AlienVault® USM Appliance™

## Powerful Threat Detection & Response for On-Premises Environments

AlienVault® USM Appliance™ accelerates and simplifies threat detection, incident response and compliance management for IT teams with limited resources, starting on Day One. With essential security controls and integrated threat intelligence built-in, AlienVault USM Appliance 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 their environments
- Respond quickly to incidents and conduct thorough investigations
- Measure, manage, and report on compliance (PCI, HIPAA, ISO, and more)
- Optimize existing security investments and reduce risk

USM Appliance 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
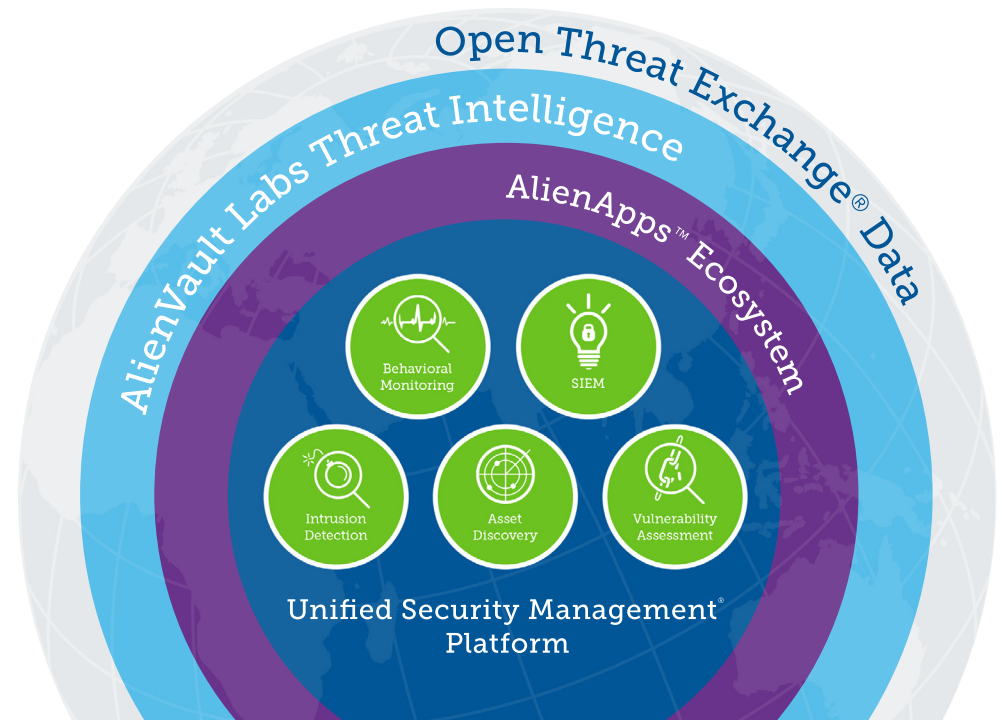

Integrated Threat Intelligence

AlienVault's Threat Intelligence subscription 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. We incorporate this expertise into our extensive and growing library of 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 Security Research Team also curates the Open Threat Exchange® (OTX™), 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 USM Appliance and enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same.

AlienVault USM Appliance: How it Works

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

- **USM Appliance Sensor** - deployed throughout your network to collect logs to provide the five essential security capabilities you need for complete visibility.

- **USM Appliance Server** - aggregates and correlates information gathered by the Sensors, and provides single pane-of-glass management, reporting and administration.

- **USM Appliance Logger** – securely archives raw event log data for forensic investigations and compliance mandates.

- **USM Appliance All-in-One** - combines the Server, Sensor, and Logger components onto a single system.
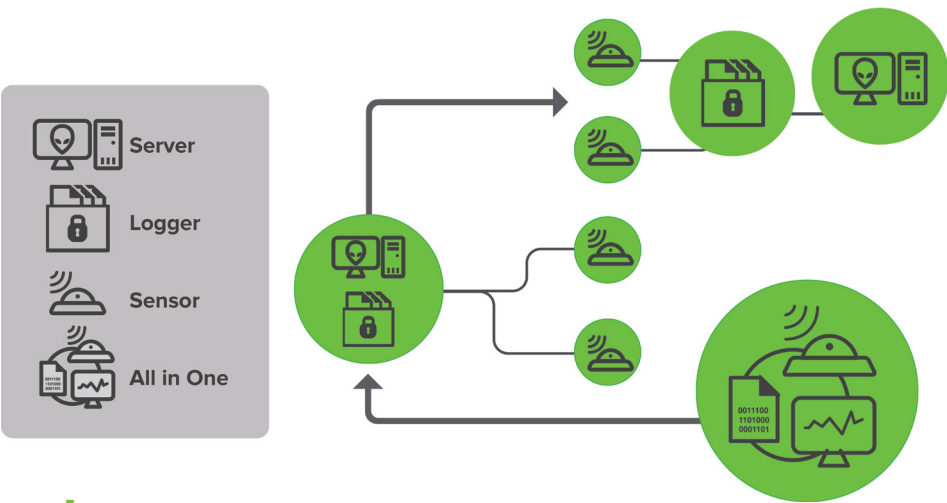
Deployment Options That Fit Your Unique Network

All of the AlienVault USM Appliance 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 USM Appliance component works the same way and is fully interoperable with all other models, minimizing the training costs. For example, you can deploy an AlienVault USM Appliance Server as a hardware appliance, USM Appliance Sensors as virtual appliances, and a USM Appliance Logger as a hardware appliance, 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 Appliance products as your environment changes and your needs evolve. Start out small and quickly expand your deployment, leveraging the power of USM Appliance from Day One.

Immediate Scalability. No Forklift Upgrades.

Our USM Appliance All-in-One products combine our Sensor, Logger, and Server. You can quickly expand these installations to become USM Appliance Standard or USM Appliance Enterprise products, where dedicated systems perform these functions. Additionally, USM Central™, a federation console is available to provide a centralized view of your data in a distributed environment.

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

DEPLOYMENT OPTIONS	HARDWARE APPLIANCE	VIRTUAL APPLIANCE	CLOUD SERVICE
USM Appliance All-in-One[1]	👽	👽	
USM Appliance Standard[2]	👽	👽	
USM Appliance Enterprise[2]	👽		
USM Central[3]			👽

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

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

[3] AlienVault USM Central provides a centralized view of your data in a distributed environment, including USM Appliance and USM Anywhere instances. Requires USM Appliance 5.4.3 or later.

	USM APPLIANCE ALL-IN-ONE					USM APPLIANCE STANDARD			USM APPLIANCE ENTERPRISE			USM CENTRAL[8]
	AIO 25A	AIO 75A	AIO 150A	AIO UA[3]	Remote Sensor[4]	Server	Logger	Sensor	Server[5]	Logger	Sensor[6]	AlienVault-hosted Cloud Service
Device Performance												
Max Assets	25	75	150	—	—	—			—			—
Max Events in Database (Millions)[1]	200					200	—	—	200	—	—	—
Max Data Collection (EPS)[1]	1,000			1,000	500	—	15,000	2,500	—	15,000	—	—
Max Data Correlation (EPS)[1]	1,000			1,000	—	5,000	—	—	10,000	—	—	—
IDS Throughput (Mbps)[1]	100			100	100	—	—	1,000	—	—	5,000	—
Max Connections to AIO's / Servers[2]	—			—	—	—	—	—	—	—	—	—
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[7] / 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)	2,794.54				665.36	2,794.54			2,794.54			—
Max Power Consumption (kVA)	0.837				0.350	0.837			0.837			—

[1] Device performance may vary depending on environment, configuration, etc.

[2] Assumes average usage of AIO's with default settings. Max connections may vary depending on alarms, events, etc.

[3] If you disable certain Sensor collection functions on the AIO appliance, you can collect up to 2,500 EPS from connected Sensors.

[4] Remote Sensor device ships with feet for desktop deployment. Rack mount not required.

[5] Enterprise Server ships with 2 x 1U devices. One device is the Enterprise Server and one is the Enterprise DB.

[6] Enterprise Sensor provides IDS capabilities only. It does not include data collection capabilities.

[7] 5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.

[8] USM Central supports federation for USM Anywhere and USM Appliance 5.4.3 or later

	USM APPLIANCE ALL-IN-ONE					USM APPLIANCE STANDARD			USM CENTRAL
	AIO 25A	AIO 75A	AIO 150A	AIO UA	Remote Sensor	Server	Logger	Sensor	AlienVault-hosted Cloud Service
Virtual Machine Requirements									
Total Cores	8				4	8			—
RAM (GB)	16				8	24			—
Storage Capacity[1] (TB) Compressed / Uncompressed	5.0 / 1.0 or 2.5 / 0.5[2]				5.0 / 1.0 or 1.25 / 0.25[3]	6.0 / 1.2	9.0 / 1.8	6.0 / 1.2	—
Virtual Interfaces	6 x 1GbE				2 x 1GbE	2 x 1GbE	2 x 1GbE	6 x 1GbE	—
Virtualization Support	VMware ESXi 4.0+ Hyper-V v3.0+ (Windows Server 2008 SP2 and later)					VMware ESXi 4.0+ Hyper-V v3.0+ (Windows Server 2008 SP2 and later)			—

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

[2] All-In-One virtual appliances available in two storage capacities: 1TB or 500GB.

[3] Remote Sensor virtual appliances available in two storage capacities: 1TB or 250GB.

Try it today. Free for thirty days.

Ready to see how AlienVault USM Appliance can help you reduce risks, pass audits, and enhance your incident response program? Try one of our USM Appliance products in your environment today for free – for the first 30 days. What's more, you can get started with AlienVault USM Appliance at a starting price of only $5,595. Please visit this site to find out more information: **www.alienvault.com/products/usm-appliance/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 crowdsourced 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. For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM