eSENTIRE

SOLUTION BRIEF:

Multi-Signal Managed Detection and Response for Healthcare Delivery Organizations

Preventing critical operational disruption with 24/7 protection from ransomware, business email compromise, system exploitation and insider threats.

The widespread reliance on the cloud and the use of electronic health records by healthcare providers such as patient clinics, hospitals, and business associates has turned healthcare delivery organizations (HDOs) into prime targets for cyberattacks.

In addition, third-party exposure, flexible access to patient care, human error, legacy operating systems, and the increasing adoption of internet-connected medical devices and other healthcare IoT (HIoT or IoMT), are all contributing factors to an ever-expanding attack surface that must be defended.

Skilled adversaries now target the healthcare sector over others due to the nature of the data that HDOs have access to–patients' electronic protected health information (ePHI).

In recent years, the severity of cyberattacks, along with how fast cybercriminals can breach the perimeter to exfiltrate healthcare data, means that your security team must be able to minimize attacker dwell time and reduce the overall scope of the damage. This means prioritizing the speed of your response–how fast your team can identify, contain, and respond to a cyber threat becomes crucial in limiting operational disruption.

Why Is The Healthcare Sector A Growing Target?

- Electronic protected health information (ePHI) is more valuable than other types of information and often fetch top dollar on the Dark Web
- Healthcare institutions are likely to pay the extortion or ransomware demands in the wake of massive operational disruptions
- HDOs struggle with prioritizing investments in security tools and digital transformation to migrate off of outdated systems while also prioritizing patient care
- Third-party risk exposure stemming from a lack of due diligence to ensure third-party vendors and service providers are taking the proper steps to protect sensitive information
- Insufficient investment in hiring enough skilled cybersecurity practitioners
- Insufficient investment in security tools and technology to mitigate a data breach
- Difficulty identifying malicious insiders

Healthcare attack timeframes to breach the perimeter and exfiltrate data

23% *< 5 hours*	**18%** *5-10 hours*	**20%** *10-15 hours*
23% *15-20 hours*	**11%** *20-25 hours*	**5%** *25 hours*

As healthcare breaches continue to make national headlines, many HDOs are outsourcing their cybersecurity needs to a Managed Detection and Response (MDR) provider that can protect their patients and critical business operations with 24/7 threat detection, investigation, and response.

Introducing eSentire

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate, and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry—financial services. Over the last two decades we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers (SOCs), hundreds of cyber experts, and 1000+ customers across 70+ countries, we have scaled to deliver cybersecurity services across highly regulated industries with a proven track record of success in securing businesses across the healthcare sector including healthcare institutions, medical technology providers, and pharmaceutical companies.

At eSentire, we go beyond the market's capability in threat response and specifically address cybersecurity risks for the manufacturing sector. eSentire's multi-signal MDR approach ingests endpoint, network, log, cloud, asset and vulnerability data that enables complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit are applied to captured data identifying known & unknown threats including suspicious activity and zero-day attacks. With two 24/7 Security Operations Centers staffed with cyber experts and Elite Threat Hunters, an industry-leading XDR Cloud Platform, and refined security operations processes, eSentire can detect and respond to cybersecurity threats in the manufacturing industry with a Mean Time to Contain of 15 minutes.

At eSentire, We Support Healthcare Delivery Organizations By:

- Supporting patient care with secure services including 24/7 threat detection, investigation and complete response
- Protecting and preventing healthcare organizations from operational disruption caused by ransomware gangs and state-sponsored actors
- Securing patients' electronic protected health information (ePHI)
- Mitigating third-party risk and supply chain risk
- Ensuring you and your business associates meet HIPAA Security compliance requirements

Our global 24/7 SOCs have discovered instances of ransomware gangs targeting our healthcare customers and have interrupted their activities before they could establish a foothold by:

- Using endpoint to prevent the disabling of defenses
- Detecting malicious administrative activity through remote access tools using proprietary machine learning algorithms
- Blocking active attempts to deploy credential collection tools, malware payloaders and even multiple ransomware attacks

Whether your organization's assets are stored in the cloud, on-premise, or in a hybrid environment, we have the visibility to see what other MDR providers miss.

As cyber threats increase, our Threat Response Unit (TRU) and 24/7 SOCs have developed extensive experience with the vulnerabilities, advanced persistent threats, and TTPs that impact the healthcare industry. By understanding your environment and attack surface, we develop specific detections across our Atlas XDR Cloud platform that filter out noise and identify high priority security events before they can impact your business. High fidelity threats are automatically blocked and suspicious activity requiring human investigation is summarized, enriched and shared with our 24/7 SOC Analysts and Elite Threat Hunters for assessment and manual containment with a Mean Time to Contain of 15 minutes.

Key Healthcare Industry Challenges	How eSentire Managed Detection & Response Helps
Protecting Patient Healthcare Information	We are adept at securing all forms of sensitive data, such as electronic protected healthcare information (ePHI), HIPAA protected data, along with financial information (PII) and credit card or payment transfer services (PCI). Our 24/7 Elite Threat Hunters and SOC Cyber Analysts actively hunt for threats across your environment. We detect intrusions and contain attacks before attackers can establish a foothold to steal patient data, or disrupt your critical operations.
Operational Disruption	We detect malicious administrative activity through remote access tools and stop intrusions before malware payloaders and multiple ransomware attacks can be deployed throughout your environment.
Avoiding Regulatory and Compliance Violations	Our MDR and Managed Risk services are designed to help you navigate the complexity of HIPAA Security Standards and put corrective controls in place. Our SOC leverages proven runbooks which include detectors mapped to requirements and reporting measures for PCI, PII, SOX, GDPR, CCPA as well as state-level regulations.
Third-Party Risk: Securing Business Associates and Technology	We can assist with creating a third-party risk management program for your business and support securing M&A and digital transformation activities. We identify core services, including electronic medical records (EMR), drug management, time tracking, file share and document signing, and prioritize these services for monitoring. Our MDR services have repeatedly caught and stopped vendor compromises before the vendor reported the vulnerability.
Becoming a Victim of Ransomware Attacks	We monitor your attack surface 24/7 to discover intrusion attempts and prevent the pervasive deployment of malware and ransomware. • We support multi-signal coverage, ensuring visibility across endpoint, network, log, cloud, and other data sources for deep investigation and response capabilities. • We offer endpoint protection to prevent your defenses from being disabled.

eSentire in Action

eSentire protects over $6.5 trillion in assets across highly regulated industries, including healthcare institutions, medical technology, and pharmaceuticals. **In fact, more than 2.5 million patients pass through healthcare facilities that are protected by eSentire.** This includes defending our healthcare customers from a 200% increase in cyberattacks during the COVID-19 pandemic.

eSentire Cybersecurity Services Portfolio

Our cybersecurity services portfolio is designed to stop breaches, simplify security, and minimize your business risk. We provide around-the-clock threat protection that is proactive, personalized, and cost-effective.

Managed Risk Services
Strategic services including Vulnerability Management and Managed Phishing and Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation, and continuously advance your cybersecurity program.

Managed Detection and Response
We deliver complete and robust Response by combining cutting-edge machine learning XDR, 24/7 threat hunting expertise and security operations leadership. We hunt and disrupt known & unknown threats before they impact your healthcare operations and patients.

Digital Forensics and Incident Response
Battle-tested Incident Commander-level expertise driving incident response, remediation, recovery, and root cause analysis. Our On Demand 24/7 Incident Response retainers include Emergency Incident Response, Security Incident Response Planning Services and an industry-leading 4-hour Threat Suppression SLA.

eSentire MDR features include:

- ✔ 24/7 Always-On Monitoring
- ✔ 24/7 Live SOC Cyber Analyst Support
- ✔ 24/7 Threat Hunting
- ✔ 24/7 Threat Disruption And Containment Support
- ✔ Mean Time To Contain: 15 Minutes
- ✔ Machine Learning XDR Cloud Platform
- ✔ Multi-Signal Coverage And Visibility
- ✔ Automated Detections With Signatures, IOCs And IPs
- ✔ Security Network Effects
- ✔ Detections Mapped To Mitre Att&Ck Framework
- ✔ 5 Machine Learning Patents For Threat Detection And Data Transfer
- ✔ Detection Of Unknown Attacks Using Behavioral Analytics
- ✔ Rapid Human-Led Investigations
- ✔ Threat Containment And Remediation
- ✔ Detailed Escalations With Analysis And Security Recommendations
- ✔ eSentire Insight Portal Access And Real-Time Visualizations
- ✔ Threat Advisories, Threat Research And Thought Leadership
- ✔ Operational Reporting And Peer Coverage Comparisons
- ✔ Named Cyber Risk Advisor
- ✔ Business Reviews And Strategic Continuous Improvement Planning

Why Healthcare Organizations Choose eSentire

There is no end to Cyber Risk so go into battle with the best.

- **Recognized** - The Authority in Managed Detection and Response
- **Simple** - We absorb the complexity of cybersecurity so you can prioritize your operations
- **Scalable** - Industry's most powerful machine learning XDR Cloud Platform can ingest data at the pace and scale of your business
- **Precise** - We're on the cutting-edge of attacker Tactics, Techniques and Procedures mitigating your risk of being breached
- **Fast** - Extreme time to value as you will be fully operational within weeks
- **Responsive** - We own the R in MDR to provide extensive response capabilities and threat hunting around the clock
- **Compliance -** Our SOC leverages proven runbooks which include plays to manage issues and reporting for HIPAA, PII, PCI, GDPR, CCPA as well as state-level rules such as NYCRR 500
- **Cost-Effective** - 24/7 threat protection, detection and response at a fraction of the cost of DIY security programs
- **Complete** - Multi Signal Coverage and comprehensive security services support
- **Team** - Cyber Risk Advisor + SOC Cyber Analyst and Elite Threat Hunters on guard for your business 24/7

$6.5T+
Total ALUM

1000+
Customers in 70+ Countries

20.5M
Daily Signals Ingested

3M
Daily Atlas XDR Automated Disruptions

6000
Daily Human-led Investigations

700
Daily Escalations

400
Daily Threat Containments

15min
Mean Time to Contain

- **Results -** Your Organization Can Expect:
  - ~50% reduction in threat detection and response total cost of ownership (TCO)
  - +50% additional coverage on top of commodity threat intelligence, leveraging proprietary technology and our Insurance network of customers
  - 99% reduction in threat detection and containment times from global averages

Certified

AICPA SOC 2 (formerly SAS 70 Reports) · ISO 27001 Certified

Mapped

MITRE ATT&CK™

Awarded

IDC Analyze the Future LEADER · Cyber Security Excellence Awards WINNER 2021 · MSSP Alert Top 250 MSSPs 2021 Edition NAMED #10 & TOP MDR PROVIDER · Global Infosec Awards WINNER Cyber Defense Magazine 2021

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 1000+ organizations in 70+ countries 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**.