eSENTIRE

DATA SHEET

eSentire MDR for Network

Protect your on-premises network and AWS cloud environments through deep packet inspection and real-time traffic interruption that enables rapid response.

24/7 Monitoring and Visibility Across On-Prem Network and AWS Cloud

eSentire MDR for Network monitors your on-prem and AWS cloud network traffic around-the-clock using proprietary deep packet inspection and advanced behavioral analytics for comprehensive visibility.

Automated Threat Blocking

Our proprietary network software and open XDR Cloud platform automatically blocks malicious connections, using a global IP blocklist that is updated in real time. We add over 200 IPs per day to the block list based on positive security investigations.

Cloud-Centric Threat Detections

Our proprietary technology is specifically designed to detect modern threats targeting AWS cloud environments with an emphasis on threat detection content that is cloud related.

Minimize Threat Actor Dwell Time

eSentire MDR for Network disrupts malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR).

With eSentire MDR for Network, we combine deep packet inspection with signature and behavioral analytics to rapidly identify and block known threats and suspicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud and across your hybrid environment.

24/7 SOC Analysts and Elite Threat Hunters act as an extension of your team to provide rapid human-led investigation and response, disrupt malicious traffic, and eliminate threats that can disrupt your business.

eSentire MDR for Network neutralizes attacks missed by traditional cybersecurity controls. Here are a few examples of network cyber threats we detect and respond to:

- Command and Control (C2) traffic, even when traffic is encrypted
- Brute force attacks
- Abnormal behavior related to zero-day attacks
- Malicious connections and executables
- Drive-by social engineering attacks
- Attacks against web server infrastructure
- Remote desktop protocol
- Service exploit attempts
- Unauthorized scanning across firewalls
- Remote access tools
- DNS Tunnelling

How We Help	Your Outcomes
✓ 24/7 network traffic monitoring across on-prem and AWS cloud environments	✓ Reduction in operating expenditure costs and resource demands
✓ Advanced insights and behavioral analysis	✓ Automated blocking and manual containment of threats that bypass existing security controls
✓ Continuous integration of the latest threat intelligence and rulesets	✓ Minimized incident recovery timeframe
✓ Proprietary global IP blocklist that is continuously updated and published to all network sensors	✓ Decrease threat actor dwell time
✓ Detection and automated blocking of known and elusive attackers	✓ Improvement in overall security posture
✓ Multi-signal visibility for stronger threat correlation and investigation	✓ Mitigation of potential business disruption
	✓ Satisfaction of compliance requirements
	✓ Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)

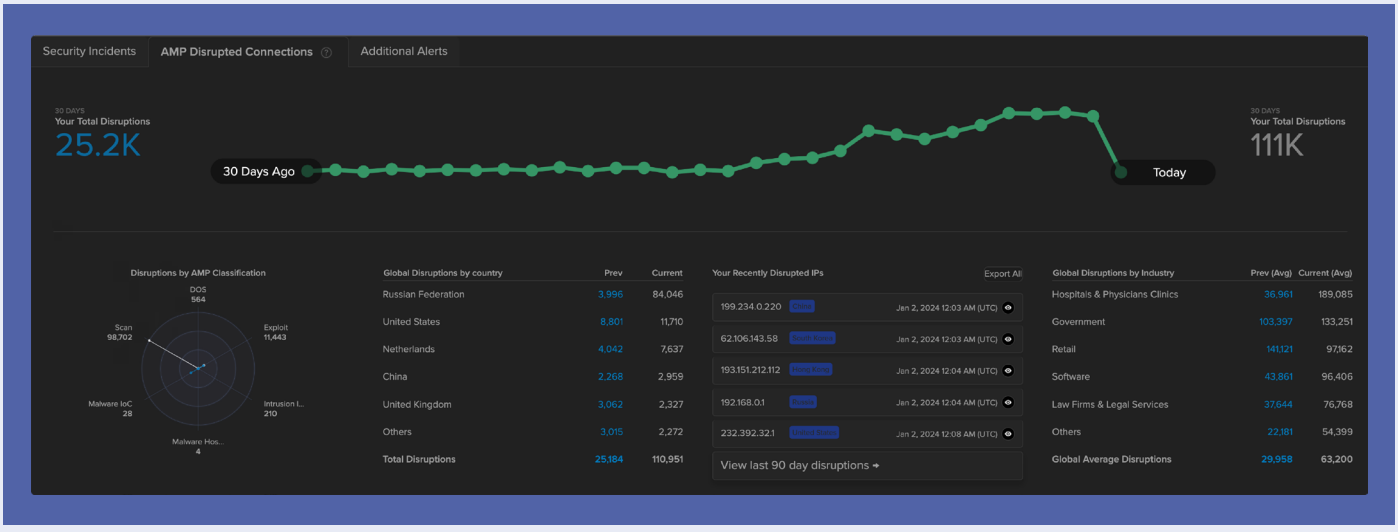
Proprietary Detection Technology

eSentire MDR for Network operates on a zero-trust approach that leverages proprietary technology and leaves threat actors nowhere to hide. It straddles your network security perimeter and ingests raw data inputs from the interior and exterior of your IT ecosystem. Then we correlate and aggregate all data into one chokepoint at the edge of your network to detect, block and respond to cyber threats 24/7.

Security Network Effects Powered by eSentire XDR Cloud Platform

Our open XDR Cloud Platform adds value by automatically blocking threats that have bypassed your security controls. It automatically protects your assets against malicious IOCs and IPs known to eSentire, using a global IP blocklist that is updated in real time by our 24/7 SOC each time a new threat vector is identified on any monitored network.

There are 12,000+ indicators of compromise (IOCs) recognized across our eSentire XDR platform and we add 200+ new IOCs on average every day.



Features

24/7 Protection Across On-Prem and AWS Cloud
We monitor network traffic around-the-clock from our two global Security Operation Centers (SOCs) with 24/7 support from our SOC Cyber Analysts.

Advanced Insights and Behavioral Analysis
eSentire MDR for Network captures categorized URL (web) traffic, rules-based malicious activity, unusual port scan information, executables downloaded, raw TCP traffic, and more.

24/7 Network Threat Containment
Our 24/7 SOC Cyber Analysts can disrupt malicious network connections on your behalf, minimizing attacker dwell time.

Granular Policy Monitoring
We curate your policy requirements and tracks usage across violations providing your security team with granularity and context. This includes Remote Desktop Protocol, Remote Access Tools, unencrypted FTP, shadow IT email servers, illegal proxy servers and more.

Full PCAP and Metadata Collection
We capture summary metadata and full network packets for targeted inquiries to confirm or explain events.

Unknown Threat Detection
Our zero-trust approach flags new network signals and suspicious activity for expert human threat hunting.

Automatic Geo-blocking
We use a proprietary DPI engine to disrupt TCP traffic from IPs that are located in a specifiific country or blocks them based on the country's geolocated IP address.

eSentire Threat Intelligence
eSentire's Threat Response Unit (TRU) develops threat intel and novel detections to block and protect your assets from malicious attacks, IOCs and IPs associated with emerging threats.

Automated Response Capabilities
We disrupt malicious traffic by integrating with industry-leading firewalls and other network-based response actions such as TCP Reset.

Available with eSentire Atlas MDR Packages
As part of our Atlas MDR packages we offer the flexibility of our Threat Intel Feed and/or our Network Service with Sensors as part of your attack surface coverage.

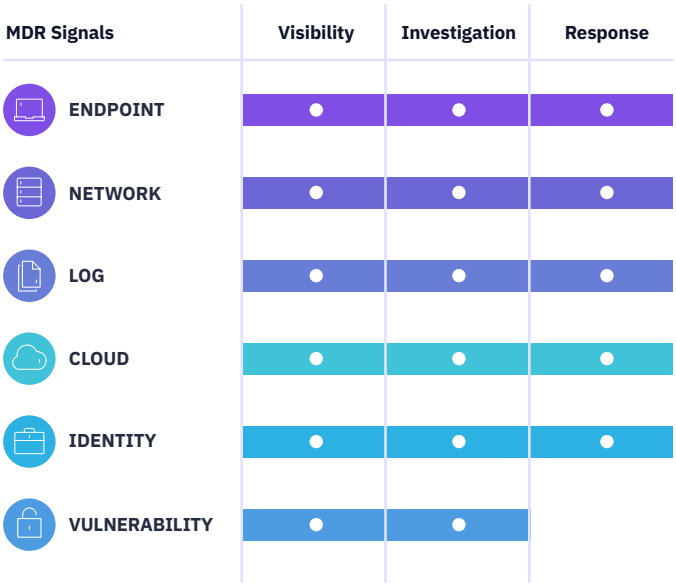
eSentire vs. Other Network Detection and Response Vendors

	eSentire MDR for Network	Other Network Detection and Response Services
24/7 continuous monitoring	✓	✓
Detection of known threats	✓	✓
Alerts and general guidance	✓	✓
Automated blocking of known cyber threats	✓	✓
Continuous management, tuning and refinement platform	✓	Limited
Capture of metadata and full network packets	✓	Limited
Continuous integration of latest threat intelligence and rulesets	✓	Limited
Remediation support	✓	Limited
Cloud-based response	✓	Limited
Firewall integration	✓	Limited
Investigation of unknown signals	✓	
Threat hunting of suspicious activity	✓	
Root cause determination	✓	
Tactical threat containment	✓	

We Do More than Network Monitoring - And Multi-Signal Matters

Our multi-signal approach ingests endpoint, network, log, cloud, identity and vulnerability data that enables complete attack surface visibility. Automated blocking capabilities built into our Open XDR Cloud Platform prevents attackers from gaining an initial foothold while our expert Elite Threat Hunters can initiate manual containment at multiple levels of the attack surface. Through the use of host isolation, malicious network communication disruption, identity-based restriction and other measures, we can stop attackers at multiple vectors and minimize the risk of business disruption.

At eSentire we recognize that the attack surface is continuously evolving and expanding. While our MDR service protects your organization from modern attackers and the vectors they target most often, we are continuously analyzing and developing new services & detections to outpace the adversaries. In our 20+ year history, we pride ourselves on the fact that no eSentire customer has experienced a business disrupting breach. With over 2000 customers across 80+ countries and 35 industries, we don't just claim to deliver complete response. We prove it and are proud to earn our global reputation as the Authority in Managed Detection and Response, each and every day.



Ready to get started?

Connect with an eSentire Security Specialist to learn how we can help you build a more resilient security operation and prevent disruption.

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**.