AlienVault Unified Security Management

AlienVault's Unified Security Management™ (USM™) platform accelerates and simplifies threat detection, incident response and compliance management for IT teams with limited resources, on day one. With essential security controls and integrated threat intelligence built-in, AlienVault USM puts complete security visibility of threats affecting your network and how to mitigate them within fast and easy reach.

Whether large or small, all organizations need complete visibility to:

- Detect emerging threats across your environment
- Respond quickly to incidents and conduct thorough investigations
- Measure, manage, and report on compliance (PCI, HIPAA, ISO, and more)
- Optimize your existing security investments and reduce risk

AlienVault's Unified Security Management solution delivers this complete security visibility by providing the five essential security capabilities in a unified platform, controlled by a single management console:

- **Asset Discovery** - active and passive network discovery
- **Vulnerability Assessment** – active network scanning, continuous vulnerability monitoring
- **Intrusion Detection** - network and host IDS, file integrity monitoring
- **Behavioral Monitoring** - netflow analysis, service availability monitoring
- **SIEM** - log management, event correlation, analysis, and reporting

Integrated Threat Intelligence

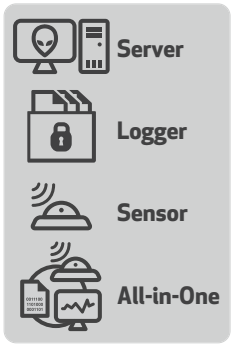
AlienVault Labs' Threat Intelligence service maximizes the effectiveness of any security monitoring program by providing regularly updated correlation directives, intrusion detection signatures, response guidance, and much more. These constant updates enable the USM platform to analyze the mountain of event data from all of your data sources, and tell you exactly what are the most important threats facing your network right now, and what to do about them. Our threat experts spend countless hours researching the latest exploits, malware strains, attack techniques, and malicious IPs, so you don't have to. They incorporate this expertise into the library of over 2,000 customizable correlation directives that ship with the USM platform, eliminating the need for you to conduct your own research and write your own correlation rules, giving you the ability to detect and respond to threats on day one.

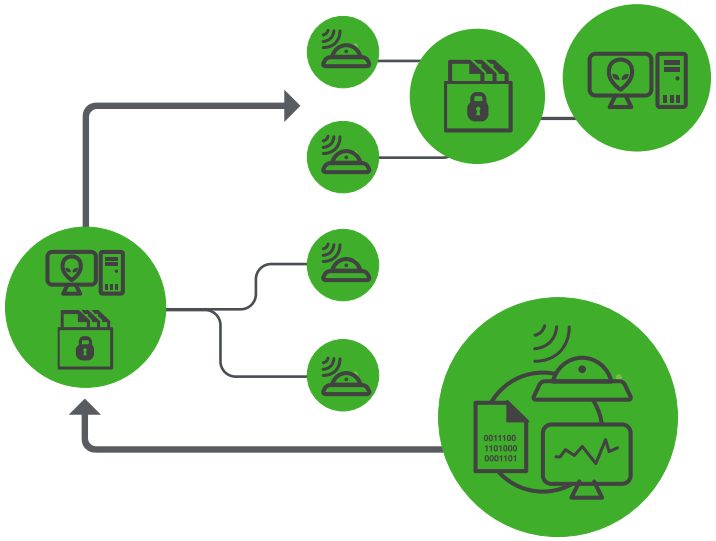
The AlienVault Labs Threat Research Team also curates the Open Threat Exchange, the world's first truly open threat intelligence community that enables collaborative defense with open access to collaborative research on emerging threats. OTX integrates with AlienVault USM and enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same.

Unified Security Management: How it Works

All AlienVault USM products include these three core components available as hardware or virtual appliances:

- **USM Sensor** - deployed throughout your network to collect logs to provide the five essential security capabilities you need for complete visibility.
- **USM Server** - aggregates and correlates information gathered by the Sensors, and provides single pane-of-glass management, reporting and administration.
- **USM Logger** – securely archives raw event log data for forensic investigations and compliance mandates.
- **USM All-in-One** - combines the Server, Sensor, and Logger components onto a single system.





Deployment Options That Fit Your Unique Network

All of the AlienVault USM products are available in various models, based on size, scale, and configuration requirements. To make things even easier, no matter what deployment option you choose, every AlienVault component works the same way and is fully interoperable with all other models, minimizing the training costs. For example, you can deploy a AlienVault USM Server as hardware appliance, Sensors as virtual appliances, and a Logger as a harware appliances if that is what your business requires. The important thing is that no matter where your assets are and what your network looks like, you have full security visibility – all managed in one place.

Additionally, you can instantly upgrade each of our USM products as your environment changes and needs evolve. Start out small and quickly expand your deployment, leveraging the power of Unified Security Management from day one.

Immediate Scalability. No Forklift Upgrades.

Our USM All-in-One products combine our Sensor, Logger, and Server. You can quickly expand these installations to become USM Standard or USM Enterprise products, where dedicated systems perform these functions.

The following deployment and configuration information will help you find the right USM product for you.

DEPLOYMENT OPTIONS	HARDWARE APPLIANCE	VIRTUAL APPLIANCE
USM All-in-One[1]	●	●
USM Standard[2]	●	●
USM Enterprise[2]	●	

[1] AlienVault USM All-in-One appliances combine the Server, Sensor, and Logger components onto a single system.

[2] The AlienVault USM Standard and USM Enterprise product lines offer increased scalability and performance by provisioning dedicated systems foreach component (Server, Sensor, and Logger).

	USM ALL-IN-ONE					USM STANDARD			USM ENTERPRISE		
	AIO 25A	AIO 75A	AIO 150A	AIO UA[1]	Remote Sensor[2]	Server	Logger	Sensor	Server[3]	Logger	Sensor[4]
Device Performance											
Max Assets	25	50	75	—	—	—			—		
Max Events in Database (Millions)	200					200	—	—	200	—	—
Max Data Collection (EPS)	1,000			1,000	500	200	15,000	2,500	200	15,000	—
Max Data Correlation (EPS)	1,000			1,000	—	5,000	—	—	10,000	—	—
IDS Throughput (Mbps)	100			100	100	—	—	1,000	—	—	5,000
Hardware Specifications											
Form Factor	1U					1U			2 x 1U	1U	
Length x Width x Height (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		
Weight (lb)	42				11	42			42		
Power Supply	2 x 700 / 750W				1 x 700/750W	2 x 700 / 750W			2 x 700 / 750W		
Network Interfaces	6 x 1GbE				2 x 1GbE	2 x 1GbE		6 x 1GbE 2 x 10GbE (option)	2 x 1GbE		6 x 1GbE 2 x 10GbE (option)
CPU	2 x Intel Xeon E5620 2.4GHz 8 Cores				1x Intel Xeon E3-1220, 3.1 MHz 4 Cores	2 x Intel Xeon E5620 2.4GHz 8 Cores	1 x Intel Xeon E5620 2.4 GHz 4 Cores		2 x Intel Xeon E5620 2.4GHz 8 Cores	1 x Intel Xeon E5620 2.4 GHz 4 Cores	
Storage Capacity (TB) Compressed[5] / Uncompressed	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
Disk Array Configuration	RAID 10				No	RAID 10			RAID 10		
Memory (GB)	24				8	24			24	48	24
Redundant Power Supply	Yes				No	Yes			Yes		
IPMI Interface	Yes					Yes			Yes		
Max Heat Dissipation (BTU/hr)	439.55				27.30	846.18	815.47	667.05 (6x1 option) 684.11 (2x10 option)	846.18	819.93	667.05 (6x1 option) 684.11 (2x10 option)
Max Power Consumption (kVA)	0.1288				0.1052	0.2480	0.2390	0.1955 (6x1 option) 0.2005 (2x10 option)	0.2480	0.2110	0.1955 (6x1 option) 0.2005 (2x10 option)

[1] If you disable the Sensor on the AIO UA appliance, you can still collect up to 2500 EPS from remote sensors.
[2] Remote Sensor device ships with feet for desktop deployment. Rack mount not required.
[3] Enterprise Server ships with 2 x 1U devices. One device is the Enterprise Server and one is the Enterprise DB
[4] Enterprise Sensor provides IDS capabilities only. It does not include data collection capabilities
[5] 5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.

	USM ALL-IN-ONE						USM STANDARD		
	AIO 25A	AIO 75A	AIO 150A	AIO UA (Sensor Disabled)	AIO UA (Sensor Enabled)	Remote Sensor	Server	Logger	Sensor
Virtual Machine Requirements									
Virtual Cores	8					4	8		
RAM (GB)	16					8	24		
Storage Capacity[1] (TB) Compressed / Uncompressed	5.0 / 1.0						6.0 / 1.2	9.0 / 1.8	6.0 / 1.2
Vmware ESXi Support	ESXi 4.0+						ESXi 4.0+		

[1]5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.

Try it today. Free for thirty days.

Ready to see how AlienVault's Unified Security Management can help you reduce risks, pass audits, and enhance your incident response program? Try one of our USM products in your environment today for free – for the first 30 days. What's more, you can get started with AlienVault USM at a starting price of only $3,900. Please visit this site to find out more information: **www.alienvault.com/free-trial**

About AlienVault

At AlienVault, we believe that open and collaborative is the best way for all companies to gain the security visibility they need. Built on proven security controls and the latest threat intelligence, AlienVault's Unified Security Management (USM) platform provides a complete, simple and affordable way for organizations with limited security staff and budget to address compliance and threat management. With the essential security capabilities already built-in, USM puts enterprise-class security visibility within easy reach of security teams who need to do more with less. For more information or to download a Free 30-day trial visit: **www.alienvault.com**

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM