eSENTIRE

DATA SHEET:

Minutes Matter

How swift response to cyberattacks saves businesses money and prevents operational disruption.

In times of emergency - like moving swiftly to extinguish a kitchen fire before it can spread and cause widespread damage - minutes matter. For businesses, "minutes matter" is just as applicable when it comes to containing cyber threats before they can spread. The faster your organization can respond to a breach, the less damaging and costly it is.

Every year, IBM releases the Cost of a Data Breach Report, regarded as one of the most comprehensive reports of its kind. In 2021, the average cost of a data breach was $4.24M. Unsurprisingly, the length of the overall breach lifecycle and how fast organizations moved to contain threats correlated with the overall cost. Unfortunately, the majority of organizations are still lagging way behind speedy threat actors and are paying the price for it.

NOT FAST ENOUGH

212 DAYS
to identify in 2021

75 DAYS
average time to contain in 2021

15 HOURS OR LESS
the amount of time it takes majority of hackers to breach and exfiltrate data

$14,774
COST PER DAY

$616
COST PER HOUR

$10.25
COST PER MINUTE

AVERAGE BREACH COST AT THE 73-DAY MARK

$1.1M

2021 Cost of a Data Breach Study

Numbers are based on four cost factors: detection and escalation, post data breach response, notification to stakeholders and lost business (lost revenue, business disruption, downtime, customer churn, etc.). Notice that these cost factors are chronological. If a breach is swiftly and effectively addressed at the detection and escalation point, then the subsequent cost factors are drastically reduced if not eliminated completely. Similarly, a small kitchen fire costs substantially less than a burned down the house.

In the context of "minutes matter," it is the 75 day average time to contain mark and the associated cost of $1.1M is the focus. The time to contain a threat is the most critical cybersecurity key performance indicator (KPI) that eSentire's Managed Detection and Response (MDR) platform dramatically improves for our customers. The following are three real-world examples where swift response to contain advanced threats saved our customers' networks from potential catastrophe and over $1M in breach costs.

NOTE: The cost savings portions of these case studies assume that if eSentire's MDR solution was not in place, the customer would have contained the breach by other means at the 75 - day MTTC mark. We used the extrapolated daily, hourly and minute costs from the 2021 Cost of a Data Breach Study to calculate the cost savings.

Third-Party Serves as Staging Point for cryptojacking Attack Using Powershell

Attack type:

Zero-day exploit, PowerShell, Cryptomining Malware

Attack summary:

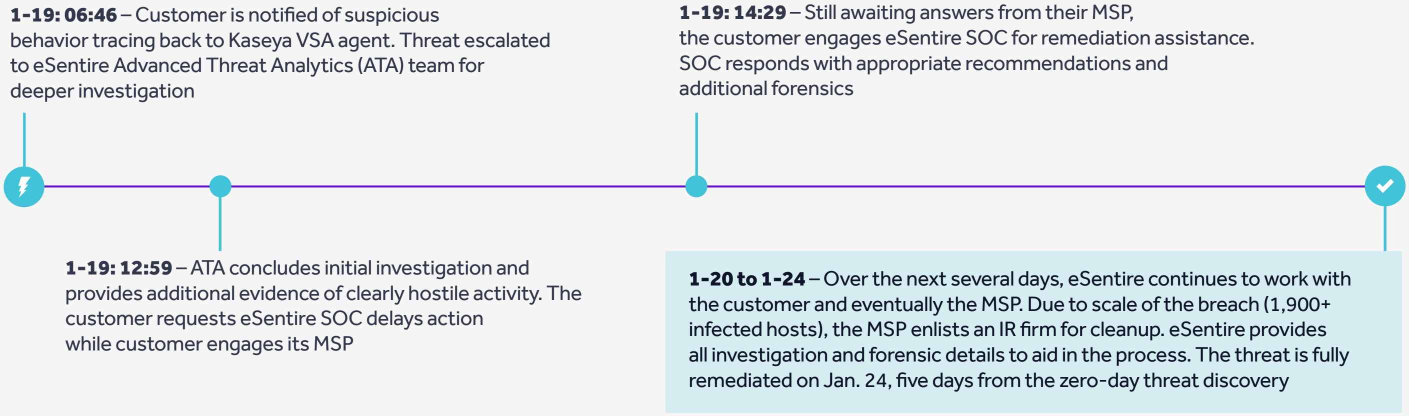
From January 19 - 24, 2018, eSentire Security Operations Center (SOC) analysts observed a threat actor leverage a zero-day vulnerability through Kaseya's popular Virtual Systems Administrator agent. The threat actor gained access through the exploit and leveraged Powershell commands to download cryptomining malware. eSentire's analysts worked with the customer and eventually their managed services provider (MSP). It was revealed that the malware was present on 1,190 systems across the MSP's customer base. eSentire notified Kaseya of the vulnerability and the threat was fully remediated in five days.

Time to contain breach:

5 days

Cost savings:

$1.1M (ATTC Cost) -
$73,870 ($14,774 x 5 Days – eSentire TTC) = **$1,026,130**



1-19: 06:46 – Customer is notified of suspicious behavior tracing back to Kaseya VSA agent. Threat escalated to eSentire Advanced Threat Analytics (ATA) team for deeper investigation

1-19: 12:59 – ATA concludes initial investigation and provides additional evidence of clearly hostile activity. The customer requests eSentire SOC delays action while customer engages its MSP

1-19: 14:29 – Still awaiting answers from their MSP, the customer engages eSentire SOC for remediation assistance. SOC responds with appropriate recommendations and additional forensics

1-20 to 1-24 – Over the next several days, eSentire continues to work with the customer and eventually the MSP. Due to scale of the breach (1,900+ infected hosts), the MSP enlists an IR firm for cleanup. eSentire provides all investigation and forensic details to aid in the process. The threat is fully remediated on Jan. 24, five days from the zero-day threat discovery

Read the full case study Here

Stay Prepared

While MDR primarily focuses on detection and containment of advanced threats, eSentire offers Managed Risk Services and Digital Forensics and Incident Response Services that covers the other aspects of the breach lifecycle, ensuring your organization is supported every step of the way.

24/7 On-Demand Incident Response

- 4-hour or 24-hour remote threat suppression SLA
- Committed SLAs for malware analysis, phone response and boots on ground
- Complete Incident Lifecycle support

Incident Response Consulting and Managed Risk Services

- Incident Response Plan Development or Assessment
- Tabletop Exercises
- Virtual CISO Services

$2.46M

Average breach cost savings with an IR Team and Plan in place vs. when not in place.

Ponemon 2019 Cost of a Data breach

MDR for Endpoint Thwarts Advanced Threat Actor Using Machine Learning

Attack type:

Malware, PowerShell

Attack summary:

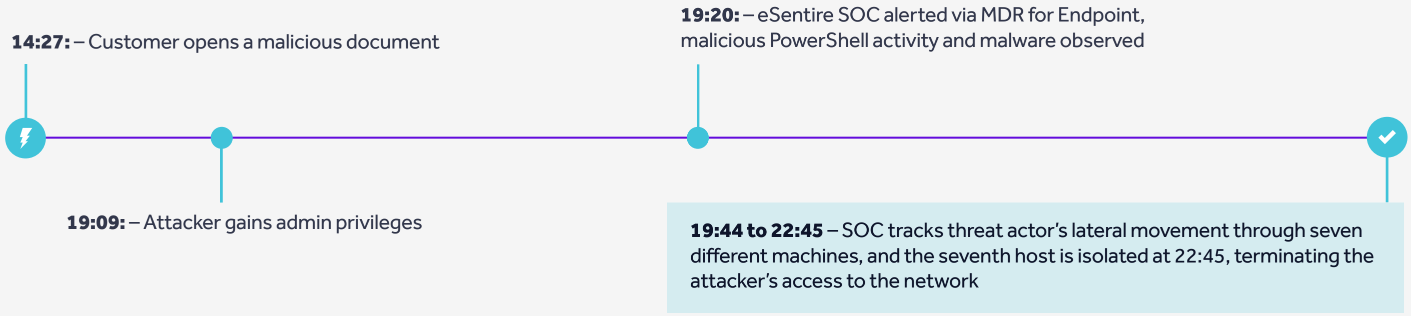
At a customer in the legal industry, a threat actor posing as a student from a local university tricked an assistant into opening a malicious document containing malware. The threat actor successfully escalated to administrative privileges using Powershell commands. eSentire's proprietary BlueSteel machine learning application picked up the suspicious Powershell activity and isolated the compromised host. A game of cat and mouse followed across seven infected hosts.

Time to contain breach:

7.5 hours

Cost savings:

$1.1M (ATTC Cost) -
$4,620 ($616 x 7.5 hours) – eSentire TTC) = **$1,095,380**



14:27: – Customer opens a malicious document

19:09: – Attacker gains admin privileges

19:20: – eSentire SOC alerted via MDR for Endpoint, malicious PowerShell activity and malware observed

19:44 to 22:45 – SOC tracks threat actor's lateral movement through seven different machines, and the seventh host is isolated at 22:45, terminating the attacker's access to the network

22 Minutes: Compromise to containment

Attack type:

Malware, PowerShell

Attack summary:

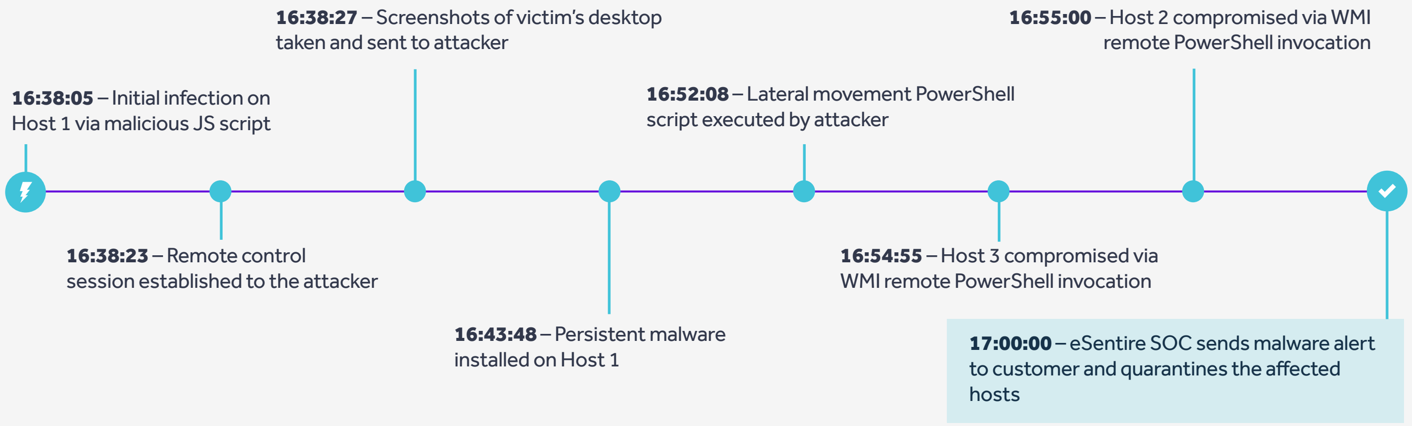
A customer at a financial services unknowingly downloaded and launched a malicious Javascript file via Internet Explorer. Utilizing a combination of MDR for Endpoint, which detected the malicious JavaScript file, machine learning from BlueSteel that detected the malicious PowerShell command and MDR for Network, which flagged a suspicious web redirect, eSentire was able to isolate the three compromised hosts and terminate the attackers' command and control channel to the network.

Time to contain breach:

22 minutes

Cost savings:

$1.1M (ATTC Cost) -
$225 ($10.25 x 22 minutes) – eSentire TTC) = **$1,099,775**



16:38:05 – Initial infection on Host 1 via malicious JS script

16:38:23 – Remote control session established to the attacker

16:38:27 – Screenshots of victim's desktop taken and sent to attacker

16:43:48 – Persistent malware installed on Host 1

16:52:08 – Lateral movement PowerShell script executed by attacker

16:54:55 – Host 3 compromised via WMI remote PowerShell invocation

16:55:00 – Host 2 compromised via WMI remote PowerShell invocation

17:00:00 – eSentire SOC sends malware alert to customer and quarantines the affected hosts

Read the full case study Here

Included Response and Remediation Actions

		eSentire	The Other Guys
Endpoint Threat Containment	MDR - Response	✓	✓
Quarantine Files	MDR - Response	✓	You're Responsible
Hash Blocking	MDR - Response	✓	You're Responsible
Account and Access Suspension	MDR - Response	✓	You're Responsible
Network Isolation	MDR - Response	✓	You're Responsible
Blocking Compromised Email Accounts	MDR - Response	✓	You're Responsible
Terminate Malicious Processes	MDR - Remediation	✓	You're Responsible
Facilitated Retroactive Email Purges	MDR - Remediation	✓	You're Responsible
System Reboot	MDR - Remediation	✓	You're Responsible
Removal of Registry Keys/Values	MDR - Remediation	✓	You're Responsible
Threat Eradication	MDR - Remediation	✓	You're Responsible
Root Cause Analysis	eSentire MDR and DFIR	✓	Limited
Digital Forensics Analysis	DFIR	✓	Limited
Crime Scene Reconstruction	DFIR	✓	Limited
E-Discovery	DFIR	✓	Limited

Ready to get started?

We're here to help! Submit your information and an eSentire representative will be in touch.

Contact Us

If you're experiencing a security incident or breach contact us ☎ 1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.