






# Managed Detection and Response

Combine cutting-edge open XDR technology, multi-signal threat intelligence, and the industry’s only 24/7 Elite Threat Hunters to build a more resilient security operation.

 <p><b>Full Threat Visibility &amp; Investigation</b></p> <p>Get multi-signal threat intelligence enabling deeper correlation and threat investigation capabilities, proven to contain threats faster.</p>	 <p><b>24/7 Threat Hunting &amp; Disruption</b></p> <p>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.</p>	 <p><b>Open XDR Cloud Platform</b></p> <p>Stay ahead of emerging threats with high fidelity detections and automated real-time threat disruption powered by unique intelligence from across our global customer community.</p>	 <p><b>Rapid, Robust Response</b></p> <p>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.</p>	 <p><b>Original Threat Intelligence</b></p> <p>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).</p>
---	--	---	--	--







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. Our open 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.

MDR Signals	Visibility	Investigation	Response
 NETWORK	●	●	●
 ENDPOINT	●	●	●
 LOG	●	●	●
 CLOUD	●	●	●
 IDENTITY	●	●	●
 VULNERABILITY	●	●	

# 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
- ✓ Open XDR Cloud Platform
- ✓ Multi-signal Coverage and Visibility
- ✓ Automated Detections with Signatures, IOCs and IPs
- ✓ Security Network Effects Amplified Across Global Customer Base
- ✓ Detections Mapped to MITRE ATT&CK Framework
- ✓ 5 Machine Learning Patents for Threat Detection and Network Traffic Disruption
- ✓ Detection of Unknown Attacks Using Behavioural Analytics
- ✓ Rapid Human-led Threat Investigations
- ✓ Threat Containment and Remediation
- ✓ Detailed Escalations with Analysis and Security Recommendations
- ✓ eSentire Insight Portal Access and Real-time Visualisations
- ✓ 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

### CLOUD INFRASTRUCTURE



### CLOUD APPLICATIONS






### SAAS PLATFORMS AND SECURITY INFRASTRUCTURE



# eSentire MDR is More Than Just Alerts

## The World's Most Complete Threat Response Capability

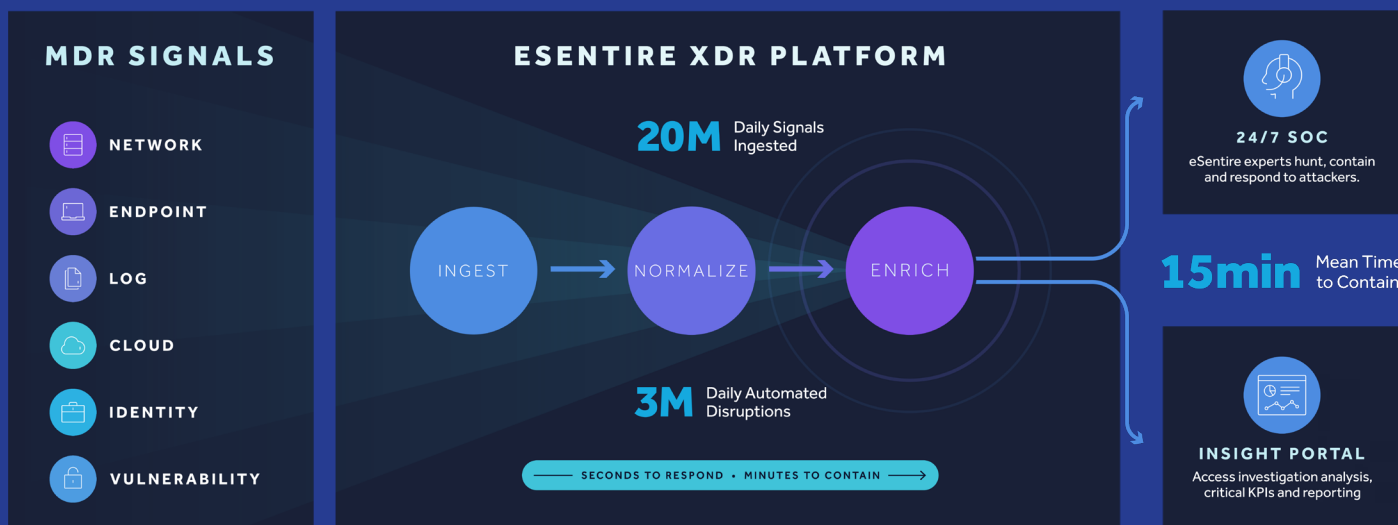
When it comes to response, it's how we do it that makes all the difference. To build a more resilient security operation, you need an MDR solution provider who has your back from Day 1.

 <b>RESPONSE SPEED</b>	 <b>RESPONSE EXPERTISE</b>	 <b>RESPONSE COVERAGE</b>
<p>Our eSentire XDR platform instantly detects and blocks millions of threats per day. We add 200+ IPs &amp; IOCs per day to our block list based on positive SOC investigations.</p> <p>When human intuition is required, we are on guard 24/7 to protect you with a Mean Time to Contain of only 15 minutes.</p>	<p>We take threat response seriously by containing and remediating cyber threats on your behalf, so your business continues to run smoothly.</p> <p>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.</p>	<p>Get continuous protection across your entire attack surface. Whenever and wherever a new cyber threat is detected, we'll always respond to protect you.</p> <p>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.</p>

## eSentire MDR is Powered by Our Open XDR Platform

One platform. Your complete attack surface protected.

With a Mean Time to Contain of <15 minutes, our powerful open XDR Platform ingests network, cloud, log, endpoint, and identity signals, correlating indicators of compromise to detect, respond to, and automatically disrupt threats in minutes.



### Benefit from Security Network Effects with the eSentire XDR Platform

Leveraging patented machine learning models and artificial intelligence pattern recognition, our open 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.

# The eSentire Difference

## Build Resilience. Prevent Disruption.

- ✔ **Operational Leadership** - Be protected by a trusted provider recognised globally as the Authority in Managed Detection and Response.
- ✔ **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 organisation.
- ✔ **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**

**CERTIFIED**

**AWARDED**

NAMED #9 & TOP MDR PROVIDER

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

**Gartner**  
**Peer Insights™**

★★★★★  
**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 >](#)

★★★★★  
**4.7 out of 5**

★★★★★

“Excellent MDR Provider, amazing value for the service that you get!”

**Michael S.**  
*Enterprise Company*

[Read full review here >](#)

★★★★★

“eSentire excels with advanced threat detection, real-time monitoring, MDR services, customised security, 24/7 SOC, and proactive threat hunting.”

**David P.**  
*Mid-Market Company*

[Read full review here >](#)

★★★★★

“Best money I have ever spent on Infosec.”

**Chris T.**  
*Enterprise Company*

[Read full review here >](#)

