AlienVault® Unified Security Management® (USM) Customer Reviews Report

Authentic Customer Reviews Collected and Vetted by Trusted Third-Party Review Sites

About This Report

This report is designed to help you make an informed decision about the AlienVault® Unified Security Management® (USM) platform. It is based on real user reviews and ratings of AlienVault USM on trusted third-party sites including Gartner Peer Insights, G2 Crowd, IT Central, and TrustRadius.

The customers shown in this report reflect a comprehensive sampling of our extensive customer base from nearly every industry including, but not limited to, Banking and Financial, Healthcare, Government, Education, Retail, and Hospitality. All customer reviews were collected and vetted by trusted third-party review sites. You can rest assured that these reviews are authentic, unbiased, and most importantly, candid.

Table of Contents

AlienVault Ratings Summary (Current Ratings as of 1/22/18)

REVIEW SITE	AVERAGE RATINGS	NUMBER OF RATINGS
Gartner Peer Insights	4.3 of 5.0	81
G2 Crowd	4.5 of 5.0	49
IT Central Station	4.2 of 5.0	55
TrustRadius	7.9 of 10	276

Gartner Peer Insights: Gartner Peer Insights offers detailed perspectives for every phase of the IT lifecycle – from evaluation and implementation to service and support. Find ratings, reviews and advice on IT solutions – right when you need them. Gartner Peer Insights ensures that you get thorough, easy-to-consume answers to your most critical questions.

Visit Gartner Peer Insights

G2 Crowd: G2 Crowd empowers business buying decisions by highlighting the voice of the customer. The G2 Crowd review platform leverages more than 170,000 independent and authenticated user reviews read by nearly 900,000 buyers each month. G2 Crowd's mission is to provide the insights business professionals need to gain confidence in their buying decisions and become more successful in their jobs.

Visit G2 Crowd

IT Central Station: IT Central Station has grown into a dynamic, real-time platform that offers user information that is current, objective, and relevant. It protects privacy in that users can either post anonymously to freely express their views or use their real names to promote their expertise. It enables knowledgeable experts, including real users and independent consultants, to share their expertise in a high-quality community of decision makers.

Visit IT Central Station

TrustRadius: TrustRadius is the most trusted review site for business technology, serving both buyers and vendors. We help buyers make better product decisions based on unbiased and insightful reviews. We also help vendors scale and harness the authentic voice of their customers across their sales and marketing channels. Every reviewer on TrustRadius is authenticated, and every review vetted by their Research Team before publication.

Visit TrustRadius

What is AlienVault® Unified Security Management® (USM)?

AlienVault Unified Security Management (USM) is a comprehensive approach to security monitoring, delivered in a single, unified platform. The AlienVault USM platform includes five core security capabilities that provide resource-constrained organizations with all the security essentials needed for effective threat detection, incident response, and compliance, in a single pane of glass. Designed to monitor cloud and on-premises environments, the AlienVault USM platform significantly reduces complexity and reduces deployment time so that users can go from installation to first insight in minutes for the fastest threat detection.

Unlike traditional security point technologies, AlienVault USM does the following:

- Unifies essential security controls including asset discovery, vulnerability assessment, intrusion detection, and SIEM into a single all-in-one security monitoring solution
- Monitors your cloud and on-premises infrastructure from a single, unified platform
- Delivers continuous threat intelligence developed by the AlienVault Labs Security Research Team, and powered by the Open Threat Exchange® (OTX™), to keep you aware of threats as they emerge and change
- Provides comprehensive threat detection and actionable incident response directives
- Deploys quickly, easily, and with minimal effort
- Reduces TCO over traditional security solutions

Customer Reviews

When researching a new technology, it is always beneficial to hear the opinions of other users. In the remainder of this guide, you will get an inside look at why customers chose AlienVault USM, the security capabilities valued most by customers, and the benefits achieved by using AlienVault USM.

Why AlienVault?

AlienVault is the champion of mid-size organizations that lack sufficient staff, security expertise, technology, or budget to defend against modern threats. The USM platform provides all of the essential security controls required for complete security visibility, and is designed to enable any IT or security practitioner to benefit from results on day one.

Ease of Use

> *"This product is easy to use, easy to understand, and the layout and dashboard are very user-friendly!"*
> — IT Security Analyst, Finance (Gartner Peer Insights)

> *"[AlienVault] USM is one of the easiest to use on the market and has very informative dashboards."*
> — Philip Clarke, IT Systems/Security Manager, R&Q (TrustRadius)

> *"The ease of use and customization. The USM platform is a work horse, no matter what devices or the number of logs we throw at it, the system processes them in real-time, correlates the events, and alerts on only events that need human review."*
> — Karl Hart, ACSE, CEH, CHFI, CISSP, Administrator in Retail (G2 Crowd)

Reliability

"The system is incredibly reliable, it provides great feedback, and the set up is also very simple."
— Technician in Information Technology (TrustRadius)

"AlienVault USM is a wonderful and vital component to our layered security!"
— Kirk Crespin, IT/IS Officer at Community State Bank (TrustRadius)

"The alarms dashboard is very useful. I have that up 100% of the time on a third monitor to watch activities in my environment. This allows me to focus on the major items like system compromise and make environmental awareness a lower priority."
— Marc Roche, CTO, Alpine Woods Capital Investors (TrustRadius)

Innovation

"Frequent improvements. AlienVault appears dedicated to improving its product. In the relatively short time we've had it in place we have received several updates to features and functionality."
— Manager in Information Technology, Automotive (TrustRadius)

"I think the frequency of updates is great as well. I like knowing that there is a team of folks constantly trying to improve the product."
— Aaron Baillio, Security Architecture and Operations Lead, University of Oklahoma (TrustRadius)

"I have also had the opportunity to speak to several individuals within AlienVault to discuss problems I have had with the product or features that I would like to see. They have always listened to me and almost all of the things that I wanted to see have actually been added to the product in the time I have used it."
— Administrator in Information Technology at a Retail company (TrustRadius)

Professional Services and Support

"The support provided is above and beyond what I would expect for the price."
— Information Technology, Finance (Gartner Peer Insights)

"[Technical Support is] Excellent! Every time I have had an issue, the customer and technical support has been outstanding. The support desk is always very helpful, and goes out of their way to make sure the issues are resolved whenever possible."
— Jacques Taljaard, Security Consultant at a tech consulting (IT Central Station)

"AlienVault's support is fascinating as they are always looking out for their customers. The staff checks up on their customers monthly to see if everything is working appropriately and if there is anything they can do to help."
— Technician in Information Technology (TrustRadius)

Documentation and Training

"Take the training courses and this will save a lot of time getting everything out of this product."
— Security Administrator, Miscellaneous (Gartner Peer Insights)

"Training was good and allowed us to immediately customize the product to our needs."
— Systems Administrator II, Finance (Gartner Peer Insights)

"There is a great deal of online training and a good user community."
— Information Technology, Finance (Gartner Peer Insights)

AlienVault vs. Competition

"I used multiple products to try and get some way towards the level of visibility afforded by AlienVault. ManageEngine SIEM, Qualys, vulnerability management, and Norton for HIDS. Having this all in one interface made more sense which swayed the decision to go with AlienVault."
— InfoSecOfficer506, Group Information Security Officer at a Consumer Goods company (IT Central Station)

"Other SIEM/USM products that we use are Splunk, LogRhythm and the free OSSIM version. The first two have a different cost model and compared to AlienVault they have (or lack) the real Swiss army knife approach. Furthermore, there is a big difference in costs, this is why in the end AlienVault takes the lead."
— Frans van Dokkumburg, Info Security Consultant at Securepoint Nederland B.V. (IT Central Station)

"I reviewed LogRythm, QRadar, and Alert Logic: QRadar - out dated visually Alert Logic - had some cumbersome attributes and was sold more as SAAS LogRythm - closest to AlienVault but had outdated features when comparing the two and couldn't provide IDS."
— Philip Clarke, IT Systems/Security Manager, R&Q (TrustRadius)

Ability to Deliver Essential Security Capabilities

The Unified Security Management® approach eliminates the complexity and costs of integrating and maintaining multiple point solutions. By combining five essential security capabilities into one platform, organizations can spend more time responding to threats rather than dealing with the headaches and hassles of deploying and integrating multiple products. In this section you'll read how customers view AlienVault's performance in: Threat Detection, Security Intelligence, Asset Management, SIEM and Log Management, Vulnerability Assessment, IDS, and Compliance.

Threat Detection

An organization's security depends on their ability to detect emerging threats in cloud and on-premises environments, and respond to them quickly. With the constantly evolving nature of the threat landscape, it can be difficult, if not impossible, to address every incident and alert that occurs in an environment. Organizations must find a tool that can help to cut through the clutter of low-risk alerts and false positives to effectively prioritize threat detection and response activities.

"It [AlienVault USM] has worked well for us and given us what we needed out of the product. We are able to be more proactive on threats and know what we have in our environment now."
— Systems Administrator II, Finance (Gartner Peer Insights)

"AlienVault has detected suspicious activity before our antivirus software could, seeing the activity prior to the scan or prior to a virus definition being written."
— Greg Baugh, VP Data Processing at Peoples National Bank - Niceville FL (TrustRadius)

Security Intelligence

Security analysts are a lot like detectives. During security incidents and investigations, they need to get to "whodunit" as quickly as possible. This is complicated, especially when mountains of security-relevant data are constantly being produced. Context is key – one piece of information by itself may mean nothing, but it might become a very important piece of a larger puzzle. Security intelligence is an essential part of putting that puzzle together.

> *"Ability to push all the logs to one central repository and do forensics. It also comes with the Open Threat Exchange® (OTX™) feature which I found very useful."*
> — Senior Security Engineer, Education (Gartner Peer Insights)

> *"Really do like the software as any company should they continue to improve their product. As I use the product more I begin to realize the cost savings we are actually accumulating such as with the new WannaCry. I hear company after company getting hit by this malware as we had already closed up the vulnerability of SMBv1 in our network due to it showing on my vuln list weeks prior. This alone has saved my company quite a bit of funds."*
> — David Cunliffe, Systems Engineer at Chargebacks911 (G2 Crowd)

> *"Others try to make use of the free Open Threat Exchange (OTX) and advertise their product "keeps up to date with the latest threats" and tell you it can show you everything on your network and problems before they are a problem but none can truly do what AlienVault does."*
> — Danny Santiago, Systems & Applications Administrator at City of Lewiston (TrustRadius)

Asset Management

Most IT networks are in a constant state of flux. With devices continually being connected or removed from the network, it's easy to lose track and leave some assets unmonitored. This creates exposure in your network that attackers can exploit to gain access and conduct malicious activity. To meet this challenge, it's necessary to possess robust asset management and inventory tools that make it easy to keep track of all of an organization's devices being added or removed from the network.

> *"Asset management and detection has been easy to use and has given us an inventory of everything on our network."*
> — Joe Chaney, Network Manager at Arbor Day Foundation (TrustRadius)

> *"Asset Discovery - AlienVault USM makes the creation and maintenance of the asset database simple. It auto-discovers devices on the network to build the database and add devices when they are added to the network. There is a passive and active scanning mode to do this. The active scan gives a lot more information about the devices which can include open ports and running operating systems."*
> — Mike Kerem, CTO at TrustNet Inc. (TrustRadius)

> *"The asset management setup was easy; just identify your networks and set up a basic asset scan all in a wizard like approach."*
> — Engineer in Information Technology at an Information Technology and Services company (TrustRadius)

SIEM and Log Management

Single-purpose SIEM software and log management tools provide valuable security information, but often require expensive and time-consuming integration efforts to bring in log files from disparate sources such as asset inventory, vulnerability assessment, and IDS products. Once you have the data, you then must research and write correlation rules to identify threats in your environment. These challenges multiply as you migrate workloads and services from on-premises infrastructure to public cloud environments.

> *"If you need a log repository you can rely on and also a tool which has some sort of IDS to it then this is the best tool. It also has a vulnerability scanner."*
> — Senior Security Engineer, Education (Gartner Peer Insights)

> *"My opinion aligns almost perfectly with the [2016] Magic Quadrant for SIEM. AlienVault's idea to blend the integrate threat intelligence and the USM platform is really the next evolution in SIEM. The AlienVault device detects a number of environmental threats that our other supported products miss."*
> — Aaron S. Moffett, Senior Information Security Consultant, VioPoint (TrustRadius)

> *"AlienVault does more than any SIEM with its HIDS agents, vulnerability scanning, asset discovery, etc. The included Open Threat Exchange subscription is also a major plus."*
> — Jon Armani, Security Analyst at ZOOM+ (TrustRadius)

Vulnerability Assessment

With network vulnerability assessment, you can find the weak spots in your critical assets and take corrective action before attackers exploit them to sabotage or steal your data.

New vulnerabilities emerge near-daily as your IT landscape changes, introduced by configuration errors, unauthorized software installs, insecure endpoint devices, and much more. To keep your data secure, you must continuously scan your systems and devices to detect vulnerabilities as they arise.

> *"I can be proactive instead of reactive to keep on top of vulnerabilities."*
> — Systems Administrator, Healthcare (Gartner Peer Insights)

> *"I find AlienVault has provided superior protection and information. Alarms, threat intelligence, and vulnerability scans have been the foundation of success in fighting threats in my environment."*
> — Executive in Other at a Financial Services company (TrustRadius)

> *"AlienVault is continuously monitoring the network for vulnerabilities and threats, which reduces amount of manual work required to maintain a good security posture."*
> — Jeremy Wanamaker, CEO at Complete Network Support (TrustRadius)

Intrusion Detection System

Intrusion detection systems (IDS) are used to monitor the events occurring in a network and analyze them for signs of possible incidents, violations, or imminent threats to security policies. AlienVault USM brings Cloud IDS, Network IDS, Host-Based IDS and File integrity monitoring into one platform.

> *"The IDS and the ease of use is fantastic! The SIEM is heavily used by our organization and has been accepted and adopted easily."*
> — Information Security Officer, Healthcare (Gartner Peer Insights)

"I am willing to recommend the product because, the product works well, and it provides a lot more features than most of the competitors' products I have tried in the past few years. AlienVault USM truly is a cybersecurity risk management tool, more than just an IDS."
— CEO, Finance (Gartner Peer Insights)

"Easily connects to all my desktops/servers using the HIDS agent, makes it simple to get setup."
— Marc Roche, CTO, Alpine Woods Capital Investors (TrustRadius)

Compliance

Many major companies within the United States are subject to some type of security regulation. These regulations include the Health Insurance Portability and Accountability Act (HIPAA), The Sarbanes Oxley Act, Federal Information Security Management Act of 2002 (FISMA), Family Educational Rights and Privacy Act (FERPA), Payment Card Industry Data Security Standard (PCI-DSS), and the Gramm Leach Bliley Act (GLBA) among other acts and regulations.

IT compliance management is often a manual process that requires the aggregation of data from multiple systems into a single view. However, software like the AlienVault USM platform has now enabled security practitioners to gain complete IT compliance management capabilities in a single platform and console view.

"Event Correlation is the most valuable feature for every SIEM. AlienVault has ISO 27001 compliance which is very helpful for the companies looking to have the ISO 27001 certification."
— Wajdi Ayari IT Engineer at an energy/utilities company (IT Central Station)

"AlienVault USM compiles/correlates logs from devices so that we can show evidence of PCI compliance by tracking and reporting on system administration activities such as additions/changes to privileged accounts, group policy objects, and firewall rules."
— Kevin Geil, Information Security Officer at NYS Olympic Regional Development Authority (TrustRadius)

"AlienVault USM is a strong solution for any organization with a large number of events to manage or those with a regulatory need to keep track of events."
— Terrance Schmitt, Senior Network Engineer at Forefront Dermatology (TrustRadius)

Ability to Provide Positive Benefits and Outcomes

AlienVault USM, combined with the power of the AlienVault Open Threat Exchange® (OTX™), the world's largest crowd-sourced threat intelligence community, makes effective and affordable threat detection attainable for resource-constrained IT teams. In this section, you will read customer reviews on AlienVault's ability to provide ROI, Fast Threat Detection, and Completeness.

ROI (Time Savings/Efficiency/Cost Reduction)

"Overall, excellent value for money. It is a swiss army knife of functionality that exactly met the needs of the organization and an acceptable price point."
— CSO, Services (Gartner Peer Insights)

"If you need what AlienVault does - don't hesitate to get the product. It is excellent value for money and provides you a large number of tools immediately."
— CSO, Services (Gartner Peer Insights)

"It is really hard to put a number on ROI but I will say that AlienVault has allowed us to close the gap on security alert timing and we can respond to incidents in a much more timely fashion which, to me, is much more valuable than a number."
— Brett Carson, IT Supervisor at an energy/utilities company (IT Central Station)

Faster Threat Detection

"Once we placed AlienVault in the product we have now, the time it takes to find and respond to real anomalies has dropped from hours to minutes!"
— SOCAnalyst701, SOC Intrusion Analyst at a tech services company (IT Central Station)

"I am able to scan for vulnerabilities quickly on existing devices and also for new devices being deployed. Since I don't have a lot of time to learn new and complicated tools, being an e-commerce company, this allows me to increase the security posture of the overall organization and also to help pass PCI compliance."
— Donald Nappi, Cissp, IT II, Manager, Information Security, Retailer (IT Central Station)

"The single pane of glass that shows threats that are in the environment."
— Kevin Marsh, IT Security Engineer II, Retailer (IT Central Station)

Completeness

"It is the central view into our security stance and provides an easy to use method for detecting and finding vulnerabilities and threats to our enterprise."
— Manager in Information Technology (TrustRadius)

"Having the AlienVault USM platform really simplifies all your tools into one interface. You really don't need a Security Admin to manage this tool."
— Will Armistead, System Administrator at AKT CPAs, Advisors, Consultants (TrustRadius)

"The largest factor is again their all in one style interface which allows me to spend time on all aspects of Information security and not just chasing threats."
— Executive in Other at a Financial Services company (TrustRadius)

In Closing...

View More Customer Reviews on:

Gartner peerinsights™ | G2 CROWD | IT Central Station Unbiased reviews from the tech community | trustradius™

Learn More About AlienVault:

[451 Research Report: AlienVault USM Anywhere]

[451 Research Report: AlienVault Open Threat Exchange (OTX)]

[Frost & Sullivan Executive Brief: AlienVault: What You SIEM is What You Get]

[Product Review: SC Media Gives AlienVault USM 5 Stars]

[AlienVault Fast Facts]

SC Media ★★★★★ | CRN Security 100 2017 | CRN Cloud Partner Program Guide 2017 | SC Awards Winner | Forbes 2017 Cloud 100 World's Best Cloud Companies | Deloitte Technology Fast 500 | Cyber Security Excellence Awards Winner 2017