





Managed Detection and Response

 <p>Multi-Signal Ingestion</p> <p>Gain full threat visibility, deep correlation and investigation capabilities, strengthening our time to contain and complete response.</p>	 <p>24/7 Threat Hunting</p> <p>Zero-Trust approach to hunt elusive attackers. Proactive and automated blocks of malicious intent plus 24/7 Elite Threat Hunting support.</p>	 <p>Atlas XDR Cloud Platform</p> <p>Rapid detection and automated threat disruption at scale. Delivers Security Network Effects to harden your defenses with every detection globally.</p>	 <p>Rapid, Robust Response</p> <p>Minimize attacker dwell time with Mean Time to Contain of 15 minutes. We disrupt, isolate and contain threats before they impact your business operations.</p>
--	--	---	--

Cloud adoption, business applications and remote users continue to expand at exponential rates. Your cybersecurity team is fighting a losing battle to keep pace with your business requirements and growing attack surface. While traditional security controls and MSSPs were once effective, they are no match for the growing speed and sophistication of modern threats.

<p>Expanding Surface</p> <p>94%</p> <p>of workloads are forecasted to be in the cloud¹</p>	<p>80%</p> <p>of organizations will allow users to continue to work remote²</p>	<p>Precise Attackers</p> <p>54%</p> <p>of attackers can breach an organization in under 15 hours³</p>	<p>Limited Resources</p> <p>87%</p> <p>Of organizations report not having enough security resources⁴</p>
---	---	--	---

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, across 35 industries, from known and unknown cyber threats. Team eSentire's mission is to hunt, investigate and stop cyber threats before they become business disrupting events.

¹ CISCO Global Cloud Index, ²Gartner HR Survey 2020, ³Nuix Black Report, ⁴451 Research

How it works

We support your cyber program with a combination of cutting-edge machine learning XDR technology, threat hunting expertise and security operations leadership to mitigate your business risk, enable security at scale and drive your cyber program forward.

Machine: Powerful XDR Platform

The eSentire Atlas XDR Cloud Platform offers unmatched visibility and employs patented machine learning to detect and to respond to threats in real time.

Team: 24/7 Security Expertise

When an automated response isn't possible our 24/7 SOC and Elite Threat Hunting team are engaged as an extension of your team, to investigate and provide rapid manual containment and threat disruption.

Operations: Proven Processes

Effective and efficient analysis, investigation, escalation and response processes refined over a two-decade history of delivering Managed Detection and Response to high-value targets.

Multi-Signal MDR

At eSentire we believe a multi-signal approach is paramount to protecting your complete attack surface. We ingest network, endpoint, log, cloud, insider and vulnerability data to enable complete attack surface visibility, and drive deeper investigations, in order to strengthen the speed and completeness of our response capability. We correlate indicators of compromise and early detections between multiple signals, and our 24/7 SOC Analysts and Elite Threat Hunters quickly investigate, contain, and enforce response actions against advanced persistent threats that bypass traditional security measures.

- **Network** - Defend brute force attacks, active intrusions and unauthorized scans
- **Endpoint** - Protect assets from ransomware, trojans, rootkits and more
- **Log** - Intelligence and visibility across AWS, O365, GCP, DevOps and more
- **Cloud** - Configuration escalations, policy & posture management
- **Insider Threat** - Detects malicious insider behavior leveraging Machine Learning models

Whether your environment is in the cloud, on-premises or somewhere in between we have the visibility to see what other MDR providers will miss.

Features

Not All MDR is Created Equal. eSentire Managed Detection and Response includes:

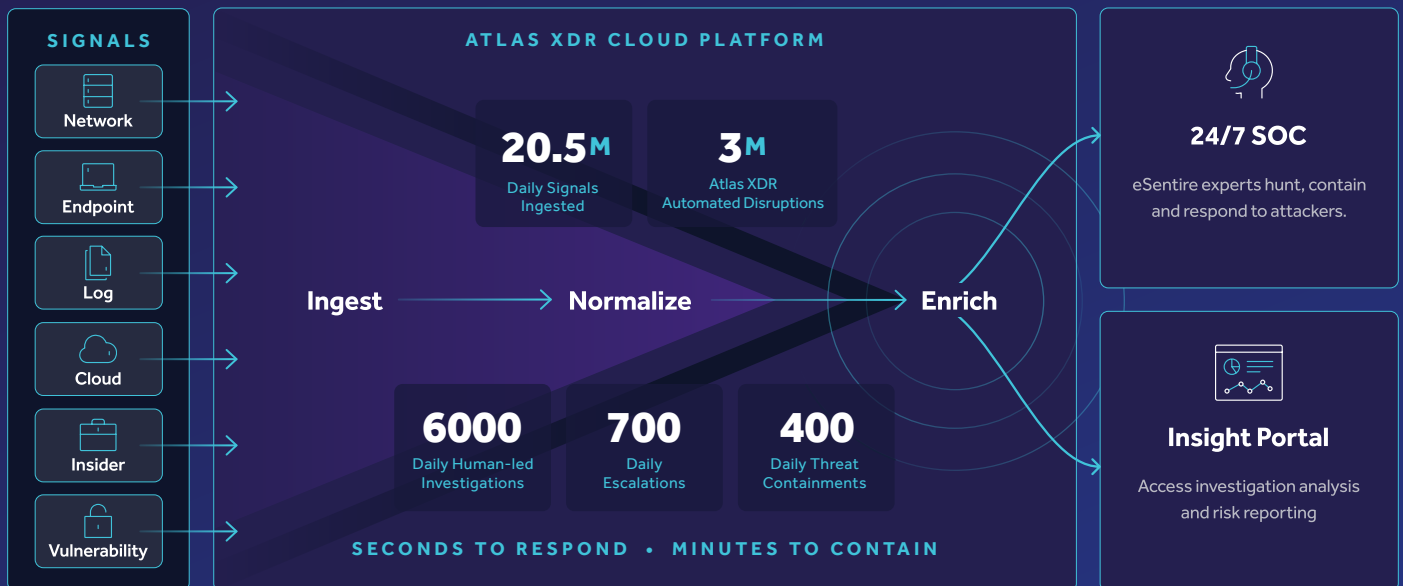
- ✓ 24/7 Always-on Monitoring
- ✓ 24/7 Live SOC Cyber Analyst Support
- ✓ 24/7 Threat Hunting
- ✓ 24/7 Threat Disruption and Containment Support
- ✓ Mean Time to Contain: 15 minutes
- ✓ Machine Learning XDR Cloud Platform
- ✓ Multi-signal Coverage and Visibility
- ✓ Automated Detections with Signatures,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

eSentire MDR is powered by Atlas XDR

Without a comprehensive, cloud-native XDR platform with adaptive machine learning, MDR services can't monitor the whole threat surface, can't make sense of the overwhelming volume of threat signals and can't respond fast enough to stop skilled attackers.

At eSentire, we're proud to be pioneers in delivering effective, efficient and scalable cybersecurity solutions. We were the first MDR vendor to introduce a cloud-native XDR platform—Atlas—providing security, reliability and redundancy at scale and on demand, so our services can grow with your business. It's not a bolt-on or add on, the Atlas XDR platform is at the core of eSentire MDR.

- Cloud-native architecture
- Proprietary Machine Learning models
- Artificial Intelligence threat hunting pattern recognition
- Multi-Signal Ingestion
- Extensive Automated Response Capabilities
- Security Network Effects at Scale



With Team eSentire, you're protected by the best in the business from Day 1.

Your named Cyber Risk Advisor prioritizes your business risk reduction and drives results for your security program. In addition you also have 24/7 access to our:

- **Security Operations Center Cyber Analysts** - Monitor your signals around the clock and are available anytime and every time for a live discussion when you need it most
- **Elite Threat Hunters** - Provide 24/7 Threat Hunting support to rapidly detect and contain attacks that bypass your security controls, accounting for the latest threat actor tactics, techniques and procedures
- **Threat Response Unit (TRU)** - Delivering threat intelligence, security research, and content models to help our SOC and overall service stay ahead of the threat curve

What's being said about eSentire



eSentire goes beyond the market's capability in Managed Detection and Response, providing M&C Saatchi with unmatched speed to resolution of security events, and deep threat hunting expertise. We have gained visibility into attacks against our infrastructure and I have peace of mind knowing that we are defended 24/7. eSentire has helped shape our security defense and helped us improve our cyber resiliency.

- Neil Waugh, Chief Information Officer, M&C Saatchi

The eSentire difference

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

- ◆ Recognized globally as the Authority in Managed Detection and Response
- ◆ Industry's most powerful machine learning XDR Cloud Platform
- ◆ Threat Hunting done right - 24/7
- ◆ End-to-end Risk Management
- ◆ Flexible pricing and multiple service tiers that fit your business
- ◆ Team eSentire - Cyber Risk Advisor + SOC Cyber Analyst and Elite Threat Hunters on guard for your business 24/7

Certified



Mapped



Awarded



\$6.5T+
Total AUM

1200+
Customers in 75+ 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

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

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ 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.