
AlienVault™
OSSIM VS. COMMERCIAL PRODUCTS

OSSIM vs. Commercial Products

AlienVault believes in an open and collaborative approach to security. Security cannot be a patchwork—a closed solution, clumsily built of proprietary point solutions.

We believe that true security demands integration and orchestration of all the essential security capabilities. We have innovated a commercial product that makes it possible for heterogeneous, best-of-breed, security tools to be built into a unified framework, our AlienVault Unified Security Management™ platform. You don't have to take on the heavy burden of integration. We do it for you. This improves your security while reducing your management and deployment overhead.

While our Unified Security Management platform is well-suited to companies of all sizes, we also make a subset available as an open-source offering. We do this because we believe that everyone should have access to the sophisticated technologies required to keep us secure, but that are often only affordable by large enterprises. The audience that needs this expanded access includes not just small companies who lack resources, but 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 full-featured product, but may lack the full component of features and services larger organizations require. If you need to secure a larger environment, need greater operating efficiency, need to prove regulatory compliance or need the latest Threat Intelligence from AlienVault Labs, take a look below and see if our commercial solution is for you...

	SUPPORT	DEPLOYMENT	MANAGEMENT	SECURITY INTELLIGENCE -CORRELATION RULES	SECURITY INTELLIGENCE -IDS RULES	USER MANAGEMENT & ACCESS CONTROL	REPORTING
OSSIM	Community	Single tier	Each component managed independently	Community developed	Community developed	Minimal user-level access control	Community developed
COMMERCIAL PRODUCTS	Up to 24x7	Multi-tier (Federated), Multi-tenant Support, High-Availability	Centralized management and configuration	AlienVault Labs Weekly Threat Update	AlienVault Labs Weekly Threat Update with Emerging Threats Pro	Rich asset-based access control with templates	AlienVault Labs developed (100+ Compliance and Threat Reports, 2500+ Report Modules, Web Wizard for Customization)

Support

Even the most elegantly automated products require a little assistance from time to time. The same is true for AlienVault OSSIM and the commercial products. If security is a business-critical function at your organization then ongoing support is a serious consideration.

OSSIM	COMMERCIAL PRODUCTS
AlienVault hosts and moderates community forums for OSSIM users. This forum can be a resource for anyone looking to have a quick question answered and is an excellent place to collaborate with peers on security projects.	Our commercial products are available with a wide range of support plans that complement the collaboration on our forums. Our support plans provide up to 24x7 support with service level agreements that guarantee prompt response.

Deployment

Every organization and network has a different set of problems. But they all started with the words 'we will come back and do it right later.' Each environment requires slightly different deployment architectures to succeed. And there's also the issue of small legal differences that further restrict data portability and introduce additional restrictions. Consider the scope of your deployment goals (for both today and tomorrow) to determine how much flexibility your environment will require.

OSSIM	COMMERCIAL PRODUCTS
Provides quick and easy deployment with all components (sensor and SIEM) installed on the same machine. When it is necessary to extend your monitoring capabilities, additional sensors can be deployed throughout the environment.	Our commercial products come with full deployment flexibility. Not only can they be distributed throughout the environment as needed, but also it is possible to deploy them in a federated model. This enables additional levels of scalability while also allowing customers who require data to be locally managed to be regulatory-complaint. In addition to supporting federation, the commercial products also provide multi-tenancy. In fact, all organizations that require strict data isolation or those using AlienVault to provide managed security services should consider multi-tenancy a necessity. Multi-tenancy provides the ability to meet those requirements without increasing the footprint of the installation or increasing the administrative overhead.

Management & Configuration

Security organizations are perpetually faced with a growing array of threats that demand more and more of their time. Paradoxically, the experts we hire to deal with these threats often spend disproportionate time configuring and maintaining the systems set up to mitigate them. In order to get the most out of your security experts, consider how efficiently you can manage and maintain your security controls.

OSSIM	COMMERCIAL PRODUCTS
OSSIM allows users to configure and manage the components installed locally with the SIEM, using a web-based interface. Note, though, that any sensors that are remotely deployed do require management using the provided command line interface.	Our commercial products allow use of a web-based interface to configure and manage all AlienVault components. Regardless of the deployment model, single-tier or federated, this web interface lets you access system status and update the configuration of all components, thus greatly reducing the time spent maintaining the installation. Whether updating a network interface or deploying a software update, these maintenance tasks can be done with a few clicks.

Threat Intelligence – Correlation Rules

Without threat intelligence, a SIEM is simply an empty shell. While a correlation engine can detect complex patterns in the events that are analyzed, those patterns must be established in advance. Insight into how attackers are exploiting systems, and staying abreast of the technologies employed, is critical to detecting the latest threats. Threat intelligence is a necessity. Does your organization have the critical capabilities and bandwidth necessary to monitor the threat landscape and create correlation rules for the latest threats?

OSSIM	COMMERCIAL PRODUCTS
Over the years the community has developed a number of correlation rules that can be used in the OSSIM product. These are strategically made available when a user chooses to share with the broader community.	The commercial products support the AlienVault Labs Threat Intelligence subscription, providing weekly updates of the correlation rules. The AlienVault Labs team employs a number of techniques to stay on top of the latest threats, including malware analysis, identifying trends in the Open Threat Exchange, collaboration with other security research teams, and deploying honeypots. The continuous stream of data from their research makes possible an ever-expanding set of correlation rules that are pushed out on a weekly basis.

Threat Intelligence – IDS Rules

Good correlation starts with good data. Monitoring your network is a proven method for detecting malicious behavior. Traditional IDS deployments occur at the perimeter, but today, malware is a primary attack vector—making this protection almost obsolete. Malicious network traffic can easily be completely contained within your perimeter, but detection of this behavior requires threat intelligence similar to that needed in your correlation rules. The behavior of the latest threats as they manifest at the network level needs to be recognized, and deployed as rules that feed your IDS deployment.

OSSIM	COMMERCIAL PRODUCTS
OSSIM uses the community supported Emerging Threats Open rule set. This is an open-source project supported by the Emerging Threats organization.	AlienVault Labs provides custom IDS signatures to help support the correlation rules we develop. Having the ability to look for malicious behavior at the network level (IDS rules), as well as the environment level (correlation rules), provides ultimate flexibility for threat detection. In addition to the rules developed by the AlienVault Labs organization, the Emerging Threats Pro rule set is also provided. This feeds a daily update of IDS rules with the latest detection capabilities for exploits, malware, CnC communication, exfiltration behavior and corporate policy violations. Imagine configuring and managing honeypots all over the world, partnering with dozens of antivirus companies, networking with all of the top security research firms AND then hiring IDS experts to turn all that information into IDS rules. No small task is it? Emerging Threats Pro makes it look easy.

User Management and Access Control

Unsurprisingly, the system that monitors your environment contains some pretty sensitive information. Maintaining proper access control is essential to preventing this information from accidentally falling into the wrong hands. The scope of your deployment and number of security analysts are important considerations when determining the level of access control that your organization will require.

OSSIM	COMMERCIAL PRODUCTS
OSSIM provides user-level access control. Each user can be created and assigned a role in the system that restricts what operations they can perform.	In our commercial products an additional layer of access control is provided. Users can be restricted to view and perform operations on an explicitly defined set of assets. For organizations with multiple data centers or sensitive network segments, isolating the scope of access any individual security analyst has allows you to comply with the security principle of 'least privilege". And we scale this; administrators can create templates for user permissions, defining the operations and assets that they have access to, thus greatly reducing the burden of provisioning new user accounts.

Reporting

Security is a multi-year commitment. You have an obligation to manage successful projects, ones that get funded year after year. Best-in-class reporting lets those who aren't on the front line understand the real nature of the threat landscape and benefit of the systems that are in place. The motivation beyond the deployment determines the specific requirements for reporting. For example, if regulatory compliance is the driver, then reports demonstrating that compliance are a requirement.

OSSIM	COMMERCIAL PRODUCTS
OSSIM comes with a number of summary and statistical reports providing information related to the operation of the system. Additional threat reports have been provided by the community and are available in the product.	AlienVault Labs provides more than 100 professionally developed compliance and threat reports. The commercial reporting system provides a module-based approach for reports, allowing more than 2500 report sections to be combined into a single snapshot report that displays exactly the information that is required. For most, simply customizing the look and feel with your own corporate logo and color palette will be enough and you can use one of the 100 reports already provided.

About AlienVault

AlienVault provides organizations of all types and sizes with unprecedented visibility across the entire security 'stack' with the AlienVault Unified Security Management™ (AV-USM™) platform. Based on OSSIM—the de facto standard open source SIEM created by AlienVault—the AV-USM platform has five essential security capabilities built-in: asset discovery, vulnerability assessment, threat detection, behavioral monitoring and security intelligence. The AlienVault Open Threat Exchange™, a system for sharing threat intelligence among OSSIM users and AlienVault customers, ensures AV-USM always stays ahead of threats. AlienVault is a privately held company headquartered in Silicon Valley and backed by Kleiner Perkins Caufield & Byers, Sigma, Trident Capital and Adara Venture Partners. For more information visit www.AlienVault.com or follow us on Twitter.

AlienVault™

www.alienvault.com