ALIEN VAULT

DATA SHEET

AlienVault® USM Anywhere™

Powerful Threat Detection for the Cloud is Now Available in the Cloud

AlienVault® Unified Security Management™ (USM™) Anywhere is a cloud-based security management platform that accelerates and simplifies threat detection, incident response, and compliance management for your cloud, hybrid cloud, and on-premises environments. USM Anywhere includes sensors that are deployed into your environments that natively monitor Amazon Web Services, Microsoft Azure Cloud, Microsoft Hyper-V, and VMware ESXi -- providing you a comprehensive solution for managing security across your public and private cloud infrastructure.

With USM Anywhere, you can rapidly deploy software sensors natively into all of your virtual, and cloud environments while centrally managing data collection, analysis and detection of threats to your business operations.

Five Essential Security Capabilities in a Single SaaS Platform

AlienVault USM AnywhereTM provides five essential security capabilities in a single SaaS platform, giving you everything you need to detect and respond to threats and manage compliance. As a cloud-based security solution, you can scale your threat detection and response capabilities as your hybrid environment changes, and pay for only exactly what you need, when you need it. Finally, you can focus on finding and responding to threats, not managing software!

Asset Discovery
- API-powered asset discovery
- Network asset discovery
- Software discovery
- Services discovery

Vulnerability Assessment
- Authenticated vulnerability assessment
- Cloud infrastructure assessment

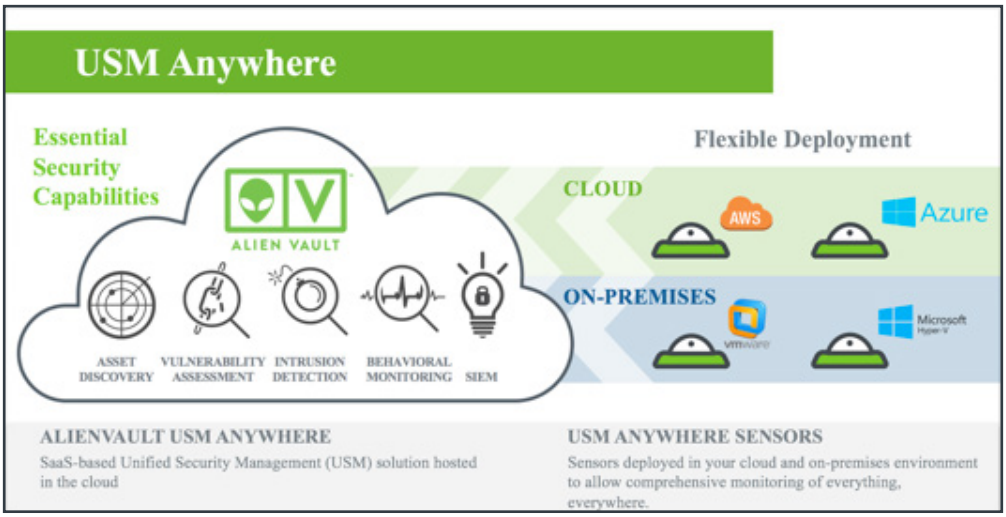
Intrusion Detection
- Network IDS
- Host IDS
- File Integrity Monitoring

Behavioral Monitoring
- Asset access logs
  - Cloud access logs (Azure: Insights, AWS: CloudTrail, CloudWatch, S3 access log, ELB access log)
- AWS VPC Flow monitoring
- VMware ESXi access logs

SIEM
- Event correlation
- Log management
- Incident response
- Integrated AlienVault Open Threat Exchange™ (OTX) Data
- 12-month raw log retention

Deploying USM Anywhere is Fast and Easy

USM Anywhere consists of a modular, scalable, two-tier architecture to manage and monitor every aspect of cloud and on-premises security. USM Anywhere Sensors collect and normalize data from all of your cloud and on-premises environments and securely transfers it to USM Anywhere to provide centralized collection, management, analysis, correlation, alerting, log management, and reporting. The only thing you deploy is the sensors into your environment. AlienVault creates, maintains and updates your USM Anywhere automatically in AlienVault's secure cloud environment.



USM Anywhere Sensors are purpose-built for each of their target environments. The sensors are built to deploy natively into each environment and utilize the API and available logs of the hypervisor or cloud platform. The sensors know the capabilities of the environment and enable features specific to that environment, e.g. agentless packet monitoring is not possible in cloud environments, so the AWS sensor does not enable the Network Intrusion Detection (NIDS), whereas in VMware environments, port mirroring at the physical layer or in the distributed virtual switch can be enabled for NIDS analysis. Another similar example is methods for discovering assets. USM Anywhere Sensor can discover assets by querying the hypervisor or cloud platform API to discover assets or to run network asset discovery based on IP ranges and CIDR, or the user can directly add assets. Cloud platforms may view network scanning as a threat and block the operation, which makes API asset discovery the better choice for continuous asset discovery in cloud environments.

USM ANYWHERE SENSOR	DEPLOYMENT FORMAT
AWS sensor	CloudFormation Template
Azure sensor	Azure Resource Manager (ARM) Template and vhd Image
VMware ESXi	ovf
Hyper-V	vhd, vhdx

Getting started with USM Anywhere is as easy as 1-2-3

1. Download and deploy USM Anywhere Sensor in your AWS, Azure, VMware ESXi, or Hyper-V environment. You will need to enter the first sensor authorization code provide by AlienVault.

2. Point the sensors to your dedicated USM Anywhere URL.

3. Follow the installation wizard to specify the log sources or network segments to be monitored. Start detecting threats.

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 agreement, however you are not restricted on which mix of sensors that are used.

We've Got a Sensor for That

The purpose-built natively deployed software sensors give you visibility into your on-premises, cloud, multi-cloud and hybrid cloud environments. The sensors conduct scans, monitor packets on the networks and collect logs from assets and the hosted hypervisor and cloud environments. The information is normalized and then securely forwarded to USM Anywhere for analysis and correlation. In addition to collecting data from the assets and networks in each of the environments, the sensor adds the following capabilities:

Amazon Web Services Cloud Sensor:

- AWS API asset discovery
- CloudTrail monitoring and alerting
- CloudWatch monitoring and alerting
- S3 access log monitoring and alerting
- ELB access log monitoring and alerting
- AWS infrastructure assessment

Microsoft Azure Cloud Sensor:

- Azure API asset discovery
- Azure Insights monitoring & Alerting
- Azure infrastructure assessment

VMware ESXi Virtual Sensor:

- Network asset discovery
- ESXi API asset discovery
- Network intrusion detection (NIDS)
- ESXi log monitoring & alerting

Microsoft Hyper-V Virtual Sensor:

- Network asset discovery
- Network intrusion detection (NIDS)

ON-PREMISES SOFTWARE SENSORS	CLOUD SENSORS
VMware ESXi	Amazon Web Services
Microsoft Hyper-V	Microsoft Azure Cloud

Windows and Linux Host Logs Collection

USM Anywhere supports collecting logs and detecting changes on Windows and Linux hosts in your environment. USM Anywhere integrates a library of plugins to support endpoint agents as well as syslog sources. The plugins have the capability to automatically detect the forwarded log format and assign the plugin to the asset or the plugin can be assigned to the asset manually.

HOST LOG FORWARDING PLUGINS
OSSEC
NxLog
Sysmon
OSQuery

Integrated Threat Intelligence for the Best Protection

Your USM Anywhere platform receives continuous updates from the AlienVault Labs Threat Research team. This dedicated team spends countless hours analyzing the different types of attacks, emerging threats, suspicious behavior, vulnerabilities and exploits they uncover across the entire threat landscape.

We supplement the AlienVault Labs' research with data from our Open Threat Exchange (OTX). OTX is the largest and most authoritative crowd-sourced threat intelligence exchange in the world, providing security for you that is powered by all. Every day, more than 47,000 participants from 140+ countries contribute over 4 million threat indicators to OTX. We automatically analyze raw OTX data through 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.

Immediate Scalability. No Forklift Upgrades.

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

- Maximum raw data ingestion per month subscription
- Includes one AlienVault USM Anywhere standard sensor
- Support and maintenance included
- AlienVault Labs Threat Intelligence subscription included
- Dedicated and segmented data stored for 12 months (3 months hot, 9 months cold)

PRODUCT NAME - MONTHLY RAW LOG INGESTION CAPACITY
USM Anywhere, 250GB
USM Anywhere, 500GB

The USM Anywhere license includes one sensor; you can add or remove sensors to any supported environment as your business needs change. This is accomplished by purchasing the appropriate number of sensor capabilities for your USM Anywhere subscription.

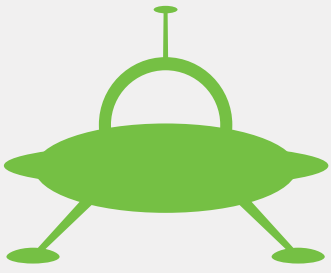
PRODUCT NAME
USM Anywhere Standard Sensor, Virtual

Each sensor for the host environment requires the following resources:

ENVIRONMENT TYPE	SYSTEM REQUIREMENTS
VMware Sensor	**Total Cores:** 4 **Ram:** 12GB **Storage:** 250GB VMware ESXi 5.1+ Internet connectivity to your USM Anywhere instance is required
Hyper-V Sensor	**Total Cores:** 4 **Ram:** 12GB **Storage:** 250GB System Center 2012 Internet connectivity to your USM Anywhere instance is required
AWS Sensor	T2.medium/m3.medium instance 12-GB EBS volume Internet connectivity to AlienVault USM Anywhere is required
Azure Sensor	Standard D2 v2 12GB data volume Internet connectivity to your USM Anywhere instance is required

Try it today. Free for 14 days.

Ready to see how AlienVault USM Anywhere can help you reduce risks, pass audits, and enhance your incident response program? Try one of our USM Anywhere in your environment today for free – for the first 14 days. Please visit this site to find out more information: www.alienvault.com/products/usm-anywhere/free-trial



About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.