
AlienVault™
Introducing Unified Security Management Platform (USM)
EVERYTHING YOU NEED TO KNOW
ABOUT ALL THE PROTECTION YOU NEED.

ESSENTIAL SECURITY

# The AlienVault Unified Security Management Platform (USM) unifies the 5 security capabilities that no company can be without:


**The platform leverages many of your favorite security tools to create a workflow-centric solution that enables a comprehensive security management, materially reducing time to visibility/security versus a homegrown solution stitched together from individual point products.**

At AlienVault we believe that simplicity and effectiveness go hand in hand. Modern threats demand a unified defense plan and process so we've built an integrated platform using validated and effective tools so you can focus more on actually securing the network.

### Collaborative Defense

The industry's general lack of security information-sharing has long given attackers a tactical advantage—refining their exploit on one organization without tipping off other potential targets. AlienVault's Open Threat Exchange™ (AV-OTX™) is built into the USM Platform, enabling anonymous sharing of threat intelligence. USM's interface to AV-OTX™ shares and receives threat updates from installations across 49 countries. When an attack is observed by an OTX participant the information is sent to AlienVault Labs for validation and is distributed to all other OTX participants. A collaborative defense model offers an improved level of security.

ESSENTIAL SECURITY CAPABILITIES

# In today's rapidly changing threat landscape, maintaining a secure and compliant environment is full of challenges.

- **HOW DO YOU KNOW WHEN NEW SYSTEMS CONNECT TO YOUR NETWORK?**
- **ARE THERE VULNERABLE SYSTEMS ON YOUR NETWORK?**
- **WHICH PART OF YOUR NETWORK IS BEING TARGETED?**
- **HOW DO YOU MAINTAIN VISIBILITY INTO NETWORK OPERATIONS TO QUICKLY SPOT ANOMALIES?**
- **CAN YOU CORRELATE DATA FROM MULTIPLE SYSTEMS TO IDENTIFY POTENTIAL ISSUES?**
- **ARE YOU AUTOMATICALLY NOTIFIED OF THREATS OTHERS HAVE ENCOUNTERED BEFORE THEY IMPACT YOUR OPERATIONS?**

## AV-USM can help you answer YES to each of these questions.

### Focus on Security, Not the Tools

Crisis gives rise to exaggeration. So it's no surprise that given the threat environment, there is a constant flow of new tools claiming to solve security's latest "unsolved" problem. But in many ways, this is contributing to the problem, creating a growing patchwork of protection and complex technology environments. A collection of point security tools means more time spent on learning and re-learning disparate user interfaces and less time spent securing the network.

## Asset Discovery—What has changed today?

Know what you have isn't as simple as it seems. AV-USM automatically identifies and inventories all the assets in your environment. The mechanism is up to you: passive network monitoring, active scanning, or an optional host-based inventory agent. Without this first step, there's no real foundation for the rest of your security efforts.

## Vulnerability Assessment—How soft is your underbelly?

AV-USM is a ruthless and honest assessor of your systems. Which is exactly what you want. We use network-based vulnerability scanning to understand the weak links in your system, delivering high-alert situational awareness.

## Threat Detection—What is in the Cross-hairs?

AV-USM will identify which systems are being targeted and the nature of the attacks. We do that by continually analyzing your environment using network intrusion detection, wireless intrusion detection, and an optional host-based model.

## Behavioral Monitoring—The watchful eye of AlienVault

Intelligent monitoring requires an understanding of both your environment and the consistently shifting nature of the threat landscape. Identifying the smallest changes in your network can be the first indicator of malicious activity. AlienVault provides this visibility using network flow analysis, service availability monitoring, and full packet inspection.

## Security Intelligence (SIEM)—What keeps you ahead of the game?

Our unified security platform is built to correlate complex patterns of activity across your network. Powered by the latest information from AlienVault labs, AV-USM sends out targeted alerts when suspicious activity is detected. False positives are the result of unsophisticated, over-eager technology. Our alerts enable you to spend your time efficiently.

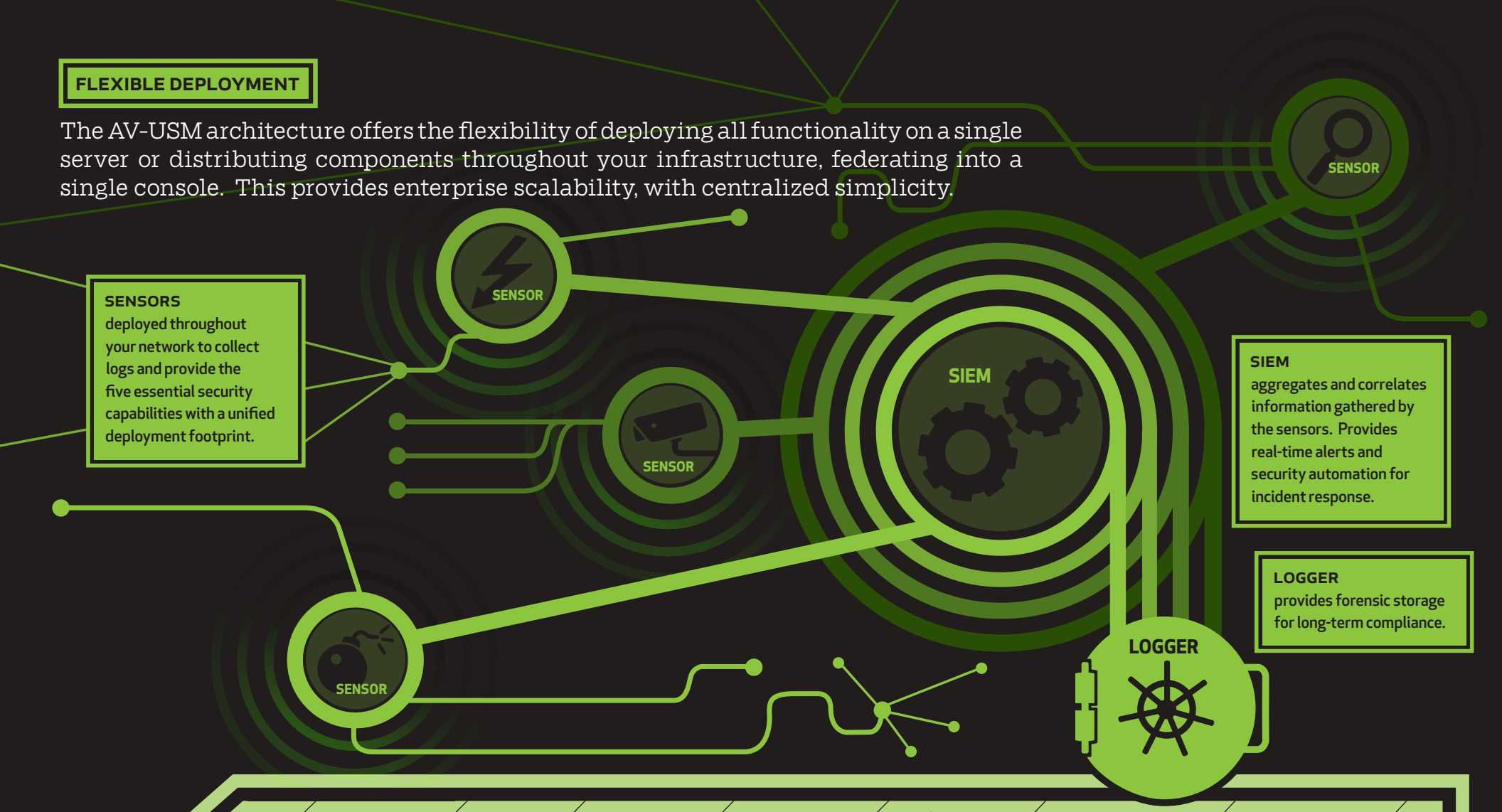
## Open Extension API—When the essential security capabilities are not enough...

AV-USM's Open Extension API improves each of the above essential security capabilities by allowing you to easily integrate other open source or commercial best of breed security and operational tools into the unified security management platform.

## FLEXIBLE DEPLOYMENT

The AV-USM architecture offers the flexibility of deploying all functionality on a single server or distributing components throughout your infrastructure, federating into a single console. This provides enterprise scalability, with centralized simplicity.

**SENSORS**
deployed throughout your network to collect logs and provide the five essential security capabilities with a unified deployment footprint.




**SIEM**
aggregates and correlates information gathered by the sensors. Provides real-time alerts and security automation for incident response.

**LOGGER**
provides forensic storage for long-term compliance.

| | **Asset Discovery**<br>Active Network Scanning<br>Passive Network Monitoring<br>Host-Based Inventory | **Vulnerability Assessment**<br>Authenticated Scanning<br>Unauthenticated Scanning | **Threat Detection**<br>Wireless Intrusion Detection<br>Network Intrusion Detection<br>Host-Based File Integrity | **Behavioral Monitoring**<br>Network Flow Analysis<br>Full Packetcapture<br>Service Availability Monitoring | **Forensic Storage**<br>Digital Signatures For Data Integrity<br>10:1 Compression<br>San/Nas Interoperability | **Security Intelligence**<br>Real-Time Correlation<br>Pattern Recognition & Contextual Behavioral Analysis<br>Security Automation<br>Dynamic Event Validation | **Unified Management**<br>Unified Management of Security Tools<br>Multi-Tenant Dashboards, Reports & Metrics | **Open Threat Exchange**<br>Collaborative Defense<br>IP Reputation Alert |
|---|---|---|---|---|---|---|---|---|
| **SENSOR** | ● | ● | ● | ● | | | | |
| **SIEM** | | | | | | ● | ● | ● |
| **LOGGER** | | | | | ● | | | |

## WHY CUSTOMERS CHOOSE ALIENVAULT

AlienVault customers range from telecom giants like **Telefonica** (the 3rd largest telco in the world), municipalities like the **City of Los Angeles,** schools like **Marquette University,** hospitality companies like **Xanterra Parks & Resorts,** infrastructure management companies like **Metro de Madrid** (the 6th longest Rail system in the world), and many banks across the United States, Europe, and Latin America.

### THREAT PROTECTION

"We selected AlienVault after a detailed study of different companies. AlienVault is a comprehensive solution, not just a simple tool. This gives us important and fundamental benefits, as classified military systems are subject to strong national and NATO regulations and must meet very strict security requirements."

Colonel Jesus M. Gonzalez Perez, Army Head of Cyber Defence,
**MINISTRY OF DEFENCE, SPAIN**

### COMPLIANCE AUTOMATION

"AlienVault USM secures infrastructure, ensures PCI compliance…
"AlienVault's built in Vulnerability Assessment and IDS saves the city money that would otherwise be spent on additional products."

Brian Caoz, System Programmer,
**CITY OF LOS ANGELES**

### OPERATIONAL EFFICIENCY

"AlienVault has been an indispensable tool in Marquette's move from reactionary to a proactive security posture; security is so much about visibility – you can only cursorily protect what you can't see. AlienVault helped us turn the lights on."

Justin P Webb, Security Analyst, IT Services,
**MARQUETTE UNIVERSITY**

CONTACT US TO LEARN MORE

AlienVault™
WWW.ALIENVAULT.COM

### Learned from our 18,000 OSSIM installations

**EASE OF USE**
"It shouldn't take days or weeks for setup and configuration" Solutions that solely rely on external log data can take days, weeks, or months to deploy and deliver value.

**INTEGRATION**
"Common security workflows span individual tools" For each newly discovered asset, seamlessly transition to a vulnerability assessment of the asset(s). Next, enable the appropriate threat detection for the asset(s)...

**COLLABORATIVE DEFENSE**
"We're all in this together" All systems should share threat information so a threat discovered in one part of the world is quickly and automatically shared with all AlienVault USM systems.