AlienVault® USM Appliance Sensor

What's happening, and where? What is the impact on your critical applications and data? What are the greatest risks to your network right now?

The USM Appliance Sensor is the front-line security module of the USM Appliance™ platform and provides detailed visibility into the assets on your network, what software and services are installed on them, how they're configured, and any potential vulnerabilities and active threats being executed against them. The USM Appliance Sensor combines Asset Discovery, Vulnerability Assessment, Intrusion Detection, and Behavioral Monitoring capabilities into a single device. You can deploy the Sensor as a stand-alone device or as part of an integrated USM All-in-One appliance, and you can deploy it as a physical appliance or virtual appliance.

The AlienVault USM Appliance platform accelerates and simplifies your ability to detect and respond to threats, on day one. It provides five essential security capabilities to maximize your security visibility and compliance management: Asset Discovery, Vulnerability Assessment, Intrusion Detection, Behavioral Monitoring and SIEM. The AlienVault Labs Security Research Team keeps these capabilities up to date against the latest threats with continuously updated Threat Intelligence.

The USM Appliance Sensor delivers these essential capabilities:

Asset Discovery — Automatically inventories critical assets

Automatic asset discovery means you won't overlook systems and data in your network, even in today's fast changing environments. Active and passive network scanning techniques create an inventory of deployed assets, an essential first step to successfully implementing a comprehensive security program. With a comprehensive network map, you can then assess vulnerabilities, detect threats, and monitor network and services for unusual behavior.

Vulnerability Assessment — Detects which assets are vulnerable to attack

Complexity and cost can put critical technologies like vulnerability assessment out of reach for many IT teams with limited resources. Vulnerability assessment identifies vulnerable systems and software, which helps you prioritize your remediation actions and improve your security posture. By combining asset discovery with vulnerability assessment, the USM Appliance platform puts essential network visibility and security awareness within reach of any size IT team.

Intrusion Detection — Identifies targeted hosts and active threats

The USM Appliance Sensor's network intrusion detection system (NIDS) capabilities analyze network traffic to detect attacks. The USM Appliance platform detects attacks targeting your network and vulnerable devices automatically. It utilizes the comprehensive understanding of system vulnerabilities created from the automated Vulnerability Assessment and the intrusion detection data to alert you to malicious traffic on your network.

Behavioral Monitoring — Identifies changes in normal operating conditions

Changes in the behavior of your network, systems, and services can indicate an attack in progress or a compromised system. The USM Appliance Sensor combines network flow analysis (NetFlow) to see changes in network traffic, packet capture for forensic analysis, active service monitoring to proactively verify changes to services, and log collection to detect anomalies reported by other elements of the infrastructure.

Seamless Security Lifecycle Management

Securing your infrastructure is a process, not an event. We built the USM Appliance Sensor to reduce the cost and complexity of implementing a comprehensive lifecycle-based security solution. AlienVault's flexible USM Appliance architecture enables you to deploy your sensors centrally with other USM Appliance elements, or distributed to strategic points in your network. Regardless of the deployment model you choose, USM Appliance maintains a seamless lifecycle-based workflow. It delivers all the power and flexibility without the cost and complexity of point solutions—the best of both worlds.

FEATURE	BENEFIT
ASSET DISCOVERY	
Passive Network Monitoring	Observes network traffic non-intrusively to identify hosts and installed software.
Active Network Scanning	Finds systems by actively polling the network, discovering hosts, and enumerating services on those hosts.
Network Discovery	Automatically discovers and maps the network topology to identify unknown devices.
VULNERABILITY ASSESSMENT	
Authenticated Scanning	Provides the most accurate method for detecting vulnerabilities by directly accessing a host's file system and inspecting installed software.
Unauthenticated Scanning	Extends scanning benefits to hosts when authentication is not possible.
INTRUSION DETECTION	
Network-based Intrusion Detection (NIDS)	Immediate visibility into the attacks against your systems.
Host-based Intrusion Decection (HIDS) and File Integrity Monitoring (FIM)	Monitors a host's internal systems to provide attack visibility and enforce security policies.
BEHAVIORAL MONITORING	
Network Flow (NetFlow) Analysis	Delivers valuable insight into bandwidth usage and applications running on your network.
Packet Capture	Capture packet data to evaluate specific traffic for detailed threat analysis.
Active Service Monitoring	Ensure that only the services you want are actively running and there are no service disruptions or unwanted services running.
Log Collection	Aggregation of remote infrastructure logs and 3rd party tools to accelerate and simplify threat detection and remediation.

THE Simple SOLUTION