AT&T Managed Threat Detection and Response

Protect your business with 24x7 threat detection and incident response from AT&T

Start detecting and responding to advanced threats sooner with AT&T.

To defend against modern cyber threats, organizations must 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. Most organizations do not have the time, resources, or expertise to do so on their own.

AT&T Cybersecurity can help.

With **AT&T Managed Threat Detection and Response**, you can 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 solution, 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.

AT&T Managed Threat Detection and Response combines decades of experience in managed security services, our unified security management (USM) platform for threat detection and response, and AT&T Alien Labs™ threat intelligence to deliver an unrivaled MDR solution.

Potential benefits:

- Help protect your business with highly effective threat detection and incident response services
- Gain centralized security visibility across your critical cloud and on-premises environments
- Move towards your security and compliance goals faster with less complexity and greater cost efficiency
- Protect your security investment with a solution that scales and adapts to your changing business and IT environment

Product features:

- 24 x 7 security monitoring by a dedicated AT&T SOC team
- Built on the AT&T's award-winning unified security management (USM) platform
- AT&T Alien Labs delivers continuous threat intelligence to help keep your defenses up to date
- Security orchestration and automation helps to streamline and accelerate response
- Response support extends to change management with other AT&T managed security services

Built on unified security management

AT&T Managed Threat Detection and Response takes advantage of our award-winning unified security management (USM) platform. Unlike other managed detection and response solutions that may be based primarily on a SIEM log management or endpoint detection and response (EDR) tool, the USM platform combines multiple security capabilities that are essential for effective threat detection and response in one unified console.

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.

Fueled with AT&T Alien Labs threat intelligence

AT&T Managed Threat Detection and Response is fueled with continuous threat intelligence from AT&T Alien Labs, so your defenses are up to date and better able to detect emerging threats. AT&T Alien Labs, the threat intelligence unit of AT&T Cybersecurity, produces and delivers timely, tactical threat intelligence directly to the USM platform.

AT&T Alien Labs has unrivaled visibility into the AT&T IP backbone, the global USM Sensor network, the Open Threat Exchange® (OTX™), and other sources of threat data. This team 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, AT&T Alien Labs helps power resilient threat detection, even as attackers change their approach and as your IT systems evolve.

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
- Identifying vulnerabilities, AWS configuration errors, and other areas of risk
- Alarm validation, review, and escalation
- Incident investigation
- Response guidance and recommendations
- Orchestrating response actions towards integrated security controls (AlienApps™)
- Implementing changes in response to identified threats within other AT&T Cybersecurity services managed by the AT&T SOC

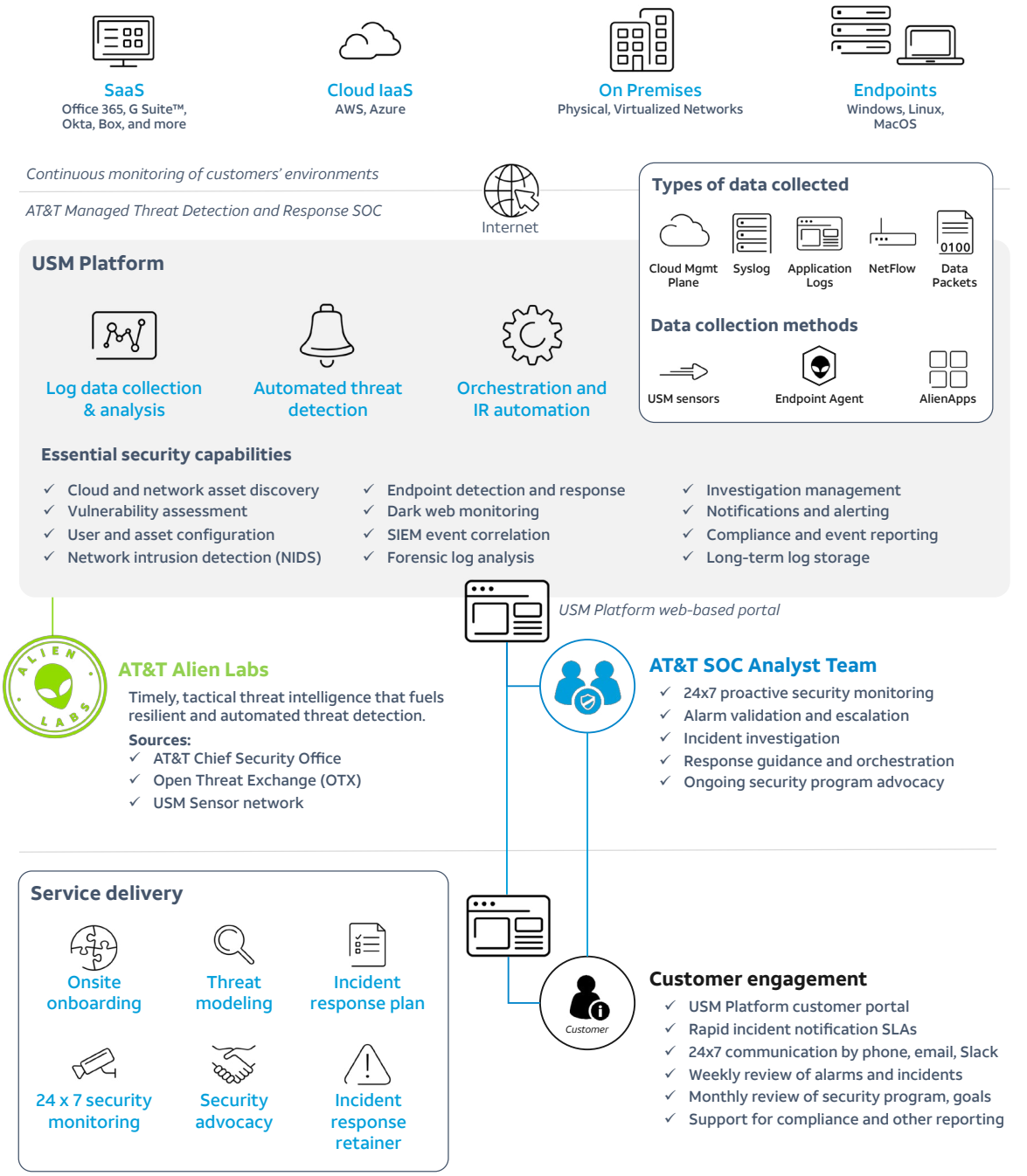
Going beyond security operations to security advocacy

Going beyond the daily functions described above, our SOC analyst team serves as your cybersecurity advocate in a high-touch service delivery model. Our team helps to support your security and compliance goals by:

- Leading an onsite deployment, training, and onboarding engagement within the first 30 days
- Learning your unique environment, priorities, and goals through threat modeling exercises and tuning your service accordingly
- Reviewing your security goals regularly and providing recommendations on policy updates and additional security controls
- Supporting your compliance reporting requirements through the USM platform

To learn more about how we can help you detect and defend against cyber threats, visit us at AT&T Cybersecurity

How it works



About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning—helping to enable our customers around the globe to anticipate and act on threats to protect their business.

© 2019 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change. | 14391-052119