eSENTIRE

DATA SHEET

Managed Detection and Response

Combine AI-driven security operations, multi-signal attack surface coverage and 24/7 Elite Threat Hunters to help you take your security program to the next level.

Full Threat Visibility & Investigation

Get multi-signal threat intelligence enabling deeper correlation and threat investigation capabilities, proven to contain threats faster.

24/7 Threat Hunting & Disruption

Gain continuous protection from our SOC Cyber Analysts and Elite Threat Hunters who rapidly investigate, contain, and shut down threats when an automated response isn't possible.

AI-Driven SecOps Platform Empowering Human Experts

Atlas AI empowers our analysts to operate swiftly and accurately at a scale humans alone can't match. We don't offer black box AI; just transparent, expert-backed protection you can trust.

Rapid, Robust Response

Disrupt, isolate, and stop threats with a Mean Time to Contain of less than 15 minutes. We detect in seconds and contain in minutes, so your business is never disrupted.

Original Threat Intelligence

Hunt the most advanced undetected threats with original threat research, curated threat intelligence and new detection models built by our world-class Threat Response Unit (TRU).

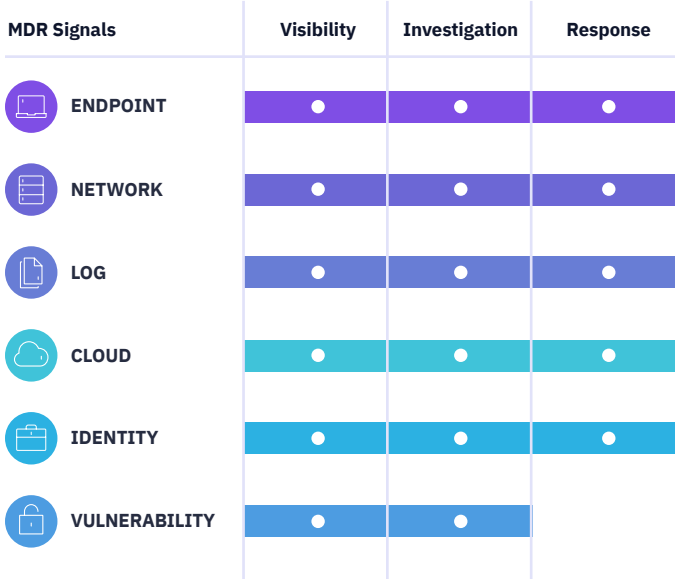
ALL-IN-ONE MDR SERVICE

Don't Settle for Partial Security. Multi-Signal Matters.

At eSentire, we believe a multi-signal approach is paramount to protecting your complete attack surface. eSentire's MDR solution means multi-signal telemetry and complete response.

Our all-in-one MDR solution ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. The Atlas XDR platform provides automated blocking capabilities to prevent attackers from gaining an initial foothold while our expert Elite Threat Hunters initiate human-led threat investigation and containment at multiple levels of the attack surface.

Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level.



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 Models and Novel Detection Runbooks
- Atlas XDR Platform
- Multi-signal Coverage and Visibility
- Automated Detections with Signatures, IOCs and IPs
- eSentire Predictive Threat Defense Network Anticipates Emerging Threats
- Detections Mapped to MITRE ATT&CK Framework
- 5 Machine Learning Patents for Threat Detection and Network Traffic Disruption
- Detection of Unknown Attacks Using Behavioral Analytics
- Rapid Human-led Threat 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

Seamless Integration and Threat Investigation Across Your Existing Tech Stack

eSentire MDR service integrates seamlessly with the existing tools and SaaS platforms in your environment to enable continuous monitoring across your hybrid footprint, ingestion of high-fidelity data sources, and 24/7 protection from sophisticated known and unknown cyber threats with proactive threat hunts. We continuously expand our multi-signal ingestion capabilities by adding new detections and runbooks for SaaS platforms and enterprise applications. When suspicious activity is detected, we stitch together context-free telemetry to identify similar attacker tactics in your environment.

Our 24/7 SOC Cyber Analysts respond on your behalf to counter threat actor Tactics, Techniques, and Procedures (TTPs) by leveraging common security infrastructure and tools (including, but not limited to):

- EDR/EPP tools
- Network security technology
- Email security platforms
- VPN providers
- Web gateway solutions
- Identity providers

CLOUD INFRASTRUCTURE

Google Cloud · Azure · aws

CLOUD APPLICATIONS

Google Workspace · Azure

SAAS PLATFORMS AND SECURITY INFRASTRUCTURE

CROWDSTRIKE · Microsoft · SentinelOne · LACEWORK · eSENTIRE · sumo logic · tenable · Barracuda · CloudGuard SaaS · citrix · CISCO · Dropbox · DUO · f5 · FORTINET · mimecast · okta · paloalto · salesforce · proofpoint · slack · Gmail · TREND MICRO · SOPHOS · zscaler · Qualys.

Security Operations Built on Expert AI

Protect What's Next

eSentire Atlas AI isn't another automation script or task eliminator. It's a multi-agent Generative AI system purpose-built and embedded across eSentire's Atlas AI Security Operations Platform to scale human expertise — trained on real-world workflows validated by investigations across 2,000+ customers globally.

Atlas AI is fully embedded into our platform and included as part of your MDR service. Designed to scale human expertise, not replace it, Atlas AI gives your security operation a competitive edge by providing transparency, context and validation previously unattainable in minutes.

We show up and prove results:

- **35%** faster threat intelligence vs commercial feeds
- **99%** noise reduction across customer environments
- **95%** SOC expert alignment with Atlas AI investigations
- **99.3%** of threats isolated at the first host
- **200** new threat protections added per day to harden customer defenses
- **43X** investigation acceleration with 5 hours of investigation work achieved in less than 7 minutes
- **96%** SOC analyst retention, with an average tenure of 6 years

Benefit from our Predictive Threat Defense Network with the eSentire Atlas XDR Platform

Leveraging patented machine learning models and artificial intelligence pattern recognition, our Atlas XDR Platform learns across our global customer base and extends security network effects, so every customer benefits with each new threat detection. We add 200+ IPs and IOCs per day to our global block list based on positive SOC investigations.

eSentire MDR is More Than Just Alerts

The World's Most Complete Threat Response Capability

When it comes to response, it's how we do it that makes all the difference. To build a more resilient security operation, you need an MDR solution provider who has your back from Day 1.

RESPONSE SPEED

The Atlas Platform instantly detects and blocks millions of threats per day. We add 200+ IPs & IOCs per day to our block list based on positive SOC investigations.

When human intuition is required, we are on guard 24/7 to protect you with a Mean Time to Contain of only 15 minutes.

RESPONSE EXPERTISE

We take threat response seriously by containing and remediating cyber threats on your behalf, so your business continues to run smoothly.

Plus, majority of our customers have less than 2 in-house resources to support their security operations so eSentire becomes a trusted extension of their team.

RESPONSE COVERAGE

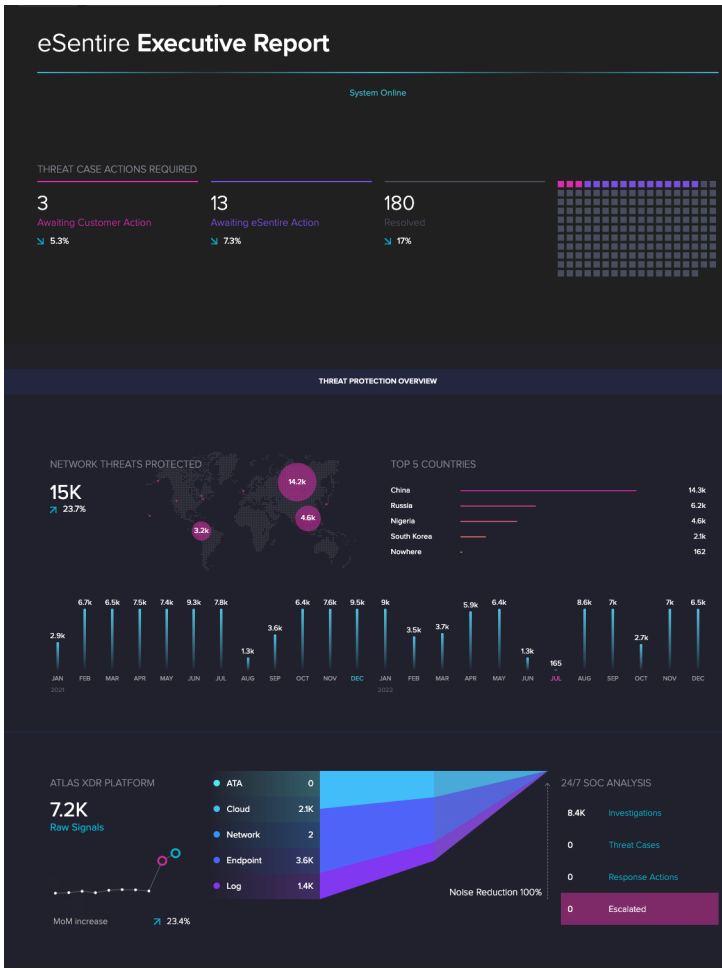
Get continuous protection across your entire attack surface. Whenever and wherever a new cyber threat is detected, we'll always respond to protect you.

Our global SOCs are home to the industry's only 24/7 threat hunters and with our unique multi-signal intelligence, you can remain confident that your defenses are always one step ahead.

The Atlas Customer Portal

Your gateway into the eSentire XDR Platform and an experience you can trust. You see what our SOC sees, can review our investigations and always understand how we are protecting your business.

- Get full transparency into the health of your environment and how we protect your critical assets from advanced cyber threats.
- Understand how your eSentire MDR services are proactively protecting you against emerging threats and helping you build cyber resilience.
- Compare your threat environment against your peers and global threat trends with total visibility into which assets are impacted by exploitable vulnerabilities.
- Assess the performance of your critical KPIs to compare your organization's cyber resilience over time against your industry peers as well as our global customer base, with easy exports so you can present findings to your leadership and board.
- Real-time visibility into what our SOC is actioning to help you stay informed about security incidents and emerging threats.
- Monitor, manage, and respond to security threats in real-time, directly from your mobile device, no matter where you are, with the eSentire Mobile App.



The eSentire Difference

Build Resilience. Prevent Disruption.

- **AI-Driven Security Operations Platform** - Our multi-agent Generative AI system is embedded across the Atlas Security Operations Platform to empower human experts that protect your complete attack surface.
- **Service Capability** - Get unmatched, complete threat response capabilities with a 15-min Mean Time to Contain, driven by our open XDR Platform.
- **Talent Expertise** - Outmaneuver even the most sophisticated attackers with the eSentire Cyber Resilience Team, who are personally dedicated to protecting your organization.
- **Threat Intelligence** - Stay ahead of advanced cyberattacks with proactive threat intelligence, original threat research, and the eSentire Threat Response Unit (TRU), a world-class team of seasoned industry veterans.
- **Measurable MDR Value** - Get full transparency into the health of your environment and how we protect your critical assets from threats with our Executive Dashboard, Insight Portal, and Cyber Resilience Score.
- **Culture & Experience** - Our team is your team and we are motivated to demonstrate each and every day that an Attack On You Is An Attack On Us.

MAPPED

MITRE ATT&CK

CERTIFIED

AICPA SOC 2 — Formerly SAS 70 Reports

bsi ISO/IEC 27001 Information Security Management CERTIFIED

AWARDED

IDC LEADER

Overall Leader — Managed Detection and Response

MSSP Alert — TOP 250 MSSPs 2024 Edition — NAMED #8 & TOP MDR PROVIDER

Forrester — WAVE STRONG PERFORMER 2025 — Managed Detection And Response Services

$7T+ Total AUM	**300+** Platform Integrations
20M Daily Signals Ingested	**3M** Daily XDR Automated Disruptions
6000 Daily Human-led Investigations	**700** Daily Escalations
400 Daily Threat Containments	**15min** Mean Time to Contain

Gartner Peer Insights™

★★★★½

4.7 out of 5

★★★★★

"eSentire Provides A Bullet-Proof Suite Of Products!"

IT Manager
In the Banking Industry

Read full review here >

★★★★★

"eSentire provides SOC services at an affordable price."

Senior Cyber Security Admin
In the Consumer Goods Industry

Read full review here >

★★★★★

"Excellent partner that is proactive with alerts, new detection intelligence, and overall very responsive to customer incidents."

Director of IT Infrastructure & Cybersec
In the Healthcare and Biotech Industry

Read full review here >

G2

★★★★½

4.7 out of 5

★★★★½

"eSentire's got your back at anytime 24/7"

Brice A.
Enterprise Company

Read full review here >

★★★★★

"Top notch MDR partner."

Verified User in Manufacturing
Enterprise Company

Read full review here >

★★★★★

"eSentire is an extension of my team."

Phil M.
Mid-Market Company

Read full review here >

Ready to Switch to eSentire MDR?

We're here to help! Submit your information and an eSentire representative will be in touch to discuss how eSentire MDR can help you build a more resilient security operation today.

CONTACT US

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

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.