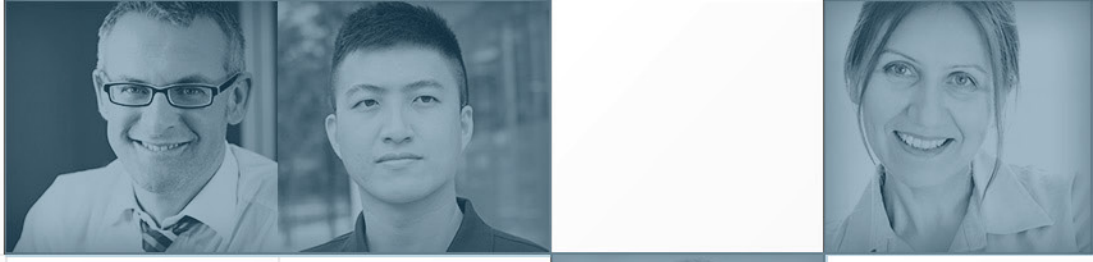
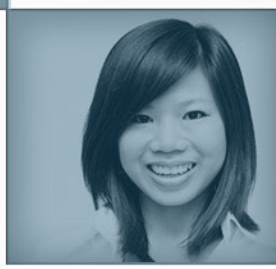




AlienVault USM™ Product Report

Curated from End-User Reviews on:

trustradius™





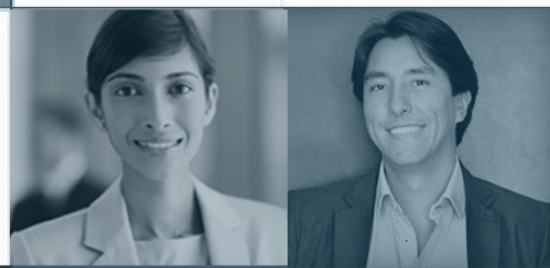



Table of Contents

ABOUT TRUSTRADIUS

TrustRadius is the leading site for business software users to share real-world insights through in-depth reviews and networking. We help users make better product selection, implementation and usage decisions. Every reviewer is authenticated and every review vetted before publication. Unlike simple rating sites, TrustRadius reviews are structured and substantive, averaging more than 400 words each. Reviewers can also update their reviews to keep them current. Founded by successful entrepreneurs and backed by the Mayfield Fund, TrustRadius is bringing transparency and efficiency to the $3.7 trillion business technology market.

To learn more, visit www.trustradius.com.

About this Report

Why read 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 80 current, in-depth, user reviews and ratings of AlienVault Unified Security Management on TrustRadius, the trusted user review site for business software. By crowd-sourcing user perspectives, we help you to get a true sense of the product.

This report includes analysis of the types of customers (company sizes, industries etc.) that use AlienVault USM, what companies and users like most about the product, areas for improvement, and a discussion of platform effectiveness and process simplification.

Our methodology

TrustRadius invited a broad, random sample of AlienVault's USM user base to review the product on TrustRadius. Reviewers were encouraged to provide candid feedback and had the option to remain anonymous. This ensured very authentic feedback. Incentives were also used to motivate response from a broad spectrum of customers, i.e. not just advocates. All reviewers were vetted by our research team to ensure that they were legitimate customers and that their feedback was authentic and unbiased.

AlienVault Product Summary

AlienVault USM

(80) trScore 8.0 out of 10

Product Description

AlienVault Unified Security Management (USM) is a unique all-in-one security management platform encompassing multiple security controls that are usually purchased separately, centrally managed through a single user interface. AlienVault's USM platform provides a unified approach to threat detection and compliance management.

The key capabilities delivered by AlienVault USM include:

- **Security Information and Event Management (SIEM):** SIEM is a security management technology that gathers and analyzes logs and event data from disparate security controls and devices across the network, and then correlates them to find related events, all from a single user interface. A SIEM tool allows security analysts to have a more comprehensive view of security logs and events than would be possible by looking at the log files of individual systems, and to link unique events across a network to detect threats that would otherwise likely go undetected.
- **Behavioral Monitoring:** Behavioral monitoring of the network establishes a benchmark for normal behavior. It then continually monitors network traffic to look for any deviations from expected or normal behavior, which can be an indication of a compromised system. USM combines this behavioral analysis with service availability monitoring to ensure essential services are running on critical systems (as well as identifying any rogue services). These technologies give a complete picture of system, service and network anomalies.
- **Asset Discovery / Vulnerability Assessment:** The first step in securing any network is to conduct asset discovery to map all the IP-enabled devices on your network, what software is installed on them, and how they are configured. Once you know what systems are on your network, the next step is to identify the vulnerabilities on those systems, as attackers will seek to exploit those vulnerabilities. USM uses both active scanning and passive scanning to discover assets, identify services running on a system, software versions and patches and compare that data with known vulnerabilities.

» **Intrusion Detection:** Intrusion detection consists of both Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS) technologies, in addition to file integrity monitoring (FIM). NIDS identifies threats targeting your vulnerable systems with signature-based anomaly detection and protocol analysis technologies. HIDS analyzes system behavior and configuration status to track user access and activity. FIM alerts you to changes in critical system files, configuration files, and content files.

» **Threat Intelligence:** The USM platform also receives updated threat intelligence from the AlienVault Labs team every 30 minutes to ensure the USM platform's correlation directives, IDS signatures, vulnerability audits, IP reputation, context-specific remediation guidance and more are up-to-date. This team is dedicated to analyzing emerging threats, suspicious behavior, and vulnerabilities from across the entire threat landscape. This internally compiled threat intelligence is augmented by the Open Threat Exchange™ (OTX), which is an open threat intelligence community that enables collaborative defense with open access, collaborative research, integration with AlienVault USM, as well as the ability to export indicators of compromise (IOCs) to almost any security product. The community currently has 37,000 participants from 140 countries, contributing over 3 million threat indicators daily.

Value Proposition

AlienVault's USM platform accelerates and simplifies threat detection, incident response and compliance management for IT teams with limited resources. AlienVault USM provides complete visibility into threats affecting the network and how to mitigate them. Three of the key value propositions are:

» **Unified Capabilities:** AlienVault USM is not just a SIEM, but is a set of unified security capabilities that include SIEM, behavioral monitoring, asset discovery, vulnerability assessment, and intrusion detection. The USM console centrally manages all of these built-in capabilities, providing unified, coordinated security monitoring and simplified security event management. No other vendor builds these essential security capabilities into a single platform without any additional feature charges.

» **Reduced Complexity:** Because this is a package of unified capabilities with centralized management, it is much easier to purchase and deploy than having to deal with a set of point products from different vendors. USM requires far fewer dedicated human resources to deploy and manage, as well as collect and analyze the data. You can deploy it quickly as either a hardware or virtual appliance, in your network.

» **Updated Threat Intelligence:** The AlienVault Labs threat research team updates the security controls within USM every 30 minutes with new threat intelligence like IP reputation data, SIEM correlation directives and vulnerability assessment signatures, to keep up with changes in the threat landscape. This data is augmented with additional community-generated threat intelligence from the AlienVault OTX. For many customers, this removes the need to have a dedicated security analyst on staff to research and correlate security data.

Best Fit For

» **Mid-Market organizations:** The AlienVault USM platform is well suited to organizations of all sizes, but especially the mid-market organizations that have limited budgets and few IT security staff or security specialists capable of managing the complexity of multiple security point products. However, we have also seen several enterprise customers successfully deploy and leverage the platform as well.

» **Organizations subject to compliance regulations:** AlienVault simplifies the compliance process through log retention, management and analysis, and the platform has auditor-ready report templates for PCI-DSS, ISO27001, HIPAA, Sarbanes-Oxley, and more.

» **Organizations with existing security point products:** In addition to its built-in security technologies, the USM platform can also integrate data from any device that generates a log. This includes other security technologies like unified threat management (UTM), next-gen firewall (NGFW), and IDS. This data integration allows users to benefit from the UTM platform's ability to significantly increase their visibility into malicious activity on their network while preserving the value of their previous investments.

AlienVault USM User Ratings

Aggregate User Ratings of AlienVault USM

Overall Experience

Client Services

Source: trScores based on end-user reviews and ratings on TrustRadius

trustradius™

Comments on Ratings

Ratings are generally quite high across the board with a very strong Likelihood to Recommend and Likelihood to Renew ratings, and overall rating of 8.

Only the usability score lags a little behind all the other scores. However, drilling down a little into the comments reveals that it is not due to lack of satisfaction with the user interface:

"The menus are well laid out for the most common functions of log management, File integrity monitoring and log analysis. The dashboards with graphs are easy to understand and are perfect for the casual glance aka single pane of glass look at your overall security rating."

Engineer
Information Technology and Services
201-500 employees
November 2015

"Ease of use is good for the most part, but there is room for improvement. With each major release, the interface becomes much better."

Director
Information Technology
201-500 employees
November 2015

Rather, the lower usability score is due to documentation and setup issues:

> **"Not enough documentation, non-descript error messages, and too much required to be done at the command line for an 'appliance'."**

Aaron Rothstein
IT Systems Architect
Rothstein.io
November 2015

> **"The product once properly configured seems to offer a wealth of information but has it has issues. I feel that the initial setup/ installation should include technical support to get up and running. My personal experience from the configuration as installed indicates that the network adaptors are not properly configured to read information. The network ports where configured to only ready 1/2 the network? So having help to get the system up and running should be part of the initial purchase."**

James Ellsworth
IT Technician, Sierra Gold Nursery
201-500 employees
December 2015

Support and Implementation comments are generally very positive supporting the high ratings:

> **"Every time we have opened a ticket with AlienVault they have managed to get us an answer. At times they are not what we want to hear, but I do appreciate the 'drive it home' attitude of tech support. I believe the other SIEM competitors could learn a lesson from AlienVault."**

Engineer
Information Technology and Services
201-500 employees
November 2015

> **"Pre-planning is crucial. We typically preconfigure all appliances before they are deployed to the client so that the only thing left to do is deploy the agents."**

Mike Kerem
CTO, TrustNet
Information Technology and Services
11-50 employees
October 2015

> **"Top-notch service at a fraction of what I pay to other vendors."**

Director
Information Technology
201-500 employees
November 2015

> **"I would plan on the initial setup taking longer than expected. File Integrity Monitoring does not have an automated way of rolling agents out with known keys."**

Engineer
Information Technology and Services
201-500 employees
November 2015

Summary of AlienVault USM User Feedback

The following is a distillation of product strengths and areas for improvement from the 63 end-user reviews of AlienVault USM on TrustRadius.

Strengths

1. Integrated components with centralized management

According to users, one of the most valuable aspects of AlienVault USM is the set of integrated capabilities, with a single management console.

> **"One of the main reasons to get AlienVault is so that you can solve several security 'problems' in one fell swoop. Rather than buying a large number of point products instead you have something that can serve many needs while reducing the amount of expertise you need to have in house."**

Administrator in Information Technology at a Company
10,001+ employees
September 2015

> **"AlienVault USM has five different security monitoring capabilities that are focused on monitoring the health of a network and network systems and are included by default. Other SIEM vendors need to integrate additional products in order to generate the same visibility, which can make a project more complex and more expensive."**

Analyst in Customer Service at an Insurance Company
November 2015

> **"Unified Management: Within a single pane of glass a security analyst may monitor and investigate correlated events from an array of log streams across the organization, deploy Host Intrusion Detection agents, deploy and customize File Integrity Monitoring, execute Vulnerability Assessments, accept input from Threat Intelligence feeds, and utilize correlation to 'bubble-up' what needs to be addressed."**

Director in Information Technology in Oil and Gas Industry
1,001-5,000 employees
December 2015

> **"AlienVault has a broad selection of tools all within the same user interface. We have been able to cover several security needs with one product that previously were done with several different tools. This has made it a lot easier to manage, as we have to learn one tool rather than many different tools."**

Administrator in Information Technology
Retail Industry
10,000+ employees
September 2015

2. SIEM log management and correlation

The SIEM log management and event correlation capabilities get high marks across the board.

"Log correlation is excellent and on par with other more expensive solutions."

Farakh Hussain
Manager Information Security, PriceMetrix
51-200 employees
December 2015

"The cross-correlation in the SIEM module is very advanced. It will take in input from as many devices as you can throw at it, and will set up alarms when it sees suspicious activity."

Mel Green
Network Security Manager, PHE
201-500 employees
November 2015

"Correlates events from different sources and displays comprehensive information about security incidents."

Alexsander Zlatanchev, Chief Information Security Officer
Nanex Technological Development
51-200 employees
November 2015

"AlienVault USM automatically correlates audit log data with security intelligence to identify policy violations."

Chris Niesen
Security Services Manager, The Tech Outfit
1-10 employees
December 2015

3. Open Threat Exchange

Users like that the AlienVault OTX provides open access to a global community of threat researchers and security professionals.

"I love the open threat exchange (OTX). While we use several professional feeds, the OTX is fairly robust and provides a decent threat feed."

Aaron Baillio, Security Architecture and Operations Lead
University of Oklahoma
5,001-10,000 employees
November 2015

"OTX has improved significantly the visibility of the existing threats and this information is not only valuable for the operation of the service we offer, but it can be a great security ally for any other SOC."

Engineer in Telecommunications Industry
5,001-10,000 employees
November 2015

> **"Open Threat Exchange (OTX) is a very important and useful feature, which helps to trace the malicious IP with reputation back to its origin, so intent is clearly visible when analyzing security events. Pulses and IOCs are very interesting and useful as well."**

Vishal Jadhav, Information Security & Pre-Sales Officer
Hemisphere Technologies
11-50 employees
November 2015

> **"OTX (Open Threat Exchange) went from something that was merely interesting and possibly useful to something that is extremely interesting and very useful for incident response. It has a lot of really good information on the many threats that you would see out in the world. It is really handy in order to hone in on the threats that actually matter to you (plus ignoring threats that do not matter)."**

Administrator in Information Technology
Retail Industry
10,000+ employees
September 2015

> **"After getting subscribed to the OTX community I was given frequent updates to the latest security threats and what to look for. To me the best aspect of the OTX activity monitoring is to know when the threat is directly affecting our network and keeping up to date on the threats."**

James Ellsworth
IT Technician, Sierra Gold Nursery
201-500 employees
December 2015

4. Intrusion Detection

Network and host-based intrusion detection tools inspect traffic across the network searching for malicious traffic.

> **"The IDS works surprisingly well. Bumping the results up against APT specific devices, AlienVault catches a large percentage of that traffic."**

Aaron Baillio, Security Architecture and Operations Lead
University of Oklahoma
5,001-10,000 employees
November 2015

> **"As a NIDS, it does a wonderful job at analyzing traffic on the network and presenting me with a clear picture of what's traveling through my network that I may not want there."**

Michael Eller, Junior System Administrator
Puget Sound Surgical Center
51-200 employees
November 2015

> **"Host-based Intrusion detection works well on Windows servers, and monitors for a number of security related events. Also contains event log monitoring."**

Greg Baugh
VP Data Processing, Peoples National Bank
11-50 employees
November 2015

> **"The AlienVault NIDS has proven to be very valuable in helping us identify traffic on our network. It has identified unauthorized traffic that was going out of our network."**

Ledan Patrick Masseus
IT Security Manager, Maspeth Federal Savings
201-500 employees
December 2015

5. Vulnerability Assessment

Network vulnerability scanning to identify and remediate asset vulnerabilities is highly effective.

> **"AlienVault's vulnerability scanning has replaced Nessus for us in the Enterprise. We now have regular, scheduled, scans of all servers and workstations, and have a monthly remediation meeting with the Systems Administrators to work through how to address the more serious vulnerabilities."**

Director in Information Technology
Banking Industry
201-500 employees
September 2015

> **"By vulnerability scanning you can check if a company or external resource is vulnerable and with that information forbid an external resource or remove vulnerability. Now we do not just sit in the dark, we can say that we efficiently manage IT security."**

Sasa Cakic, IT Security Officer,
Vienna Insurance Group
501-1,000 employees
October 2015

"The vulnerability scanning aspect of AlienVault is once again very straightforward. Since assets are already in the system for SIEM, it's great to be able to immediately run an scan on a single device, a group of devices, a specific network, or the entire organization. It also gives you the ability to run a lighter scan or a deeper scan."

Manager Information Technology
Retail Industry
1,001-5,000 employees
October 2015

"The vulnerability scanner provides solid and little known information about assets."

Chris Niesen
Security Services Manager, The Tech Outfit,
1-10 employees
December 2015

6. Product deployment

AlienVault USM is considered by reviewers to be exceptionally straightforward and fast to deploy, with a very short time-to-value.

"As far as setting up the product for log collection, it's fairly straightforward and relatively painless. After walking through the setup wizard for the main appliance, pushing out the agents to all your windows devices is quick and easy. Some tweaking needs to be done once deployed, but overall the process is better than what I have experienced in the past with prior companies."

Manager Information Technology
Retail Industry
1,001-5,000 employees
October 2015

"The product also provides an easy to use getting started wizard on setup that allows users using an all-in-one version of the product to quickly get a running start on getting deployed and monitoring their assets."

Engineer in Professional Services
Computer and Network Security
11-50 employees
November 2015

"We completed the installation of AlienVault USM in the corporate environment through telephone consultations within a short time of 2-3 weeks."

Валерий Ткаченко
Chief Information Security Officer, Oil and Energy Industry
1,0001-5,000 employees
November 2015

"It is really easy to deploy, which allows us to show value to our customers right away."

C-Level Executive in IT
Chemical Industry
10,000+ employees
November 2015

7. Access to command line interface

Several of the more technical users commented on the fact that they appreciate having access to the Linux command line, which is useful when the UI has limitations.

"Complete access to the underlying OS. I am not particularly fond of products that limit access to all aspects of the product. It is one thing to have proprietary code it is another to limit root or admin access to a box your company paid for. In AlienVault you can get into the command line anytime you want (it is built on a Linux OS). If you need to do some troubleshooting with which the UI is simply not sufficient, you can!"

Administrator in Information Technology, Retail Industry,
10,000+ employees
September 2015

USM is quite open, and you are pretty free to do what you want by using the command line (although that's less and less supported by AlienVault, which is a pity)."

Koen Vanhees, Security Engineer
Cegeka, Information Technology and Services
1,001-5,000 employees
September 2015

Areas for Improvement

1. Data Plug-ins

The most frequent area highlighted for improvement is that of data plug-ins. Data is transmitted from devices via plug-ins, many of which are pre-built. Building customized plug-ins however is more difficult than some would like.

> **"I do not like dealing with the plugins for data. Some of this could be merely my lack of ability in log reading and writing filters but the feature I want to see most improved is how you use plugins within AlienVault. It can definitely be streamlined and made user-friendly. I buy tools like this so I do not have to write my own correlation rules and log interpretation filters. It is certainly usable but kind of clunky."**

Administrator in Information Technology
Retail Industry
10,000+ employees
September 2015

> **"Building customized plugins for systems that do not already have plugins is very daunting. Some tool to help with analyzing the data from new log sources and helping to build the new plugin would be great."**

Mayson Morrissey
Senior Information Systems Administrator
City of Covington
201-5500 employees
September 2015

> **"Plugins for data could use some improvements. Newer plugins and a more user-friendly way of creating them rather than writing regex would greatly improve the ability to add additional data sources."**

Manager Information Technology
Computer Software Industry
51-200 employees
September 2015

> **"Plugins are limited (although they are adding more as time goes on). If you need a plugin that is not available you will need to create one on your own which requires modification of a number of files and can be daunting for someone new to the platform."**

Farakh Hussain
Manager Information Security, PriceMetrix
51-200 employees
December 2015

2. Documentation

The lack of complete documentation can be an obstacle, although support and user forums are helpful. And, a newly rolled out documentation center will also help customers better self-serve.

> **"AlienVault's documentation is poor. Taking their one-week Security Analyst and Security Engineer certification training helped since the course documentation was more concise and centralized than anything I could find online."**

Director, Information Technology
Banking Industry
201-500 employees
September 2015

> **"As a young company, the documentation and support knowledgebase are still not completed and they can improve it in order to make an even better product."**

Engineer in Telecommunications Industry
5,001-10,000 employees
November 2015

> **"Documentation can be improved. The knowledge base and help are being redone and they have yet to catch up to the latest version. They provide some help but need to add detail for advanced trouble-shooting. Forums can sometimes be helpful and the support also is helpful."**

Manager, Information Technology
Computer Software Industry
51-200 employees
September 2015

> **"Comprehensive online up-to-date manuals to help in configuration of systems and known issues. Whilst the community is great there can be a lot of confusion about what is best."**

Barry Stephenson, Information Security Officer
McCurragh, Consumer Goods Industry
1,001-5,000 employees
November 2015

3. System Updates

System updates and patches tend to be inadequately tested and can cause problems.

> **"Application of updates to the platform - with lots of moving pieces, and the myriad of Linux dependencies, upgrades could be made a bit less burdensome for administrators."**

Manager in Information Technology
IT and Services
501-1,000 employees
November 2015

> **"Upgrade to new major releases is poorly QA'ed and tested introducing new bugs that should have been caught in the QA process which has brought down customer production equipment."**

Alissa Knight, Managing Partner
Brier & Thorn UK, Computer & Network Security
11-50 employees
November 2015

> **"New versions appear to be released without the extensive testing expected from more mainstream closed source products. Using the product to its fullest will result in frustration with bugs and some components which flat out don't work as intended. The interface and functionality provided lacks 'polish'."**

Director, Information Technology
Oil and Gas Industry
1,001-5,000 employees
December 2015

> **"Upgrading to the newest revision is painful and fraught with peril. We recently upgraded and then had to rebuild the entire system."**

Manager, Information Technology
Telecommunications Industry
201-500 employees
December 2015

4. Reporting

Some users are unhappy with reporting capabilities, and struggle particularly with building custom reports.

> **"There are a ton of built-in reports, however there is not a lot of guidance available on building customized reports, and the tools are not as robust as I would like."**

Mel Green
Network Security Manager, PHE
201-500 employees
October 2015

> **"Some of the reports aren't applicable depending on the information being collected and the canned reports can have gaps. There's a good base of content to do custom reports, but other products seem to do reporting better and more coherently out of the box."**

Partner in Professional Services
Information Technology and Services
1-10 employees
December 2015

> **"Reporting is flexible, but more advanced grouping and customization options are desired."**

Engineer in Telecommunications Industry
5,001-10,000 employees
November 2015

However, some users are quite happy with current reporting capabilities:

> **"The automated reporting and report distribution has been extremely useful, allowing us to schedule reports on things like asset updates, discovered vulnerabilities and systems being attacked. We automate these reports and distribute them by mail without additional intervention."**

Derick Burton
Group Security Operations Manager, Digicel Group
Telecommunications
September 2015

> **"Reporting is very good; it has variety and huge options to choose from, though the output format has potential to improve."**

Vishal Jadhav, Information Security & Pre-Sales Officer
Hemisphere Technologies
11-50 employees
November 2015

AlienVault USM Threat Detection: Effectiveness and Simplification

TrustRadius asked reviewers of AlienVault USM two additional questions about effectiveness and simplification. Firstly "When compared to other security technology, how effective is AlienVault USM in helping detect real security threats?" Secondly, "Has AlienVault USM reduced the amount of work you need to do to detect threats?"

The answers to both of these questions were generally that the platform is highly effective at threat detection, and also simplifies the amount of work required to detect threats, although some reviewers said that they needed more time before being certain. Here is a sampling of answers to those two questions:

Effectiveness

The most frequent area highlighted for improvement is that of data plug-ins. Data is transmitted from devices via plug-ins, many of which are pre-built. Building customized plug-ins however is more difficult than some would like.

"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. It has also reported a number of vulnerabilities we did not know we had, and in some cases helped us to trouble shoot bad settings, and faulty programs by showing us the suspicious activity. It looks at activity and behavior, not just comparing programs to a list of known viruses."

Greg Baugh
VP Data Processing, Peoples National Bank
11-50 employees
November 2015

"It's pretty good, like I said; it catches that 60-70% of the bell curve of threat activity. Not everything, but pretty good."

Aaron Baillio, Security Architecture and Operations Lead
University of Oklahoma, 5,001-10,000 employees
November 2015

"The IDS function in AlienVault in particular has helped us find quite a number of issues that we have had to deal with. The very nature of the tool is to monitor your environment and report on potential issues. As a SIEM (plus many other things) it tends to be one of the first indicators of compromise or some other security issue. In addition to that the range of tools within AlienVault has given us a lot of visibility that we did not have before."

Administrator
Information Technology, Retail Industry
10,000+ employees
September 2015

"AlienVault USM has been very effective in helping to spot several threats in our environment. AV was able to spot a potential DLP event recently, which was not noticed on our Mail Gateway. AlienVault has also spotted C&C activity."

Director Information Technology
Banking Industry
201-500 employees
September 2015

"AlienVault has allowed us to see warnings that have been hidden deep within our network. The number of resources we would have required to effectively sort through logs would have exceeded the cost of what the AlienVault system is capable of accomplishing in a single device. It allows us to detect trends and check our traffic with currently known ongoing attacks."

Administrator
Information Technology, Hospital & Health Care
11-50 employees
December 2015

Simplification/ Work Timesavings

"We are new to AlienVault but the little we have seen it do is remarkable. Instead of going through the system's device logs, you can easily access the logs and all the issues relating to the devices with just a click. It has reduced the amount of time we spent investigating issues on our network devices."

Augustine Oteng Brobbey
Network and Systems Engineer, Genteq Systems
December 2015

"I believe our organization has greatly reduced the amount of work it would traditionally take us to identify security threats. Between the USM's vulnerability scanning, traffic monitoring, and HIDS capabilities along with the syslog information from our firewalls on our perimeter, it aggregates all the data into an easy to read format and you can find it all in one place."

Michael Eller, Junior System Administrator
Puget Sound Surgical Center
51-200 employees
November 2015

"Using AlienVault has resulted in reduced effort to detect and manage threats. The SEIM component means we are no longer responding to every IDS alert and have spent for less time tuning the signatures as the SEIM component does enough analysis in most instances to provide real value."

Derick Burton, Group Security Operations Manager,
Digicel Group, Telecommunications
September 2015

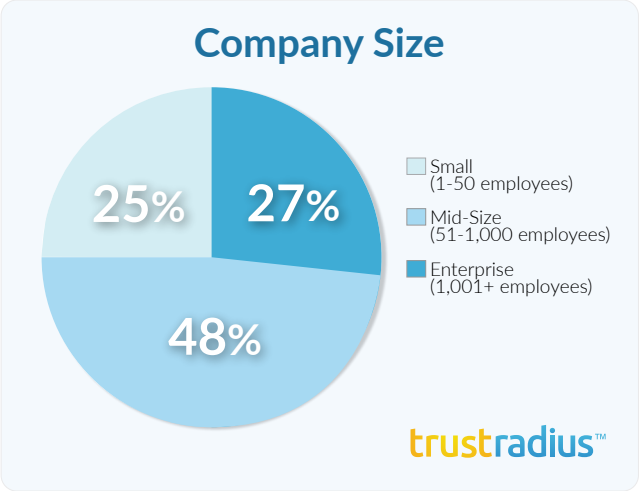
"Yes, AlienVault Unified Security Management not only has a very minimum entry barrier but it's also very effective and you don't need a large team to operate it. Even the casual IT guy can make best use of it with a few days of training."

Analyst, Information Technology and Services
201-500 employeess
November 2015

AlienVault USM Customer Demographics

AlienVault's target market is primarily mid-sized organizations. Small and medium organizations make up 52% of the reviews on TrustRadius. However, a sizeable 27% of reviewers actually belong to enterprises with over 1,000 employees, indicating that the AlienVault value proposition is also attractive to larger organizations. The breakdown of ratings by company size however does reveal stronger ratings from mid-sized companies.

Reviewer's comments tend to support the view that the platform is flexible enough to support a broad range of organizations from small to very large, although some feel that the sweet spot is mid-sized to large organizations, rather than very large enterprises.



"AlienVault excels in a small to medium sized environment and it packs a lot of value into its footprint. I recommend it almost every day to clients. It is an excellent place to start the security journey."

Aaron S. Moffet
Senior Information Security Consultant, VioPoint
11-50 employees
November 2015

"Small offices with no web facing assets may not be the most ideal candidates for the USM platform. I would imagine this is best suitable for a medium to large sized business with at least one if not several web facing assets."

Michael Eller, Junior System Administrator
Puget Sound Surgical Center
51-200 employees
November 2015

"Cost and complexity are always concerns, but if you buy the right package and deploy it correctly it can cover any environment. There are simple deployments, complex deployments, and even managed deployments. It can cover your needs if setup correctly."

Greg Baugh
VP Data Processing, Peoples National Bank
11-50 employees
November 2015

"AlienVault Unified Security is too expensive for small operations and not scalable enough for very large operations. I would recommend this for companies that have maybe five thousand hosts at most, and no less than a few hundred."

Jacob Lovell
IT Security Analyst Associate
University of Georgia, Information Technology and Services
10,000+ employees
December 2015

"Because of its flexibility, and its ability to be deployed in a distributed manner, the platform is very scalable and can be used anywhere, from very small environments, to large enterprises. However, we have found that for very small companies the cost can be prohibitive if an appliance needs to be deployed."

Mike Kerem
CTO, TrustNet
Information Technology and Services
11-50 employees
October 2015

"AlienVault Unified Security Management is a perfect system for small to medium-sized deployments. I could see some challenges with larger deployments that would require additional time and effort to get it functioning appropriately, but it definitely can be done."

Farakh Hussain
Manager Information Security, PriceMetrix
51-200 employees
December 2015

AlienVault Company and Product Deployment Details

Company Status	Private
Founded	2007
Headquarters	San Mateo CA
Customers	Over 3,000 commercial customers
Customer Verticals	Automotive, Chemical, Consumer Products, Education, Energy / Utilities, Financial Services, Government, Health Care, Law Practice / Legal Support, Manufacturing, Retail, Technology / IT Services / Service Provider, Telecommunications, Transportation, Gaming
Employees on LinkedIn	227

Architecture and Deployment Options

The AlienVault USM platform can be deployed in a number of ways. It can be deployed as a single virtual or hardware appliance. There are three components to the USM platform: USM Sensor, USM Server, and USM Logger. You can deploy them as separate components (in any combination of hardware and virtual appliances) or as an All-in-One device (with each of these components combined into a single system).

- The Sensor is responsible for data collection and performs asset discovery and vulnerability assessment scans as well as network-based intrusion detection systems (Host IDS requires the installation of a lightweight sensor on individual systems). Multiple Sensors can be deployed across locations.
- All data collected by the sensor is forwarded to the Server for analysis and reporting.
- The Logger retains core log data to meet long-term retention requirements.

For those who already have an Amazon Web Services cloud infrastructure, a version of the AlienVault USM for AWS is also available. The architecture consists of Sensor Nodes reporting into a Control Node.

Pricing

The USM All-in-One virtual appliance pricing starts at $5,050, and the All-in-One hardware appliance starts at $14,000. Sensors, servers and loggers can be purchased separately as well. A subscription to the AlienVault Labs threat intelligence updates is included in the first year purchase price, along with support and training. Professional services have an additional cost.

Interview with AlienVault CEO, Barmak Meftah

2015 was a great year for AlienVault, what drove that momentum?

Yes, 2015 was a record year for us. In fact, our past four years have been record years, which is very encouraging. We currently have 3,000 commercial customers, who rely on our platform for threat detection; and 285 MSSP partners who wrap their services around our product.

The main reason for this success is two-fold. Firstly, our approach to threat detection and threat response is unique: we have a unified and simplified approach to how we help organizations of all sizes. We combine all the core security controls together with expert threat intelligence from our labs team and Open Threat Exchange, which reduces the cost and complexity of threat detection.

The other thing is the sheer size of the addressable market. We're going after companies of any size: They can be small companies or big companies, but they share common attributes - their security organizations are typically small; there is a lack of security expertise and a lack of funds for expensive point solutions. That market is pretty big and largely untapped. Those organizations really need simple, unified solutions for threat detection and response. I don't think the security concerns of organizations have changed significantly; however, the cybersecurity skills shortage is on the rise. As more organizations struggle with the challenges of hiring and retaining staff, as well as the complexity of deploying and managing multiple products, we've seen a surge in both end user customers and MSSP partners deploying USM.

The original market you serviced was largely the SMB, but I think you are now starting to sell to much larger organizations as well. Is the product equally appealing to large companies?

I would characterize our target market as being the mid-market which is a little different to SMB. However, we do go after SMB's too. The reality is that we provide a solution for

any size organization that lacks the security resources to implement and manage a threat detection strategy. We have hundreds if not thousands of very large customers, but they have small security organizations or limited resources to address their threat detection needs.

Having said that, I think your observation is spot on. As our brand recognition is increasing, and our approach to threat detection is getting more traction, we are getting pulled up-market so we are seeing increased numbers of larger deals. What's great about it is that we sell the same product, AlienVault USM, to smaller companies that we sell to larger companies. However, the larger companies need more of our products because the size of their IT assets is much larger than the typical smaller company. Our USM platform can be collapsed into a very small form-factor or it can scale out horizontally to a very large company that can also enjoy that all-in-one approach to threat management and threat detection. We also offer a lot of deployment flexibility since the USM platform is available as a virtual, physical and cloud appliance.

How are you approaching threat detection differently than other vendors?

There are three main things that differentiate us from some of the other vendors that have been in the market for a while.

The first thing is that, in general, our approach to security visibility and threat management is more of a "let's solve the business problem" approach, rather than "let's focus on the technology point product". In our addressable market, the ability to consume a form factor that is less complicated and has a lot of security controls that are already orchestrated in a unified security management platform is an absolute must.

From my experience of being in this market for a long time, if you want to sell into this segment, selling point products and then expecting the end user to hire an expensive system integrator to glue those point products together doesn't work. It's very expensive – it doesn't fit their CapEx and OpEx budgets. But more importantly, there is an inherent lack of expertise in these organizations where they are not able to ingest all the data and orchestrate all these security controls on their own. We've taken a very unique approach to threat detection and threat management by providing an integrated security platform that delivers all the core security capabilities required for threat detection.

The second key strength is that we have an integrated threat intelligence platform. As you know, when you think about security, there are three components to it. There's the automation platform, so the first thing we did was simplify the automation platform by bundling a lot of these point solutions under a unified security management platform. The second thing in security is content. The security controls don't know what to do if they're not provided a rich set of threat data. We have a very integrated approach to that threat intelligence. The threat data and threat intelligence that we have includes correlation rules, intrusion signatures, and threat vectors, which are all fed into our USM platform whether it be virtual, physical, or in the cloud, in a fully automated fashion.

That exponentially reduces the complexity of ingesting threat intelligence.

The third differentiator that we have is the way we gather that threat data. We leverage a crowd-sourced approach to threat data sharing through our Open Threat Exchange, which enables security practitioners to openly research and collaborate on emerging threats. This is a product unto itself that we launched three years ago and, in a very short amount of time, it's gotten a lot of traction around the globe, in more than 140 countries. And, we have a very rich partner ecosystem supporting the Open Threat Exchange including big security companies, HP and Intel, and several small vendors. What we do is crowd-source threat data; everybody in the community contributes their threat data and, in return, they get access to everybody else's threat data. We anonymize it so there's no attribution back to whoever submitted that threat data, to protect their identity. That allows for a very disaggregated, crowd-sourced, open and collaborative way to get threat intelligence from around the world from actual victims of breaches, which is invaluable. One of the benefits we provide to our customers, is that we synthesize that threat data, write correlation rules and directives and provide those automatically to our unified security management platform – a service that no other vendor provides it's customers.

So, the combination of a simplified security management platform, automated threat intelligence feeds, and our community-sourced threat data gives us a very unique advantage to go after that under-resourced market. If you look at the Gartner Magic Quadrant, we are the only company positioned in the "Visionary" quadrant and that is because of the combination of those three differentiators.

Do customers buy AlienVault primarily to improve network security, or to meet compliance requirements like PCI DSS? How important a requirement is compliance?

It's a bit of both, and it really depends on two vectors. It depends on the vertical industry that the company is in, and the compliance requirements that have been imposed on them. It also depends on the size of company and the maturity of the organization in their approach to threat detection. In fact, when we survey newly acquired customers and ask them why they bought our platform, the three common answers that come back are threat detection, security visibility, and compliance.

We have a very horizontal sell in that we care about the size of your security organization. If you look at our customers in the different vertical industries like banking, credit unions, ecommerce, electronic retailers; these are people that typically have a very heavy PCI compliance requirement, and healthcare also has HIPAA compliance, etc. The main driver then starts with, "I need to comply with PCI". They start there, but then realize they can use the same product for threat management. If you look at other industries that are not heavily regulated, they are more interested in being proactive with threat management to protect their brand. So it really depends on the industry. The good news is wherever the company decides to start; there is no reason to only buy the product for compliance or threat management, as it can handle both.

Following some very public data breaches, security issues are increasingly recognized as a significant risk factor for organizations. Is security a C-level issue now, or is it still primarily an IT concern?

It's definitely becoming more of a boardroom issue and that's been the case for the past three or four years. In fact, I sit on many industry forum panels, and this is a pretty big conversation; the role of information security in general, and then, more specifically, the role of the CISO is getting elevated dramatically. If you compare where the industry has been the last 5-10 years, to where it is right now, there is an amplification of the role of security, and that topic is definitely discussed in the boardroom.

In much the same way that companies care about their risk profile in doing business, I think the information risk or cyber risk is getting elevated, and is being talked as about as a component of the overall risk to the business, which is a great thing. That's increasing the awareness and accentuating the amount of financial and human capital resources that should be available for information security quite a bit. Having said that, there is still a heavy shortage of information security expertise out there and, if you look into our addressable market, if you exclude the Fortune 500 where the security organizations are very big and have a lot of financial and human capital available to them, the vast majority of the market still suffers from a lack of security information expertise and a lack of financial affordability. So although the role of information security is getting elevated, there is still a big shortage of expertise and thus there is a need to simplify threat detection and threat response in the addressable market that we go after.

What are some of the third-party endorsements you have received?

We're always honored when somebody recognizes AlienVault for what we stand for, and we've been fortunate enough to win several awards recently. We were named to Deloitte's 2015 "Technology Fast 500" list of the fastest-growing companies in North America. And, we were also named to Forbes' list of hottest cybersecurity startups and ranked third in the Cybersecurity 500 List of Companies to Watch in 2015, which is a great honor. We've also been recognized by SC Magazine, European IT & Software Excellence, and Computing Security. And, of course, we were again placed in the Visionary quadrant for Gartner's SIEM Magic Quadrant.

What's great is that a lot of these awards corroborate the vision that we have, and the approach that we take and that's great to see. As an entrepreneur when you start a company you always have a hypothesis around the product and what the product does, and how you want to go to market. But, until the market validates it, you really don't know that you're at the right place, and you feel really good that the fit is the right one for the market we're going after.

What's on the roadmap for AlienVault in 2016?

A couple of things: We're a very customer-centric organization and the customer experience is something that is built into the DNA of the company. We have an inherent

belief that we can build the best products out there, but if those products aren't being enjoyed by our customers or our partner ecosystem, we haven't really made that much of a stride. So we constantly send surveys out to our customers and we keep an open ear to what they're telling us and incorporate that into our roadmap.

They are going to be some immediate tactical enhancements in the product as a result of us listening to our customers and partner ecosystem. In the near term, documentation is going to be improved dramatically; we're also going to put a lot more emphasis on our support organization; and our 3rd-party components are going to be enhanced. I think we have a very good and extensible way to integrate 3rd-party components, but this integration is going to be enhanced. The good news is that a lot of the core capabilities of our product are being enjoyed by our customers so the results of our most recent survey were very encouraging and confirmed the core features around intrusion detection and threat intelligence are working very well.

In the broader horizon, our development team has been working on some really exciting advances for our USM platform that we hope to announce later in 2016. There are some key developments around extensibility, scalability and more ease-of-use features in the product. What we want to do is provide a comprehensive security management platform that is easy to deploy, and easy to consume, but at the same time delivers improved scalability. We're also making our platform more extensible so that other 3rd-party security controls can be built on top of our platform. That's all on the innovation side.

On the go-to-market side we are going to concentrate on leveraging our channel ecosystem. We are at a size now where the channel provides big operating leverage for us, and we want to go after that pretty aggressively. We've hired a very able channel executive, who will own the entire channel ecosystem, so there will be a big emphasis on how we use the channel as an extension to our field to accelerate growth and meet the needs of our customers even more.