AlienVault USM Appliance

Powerful threat detection and response for on-premises environments

AlienVault® USM Appliance™ from AT&T Cybersecurity accelerates and simplifies threat detection, incident response, and compliance management for IT teams with limited resources, as early as day one.

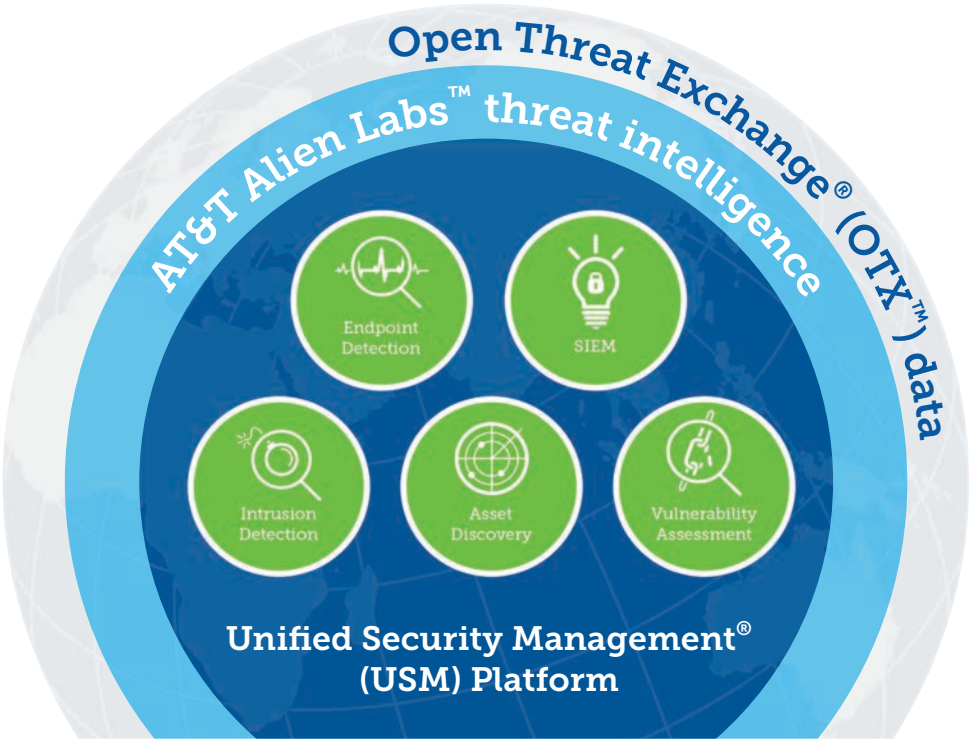
With essential security controls and integrated threat intelligence built-in, AlienVault USM Appliance™ provides complete visibility of security threats affecting your network and shows you how to mitigate them. It delivers this visibility by providing 5 essential security capabilities in a unified platform, controlled by a single management console: asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, and security information and event management (SIEM).

Potential benefits:

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

Product features:

- 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
- Security information and event management (SIEM)—log management, event correlation, analysis, and reporting



Integrated threat intelligence

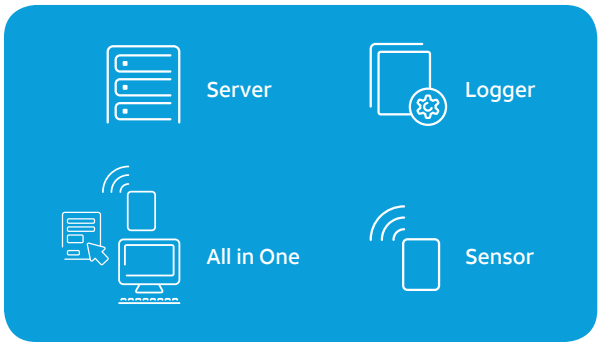
The AT&T Alien Labs™ threat intelligence subscription maximizes the effectiveness of any security monitoring program by providing regularly updated correlation directives, intrusion detection signatures, response guidance, and much more. These constant updates enable the USM platform to analyze the mountains 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.

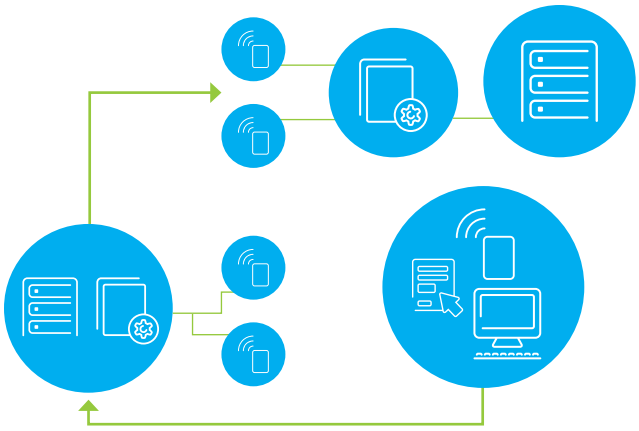
The Alien Labs security research team also curates the Open Threat Exchange® (OTX™), an open threat intelligence community that enables collaborative defense with open access to collaborative research on emerging threats. OTX integrates with USM Appliance and enables everyone in the OTX community to 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 3 core components available as hardware or virtual appliances:

- USM Appliance Sensor—deployed throughout your network to collect logs to provide 5 essential security capabilities you need for complete visibility
- SM Appliance Server—aggregates and correlates information gathered by the Sensors, and provides single pane-of-glass management, reporting and administration
- USM Appliance Logger—highly secure archiving of 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 quickly upgrade each of our USM Appliance products as your environment changes and your needs evolve. Start out small and quickly expand your deployment, utilizing 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 Sever, 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
	AIO 25A	AIO 75A	AIO 150A	AIO UA	Remote Sensor [3]	Server	Logger	Sensor	Server [4]	Logger	Sensor [5]	AlienVault-hosted cloud sevice
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	1,000	—	15,000	—	—
Max data correlation (EPS) [1]	1,000			1,000	—	4,000	—	—	4,000	—	—	—
IDS throughout (Mbps) [1]	100			100	100	—	—	1,000	—	—	5,000	—
Max connections to AIO's/ servers [2]	—			—	—	—	—	—	—	—	—	—
Hardware Specifications												
Form factor	1U					1U						—
Length x width x height (In)	23.9 x 17.11 x 1.69			15.05 x 17.11 x 1.69		23.9 x 17.11 x 1.69			23.9 x 17.11 x 1.69			—
Weight (lb)	37.44 (max)			19.14 (max)		37.44 (max)			37.44 (max)			—
Power supply	2 x 800W			1 x 290W		2 x 800W			2 x 800W			—
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	1 x Intel Xeon E5-2630 v4 2.2GHz 10 Cores			1 x Intel Xeon E3-1220 v5 3.0GHz 4 Cores		1 x Intel Xeon E5-2630 v4 2.2GHz 10 Cores		1x Intel Xeon E5-2620 v4 2.1GHz 8 Cores	1 x Intel Xeon E5-2630 v4 2.2GHz 10 Cores			—
Storage capacity (TB) compressed [6]/ 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)	32			8		32			32			—
Redundant power supply	Yes			No		Yes			Yes			—
iLO Dedicated interface / shared interface	No/Yes					No/Yes			No/Yes			—
Max heat dissipation (BTU/hr)	691.45			400.57		733.65	691.45	733.65	733.65	837.71	733.65	—
Max power consumption (W)	202.77			117.47		215.15	202.77	215.15	215.15	245.66	215.15	—

[1] Device performance may vary depending on environment and configuration. EPS numbers assume events are being parsed across at least 4 plug-ins.
[2] Assumes average usage of AIO's with default settings. Max connections may vary depending on alarms, events, etc.
[3] Remote Sensor device ships with feet for desktop deployment. Rack mount not required.
[4] Enterprise Server ships with 2 x 1U devices. One device is the Enterprise Server and one is the Enterprise DB.
[5] Enterprise Sensor provides IDS capabilities only. It does not include data collection capabilities.
[6] 5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.
[7] USM Central supports federation for USM Anywhere and USM Appliance 5.4.3 or later.

Try it today. Free for 30 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.

Please visit this site to find out more information:
www.alienvault.com/products/usm-appliance/free-trial

About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning—helping to enable our customers around the globe to anticipate and act on threats to protect their business.