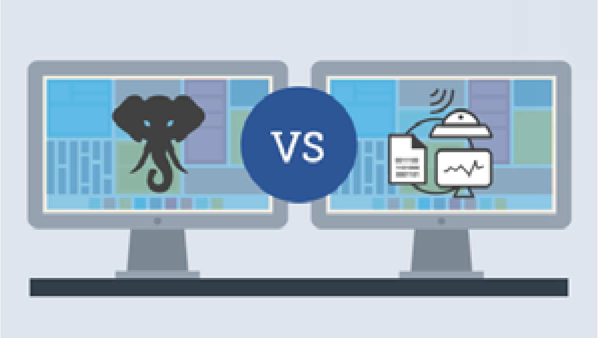
WHITE PAPER

Comparing OSSIM to USM™

How to Choose Between Open Source and Commercial Products

AlienVault® believes in an open, collaborative and integrated approach to security, not a patchwork built of proprietary point solutions.



We believe that the best IT security requires integrated capabilities. AlienVault® has built a unified framework, which is available as an Open Source (OSSIM) and a commercially supported product — AlienVault® Unified Security Management™ (USM™).

With AlienVault USM, you don't have to take on the heavy burden of integrating standalone data sources. We do it for you. This improves your ability to detect threats while reducing the resources required to deploy and manage your threat detection and incident response, this approach is faster and easier than implementing many disparate point products.

While our Unified Security Management platform is well-suited to companies of all sizes, we also make a subset of its features available as an open source offering — OSSIM. We do this because we believe that everyone should have access to the sophisticated technologies required to keep our networks secure, but are often only affordable by large enterprises. The audience that benefits from using OSSIM include IT professionals at smaller organizations with very few resources, but also security researchers and the academic community. We are committed to supporting the unsung heroes who can't convince their management that security is a problem.

We do this because we believe that until everyone is secure, no one can truly be secure.

Our open source solution is a feature-rich product, but lacks the full complement of capabilities many organizations require. To achieve greater operating efficiency, prove regulatory compliance, and leverage the latest Threat Intelligence from AlienVault Labs, you'll want to consider deploying the AlienVault USM platform, AlienVault's full-feature commercial product. Take a look at the table below to see if our open source or commercial solution better suits your needs.

Find the Right Solution for You!

	OSSIM / OPEN SOURCE	ALIENVAULT USM PLATFORM
Threat Intelligence	None	• Threat Intelligence Updated 4x Weekly by AlienVault Labs • 8 coordinated rulesets keep detection & response capabilities up-to-date
Curated Correlation Directives	None	Over 2500 Correlation Directives Updated Weekly by the AlienVault Labs Threat Research Team
Threat Data	Community-Powered Threat Data via OTX (Open Threat Exchange)	Community-Powered Threat Data via OTX (Open Threat Exchange)
Log Management	Log Retention Only for SIEM Events	Robust Log Management, Log Search & Secure Long-Term Log Retention
Reporting	Basic Reports	200+ Customizable Reports, Including Compliance-Specific Reports
Deployment Architecture	Single Server Deployments	• Multiple Servers Across Geographies or Single Server with Multiple Sensors • Multi-Tier Federated Architecture for Managed Security Service Providers
Administration	Multi-User	Multi-User, Role-based Access Control with Permission Templates
Licensing	Open Source	Commercial
Documentation	None	Full Documentation and Knowledge Base
Support	Community Support via the AlienVault Forums	• Dedicated phone & email support from AlienVault Support Team • AlienVault Product Forums • Free Monthly Training Webinars

Threat Intelligence

Without threat intelligence, a SIEM is basically an empty shell. The threat landscape is constantly changing with the almost daily discovery of new vulnerabilities, new attack techniques, and new strains of malware. You don't have the time or the resources to research these emerging threats or determine if your environment is at risk, or already compromised. Instead, busy IT security teams turn to the AlienVault Labs Threat Intelligence subscription to stay up to date on the latest information about malicious actors, their tools, infrastructure and methods.

OSSIM	USM
None	USM's integrated threat intelligence from AlienVault Labs eliminates the need for IT teams to spend precious time conducting their own research. The AlienVault regularly delivers threat intelligence as a coordinated set of advanced correlation rules and product updates four times each week (on average), including up-to-the-minute guidance on emerging threats and context-specific remediation guidance, which accelerates and simplifies threat detection and remediation. There are over 2,500 curated correlation rules built into the USM platform. Because we own both the data sources as well as the management platform, our threat experts have a comprehensive understanding of the interactions between the different data types being correlated and analyzed as well as the latest attack techniques. We embed this expertise in the built-in security controls and seamlessly integrated threat intelligence we deliver, to allow you to detect the latest threats as well as instruct you on how to mitigate the threats quickly and effectively, regardless of your network environment.

Curated Correlation Directives

Correlation directives are what SIEM technologies use to convert mountains of data into actionable information. They analyze events from across the network to identify malicious activity. Correlation directives need to be curated to be effective, to ensure they are up-to-date with the latest threat information and techniques. Curation enables USM to identify and link the few discrete events from across your network that indicate malicious behavior.

OSSIM	USM
None	IT teams of all sizes suffer from too much data and not enough information, as security tools generate a steady stream of alerts. IT teams without deep security expertise are then required to conduct research into each alarm to understand its significance and how to respond. The AlienVault Labs threat research team spends countless hours mapping out the different types of attacks, the latest threats, suspicious behavior, vulnerabilities and exploits they uncover across the entire threat landscape. The Labs team uses this knowledge to curate over 2,500 correlation directives that ship with the USM platform, to help you detect, prioritize, and respond to threats faster.

Threat Data

AlienVault® Open Threat Exchange™ (OTX™) is the world's first truly open threat intelligence community. It enables collaborative defense with actionable, community-powered threat data and global insight into attack trends and bad actors. OTX pulses provide users with a summary of the threat, a view into the software targeted and the related indicators of compromise (IOC) that can be used to detect the threats. IOCs include:

- IP addresses
- Domains
- Hostnames (subdomains)
- Email
- URL
- URI
- File Hashes: MD5, SHA1, SHA256, PEHASH, IMPHASH
- CIDR Rules
- File Paths
- MUTEX name
- CVE number

OSSIM	USM
Community-Powered Threat Data via OTX (Open Threat Exchange)	Community-Powered Threat Data via OTX (Open Threat Exchange)

Log Management

You need to consider your log retention requirements — especially if you are in a regulated industry or have stringent log retention requirements as a best practice. USM includes the AlienVault Logger for log management and retention, an additional component that OSSIM does not have.

OSSIM	USM
OSSIM retains SIEM events only.	AlienVault USM provides robust log management, log search & secure long-term log retention.

Reporting

Compliance and management reporting may be important at your company and should not be overlooked. The OSSIM product includes management reporting to let those who aren't on the front lines of security understand the dynamic nature of the threat landscape and the value of the security systems that you have put in place.

OSSIM	USM
OSSIM comes with basic reports.	AlienVault's USM provides more than 200 professionally developed compliance and threat reports out-of-the-box. Compliance-specific reports include • PCI-DSS • HIPAA • NERC CIP • GLBA • FISMA You can clone and customize these reports, or create entirely new reports as well. The commercial reporting system provides a module-based approach to reporting, allowing you to combine more than 2500 report components into a single snapshot report that displays exactly the information you require. It also allows you to customize the look and feel of reports with your corporate logo and color palette.

Deployment Architecture

Consider the scope of your deployment goals (for both today and tomorrow) to determine how much flexibility your environment will require.

OSSIM	USM
Allows quick and easy deployment with a Sensor and Server installed on the same machine.	The AlienVault USM platform provides you with a full range of deployment options, including on-premise (with both physical and virtual hardware options) . You can deploy multiple servers across geographies or a single server with multiple sensors. You can deploy a single All-in-One appliance, or separate Sensor, Logger, and Management Server. The USM platform also supports multi-tier deployments with its Federated architecture for MSSPs. Federated deployment also allows customers with multiple remote locations that require data to be locally managed (e.g., due to regulatory requirements or internal policies).

Administration and Access Control

Security systems monitoring your environment contain sensitive information. Maintaining proper access control is essential to preventing this information from falling into the wrong hands. The scope of your deployment and number of IT people accessing the system are important considerations when determining the level of access your organization requires.

OSSIM	USM
OSSIM provides user-level access control. You can create and assign a role for each level of user in the system that restricts what operations that level can perform.	AlienVault's USM provides an additional layer of access control. You can restrict users to view and perform operations on an explicitly defined set of assets. For organizations with multiple data centers or sensitive network segments, limiting the scope of access of any individual security analyst adheres to the security best practice of "least privilege". Administrators can also create templates for user permissions (Role Based Access Control), defining access to functions and assets.

Licensing

You have the flexibility to choose the product that best fits your requirements and budget.

OSSIM	USM
Open Source	Commercial

Documentation

Documentation, including deployment guides, user guides, and knowledge base articles, help you get the most out of your AlienVault products.

OSSIM	USM
None	Full Documentation and Knowledge Base

Support

Even the best products require a little assistance from time to time. If security is a business-critical function at your organization, ongoing support is a serious consideration.

OSSIM	USM
AlienVault hosts and moderates community forums for OSSIM users. The forum is a resource for anyone looking to have a quick question answered and is an excellent place to collaborate with peers on security topics. We also offer OSSIM user training sessions in the product forum.	AlienVault offers a range of paid support options for USM customers in addition to the no-cost collaborative community forums. We provide dedicated phone & email support from the AlienVault Support Team, as well as free monthly product training webinars.

An Analyst Perspective on AlienVault USM:

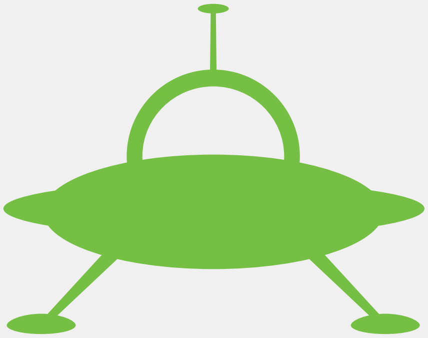
- Frost & Sullivan Executive Brief: SIEMplifying Security Monitoring for SMBs

Learn more about OSSIM:

- Download Here

Learn more about AlienVault USM:

- Download a Free 30-Day Trial
- Create Your Personalized Demo
- Join Us for a Live Demo



About AlienVault

AlienVault® has simplified the way organizations detect and respond to today’s ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault’s Open Threat Exchange, the world’s largest crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures. For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).