The AlienVault Server

Security Automation, Unified Management, and Shared Intelligence simplify and accelerate your ability to detect and respond to threats

AlienVault's Server, the cornerstone of the Unified Security Management (USM™) Platform combines Security Automation, Unified Management, and Threat Intelligence to correlate data, spot anomalies, reduce risk, and improve your operational efficiency.

AlienVault USM enables you to quickly and effectively configure, manage, and control the five essential security capabilities that no company should be without: Asset Discovery, Vulnerability Assessment, Threat Detection, Behavioral Monitoring, and Security Intelligence/SIEM. By unifying these 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.

Security Automation — Accelerates your threat response

AlienVault offers superior security automation to give you the information you need to react appropriately to events in your network. In addition to providing the standard SIEM event correlation you expect (collection, normalization, and correlation), USM leverages the asset, vulnerability, and threat information it's collected. This offers a more comprehensive accurate assessment of security incidents. Moreover, the two-way data flow between event correlation and the integrated USM security controls provides dynamic event validation to automate the initial steps of incident response. AlienVault's comprehensive security automation produces highly accurate, actionable alerts allowing analysts to spend their vaulable time responding to the highest priority threats facing your network right now.

Unified Management — Reduces cost and complexity of securing your network

Unified management reduces complexity and simplifies operation of the USM platform. This allows you to spend more time monitoring your network, not managing separate security tools. By designing the USM platform as a unified solution, AlienVault enables you to do everything from a single console: Identify an attack, isolate the breach, ascertain its success, and determine the extent of the compromise. A unified reporting framework with easy-to-use wizards and customizable report templates accelerates your regulatory compliance.

Shared Intelligence — Enables a collaborative and improved defense

AlienVault's Open Threat Exchange™ (OTX™) is the world's largest repository of threat intelligence. OTX receives threat data from more than 140 countries and enables anonymous sharing of threat intelligence to anyone who wants to participate. The AlienVault Labs aggregates and validates the threat intelligence, and distributes it to all OTX participants. This collaborative defense model offers AlienVault users a significantly improved level of security over standalone alternatives.

Security Intelligence in Action

Imagine a single management console that can deliver the following functions seamlessly:

Your firewall detects a port scan, with the source address of the scan correlated with the destination address of an SSH session from an internal host. A lookup in an asset database automatically identifies the risk profile of the internal host -- the host is critical to business operations, creating a critical security incident. Your integrated vulnerability assessment tools then scan the compromised host for other vulnerabilities, discovering a missing critical security patch. Your management console creates a ticket in a third-party patch management system, which patches the compromised host and returns it to service. A complete forensic analysis of the compromised host for the past 30 days determines that no additional corrective action is required. The incident is automatically reported to AlienVault Open Threat Exchange (OTX) so that everyone who receives threat intelligence updates from OTX can protected themselves from a similar exploit.

You can have this functionality today with AlienVault's Unified Security Management platform.

	FEATURE	BENEFIT
UNIFIED MANAGEMENT	Unified Management of Security Tools	Reduced cost of ownership through central monitoring and configuration for Sensors and Loggers.
	Federated Management	Roll-based management allows separation of duties mandated by IT organizational requirements and/or regulatory bodies.
	Over 100 Pre-Defined Compliance & Threat Reports	Easily generate reports for incidents, alarms, vulnerabilities, trouble tickets, assets, service availability, and network health.
	Over 2500 Report Modules	Reduced time spent on creating custom reports by reusing modules of existing reports.
	Wizard-Driven Custom Reporting	Rapidly fulfill an organization's unique compliance and operational reporting requirements.
	Configurable & Extensible Dashboards	Creates custom views of threat, compliance, and operational data for each user.
	3D Visualization Support	View 3D network and security applications like Geo-location and botnet maps.
SECURITY AUTOMATION	Real Time Correlation	Improves productivity of security operations by converting raw events into actionable alerts.
	Over 1,800 Pre-Defined Correlation Rules	Ensures maximum effectiveness of integrated security controls.
	Wizard to Create Custom Correlation Rules	Easily create correlation rules to meet the specific security and compliance requirements of your organization.
	Contextual Behavior Analysis	Assess the risk of the anomalous activity by correlating it to environmental information like importance of the asset.
	Pattern Recognition & Behavior Analysis	Accelerates corrective action by correlating current threat intelligence with the security incident.
	Dynamic Event Validation	Automates initial troubleshooting by querying built-in security tools to gather more information on status of network and assets.
SHARED INTELLIGENCE	Interface with Open Threat Exchange (OTX)	The world's largest open-source repository of threat intelligence ensures that your security systems always have the latest intelligence.

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM