SIEM

Security Information and Event Management (SIEM)

Buyer's Guide and Reviews

October 2018

IT Central Station
Unbiased reviews from the tech community

Get a custom version of this report...personalized for you!

Thanks for downloading this IT Central Station report.

Note that this is a generic report based on reviews and opinions from the entire IT Central Station community. We offer a customized report personalized for you based on:

- Your industry
- Company size
- Which solutions you're already considering

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

Get your personalized report here.

Contents

© 2018 IT Central Station

Vendor Directory

AlienVault	AlienVault
Centrify	Centrify Analytics Services
Exabeam	Exabeam
FireEye	FireEye Threat Analytics
Fortinet	Fortinet FortiSIEM (AccelOps)
IBM	IBM QRadar
IBM	IBM Watson for Cyber Security
Ignite Technologies	SenSage SIEM
Intersect Alliance	Snare
Interset	Interset
IS Decisions	FileAudit
JASK	JASK
LogPoint	LogPoint
LogRhythm	LogRhythm NextGen SIEM
Logsign	Logsign
ManageEngine	ManageEngine Log360
ManageEngine	ManageEngine EventLog Analyzer
Masergy	Masergy
McAfee	McAfee Enterprise Security Manager (McAfee ESM)
Micro Focus	ArcSight
Micro Focus	NetIQ Sentinel
NETMONASTERY	DNIF
Netsurion	EventTracker
NNT	NNT Log Tracker Enterprise
Oracle	Oracle Security Monitoring and Analytics Cloud Service
Rapid7	InsightIDR
RSA	RSA NetWitness Logs and Packets (RSA SIEM)
RSA	RSA enVision
Securonix Solutions	Securonix Security Analytics
Sematext	Sematext Logsene
SolarWinds	SolarWinds LEM
SolarWinds	SolarWinds MSP Threat Monitor
Splunk	Splunk
SQRRL	SQRRL
SurfWatch Labs	SurfWatch Labs SurfWatch
ThetaRay	ThetaRay
TIBCO	LogLogic
Trustwave	Trustwave SIEM

© 2018 IT Central Station

Top Security Information and Event Management (SIEM) Solutions

Over 293,539 professionals have used IT Central Station research. Here are the top Security Information and Event Management (SIEM) vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

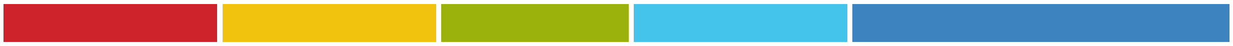
Chart Key

● **Views**	● **Comparisons**	● **Reviews**	● **Followers**	● **Average Rating**
Number of views	Number of times compared to another product	Total number of reviews on IT Central Station	Number of followers on IT Central Station	Average rating based on reviews

Bar length

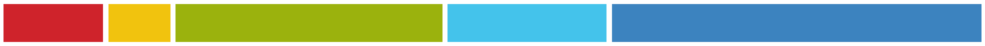
The total ranking of a product, represented by the bar length, is based on a weighted aggregate score. The score is calculated as follows: The product with the highest count in each area gets the highest available score. (20 points for **Reviews**; 16 points for **Views**, **Comparisons**, and **Followers**.) Every other product gets assigned points based on its total in proportion to the #1 product in that area. For example, if a product has 80% of the number of reviews compared to the product with the most reviews then the product's score for reviews would be 20% (weighting factor) * 80% = 16. For **Average Rating**, the maximum score is 32 points awarded linearly based on our rating scale of 1-10. If a product has fewer than ten reviews, the point contribution for Average Rating is reduced (one-third reduction in points for products with 5-9 reviews; two-thirds reduction for products with fewer than five reviews). Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

1 Splunk



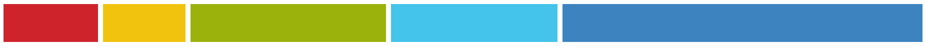
103,815 views **67,086** comparisons **47** reviews **2,787** followers **8.8** average rating

2 LogRhythm NextGen SIEM



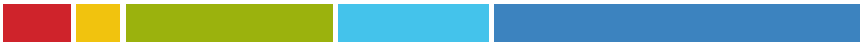
48,405 views **19,496** comparisons **67** reviews **2,074** followers **8.7** average rating

3 IBM QRadar



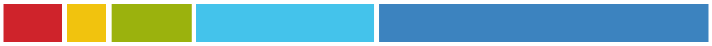
45,751 views **25,922** comparisons **49** reviews **2,173** followers **8.4** average rating

4 AlienVault



32,754 views **13,921** comparisons **52** reviews **1,974** followers **8.6** average rating

5 ArcSight



28,357 views **12,234** comparisons **20** reviews **2,320** followers **7.7** average rating

© 2018 IT Central Station

6 McAfee Enterprise Security Manager (McAfee ESM)

9,257 views **5,201** comparisons **5** reviews **250** followers **7.6** average rating

7 InsightIDR

1,798 views **679** comparisons **5** reviews **111** followers **9.0** average rating

8 SolarWinds LEM

11,711 views **6,212** comparisons **1** reviews **454** followers **9.0** average rating

9 RSA NetWitness Logs and Packets (RSA SIEM)

7,689 views **4,192** comparisons **3** reviews **570** followers **7.7** average rating

10 Fortinet FortiSIEM (AccelOps)

16,094 views **7,470** comparisons **4** reviews **373** followers **6.0** average rating

© 2018 IT Central Station

Top Solutions by Ranking Factor

● Views

SOLUTION		VIEWS
1	**Splunk**	103,815
2	**LogRhythm NextGen SIEM**	48,405
3	**IBM QRadar**	45,751
4	**AlienVault**	32,754
5	**ArcSight**	28,357

● Reviews

SOLUTION		REVIEWS
1	**LogRhythm NextGen SIEM**	67
2	**AlienVault**	52
3	**IBM QRadar**	49
4	**Splunk**	47
5	**ArcSight**	20

● Followers

SOLUTION		FOLLOWERS
1	**Splunk**	2,787
2	**ArcSight**	2,320
3	**IBM QRadar**	2,173
4	**LogRhythm NextGen SIEM**	2,074
5	**AlienVault**	1,974

© 2018 IT Central Station

Splunk

See 47 reviews >>

Overview

Splunk software has been around since 2006 and the company has since grown to become an industry leader. Splunk's vision is to make machine data accessible, usable and valuable to everybody. The company offers a wide range of products to turn machine data into valuable information by monitoring and analyzing all activities. This is known as Operational Intelligence and is the unique value proposition of Splunk.Splunk is well-known for its Log Management capabilities and also for its Security Information and Event Management (SIEM) solutions.

SAMPLE CUSTOMERS

Splunk has more than 7,000 customers spread across over 90 countries. These customers include Telenor, UniCredit, ideeli, McKenney's, Tesco, and SurveyMonkey.

TOP COMPARISONS

IBM QRadar vs. Splunk ... Compared 19% of the time [See comparison]
LogRhythm NextGen SIEM vs. Splunk ... Compared 13% of the time [See comparison]
ArcSight vs. Splunk ... Compared 8% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 17%
Comms Service Provider ... 10%
Energy/Utilities Company ... 7%
Manufacturing Company ... 6%

COMPANY SIZE

1-200 Employees ... 14%
201-1000 Employees ... 19%
1001+ Employees ... 67%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 21%
Retailer ... 15%
Energy/Utilities Company ... 12%
University ... 9%

COMPANY SIZE

1-200 Employees ... 21%
201-1000 Employees ... 13%
1001+ Employees ... 66%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Splunk

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Colt Rodgers

The ability to view all of these different logs, then drilling down into specific times or into specific data sources, has proved to be the greatest aspect in decreasing our troubleshooting overhead time. The added security has proven effective as well, but given that we have not yet created the perfect model, we still find ourselves striving to develop a more efficient and predictive security analysis and action plan within Splunk. [Full Review]

david hourani

Splunk can be seen as a huge box that allows the storage of all sorts of logs. This allows the centralization of data and makes possible new sorts of correlations that were previously impossible using traditional SIEMs such as ArcSight or QRadar. Splunk allow schema on the fly and therefore simplifies all the data onboarding process. All that leads to flexibility when it comes to defining the metadata since it is not necessary to have all the fields defined and extracted to be able to use Splunk. Another great feature is the field extractor that all... [Full Review]

Kent Farries

There are too many features to list, but here are a few: * Schema on the fly * Ease of on-boarding data * Machine learning * Apps or Splunk base. * Great list of apps to use and also build upon once you learn more about how Splunk works. * We build many of our own apps by leveraging the logic in the others. * Ease of correlation, creating correlation searches are easy and you can combine multiple sources with little effort * Data Models Acceleration for super fast searches across tens of millions of events * Common Information Model * Security Essen... [Full Review]

Joshua Biggley

Splunk has a single purpose in life: ingest machine data and help analyze and visualize that data. The breadth of the data sources that Splunk can ingest data from is broad and deep and it does an exemplary job at handling structured data. It does a great job at handling unstructured data. Breaking data into key/value pairs so that it can be searched is relatively painless. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Colt Rodgers

Splunk has helped our organization mainly on our increased use of the security side. We use Splunk to monitor all machine logins (both successful and unsuccessful) and actions taken on those machines under each user. We have set up some predictive and proactive models, which are programmed to take action on anything outside of the normal usage. These actions range from alerts being sent to the Splunk page, administrators being notified, and if escalated enough, automatic account locks. [Full Review]

david hourani

Splunk helped reduce development cost since it provides free applications on Splunkbase that can save a huge amount of time and effort. It also gave us the ability to dig into logs to find not just one needle but many needles in the haystack of data, and that helped solve multiple production issues and reduced system downtime. A great improvement brought by Splunk is the ability to remove sensitive data before displaying it in reports. This allows Splunk administrators to filter data according to the user's clearance level. [Full Review]

Gregg Woodcock

Out clients went from unhappy using inflexible, poorly-supported products. Not only are they able to do their security jobs and investigations, but they are also easily able to modify and evolve their implementations themselves to keep up with the shifting sands, which is the SecOps landscape. [Full Review]

© 2018 IT Central Station

Splunk

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Colt Rodgers

Splunk has continually been increasing its features and also expanding and perfecting its core functionality. I would like to see it to continue to improve its predictive analytics and machine learning tools. It is not to be said that they are currently lacking, I don't believe it is, but given the current state and direction of the Information Technology world, I feel as though a major focus of upcoming releases should be set on Machine Learning, Predictive Analytics, and I would enjoy to see more security focused add-ons and apps developed by the ... [Full Review]

david hourani

Adding custom visualization in Splunk has been improved over the years but can still be made better by integrating more and more JavaScript visualization sources. [Full Review]

Gregg Woodcock

* It needs integration with a configuration management solution. * It could use better password management for forwarders. * It needs a better way to export dynamic views without requiring a ton of code and user/pw. [Full Review]

Paul Gilowey

Official training, even CBT, is expensive so not many people are able to get certified. This leads/causes the users to make use of the most basic functionality only. It is a challenge to manage the environment in such a way, that one's log, even with the bandwidth license, isn't exceeded. Splunk has moved towards not applying hard caps in data ingestion, and this will help us in the future. However, I'd like an easier way to flag certain source log files as non-critical and have Splunk automatically disable those event sources when the license capac... [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Colt Rodgers

Setup cost is cheap: It is free, it is user-friendly, and it is fast. I would highly recommend anyone evaluating this option to download the free trial which allows for the ingestion of 500MB of data per day in order to get a feel for what Splunk does at its core. It will get pricey once your ingestion rates start to sky rocket, but I would consider it expensive given the amount of information that it allows you to analyze and react on straight out-of-the-box. [Full Review]

david hourani

Splunk licensing model might seem expensive but with all the gain in functionalities you will have compared to traditional SIEM solutions I think it's worth the price. Also, when you have small volumes of data to index daily (which might account for high EPS) you will be gaining the full advantage of using Splunk for a very low price. [Full Review]

Gregg Woodcock

Get free PS if you can (ask) or USE THE DOCS. The documentation will get you to success. If you are not getting more value out of Splunk than the license you are paying, then you are doing something wrong and should spend a tiny bit more to get a consultant like Splunxter.com to help you. [Full Review]

LogRhythm NextGen SIEM

See 67 reviews >>

Overview

LogRhythm, a leader in security intelligence and analytics, empowers organizations with it's Threat Lifecycle Management Platform, which provides a complete, end-to-end workflow for detecting, investigating and responding to cyber threats.

The company’s award-winning platform unifies next-generation SIEM, log management, network/endpoint forensics, and advanced security analytics.

In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence.

SAMPLE CUSTOMERS

Macy's, NASA, Fujitsu, US Air Force, EY, Abbott, HD Supply, SAB Miller, UCLA, Raytheon, Amtrak, Cargill

TOP COMPARISONS

Splunk vs. LogRhythm NextGen SIEM ... Compared 47% of the time [See comparison]
IBM QRadar vs. LogRhythm NextGen SIEM ... Compared 14% of the time [See comparison]
AlienVault vs. LogRhythm NextGen SIEM ... Compared 12% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 20%
Comms Service Provider ... 9%
Healthcare Company ... 7%
Manufacturing Company ... 6%

COMPANY SIZE

1-200 Employees ... 18%
201-1000 Employees ... 25%
1001+ Employees ... 57%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 33%
Energy/Utilities Company ... 10%
Healthcare Company ... 8%
Manufacturing Company ... 8%

COMPANY SIZE

1-200 Employees ... 9%
201-1000 Employees ... 25%
1001+ Employees ... 65%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

LogRhythm NextGen SIEM

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Reno Thomas

Provides visibility into the network. We got it for PCI compliance for the most part, and we also do SOC 1 and SOC 2 compliance, so we can show that we're secure to our clients. We have a lot of financial and other customers that care about security with the kind of business that we do. But we're looking at it to do SOC Light, not 24/7, but we want have a visibility into everything that is going on in our network, be able to respond, and do incident response using LogRhythm as our main console. [Full Review]

Jack Callaghan

The breadth and harvesting of information the SIEM is capable of doing. I've been in this probably going on 30 years, and I've seen the growth. I found a resource that's outstanding in finding information and then the most important thing, distilling it, putting it together, which is a real big challenge in this field. [Full Review]

Aaron Mueller

The PCI compliance pieces that help us produce reports for our external auditor, and their support. I constantly sing the praises of their support group. It's a complicated, vast product with a lot of breadth and depth. Things go wrong. But when I have a problem their support group will get a hold of me within minutes to hours, at the most. If it takes a group of people to solve the problem they pull a group of people together. They will create remote sessions. I don't have any other vendors with the same level of support that LogRhythm does. [Full Review]

Kevin Merolla

The ability for me to go into the Web UI, and just learn what's going on in my environment. Being able to go in and show our company's management, "Look, this is what we can see. This is what we can now know about our environment." Then, using the past several months to baseline what's normal, it has been invaluable, and we have also been able to stop things that were bad, at the same time. We were able to actually show value, while we were still building out the solution. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Reno Thomas

It takes good log sources. We have investments in endpoint protection and Mail Gateway, and our firewalls are going to be catching up soon. To have all the logs centralized, we haven't had that before across the enterprise. We had it logging at one or two locations, but this is the first time this year that we actually had all the logs go to one spot and be able to have alerts and alarms set up. We use CrowdStrike as our endpoint, so we are in the process of getting those logs into the SIEM and we haven't got that done yet, but that's going to be a ... [Full Review]

Jack Callaghan

We're a financial service. As our title implies we deal in mortgages, which means we see a lot of personal information, credit reports, financial instruments. We're really concerned that we are able to monitor the movement of that kind of information and protect it. LogRhythm has been extremely efficient in helping us find the bad guys, who are really out there, they're targeting businesses like us. They specifically want the findings, the money. If you can get in the middle of a loan you may have to go after 10,000 people trying to find the data, b... [Full Review]

Aaron Mueller

Absolutely. It has helped us gain visibility into events that we didn't have before at all. We have a lot of remote locations. We manage national parks and point-of-sale devices on ships, at the top of mountains and little cabins, gas stations in the middle of Death Valley; we have a lot of difficulty around trying to keep an eye on things, and LogRhythm lets us have agents running almost anywhere we want. It also has provided us ways to do compensating controls for systems that we couldn't otherwise secure, because of different product upgrade path... [Full Review]

© 2018 IT Central Station

LogRhythm NextGen SIEM

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Reno Thomas

Our key challenge is working with disparate IT groups. We are a brand new security team within our organization. It's a pretty small company. They have grown their infrastructure by acquisitions, so they have a lot of separate naming conventions at each location, different staff, different log sources, and firewalls, which are different at each location. It is has been a challenge. This has been one of the first applications that we've had. This and a couple others that security teams brought in recently that works across the enterprise. So, we've h... [Full Review]

Jack Callaghan

I really can't think of a particular one, I've been very satisfied with what's happening. I know they're going to get another spike in customer base, hopefully they'll have the ability to ramp up people in support along with the customer ramp up. That's a hard game to play. I've been part of a number of beta tests, so when CloudAI came out - which is phenomenal: The ability for something to give you information in a SIEM environment, you're often gathering data, writing rules to monitor the data, so you can see what you think you should see. But the... [Full Review]

Aaron Mueller

Global management for registry integrity monitoring. Right now you have to apply what they call RIM policies, Registry Integrity Monitoring policies, one agent at a time. If you have thousands of endpoint agents, you have to touch each one of those one at a time. That is a pain in the rear, so I would really like to see some type of group or global management for RIM policies, like they have already for FIM, the File Integrity Monitoring. You can grab hundreds of agents at one time, and apply them across the board. I don't know why you can't do that... [Full Review]

Kevin Merolla

My biggest challenge always come back to log sources. We are a manufacturing company, so we have a lot of old stuff, and it has been a challenge to get some of our old stuff to light up within LogRhythm in a way that makes sense. I have probably submitted half a dozen log parser requests, and I keep finding more stuff that we need to keep an eye on that doesn't have a definition in LogRhythm. I keep pressing through, and I know they are working hard on it, but that is our biggest challenge. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Kevin Merolla

Definitely do a PoC. * Get an appliance in your system and your company. * Get your PoC guys to sign their CTU. * Then, truly think through the business case for this device. What is it that the business finds important, and how can this appliance/device enable the business to know more about the solution, and to protect that solution from anything. Because if you start with what we like in the tech industry and what we want to do, you are going to be talking about red team exercises and hacking attempts, and those are all good things to have, but t... [Full Review]

reviewer711480

Look closely at the cost of licensing of other products. This should include setups and the need for support services. I did a RFQ to 2 other vendors before choosing this product. One major issue for me was a product that you can't use if you go over on logs collected. Where I work it can take forever to get funding to fix a overage issue. This is one product that use a true up at the end of the year to address this issue. [Full Review]

Securityd96b

I would recommend that whatever sales quotes to them upfront, they will probably go up. Because they are probably going to outgrow that very quickly or once they start getting everything into it, they are going to have to move up anyway. Better to do it upfront and have that headroom. [Full Review]

© 2018 IT Central Station

IBM QRadar

See 51 reviews >>

Overview

The IBM QRadar security and analytics platform is a lead offering in IBM Security's portfolio. This family of products provides consolidated flexible architecture for security teams to quickly adopt log management, SIEM, user behavior analytics, incident forensics, and threat intelligence and more. As an integrated analytics platform, QRadar streamlines critical capabilities into a common workflow, with tools such as the IBM Security App Exchange ecosystem and Watson for Cyber Security cognitive capability.With QRadar, you can decrease your overall cost of ownership with an improved detection of threats and enjoy the flexibility of on-premise or cloud deployment, and optional managed security monitoring services.

SAMPLE CUSTOMERS

Clients across multiple industries, such as energy, financial, retail, healthcare, government, communications, and education use QRadar.

TOP COMPARISONS

Splunk vs. IBM QRadar ... Compared 49% of the time [See comparison]
ArcSight vs. IBM QRadar ... Compared 11% of the time [See comparison]
LogRhythm NextGen SIEM vs. IBM QRadar ... Compared 11% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 20%
Comms Service Provider ... 13%
University ... 6%
Healthcare Company ... 6%

COMPANY SIZE

1-200 Employees ... 25%
201-1000 Employees ... 19%
1001+ Employees ... 57%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 26%
Transportation Company ... 19%
Health, Wellness And Fitness Company ... 7%
Security Firm ... 7%

COMPANY SIZE

1-200 Employees ... 31%
201-1000 Employees ... 13%
1001+ Employees ... 56%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

© 2018 IT Central Station

IBM QRadar

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

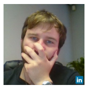
See more Valuable Features >>

GlobalSe999a

* The ability to correlate data across our global enterprise in near real time * The ability to integrate a lot of third-party solutions * The machine learning pieces with Watson, indicators of compromise, and utilizing that across the value stream I look at the solution as the best-of-the-breed product. The fact that it can work with what everybody else is doing in the cyber landscape is really what gives it the edge. [Full Review]

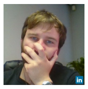
SeniorSe6fa8

Some of the most valuable things that I get from QRadar are the custom parsers. A lot of the syslog items I get pushed to QRadar, instead of trying to build a custom parser to parse out the information that we need in order to do our investigations or to review that data. There's a ton of already defined ones in the application. Plus, when you build rules, it's a really good user experience. It's like plug-and-play rules to flow out what you want, for whether what you want to look at has a certain level of severity or if you want real-time alerting ... [Full Review]



Willem Albertus Potgieter

The threat protection network is the most valuable feature, because when you get an offense, you can actually trace it back to where it originated from, how it originated, and why. [Full Review]



Willem Albertus Potgieter

The threat protection network is the most valuable feature because when you get an offense, you can actually trace it back to where it originated from, how it originated, and why. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

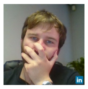
See more Improvements To My Organization >>

GlobalSe999a

The solution has improved the efficiency of our security team. These improvements prevent the need for more proactive security activities. The improvements did not reduce our staff. It's funny, because IBM keeps on having this conversation about staff headcount. It probably sounds good to senior leadership, like to a CIO. The reality is that nobody's looking to decrease the number of staff who they are hiring. We're looking at refocusing those resources and energy on being able to do additional, higher-value activities. It's more of the case that I ... [Full Review]

SeniorSe6fa8

I think it has improved our organization by the speed at which I can run queries compared to other software that I've used in the past. It's a lot quicker and holds a lot more information. It helps keep a good cognitive overview of our environment from a security standpoint. [Full Review]



Willem Albertus Potgieter

Normally, an offense comes in and an offense is something negative, it triggers when certain events don't comply with the rules, to put it plainly, it is something that will have impacted your environment very negatively. Once it comes through, you can then see from the QRadar log sources, who or what triggered the offense. For example, if an IP is browsing somewhere where it shouldn't be browsing. Let's say that one of your log sources reported it back to QRadar. You can see if the IP that browsed on certain websites where it shouldn't be browsing.... [Full Review]

© 2018 IT Central Station

IBM QRadar

Continued from previous page

ROOM FOR IMPROVEMENT

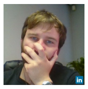
See more Room For Improvement >>

GlobalSe99 9a

Room for improvement is more in relation to a lot of the features, the automation of incidents themselves, and being able to automate workflow responses. Overall, I love the product. IBM usually puts good resources and talent behind things. What they fail to do is to bring all the security together and make sure everything inter-operates and creates one pane of glass. Actually, I don't want to say "one pane of glass" because we have seen other vendors do that. They fail miserably because they do not understand where people are coming from. In terms ... [Full Review]

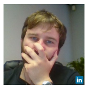
SeniorSe6fa 8

I'd like to see it being able to be integrated with more security products. I'm a big Guardian user; it's nice for the bidirectional. I can do some stuff, like a SQL injection, or if something is happening. But if there were other security tools that it could better integrate with, like to go both ways; say it knows that a user is having heavy traffic, maybe it integrates with DOP to look at different sessions that they're doing. Something like that; like backwards compared to DOP, like reporting to it. It's really good, but there's room for improve... [Full Review]



Willem Albertus Potgieter

I would like to see a more user-friendly product. I would like them to make it more user-friendly. At this stage, you need to use a lot of regular expressions to do your searches. [Full Review]



Willem Albertus Potgieter

I would like to see a more user-friendly product. I would like them to make it much more user-friendly. At this stage, you need to use a lot of widgets to do your searches. To advance searches, you must do a lot of Regex expressions. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Horacio Agustin Lo Brutto

The pricing and licensing policies are really competitive. These solutions are not for a really small business, but having just one license variable is really good. You simple tell the partner or sales representative the number of EPS you want to receive in your appliance and that's it. Other solutions have a 'correlation' license, which is more like a trap than anything else. [Full Review]

Informat59d 6

Most of the time, it is easier and cheaper to buy a new product or the QRadar box. For example, with the QRadar Event Collector 1605, as and when you need to expand your EPS and the number of log sources; it's much cheaper and the boxes usually ship with the default 1000 EPS and 750 log source limit. They have another advantage, i.e., the storage. [Full Review]

Steven Edwards

Do your due diligence. I found other solutions, with more features at the same cost or less. You don't have to leave the Gartner Magic Quadrant to beat their price. [Full Review]

© 2018 IT Central Station

AlienVault

See 56 reviews >>

Overview

Unified Security Management (USM) is AlienVault's comprehensive approach to security monitoring, delivered in a unified platform. The 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, hybrid cloud and on-premises environments, AlienVault USM significantly reduces complexity and reduces deployment time so that users can go from installation to first insight in minutes for the fastest threat detection.

The vendor says unlike traditional security point technologies, AlienVault Unified Security Management does the following:

o ... [Read More]

SAMPLE CUSTOMERS

Abel & Cole, Bank of Ireland, Bluegrass Cellular, CareerBuilder, Claire's, Domino's, GameStop, Hays Medical Center, Hope International, McCurrach, McKinsey & Company, Party Delights, Pepco Holdings, Richland School District, Ricoh, SaveMart, Shake Shack, Steelcase, Subaru, TaxAct, US Air Force, Vonage, Ziosk

TOP COMPARISONS

Splunk vs. AlienVault ... Compared 32% of the time [See comparison]
LogRhythm NextGen SIEM vs. AlienVault ... Compared 16% of the time [See comparison]
IBM QRadar vs. AlienVault ... Compared 11% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 17%
Healthcare Company ... 14%
Comms Service Provider ... 9%
Marketing Services Firm ... 8%

COMPANY SIZE

1-200 Employees ... 28%
201-1000 Employees ... 33%
1001+ Employees ... 38%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 20%
Healthcare Company ... 17%
Comms Service Provider ... 10%
Retailer ... 7%

COMPANY SIZE

1-200 Employees ... 42%
201-1000 Employees ... 32%
1001+ Employees ... 26%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

AlienVault

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Vinod Shankar

Flexible Deployment Architecture – This is where the Open Source roots really start to flex their muscles when it comes to AV USM. The main components of the architecture are as follows: * AV Sensor: AV Sensors perform Asset Discovery, Vulnerability Assessment, Threat Detection, and Behavioral Monitoring in addition to receiving raw data from event logs and helping in monitoring network traffic (including Flow). The sensors also perform normalization of the received raw events and communicates them to the AV Server for correlation and reporting. * A... [Full Review]

SystemsA3512

It's hard to pick just one valuable feature for this product. I like everything the product has to offer. The dashboards are very descriptive and contain just the right amount of information. The activity alarms and events contain a plethora of data that is very descriptive and useful. Vulnerability scans, IDS scans, asset scans. It's pretty much the whole USM Anywhere tool. Everything in here is pretty important. It gives you all the vulnerabilities of your assets. It goes through and it actually shows you the software on there, if it's missing pat... [Full Review]

reviewer673236

* Real-time email alerts * Event correlations * Log management * System monitoring * Network monitoring * Up-time monitoring * OTX threat intelligence * Vulnerability scanning reporting There are too many to list. [Full Review]

Karl Hart, Acse, Ceh, Chfi, Ci

The ease of use and customization. The USM 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. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Vinod Shankar

A jack-of-all trades: The best thing about AlienVault USM is it being a “Jack-of-All Trades” solution. It provides SIEM, HIDS/NIDS, FIM, NetFlow, Asset Management, Vulnerability Management, etc., under one USM platform. None of the commercial SIEM vendors like ArcSight, McAfee, etc., can boast of such a diverse feature set. * QRadar is the closest to AV USM in terms of feature diversity. While all the features are formerly isolated Open Source community projects, the USM does a good job of integrating them into a feature set. While they are not grea... [Full Review]

SystemsA3512

This product has streamlined productivity by having all the information in one place. It has really helped eliminate a lot of manual work because its automation is pretty robust and important. It puts everything in one place for me. It is also helping us get HITRUST certified, which is a certification we need for New York State. So this tool is a requirement, and it's going to help us stand out with New York State. [Full Review]

reviewer673236

It has given us insight into our network: * What is on it * What traffic is on it * What is happening on our servers It is one location to view many things. [Full Review]

© 2018 IT Central Station

AlienVault

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Vinod Shankar

This product is jack-of-all trades, but master of none. As mentioned in the good, being a jack-of-all trades is well suited for certain organizations. However, the lack of mature functionality and expertise in any of those areas is a strong negative. For example, the correlation engine is nowhere close to the likes of ArcSight , QRadar, or Splunk, etc. The threat Intelligence is not as good as QRadar, McAfee, RSA, etc. When it comes to critical functionality expertise, AV USM is found lacking. * Database: AV USM is using MySQL for its database. All ... [Full Review]

SystemsA3512

Honestly, the product itself is great. The only room for improvement I can mention is the initial installation procedures. I found that the online installation instructions for the product were missing important details, they lacked necessary steps. The product itself is fine. [Full Review]

reviewer673236

The menu system can be a little confusing, until you use it for a while. Such as at the top right there is a “settings” menu. Which is more of a user profile menu. I would like that to say what it is “My Profile.” Under the “Settings” menu I had rather see true system settings. Such as User Accounts, Configuration Backups/Restore, SMTP server Setting, AD, Network Traffic In/Out performance for each NIC, and etc. Currently Threat Intelligence items are also under Configuration. I would make a separate “Threat Intelligence” menu and expand upon it to ... [Full Review]

Karl Hart, Acse, Ceh, Chfi, Ci

The one thing I continue to dislike about the USM is the limitation on reports. Hard to get what you need in a report and once you do, there is no control over the formatting. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Vinod Shankar

One of the areas where AV USM benefits is price. It is affordable while offering a whole lot of SIEM features. This turns out to be the deciding factor for small and medium enterprise segments. QRadar, ArcSight and Splunk are some of the most expensive SIEM products out there in the market and not everyone has the budget to buy them. In such cases, AV USM is a very cost effective alternative. [Full Review]

Karl Hart, Acse, Ceh, Chfi, Ci

Have a look at how AlienVault does Events Per Second (EPS) compared to others. Most other products charge based on EPS, the more events the more you have to pay. This causes most companies to limit the amount of logs sent and processed. AlienVault charges by the number of devices managed. You can send anything and everything to the USM. The more logs you can process the better correlation you will have. I have found that companies that limit their logs and then have a security incident would have been able to identify the attack if they would have b... [Full Review]

Layla Bartram

Our company normally handles everything from setup to configuration, refinement, and monitoring. We are an MSSP so we all handle this for the customer when they inquire about services. [Full Review]

© 2018 IT Central Station

ArcSight

See 20 reviews >>

Overview

ArcSight is Micro Focus' leading Security Information and Event Management (SIEM) solution. ArcSight helps businesses protect their data through compliance solutions and security analytics.

There are a number of different products and solutions in the ArcSight family so you are able to pick and choose those that are best suited to your business requirements.

With ArcSight, IT can:

Monitor IT infrastructure.Manage insider security with secure identity and access control.Automate compliance.Monitor applications.Manage security risks.Identify APTs.

SAMPLE CUSTOMERS

Lake Health, U.S. Department of Health and Human Services, Bank AlJazira, Banca Intesa, and Obrela.

TOP COMPARISONS

Splunk vs. ArcSight ... Compared 39% of the time [See comparison]
IBM QRadar vs. ArcSight ... Compared 22% of the time [See comparison]
LogRhythm NextGen SIEM vs. ArcSight ... Compared 8% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 27%
Comms Service Provider ... 15%
Media Company ... 10%
University ... 6%

COMPANY SIZE

1-200 Employees ... 15%
201-1000 Employees ... 22%
1001+ Employees ... 63%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 40%
Comms Service Provider ... 27%
Retailer ... 7%
Media Company ... 7%

COMPANY SIZE

1-200 Employees ... 17%
201-1000 Employees ... 21%
1001+ Employees ... 62%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

© 2018 IT Central Station

ArcSight

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

[See more Valuable Features >>]

ProductS99
07

One of the most valuable features is the Active List/Session List capability. Multiple use cases were only possible to be created due to this feature list. The feature list allows us to input data dynamically to list it as a rule action. For example: If you need to take a Source IP from an IPS event and put it in an ActiveList suspicious IP, you can create another rule for AntiVirus events where it only matches IPs within that list. [Full Review]

Merana
Sadikovic
Mandzukic

The valuable features are: * Integration and log collection with different devices. * Collecting logs from many different sources. If you have your own app, you can do logging for it. In addition, you can customize log parsing. * Correlations of logs from different device types. * Built-in content such as reports, dashboard, compliance, and standard packages. * Option to correlate logs with business data. * Option to adjust the product to different roles: operations, decision makers, and administrators. * You can adjust the web console interface to ... [Full Review]

Karlo Luiten
Crisc Cissp

* Large scale installations work well. * The new user interface is nice. * The real-time analysis adds value. * The default packages on the new HPE Marketplace are useful and give nice default dashboards and reports for most of the well-known products. [Full Review]

LaszloKeres
zturi

* Event correlation across multiple device categories: It allows us to have a full picture of what is happening in the environment. * Flexible event collection: Besides hundreds of standard devices, you can send custom CEF Syslog prepared with your own scripts. * Customization of alerts: Velocity macros allows you to send very clear and user-friendly alerts. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

[See more Improvements To My Organization >>]

ProductS99
07

Having a SIEM solution in general improves the way an organization functions, especially in the SOC part. With HPE ArcSight, we were able to deploy multiple dashboards, reports, and use case views that combine different views, data, and variables. [Full Review]

Karlo Luiten
Crisc Cissp

* User behavior and problems on the network are visible, which we can then solve. * We can align policies with how people actually behave. * MSSP options are very good. [Full Review]

LaszloKeres
zturi

This product gave us a clear picture of the network traffic, including the useless parts. It also allowed us to detect a large range of threats, starting from the malware infected workstations to misconfigured devices. [Full Review]

© 2018 IT Central Station

ArcSight

Continued from previous page

ROOM FOR IMPROVEMENT

[See more Room For Improvement >>]

ProductS9907

The main area is the GUI interface. Although a lot of improvements were made on the GUI in the last version (6.9.1), there are still a lot of configurations that need to be done using the console. The console is not a bad tool to use. I personally like to use it. However, compared to competitive solutions (Splunk, QRadar), it appears to be a weakness. [Full Review]

Merana Sadikovic Mandzukic

I would like to see the following improvements: * Less time to administer and track logs on separate devices. * Ease of changing the product underneath. For example, instead of Juniper routers, we started to use Check Point routers. * Reporting: I would like an easier way to find the root cause. * Simplicity: I would like to see an easier way to figure out which column has the mapped data. * Component accessibility: Components are managed in different places; console, web console, and administration web. It would be nice to have easier access. * Bet... [Full Review]

Karlo Luiten Crisc Cissp

HPE ArcSight has a quite steep learning curve. If you get to know the product well, it is the most powerful product that I have worked with. It would be nice if new users could start using the product more easily. [Full Review]

david hourani

Ease of use, access and simplicity: HPW ArcSight makes it hard to capitalize on reports without the use of the console. Other SIEM tools have made it clear that event correlation results can be used not only to send out alerts, but also to provide easily accessible results to management. ArcSight can be quite complicated to use for "non-IT" user. In terms of "ease of use", access and simplicity, HPE could do a better job, since customers acquiring the product should be spending more time on implementing use cases than on understanding the product an... [Full Review]

PRICING, SETUP COST AND LICENSING

[See more Pricing, Setup Cost And Licensing >>]

Karlo Luiten Crisc Cissp

Do not scale out (horizontally) too quickly. A good box can handle a lot of EPS. You will not need to buy more licenses if you use one box in a good way. Also, aggregation can help a lot in pushing down licensing costs. [Full Review]

LaszloKereszturi

In order to avoid huge licensing costs, you should use pre-filtering of events, outside the ArcSight solution. We did this for Cisco ASA firewalls, Microsoft TMG proxies, etc. Of course, this approach may not work, if you have regulatory constraints and have to collect everything. [Full Review]

david hourani

Price is fair compared to other SIEMs (Splunk, QRadar, etc.). It's not the go-to product if you are looking for something cheap. Go for ArcSight, if it provides specific features that your IS requires. [Full Review]

© 2018 IT Central Station

McAfee Enterprise Security Manager (McAfee ESM)

See 5 reviews >>

Overview

McAfee Enterprise Security Manager - the foundation of the security information and event management (SIEM) solution family from McAfee delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

SAMPLE CUSTOMERS

San Francisco Police Credit Union, Wªstenrot Gruppe, Volusion, California Department of Corrections & Rehabilitation, Government of New Brunswick, State of Colorado, Macquarie Telecom, Texas Tech University Health Sciences Center, Cologne Bonn Airport

TOP COMPARISONS

Splunk vs. McAfee Enterprise Security Manager (McAfee ESM) ... Compared 36% of the time [See comparison]
IBM QRadar vs. McAfee Enterprise Security Manager (McAfee ESM) ... Compared 24% of the time [See comparison]
ArcSight vs. McAfee Enterprise Security Manager (McAfee ESM) ... Compared 14% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm	... 19%
Logistics Company	... 9%
University	... 9%
Energy/Utilities Company	... 7%

COMPANY SIZE

1-200 Employees	... 17%
201-1000 Employees	... 29%
1001+ Employees	... 53%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees	... 17%
201-1000 Employees	... 25%
1001+ Employees	... 58%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

© 2018 IT Central Station

McAfee Enterprise Security Manager (McAfee ESM)

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Laeeq Ahmed

VirusScan Enterprise provides protection against real-time malware attacks. We use it for logging the network traffic, when required. It blocks the things which are not to be allowed. It has an adaptive mode where it learns for itself. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Mazhar Hamayun

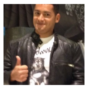
We perform security event monitoring for over 700 individual servers, firewalls, and applications. It's not possible to monitor over 500 million events per day with SIEM. [Full Review]

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Laeeq Ahmed

There are always multiple bugs in the product. For example, the console page was hanging multiple times. Afterwards, they released multiple upgrades for the same, multiple patches from McAfee. Also, there's no software support from McAfee. It seems McAfee does not test its product before releasing. When we - not only us, other companies also - deploy McAfee, we face multiple issues from the customer side, after which, McAfee reacts and fixes the bugs. [Full Review]



Vagner Araujo Silva

I had a couple of problems collecting Windows events. The local plugin should be easier to use, because when ESM is collecting through the manager, many performance issues occur. [Full Review]

Murray Neish

* Product currently requires Flash. * Update to user interface from version 9 is cosmetic in some aspects, and after a few clicks you are back on the old interface. * Some filters are still very low level "magic numbers", which do not make sense on the high level user interface. * We would welcome integrations with some of the new McAfee acquisitions, e.g., behavioral analytics. [Full Review]

© 2018 IT Central Station

InsightIDR

See 6 reviews >>

Overview

Parsing hundreds of trivial alerts. Managing a mountain of data. Manually forwarding info from your endpoints. Forget that. InsightIDR instantly arms you with the insight you need to make better decisions across the incident detection and response lifecycle, faster.

SAMPLE CUSTOMERS

Liberty Wines, Pioneer Telephone, Visier

TOP COMPARISONS

Splunk User Behavior Analytics vs. InsightIDR ... Compared 40% of the time [See comparison]
Rapid7 NeXpose vs. InsightIDR ... Compared 17% of the time [See comparison]
Darktrace vs. InsightIDR ... Compared 13% of the time [See comparison]

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

© 2018 IT Central Station

InsightIDR

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Chad Kliewer

InsightIDR's ability to process millions of transactions per day, and to notify me of the most critical ones, is priceless. InsightIDR has the alerts tuned, and has the ability to quickly drill down to determine the threat level, which is very important to me as a one-person security department. Another very important part of insightIDR is the ability to collect data from endpoint devices via agent software. With a large remote workforce, this allows visibility into the endpoints that are connected to the internet, but not to the corporate network. [Full Review]

Informate3db

The incident case management is the most valuable feature. Even though there's always something I find I would like to add to that feature, the ability to quickly sort through all the logs, network and endpoint data, etc., and add it to an incident case as part of the investigation, is nice. Having it automatically timeline that additional data into the original incident timeline, and correlate it to other notable events and activities on the network, results in a huge improvement in our overall confidence that we've quickly traced down the right so... [Full Review]

Aaron Harris

* Intelligent alerting to avoid the common problem of alert fatigue associated with traditional SIEMs. * Great coverage of all systems within our network from endpoint to firewall. * Integration with threat modeling from the Metasploit and InsightIDR repositories. * Enables the use of honey pots, honey users, and honey files to monitor for suspicious patterns. It gives all the advantages of a SIEM. However, using clever AI, it looks for patterns of behavior rather than just flooding me with all the alerts. [Full Review]

Databasea5f3

* User behavioral analytics allows us to pinpoint abnormal or suspicious behavior among millions of events every day. * Log search allows us to dive deep into aggregated logs and query all event types at once. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Chad Kliewer

With the full suite of Rapid7 products, I am able to provide effective oversight to the information security program with measurable progress. This is a very difficult thing to measure with the ever-changing threat landscape. Dashboards, including the main screen, provide much-needed information at a glance, without hours of coding and sifting through logs to find it. In case of an actual security incident, I have faith that insightIDR has retained all logs in a secure manner that prevents log tampering as well. [Full Review]

Informate3db

The focus on users/endpoints gives us so much more understanding of the events going on across the network, allowing us to step back from looking at logs only to see the actual behavior patterns instead. [Full Review]

© 2018 IT Central Station

InsightIDR

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Chad Kliewer

I would like the ability to adjust the threshold of certain existing alerts. Currently the only option is to change the notifications or create my own alert. [Full Review]

Informate3d b

The reporting is the weakest aspect. There needs to be multi-level grouping for events (for example, group by user and destination). Right now, we can do a group by user and a separate table or group by destination. But I'd be more interested in where a person was logging into instead of who was logging in or where he was logging in. [Full Review]

Aaron Harris

Although the solution has been improving continually in the time I have been using it, there could be areas of improvement. The one thing that springs to mind is easier API integration with ITSMs. We are evaluating a new ITSM and I would like to have InsightIDR create a ticket when an attack is identified, and the ticket would be closed in InsightIDR when the ITSM resolution is completed. This would take out the "single point of failure" we currently have, if the email recipient is somehow absent, in recording the risk appetite for the incident and ... [Full Review]

Josh Serna

Personally, I feel it would greatly benefit from more supported log sources. Additionally, the ability to tune the collector for custom logs would greatly help. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Chad Kliewer

Licensing is straightforward. If, for some reason, you don’t meet the minimum licensing requirements, there is a third-party managed service that can help. [Full Review]

Informate3d b

Licensing is by endpoint and amount of retention time (at least ours is). Default retention was one year, but we are able to push the retention further if needed. There's also a provide-your-own-S3 option for longer retention if you don't want to pay for the additional retention years in your Rapid7 agreement. [Full Review]

Josh Serna

This is a great product. The team is very willing to work with companies. My suggestion is to call the Rapid7 sales department and see how they can help. [Full Review]

© 2018 IT Central Station

SolarWinds LEM

See 1 review >>

Overview

When TriGeo was acquired by SolarWinds, TriGeo SIM became known as SolarWinds Log & Event Manager. This product is a leading Security Information and Event Management (SIEM) product and log management solution, which provides log collection, analysis, and real-time correlation.

SAMPLE CUSTOMERS

NetSuite, EasyStreet, Legacy Texas Bank, and Energy Federal Credit Union, to name a few.

TOP COMPARISONS

Splunk vs. SolarWinds LEM ... Compared 57% of the time [See comparison]
AlienVault vs. SolarWinds LEM ... Compared 9% of the time [See comparison]
LogRhythm NextGen SIEM vs. SolarWinds LEM ... Compared 8% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 11%
Manufacturing Company ... 10%
Marketing Services Firm ... 8%
Cloud Provider ... 8%

COMPANY SIZE

1-200 Employees ... 33%
201-1000 Employees ... 21%
1001+ Employees ... 46%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

© 2018 IT Central Station

SolarWinds LEM

Continued from previous page

Top Reviews by Topic

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

It allows us to monitor access and pull cyber reports quickly. No more searching through logs on each server. There was not much customization, which we had to do with Splunk. [Full Review]

Jeffrey Robinette

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Licensing is on devices, so if you have many, then this may be high. The storage can be an issue as well, we already had a SAN setup, but this is true for any SIEM. [Full Review]

Jeffrey Robinette

© 2018 IT Central Station

RSA NetWitness Logs and Packets (RSA SIEM) [See 3 reviews >>]

Overview

If you’re relying on log data to detect and prevent cyber threats, you’re in trouble. Attackers increasingly evade detection of log-centric security and network monitoring tools. But logs combined with full packet, endpoint NetFlow data are proven to provide the essential details for early threat detection. Here’s a closer look at our solution.

SAMPLE CUSTOMERS

Los Angeles World Airports, Reply

TOP COMPARISONS

Splunk vs. RSA NetWitness Logs and Packets (RSA SIEM) ... Compared 24% of the time [See comparison]
IBM QRadar vs. RSA NetWitness Logs and Packets (RSA SIEM) ... Compared 17% of the time [See comparison]
ArcSight vs. RSA NetWitness Logs and Packets (RSA SIEM) ... Compared 16% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 25%
Energy/Utilities Company ... 15%
Comms Service Provider ... 14%
Retailer ... 12%

COMPANY SIZE

1-200 Employees ... 16%
201-1000 Employees ... 18%
1001+ Employees ... 66%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

© 2018 IT Central Station

RSA NetWitness Logs and Packets (RSA SIEM)

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

reviewer619134

Full packet capture: A must in an SOC Possibility to investigate incidents based on logs and raw packets, such as extracting files sent over the network Built-in Incident Management module for small security/SOC teams Advanced correlation engine based on metadata flow: Provides nearly real time correlation Rich reporting options [Full Review]

muntaser bdair

RSA NetWitness is a SIEM and real-time network traffic solution. It collects logs/packets and applies a set of alerting, reporting and analysis rules on them. Thus, it provides the enterprise with a full visibility of the networks and activities of the systems. Its main features/components are: * Investigation Module: It is the location where the SOC analysts can find all logs/packets captured in a time-frame, that are related/non-related and have drill-down/filtration capabilities all in one table, for investigation and analysis. * Alerting Module:... [Full Review]

Elias Lefate Tebele

* Packet Solution: Allows analyst proactive hunting and alerting on daily sophisticated APTs. * Broker service: Aggregate multiple concentrator devices deployed in various sites which accelerates analyst's duties. * Archiver – Does log retention for three to five years for forensics purposes or targeted investigations in the future. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

reviewer619134

We can monitor all traffic to/from our company. It is possible to track end user behaviour. With RSA NetWitness Endpoint, we are able to monitor not only the network, but also what's happening on endpoints, i.e., behaviour analytics for processes inside the operating system. Thanks to this tool, we have a small SOC running in our company. [Full Review]

muntaser bdair

As mentioned elsewhere, this product provides full visibility for the activities in the networks and systems. For example, it provides detection of the attacks in early stages (brute-force attacks), by which the attackers try to gain access to the systems, by trying to log in using different usernames and passwords (might be in a dictionary). [Full Review]

Elias Lefate Tebele

Reliable in terms of no data loss. Plays a huge role in device health checks (Event Source Monitor). Provides FSEs relevant information prior to end user problem solutions (if data sources are integrated and parsed properly). [Full Review]

© 2018 IT Central Station

RSA NetWitness Logs and Packets (RSA SIEM)

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

reviewer619134

Integration with external tools should be built-in, such as an external sandbox for files. We can import data using external feeds, using STIX or CVS files. The REST API is poor The system architecture is complex and sometimes it's hard to troubleshoot potential problems. RSA should improve backup options and High Availability architecture. Data is stored on separate components without redundancy. It's possible to have backup for data, but you have to use an external backup solution. [Full Review]

Elias Lefate Tebele

Advance monitoring and alerting feature is not stable (Event Stream Analysis). Does not allow certain use cases running parallel. The reporting module: If only their dashboards resembled anything you would see on any BI reporting tools. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

reviewer619134

Prepare use cases, i.e., what to do and how. Collect information about EPS for logs and total bandwidth for packets. This will allow you to properly size the licensing. Hardware is too expensive in my opinion (Eastern Europe). It's cheaper to run virtual machines in a VMware environment. (Keep in mind that CPU, RAM, and especially HDD requirements must be matched.) [Full Review]

Elias Lefate Tebele

RSA licensing ranges per core devices and services. An additional Designated Support Engineer can be acquired at quite a pricy cost. They are reliable as your system and will be given a higher priority than any other support case(s). [Full Review]

© 2018 IT Central Station

Fortinet FortiSIEM (AccelOps) See 4 reviews >>

Overview

FortiSIEM (formerly AccelOps 4) provides an actionable security intelligence platform to monitor security, performance and compliance through a single pane of glass.

Companies around the world use FortiSIEM for the following use cases:

Threat management and intelligence that provide situational awareness and anomaly detectionAlleviating compliance mandate concerns for PCI, HIPAA and SOXManaging “alert overload”Handling the “too many tools” reporting issueAddressing the MSPs/MSSPs pain of meeting service level agreements

SAMPLE CUSTOMERS

FortiSIEM has hundreds of customers worldwide in markets including managed services, technology, financial services, healthcare, and government. Customers include Aruba Networks, Compushare, Port of San Diego, Cleveland Indians, Infoblox, Healthways, and Referentia.

TOP COMPARISONS

Splunk vs. Fortinet FortiSIEM (AccelOps) ... Compared 29% of the time [See comparison]
AlienVault vs. Fortinet FortiSIEM (AccelOps) ... Compared 13% of the time [See comparison]
LogRhythm NextGen SIEM vs. Fortinet FortiSIEM (AccelOps) ... Compared 10% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 22%
Comms Service Provider ... 11%
Marketing Services Firm ... 8%
Media Company ... 5%

COMPANY SIZE

1-200 Employees ... 23%
201-1000 Employees ... 17%
1001+ Employees ... 60%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Aerospace/Defense Firm ... 11%
Software R&D Company ... 11%
Retailer ... 11%
Integrator ... 11%

COMPANY SIZE

1-200 Employees ... 15%
201-1000 Employees ... 38%
1001+ Employees ... 46%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

© 2018 IT Central Station

Fortinet FortiSIEM (AccelOps)

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Nick Korosi

The ability to write my own parsers for the devices that are not supported by Fortinet is the most valuable feature. It's impossible to find an application that supports every device/manufacturer that we have. Thus, being able to write my own parsers for device logs, allows for greater scalability. [Full Review]

Wander Menezes

AccelOps can handle a lot of data and it's just so important to true monitoring. That is the strong point of AccelOps. The second one is detecting. I can create a lot of rules to detect anything I like, and this is another strong point. It's also the only SIEM platform on the market that has health monitoring capabilities, and correlates. For example, if a service is going down I can detect that it is going down and correlate it. For example, if it's because of an exploit can correlate this. It's a nice feature. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Nick Korosi

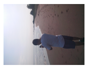
It is provides extremely fast and flexible query of logs/events on the network. For example, it's easy to write a quick query for all the "authentication" requests on the network, regardless of where they came from, i.e., during the past days, weeks or months. [Full Review]

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Nick Korosi

The reporting feature is not very attractive for the upper management and I am not able to perform complex/nested queries. However, it does function well for our day-to-day operations. [Full Review]



Muhamad Abdurrohman

In the CMDB configuration monitoring. Example, if there is a configuration on the wrong side of the network or there are changes that result in harm to our IT infrastructure, the solution should immediately fix it. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Nick Korosi

I haven't looked at the latest offerings or licensing models since Fortinet bought this product. Previously, AccelOps was looking to add other Tableau reporting modules for more complex reporting purposes. This was not attractive to us, due to the high cost of Tableau's licensing. Also, it required licensing for an event forwarding engine to be installed on the servers. The cost was getting high when we looked at licensing for 50-plus servers. [Full Review]

© 2018 IT Central Station

Answers from the Community

What Solution for SIEM is Best When Meeting NIST 800-171 Requirements?

My organization has one last piece to the puzzle in our completion for NIST 800-171 compliance. I know nothing about Network Security and Event Management. I have a team of two Systems and Network Admins that already spend a lot of time ensuring the organization is running smooth, dealing with any technical issues, and ensuring the infrastructure is performing well. What solution is recommended for something that can automate and run with little to no interaction, but ensure the requirements and needs are met? Is there a solution that does not require heavy configuration, one that can give you an overview of the network and tell you exactly what is going on inside the network, and if needed any penetration alerts, if they exist?

David Burton

There are many good SIEM products on the market today. Our company evaluated several SIEM products, LogRhythm, Splunk, AlienVault, Fortinet, and EventTracker. They all are great products. We settled on EventTracker and purchase the licenses through a 3rd party. Because these companies have internal teams of trained security analysts. They take on the heavy lifting of reviewing alerts, threat analysis, etc. The required manpower is a critical piece when evaluating SIEMs.

Perry Jurancich

As David mentioned above, there are many good SIEM products available. The challenge is, in the environment as described, is getting the value out of it if you run it yourself. There is a lot of overhead when it comes to running a SIEM, especially for the uninitiated and non-cyber minded folks. This question is interesting because I had this very conversation with a customer yesterday. My company provides consulting services to myriad companies around the world. Under 800-171 section 3.3 (800-53r4 AU controls), you have to demonstrate you retain logs for your cybersecurity environment (3.3.1), review logs on a regular basis (3.3.3), have the ability to 'audit' the logs (3.3.5) and alert events (AU-6). IMHO, the best solution for an organization that has limited staff and time, a hosted version of SIEM services is best. Not just a hosted SIEM, but have an AI/ML behavioral analysis processing engine with...

itsecuri350985

I have been working with SIEM Technology for more than 10 years. LogRhythm no doubt is one of the best for a small to mid size company.

See all 37 answers >>

© 2018 IT Central Station

Answers from the Community

When evaluating Security Information and Event Management (SIEM), what aspect do you think is the most important feature to look for?

One of our community members wrote that what's important is "compatibility with diverse sources, including the ability to adapt to unknown ones, performance, and the ability to do multi-level correlation."
What do you think?
See other excellent answers below.
Let the community know what you think. Share your opinions now!

Michael SCHLEICH

Based on my experience with SIEM, 7 years I worked with ArcSight on a daily basis. I would say that there are 3 mains points. 1) Objectives What you would like to do with the SIEM. What you have to achieve? This is very important. If you just need a solution to manage your logs and make searches for incident investigation. I will use Splunk If you need to build security monitoring use case with automatic notification I will use ArcSight or QRadar. 2) Perimeter to monitor What is the size of the infra to monitor? How many AD users? How many logs per day Which logs to collect? How many different vendors or logs type If you have a big environment to monitor You have no other choice to choose ArcSight If it less QRadar could be used. 3) Security Team Who will work with the SIEM? This is...

it_user331212

Real-time threat analysing and reporting capabilities

Stephen Hockley

Ability to quickly extract information when required (forensic). The ease at which you can integrate your devices which are logging(agnostic) . Ability of the device to capture all your required logging and maintain it for a reasonable time frame (capacity).

[See all 35 answers >>](https://www.itcentralstation.com/categories/security-information-and-event-management-siem)

About this report

This report is comprised of a list of enterprise level Security Information and Event Management (SIEM) vendors. We have also included several real user reviews posted on ITCentralStation.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About IT Central Station

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors but what you really want is objective information from other users.

We created IT Central Station to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

We commit to offering user-contributed information that is valuable, objective and relevant. We protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

IT Central Station helps tech professionals by providing:

- A list of enterprise level Security Information and Event Management (SIEM) vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use IT Central Station to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

IT Central Station
244 5th Avenue, Suite R-230 • New York, NY 10001
www.ITCentralStation.com
reports@ITCentralStation.com
+1 646.328.1944

© 2018 IT Central Station