Threat Detection and Response for Manufacturers

Manage your critical cloud and network infrastructure in a single pane of glass

Innovate and adapt without compromising your investment

As the manufacturing industry undergoes a digital industrial revolution into Industry 4.0, organizations are racing to modernize and embrace new connected factory and supply chain capabilities to keep pace with fast moving competitors. Manufacturing companies are looking for new ways to automate processes and monitor their systems in near real time in order to increase their bottom line. This 'factory of the future' requires highly secure networking and connectivity solutions that can meet demand while protecting their business and consumers. While these new technologies help enable automation, they also create new entry points for cybercriminals to access sensitive data, shut down operations, or even cause equipment to produce faulty product.

The entire IT landscape is changing with the growth of Internet of Things (IoT) endpoints, the shattering of the network perimeter, process automation, and the explosion of data. For cybercriminals, this represents a wider threat landscape to infiltrate your network. Manufacturing leaders must think differently about their security and shift from simply responding to cyberthreats to instilling a pre-emptive cybersecurity defense.

Potential benefits:

Improved security monitoring

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

Simplified security

Combines multiple security essentials so you can embrace new connected factory and supply chain capabilities.

Automated 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 reporting templates to help sustain security governance.

Phenomenal threat intelligence

Helps to prepare you to face future threats with our unrivaled visibility and provides actionable intelligence from Alien Labs to save you time.

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 24 x 7 proactive security monitoring, alarm validation, incident investigation and response, and more in one turnkey service. With it, you can quickly establish or augment your threat detection and response strategy while helping reduce cost and complexity.

Manufacturing challenges

Growing attack surface with digital transformation

Manufacturing companies are looking for new ways to automate process and monitor their systems in near real time in order to increase their bottom line. As a result, companies are introducing more connected devices, moving workloads to the cloud, and relying on more technology for monitoring their systems. These technologies are great for their bottom line, but they are increasing their attack surface area and there is often a lack of visibility into everything that is going on.

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. This helps 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. Manufacturers are modernizing and expanding their environments and relying on more advanced technology, creating more entry points for a cybercriminal to try to exploit. Manufacturers in particular are more susceptible to malware, phishing and compromised webpages. To defend against the ever-evolving cyberthreats, manufacturing 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. Yet, a truly effective threat detection and response program is difficult to achieve.

AT&T Managed Threat Detection and Response is fueled with continuously updated threat intelligence from AT&T Alien Labs, helping to provide that your defenses are up-to-date and able to 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.

The network perimeter is shattered

There's a new reality when it comes to network security, driven by the idea that the "perimeter" is vanishing. The explosion of remote workers and the rise of Industry 4.0 warrants a re-examination of the tools and technologies we use to help protect organizations from cyber-attacks. Traditional protection and prevention controls are no longer enough. As the way we do business evolves, new vulnerabilities are created, and cybercriminals are constantly shifting their tactics to exploit these new vulnerabilities.

In addition to protection and prevention controls, organizations need a way to continuously monitor what's happening on their networks, cloud environments, critical endpoints and remote locations. With AT&T Managed Threat Detection and Response, organizations gain centralized visibility into their entire environment, on premises, in the cloud, on endpoints, and in SaaS applications. Our analyst team is continually monitoring each customer's environment, detecting and validating threats, and quickly responding to any anomalies or unusual behavior.

Shortage of skilled security personnel

It's no secret that the cybersecurity industry is facing a 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 does it work?

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, AWS® 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 takes advantage of 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.

About AT&T Cybersecurity

AT&T Cybersecurity helps 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.