

Mobile: 314.368.5289

Phil Battaglia

Regional Vice President – Sales

Email: phil.battaglia@esentire.com

Mobile: 281.216.4383

If you're experiencing a security incident or breach contact us  1-866-579-2200

eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1500+ organizations in 80+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow @eSentire.