DATA SHEET

esNETWORK

Real-time network threat detection and response

As the principal component for eSentire's Managed Detection and Response™ (MDR) service, esNETWORK™ is a zero latency IPS/IDS designed to provide full network visibility eliminating attack blind-spots that traditional technologies miss.

Operating on a philosophy that all network signals from security appliances are potentially malicious until analyzed, eSentire Security Operations Center (SOC) analysts leverage always-on full packet capture (PCAP) with our proprietary attack pattern and behavioral analytics engine to ensure every threat is detected.

More than relying on simplistic signatures or IOCs with meaningless alerts, our network information and human-driven forensic analysis enables rapid detection and investigation of attacks. This enables alerting and response to not only known threats, but unknown threats and suspicious behavior. Once a threat is confirmed, SOC analysts can disrupt malicious traffic on your behalf and conduct post-attack forensics to aid in co-managed remediation to minimize the risk of business disruption.

WHAT DOES esNETWORK HELP YOU SOLVE?

- Limited network visibility
- Identification of threats preventative technologies miss
- Inadequate detection capabilities of unknown threats and anomalous behavior
- Prolonged incident dwell time
- Alert fatigue: Chasing too many false positives
- Lack of in-house expertise to proactively hunt, contain, forensically investigate and respond to threats

BENEFITS

- Alerts and responses are directed to the threats that matter
- Proactive hunting for the needle in the haystack
- Full forensic investigation and co-remediation at no extra cost, no retainer required
- Vastly reduces detection, containment and remediation time-frame

WHAT DOES esNETWORK DETECT?

BRUTE FORCE ATTACKS

ABNORMAL BEHAVIOUR

SERVICE EXPLOITS ATTEMPTS

ACTIVE INTRUSIONS THAT BYPASSED TRADITIONAL MEASURES

INSIDER ATTACKS

DRIVE-BY ATTACKS

MALICIOUS CONNECTIONS

MALICIOUS EXECUTABLES

SCANNING ACROSS THE FIREWALL

DOS/DDOS

WEB APPLICATION ATTACKS

FEATURES

ALWAYS-ON MONITORING

- 24x7x365 Continuous Monitoring: eSentire SOC analysts monitor all network activity 24x7x365, with no reduced coverage and no after-hours beepers. We average 35 seconds or under from notification of a possible event to begin a human investigation.

VISIBILITY EMPOWERS DETECTION

- Active Threat Hunting:

  Signals that are unusual are marked as threats and fed into eSentire's analytics pipeline and suspicious activity identified via human investigation and confirmation.
- URL History: Captures HTTP traffic and provides full forensics view complete with referrer and user agent. It also uses a proprietary Deep Packet Inspection (DPI) engine to detect and capture URLs.
- Data Loss Analysis: Provides outbound file capture, such as email attachments, for threat qualification and forensic analysis including SMTP, cloud storage, FTP transfers, etc.
- Full PCAP & Netflow: SOC analysts leverage summary metadata and targeted queries into full PCAP data to confirm or explain the event with forensic analysis techniques
- Country Killer: Uses a proprietary DPI engine to stop traffic from IPs that are located in a specific country or blocks them based on the country's domain.
- Executable Analysis and Blocking: Provides whitelist-based executable download detection and mitigation. If a file is not in the whitelist, analysts intervene and block the download by killing the connection in real time.
- Packet Analyzer: Detects suspicious behavior such as unusual ports scans, sequential scans and "spamming" machines.
- Bandwidth Profiler: Notifies the client and the SOC of abnormal bandwidth usage if there is a suspected internal threat (exfiltration or otherwise) or a Distributed Denial of Service (DDOS) attack.
- SSL Decryption and Traffic Disruption: Detects SSL based malware for profiling and threat signature creation.

FEATURES

ANALYSIS

The esNETWORK sensor captures the following type of network traffic that, when appropriate, is used for forensic analysis:

- Categorized URL (web) traffic
- Categorized rules-based detected traffic
- Unusual port scan information
- Executables downloaded
- Email attachments sent
- Raw TCP traffic
- Information resulting from DPI detection

RESPONSE

- Rapid Communication:

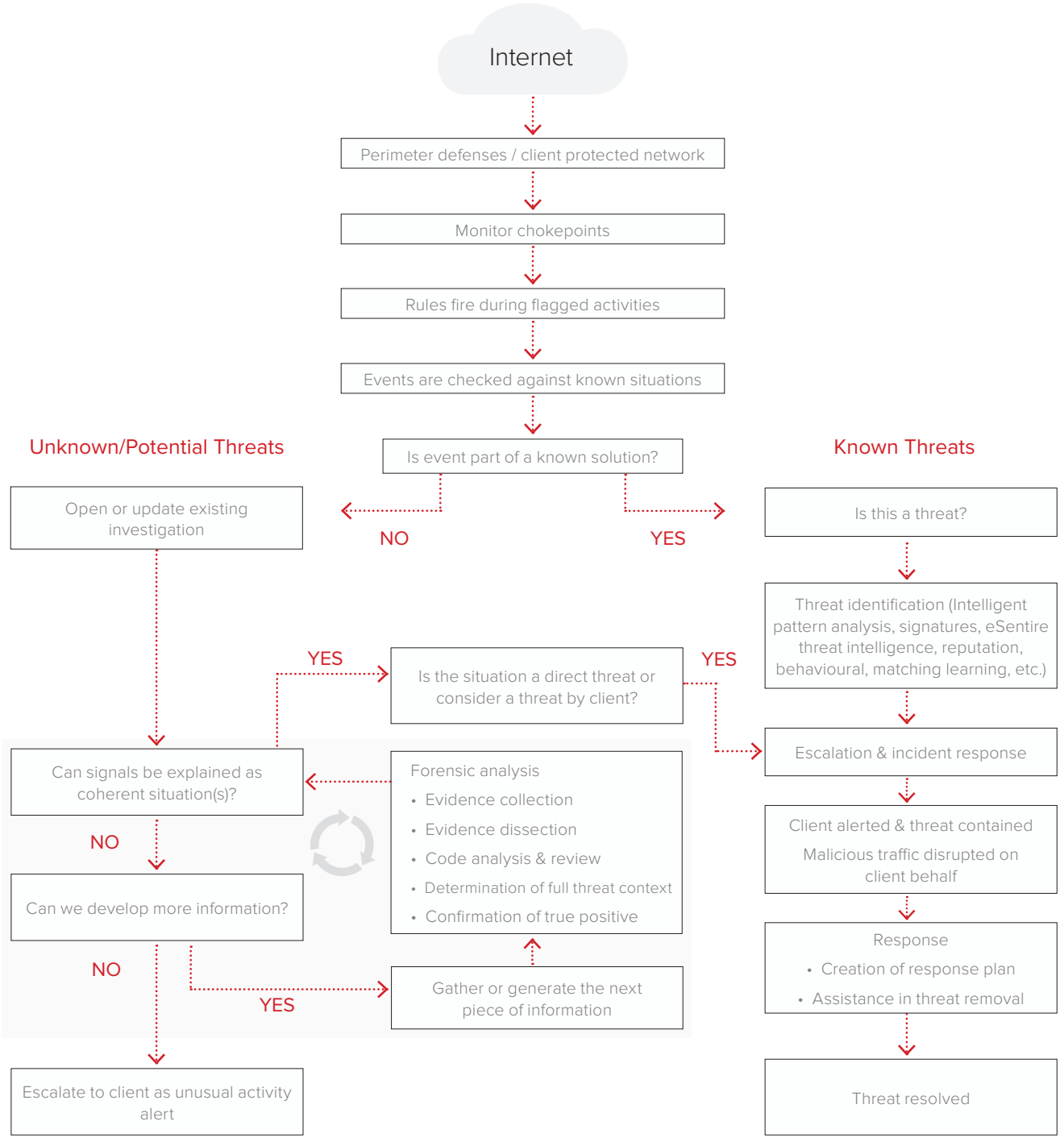
  Immediate alerting from human analyst from eSentire SOC upon detection of both confirmed threats and unusual behaviors or activity.

- Forensic Investigation: Embedded SOC support includes forensic investigation to determine the root cause and corrective actions.
- Event Management: SOC analysts deliver deeper analysis to determine true positives and further escalation of security incidents for corrective action with defined threat context.
- Co-Managed Remediation: Analysts provide co-managed remediation until the threat actor is completely eliminated, not simply alerts and general guidance.
- Tactical Threat Containment: eSentire provides a rule-based detection and mitigation service that can be configured to automatically “kill” TCP connections in real-time or to notify the SOC. The SOC can also manually “kill” TCP connections on the client’s behalf.
- Continued Monitoring for Re-entry: Analysts will continue to monitor for attacker re-entry related to the successful attack leveraging details of forensic investigation as well as previous attackers TTP used in other engagements.

HOW DOES IT WORK?

The esNETWORK sensor is deployed on site and captures network traffic, detects and identifies threats (through intelligent pattern analysis), notifies the eSentire SOC of the threats, and if appropriate, mitigates threats in real time by disrupting the inappropriate network traffic.

The SOC provides threat and site-specific contextual analysis, qualifying and classifying the threats using forensic analysis techniques. If appropriate, the SOC alerts the client about a threat, configures the sensor to mitigate the threat and conducts further forensic analysis.



ESENTIRE VS. OTHER SECURITY PROVIDERS

	Other MDR	eSentire MDR
24x7 always-on continuous monitoring	Limited	✓
Real-time inspection of every packet utilizing full packet capture	Limited	✓
Detection utilizing signatures and IOCs	✓	✓
Detection of unknown attacks leveraging patterns and behavioral analytics	Limited	✓
Active threat hunting	Limited	✓
Full forensic analysis to confirm threat and eliminate false positives	Requires an IR retainer	✓
Alerting of suspicious behavior	Limited	✓
Alerting of confirmed threats	✓	✓
Tactical threat containment on client's behalf via TCP disruption	✗	✓
Remediation recommendations	✓	✓
Full support until incident is remediated and threat actor is eliminated	Requires an IR Retainer	✓

MAKE THE CASE FOR esNETWORK

Active Threat Hunting
We assume all network signals are potentially malicious and proactively hunt for the needle in the haystack.

Elimination of False Positives
We support your team by ensuring alerts and responses are directed to the threats that matter.

Tactical Containment
We tactically contain threats on your behalf, reducing attacker dwell time.

Unlimited Embedded Incident Response
Beyond alerts, we provide complete incident management, forensic investigation and co-remediation at no extra cost and no retainer required.

Threat Intelligence
We integrate intelligence from our MDR platform that detects threats that bypass traditional controls and distribute proactive measures to all esNETWORK clients.

Better Together
We correlate both endpoint and network information during investigations to reveal the full picture of what happened and deliver timely and focused incident response.

esNETWORK IN ACTION

An Adversary on the Network

For one of eSentire's clients, technology wasn't enough to stop a targeted threat actor from infiltrating its network. With the help of eSentire Managed Detection and Response™ and a team of dedicated security analysts and experts, one eSentire client narrowly avoided an adversary attack.

Read the full report

Locky Ransomware Attempt

Released in 2016, Locky works by locking users out of their systems and is most commonly deployed by hackers using phishing campaigns that leverage Microsoft Word documents and malicious macros. At the height of its distribution, a number of eSentire clients were targeted by Locky, but experienced no loss of data thanks to the detection capabilities of esNETWORK™.

Read the full report

Zero Day Attack

A Registered Investment Advisor (RIA), employing eSentire Managed Detection and Response™, was infected with ransomware. Over the next 40 minutes, eSentire analysts learned what happened, how the ransomware was deployed, and how we helped the firm resolve the situation.

Read the full report

NEXT STEPS

Put eSentire MDR to the test

Learn more about eSentire Advisory Services

Learn more about eSentire MDR

Access free cybersecurity tools and resources

eSENTIRE

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $5 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire.**