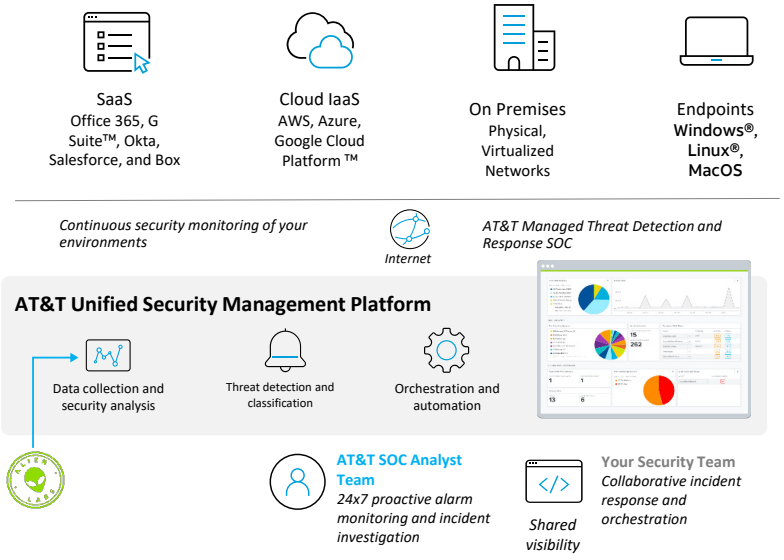
Multiple security capabilities in one platform, one single pane of glass.

AT&T Managed Threat Detection and Response

AT&T Managed Threat Detection and Response can help detect and respond to advanced threats and exposed risk to protect your agency. A sophisticated managed detection and response (MDR) service, it provides threat management in one turnkey service, including 24x7 proactive security monitoring, alarm validation, incident investigation and response.



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.

Powered by Unified Security Management® (USM) platform, is a two-tiered security management system that provides customers with a holistic view of their network, computing assets, and key systems.

DISCOVER
- » Network Asset Discovery
- » Software & Services Discovery
- » AWS, Azure and GCP Asset Discovery

ANALYZE
- » SIEM Event Correlation
- » User Activity Monitoring
- » 90 Days Of Online, Searchable Events

DETECT
- » Cloud , Network and Host Intrusion Detection
- » Endpoint Detection & Response
- » File Integrity Monitoring

RESPOND
- » Automated Response
- » Orchestration
- » Notification And Ticketing Integrations (400+ Basic and Advanced AlienApps)

ASSESS
- » Vulnerability and Configuration Scanning
- » Cloud Infrastructure Assessment
- » Investigations (Chain of Custody)

REPORT
- » Pre-built Compliance Reporting
- » Pre-built Event Reporting
- » Customizable Views And Dashboards and Reporting

Tier 1 — USM Anywhere Sensors and Agents

USM Anywhere Sensors deploy natively into each environment and help you gain visibility into all of your on-premises and cloud environments. Sensors collect and normalize logs, monitor networks and collect information about the environments and assets deployed in your hybrid environments. Sensors are a key component of the USM Anywhere solution.

USM Sensors operate either on-premises or in the cloud, performing the following tasks:

- Discovering your assets.
- Scanning assets for vulnerabilities.
- Monitoring packets on your networks and collecting data.
- Collecting log data and normalizing it before securely sending it to USM Anywhere Cloud.

USM Anywhere Agents deploy on your network host and provide the following:

- Endpoint detection and response
- Network asset monitoring
- Log collection

Tier 2 — USM Anywhere Cloud

USM Anywhere receives the previously described data sent to it by the USM Anywhere Sensor and uses it to provide essential security capabilities in a single SaaS platform:

- Centralized system security management
- Log data analysis and correlation
- Detection
- Alerting
- Log management
- Reporting

Cloud Connectors provide operational visibility into the security of your environment and perform the task of log collection.

USM Anywhere also integrates log management and securely retains raw logs long-term for forensic investigations and compliance mandates.

AT&T Cybersecurity

A High Touch Model

AT&T

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

AT&T Security Operations Center

Building on decades of experience in delivering managed security services to some of the world's largest and highest-profile Federal, Local and State Agencies, the AT&T Security Operations Center (SOC) has a dedicated team of security analysts who are solely focused on helping you to protect your agency 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
- Implementing changes in response to identified threats within other AT&T Cybersecurity services managed by the AT&T Security Operations Center.

High touch service delivery

Deployment is fast and simple, thanks to our high-touch service delivery model and a modern SaaS platform deployment model. Within 30 days of signing the contract, our SOC analysts can be monitoring your critical infrastructure and responding to threatsaccording to your individualized Incident Response Plan.

Onboarding includes:

- Threat Model Workshop conducted by AT&T Cybersecurity Consultants
- Installation, configuration, and tuning of your USM Platform to meet your requirements
- Integrate with other security technologies that are in scope of our AlienApp Framework
- Development of a custom Incident Response Plan in collaboration with your security team
- Training your personnel on the USM platform

Threat Model Workshop

At AT&T, we take the time to get to know our customers and their business. Every AT&T Managed Threat Detection and Response service begins with an on-site or remote threat model workshop led by AT&T Cybersecurity Consulting. This workshop helps enable AT&T to document vital business functions and resources, define infrastructure scope, confirm deployment requirements, diagnose existing security program gaps, and establish ongoing security program objectives. The in-depth knowledge of the customer systems gained through the workshop allows our SOC analysts to determine the most effective strategy for monitoring the customer's environment as we begin the deployment of the USM platform.

The Threat Model Workshop will focus on three primary components:

- **Critical Resources:** Resources that maintain sensitive data, that if breached, would require significant incident response to remediate.
- **Threat Surface Area:** Describes the exposed surfaces limited to the scope of the Critical Resources.
- **Identified Likely Threat Vectors:** Describes the consultant's assessment of the most relevant threats to the customer's Critical Resources given their Threat Surface Area.

Fueled with Alien Labs threat intelligence

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

Alien Labs has unrivaled visibility into the AT&T IP backbone, the global USM Sensor network, the AT&T Alien Labs 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, Alien Labs helps power resilient threat detection, even as attackers change their approach and as your IT systems evolve.

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-premise 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:

- Security monitoring by a dedicated AT&T SOC team
- Built on the AT&T's awardwinning 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
- Threat Model Workshop conducted by AT&T Cybersecurity Consultants