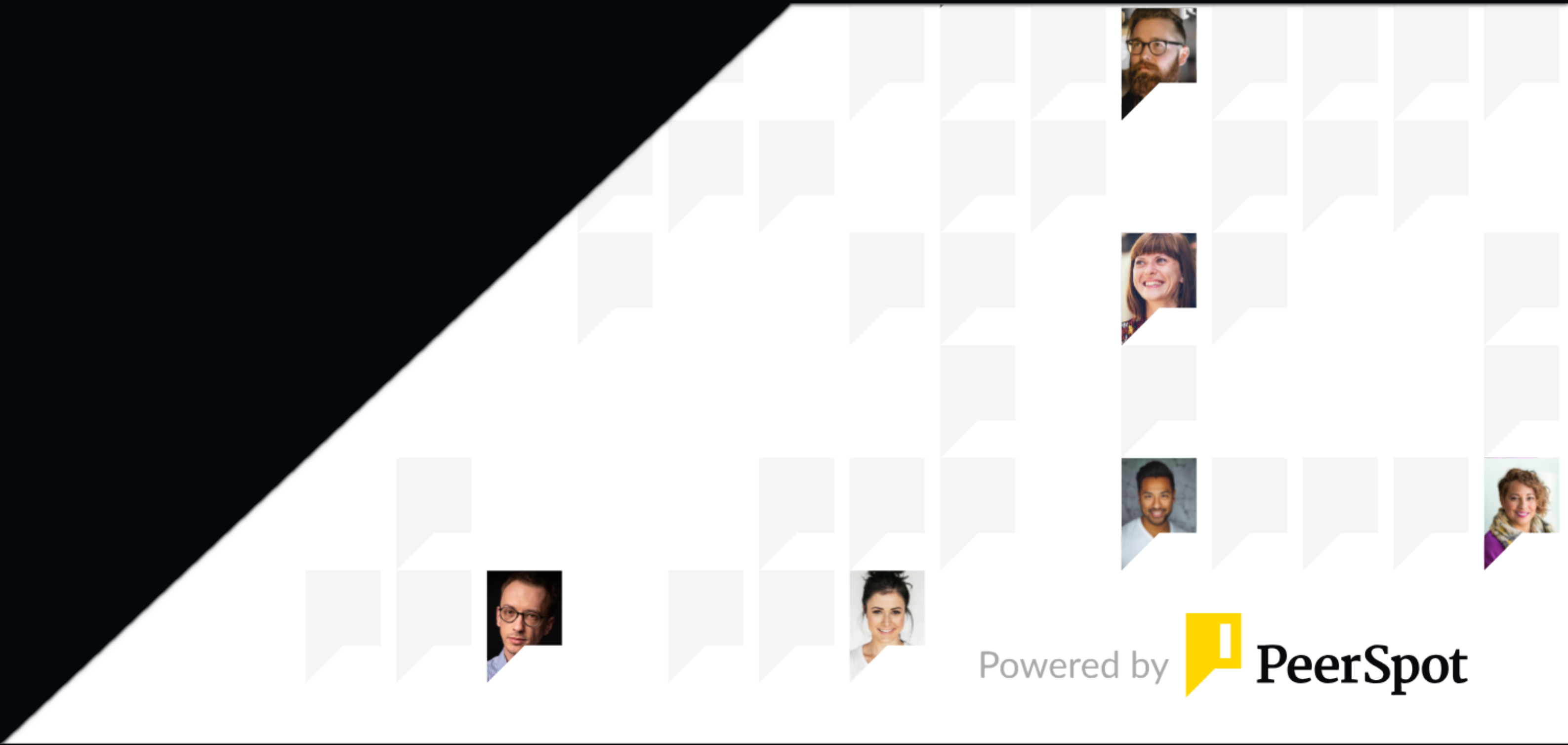
aws marketplace

Splunk Enterprise Security

User Interviews: ROI and Why They Chose Splunk

August 2024



Powered by PeerSpot

Contents

Product Recap

Splunk Enterprise Security

Splunk Enterprise Security Recap

Splunk Enterprise Security is a SIEM, log management, and IT operations analytics tool. The solution provides users with the ability to secure their information and manage their data in the cloud, data centers, or other applications. Splunk Enterprise Security also offers visibility from different areas, levels, and devices, rather than from a single system, thus, providing its users with flexibility. Splunk Enterprise Security can monitor data and analyze, detect, and prevent intrusions. This benefits users as it provides alerts to possible intrusions, helps users to be proactive, and reduces risk factors.

Full visibility across your environment

Break down data silos and gain actionable intelligence by ingesting data from multicloud and on-premises deployments. Get full visibility to quickly detect malicious threats in your environment.

Fast threat detection

Defend against threats with advanced security analytics, machine learning and threat intelligence that focus detection and provide high-fidelity alerts to shorten triage times and raise true positive rates.

Efficient investigations

Gather all the context you need and initiate flexible investigations with security analytics at your fingertips. The built-in open and extensible data platform boosts productivity and drives down fatigue.

Open and scalable

Built on an open and scalable data platform, you can stay agile in the face of evolving threats and business needs. Splunk meets you where you are on your cloud journey, and integrates across your data, tools and content.

Other Solutions Considered

“Compared to IBM QRadar, Splunk Enterprise Security offers faster alert resolution. Its superior indexing and searching capabilities deliver quicker query results. While QRadar boasts a more user-friendly interface, Splunk provides numerous pre-built use cases that effectively reduce false positives and feature comprehensive application dashboards.

For instance, I encountered a use case unavailable in QRadar which appears to utilize the Cyber Kill Chain framework. MITRE ATT&CK enjoys wider adoption, and Splunk leverages this framework whereas QRadar persists with the Cyber Kill Chain. Additionally, Splunk integrates with a third-party app exchange, offering functionalities like vulnerability dashboards, threat intelligence, correlation dashboards, and EPS dashboards. This extensive library of applications caters to diverse business use cases. Users can install these applications as needed, making Splunk a highly customizable and feature-rich solution. Although undeniably expensive, its capabilities justify the cost.”

Read full review

Verified user

Manager at a consultancy with 1-10 employees

“Before using Splunk, I relied on the built-in tools of Linux operating systems, such as Syslog NG, but specifically the open-source versions. I haven't had experience with the commercial version of Syslog NG, which is a more advanced tool. In this category, Splunk is essentially my first exposure to such advanced features.
”

Read full review

Verified user
Owner at a computer software company with 1-10 employees

“Before Splunk Enterprise Security, I used various solutions, including LogRhythm. I chose Splunk because it proved to be more stable and reliable, especially compared to the issues I experienced with LogRhythm. With Splunk Enterprise Security, it takes my analysts approximately 30-40% less time to resolve alerts compared to our previous solution.
”

Read full review

Verified user
CEO at a retailer with 51-200 employees

“I have looked at other competitors. We recently looked at CrowdStrike's LogScale solution. It feels like Splunk to me. I cannot say how we would reproduce what we have done in Splunk on the infrastructure side or backend. Our environment is uniquely different. Technically, I am the only person who runs Splunk for our entire organization, similar to the way the previous person ran ArcSight for the organization. If I were to compare apples to apples, Splunk to me is still number one in that category.

Splunk's community is the biggest benefit. It is so easy to go to Slack and hit someone up. There is a good chance that you will find someone out there who has run into the exact same issue that you are having. Their documentation is fantastic. Because I am the only one who runs it for our organization, it is easy for me just to Google it, find the document, and just follow it. It is as simple as that. It gets a little dicey with XDR and all the other things that are happening in the market, such as using a data lake. Instead of putting our eggs in one basket or using Splunk, we might use something like Snowflake.”

Read full review

Verified user

Sr Cybersecurity Engineer at a energy/utilities company with 10,001+ employees

“We do an evaluation annually. It is important for us to do a market comparison and make sure we are looking at options in our work. What makes Splunk Enterprise Security competitive is the variabilities that they bring to the table for the overall solution. It has things like APIs that you can tie into. There is also the bonus functionality of being able to do analytics there. User behavior analytics is important for us.”

Read full review

Verified user

Cyber Security at a financial services firm with 5,001-10,000 employees

“We evaluated other options. We had to evaluate the pros and cons in terms of the cost and the capabilities of each tool. A lot of that went into the proof of concept. We did our due diligence and determined that Splunk was the best fit for us.”

Read full review

Bryan Castleberry
IT Specialist at a government with 10,001+ employees

ROI

Real user quotes about their ROI:

“The return on investment is quite favorable with Splunk, particularly for large enterprises that have made the initial purchase and possess the requisite expertise and technical support.”

Read full review

Verified user

Owner at a computer software company with 1-10 employees

“Splunk Enterprise Security has delivered a return on investment through its effective threat detection and vulnerability response capabilities. We have successfully demonstrated this positive impact on our customers through comprehensive reports.”

Read full review

Amine Besrour.

Risk Manager at Samapartners

“I have witnessed an ROI while using Splunk. There were some incidents previously in which the company lost millions of dollars. Bringing in Splunk has curbed that. ”

Read full review

Oluwaseun Oke

Owner at Py Concepts

“The company has witnessed an ROI in terms of the amount of time saved via being able to tweak our searches. The docs are great. They help tremendously in filling knowledge gaps. The ROI is solid. ”

Read full review

Reviewer343335
Security Engineer at State of Nevada

- - - - - - - - - - - - - -

“Its time to value was about a year. It took us about a year because back in 2017, we were making that conversion from an on-premise ArcSight deployment to a Splunk Cloud deployment. We had to make sure that everything that was being sent to ArcSight was sent correctly to Splunk. We had to make sure that everything was in a common information model format and that we could rebuild the content.”

Read full review

Verified user
Sr Cybersecurity Engineer at a energy/utilities company with 10,001+ employees

- - - - - - - - - - - - - -

“There are a lot of things for which you can measure a return on investment, but security is something on which it is hard to put a dollar value and measure how much return you have got. However, in terms of helping the administrator or helping the company to put security in place, Splunk does a great job. I cannot imagine a life without Splunk.”

Read full review

Jesse Gan
IT Director at Administrative Office U.S. Courts

Use Case

“We use Splunk Enterprise Security for security correlation and event management.

Splunk Enterprise Security is deployed as a hybrid model where the core component is on the cloud and is integrated with an on-premises solution.”

Read full review

Verified user
Manager at a consultancy with 1-10 employees

“Through Splunk Enterprise Security, we have implemented extensive login integration. This allows us to monitor and restrict access for sensitive accounts, such as superuser and master accounts when password rotations occur. If a login attempt is made for such an account, Splunk triggers a real-time workflow that automatically generates a P1 ticket for the Help Desk and IAM Operations teams to investigate and take necessary action.

Beyond real-time monitoring, we have established additional security measures. We utilize locks within JBOS to control manual account check-ins and user server activity, such as password verifications. Splunk ingests logs from any configured PAM solutions, enabling auditors and our technical team to readily access and analyze all privileged activities. We can also generate reports for session management, session logs, and audit logs.
”

Read full review

Avinash Gopu.
Associate VP & Cyber Security Specialist at US Bank

“We typically suggest Splunk IT builds for customers with significant EPS requirements and large-scale data environments. While other solutions like Foundry and IBM QRadar may be popular, they often have limitations in handling big data effectively.”

Read full review

Maaz Khalid
Cyber Security Analyst at Rewterz

“The primary focus of our work with Splunk is on security incident monitoring and security log monitoring. This involves utilizing it to analyze and respond to security events effectively. Additionally, compliance with regulatory requirements is another crucial aspect of your role. We also extend Splunk's functionality to custom applications by writing custom parsers and handling logs specific to those applications. This includes the development of unique dashboards tailored to the needs of each application.
”

Read full review

Verified user
Owner at a computer software company with 1-10 employees

“We use Splunk Enterprise Security to enhance our overall security posture by proactively managing our threat profile across the enterprise. This enables us to see valuable insights and effectively monitor all OEM devices.”

Read full review

Nagendra Nekkala.
Senior Manager ICT & Innovations at Bangalore International Airport Limited

"We employed Splunk Enterprise Security for one of our projects. Integrating it into our environment involved opening network ports and making necessary connections."

Read full review

Verified user

Project manager at a computer software company with 10,001+ employees

Top Industries

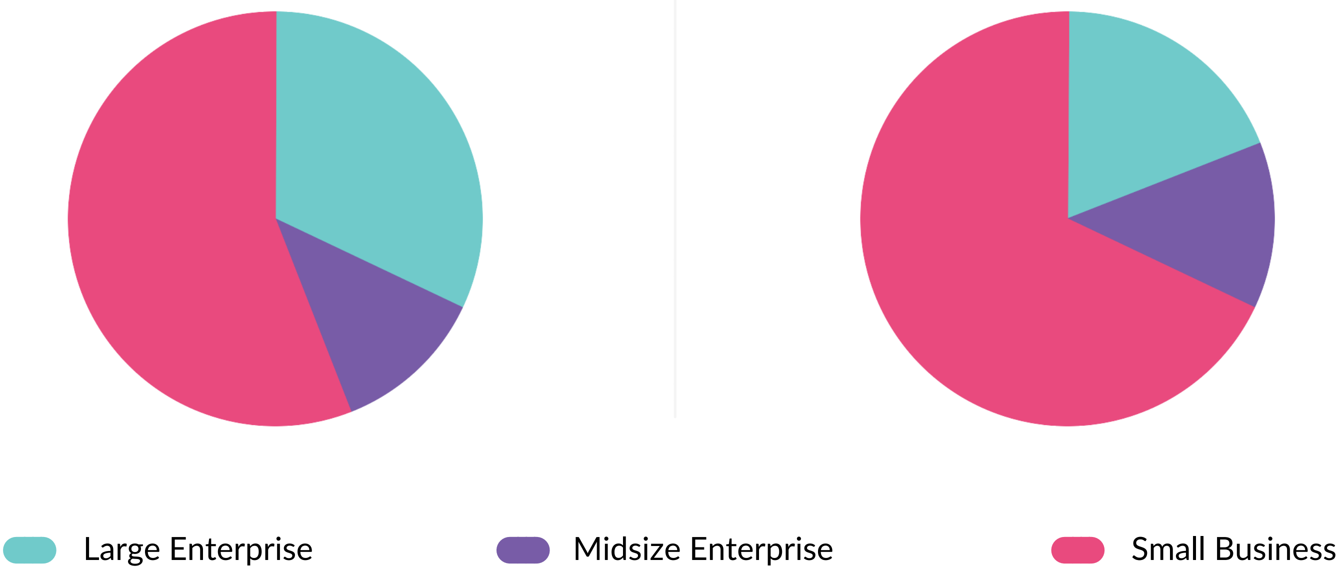
by visitors reading reviews

Financial Services Firm	15%
Computer Software Company	14%
Government	9%
Manufacturing Company	7%

Company Size

by reviewers

by visitors reading reviews



About this buyer’s guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot’s team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

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

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

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

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

Get your personalized report here.

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer’s guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944