Threat Detection and Response for Retailers

Streamlining cybersecurity monitoring to detect and respond to emerging threats

Modern retail trends increase risks for you and your customers

Retailers are undergoing a digital transformation to modernize customer experiences online and in store and to improve their operations and logistics. They are relying more heavily on public cloud infrastructure and applications for online ordering and inventory and supply chain tracking, and while these new technologies can help drive operational efficiencies and lower costs, they also introduce more connected devices and expand the threat surface area.

For cybercriminals, this represents a wider threat plane to infiltrate into your network. For businesses, this means the need for an array of security products, security specialists, and up-to-date threat intelligence to identify and respond to evolving threats. It is critical that these new solutions be deployed in a thoughtful way, providing that sensitive information is not at risk. Retail leaders must think differently about their security to help provide that the technology used to enhance their customers' experience is better protected from cyberthreats.

Potential Benefits

Improved security monitoring

- Centralizes security visibility across public cloud environments, on premises networks, and endpoints.

Simplified security

- Combines multiple security essentials to help you deliver smarter, more trusted interactions.

Automate threat hunting

- Our continuous threat intelligence and log data help fuel early threat detection so we can respond quickly.

Accelerate compliance

- Address regulatory standards and streamline compliance efforts with pre-built reports for PCI DSS and more.

Phenomenal threat intelligence

- Helps to prepare you to face future threats with our unrivaled visibility and provides actionable intelligence from Alien Labs resulting in a faster response.

AT&T Cybersecurity can help. With AT&T Managed Threat Detection and Response, we can help you detect and respond to advanced threats and exposed risk to protect your business and your brand. A sophisticated managed detection and response (MDR) service, it provides threat management in one turnkey service, including 24 x 7 proactive security monitoring, alarm validation, and incident investigation and response. With it, you can quickly establish or augment your threat detection and response strategy while helping reduce cost and complexity.

Retailer Challenges

Digital Transformation increases the attack surface area

Whether the goal is to improve customer experience, streamline operations, or reduce costs, retailers are becoming increasingly dependent on technology. The shift to more online ordering and the use of SaaS applications for inventory and supply chain tracking has caused organizations to change the way they do business. But as they bring on new technologies, organizations also bring on new vulnerabilities for cybercriminals to exploit.

With AT&T Managed Threat Detection and Response, you have a flexible solution that readily adapts to your changing IT environment. As you bring on more tools and SaaS applications, the USM platform makes it easy to extend security orchestration and automation capabilities with other IT security and operations products and business-critical applications through AlienApps, helping to unify your security architecture and orchestrate your threat detection and response activities from a centralized platform.

Constant attack evolution

As technology grows more sophisticated, so do malicious actors. Retailers are shifting to a more online presence, creating new ways for cybercriminal to try to exploit vulnerabilities. The number of bot attacks and DDoS attacks targeting retailers are significantly increasing, with the goal of disrupting online activities. To defend against the ever-evolving cyberthreats, organizations must stay up to date with the latest threat intelligence and be able to constantly monitor their critical networks and devices on premises, in the cloud, and in remote locations to identify and contain potential threats before they cause harm.

AT&T Managed Threat Detection and Response is fueled with continuously updated threat intelligence from AT&T Alien Labs, providing that your defenses are up-to-date and able to help detect emerging and evolving threats. AT&T Alien Labs, the threat intelligence unit of AT&T Cybersecurity, produces timely threat intelligence that is integrated directly into the USM platform in the form of correlation rules and other higher-order detections to automate threat detection. The SOC analyst team is in constant communication with Alien Labs to understand the evolving threat landscape and help to fine tune the new detections that are sent to the USM platform daily.

Maintaining compliance requirements

Today's businesses face a variety of compliance requirements to help protect consumers. Retailers collect a lot of customer data, including credit and debit card information, and because of the sensitive nature of that data, retailers in particular are heavily regulated. But compliance can be difficult to maintain and report and failing to comply is expensive and can damage brand reputation.

AT&T Managed Threat Detection and Response helps to support your compliance and risk management goals in multiple ways. The USM platform delivers a comprehensive library of predefined report templates for PCI DSS, NIST CSF, and ISO 27001, as well as 50+ predefined event reports by data source and data type. As part of your Threat Model Workshop, we address your specific compliance requirements and your security monitoring environment is tuned accordingly. AT&T Cybersecurity Consulting services, such as vulnerability scanning and penetration testing, can be used in parallel to help meet PCI DSS requirements.

Shortage of skilled security personnel

It's no secret that the cybersecurity industry is facing major talent shortage with little relief in sight. Skilled security professionals are in high demand, making it a challenge for organizations to hire and retain top talent. To make matters worse, already understaffed security teams often struggle to focus on strategic security projects as they're busy dealing with the daily operations and maintenance of their security tools, reviewing and investigating noisy SIEM alarms, and manually updating security policies across their systems in response to incidents or vulnerabilities.

The AT&T Managed Threat Detection and Response security operations center (SOC) analyst team monitors your environment and critical IT assets 24/7. They handle the daily security operations of monitoring and reviewing alarms and work to reduce false positives so that your team can focus on responding to actual threats, rather than sifting through noise. In addition, our analysts conduct in-depth incident investigations, providing your incident responders with rich threat context and recommendations for containment and remediation, helping your team to respond quickly and efficiently. Our analysts can even initiate incident response actions, taking advantage of the built-in security orchestration and automation capabilities of the USM platform.

How it works

Managed 24 x 7 by our SOC experts

Building on decades of experience in delivering managed security services to some of the world's largest and highest-profile companies, the AT&T Security Operations Center (SOC) has a dedicated team of security analysts who are solely focused on helping you to protect your business by identifying and disrupting advanced threats around the clock.

The AT&T Managed Threat Detection and Response SOC analyst team handles daily security operations on your behalf so that your existing security staff can focus on strategic work. Responsibilities include:

- 24 x 7 proactive alarm monitoring, validation, and escalation
- Identifying vulnerabilities, configuration errors, and other areas of risk
- Incident investigation
- Response guidance and recommendations
- Orchestrating response actions towards integrated security controls (AlienApps™)
- Reviewing your security goals regularly and providing recommendations on policy updates and additional security controls

Built on unified security management

AT&T Managed Threat Detection and Response utilizes our award-winning USM platform. Key capabilities include asset discovery, vulnerability assessment, network intrusion detection (NIDS), endpoint detection and response (EDR), SIEM event correlation, and long-term log management, incident investigation, compliance reporting, and more. With these capabilities working in concert, the USM platform is able to provide broader threat coverage and deeper environmental context than point solutions alone, helping to enable early detection, reduce false positives, and streamline incident investigations.

Threat Intelligence powered by AT&T Alien Labs

We bring together near-real-time intelligence, innovative threat detection and leading data scientists at AT&T Alien Labs to help provide that you're ready to face and defend against cyberthreats, so you can accelerate your digital transformation. AT&T Alien Labs goes beyond simply delivering threat indicators to performing deep, qualitative research that provides insight into adversary tools, tactics and procedures (TTPs). By identifying and understanding the behaviors of adversaries (and not just their tools), we can help power resilient threat detection, even as attackers change their approach or your IT systems evolve.

Contact us to learn more, or speak with your sales representative.

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange,™ and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.