DATA SHEET:

eSentire MDR for Network

Guard your network on-prem and in the cloud 24/7 with real-time network detection and 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 open XDR Cloud platform automatically blocks malicious connections, using a global IP blocklist that is updated in real time by our 24/7 Elite Threat Hunters each time a new threat vector is identified on any monitored network.

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. Suspicious activity is investigated by 24/7 Elite Threat Hunters that confirm attacker presence and determine root cause. When a cyber threat is identified, our SOC Cyber Analysts and Elite Threat Hunters disrupt malicious traffic to minimize threat actor dwell time, then manage the remediation, acting as an extension of your team.

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
- Cloud-specific attacks
- Remote desktop protocol
- Service exploit attempts
- Unauthorized scanning across firewalls
- Remote access tools
- DNS Tunnelling

How We Help

- ✓ 24/7 network traffic monitoring across on-prem and AWS cloud environments
- ✓ Advanced insights and behavioral analysis
- ✓ Continuous integration of the latest threat intelligence and rulesets
- ✓ Proprietary global IP blocklist that is continuously updated and published to all network sensors
- ✓ Detection and automated blocking of known and elusive attackers
- ✓ Multi-signal visibility for stronger threat correlation and investigation

Your Outcomes

- ✓ Reduction in operating expenditure costs and resource demands
- ✓ Minimized incident recovery timeframe
- ✓ Decrease threat actor dwell time
- ✓ Improvement in overall security posture
- ✓ Mitigation of potential business disruption
- ✓ Satisfaction of compliance requirements
- ✓ Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)

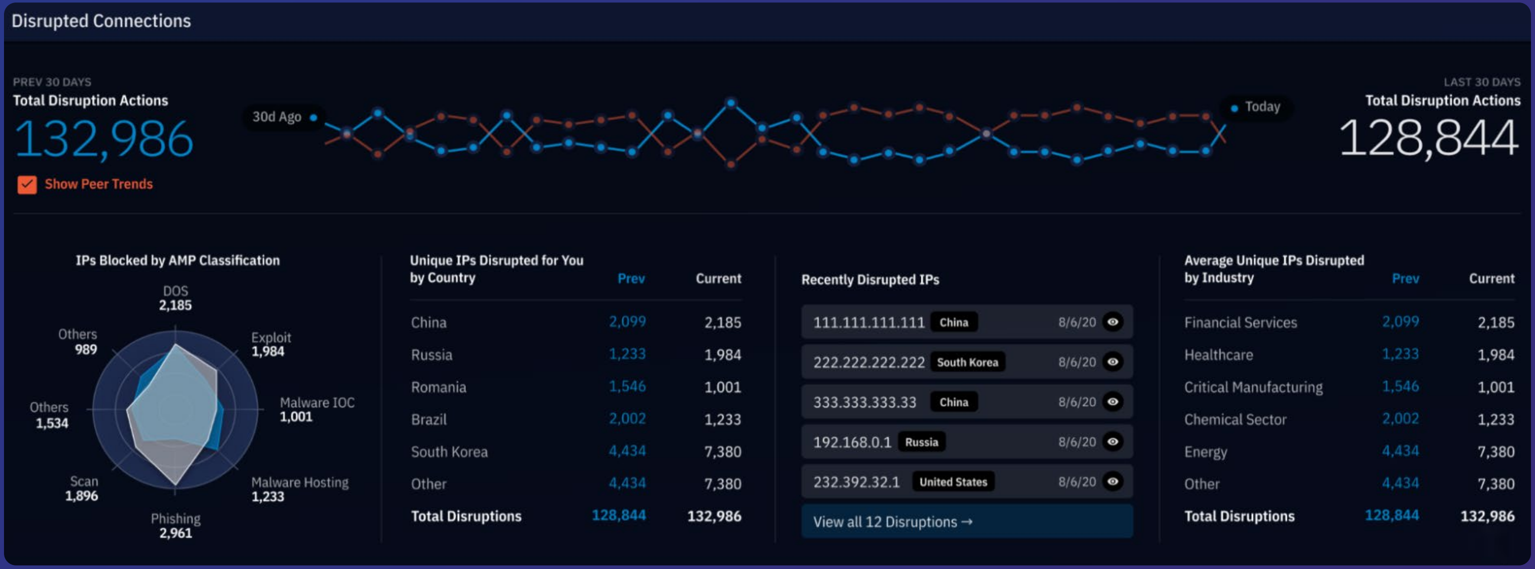
Proprietary Detection Technology

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+ on average every day.



Disrupted Connections

PREV 30 DAYS
Total Disruption Actions
132,986

☑ Show Peer Trends

LAST 30 DAYS
Total Disruption Actions
128,844

Unique IPs Disrupted for You by Country	Prev	Current
China	2,099	2,185
Russia	1,233	1,984
Romania	1,546	1,001
Brazil	2,002	1,233
South Korea	4,434	7,380
Other	4,434	7,380
Total Disruptions	128,844	132,986

Recently Disrupted IPs

111.111.111.111	China	8/6/20
222.222.222.222	South Korea	8/6/20
333.333.333.33	China	8/6/20
192.168.0.1	Russia	8/6/20
232.392.32.1	United States	8/6/20

View all 12 Disruptions →

Average Unique IPs Disrupted by Industry	Prev	Current
Financial Services	2,099	2,185
Healthcare	1,233	1,984
Critical Manufacturing	1,546	1,001
Chemical Sector	2,002	1,233
Energy	4,434	7,380
Other	4,434	7,380
Total Disruptions	128,844	132,986

Features

24/7 Protection Across On-Prem and AWS Cloud

Monitors network traffic around the clock from eSentire's two global Security Operation Centers (SOCs) with 24/7 support from our SOC Cyber Analysts.

Advanced Insights and Behavioral Analysis

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

Cyber Analysts can disrupt malicious network connections on your behalf, minimizing attacker dwell time.

Granular Policy Monitoring

eSentire curates 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

Captures summary metadata and full network packets for targeted inquiries to confirm or explain events.

Unknown Threat Detection

eSentire's zero-trust approach flags new network signals and suspicious activity for expert human threat hunting.

Automatic Geo-blocking

Uses a proprietary DPI engine to disrupt TCP traffic from IPs that are located in a specific 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

Disrupts malicious traffic by integrating with industry-leading firewalls and other network-based response actions such as TCP Reset.

eSentire vs Other Network Detection and Response Vendors

	Other Network Detection and Response Services	eSentire
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	✓
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 eSentire Atlas XDR Cloud Platform prevent 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 twenty year + history, we pride ourselves on the fact that no eSentire client 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.

	MDR Signals	Visibility	Investigation	Response
24/7 Investigation and Response	Network	●	●	●
	Endpoint	●	●	●
	Log	●	●	●
	Cloud	●	●	●
Context Drivers	Insider	●	●	
	Managed Vulnerability Service	●	●	

Ready to get started?

We're here to help! Submit your information and an eSentire representative will be in touch to demonstrate how eSentire Multi-Signal MDR stops threats before they impact your business.

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**.