TOTEM POLE TECHNOLOGY

eSENTIRE

SOLUTION BRIEF:

Multi-Signal Managed Detection and Response for Insurance Companies

With Sensitive Data And Vulnerable Attack Surfaces, Insurers Must Protect Their Policyholders And Business Reputation From Cyber Threats

Whether you operate as an insurance carrier, brokerage, dealer, or underwriter, your organization has unparalleled access to valuable information across all facets of your clients' business and consumer life. Threat actors know how to launch attacks that can lead to crippling ransomware outages and significant reputational damage for your organization.

Although your company may sell cyber insurance coverage to your clients, it cannot be underestimated that your organization is a high profile target given the vast Personal Identifiable Information (PII), financial, and even health information under your purview.

A combination of business factors and security vulnerabilities are increasing the risks you face as attackers seek to:

- Leverage stolen policyholder data to target your clients and negotiate ransom payments that fall within their coverage to guarantee payment.
- Fine-tune their campaigns and craft highly-convincing phishing campaigns, which can sour the relationship between policyholders and your organization.
- Retaliate against insurance firms for representing certain clients.
- Use insider information to island hop and disable defenses.
- Use business email compromise (BEC) attacks for claim payment requests and invoices.

Introducing eSentire

We are recognized globally as the Authority in Managed Detection and Response (MDR) because we hunt, investigate and stop cyber threats before they become business-disrupting events. In fact, eSentire was founded in 2001 to secure the environments of the world's most targeted industry - financial services. Now with over 1500 customers, across 80+ countries globally, we have scaled to deliver cybersecurity services across highly regulated industries, with a proven track record of success in securing businesses across the insurance sector.

At eSentire, we go beyond the market's capability in threat response. 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 with a Mean Time to Contain of 15 minutes.

At eSentire We Support Insurance Companies And Brokerages By:

- Preventing operational disruption with a combination of 24/7 Managed Detection and Response, Managed Risk Services, and Incident Response Services
- Protecting highly-valuable client data and the firms' reputation
- Mitigating carrier-agent risk

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.

Our services include:

Managed Risk Services

Strategic services including Security Assessments, Managed Phishing and Security Awareness Training and Managed Vulnerability Scanning to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

Managed Detection and Response

By combining our cutting-edge XDR platform, 24/7 threat hunting and security operations leadership, we hunt and disrupt known and unknown threats before they impact your business.

Digital Forensics and Incident Response

Battle-tested Incident Commander level expertise driving cyber investigations, emergency incident response, and root cause analysis. We offer an incident response retainer with an industry-leading 4-hour remote threat suppression service level agreement.

eSentire Atlas XDR Cloud Platform:

The industry's most advanced XDR Cloud Platform offers unmatched visibility, and employs patented machine learning to detect and respond to the most elusive threats in real time. Atlas cuts the noise to our SOC and your team by automatically disrupting 3M+ threats per day, stopping breaches before they disrupt your business. Our platform learns with each detection, correlating and amplifying data across our global customer base hundreds of times each day to deliver proactive security network effects that harden your defenses.

24/7 Threat Hunting & Security Expertise:

Filtering suspicious activity requires human intuition. Our Security Operations Centers are staffed 24/7 with Cyber Analysts and Elite Threat Hunters who provide rapid investigation and response. Plus as part of Team eSentire you're supported by a Cyber Risk Advisor from Day 1.

Security Operations Leadership:

Effective and efficient analysis, investigation, escalation and response refined over a two-decade history of delivering managed detection and response services to high value targets.

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

Our global 24/7 SOCs have discovered instances of ransomware gangs targeting our insurance 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 insurance 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 Insurance Industry Challenges	How eSentire Managed Detection & Response Helps
Access to Confidential Information	Our 24/7 Elite Threat Hunters and SOC Cyber Analysts actively hunt for threats across your environment. We detect intrusions and contain attacks before data can be exfiltrated.
Operational Disruption	We detect malicious administrative activity through remote access tools and stop intrusions before malware can be deployed throughout your environment
Becoming a Victim of Ransomware Attacks	We monitor your attack surface 24/7 to discover intrusion attempts, preventing 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

We Protect Highly-valuable Client Data And Your Firms' Reputation

For decades, we have successfully protected insurance firms and brokerages that manage protected data, and recognize that the heart of the insurance industry is based on long-term trusted relationships with your clients.

A successful data breach will undoubtedly jeopardize this critical client connection, especially if your clients include high net worth individuals who are more likely to be targeted for fraud or extortion based on exposure of sensitive data.

eSentire MDR detects intrusions and is designed to catch them in the early stage of an attack before they can establish a foothold, and cause a business disrupting event.

How We Mitigate Carrier-Agent Risk

The insurance industry is based on a network of clients, agents, brokers and carriers to provide services and coverage to major companies, high-net-worth individuals, employees and families. Your business is continuing to adopt new technologies that connect clients to the ability to purchase products online and submit claims. Agents and brokers work directly with both parties and obtain and store valuable client information.

Unfortunately, many agents & brokers operate with consumer-grade security technology not suitable to protect the asset they manage. This unmeasured level of security constantly changes as smaller firms merge and connect their IT environments. You need a partner acting as a true extension of your team to manage your cybersecurity program end-to-end.

In addition, many breaches are all too often traced back to vendors and our 24/7 SOC Cyber Analysts and Threat Hunters have repeatedly caught and stopped 3rd party compromises before the vendor reported the vulnerability by identifying and prioritizing core services for monitoring, including document management, time tracking, file share and document signing. Our Managed Risk experts support in building your security strategy, provide risk assessments, and recommend minimum security measures.

As an example, our team detected and blocked the malicious web shell scripts associated with the 2021 Microsoft Exchange vulnerabilities, worked with clients to secure their SolarWinds Orion issues, and discovered multiple remote administrator tools vulnerabilities.

eSentire in Action

Company Profile

- Private-equity affiliated holding company specializing in insurance
- Dynamic multi-cloud network of over 1000 endpoints
- CISO and small team oversee security

Primary Challenges

- Lack of human resources and 24/7 security coverage
- Controlling and consolidating security spend
- Taking full advantage of the organization's investment in M365 E5 licensing

How eSentire MDR Helped

- Customer deployed multi-signal MDR solution deployed across network, cloud endpoint, and log
- eSentire facilitated seamless transition from redundant endpoint licensing to Microsoft Defender for Endpoint

Why Enterprises 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 PII, PCI, HIPAA, 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

1500+
Customers in 80+ 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 Firm 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

bsi ISO/IEC 27001 Information Security Management CERTIFIED

MAPPED

MITRE ATT&CK™

AWARDED

IDC LEADER

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

MSSP Alert Top 250 MSSPs – NAMED #9 & TOP MDR PROVIDER

THE CHANNEL CO. CRN TECH INNOVATORS WINNER 2022

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

eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1500+ organizations in 80+ 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**.