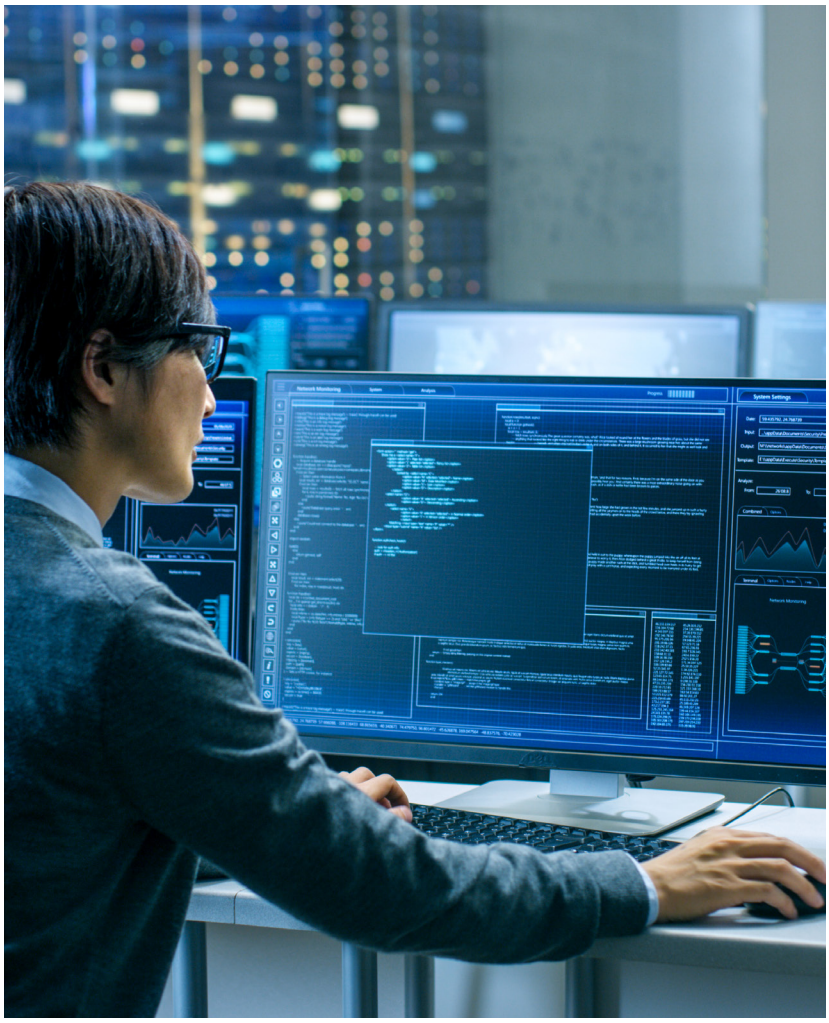
AT&T Business

AT&T Managed Extended Detection and Response (Managed XDR)



Benefits

- Single pane of glass provides one centralized view into alarms, vulnerabilities, and assets across customer's attack surface
- An open platform that allows customers to keep the security products they already have in place
- Automated threat detection and response for faster more efficient incident response
- Extensible platform that can accommodate customers' changing business needs
- Continually updated threat intelligence for faster triaging of alerts and more efficient identification of threats
- Around-the-clock monitoring and management so customer's security team can focus on other critical security initiatives

One contextualized view into threats across your environment to accelerate detection and response

As cyber actors continue to find new ways to exploit vulnerabilities and evade detection, organizations are finding it more and more difficult to protect against destructive attacks that result in disruption to their business.

Additionally, as business and workforce needs have evolved, the traditional network perimeter has dissolved, and the attack surface has expanded. Security teams today must manage and protect a myriad of users and devices across networks, endpoints, and cloud environments, and most organizations do not have the time, resources, or expertise to do so on their own. Disconnected security tools lead to security siloes, and without centralized visibility, security teams lack the context they need to detect, investigate, and respond to potential threats quickly and effectively.

AT&T Managed XDR combines AT&T Managed Threat Detection and Response with AT&T Managed Endpoint Security with SentinelOne to give one unified view across your environment so you can find and respond to threats before they impact your business.

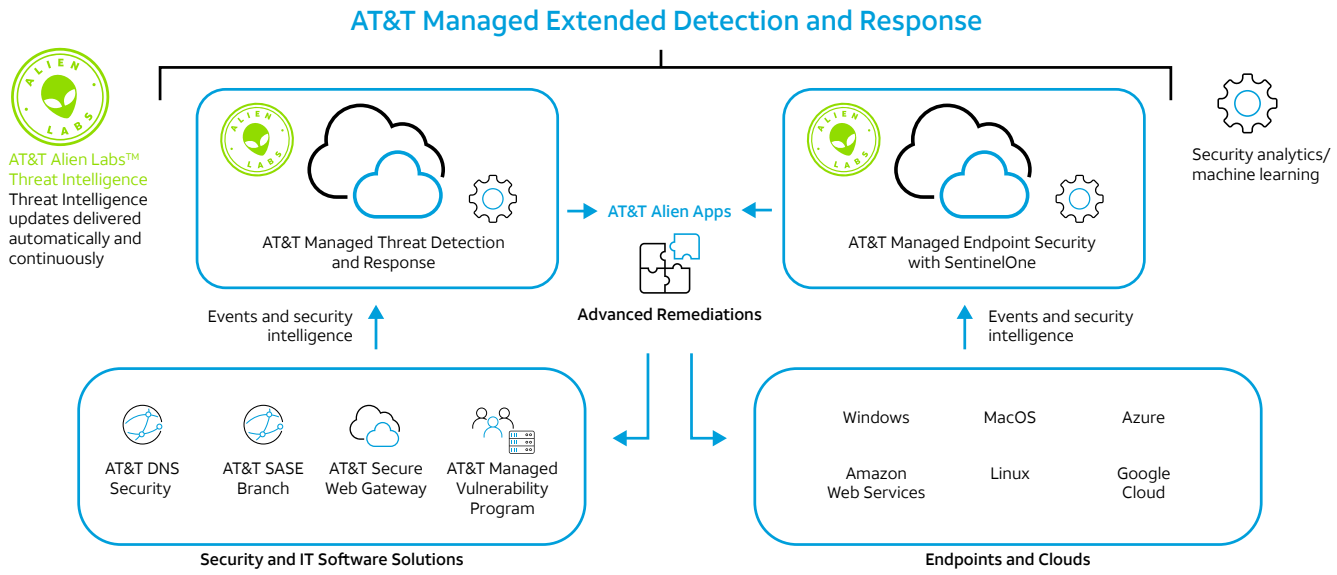
A holistic approach to threat detection and response

AT&T Managed Extended Detection and Response, or AT&T Managed XDR, builds on our decades of expertise in managed security services to help protect your business.

We provide 24x7 threat monitoring and management by automatically collecting, correlating, and analyzing data from across your attack surface and providing it in one holistic view so threats can be detected and responded to in near real time. Not only can our security team find and take action against threats in your network, but they can also detect and respond to threats such as malware and ransomware on your endpoints.

The network and endpoint data are brought together and enhanced with tactical information from the AT&T Alien Labs threat intelligence unit to give AT&T Security Operations Center (SOC) analysts the information they need to quickly understand and respond to threats in your environment.

By consolidating threat detection and response tools into a single unified solution managed by a common SOC team, we can enhance your security posture and help ensure your business operates without interruption.



An open platform that can scale with your business

AT&T Managed XDR employs our award-winning USM Anywhere™ platform to surface ongoing attacks against the customer's network, both in the cloud and on premises. The platform can automate collection and analysis of data across your attack surface to deliver context for faster and more accurate detection of threats and coordinated, efficient incident response.

Hosted in our elastic cloud environment, the highly extensible platform readily scales to accommodate your changing IT environment and growing business needs.

The platform is open, which means you can keep the security products you have already invested in, Through the AlienApps™ framework, the platform can integrate with a large ecosystem of best-of-breed security and productivity tools for orchestrated and automated incident response.

Identify threats based on behaviors rather than signatures

AT&T Managed XDR also incorporates next-generation endpoint technology from SentinelOne, which includes both endpoint protection and endpoint detection and response (EDR), to help protect against known and unknown threats.

Signature-based antivirus, which helps protect networks from known threats, is no longer sufficient to defend against malware, ransomware, and fileless attacks. AT&T Managed XDR can uncover abnormal activity and patterns that indicate ransomware is present. The solution utilizes SentinelOne Endpoint Security to monitor processes in real time and identify threats based on behaviors rather than signatures.

With AT&T Managed XDR, ransomware threats can be neutralized using automated remediation actions such as deleting the source code, killing malicious processes, quarantining suspicious files, or even disconnecting endpoints from the network. Endpoints can be rolled back to a previous clean state without having to reimage machines, restore from external backup solutions, or write scripts.

Fueled with Alien Labs threat intelligence

With AT&T Managed XDR, continually updated tactical information from AT&T Alien Labs, our threat intelligence unit, is fed directly into the USM Anywhere platform, so your defenses remain up to date and are better able to detect emerging threats.

Alien Labs collects and analyzes threat data from many different sources, including the AT&T IP network, the USM global sensor network, and the AT&T Alien Labs Open Threat Exchange® (OTX™), which is the world's largest open threat intelligence community.

But Alien Labs goes beyond delivering threat indicators. They perform research that provides insight into attacker tactics, techniques, and procedures, or TTPs, so we can identify and understand attacker behaviors as well as their tools.

By understanding what an attacker will do when they come into a network, we can help organizations reduce risk—and respond faster to threats—even when attackers are using zero-day attacks.

A world-class managed service

Our premium managed service gives customers access to the skills and expertise they need to continuously detect and respond to threats while reducing cost and complexity.

AT&T Managed XDR relies on AT&T's established technology and infrastructure and decades of experience delivering managed security services to some of the world's largest companies to help you protect your business and your brand.

The AT&T SOC team monitors your environment and critical assets around the clock. Our dedicated analysts are focused on helping you to protect your business by identifying and disrupting advanced threats. They handle the day-to-day security operations of monitoring and reviewing alarms and working to reduce false positives so your team can focus on responding to actual threats and other strategic initiatives.

In addition, our analysts conduct in-depth incident investigations, providing your incident responders with rich threat context and recommendations for containment and remediation, so they can respond quickly and efficiently. Our analysts can even initiate incident response actions.

The AT&T SOC analyst team responsibilities include:

- 24 x 7 proactive alarm monitoring, validation, and escalation
- Identify vulnerabilities, AWS® configuration errors, and other areas of risk
- Incident investigation
- Response guidance and recommendations
- Orchestrate response actions (AlienApps™)
- Review your security goals regularly and provide recommendations on policy updates and additional security controls

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.