Gestión Unificada de Seguridad USM AlienVault

La plataforma Unified Security Management™ (USM™, Gestión Unificada de Seguridad) acelera y simplifica la detección de amenazas, la respuesta a incidentes y la gestión del cumplimiento normativo para equipos de TI con recursos limitados, desde el primer día. Con controles esenciales de seguridad y conocimientos de amenazas ya integrados, AlienVault pone a su disposición y a su alcance visibilidad completa de amenazas de seguridad que acechan a su red y el modo de mitigarlas de forma rápida y sencilla.

Tanto grandes como pequeñas, todas las organizaciones necesitan visibilidad completa para:

- Detectar amenazas emergentes por todo el entorno
- Responder rápidamente a incidentes y llevar a cabo investigaciones exhaustivas
- Medir, gestionar e informar del cumplimiento de normas (PCI, HIPAA, ISO y más)
- Optimizar sus inversiones existentes en seguridad y reducir el riesgo

La solución de Gestión Unificada de Seguridad (USM) de AlienVault proporciona esta visibilidad completa de seguridad proporcionando las cinco capacidades esenciales de seguridad en una plataforma unificada, controlada por una única consola de gestión:

- **Descubrimiento de activos:** descubrimiento activo y pasivo en la red
- **Evaluación de vulnerabilidades:** escaneo activo de la red, monitorización continua de vulnerabilidades
- **Detección de intrusiones:** IDS (Detección de intrusión en red) en red y host, monitorización de integridad de archivos
- **Monitoreo de comportamiento:** análisis del flujo de red, monitorización de disponibilidad del servicio
- **SIEM:** gestión de registros, correlación de eventos, análisis e informes

Conocimiento Integrado de Amenazas

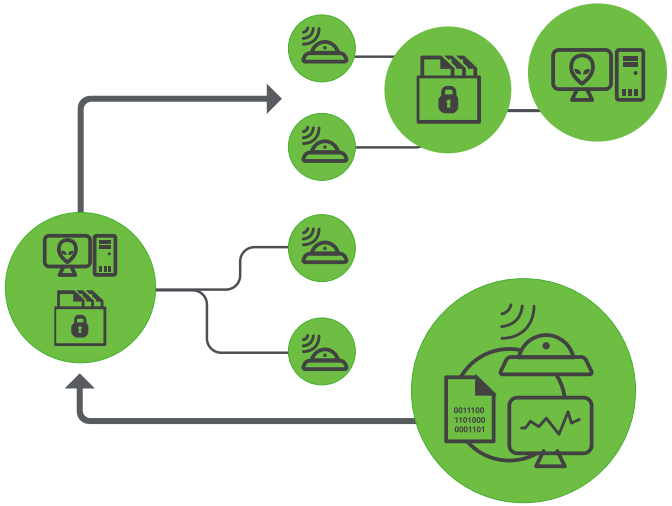
El servicio de Conocimiento de Amenazas de AlienVault Labs maximiza la efectividad de cualquier programa de monitoreo de seguridad, proporcionando regularmente directivas de correlación actualizadas, firmas de detección de intrusiones, guía de respuesta y mucho más. Estas actualizaciones continuas permiten que la plataforma USM analice la gran cantidad de datos de eventos procedentes de todas sus fuentes de datos, y le dice cuáles son exactamente las amenazas más importantes a las que se enfrenta su red ahora mismo y qué hacer al respecto. Nuestros expertos en amenazas emplean innumerables horas investigando los últimos exploits, cepas de malware, técnicas de ataque e IP maliciosas, para que usted no tenga que hacerlo. Incorporan esta experiencia a la biblioteca de más de 2.000 directivas de correlación personalizables que vienen con la plataforma USM, eliminando la necesidad de que usted tenga que realizar su propia investigación y escribir sus propias reglas de correlación, y ofreciéndole la capacidad de detectar y responder a amenazas desde el primer día.

El equipo de Investigación de Amenazas de AlienVault Labs también mantiene el Intercambio Abierto de Amenazas (OTX), la primera comunidad de conocimiento de amenazas verdaderamente abierta que permite la defensa colaborativa con acceso abierto a la investigación colaborativa sobre amenazas emergentes. OTX se integra con USM de AlienVault y permite que todas las personas de la comunidad OTX colaboren activamente, fortaleciendo sus propias defensas mientras ayudan a otros a hacer lo propio.

Gestión Unificada de Seguridad: cómo funciona

Todos los productos USM AlienVault incluyen estos tres componentes fundamentales, disponibles como dispositivo de hardware o virtual:

- **Sensor USM:** implementado por toda su red para recopilar registros con el fin de proporcionar las cinco capacidades de seguridad esenciales que necesita para una visibilidad completa.
- **Servidor USM:** agrega y correlaciona información reunida por los sensores, y proporciona gestión, generación de informes y administración desde un único panel.
- **Registrador USM:** archiva de forma segura los datos sin modificar de registro de eventos para investigaciones forenses y mandatos de cumplimiento de normativas.
- **USM Todo en uno:** combina los componentes del Servidor, el Sensor y el Registrador en un único sistema.



Opciones de implementación que se adaptan a las características únicas de su red

Todos los productos USM AlienVault están disponibles en varios modelos, según los requisitos de tamaño, escala y configuración. Para poner las cosas más fáciles, independientemente de la opción de implementación que elija, todos los componentes de AlienVault funcionan de la misma manera y son completamente interoperables con todos los demás modelos, minimizando así los costes de formación. Por ejemplo: puede implementar un Servidor USM AlienVault como dispositivo de hardware, los Sensores como dispositivos virtuales y un Registrador como dispositivo de hardware, si eso es lo que necesita su empresa. Lo importante es que, independientemente de dónde estén sus activos y del aspecto de su red, obtiene una completa visibilidad de la seguridad, y todo ello gestionado desde un solo lugar.

Adicionalmente, puede actualizar instantáneamente cada uno de sus productos USM a medida que su entorno cambia y necesita evolucionar. Comience por algo pequeño y expanda rápidamente su implementación, sacando el máximo partido de la Gestión Unificada de Seguridad (USM) desde el primer día.

Escalabilidad inmediata. Sin actualizaciones a gran escala.

Nuestros productos USM Todo en uno combinan nuestro Sensor, nuestro Registrador y nuestro Servidor. Podrá ampliar rápidamente estas instalaciones para convertirlas en productos USM Standard o en USM Enterprise, en los que estas funciones las realizan sistemas especializados.

La siguiente información sobre implementación y configuración le ayudará a encontrar el producto USM adecuado para usted.

OPCIONES DE IMPLEMENTACIÓN	DISPOSITIVO DE HARDWARE	DISPOSITIVO VIRTUAL
USM Todo en uno[1]	●	●
USM Standard[2]	●	●
USM Enterprise[2]	●	

[1] Los dispositivos USM Todo en uno de AlienVault combinan los componentes del Servidor, el Sensor y el Registrador en un único sistema.

[2] Las líneas de productos USM Standard y USM Enterprise de AlienVault ofrecen escalabilidad y rendimiento aumentados al proporcionar sistemas exclusivos para cada componente (Servidor, Sensor y Registrador).

	USM TODO EN UNO USM					USM STANDARD			USM ENTERPRISE		
	AIO 25A	AIO 75A	AIO 150A	AIO UA[1]	Sensor Remoto[2]	Servidor	Registrador	Sensor	Servidor[3]	Registrador	Sensor[4]
Rendimiento del dispositivo											
Activos máx.	25	50	75	—	—	—			—		
Eventos máx. en base de datos (millones)	200					200	—	—	200	—	—
Recopilación máx. de datos (EPS)	1.000			1.000	500	200	15.000	2.500	200	15.000	—
Correlación máx. de datos (EPS)	1.000			1.000	—	5.000	—	—	10.000	—	—
Flujo de IDS (Mbps)	100			100	100	—	—	1.000	—	—	5.000
Especificaciones de hardware											
Factor de forma	1U					1U			2 x 1U	1U	
Largo x ancho x alto (in)	26,6 x 17,2 x 1,7				11,3 x 17,2 x 1,7	26,6 x 17,2 x 1,7			26,6 x 17,2 x 1,7		
Peso (lb)	42				11	42			42		
Fuente de alimentación	2 x 700 / 750W				1 x 700/750W	2 x 700 / 750W			2 x 700 / 750W		
Interfaces de red	6 x 1GbE				2 x 1GbE	2 x 1GbE		6 x 1 GbE 2 x 10 GbE (opción)	2 x 1GbE		6 x 1 GbE 2 x 10 GbE (opción)
CPU	2 x Intel Xeon E5620 2,4 GHz 8 núcleos				1x Intel Xeon E3-1220 3,1 MHz 4 núcleos	2 x Intel Xeon E5620 2,4 GHz 8 núcleos	1 x Intel Xeon E5620 2,4 GHz 4 núcleos		2 x Intel Xeon E5620 2,4 GHz 8 núcleos	1 x Intel Xeon E5620 2,4 GHz 4 núcleos	
Capacidad de almacenamiento (TB) comprimido[5] / sin comprimir	9,0 /1,8				5,0 / 1,0	6,0 / 1,2	9,0 / 1,8	6,0 /1,2	6,0 / 1,2	11,0 / 2,2	6,0 / 1,2
Configuración de la matriz de discos	RAID 10				No	RAID 10			RAID 10		
Memoria (GB)	24				8	24			24	48	24
Fuente de alimentación redundante	Sí				No	Sí			Sí		
Interfaz IPMI	Sí					Sí			Sí		
Disipación máx. de calor (BTU/hora)	439,55				27,30	846,18	815,47	667,05 (opción 6x1) 684,11 (opción 2x10)	846,18	819,93	667,05 (opción 6x1) 684,11 (opción 2x10)
Consumo máx. de energía (kVA)	0,1288				0,1052	0,2480	0,2390	0,1955 (opción 6x1) 0,2005 (opción 2x10)	0,2480	0,2110	0,1955 (opción 6x1) 0,2005 (opción 2x10)

[1] Si desactiva el Sensor del dispositivo AIO UA, puede seguir recopilando hasta 2500 EPS desde sensores remotos.

[2] El dispositivo Sensor Remoto se envía con patas para implementaciones de sobremesa. No se requiere montaje en bastidor.

[3] El Servidor Enterprise se envía con dispositivos 2 x 1U. Un dispositivo es el Servidor Enterprise y otro es el Enterprise DB

[4] El Servidor Enterprise únicamente proporciona capacidades IDS. No incluye capacidades de recopilación de datos

[5] El valor medio del coeficiente de compresión experimentado por nuestros clientes es de 5:1. La compresión real puede ser mayor o menor, dependiendo del tipo de datos que se registren.

	USM TODO EN UNO						USM STANDARD		
	AIO 25A	AIO 75A	AIO 150A	AIO UA (Sensor desactivado)	AIO UA (Sensor activado)	Sensor remoto	Servidor	Registrador	Sensor
Requisitos de la máquina virtual									
Núcleos virtuales	8					4	8		
RAM (GB)	16					8	24		
Capacidad de almacenamiento[1] (TB) comprimido / sin comprimir	5,0 / 1,0						6,0 / 1,2	9,0 / 1,8	6,0 / 1,2
Soporte Vmware ESXi	ESXi 4.0+						ESXi 4.0+		

[1]El valor medio del coeficiente de compresión experimentado por nuestros clientes es de 5:1. La compresión real puede ser mayor o menor, dependiendo del tipo de datos que se registren

Pruébelo hoy. Gratis durante treinta días.

¿Preparado para comprobar cómo la Gestión Unificada de la Seguridad (USM) de AlienVault puede ayudarle a reducir riesgos, pasar auditorías y potenciar su programa de respuesta a incidentes? Pruebe hoy en su entorno uno de nuestros productos USM, gratis los primeros 30 días. Y lo que es más, puede comenzar con USM de AlienVault por un precio inicial de solo 3.900 USD. Visite este sitio web para obtener más información: **www.alienvault.com/free-trial**

Sobre AlienVault

En AlienVault creemos que el mejor modo que tienen todas las empresas de obtener la visibilidad de la seguridad que necesitan es el modo abierto y colaborativo. Desarrollado en base a controles de seguridad probados y los últimos conocimientos sobre amenazas, la plataforma Gestión Unificada de la Seguridad (USM) de AlienVault ofrece un modo completo, sencillo y asequible para que las organizaciones con presupuesto y plantilla de seguridad limitados aborden el cumplimiento de normativas y la gestión de amenazas. Con las capacidades esenciales de seguridad ya integradas, USM pone la visibilidad de seguridad de calidad empresarial al alcance de los equipos de seguridad que necesitan conseguir más con menos. Para más información o para descargar una prueba gratis durante 30 días, visite **www.alienvault.com**

CONTÁCTENOS PARA SABER MÁS

WWW.ALIENVAULT.COM