AlienVault® USM Appliance Server

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

AlienVault's USM Appliance Server, the cornerstone of the USM Appliance™ platform, combines security automation, unified management, and threat intelligence to correlate data, identify threats in your network, provide remediation guidance, and improve your operational efficiency.

AlienVault USM Appliance 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, Intrusion Detection, Behavioral Monitoring, and SIEM. By unifying these five capabilities within the single USM Appliance platform, AlienVault simplifies your management and reduces complexity, allowing you to spend more time securing your network and less time deploying and configuring tools, writing correlation rules, and researching threats.

Security Automation — Accelerates your threat response

The AlienVault USM Appliance Server automates critical activities to simply the threat detection process and gives you the information you need right now to respond to events in your network. The USM Appliance platform collects and correlates the asset, vulnerability, threat, and behavioral information collected from its built-in data sources to create a network-wide view of suspicious or malicious activity. The pre-configured correlation rules sift through all of the event data in your log files to identify the security incidents that matter most. The USM Appliance Server's comprehensive security automation produces highly accurate, actionable alerts allowing you to spend valuable time responding to the highest priority threats facing your network, instead of manually searching log les and researching threats.

Unified Management — Reduces cost and complexity of securing your network

Unified management reduces the complexity of trying to stay ahead of the threats facing your network. This allows you to spend more time monitoring your network instead of trying to manage separate security tools. By designing the USM Appliance 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 as well, giving the auditors the information they need.

Threat Intelligence — Eliminates the need to conduct your own research

USM Appliance's integrated Threat Intelligence from AlienVault Labs Security Research Team eliminates the need for IT teams to spend precious time conducting their own research on emerging threats or on alarms triggered by their security tools. The AlienVault Labs team regularly delivers threat intelligence as a coordinated set of updates to the USM Appliance platform, which accelerates and simplifies threat detection and incident response. The USM Appliance platform also integrates data from the Open Threat Exchange™ (OTX™), the world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data.

Threat Intelligence in Action

Imagine a single management console that can deliver the following functions seamlessly: Your firewall detects a port scan, and your IP reputation service identifies the source address of the scan as an active malicious host. Your SIEM then correlates that malicious source address as the destination address of an SSH session from an internal host. A lookup in your asset database identifies the risk profile of the internal host — the host is essential to business operations, creating a critical security incident. Your vulnerability assessment tool then scans 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 to instruct the sysadmin to patch the compromised host and return it to service. A complete forensic analysis of the compromised host for the past 30 days determines that no additional corrective action is required.

You can have this functionality today with AlienVault's USM Appliance platform, and benefit from being able to configure and manage all of these features from a single console. And because information about the source IP address and attack behavior is automatically reported to the Open Threat Exchange, everyone who receives threat intelligence updates from OTX can protected themselves from a similar exploit.

FEATURE	BENEFIT
UNIFIED MANAGEMENT	
Unified Management of Security Tools	Reduced cost of ownership through central monitoring and configuration for Sensors and Loggers.
Federated Management	Supports separation of duties mandated by organizational or regulatory requirements; supports multi-tenant environments for service providers.
Hundreds of Pre-Defined Compliance & Threat Reports	Easily generate reports for incidents, alarms, vulnerabilities, trouble tickets, assets, service availability, and network health.
Over 2,500 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.
SECURITY AUTOMATION	
Real Time Correlation	Improves productivity of security operations by converting raw events into actionable alerts.
Extensive Library of Pre-Defined Correlation Rules	Ensures maximum effectiveness of integrated security controls.
Wizard to Create Customer Correlation Rules	Easily create correlation rules to meet the specific security and compliance requirements of your organization.
Contextual Behavior Analysis	Easily create correlation rules to meet the specific security and compliance requirements of your organization.
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.

THREAT INTELLIGENCE	
AlienVault Labs Threat Intelligence	Regular threat intelligence updates to the USM platform eliminate the need for you to conduct your own research, accelerating and simplifying threat detection and response.
Integrated community-powered threat data from OTX	OTX is the world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data that provides global insight into attack trends and bad actors.