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 cyberthreats before they can spread. The faster your organization can respond to a breach, the less damaging and costly it is.

Every year, the Ponemon Institute releases the Cost of a Data Breach Report, regarded as one of the most comprehensive reports of its kind. In 2019, the average cost of a data breach was $3.92M. 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

73
DAYS
the mean time to contain a data breach in FY2019

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

$15,433
COST PER DAY

$643
COST PER HOUR

$10.71
COST PER MINUTE

AVERAGE BREACH COST AT THE 73-DAY MARK

$1.12M

Ponemon 2019 Cost of a Data Breach Report

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 73-day mean time to contain mark and the associated cost of $1.12M 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 73-day MTTC mark. We used the extrapolated daily, hourly and minute costs from the 2019 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:
$1.12M - $77,165 ($15,433 x 5 Days) = **$1,042,835**

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 advisory services that covers the other aspects of the breach lifecycle, ensuring your organization is supported every step of the way.

Virtual CISO (vCISO)

- Security Program Maturity Assessment
- Security Incident Response Planning

Robust services include incidence response (IR) tabletop exercises, public relations, notification policy and more.

Penetration testing and red team exercises

Test your organization's ability to respond to simulated threats with customized penetration testing and/or red team exercises.

$360,000
Total breach cost reduction when having an Incident Response team in place

$320,000
Total breach cost reduction when Incident Response plan is regularly tested

Ponemon 2019 Cost of a Data breach

esENDPOINT 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:

$1.12M - $4,822 ($643 x 7.5 hours) = **$1,115,178**

14:27: – Customer opens a malicious document

19:09: – Attacker gains admin privileges

19:20: – eSentire SOC alerted via esENDPOINT, 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

Read the full case study **HERE**

The MDR toolkit

Threat blocking and containment techniques used by eSentire SOC analysts

Network blocking
(TCP/IP reset) - esNETWORK

Endpoint host isolation
esENDPOINT

IP blacklisting
esNETWORK

Geo-blocking
esNETWORK

Executable blocking
esNETWORK

Policy based blocking
esNETWORK,
Managed Endpoint Defense

Hash blocking
esENDPOINT

Suspending credentials
SOC Guidance

22 MINUTES: COMPROMISE TO CONTAINMENT

Attack type:

Malware, PowerShell

Attack summary:

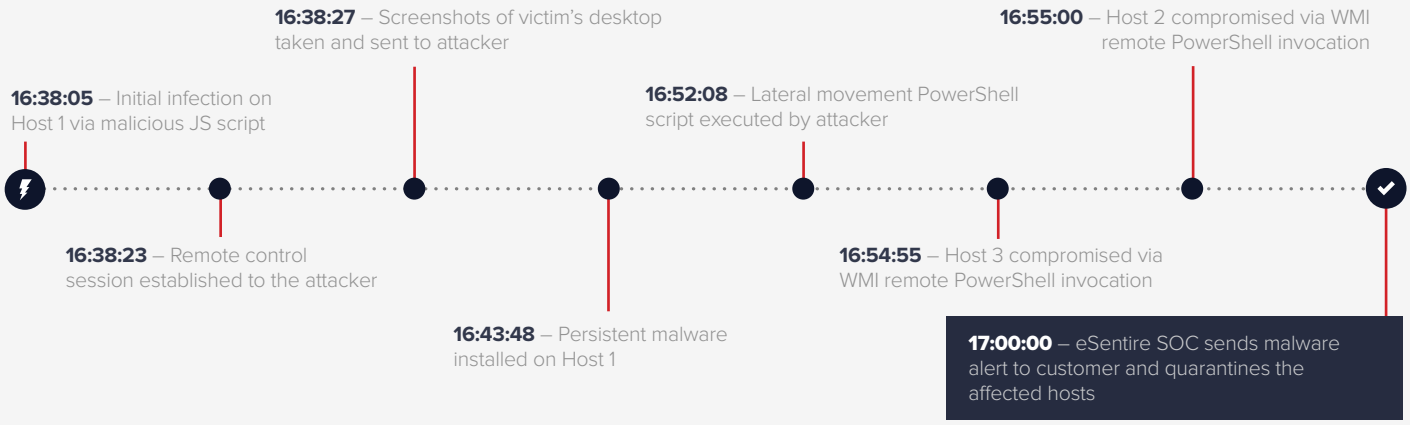
A customer at a financial services unknowingly downloaded and launched a malicious Javascript file via Internet Explorer. Utilizing a combination of esENDPOINT, which detected the malicious JavaScript file, machine learning from BlueSteel that detected the malicious PowerShell command and esNETWORK, 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:

$1.12M - $241 ($10.71 x 22 minutes) = **$1,119,759**



Read the full case study **HERE**

eSENTIRE

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks 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 $5.7 trillion AUM in the financial sector alone, 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**.