eSENTIRE

DATA SHEET

eSentire Open XDR Cloud Platform

One platform. Your complete attack surface protected.

Open, Cloud-Native Architecture

Our distributed platform easily integrates with your existing security investments and ingests and analyzes massive amounts of data from signals across our global customer base.

Proprietary Machine Learning

Our adaptive machine learning and artificial intelligence models eliminate noise and provide real-time detection of even the most advanced cyberattacks, including zero-day attacks.

Multi-Signal Coverage

We normalize and correlate data from network, endpoint, logs, behavioral sources, vulnerability scans, cloud environments, and identity assets to monitor your entire attack surface and enable effective threat investigation.

Extensive Response Capability

We implement threat-specific containment measures in seconds at the network, endpoint, cloud and identity levels across our entire customer base.

Threat Intelligence

Our detection rules and investigative runbooks are informed by 24/7 visibility into our global customer base combined with proactive threat hunting, open-source intelligence (OSINT), and commercial threat feeds.

Automated Disruptions

We automatically block all known malicious IOCs and IPs known to eSentire. When human intuition is required, the SOC team is engaged to perform deep investigation and manual threat response.

Open XDR Platform: The Foundation of Effective MDR

Detection in seconds, automatic containment in minutes, and security network effects at scale.

The eSentire Open XDR Platform powers our MDR service and 24/7 SOC, adding efficiency and value to your security operation by automatically blocking millions of attacks each day. Using a global IP deny list, our XDR Platform automatically protects your assets against malicious IOCs and IPs known to eSentire. There are 12,000+ indicators recognized across our eSentire XDR platform, and we add 200 IOCs/IPs on average every day.

eSentire XDR platform makes proactive Security Network Effects possible by pushing new threat detection and containment content to every eSentire customer. Once it automatically responds to a new threat, the XDR Platform leverages patented artificial intelligence (AI) and scalable machine learning (ML) to process all the threat signals across our global customer base.

Our open XDR platform cuts the noise, letting our experts focus on high priority security events.

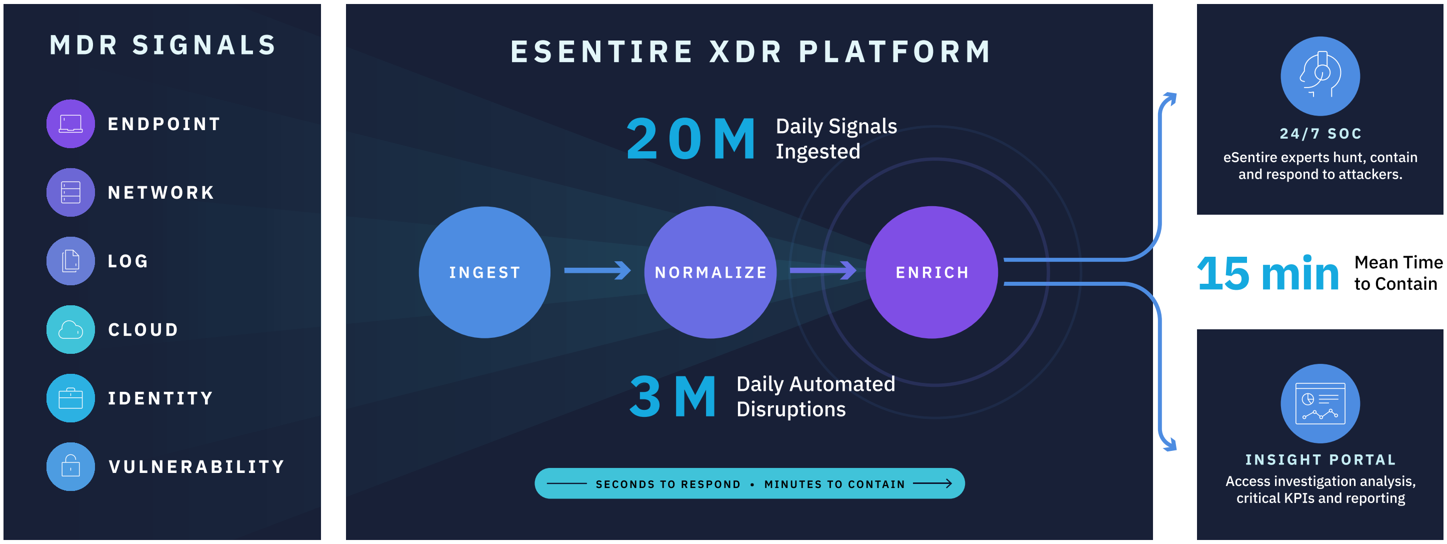
Powering Your eSentire Protectors

Our open XDR platform automatically disrupts high fidelity threats, which allows our 24/7 SOC, staffed with Elite Threat Hunters and experienced Cyber Analysts, to focus on multi-signal investigation, threat containment and response. Backed by our industry-renowned Threat Response Unit(TRU), we offer around-the-clock security monitoring, unlimited threat hunting, threat disruption, containment, and unlimited incident handling and remediation.

The time from alert to action is critical to prevent disruption across your business. The eSentire XDR platform equips our team with the insights and tools they need to perform deep threat investigations and execute manual containment, when required, in minutes.

How eSentire XDR Platform Works

Our Open XDR Platform reduces noise and enhances SOC investigations by aggregating and normalizing data from endpoints, networks, logs, and cloud assets. Then the XDR platform correlates the data with the latest IoCs, to identify genuine threats and facilitate complete response.


MDR SIGNALS
ENDPOINT
NETWORK
LOG
CLOUD
IDENTITY
VULNERABILITY
ESENTIRE XDR PLATFORM
20M Daily Signals Ingested
INGEST
NORMALIZE
ENRICH
3M Daily Automated Disruptions
SECONDS TO RESPOND • MINUTES TO CONTAIN
24/7 SOC
eSentire experts hunt, contain and respond to attackers.
15 min Mean Time to Contain
INSIGHT PORTAL
Access investigation analysis, critical KPIs and reporting

Seamless Integration and Threat Investigation Across Your Existing Tech Stack

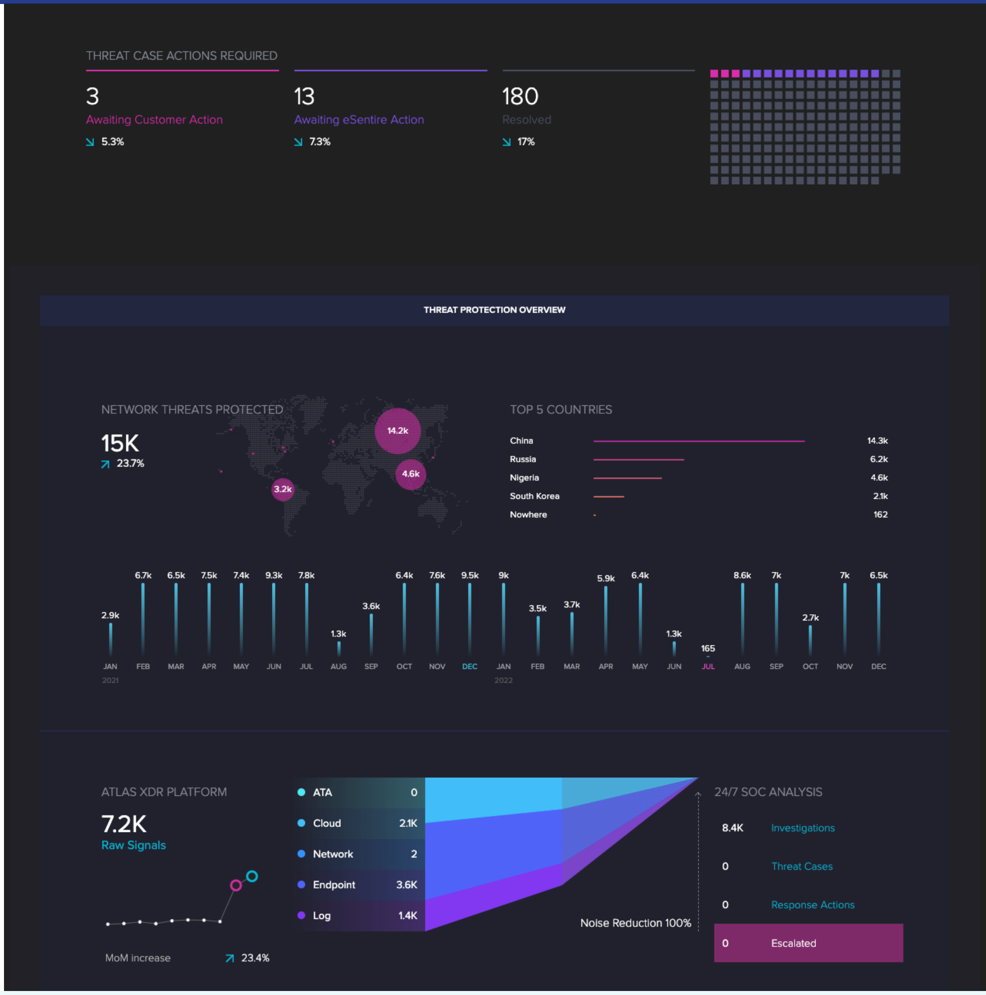
By supporting 300+ technology integrations, the eSentire Open XDR Platform integrates seamlessly with existing tools and SaaS platforms in your environment to enable continuous monitoring across your hybrid footprint, ingestion of high-fidelity data sources, and 24/7 protection from sophisticated known and unknown cyber threats.

aws	Google Cloud	Azure	CROWDSTRIKE
Microsoft	SentinelOne	sumo logic	tenable

eSentire's 24/7 Portal Experience

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.



Ready To Get Started?

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**.