eSENTIRE

SOLUTION BRIEF

Multi-Signal Managed Detection and Response for Retail

From production to payment - prevent operational disruption with 24/7 protection across your retail supply chain

Retailers face an increasingly complex set of challenges when it comes to protecting consumer and business data as they strive to reach broader markets by selling their goods through multiple channels. Digital disruption has led nearly every major retailer to adopt an e-commerce strategy in addition to their brick-and-mortar locations while many new retailers focus solely on e-commerce. What's more, digital disruption is also changing the way that consumers pay for goods and services and how retail support services provision credit, delivery services, advisory services, and a range of other customer engagement, convenience and support services.

Unfortunately, margin pressures, rising competition, and an uncertain economic outlook create an uphill battle to obtain the funding and resources required to protect retail environments. Compounding this challenge is the increasing speed and precision with which threat actors are accomplishing their objectives against the retail industry. Although cybersecurity awareness gains traction at the executive and board levels, cybersecurity teams continue to find themselves under-resourced against today's threat landscape.

As a security leader, there are many factors contributing to how you need to think about increasing cyber risk within the retail supply chain. These risks are driven by a combination of business factors and security vulnerabilities, especially as threat actors seek to:

- Exploit the adoption of hybrid brick-and-mortar and e-commerce business models as retailers look to expand customer interaction and purchasing opportunities.
- Disrupt IoT-based Point-of-Sale 2.0 systems that offer faster and contactless payment options to customers.
- Take advantage of insufficient investment in skilled cybersecurity personnel, tools, and technology needed to mitigate a security incident.
- Attack vulnerable web applications to steal account credentials and access customers' personally identifiable information (PII).
- Capitalize on weaknesses across the attack surface stemming from multiple third party vendor relationships intertwined to deliver a quick and convenient customer experience
- Fine-tune their malware and craft highly convincing phishing and business email compromise (BEC) campaigns, which can sour the relationship between retailers and their consumers or third-party vendors.

Prevent Operational Disruption Across The Retail Supply Chain

The retail supply chain consists of manufacturers, wholesalers, retailers, fulfillment centers, and the end consumers.

Cyber Threats Affecting Retailers[1]:

25% of retailers have been the target of cyberattacks

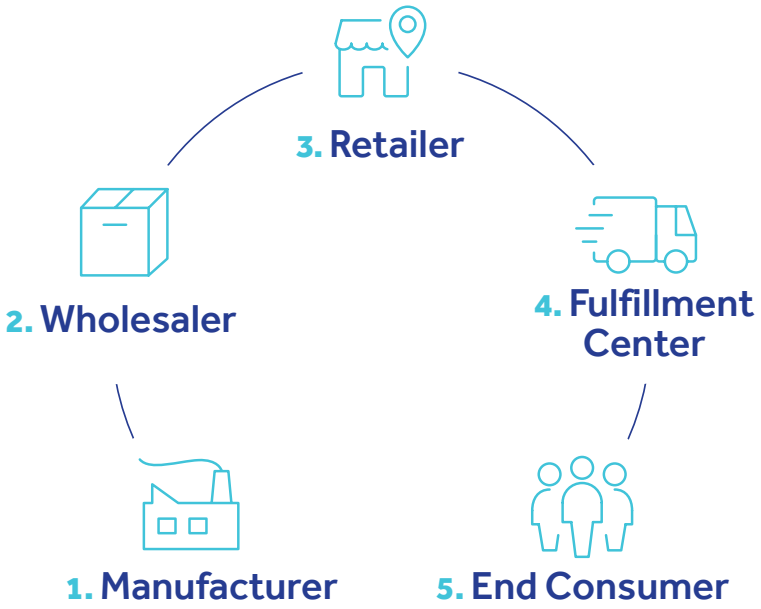
and

over **60%** of consumers lack confidence in a retailer's ability to protect their data.

Attacks against retailers and the supply chain include:

- Credential phishing
- Malware
- Ransomware
- Distributed denial-of-service (DDoS) attacks

The Retail Supply Chain



1. Produces the goods using machines, raw materials, and labor
2. Purchases finished goods from the manufacturers and sells those goods to retailers in large bulk quantities
3. Sells the goods in small quantities to the end consumer at a higher price, ideally at the manufacturer's suggested retail price (MSRP)
4. Provides warehousing and dropshipping services that deliver the goods post-purchase to the end consumer
5. Buy the goods from the retailer

Across the retail supply chain, these organizations are susceptible to multiple cyberattacks including:

- Deployment of malware to the internal systems and equipment controls
- Compromised IIoT sensors and wireless systems
- Inventory interception or direct theft

Without the appropriate security measures in place to detect and respond rapidly, these threats can result in:

- Disclosure of sensitive information or regulated data, such as confidential business data or the end consumers' personal identifiable information (PII)
- Costly disruption of fulfillment operations
- Financial and legal penalties resulting from a breach of contract due to downtime

[1] Fortinet Retail Cybersecurity Statistics Report

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 1200+ customers across 75+ countries, we have scaled to deliver cybersecurity services across highly regulated industries with a proven track record of success in protecting businesses across the retail industry - securing the end-to-end supply chains of department stores, grocery stores, wholesale retailers, specialty/ outlets, convenience stores, discount retailers, internet/mobile providers, automotive services and retail manufacturers.

At eSentire, we go beyond the market's capability in threat response and specifically address cybersecurity risks for the retail sector. eSentire's multi-signal MDR approach ingests endpoint, network, log, cloud, asset and vulnerability data to enable complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit (TRU) are applied to captured data identifying known & unknown threats including suspicious activity and zero-day attacks. Our SOC Cyber Analysts and Elite Threat Hunters are mission-driven to put retailers ahead of business disruption. Powered by our industry-leading XDR cloud platform and unique threat intelligence, eSentire can detect and respond to cybersecurity threats in the retail industry with a Mean Time to Contain of 15 minutes.

At eSentire We Support Retailers By:

- Preventing operational disruption of internal and consumer-facing retail services through a combination of 24/7 Managed Detection and Response, Managed Risk Services, and Incident Response Services
- Ensuring that any regulatory penalties and third-party costs associated with data breaches are minimized
- Ensuring your business remains compliant to regulatory frameworks such as PCI DSS, GDPR and CCPA
- Protecting your data and customer data from ransomware, data theft or exposure, and insider threats

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

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

Whether your organization's assets are stored in the cloud, on-premises, or in a hybrid environment, we detect and contain threats that 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 retail 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 Cyber Analysts and Elite Threat Hunters for assessment and manual containment with a Mean Time to Contain of 15 minutes.

Key Retail 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.
Protecting Against Supply Chain and Third-Party Vendor Risk	We mitigate supply chain and third-party vendor risk. • eSentire Managed Risk Service experts support in security assessments, testing and make strategic recommendations to offset risks for the retail sector. • eSentire Managed Detection and Response has repeatedly caught and stopped vendor compromises before the vendor reported the vulnerability.
Preventing 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 kill-switch response capabilities. • We offer endpoint protection to prevent your defenses from being disabled.
Avoiding Regulatory and Compliance Violations	Our 24/7 Global SOCs leverage proven run books which include detectors mapped to requirements and reporting measures for PCI DSS, PII, CCPA, GLBA, SOX, NYCRR, HIPAA, GDPR, as well as state-level regulations.

Whether your organization is a brick-and-mortar, e-commerce retailer, or both, threat actors are going to capitalize on vulnerable systems and human nature to achieve their objectives. Therefore, you must be able to:

- Protect your network data 24/7
- Meet the PCI DSS and other compliance requirements for payment information
- Protect Point-of-Sale systems and cardholder data
- Implement strong access control measures, especially for privileged users
- Defend against attackers targeting your supply chain or third-party vendors

Helping Your Organization Meet PCI DSS Regulations

The Payment Card Industry (PCI) Security Standards Council is focused on the protection of payment account data throughout the payment lifecycle. Through twelve key requirements, it outlines cybersecurity technology and practice requirements that are audited for compliance annually.

PCI DSS directs how organizations should securely manage credit card account numbers and payment card data to best protect the collection, storage, and transmission of cardholder data from e-commerce transactions. Any retailer that transacts with any one of the major credit card companies must adhere to the PCI Data Security Standards (PCI DSS) and failure to comply results in fines ranging from $5,000 to $100,000 per month.

Compliance with PCI DSS may seem challenging but we are here to help you navigate these requirements. We have achieved the most stringent certification in PCI DSS compliance conducted by an independent auditor to demonstrate:

- A proactive approach to security and industry compliance requirements
- Sensitivity to our clients' specific needs and business objectives
- Ability to help our clients meet the global PCI DSS compliance standards

Gain Confidence, Control & Expertise

Managed Risk Services

TAKE CONTROL OF CYBER RISK

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

Managed Detection & Response

PREVENT THREATS BECOMING BUSINESS DISRUPTING EVENTS

We deliver Response + Remediation you can trust. 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.

Incident Response & Digital Forensics

BE READY WITH THE WORLD'S FASTEST THREAT SUPPRESSION

Battle-tested Incident Commander level expertise, crime scene reconstruction and digital forensics investigations that can bear scrutiny in a court of law. The world's fastest threat suppression with a 4-hour SLA available with our IR Retainer.

eSentire MDR features include:

- ✔ 24x7 Always-on Monitoring
- ✔ 24x7 Live SOC Cyber Analyst Support
- ✔ 24x7 Threat Hunting
- ✔ 24x7 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 Retail Organizations Choose eSentire

Put Your Business Ahead of Disruption

- **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 24/7 Global SOCs leverage proven runbooks which include plays to manage issues and reporting for PCI DSS, PII, CCPA, GDPR, HIPAA, 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

- **Results**
  - Retail Organizations 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 Retail network of customers
  - 99% reduction in threat detection and containment times from global averages

$6.5T+
Total AUM

1200+
Customers in 75+ 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

Awarded

IDC 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

Certified

AICPA SOC 2 — AICPA Service Organization Control Reports — Formerly SAS 70 Reports

Information Security Management ISO 27001 Certified

PCI DSS COMPLIANT

Mapped

MITRE ATT&CK™

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**.