eSENTIRE

DATA SHEET:

Managed Detection and Response

Build a more responsive security operation to put your business ahead of disruption.

Full Threat Visibility & Investigation

See the complete picture of your attack surface with multi-signal intelligence enabling deeper correlation and investigation capabilities, proven to contain threats faster.

24/7 Threat Hunting & Disruption

Be confident you're continuously protected by our SOC Analysts and Elite Threat Hunters who rapidly investigate, contain and close down threats when an automated response isn't possible.

Atlas XDR Cloud Platform

Stay ahead of new and emerging threats with high fidelity detection and automated real-time threat disruption powered by unique intelligence from across our global customer community.

Rapid, Robust Response

See even the most advanced threats disrupted, isolated and stopped 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

Add world class threat researchers to your team to hunt the most advanced undetected threats. Our Threat Response Unit (TRU) delivers original research, curates threat intelligence and builds new detection models to ensure you stay ahead of attackers.

An Attack On You Is An Attack On Us

We stand with you, every moment of every day and push boundaries, to keep you ahead.
With hybrid working and cloud-services expanding your threat surface, cybercriminals becoming increasingly sophisticated and security expertise harder than ever to find, we understand how challenging it has become to protect your businesses from disruption.

To respond fast and mitigate business risk, you need complete visibility and coverage of your cyberattack surface which we uniquely deliver through our multi-signal approach to MDR. Our powerful Atlas XDR Platform ingests network, cloud, log, endpoint and insider threat signals, correlating indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Our 24/7 SOC Analysts and Elite Threat Hunters rapidly respond to investigate, contain and stops threats the Atlas XDR Platform senses have the potential to bypass automated security controls.

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's Best of Breed Ecosystem of Technology Partners and Proprietary Detection Technology

eSentire MDR offers you the flexibility and choice of leveraging technology platforms from our best in class ecosystem of partners. If you have already made a technology investment you can always Bring Your Own License (BYOL) to eSentire for optimization, and 24/7 MDR support.

We go beyond most MDR providers by developing custom detection engineering based on our threat intelligence and proprietary ML applications that hunt and respond to threats.

eSentire MDR for Network

eSENTIRE

Proprietary Technology

eSentire MDR for Endpoint

vmware Carbon Black

CROWDSTRIKE

Microsoft

SentinelOne

eSentire MDR for Log

sumo logic

Microsoft

eSentire MDR for Cloud

Microsoft

Google Cloud

aws

LACEWORK

sumo logic

eSentire Managed Vulnerability Service

tenable

Security without compromise

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 MDR means multi-signal telemetry and complete response. 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.

Our multi-signal approach ingests high-fidelity data sources from endpoint, network, log, cloud, insider threat, assets, and vulnerability data that enables complete attack surface visibility. Automated blocking capabilities from our eSentire Atlas XDR Cloud Platform prevent attackers from gaining an initial foothold while our expert Elite Threat Hunters can initiate human-led investigation and containment at multiple levels of the attack surface. Through the use of host isolation, malicious network communication disruption, account-based suspensions and other measures, we can stop the attacker at any level.

	MDR SIGNALS	INVESTIGATION	RESPONSE
	Data Collection	Correlation	Kill Switch
24/7 INVESTIGATION AND RESPONSE	Network	✓	✓
	Endpoint	✓	✓
24/7 INVESTIGATION CONTEXT DRIVERS	Log	✓	
	Cloud	✓	
	Insider	✓	
	Vulnerability	✓	

WE OWN THE R IN MDR

The World's Most Complete Threat Response Capability

To build a more responsive security operation, you need more than just alerts. You need a partner who goes further to prevent your business from ever being disrupted. When it comes to response, it's how we do it that makes all the difference.

RESPONSE SPEED

We Find and Stop Cyber Threats Faster Than Anyone

When your business's reputation and operations are under attack, every minute matters. Our Atlas XDR platform instantly detects and blocks threats millions of times per day. When human intuition is required, our 24/7 experts are on guard to protect you with a Mean Time to Contain of only 15 minutes.

RESPONSE EXPERTISE

We Don't Just Alert You to Cyber Threats, We Act On Them

We never throw alerts over the fence to you like other MSSPs and MDR providers. We take real ownership of protecting your business, responding to ensure cyber threats are contained and remediated, and your business operations continue to run smoothly. An attack on you, is an attack on us.

RESPONSE COVERAGE

We Continuously Protect You Across Your Complete Cyberattack Surface

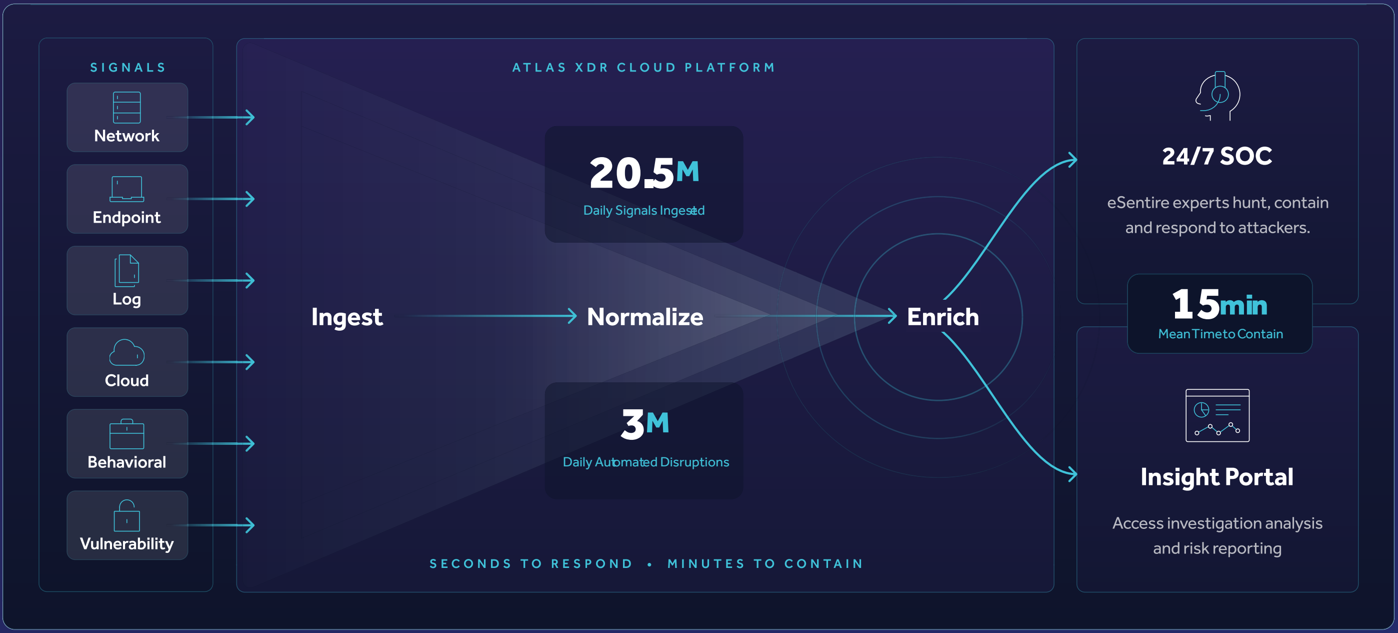
Be confident your defenses are always one step ahead. Our global SOCs are home to the industry's only 24/7 threat hunters and with eSentire's unique multi-signal intelligence, you can sleep easy knowing that whenever, wherever a new cyber threat is detected, we'll always respond to protect you.

eSentire MDR is powered by Atlas XDR

One platform. Your complete attack surface protected.

To respond fast and mitigate business risk, you need complete visibility and coverage of your attack surface which we uniquely deliver through our multi-signal approach to Managed Detection and Response. Our powerful Atlas XDR Platform ingests network, cloud, log, endpoint and insider threat signals, correlating indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes.

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—and our clients are already enjoying the benefits while the market plays catch up. It's not a bolt-on or add on, the Atlas XDR platform is at the core of eSentire MDR. You've got the weight of the world on your shoulders, so as the name implies, Atlas does the heavy lifting for you.



Leveraging patented machine learning models and artificial intelligence pattern recognition, Atlas XDR learns across our global customer base and extends security network effects so every customer benefits with each specific detection. This ability to rapidly learn and work at cloud scale, combined with expert human actions, stops breaches and proactively mitigates customer risk in ways unattainable by legacy security products, traditional MSSPs and other MDR providers.

24/7 THREAT HUNTING & DISRUPTION

How we help put your business ahead of disruption

Our team doesn't drown you in alerts, we go beyond other MDR providers to drive results.

We support your program with security experts, cutting-edge machine learning XDR technology and unique intelligence to mitigate business risk and drive your security program forward.

Our renowned cybersecurity experts are mission driven to protect your business. We stand guard 24/7 so you don't have to.

We understand what is at stake for you and pride ourselves in our ability to respond as one dedicated global team, taking real ownership over protecting your business from disruption.

PEOPLE

An Attack On You Is An Attack On Us

From day one, our team is your team. Your Cyber Risk Advisor is dedicated to keeping your business ahead of disruption and alongside them, you're joining forces with experienced cybersecurity veterans, elite threat hunters, and industry-renowned threat researchers. Your protection is personal to us and together, we are committed to making your cybersecurity operation more responsive and your business more cyber resilient.

PLATFORM

One Platform provides Complete Attack Surface Protection

Don't settle for partial security. Our Atlas XDR Platform continuously ingests and correlates millions of threat signals across your environment, giving you complete cyberattack surface visibility. Patented AI and machine learning eliminate noise, power real-time detection and response, and automatically block over 3M attacks every single day – so our experts can focus on your highest priority cybersecurity events.

INTELLIGENCE

Unique Intelligence That Puts You Ahead of The Threat Curve

Ready to reclaim the advantage over the most sophisticated cybercriminals? When you combine real-time cyber threat signals from across our global customer community with patented AI pattern recognition, powerful machine learning models and the 24/7 expertise of our industry leading Cyber Analysts, your business can scale, securely.

★★★★★
4.8 out of 5

★★★★★

"eSentire - The first and best MDR in the industry."

Eric M, SVP - CISO & Head of Infrastructure, Risk and Security Technology
Mid-Market Company

★★★★★

"I feel safer, more secured and part of an extended team."

Byron S,
Enterprise Company

★★★★★

"eSentire - trusted security partner"

Amy M, CISO / Manager of Information Security
Mid-Market Company

The eSentire difference

Put your business ahead of disruption

- Recognized globally as the Authority in Managed Detection and Response
- The world's most advanced XDR Cloud Platform
- 24/7 Threat Hunting & Disruption
- 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

AICPA SOC 2

bsi ISO/IEC 27001 Information Security Management CERTIFIED

MAPPED

MITRE ATT&CK™

AWARDED

IDC LEADER

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

MSSP Alert Top 250 MSSPs 2022 EDITION

NAMED #9 &
TOP MDR PROVIDER

THE CHANNEL CO. CRN TECH INNOVATORS WINNER 2022

REVIEWS

G2
4.8 out of 5

Gartner Peer Insights™
4.8 out of 5

Software Reviews GOLD MEDAL 2022 MANAGED DETECTION & RESPONSE
9 out of 10
COMPOSITE SCORE

$6.5T+
Total AUM

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?

Contact Us

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**.