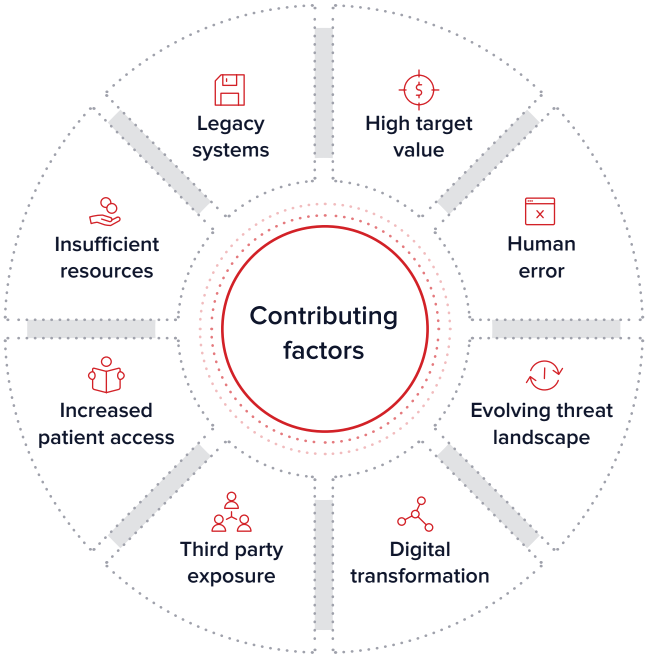
SOLUTION BRIEF:

Focus on Cybersecurity: Healthcare

Healthcare organizations and their business associates are a one-stop-shop for some of the most lucrative cyberattacks. Patient and employee information, proprietary research and ransom of critical healthcare systems represent opportunities to extract substantial value for cybercriminal efforts. In addition, potentially leaky third parties, flexible patient access, stress induced human error and expanding usage of cloud and internet connected medical devices are all contributing factors to an overwhelming digital landscape that must be defended.

As public healthcare breaches continue to make national headlines and regulatory bodies increase penalties, the spotlight on cyber defenses has never been greater. Despite 72%[1] of cybersecurity teams reporting additional investment in their programs, healthcare breaches increased 37 percent year-over-year[2] resulting in reputational damage, patient endangerment and exposure of over 41 million records.



Top Sources of Malicious Security Incidents[1]

1. Email (phishing, spear phishing, whaling, business email compromise)
2. Hacker (cybercriminal)
3. Social engineer (non-phishing)
4. Malicious insider
5. Nation-state
6. Hactivist

Top Sources of Benign Security Incidents[1]

1. Negligent insider
2. Vendor or consultant
3. Third party partner (non-vendor or consultant)
4. Researcher

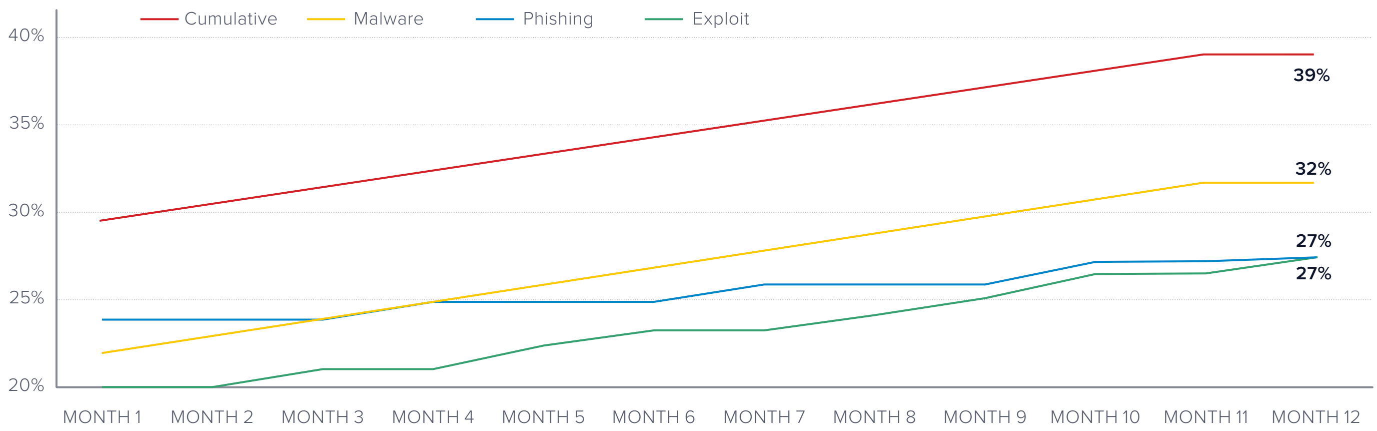
[1] *2019 HIMSS Cybersecurity Survey*

[2] *https://www.hipaajournal.com/2019-healthcare-data-breach-report/*

eSentire: Observing Risks to the Healthcare Industry for Two Decades

We understand the unique challenges your cybersecurity team faces. For two decades, we've seen the dynamic nature of threats that specifically target healthcare organizations and their associates. For example, in 2019 our Security Operation Centers (SOCs) detected an alarming number of threat actors that were able to bypass healthcare providers' existing security controls.

Observed probability of one or more security events due to a bypass of existing security controls per location



And, industry reports indicate that healthcare organizations have the highest conversion rate from incident to data disclosure of all observed industries. This is due to the speed at which attackers have reported they can breach the perimeter, identify critical data and exfiltrate before their presence is identified

Unfortunately, the financial consequences of data disclosure have proven devastating to healthcare organizations. Detection and escalation, notification, post breach and lost business costs are the highest amongst observed industries. Due to the sophisticated nature of healthcare attackers and a multitude of contributing factors, cybersecurity teams continue to see rising timeframes to identify and contain security incidents.

84% Attackers that can breach the perimeter of healthcare organizations and exfiltrate data in 15 hours or less[3]

65% Conversion rate of security event to data disclosure - the highest amongst measured industries[4]

$429 per record lost[5]

$6.45M average cost[5]

$2.33M in lost business costs[5]

$2M in detection and escalation costs[5]

$1.76M in post breach costs[5]

$384K in notification costs[5]

236DAYS Mean time to identify[5]

93DAYS Mean time to contain[5]

[3] *Nuix Black Report*

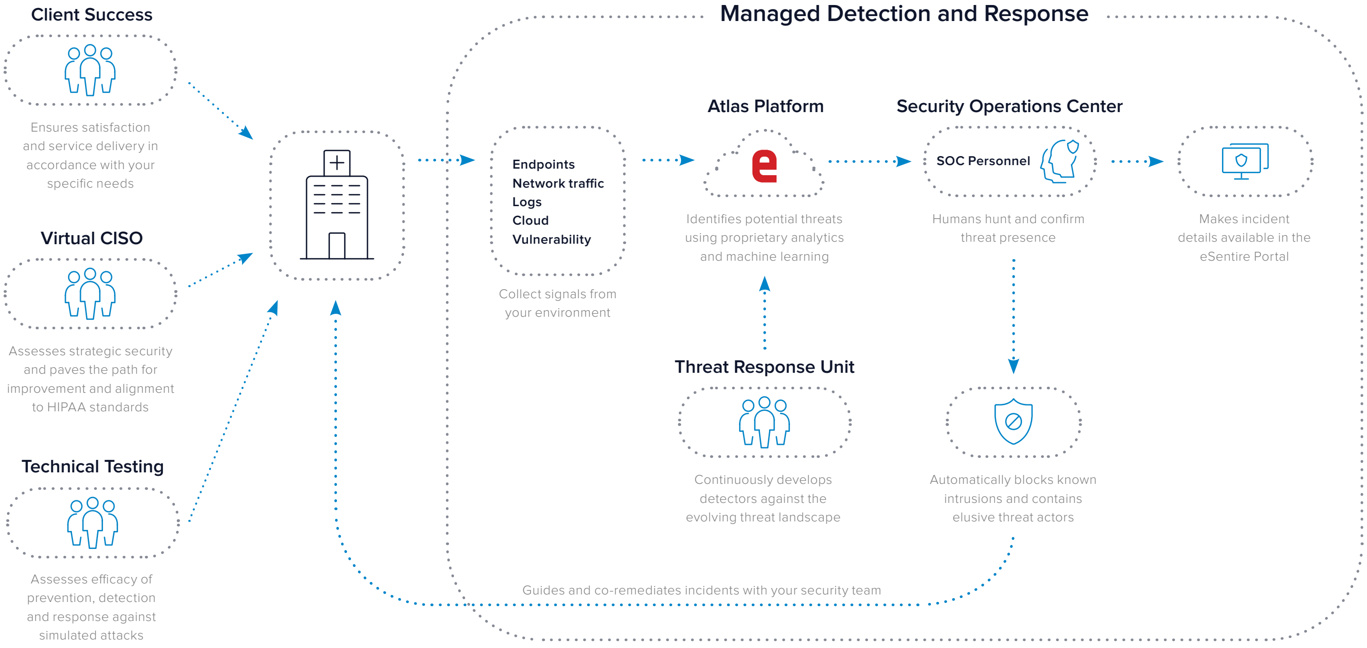
[4] *2019 Verizon DBIR Report*

[5] *2019 Ponemon Cost of a Data Breach Report*

A Comprehensive Approach to Healthcare Protection

Whether your organization is an individual practice or a large regional provider with multiple facilities, threat actors are going to capitalize on vulnerable systems and human nature. Ultimately, the difference between business protection and business disruption will come down to the speed at which you can identify and contain an attack.

At eSentire, our comprehensive approach helps organizations test, mature, measure and protect their environments from a multitude of risk factors. Our Managed Detection and Response (MDR) services rapidly identify and contain threats that bypass traditional security controls. Ingesting signals from your on-premises, cloud and hybrid environments, we combine endpoint, network, log, vulnerability and cloud data to identify known and elusive threats. Averaging 20 minutes from identification to containment, we ensure attackers don't have the time to achieve their objectives. Our Risk Management services test your existing defenses against simulated attacks, assess and measure your security posture and pave a path for resiliency that aligns to regulatory frameworks. All of these services are supported by a dedicated team focused on delivering in accordance with your organization's unique requirements and business objectives.



Client Success

Ensures satisfaction and service delivery in accordance with your specific needs

Virtual CISO

Assesses strategic security and paves the path for improvement and alignment to HIPAA standards

Technical Testing

Assesses efficacy of prevention, detection and response against simulated attacks

Managed Detection and Response

Endpoints
Network traffic
Logs
Cloud
Vulnerability

Collect signals from your environment

Atlas Platform

Identifies potential threats using proprietary analytics and machine learning

Security Operations Center

SOC Personnel

Humans hunt and confirm threat presence

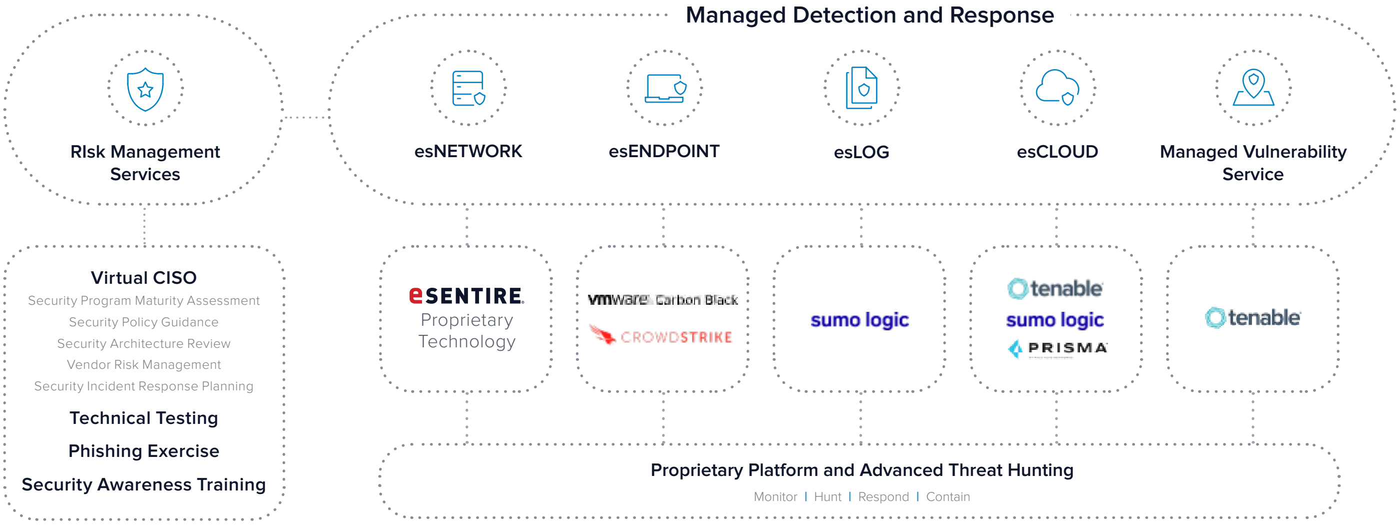
Makes incident details available in the eSentire Portal

Threat Response Unit

Continuously develops detectors against the evolving threat landscape

Automatically blocks known intrusions and contains elusive threat actors

Guides and co-remediates incidents with your security team



RIsk Management Services

Virtual CISO

Security Program Maturity Assessment
Security Policy Guidance
Security Architecture Review
Vendor Risk Management
Security Incident Response Planning

Technical Testing

Phishing Exercise

Security Awareness Training

Managed Detection and Response

esNETWORK

esENDPOINT

esLOG

esCLOUD

Managed Vulnerability Service

eSENTIRE Proprietary Technology

vmware Carbon Black
CROWDSTRIKE

sumo logic

tenable
sumo logic
PRISMA

tenable

Proprietary Platform and Advanced Threat Hunting

Monitor | Hunt | Respond | Contain

eSentire Service Alignment to Healthcare’s Top Malicious Incident Causes

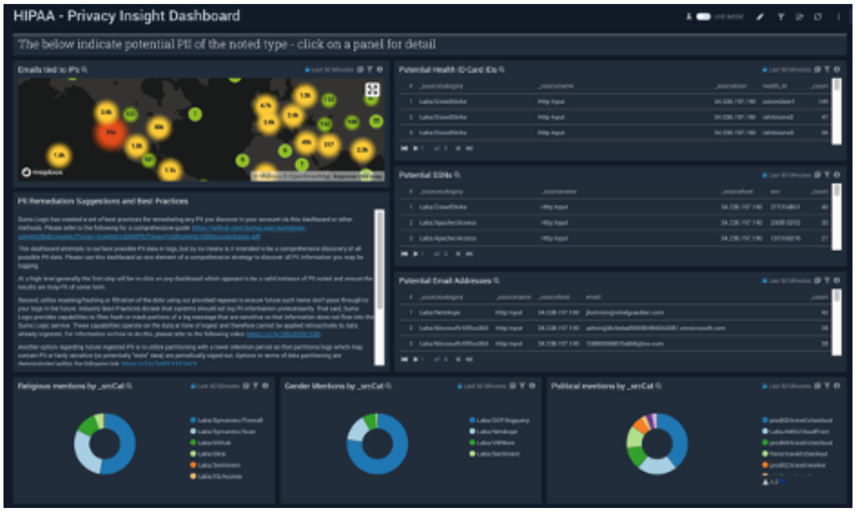
	eSentire Managed Detection and Response	eSentire Risk Management Services
Email (phishing, spear phishing, whaling, business email compromise)	• esENDPOINT • esLOG • esNETWORK	• Security Awareness Training • Phishing Exercise
Hacker (cybercriminal)	• esNETWORK • esENDPOINT • esLOG • esCLOUD • Managed Vulnerability Service	• Virtual CISO • Security Program Maturity Assessment • Security Policy Guidance • Security Architecture Review • Security Incident Response Planning • Technical Testing
Social engineer (non-phishing)		• Security Awareness Training • Phishing Exercise
Malicious insider	• esENDPOINT • esLOG • esCLOUD	• Virtual CISO • Security Program Maturity Assessment • Security Policy Guidance • Security Architecture Review • Security Incident Response Planning • Vendor Risk Management • Technical Testing
Nation State and hacktivists	• esNETWORK • esENDPOINT • esLOG • esCLOUD • Managed Vulnerability Service	• Virtual CISO • Security Program Maturity Assessment • Security Policy Guidance • Security Architecture Review • Security Incident Response Planning • Technical Testing

Service Alignment to Healthcare’s Top Benign Incident Causes

Negligent insider	• esENDPOINT • esLOG • esCLOUD	• Virtual CISO • Security Policy Guidance • Security Architecture Review • Security Incident Response Planning • Technical Testing
Vendor, consultant, third party partner or researcher	• esNETWORK • esENDPOINT • esLOG • esCLOUD	• Virtual CISO • Vendor Risk Management • Technical Testing

Helping Your Organization Meet HIPAA Requirements

The Office for Civil Rights has increased regulatory requirements and penalties totaling $116M to date for non-compliance of HIPAA rules. In the wake of a record-breaking year for healthcare breaches, oversight is expected to increase putting additional pressures on constrained security teams. Our MDR and Risk Management services are designed to help you navigate the complexity of HIPAA standards and put in place corrective controls. To see a detailed breakdown of how eSentire's services align with HIPAA rules [click here](#).



HIPAA - Privacy Insight Dashboard

The below indicate potential PII of the noted type - click on a panel for detail

Emails tied to IPs

Potential Health ID Card IDs

Potential SSNs

PII Remediation Suggestions and Best Practices

Potential Email Addresses

Religious mentions by _srcCat

Gender Mentions by _srcCat

Political mentions by _srcCat

Experience the eSentire Difference

Organizations all over the world trust eSentire as their last line of defense and trusted advisor against an overwhelming threat landscape. Our 97 percent client retention rate is testament to delivering on our core mission: a client's network can never be compromised. Our specialized teams that deliver and support our services are consistently developing the latest methods that ensure your organization is protected against the latest threat actors and aligned to stringent HIPAA requirements that keeps your patients, employees and systems safe from disruption.

97%
CUSTOMER RETENTION RATE

750+
GLOBAL CUSTOMERS

ACROSS
6
CONTINENTS

IN
48
COUNTRIES

6+
INVESTIGATIONS EVERY MINUTE

640+
CONFIRMED SECURITY INCIDENTS A DAY

	eSentire MDR	PSUEDO MDR
24x7 always on monitoring	✓	Limited
Full spectrum visibility (PCAP, Endpoint, Log, Vulnerability, Cloud)	✓	Limited
Detection utilising signatures and IOCs	✓	✓
Detection of unknown attacks leveraging patterns and behavioural analytics	✓	Limited
Continuous elite threat hunting	✓	✗
Alerting of suspicious behaviour	✓	Limited
Alerts	✓	✓
Confirmation of true positive	✓	Limited
Remediation recommendations	✓	✓
Tactical threat containment on client's behalf	✓	Limited
24x7 investigation and SOC support	✓	✗ Need IR Retainer
Incident response plan	✓	✗ Need IR Retainer
Remediation verification	✓	✗ Need IR Retainer

> “eSentire has helped my business by being very adept at answering any questions and providing excellent and prompt notices of any potential issues or threats against our network.”

IT Specialist
Small Business Healthcare Company

> “eSentire has helped my business by enabling 24x7x365 monitoring of our cloud environments and endpoints.”

Chief Security Officer
Medium Enterprise Healthcare Company

Ready to get started? We're here to help.

Reach out schedule a meeting to learn more about MDR

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 $6 trillion AUM, 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**.