User Reviews of

IBM QRadar and Splunk

A Peek Into What Real Users Think

July 2017

IT Central Station
Unbiased reviews from the tech community

Contents

Overview

SOLUTION	IBM QRadar	Splunk
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...	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...
SAMPLE CUSTOMERS	Clients across multiple industries, such as energy, financial, retail, healthcare, government, communications, and education use QRadar.	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	Splunk vs. IBM QRadar Compared 34% of the time HPE ArcSight vs. IBM QRadar Compared 13% of the time LogRhythm vs. IBM QRadar Compared 8% of the time	IBM QRadar vs. Splunk Compared 13% of the time HPE ArcSight vs. Splunk Compared 10% of the time LogRhythm vs. Splunk Compared 9% of the time
TOP INDUSTRIES, BASED ON REVIEWERS*	University ... 5% Philanthropy ... 7% Comms Service Provider ... 14% Financial Services Firm ... 21%	Marketing Services Firm ... 7% Energy/Utilities Company ... 8% Comms Service Provider ... 10% Financial Services Firm ... 17%
TOP INDUSTRIES, BASED ON COMPANIES READING REVIEWS*	Health, Wellness And Fitness Company ... 8% Pharma/Biotech Company ... 8% Transportation Company ... 21% Financial Services Firm ... 25%	Insurance Company ... 6% Energy/Utilities Company ... 18% Retailer ... 18% Financial Services Firm ... 29%
COMPANY SIZE, BASED ON REVIEWERS*	201-1000 Employees ... 19% 1-200 Employees ... 23% 1001+ ... 58%	1-200 Employees ... 14% 201-1000 Employees ... 18% 1001+ ... 68%
COMPANY SIZE, BASED ON COMPANIES READING REVIEWS*	1-200 Employees ... 27% 201-1000 Employees ... 9% 1001+ ... 64%	1-200 Employees ... 11% 201-1000 Employees ... 7% 1001+ ... 81%

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

Top Reviews by Topic

SOLUTION	IBM QRadar	Splunk
VALUABLE FEATURES	 Damian Scott * Correlation Rule Engine, built-in use cases: QRadar has the highest number of built-in use cases among any SIEM on the market. There are many built-in rules that are enabled by default and easily tunable to meet the specific needs of each organization. The correlation engine automates what is a manual process for many SIEM platforms. * Network-Based Anomaly Detection (NBAD): Using NetFlow, JFlow, SFlow, or QFlow (all 7 layers), offenses are detected as a response when a rule is triggered. * QR... [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]
	 Vulnerab7e86 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]	 Mark Kline * Splunk delivers a holistic view of an application (the big picture). * Splunk provides immediate visibility into key business metrics and new business insights that deliver immediate value. * Significant reduction in mean-time-to-investigate (MTTI) and mean-time-to-resolve (MTTR) production incidents from days to hours. * Splunk visualization capabilities help pinpoint problem areas, spikes, and anomalies easier and faster. * Ability to monitor and resolve integration problems before they impa... [Full Review]
	 Horacio Agustin Lo Brutto In my understanding, the best features are: * DSMs (Device Support Modules), * Device auto-discovery, and * Hundreds of rules and reports already created for you to mix up. These features are keeping QRadar on top in Gartner. You can have it running in a few hours, then start collecting your logs and events in no time. [Full Review]	 Timur Baitenov Splunk's schema-on-read technology is one of the most valuable characteristics of this solution. It allows us to store raw data and use it repeatedly for different domains. You don't need to prepare the data upfront. Splunk's Search Processing Language (SPL) is another beneficial feature. It is a very powerful tool that gives you the ability to do almost anything with your data. [Full Review]

Top Reviews by Topic

SOLUTION

IBM QRadar

Splunk

IMPROVEMENTS TO MY ORGANIZATION

Damian Scott

As a Professional Services consultant, I have heard many reports of how QRadar SIEM has quickly identified offenses which the users were unaware of previously. In addition to giving CISO's gained visibility and increasing security posture, QRadar adheres to many compliance regulations across vertical industries. [Full Review]

Vulnerab7e86

Normally, an offense comes in and an offense is something negative, to put it plainly, that impacted your environment. 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. When you right-click and go to the threat prote... [Full Review]

Horacio Agustin Lo Brutto

I have implemented QRadar in a big airline company, where they needed to get all their security information in one place. It helped in reducing the amount of time that was needed to evaluate the risk of every event. Configuring the alerts has never been easier; you just search for the event you think you need and start creating the rules that way. It is really straightforward and you don't need much IT knowledge for it. Of course, your experience with the product and a generalist view of the inf... [Full Review]

Joshua Biggley

Imagine a single application with 17 application servers and dozens of log files per server that rotate as often as once per hour. How do you track and analyze anomalies in those log files with the ability to go back and correlate data for the past X weeks? That was use case for just our team, not to mention the hundreds of other application teams. [Full Review]

Paul Gilowey

MTTR is drastically reduced, because the developers and other IT support staff have instant access to log events. People costs are saved by not having to involve the domain developers from multiple teams, when tracing a problem that spans multiple platforms. Security is improved by not having to give as many people access to log on to the servers. [Full Review]

Mark Kline

It is deployed to investigate, detect, respond, and prevent security incidents and threats by providing valuable context and visual insights to make faster and smarter security decisions. [Full Review]

Top Reviews by Top

SOLUTION	IBM QRadar	Splunk
ROOM FOR IMPROVEMENT	Vulnerab7e86 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. [Full Review]	Joshua Biggley Deploying Splunk as scale is not easy. It requires a significant amount of relatively complex architecture once you push past the single server instance. Breaking out your search and indexing layer requires someone with Splunk experience. Want to add search layer replication for HA? Want to host in AWS and do cross-region index replication? Splunk expertise is in high demand today and finding talented engineers to pull off your large-scale implementation is hard. Do your homework. [Full Review]
	 Miguel Angel Beltran Vargas From my point of view, they should improve the backup procedures. QRadar does not allow sending backups by FTP or SFTP, limiting the tool. I had to make a script but it is a manual process. It would be great to have it automated. [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 automatic... [Full Review]
	Informat59d6 This product has room for improvement in a lot of areas including the default emailing template that it uses to alert on offenses. It also needs a lot of work in terms of the flows and the log source parsing. A lot of the times, it is very difficult to add a new/uncommon log source to this tool, as we need to map a lot of fields, rather than simply extracting these from the payload. QVM is another instance where they need to revise the vulnerability scoring and the proper remediation details. IB... [Full Review]	Mark Kline We usually have to follow up with technical support on our open cases. Otherwise, Splunk listens to customers and is constantly incorporating their feedback in future releases. [Full Review]

Vendor Directory

AlienVault	AlienVault
Cybereason	Cybereason
EventTracker	EventTracker
IS Decisions	FileAudit
Fortinet	Fortinet FortiSIEM (AccelOps)
Hewlett Packard Enterprise	HPE ArcSight
IBM	IBM QRadar
Interset	Interset
TIBCO	LogLogic
LogPoint	LogPoint
LogRhythm	LogRhythm
Logsign	Logsign
ManageEngine	ManageEngine Log360
Masergy	Masergy
Intel Security	McAfee Enterprise Security Manager
Micro Focus	NetIQ Sentinel
NNT	NNT Log Tracker Enterprise
RSA	RSA enVision
RSA	RSA NetWitness Logs and Packets
Securonix Solutions	Securonix Security Analytics
Sematext	Sematext Logsene
SenSage	SenSage SIEM
Intersect Alliance	Snare
SolarWinds	SolarWinds LEM
Splunk	Splunk
SQRRL	SQRRL
SurfWatch Labs	SurfWatch Labs SurfWatch
ThetaRay	ThetaRay
ThreatStream	ThreatStream OPTIC
Trustwave	Trustwave SIEM

Top Security Information and Event Management (SIEM) Vendors, Weighted

Over professionals have used IT Central Station research on enterprise tech. Here are the top 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 (i.e. bar length) is based on a weighted aggregate ranking of that product's Views (weighting factor = 17.5%), Comparisons (17.5%), Reviews (17.5%), Followers (17.5%), and Average Rating (30%). Reviews and ratings by resellers are excluded from the rankings. For each ranking factor, the score (i.e. bar segment length) is calculated as a product of the weighting factor and its position for that ranking factor. For example, if a product has 80% of the number of reviews compared to the product with the most reviews in its category, then the product's bar length for reviews would be 17.5% (weighting factor) * 80%.

1 Splunk

82,836 views **63,694** comparisons **18** reviews **3,805** followers **7.9** average rating

2 IBM Security QRadar SIEM

35,210 views **24,287** comparisons **37** reviews **3,105** followers **8.3** average rating

3 AlienVault

23,133 views **11,949** comparisons **41** reviews **3,345** followers **8.4** average rating

4 HPE ArcSight

30,073 views **18,067** comparisons **31** reviews **3,749** followers **7.9** average rating

5 LogRhythm

47,297 views **21,600** comparisons **17** reviews **3,450** followers **8.1** average rating

6 Fortinet FortiSIEM (AccelOps)

40,145 views **32,243** comparisons **11** reviews **1,963** followers **7.7** average rating

7 RSA NetWitness Logs and Packets

6,869 views **4,816** comparisons **2** reviews **1,591** followers **8.5** average rating

8 McAfee Enterprise Security Manager

8,191 views **5,524** comparisons **6** reviews **1,136** followers **7.7** average rating

9 RSA enVision

1,701 views **1,376** comparisons **1** reviews **1,118** followers **8.0** average rating

10 NetIQ Sentinel

3,215 views **1,976** comparisons **3** reviews **1,097** followers **7.3** average rating

Top 5 Solutions by Ranking Factor

Views

SOLUTION		VIEWS
1	Splunk	82,836
2	LogRhythm	47,297
3	Fortinet FortiSIEM (AccelOps)	40,145
4	IBM Security QRadar SIEM	35,210
5	HPE ArcSight	30,073

Reviews

SOLUTION		REVIEWS
1	AlienVault	41
2	IBM Security QRadar SIEM	37
3	HPE ArcSight	31
4	Splunk	18
5	LogRhythm	17

Followers

SOLUTION		FOLLOWERS
1	Splunk	3,805
2	HPE ArcSight	3,749
3	LogRhythm	3,450
4	AlienVault	3,345
5	IBM Security QRadar SIEM	3,105

About this report

This report is comprised of a list of enterprise level 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 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