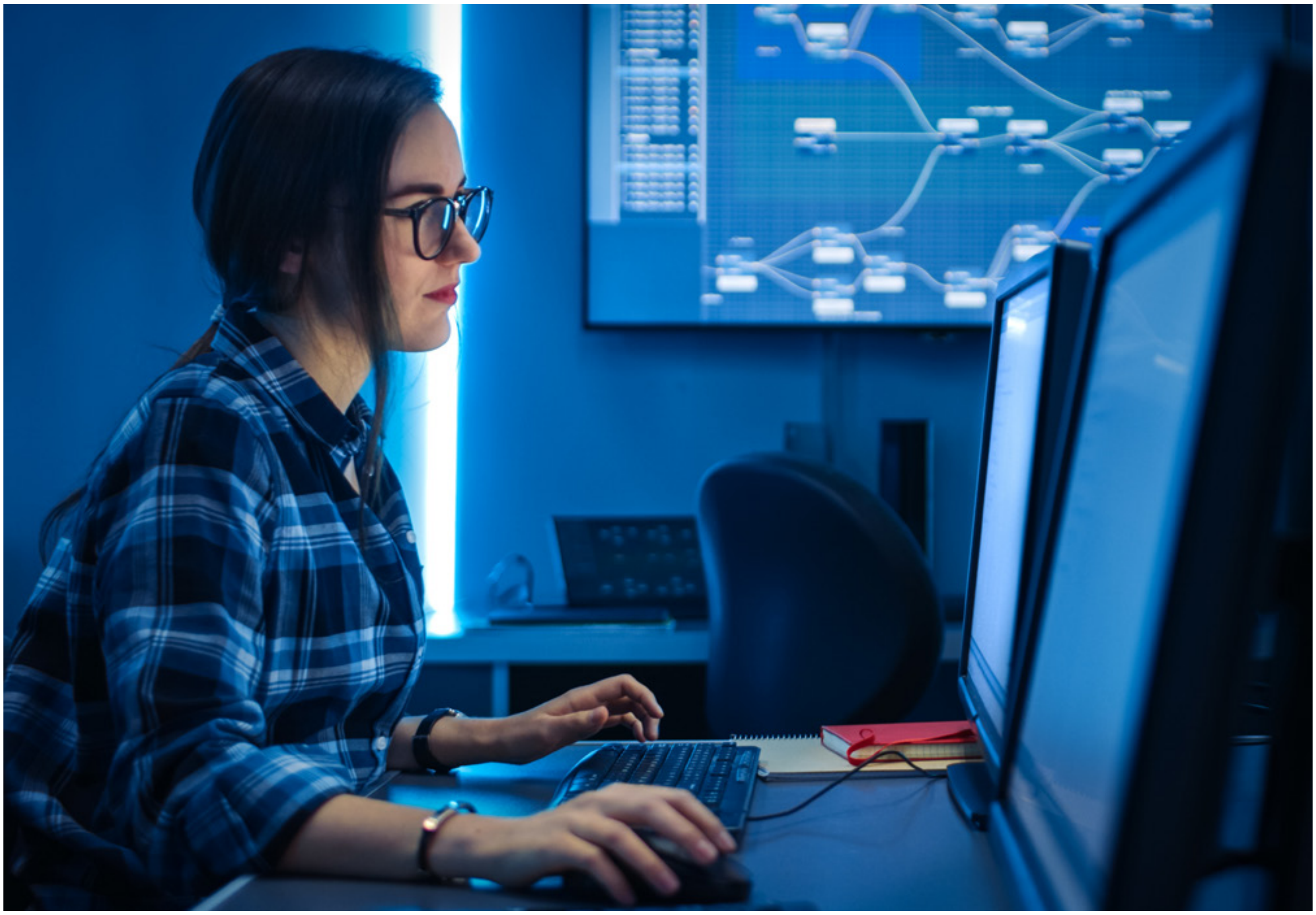
USM Anywhere

Powerful threat detection and incident response for all your critical infrastructure



USM Anywhere™ delivers powerful threat detection, incident response, and compliance management in one unified platform.

It combines the essential security capabilities needed for effective security monitoring across your cloud and on-premises environments: asset discovery, vulnerability assessment, intrusion detection, endpoint detection and response, behavioral monitoring, SIEM log management, and continuous threat intelligence.

Built for today's resource-limited IT security teams, USM Anywhere is more affordable, faster to deploy, and easier to use than traditional solutions. It eliminates the need to deploy, integrate, and maintain multiple point security solutions in your data center. A cloud-hosted platform delivered as a service, USM Anywhere offers a low total cost of ownership (TCO) and flexible, scalable deployment options for teams of any size or budget.

With USM Anywhere, you can focus on what matters most—helping to protect your IT infrastructure against today's emerging threats.

Multiple essential security capabilities in a single SaaS platform

USM Anywhere provides multiple essential security capabilities in a single SaaS solution, giving you what you need for threat detection, incident response, and compliance management—all in a single pane of glass. With USM Anywhere, you can focus on finding and responding to threats, not managing software.

An elastic, cloud-based security solution, USM Anywhere can readily scale to meet your threat detection needs as your IT environment changes and grows.

Asset discovery

- API-powered asset discovery
- Network asset discovery
- Software and services discovery

Vulnerability assessment

- Network vulnerability scanning
- Cloud vulnerability scanning
- Cloud infrastructure assessment

Intrusion detection

- Network Intrusion Detection (NIDS)
- Cloud intrusion detection

Endpoint detection and response

- Host-based Intrusion Detection (HIDS)
- File integrity monitoring
- Continuous endpoint monitoring & proactive querying

Behavioral monitoring

- Asset access logs
- Cloud access and activity logs (Microsoft Azure® Monitor, AWS®: CloudTrail®, CloudWatch, S3, ELB)
- AWS VPC Flow monitoring
- VMware® ESXi access logs

SIEM & log management

- Event correlation
- Log management
- Incident response
- Integrated threat intelligence from the AT&T Alien Labs™ security team and the Alien Labs Open Threat Exchange® (OTX™)

Key product features and highlights

Centralized security monitoring for your cloud and on-premises environments

USM Anywhere gives you powerful threat detection capabilities across your cloud and on-premises landscape, helping you to eliminate security blind spots and mitigate unmanaged shadow IT activities. Even as you migrate workloads and services from your data center to the cloud, you have the benefit of virtually seamless security visibility.

USM Anywhere natively monitors –

- AWS, Microsoft Azure, and Google Cloud™ Platform public clouds
- Windows, Linux® and macOS endpoints in the cloud and on premises
- Virtual on-premises IT on VMware / Hyper-V
- Physical IT infrastructure in your data center
- Other on-premises facilities (e.g., offices, retail stores, etc.)
- Cloud applications like Office 365 and G-Suite™

Automated response orchestration

USM Anywhere provides advanced security orchestration rules that automate actions and responses according to your needs, making your work more efficient. You can –

- Reduce alarm "noise" with suppression rules
- Generate alarms based on custom parameters
- Auto-respond to events with orchestration rules
- Create orchestration rules for third-party apps

Powerful security analytics at your fingertips

When you centralize security monitoring of all your cloud and on-premises IT environments, you need a highly efficient way to search and analyze large amounts of data from across a complex and dynamically changing IT infrastructure. USM Anywhere provides an intuitive and flexible interface to search and analyze your security-related data. With it, you can –

- Search and analyze your data to investigate incidents
- Pivot between assets, vulnerabilities, and event data to pinpoint the data you need
- Create and export custom data views for compliance-ready reporting

Built natively in the cloud for the cloud

Unlike other legacy security solutions that have been modified to work in the cloud, USM Anywhere is a truly cloud-native security monitoring solution that utilizes the unique security elements of public cloud infrastructure. It uses direct hooks into cloud APIs to give you a richer data set, greater control over the security of your cloud infrastructure and SaaS applications, and more immediate visibility across your entire environment as early as within minutes of installation.

Advanced graph-based analytics engine

USM Anywhere takes an enhanced approach to SIEM event correlation that makes security analysis faster, more flexible, and more effective than ever. With our unique, graph-based approach to correlation, you can:

- Quickly and efficiently run ad-hoc queries on large and complex data sets
- Enhance correlation by keying off connections between assets, users, and activities and the changes occurring between them

Extended security orchestration with AlienApps

USM Anywhere is a highly extensible platform that utilizes AlienApps™—integrations with third-party security and productivity tools—to extend your security orchestration capabilities. With AlienApps, you can –

- Extract and analyze data from third-party security applications
- Visualize external data within USM Anywhere's rich graphical dashboards
- Push actions to third-party security tools based on threat data analyzed by USM Anywhere
- Gain new security capabilities as new AlienApps are introduced into USM Anywhere

USM Anywhere currently ships with out-of-the-box integration with leading security apps, including Cisco Umbrella™ and Palo Alto Networks® to provide data collection and action response orchestration.

Deploying USM Anywhere is fast and easy

USM Anywhere consists of a highly scalable, two-tier architecture to manage and monitor your cloud and on-premises security. USM Anywhere sensors and USM Anywhere agents collect and normalize data from your cloud and on-premises environments and transfers that data to USM Anywhere for centralized collection, security analysis, threat detection, and compliance-ready log management. The only thing you deploy in your environment are sensors and agents. AT&T Cybersecurity maintains and updates USM Anywhere automatically.

From installation to security insights in 3 simple steps

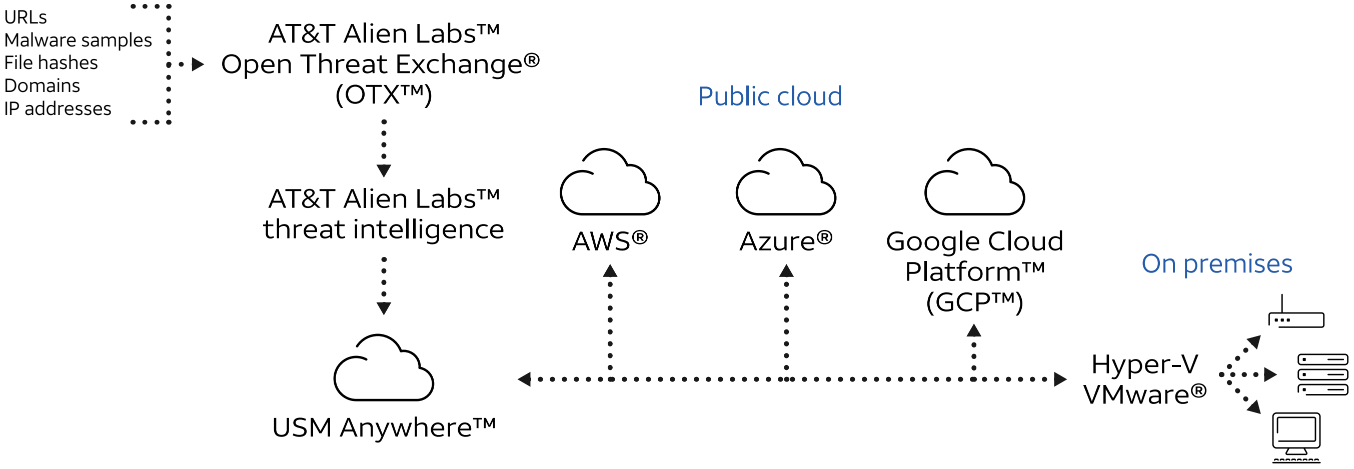
1. Deploy a USM Anywhere sensor in your cloud or on-premises environment. Enter the first sensor authorization code provided by AT&T Cybersecurity, and then point the sensor to your dedicated USM Anywhere URL.
2. Log into your USM Anywhere account to deploy and manage USM Anywhere agents, run asset discovery and vulnerability scans, and much more..
3. Start monitoring for threats and malicious activities. From USM Anywhere, you can search and analyze your data, and orchestrate your security responses and alarms.

Integrated threat intelligence for better protection

USM Anywhere receives continuous threat intelligence updates from the Alien Labs security research team. This dedicated team spends countless hours researching and analyzing the different types of attacks, emerging threats, vulnerabilities, and exploits—so you don't have to.

Additionally, Alien Labs utilizes community-sourced threat intelligence from the Open Threat Exchange (OTX). OTX™ is the largest crowd-sourced threat intelligence exchange in the world, providing security for you that is powered by a global community of threat researchers and security professionals.

Over 130,000 participants from more than 140 countries contribute 20 million threat indicators daily to OTX. Alien Labs analyzes raw OTX data with a powerful discovery engine that is able to granularly analyze the nature of the threat, and a similarly powerful validation engine that continually curates the database and certifies the validity of those threats. The result—your USM Anywhere environment uses the latest emerging threat intelligence to help keep your organization protected.


URLs
Malware samples
File hashes
Domains
IP addresses
AT&T Alien Labs™ Open Threat Exchange® (OTX™)
AT&T Alien Labs™ threat intelligence
USM Anywhere™
Public cloud
AWS®
Azure®
Google Cloud Platform™ (GCP™)
On premises
Hyper-V
VMware®

Immediate scalability. No forklift upgrades.

USM Anywhere scales with your business needs. You can add or remove software sensors and agents, bring on additional cloud services, and scale central log management as your business needs change. The USM Anywhere subscription is based on the monthly raw log ingestion capacity. All of the essential security capabilities are included in the subscription and scale with the system's capacity.

- Maximum raw data ingestion per month subscription
- Subscription tiers for all environment sizes starting at 250GB per month
- Support and maintenance included
- Integrated Alien Labs threat intelligence included
- Cold storage included for the life of the active USM Anywhere subscription

USM Anywhere sensors and agent

The USM Anywhere agent is a lightweight, adaptable endpoint agent based on osquery that extends the powerful threat detection capabilities of USM Anywhere to the endpoint. It enables endpoint detection and response (EDR), file integrity monitoring (FIM), and rich endpoint telemetry capabilities that are essential for complete and effective threat detection, response, and compliance. You can deploy the USM Anywhere agent on your Windows, Linux, and macOS endpoints in the cloud, on premises, and remote.

USM Anywhere sensors give you deep security visibility into your cloud and on-premises environments. The sensors conduct scans, monitor packets on the networks, and collect logs from assets, the host hypervisor, and cloud environments. This data is normalized and sent to USM Anywhere for analysis and correlation.

Sensor type	System requirements
AWS Sensor	An m5.large instance in Amazon VPC or m3.large instance in EC2-Classic network 100GB EBS volume for short-term storage as data is processed
Azure Sensor	D2 Standard or DS2 Standard 12 GB Data volume
Google Cloud Platform Sensor	An n1-standard-2 instance, standard instance with 2vCPUs and 7.5 GB of memory Zonal SSD persistent disk 50GB
VMware Sensor	**Total Cores:** 4 **Ram:** 12 GB of memory dedicated to VMware **Storage:** 100 GB data device and 50 GB root device (150 GB total) VMware ESXi 5.1 or later
Hyper-V Sensor	**Total Cores:** 4 **Ram:** 12 GB of memory dedicated to the Hyper-V virtual machine **Storage:** 100 GB data device and 50 GB root device (150 GB total) 2012 R2 OS with Hyper-V Manager or System Central Virtual Manager (SCVMM) 2012, or Windows Server 2016

Sensor performance	
IDS Throughput (Mbps)[2,3]	600

[1] In each environment listed above, internet connectivity to your USM Anywhere instance is required.
[2] Actual sensor performance may vary depending on environment, configuration, etc.
[3] IDS throughput relates to on-premises network-based IDS. It applies to the VMware and Hyper-V sensor types only.

Additional sensors can be added to your USM Anywhere by retrieving additional sensor authorization codes from the Deployment UI page. You cannot exceed number of sensors that are included in your subscription, however you are not restricted on which mix of sensors that you use. You can purchase additional sensor licenses as you need.

Experience the power of USM Anywhere – try it free!

Ready to experience the power of USM Anywhere? Why not take it for a test drive? Visit us here and get immediate access to a free hands-on demo environment – no download or installation required.

Ready to get started? Try USM Anywhere in your environment – free for the first 14 days. Terms and conditions apply. Visit us for more information.

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 your business to innovate.