DETAILS

Vendor AlienVault

Price Starts at $650/month

Contact alienvault.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★¾

Strengths Easy to use product that provides excellent correlation of events with a ton of additional features at a great price point.

Weaknesses System is memory intensive and can freeze up at times of heavy use. Limited information included inside error messages.

Verdict AlienVault continues to be an amazing UTM solution for businesses of all sizes.

Global Headquarters:
1875 S. Grant Street Suite 200
San Mateo, CA 94402
650-713-3333
www.alienvault.com

AlienVault

AlienVault USM Anywhere

We have been using AlienVault for a while now and the only question we really have is "what is left to say about this great product?" AlienVault USM does everything you ask of it and then some. Setup and deployment are straightforward and can be completed with little time or effort. For assistance, AlienVault's professional services teams or one of their many trusted partners can get this set up in your environment.

The typical deployment requires a sensor that can run in VMware or Hyper-V as well as hosted in the cloud on AWS or Microsoft Azure. There is also a software version that can be deployed on a physical server. Starting at $650 a month, this solution is a must-have for any business that values information.

AlienVault's web user interface provides an all-encompassing picture and lets you drill down as far as you need. It correlates logs from all types of sources, including Windows Event logs, MS SQL, syslog and even NetFlow. AlienVault pulls data on file integrity and intrusion detection, which can be configured toward an agent or even agentless. USM Anywhere centrally collects and securely stores log and event data from on-premises and cloud environments, and from cloud applications like Office 365 and G Suite. Data can also be collected from Windows and Unix-based systems using a host-based agent and/or syslog as available.

A feature that we use often during testing inside SC Labs is log correlation, and AlienVault delivers a rich analytical toolset that allows the user to view raw logs and filter down to what they are looking for. Logs are encrypted and preserved so you can perform a forensic analysis on an incident.

The AlienVault Labs Threat Research Team leverages original threat research and crowd-sourced intelligence from the largest crowd-sourced intelligence exchange, comprising of more than 80,000 members, the AlienVault Open Threat Exchange (OTX) community, delivering continuously updated threat intelligence directly to AlienVault USM to support threat detection use cases. This threat intelligence includes IDS signatures, vulnerability signatures, and correlation rules designed to detect threats within the cloud and on-premises environments.

AlienVault USM Anywhere provides asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring and log management. USM Anywhere also includes out-of-the-box reports for common compliance regulations such as PCI-DSS and HIPAA, and offers the ability to create, filter, and save customized reports, just about anything you could ask from a regulatory compliance perspective.

AlienVault offers a wide variety of well-written support documentation through its support portal. The website also contains videos and other useful information. There are many third-party forums with extensive community support.

– Michael Diehl with Dan Cure; tested by Matt Hreben and Michael Diehl