USM Anywhere™

Threat Detection & Incident Response

AT&T Business

USM Anywhere

USM Anywhere centralizes security monitoring of networks and devices in the cloud, on premises, and in remote locations, helping you to detect threats virtually *anywhere*. A modern software-defined platform, USM Anywhere automates threat detection, powered by AT&T Alien Labs threat intelligence. Plus, it orchestrates incident response with other leading security technologies—helping you to achieve security without the seams.

Data Analysis

Threat Detection

Automation & Response

AT&T Business

We're changing the cost and complexity of security

"In today's security landscape, the average company uses **more than 20 security technologies**."

— Cisco, February 2020

62% of companies say their organization's cybersecurity team is understaffed

— ISACA's State of Cybersecurity, June 2020

AT&T Business

How USM Anywhere Works

Smart, Automated Data Collection & Analysis

USM Anywhere automatically collects and analyzes data across your attack surface – helping you to quickly gain centralized security visibility without having to deploy, integrate, or normalize data from multiple disparate security technologies.

Threat Detection Powered by Alien Labs Threat Intelligence

With tactical threat intelligence from Alien Labs delivered to the platform continuously and automatically, we do the threat hunting for you. So, instead of having to write correlation rules and queries to sift through data, your team can focus on investigating and responding to actual security alerts.

Automated & Orchestrated Incident Response

Respond to incidents quickly and easily with orchestrated and automated actions towards other best-of-breeds security technologies, delivered as AlienApps. A highly extensible platform, USM Anywhere supports a growing ecosystem of AlienApps, enabling collaborative defenses.

AT&T Business

AT&T Threat Detection and Response simplifies

Asset discovery
Know who and what is connected to your environment

Vulnerability assessment
Know where the vulnerabilities are on your assets to avoid compromise

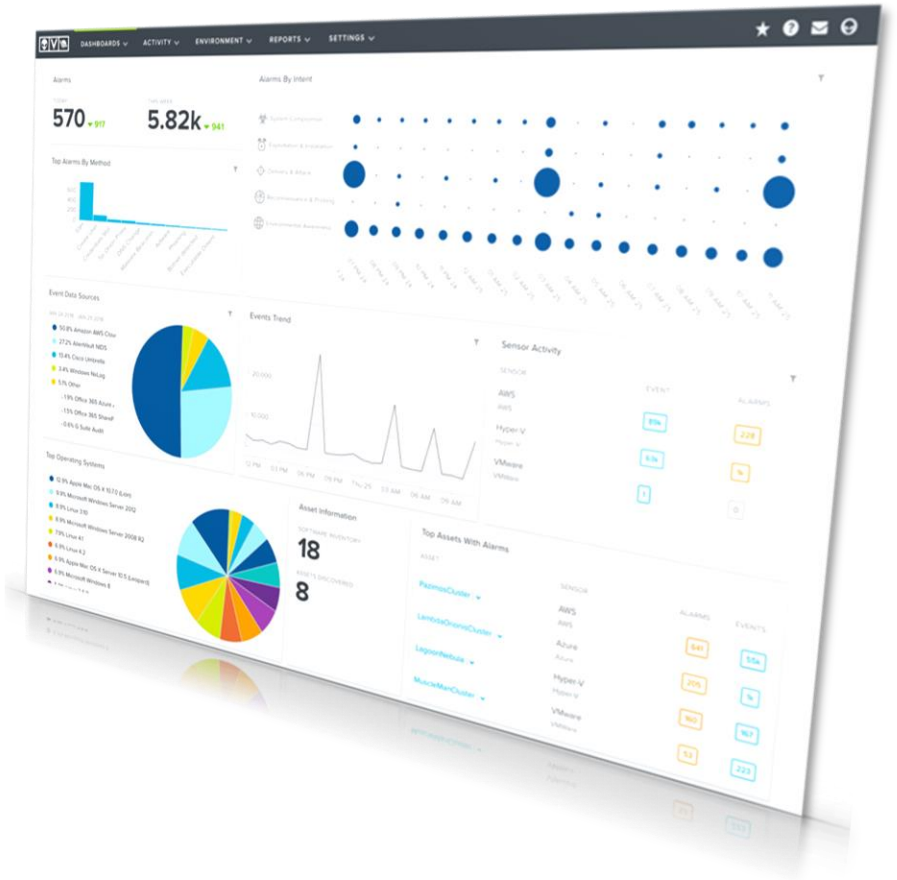
Intrusion detection
Know when suspicious activities happen in your environment

Endpoint detection & response
Continuously monitor your endpoints in the cloud and on premises to detect threats and changes to critical files.

Behavioral monitoring
Identify suspicious behavior and potentially compromised systems

SIEM & log management
Correlate and analyze security event data from across your network and respond

Security & compliance reporting
Pre-built, customizable reports for regulation standards and compliance frameworks



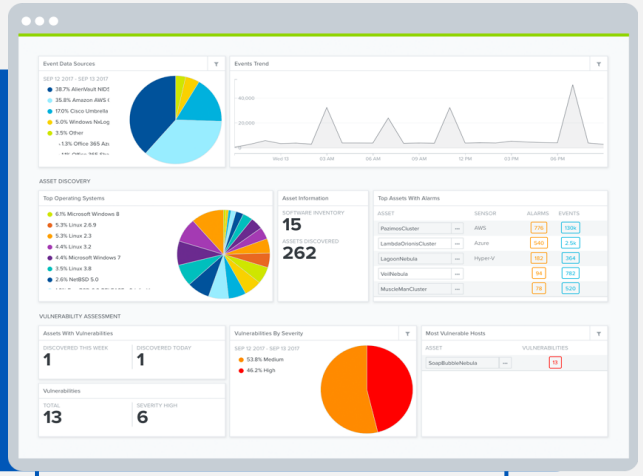
A unified security platform for threat detection, incident response & compliance

Centralized visibility across all environments

Continuous Security Monitoring in One Unified Platform

USM Anywhere has a broad set of data collection methods, including sensors, agents, and apps that are purpose-built for their environments to automatically collect security-relevant data.

With its integrated threat intelligence from Alien Labs, USM Anywhere normalizes, enriches, and analyzes this data to help detect threats. Simply put, we know what to look for and how to find it.



SaaS
Office 365, G Suite™, Okta, and more

Cloud IaaS
AWS, Azure, GCP

On Premises
Physical, Virtualized Networks

Endpoints
Windows, Linux®, MacOS

Users
Active Directory, Azure AD, Amazon, GCP, G-Suite, and more

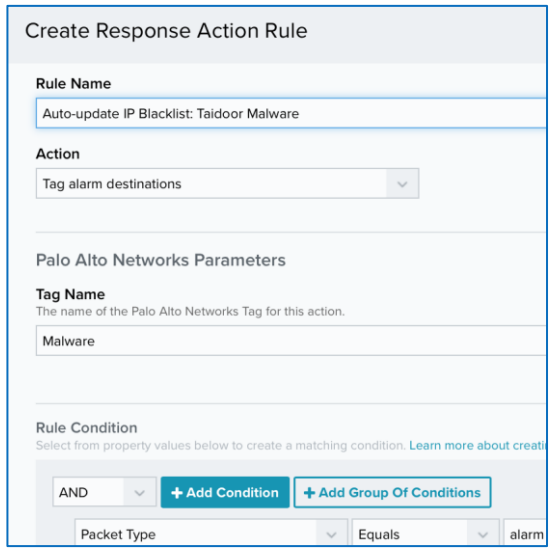
Advanced AlienApps

Cloud infrastructure, IT virtualization, productivity apps, IT operations, IT security

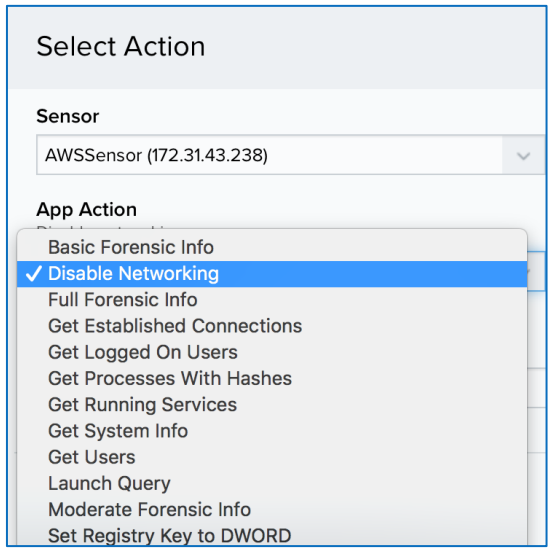
- Deeper integrations that enable response actions to third-party tools
- Orchestration rules help to automate response actions
- Collection and enrichment of data from specific environments
- Visualize threat data to aid threat investigations

AlienApps for Response Orchestration

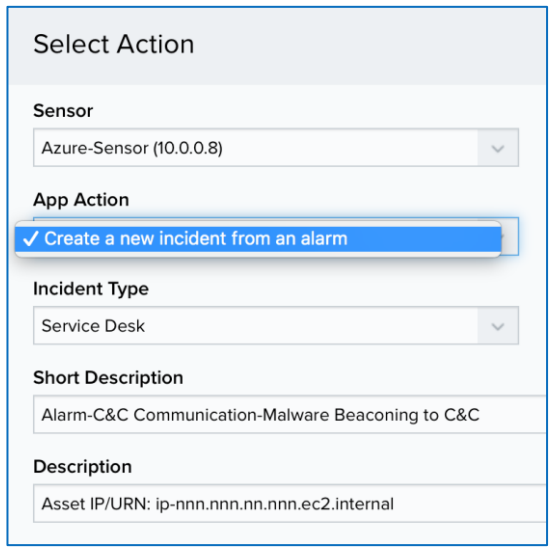
Notify your team of a security incident.



Update your protection tools to block activity.



Isolate an endpoint from the network.



Open a ticket in your existing IT workflow.

AT&T Business

USM Anywhere + SentinelOne | Benefits

Enhance threat detection and response capabilities

- Defend your endpoints from sophisticated cyber threats and automatically detect and respond directly from USM Anywhere
- Reduce unwanted “noise” by collecting only threat data from the endpoints
- Integrated endpoint threat data correlated with USM Anywhere event data detects behavioral patterns across assets
- Investigate incidents efficiently with rich and contextualized threat data in a single pane of glass

Gain a more complete picture of your assets

- SentinelOne asset discovery identifies unknown or unsecure Windows, macOS, and Linux® devices through passive scans
- Automatically integrate your asset data with USM Anywhere to create an authoritative view of assets

Accelerate time to response with improved visibility

- Gain a centralized view of your entire environment and any threats detected at the endpoint, allowing you to respond more quickly
- Quickly prioritize threats based on the latest Open Threat Exchange (OTX) and Alien Labs Threat Intelligence and business context

Powered by Phenomenal Threat Intelligence

AT&T Alien Labs provides the tactical threat intelligence that powers the automated security engineering, threat detection, and threat hunting activities in USM Anywhere. With continuous and automatic threat intelligence updates from Alien Labs, your defenses stay current even as the threat landscape changes.

High Volume Data Feeds

AI & Machine Learning

Human Expertise

Continuous Updates

AT&T Business

Helping to Make Your Security Operations Effective & Efficient

80%

Improvement in security operations staff productivity[1]

2000

Hours saved annually per audit[1]

46%

Customers with an alarm in first day after deployment[2]

1. Forrester 2018 - Total Economic Impact of AlienVault Unified Security Management
2. AlienVault user data analytics

AT&T Business

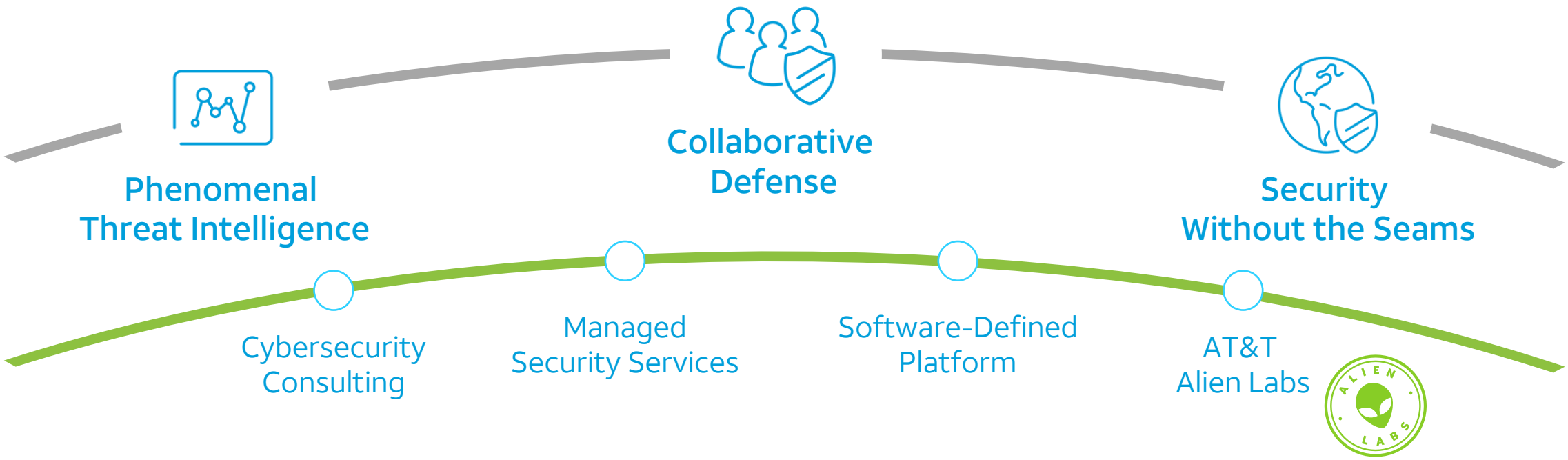
USM Anywhere Supports Key Initiatives

- Cloud Security
- Digital Transformation
- Threat Detection & Response
- Security Operations
- IT Compliance Management

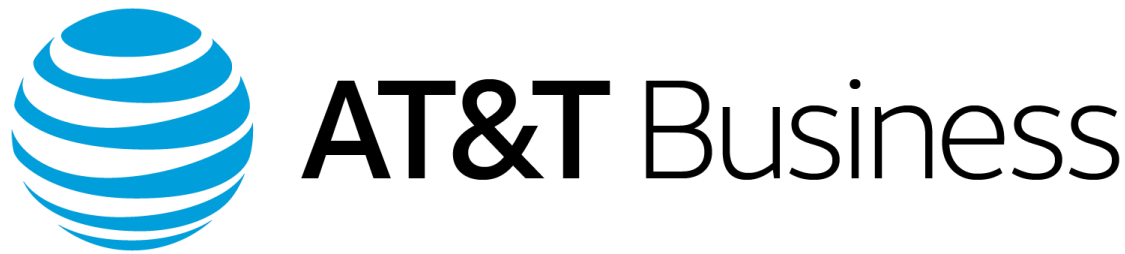
AT&T Business

AT&T Cybersecurity

Unified Security Management



AT&T Business


AT&T Business