DATA SHEET:

esNETWORK

Managed Network Detection and Response

GUARD YOUR NETWORK 24/7

Monitors network traffic around the clock using proprietary deep packet inspection and advanced behavioral analytics.

PREVENT INITIAL INTRUSIONS

Automatically blocks malicious connections, executables and notifies your team of policy violations.

HUNT ELUSIVE ATTACKERS

Investigates suspicious activity using expert threat hunters to confirm threat actor presence.

MINIMIZE THREAT ACTOR DWELL TIME

Disrupts malicious traffic on your behalf with root cause determination and co-remediation support.

esNETWORK is a zero latency Managed Network Detection and Response (MDR) service that neutralizes attacks missed by traditional network security controls. Operating on a zero-trust philosophy, esNETWORK combines always-on full packet capture (PCAP) with proprietary attack pattern analysis and behavioral analytics to rapidly identify known threats and suspicious activity.

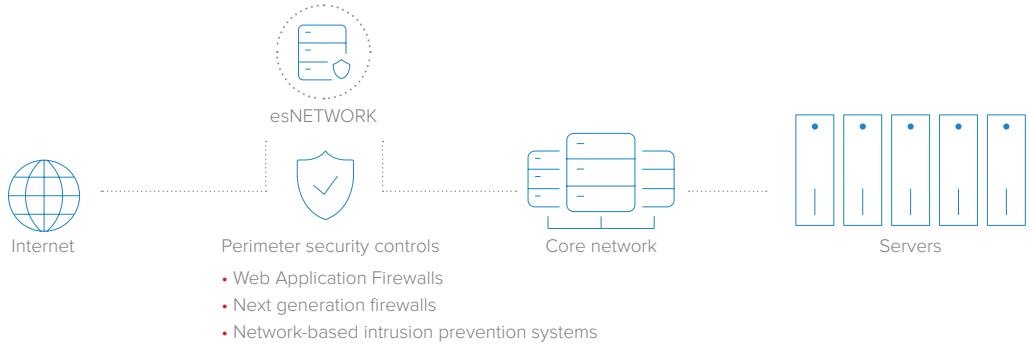
esNETWORK automatically blocks malicious connections and executables and notifies your security team of policy violations. In addition, suspicious activity is investigated by elite security analysts that confirm attacker presence and determine root cause. When a threat is identified, eSentire disrupts malicious traffic for you to minimize threat actor dwell time, then co-manages remediation with your security team.

WHAT DOES ESNETWORK DETECT?

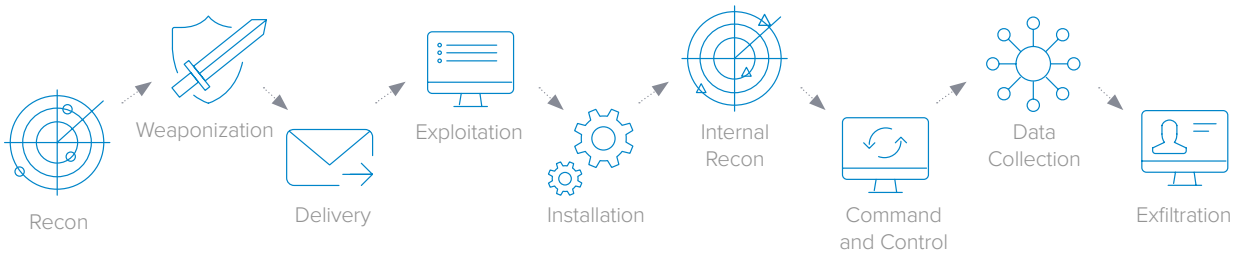
- Brute force attacks
- Abnormal behavior
- Malicious connections and executables
- Drive-by-attacks
- Active intrusions that bypassed traditional measures
- Service exploit attempts
- Unauthorized scanning across firewalls
- Remote desktop protocol
- Remote access tools

DEPLOYMENT

esNETWORK straddles (out-of-band) your network security perimeter and ingests raw data inputs from the interior and exterior of your IT ecosystem. esNETWORK correlates and aggregates all data into one chokepoint at the edge of your network to detect, block and respond to threats that traditional technologies miss.



Attack Chain Coverage



	Recon	Weaponization	Delivery	Exploitation	Installation	Internal Recon	Command and Control	Data Collection	Exfiltration
Monitoring and traffic capture	✓		✓	✓			✓		✓
Automated Blocking	✓		✓	✓			✓		✓
Tactical Containment			✓	✓			✓		✓

FEATURES

Monitoring and Deep Network Visibility

24x7x365 Coverage
Monitors network traffic around the clock from eSentire's award-winning global Security Operation Centers (SOCs).

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

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

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

Detection and Automated Blocking

IDS/IPS Detection Engine
Best of breed signature and pattern matching combined with proprietary eSentire threat analytics identifies indicators of compromise.

IP Blacklist
Disrupts malicious network connections using a proprietary global IP blacklist that is continuously published to all esNETWORK sensors.

Granular Policy Monitoring
eSentire curate's customer 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.

Unknown Detection
eSentire zero trust approach flags new network signals and suspicious activity for human threat hunting.

Country Killer
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.

FEATURES CONTINUED

Threat Hunting and Remediation

Threat Hunting
Signals that are unusual are marked as threats and fed into eSentire's SOCs for expert analyst investigation and root cause analysis.

Event Management
SOC analysts deliver deep analysis to determine true positives and further escalation of security incidents for corrective action with defined threat context.

Co-Managed Remediation Support
Analysts work with your internal security team providing co-managed remediation guidance until the threat actor is eliminated, not simply alerts and general guidance.

Alerts
Immediate alerting upon detection of confirmed threats and unusual behaviors or activity.

Tactical Threat Containment
eSentire analysts can "kill" TCP connections on a customer's behalf in real-time minimizing threat actor dwell time.

EXPERIENCE THE eSENTIRE DIFFERENCE

	Others	esNETWORK
24x7 continuous monitoring	✓	✓
Continuous management, tuning and refinement platform	Limited	✓
Capture of metadata and full network packets	Limited	✓
Continuous integration of latest threat intelligence and rulesets	Limited	✓
Detection of known threats	✓	✓
Alerts and general guidance	✓	✓
Investigation of unknown signals	✗	✓
Automated blocking of known threats	✓	✓
Threat hunting of suspicious activity	✗	✓
Root cause determination	✗	✓
Tactical threat containment	✗	✓
Co-remediation support	Limited	✓

MAKING THE CASE FOR esNETWORK

- Rapid deployment and quick time to value
- Reduction in operating expenditure costs and resource demands
- Always-on network traffic monitoring
- Continuous integration of latest threat intelligence and rulesets
- Detection of known and elusive attackers
- Automated blocking and manual containment of threats that bypass existing security controls
- Minimized incident recovery timeframe
- Improvement in overall security posture
- Mitigation of potential business disruption
- Satisfaction of compliance requirements

eSENTIRE HAS HELPED PROTECT MY BUSINESS BY...

"Building a system that can accurately filter traffic to allow human eyes the time and data necessary to protect my network."

IT Director
Small business Financial Services Company

"Preventing malicious activity before it enters the network. This has been particularly helpful with people working remotely."

Seth Waldman
System Administrator, EnCap Investments LP

eSENTIRE

eSentire, Inc., founded in 2001, is the category creator and world's largest **Managed Detection and Response (MDR)** company, safeguarding businesses of all sizes with the industry-defining, cloud-native Atlas platform that removes blind spots and enables 24x7 threat hunters to contain attacks and stop breaches within minutes. Its threat-driven, customer-focused culture makes the difference in eSentire's ability to attract the best talent across cybersecurity, artificial intelligence and cloud-native skill sets. Its highly skilled teams work together toward a common goal to deliver the best customer experience and security efficacy in the industry. For more information, visit **www.esentire.com** and follow **@eSentire**.