The AlienVault 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?

AlienVault's Sensor combines Asset Discovery, Vulnerability Assessment, Threat Detection, and Behavioral Monitoring to provide full situational awareness. The Sensor is the front-line security module of the Unified Security Management (USM™) platform and provides detailed visibility into your deployed assets, vulnerabilities, attack targets and vectors, and services. You can deploy it as a stand-alone sensor or integrated in an All-in-One appliance, as a physical or virtual appliance, or Amazon AWS AMI.

AlienVault USM enables you to more easily and efficiently configure, manage, and control the essential security capabilities that no company should be without. By unifying the five capabilities within the single USM platform, AlienVault simplifies your management and reduces complexity, allowing you to spend more time securing your network and less time learning, deploying, and configuring tools.

Asset Discovery — Automatically inventories critical assets

You don't know what you don't know. Automatic asset discovery means you won't overlook systems and data, even in today's fast changing environments. Actively surveying the network to create an inventory of deployed assets is the first step to gaining situational awareness and deploying a comprehensive security program. Asset discovery creates the foundational understanding of your environment, ensuring full coverage for assessing vulnerabilities, detecting threats, and monitoring network and service behavior for deviations from the norm.

Vulnerability Assessment — Detects which assets are vulnerable to attack

Complexity and cost can put critical proactive measures like vulnerability assessment out of reach for many organizations with limited resources. By combining complete system visibility with vulnerability assessment tools, AlienVault has put essential security awareness within reach of any size IT team. Vulnerability assessment catalogs potential system weaknesses to help you prioritize your remediation actions to improve your security posture.

Threat Detection — Identifies targeted hosts and exploits used in attack

Utilizing the comprehensive understanding of system vulnerabilities created from automated Vulnerability Assessment, the AlienVault Sensor actively monitors for attacks targeting your vulnerable systems. The Sensor's network intrusion detection system (IDS) analyzes network traffic to detect known attacks, and identify patterns of attack methods. This provides immediate visibility into the attacks being used against your system.

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 Sensor combines network flow analysis (to see changes in network traffic), full packet capture (for forensic analysis), active service monitoring (to proactively verify changes to services), and log collection (to leverage anomalies reported by other elements of the infrastructure).

Seamless Security Lifecycle Management

Securing your infrastructure is a process, not an event. We built the AlienVault Sensor to reduce the cost and complexity of implementing a comprehensive lifecycle-based security solution. AlienVault's flexible USM architecture enables you to deploy you sensor centrally with other USM elements, or distributed to strategic points in your network. Regardless of the deployment model you choose, USM 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 packages.
	Active Network Scanning	Finds systems that are not currently active by polling the network, discovering hosts, and enumerating the running services.
	Host-based Inventory	Maintains a detailed inventory of hardware and software configurations.
	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.
THREAT DETECTION	Network Intrusion Detection	Immediate visibility into the attacks against your systems.
	Host-based IDS and File Integrity	Monitors a host's internal systems to provide attack visibility and enforce security policies.
BEHAVIORAL MONITORING	Network Flow Analysis	Delivers valuable insight into bandwidth usage and applications running on your network.
	Packet Capture	Capture full 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.

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM