DATA SHEET

# Rapid Assist

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 of how to eliminate all traces of the threat.

### MONITOR FOR REENTRY

Rapid Assist monitors for threat reentry, ensuring the network and endpoints are not susceptible to new points of attack.

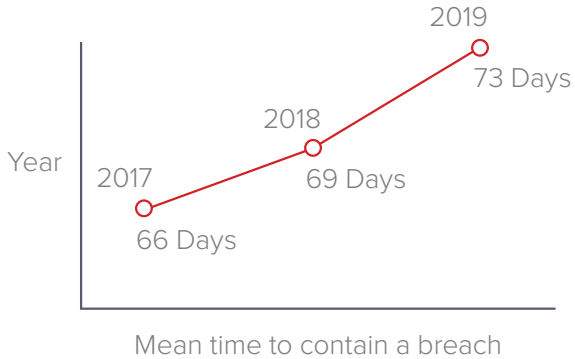
## THE PROBLEM

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.

## 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 of how an attacker gained entry so all traces and vulnerabilities can be eliminated. Post-remediation, Rapid Assist continues to monitor for threat reentry, ensuring blind spots are illuminated and your organization is safe from further attack.

In the past two years, 53% of organizations have had more than one data breach.[2]




Mean time to contain a breach

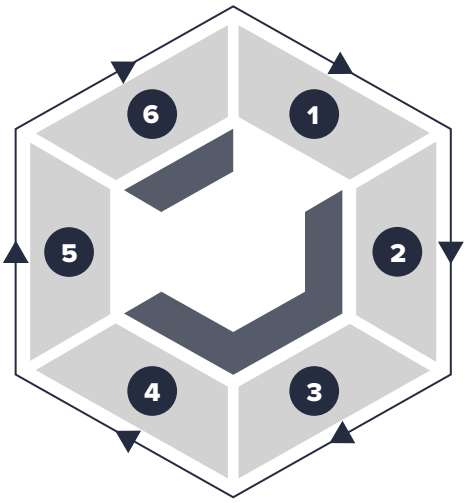
[1] *The Black Report: Decoding The Minds of Hackers 2018*
[2] *Ponemon, A Cyber Resilient Organization, 2019*

**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 reentry





24x7 threat hunting and unlimited embedded incident response

**1** | Detection
**2** | Containment
**3** | Investigation
**4** | Remediation
**5** | Confirmation/Reentry
**6** | Recovery
**7** | Post-Incident Option to Convert to (MDR)

On-Site/Remote Incident Responders

Rapid Assist

Managed Detection and Response (MDR)

## 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 reentry

## FEATURES

### 1.

**Rapid deployment**

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

### 2.

**24x7 Monitoring and threat hunting**

Always-on Monitoring
eSentire global Security Operations Centers (SOCs) monitor network traffic and endpoints around-the-clock for 30 days.

Integrated Threat Hunting
Signals that are unusual are marked as threats and fed into eSentire's analytics pipeline for human investigation and confirmation.

### 3.

**Critical visibility**

Endpoint Activity Recording
Accelerates forensic investigation, acting as a "black box" flight recorder that continuously records, centralizes and retains vital endpoint activity.

Deep Network Packet Capture and Inspection
Deep packet inspection and targeted analyst queries into metadata and full PCAP data confirm or explain events with forensic analysis techniques.

### 4.

**Rapid detection and containment**

Advanced Detection of Known, Unknown and Zero-Days
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.

Network Tactical Threat Containment

Rule-based detection and mitigation capabilities can automatically "kill" TCP connections in real-time or 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

SOC analysts can perform host isolation by locking down and isolating compromised endpoints to prevent lateral spread.

### 5.

**Continuous monitoring for reentry**

24x7 Continuous Montitoring

Analysts will continue to monitor for attacker reentry related to the successful attack by leveraging details of forensic investigation as well as previous attacker TTPs.

## HOW DOES IT WORK?

A BREACH OCCURS

ESENTIRE RAPID ASSIST TOOLS DEPLOYED BY ESENTIRE PARTNERS. ESENTIRE AND RAPID ASSIST RESPONDERS ARE ENGAGED.

ESENTIRE RAPID ASSIST COLLECTS AND CONTAINS

During this phase:

- Malicious threat actor is identified
- eSentire SOC analysts contain the threat
- eSentire SOC continues collecting evidence that facilitates on-site incident respoders


ON-SITE INCIDENT RESPONDERS ARRIVE

- Forensic investigation begins
- Rapid Assist provides responders 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 REENTRY AND CONFIRM NETWORK CHANGES ARE HARDENED AGAINST NEW AND RELAUNCHED ATTACKS

Day 0

Rapid Assist continuously monitors for new attacks against the client.

Day 30

## MAKE THE CASE FOR RAPID ASSIST

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

## A BETTER APPROACH TO INCIDENT RESPONSE

| | Traditional Incident Response (IR) | eSentire 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 reentry | | ✓ |
| 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 | ✓ | |

*if esENDPOINT is deployed

**Learn more about Rapid Assist today!**

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.