eSENTIRE®

DATA SHEET

Rapid Assist

You've Been Breached. Every Second Counts.

DETERMINE THE EXTENT

Rapid Assist collects critical network and endpoint data providing on-site and remote incident response teams with crucial information that speeds forensic investigation.

DISRUPT THE THREAT

Rapid Assist minimizes threat actor dwell time with embedded containment capabilities via host isolation and network communication disruption.

ELIMINATE ALL TRACES

Rapid Assist captures full network packets and endpoint telemetry ensuring incident responders have a comprehensive picture on how to eliminate all traces of the threat.

MONITOR FOR RE-ENTRY

Rapid Assist monitors for threat re-entry ensuring the network and endpoints are not susceptible to new points of attack.

THE PROBLEM

Fifty-four percent of attackers claim they can breach the perimeter, locate critical data and exfiltrate in under 15 hours[1]. No industry is immune and time is not on your side. On-site and remote responders need information as quickly as possible to speed forensic investigation and determine the best steps for containment and threat elimination. Meanwhile, the clock ticks as attackers close in.

> In the past 12 months 57% of organizations say the time to detect, contain and respond to a cyber crime has increased or significantly increased.[2]

THE ANSWER

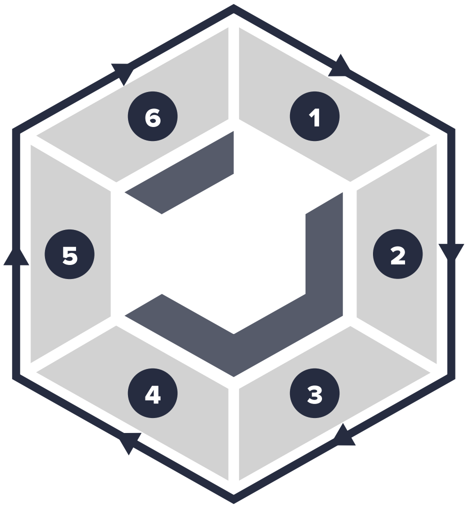
Critical information that speeds forensic investigation and rapid containment capabilities will be the difference in avoiding further disruption. Rapid Assist augments incident responders collecting network and endpoint data that speeds threat hunting and investigation. Embedded containment capabilities via host isolation or network communication disruption contains a threat actor earlier in the kill chain while responders perform remediation and network hardening. Rapid Assist's full network packet capture and endpoint visibility provides responders with a comprehensive picture on how an attacker gained entry so all traces and vulnerabilities can be eliminated. Post remediation, Rapid Assist continues to monitor for threat re-entry ensuring blind spots are illuminated and your organization is safe from further attack.

[1] *The Black Report: Decoding The Minds of Hackers 2018*

[2] *Ponemon: Annual Study on Cyber Resilient Organization, March 2018*

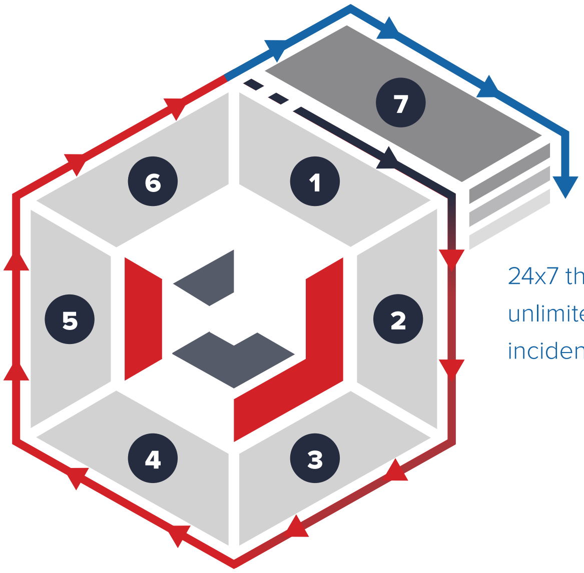
TRADITIONAL INCIDENT RESPONSE

Threat Actor Dwell Time is Extended



WITH RAPID ASSIST

Rapid Containment, Reduced Threat Actor Dwell Time, Confirmation of Threat Elimination and Monitoring For Re-entry



24x7 threat hunting and unlimited embedded incident response.

1	Detection
2	Containment
3	Investigation
4	Remediation
5	Confirmation/Re-entry
6	Recovery
7	Post Incident Option to Convert to Managed Detection and Response

■	On-Site/Remote Incident Responders
🟥	Rapid Assist
🟦	Managed Detection and Response

WHAT IS RAPID ASSIST DESIGNED TO SOLVE?

- ✓ Prolonged incident dwell time
- ✓ Prolonged containment timeframes
- ✓ Limited visibility across network and endpoint activity
- ✓ Lack of in-house tools to collect data to aid forensic investigation
- ✓ Expertise needed to conduct forensic investigation
- ✓ Lack of expertise to determine go-forward plans for detection and response
- ✓ Required monitoring for threat re-entry

FEATURES

1

RAPID DEPLOYMENT

- Up and running within hours, not days, collecting data critical for on-site or remote incident responders

2

CONTAINMENT

- Network Tactical Threat Containment
  Rule-based detection and mitigation capabilities can automatically "kill" TCP connections in real-time or to notify SOC analysts. The SOC can also manually "kill" TCP connections on the client's behalf preventing a threat actor's spread.
- Endpoint Tactical Threat Containment
  Security Operations Center (SOC) analysts can perform host isolation by locking down and isolating compromised endpoints to prevent lateral spread.

3

CRITICAL VISIBILITY THAT SUPPORTS FORENSIC INVESTIGATION

- Endpoint Activity Capture
  Continuously records, centralizes and retains vital endpoint activity including file modifications, cross-process events, registry modifications, file executions, executed binaries and network connections.
- Full Network Packet Capture (PCAP)
  Summary metadata and targeted queries into full PCAP data to confirm or explain an event with forensic analysis techniques.
- 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.
- IP Blacklist (AMP)
  Uses a proprietary Deep Packet inspection (DPI) engine to detect traffic from blacklisted IPs.
- Data Loss Analysis
  Provides outbound file capture, such as email attachments, for threat qualification and forensic analysis including SMTP, cloud storage, FTP transfers, etc.
- Packet Analyzer
  Detects suspicious behavior such as unusual ports scans, sequential scans and "spamming" machines.
- SSL Decryption and Traffic Disruption
  Detects SSL based malware for profiling and threat signature creation.
- Country Killer **[Optional but disabled by default]**
  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 **[Optional but disabled by default]**
  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.
- Bandwidth Profiler
  Detects abnormal bandwidth usage if there is a suspected internal threat (exfiltration or otherwise) or a Distributed Denial of Service (DDOS) attack.

4

CONTINUOUS MONITORING FOR RE-ENTRY

- 24x7 Continuous Montitoring
  Analysts will continue to monitor for attacker re-entry related to the successful attack leveraging details of forensic investigation as well as previous attacker TTPs.

HOW DOES IT WORK?

A BREACH OCCURS

EXTERNAL INCIDENT RESPONDERS CALLED AND DEPLOYED

INCIDENT RESPONDERS ARE IN TRANSIT

During this phase:

- Rapid Assist deploys network and endpoint sensors into the client infrastructure that sends data back to eSentire's SOC
- Threat location is identified
- SOC analysts contain the threat
- SOC continues collecting evidence on how it happened

INCIDENT RESPONDERS ARRIVE

- Forensic investigation begins
- Rapid Assist provides them with information on the incident

INCIDENT RESPONDERS ACT

- Investigation is completed
- Root cause is fixed
- Communications sent
- Lessons learned are implemented for future response activities

RAPID ASSIST CONTINUES TO MONITOR FOR RE-ENTRY AND CONFIRM NETWORK CHANGES ARE HARDENED AGAINST NEW AND RELAUNCHED ATTACKS

Rapid Assist continuously monitors for new attacks against the client

A BETTER APPROACH TO INCIDENT RESPONSE

	Traditional Incident Response (IR)	Rapid Assist
Monitoring during incident response process for additional attacks		✓
Containment of threat: host isolation		✓
Containment of threat: network communication disruption		✓
Evidence collection for forensic investigation	✓	Augments, collecting evidence prior to IR team deployment and during investigation
Determine priority, scope and root cause	✓	Augments, collecting evidence prior to IR team deployment and during investigation
Repair of affected systems	✓	
Implementation of network changes	✓	
Communication and instructions to affected partners	✓	
Confirmation of containment		✓
Post event monitoring for threat actor re-entry		✓
Confirmation that network changes are hardened against new attacks		✓
Analysis of incident for procedural and policy implications	✓	
Incorporation of lessons learned into future response activities and training	✓	

MAKE THE CASE FOR RAPID ASSIST

- Deploys within hours providing deep level visibility across network traffic and endpoints
- Vastly reduces forensic investigation timeline resulting in minimized threat actor dwell time
- Contains threats via host isolation and TCP resets preventing lateral spread and exfiltration
- Monitors for threat re-entry
- Confirms network changes and remediation measures are successful

Contact us to schedule your Rapid Assist today! ▶▶

eSENTIRE

Rapid Assist is powered by eSentire, the global leader in Managed Detection and Response (MDR) providing the last line of defense for organizations all over the world with rapid detection, response and containment of threats that evade traditional security measures 24x7x365.