LogRhythm®
The Security Intelligence Company

Loss prevention reinvention:
Cybersecurity and retail

LogRhythm
The Security Intelligence Company

Retailing renaissance

Since early civilisation, retail has seen continual change thanks to technology. Whether it was the change from bronze tools to iron, or the shift from water transport to railways, every disruptive, transformative technology has challenged retailers to adapt.

Information technology is the latest challenge. It brings plenty of benefits: easier, more direct communication with customers, a plethora of payment options, online sales to expand geographic reach, better inventory control, faster data collection and more.

The opportunities available to the retail industry are growing. However, so are the threats. The UK's Information Commissioner's Office announced that the number of retailers reporting data breaches doubled in the space of a year[1].

Taking stock

With a 30 per cent increase in cyberattacks[2], retailers are keenly aware of the relevance of cybersecurity to their businesses. A 2016 survey by BDO saw 100 per cent of retailers identify cybersecurity as a cause for concern – up from 55 per cent in 2011 and 26 per cent in 2007[3]. Increased awareness is a good start, but effective cybersecurity can be particularly challenging for a retailer.

This is because retailers must deal with a distributed environment, covering stores, warehouses, suppliers and back offices. These locations often have low bandwidth and may run different, often ageing systems, making it difficult to obtain a centralised view of operations. Dealing with multiple systems or having to make site visits to investigate possible compromises can stretch IT staff too thinly and waste time.

The advent of GDPR means those IT staff are going to have even more to do. Retail organisations collect and hold significant amounts of customer data, including names, addresses, dates of birth and credit card details.

[1] Cyber attacks on online retailers double in a year as hackers try to steal shoppers' details
https://www.telegraph.co.uk/news/2017/08/13/cyber-attacks-online-retailers-double-year-hackers-try-steal/
[2] Cyber security threats to the retail sector
https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/spotlight-on-cyber-security/cyber-security-threats-to-the-retail-sector.html
[3] 2016 BDO Retail Riskfactor Report
https://www.bdo.com/insights/industries/retail-consumer-products/2016-bdo-retail-riskfactor-report

LogRhythm
The Security Intelligence Company

Under the new GDPR requirements, data breaches must be reported within 72 hours of discovery[4]. This makes the need to identify the nature and extent of a breach quickly, and respond to it in those crucial hours, even more pressing. Such compromises are expensive to clean up, open the business to legal action, and research shows that retail organisations can lose up to nine per cent of their share value within 30 days of a breach being reported[5].

Securing a retail organisation's network is extremely difficult because every point-of-sale (POS) device, web service, supply chain system, and any other device that must connect to the business, is a potential point of compromise. Furthermore, the rise of the Internet of Things (IoT), which allows retailers to create stronger, more convenient connections with customers through devices such as in-store cameras, smart speakers, sensors and smartphones, opens yet more doors for cybercriminals[8].

Window shopping

To address cybersecurity challenges, a retail organisation needs a single view into the IT and OT environments of the business. Finding such a window that provides insight across a dispersed network comprising disparate systems requires monitoring that works across the whole system, breaking down silos. The complete picture this provides allows the detection of malicious activity, whether from outsider threats or from insiders. As internal threats (inside operators, lost hardware or files, or system glitches) account for 58 per cent of cybersecurity incidents, being able to identify threats or vulnerabilities inside your network is as crucial as thwarting attacks from the outside[9].

Being able to see what's happening is the first step to security but to reduce the mean time to detect (MTTD) threats requires a system that continually learns what is normal behaviour for an organisation, allowing quick, automated detection of dangerous activity. This type of security information and event management (SIEM) can employ user and entity behaviour analytics (UEBA) to not only detect anomalous activity but also respond automatically.

Target gets hit

Several high-profile breaches have given unwanted publicity to retailers, including TJX (owner of retailers Marshalls, TJ Maxx and others)[6], and, perhaps the most famous retail breach, Target[7].

The Target breach affected up to 110 million customers and is estimated to have cost $162m to resolve. The vector for the attack was a third-party HVAC vendor that attackers compromised and used to gain access to Target's POS system.

In addition to the reputation damage, decreased share price, and remediation and legal costs, Target's CEO was forced to resign after the breach.

[4] Notification of a personal data breach to the supervisory authority
https://gdpr-info.eu/art-33-gdpr/
[5] Risky business: The impact of data breaches
http://blog.kenan-flagler.unc.edu/risky-business-the-impact-of-data-breaches/
[6] Massive TJX Security Breach Reveals Credit Card Data
https://www.csoonline.com/article/2121609/malware-cybercrime/massive-tjx-security-breach-reveals-credit-card-data.html
[7] The 17 biggest data breaches of the 21st century
https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
[8] Top 5 Security Threats for Retailers in the Digital Age
https://blogs.cisco.com/retail/top-5-security-threats-for-retailers-in-the-digital-age
[9] Managing digital risks in the retail world
http://www.willis.co.uk/documents/Industries/Willis_Retail_Risk_Insight_Digital_Risks_in_the_Retail_World.pdf

LogRhythm
The Security Intelligence Company

For example, if an employee of a retail outlet is accessing a client database and emailing those records to an email account outside the business, the system can send an alert, block the employee's access to the network and stop the email until the incident can be investigated.

Reducing the mean time to respond (MTTR) to incidents is key to reducing the cost and damage of a compromise. Monitoring can be handled by in-house staff or through offsite specialists as a managed service.

Getting a centralised window onto the business also helps facilitate PCI-DSS and GDPR compliance. Having finer control over such data can also serve business needs, enabling a retailer to detect and manage fraud better, whether it be online or in-store, detecting unusual patterns of activity, such as refund fraud, or the use of stolen cards. It can also reveal new opportunities for efficiencies or using existing data to offer new products or services.

A one-stop shop for diverse needs

The LogRhythm NextGen SIEM Platform provides infrastructure monitoring to detect malicious activity — whether from outsider or insider threats — system-wide. UEBA enables SecOps teams to detect anomalous activity and respond with alerts and automated mitigation. SmartResponse™ automation frees up time so in-house SecOps teams can focus on other important tasks and improve operational efficiency. LogRhythm also offers 24/7 monitoring in an ISO27001-compliant SOC, increasing security without increasing headcount.

LogRhythm's centralised solutions for dedicated log management and NextGen SIEM are designed for quick deployment and scalability. They provide visibility across networks and notify users immediately when suspicious activity is detected. They also deliver additional insights for other performance issues, such as remote access connection failures or missed scheduled software updates.

LogRhythm's Compliance Automation Suites deliver embedded content to enable long-term and secure data storage as well as wizard-based data recovery. Other capabilities include privileged user monitoring, web application defence, rapid forensics and advanced correlation and pattern recognition.

A recently introduced capability is LogRhythm CloudAI, which takes data from key applications and forwards it to the cloud. Once in the cloud it is subjected to machine learning across long

LogRhythm delivers the goods

LogRhythm protects retailers from the storefront to the back office and at all points in-between with a multipronged response to cyberthreats:

- NextGen SIEM
- User authentication, verification and monitoring
- Managed-service option
- Compliance Automation Suites
- Rapid detection, mitigation and auditing of threats
- UEBA/CloudAI
- Automation/SmartResponse™
- Real-time File Integrity Monitoring

periods to decipher normal or unusual patterns of behaviour to give an indication of compromise. CloudAI then sends alerts with a risk score to suggest whether something warrants attention or investigation.

As the opportunities for retailers grow, companies need a partner to help safeguard them from the growing threats. Together, LogRhythm's offerings provide industry-leading automation, compliance and auditing support, comprehensive reporting and protection against advanced threats. For retailers facing increased interest from cybercriminals, while dealing with a distributed environment and new data requirements, these capabilities will be invaluable. High security on the high street is now a reality.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation & orchestration (SAO) in a single end-to-end solution.

LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

"LogRhythm provides real-time actionable intelligence within a single pane of glass based on events across my entire infrastructure and allows me to quickly isolate unusual network behaviour by a user, machine or network device."

Jason Riggins, Network Administrator, Kansas Medical Mutual Insurance Company

LogRhythm®

The Security Intelligence Company

Security. Made Smarter.

Contact us

UK: **+44 (0)1628 918 330**
Germany: **+49 89 919292 - 200**
Middle East & North Africa: **+971 55 6422224**
europe@logrhythm.com | **www.logrhythm.com**

LogRhythm, Clarion House, Norreys Drive, Maidenhead, SL6 4FL, United Kingdom.