AT&T Cybersecurity

FICHA TÉCNICA

AlienVault® USM Anywhere™

Potente detección de amenazas y respuesta a incidentes para toda su infraestructura crítica

AlienVault® USM Anywhere™ acelera y centraliza la detección de amenazas, la respuesta a incidentes y la gestión del cumplimiento normativo para sus entornos en la nube, locales e híbridos. USM Anywhere incluye sensores de nube especialmente diseñados que controlan sus entornos de nube Amazon Web Services (AWS) y Microsoft Azure. A nivel local, los sensores virtuales livianos funcionan sobre Microsoft Hyper-V y VMware ESXi para controlar su infraestructura de TI física y su nube privada virtual.

Con USM Anywhere, puede implementar sensores con rapidez en sus entornos de la nube y locales mientras que administra de manera centralizada la recopilación de datos, los análisis de seguridad y la detección de amenazas desde la nube segura de AlienVault.

Múltiples capacidades esenciales de seguridad en una sola plataforma SaaS

AlienVault USM Anywhere brinda múltiples capacidades esenciales de seguridad en una sola solución SaaS para que tenga todo lo que necesita para la detección de amenazas, la respuesta a incidentes y la gestión del cumplimiento normativo, todo en una sola pantalla. Con USM Anywhere, puede enfocarse en encontrar y responder a amenazas, y no en gestionar software. USM Anywhere, una solución de seguridad elástica basada en la nube, puede adaptarse con facilidad para satisfacer sus necesidades de detección de amenazas a medida que su entorno de TI cambia y crece.

Descubrimiento de activos
- Descubrimiento de activos impulsado por API
- Descubrimiento de activos en la red
- Descubrimiento de software y servicios

Evaluación de vulnerabilidades
- Análisis de vulnerabilidades de la red
- Análisis de vulnerabilidades de la nube
- Evaluación de la infraestructura de la nube

Detección de intrusiones
- IDS en la nube
- IDS en la red
- IDS del host
- Supervisión de la integridad de los archivos

Supervisión del comportamiento
- Registros de acceso de activos
- Registros de acceso a la nube (Azure Monitor, AWS: CloudTrail, CloudWatch, S3, ELB)
- Supervisión del flujo de VPC de AWS
- Registros de acceso a VMware ESXi

SIEM y gestión de registros
- Correlación de eventos
- Gestión de registros
- Respuesta a incidentes
- Datos integrados de Open Threat Exchange® (OTX™) de AlienVault®
- Retención de archivos sin procesar durante 12 meses

Principales características y ventajas del producto

Supervisión de seguridad centralizada para sus entornos en la nube y locales

USM Anywhere le brinda potentes capacidades de detección de amenazas en todo su entorno de la nube y local, lo que lo ayuda a eliminar los puntos ciegos de la seguridad y a mitigar la TI paralela. Incluso cuando migra cargas de trabajo y servicios desde su centro de datos a la nube, tiene la garantía de tener total visibilidad sobre la seguridad.

USM Anywhere supervisa de manera nativa:

- Las nubes públicas AWS y Microsoft Azure
- TI virtual en las instalaciones sobre VMware / Hyper-V
- Infraestructura de TI física en su centro de datos
- Otras instalaciones locales (por ejemplo, oficinas, tiendas minoristas, etc.)

Orquestación automatizada de respuestas

USM Anywhere brinda reglas avanzadas de orquestación de seguridad que automatizan las acciones y las respuestas de acuerdo con sus necesidades, lo que hace que su trabajo sea más eficiente. Usted puede:

- Reducir el “ruido” de las alarmas con reglas de supresión
- Generar alarmas personalizadas basadas en cualquier parámetro
- Responder automáticamente a eventos con reglas de orquestación
- Crear reglas de orquestación para aplicaciones de terceros

Análisis de seguridad potentes a su alcance

Cuando centraliza la supervisión de seguridad de todos sus entornos de TI locales y en la nube, necesita una manera muy eficiente para buscar y analizar grandes cantidades de datos en una infraestructura de TI compleja y muy cambiante. USM Anywhere brinda una interfaz intuitiva y flexible para buscar y analizar sus datos relacionados con la seguridad. Con esto, usted puede:

- Buscar y analizar sus datos para encontrar amenazas e investigar incidentes
- Cambiar entre activos, vulnerabilidades y datos de eventos para determinar los datos que necesita
- Crear y exportar vistas de datos personalizados para informes que cumplan con las normas

Creado directamente en la nube para la nube

A diferencia de otras soluciones de seguridad tradicionales que han sido modificadas para trabajar en la nube, USM Anywhere es una solución única nativa de la nube que aprovecha los elementos de seguridad únicos de la infraestructura de la nube pública. Usa ganchos directos a las API de la nube para brindarle un conjunto de datos más rico, mayor control sobre la seguridad de la nube, y más visibilidad inmediata de su entorno de la nube a solo minutos de la instalación

Motor de análisis basado en gráficos avanzado

USM Anywhere adopta un nuevo enfoque para la correlación de eventos SIEM que hace que el análisis de seguridad sea más rápido, flexible y eficaz que nunca. Con nuestro enfoque único basado en gráficos para la correlación, usted puede:

- Ver un modelo de estado completo de su entorno en cualquier momento y comparar diferentes períodos.
- Ejecutar consultas ad hoc de manera rápida y eficiente sobre conjuntos de datos grandes y complejos
- Mejorar la correlación al articular conexiones entre activos, usuarios y actividades, y los cambios que ocurren entre ellos

Orquestación de seguridad extendida con AlienApps™

USM Anywhere es una plataforma muy extensible que potencia AlienApps (integraciones con herramientas de seguridad y productividad de terceros) para ampliar sus capacidades de orquestación de seguridad. Con AlienApps, usted puede:

- Extraer datos desde aplicaciones de seguridad de terceros
- Visualizar datos externos dentro de los ricos paneles de control gráfico de USM Anywhere
- Impulsar acciones a las herramientas de seguridad de terceros basadas en los datos de las amenazas analizadas por USM Anywhere
- Obtener nuevas capacidades de seguridad a medida que se introducen nuevas AlienApps en USM Anywhere

USM Anywhere actualmente se envía con integración inmediata con las principales aplicaciones de seguridad, entre las que se incluyen Cisco Umbrella y Palo Alto Networks, para brindar recopilación de datos y orquestación de respuesta a acciones.

Implementar USM Anywhere es rápido y fácil

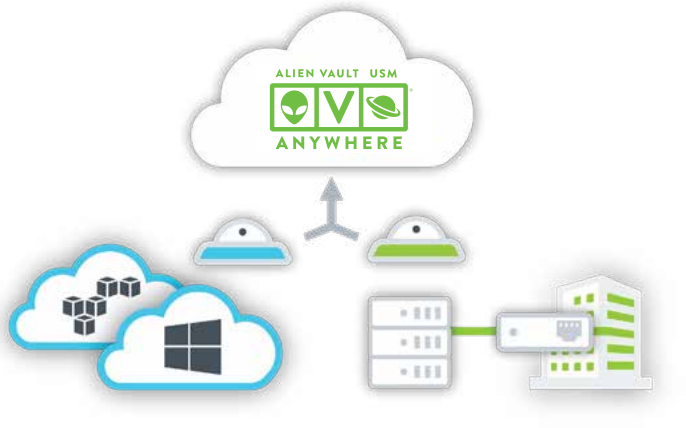
USM Anywhere consta de una arquitectura de dos niveles muy escalable para administrar y controlar todos los aspectos de su seguridad local y en la nube. Los sensores USM Anywhere recopilan y normalizan los datos desde sus entornos en la nube y locales, y transfieren esos datos de manera segura a USM Anywhere para acciones centralizadas de recopilación, análisis de seguridad, detección de amenazas y gestión de registros. Lo único que implementa son los sensores en su entorno. AlienVault mantiene, asegura y actualiza USM Anywhere automáticamente.

Desde instalación hasta información sobre seguridad en 3 simples pasos

1. Descargue e implemente un sensor USM Anywhere en su entorno en la nube o local. Ingrese el primer código de autorización de sensor proporcionado por AlienVault y luego dirija el sensor a su URL específica de USM Anywhere.

2. Ingrese a su cuenta USM Anywhere, el centro de control para su seguridad en la nube híbrida. Siga los pasos del asistente de instalación para identificar las fuentes del registro y los segmentos de la red que supervisará.

3. Comience a supervisar amenazas y actividades maliciosas. Desde USM Anywhere puede programar escaneos de vulnerabilidad, buscar y analizar sus datos, y orquestar sus respuestas y alarmas de seguridad.



Almacenamiento de datos en USM Anywhere

Almacenamiento de datos especial de tenencia única

Cuando envía datos sensibles relacionados con la seguridad a una solución de monitoreo de seguridad en la nube, usted quiere estar seguro de que los datos están protegidos y no se filtrarán. Por eso, AlienVault utiliza una arquitectura de almacenamiento de datos de tenencia única para administrar todas las cuentas de nuestros clientes de manera segura.

Con USM Anywhere, sus datos se almacenan en su propio contenedor dedicado, que está completamente aislado de los datos de otros clientes. Mientras que la tenencia múltiple suele tener filtraciones y roturas de datos que pueden afectar muchas cuentas de clientes, especialmente a medida que se escalan los proveedores de SaaS, la tenencia única garantiza que todos los datos del cliente estén guardados de manera separada y que no se filtren. Esta arquitectura es mejor para usted y para nosotros.

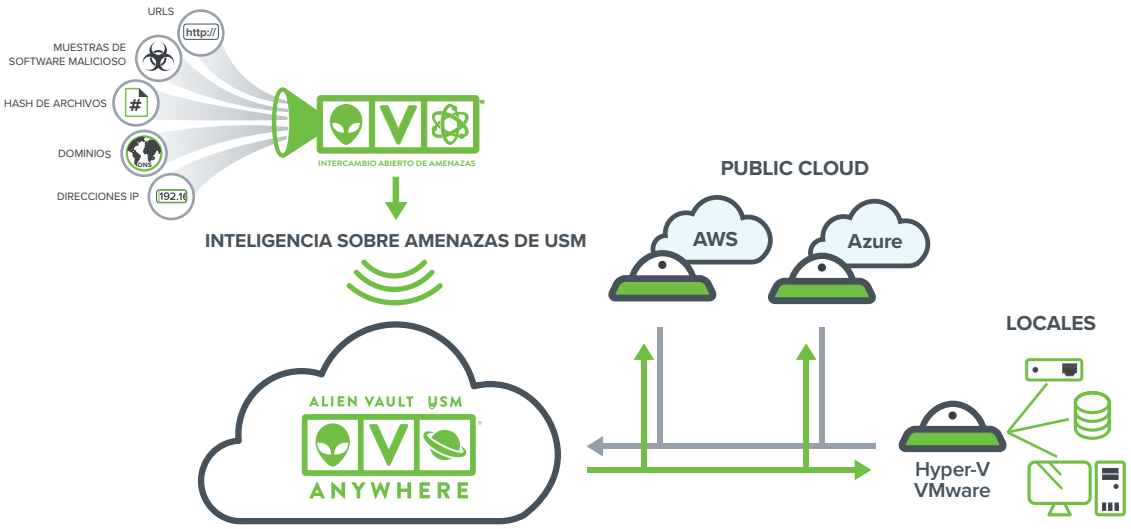
Almacenamiento en frío listo para el cumplimiento normativo

USM Anywhere admite la retención de registros a largo plazo, conocida como “almacenamiento en frío”. Por defecto, USM Anywhere permite 12 meses de almacenamiento en frío con la posibilidad de ampliar su capacidad de almacenamiento a largo plazo. Además, USM Anywhere admite un enfoque de “una sola escritura y múltiples lecturas” (Write once, read many, WORM) para evitar la modificación de los datos de los registros. Los registros se pueden solicitar para un rango de fechas específico desde USM Anywhere según sea necesario.

Inteligencia de amenazas integrada para la mejor protección

USM Anywhere recibe actualizaciones constantes de inteligencia de amenazas por parte del equipo de investigación de seguridad de AlienVault Labs. Este equipo especial pasa incontables horas investigando y analizando los diferentes tipos de ataques, amenazas emergentes, vulnerabilidades y ataques, para que no tenga que hacerlo usted.

AlienVault Labs usa la información abierta sobre amenazas del intercambio abierto de amenazas AlienVault Open Threat Exchange (OTX). OTX es la comunidad de intercambio de información sobre amenazas más grande e importante del mundo, que le brinda una seguridad lograda por todos. En OTX colaboran más de 65.000 personas de más de 140 países, con más de catorce millones de indicadores de amenazas todos los días. AlienVault Labs analiza los datos sin analizar de OTX con un potente motor de descubrimiento capaz de analizar minuciosamente la naturaleza de la amenaza, y un motor de validación igual de poderoso que organiza constantemente la base de datos y certifica la validez de esas amenazas. El resultado: su entorno USM Anywhere usa lo último en información sobre amenazas para mantener la seguridad de su organización.



Escalabilidad inmediata. Sin actualizaciones costosas.

USM Anywhere se adapta a sus necesidades comerciales. Puede agregar o eliminar sensores de software, agregar servicios adicionales en la nube y adaptar la gestión central de registros a medida que cambian sus necesidades comerciales. La suscripción de USM Anywhere está basada en la capacidad de incorporación de registros mensuales sin analizar. Las cinco capacidades esenciales de seguridad están incluidas en la suscripción y se adaptan a la capacidad del sistema.

- Incorporación máxima de datos sin analizar por suscripción mensual
- Niveles de suscripción para entornos de todos los tamaños, desde 250 GB a 4 TB por mes
- Incluye un sensor estándar AlienVault USM Anywhere
- Incluye soporte y mantenimiento
- Incluye información sobre amenazas de AlienVault Labs integrada
- Incluye 12 meses de almacenamiento en frío, con la capacidad de ampliar la capacidad de almacenamiento

Pruébelo hoy. Gratis por 14 días.

¿Está listo para ver de qué manera AlienVault USM Anywhere puede ayudarlo a reducir riesgos, pasar auditorías y mejorar su programa de respuesta a incidentes? Pruebe USM Anywhere en su entorno, gratis los primeros 14 días. Visite este sitio para obtener más información. www.alienvault.com/products/usm-anywhere/free-trial

Tenemos un sensor para eso

Los sensores de USM Anywhere le brindan mayor visibilidad de seguridad en sus entornos en la nube y locales. Los sensores realizan escaneos, supervisan paquetes en las redes y recopilan registros de activos, hipervisor de host y entornos en la nube. Estos datos se normalizan y se envían de manera segura a USM Anywhere para su análisis y correlación. Además de recopilar datos de activos y redes en cada uno de los entornos, los sensores agregan las siguientes capacidades:

Sensor de nube de Amazon Web Services:

- Descubrimiento de activos de AWS API
- Supervisión y alertas de registros de acceso de ELB
- Supervisión y alertas de registros de acceso de S3
- Supervisión y alertas de CloudTrail
- Supervisión y alertas de CloudWatch
- Evaluación de la infraestructura de AWS
- Detección de intrusos en la nube (Cloud Intrusion Detection, IDS)

Sensor de nube de Microsoft Azure:

- Descubrimiento de activos de Azure API
- Supervisión y alertas de Azure Monitor
- Evaluación de la infraestructura de Azure
- Detección de intrusos en la nube (Cloud Intrusion Detection, IDS)

Sensor virtual de Microsoft Hyper-V:

- Descubrimiento de activos en la red
- Detección de intrusos en la red (Network Intrusion Detection, NIDS)

Sensor virtual de VMware ESXi:

- Descubrimiento de activos en la red
- Descubrimiento de activos de ESXi API
- Detección de intrusos en la red (Network Intrusion Detection, NIDS)
- Supervisión y alertas de registros de ESXi

TIPO DE ENTORNO	REQUISITOS DEL SISTEMA
Sensor AWS	Instancia t2.large en Amazon VPC o m3.large en EC2-Classic Volumen EBS de 12 GB para almacenamiento a corto plazo mientras se procesan los datos
Sensor Azure	12 GB de volumen de datos en D2 Standard o DS2 Standard
Sensor VMware	**Núcleos totales:** 4 **Ram:** 12 GB dedicados a VMware **Almacenamiento:** 100 GB VMware ESXi 5.1+
Sensor Hyper-V	**Núcleos totales:** 4 **Ram:** 12 GB dedicados a Hyper-V **Almacenamiento:** 100 GB Sistema operativo 2012 R2 con Hyper-V Manager o Virtual Machine Manager

En cada entorno mencionado anteriormente, se requiere conexión a Internet a su instancia de USM Anywhere.

Puede agregar sensores adicionales a su USM Anywhere al recuperar los códigos adicionales de autorización del sensor desde la página Deployment UI. No puede superar la cantidad de sensores que están incluidos en su suscripción, aunque no hay restricciones respecto a qué mezcla de sensores usa. Una suscripción a USM Anywhere incluye la licencia de un sensor. Puede comprar licencias de sensores adicionales según sea necesario.