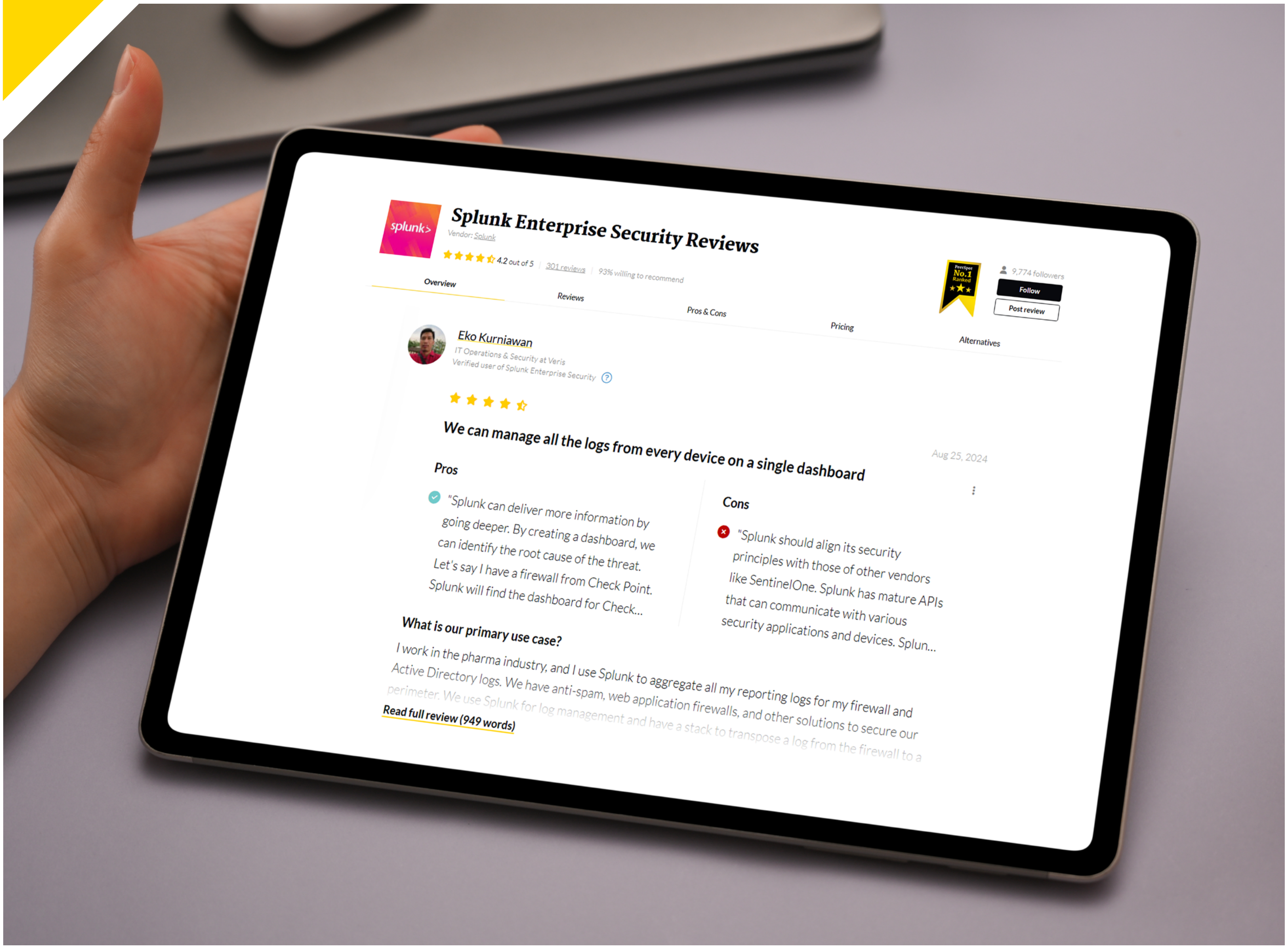
PeerPaper™ Report 2024

Based on real user reviews of Splunk Enterprise Security

# Security Visibility, Contextual Detection, and SecOps Efficiency

## Splunk Enterprise Security Customers Reveal the Top Benefits of the #1 Rated SIEM on PeerSpot



Splunk Enterprise Security Reviews

Vendor: Splunk

4.2 out of 5 | 301 reviews | 93% willing to recommend

Eko Kurniawan

IT Operations & Security at Veris

Verified user of Splunk Enterprise Security

We can manage all the logs from every device on a single dashboard

Aug 25, 2024

Pros

"Splunk can deliver more information by going deeper. By creating a dashboard, we can identify the root cause of the threat. Let's say I have a firewall from Check Point. Splunk will find the dashboard for Check...

Cons

"Splunk should align its security principles with those of other vendors like SentinelOne. Splunk has mature APIs that can communicate with various security applications and devices. Splun...

What is our primary use case?

I work in the pharma industry, and I use Splunk to aggregate all my reporting logs for my firewall and Active Directory logs. We have anti-spam, web application firewalls, and other solutions to secure our perimeter. We use Splunk for log management and have a stack to transpose a log from the firewall to a

Read full review (949 words)

PeerSpot

# Contents

Page 1. **It's a Jungle Out There**

Page 3. **Core Benefits of Using a Best-of-Breed SIEM**

Page 4. Comprehensive Visibility

Page 5. Visualization and Reporting

Page 7. Security Monitoring

Page 9. Accurate Detection With Context

Page 9. Anomaly Detection

Page 12. Risk-Based Alerting (RBA)

Page 14. Efficient SecOps

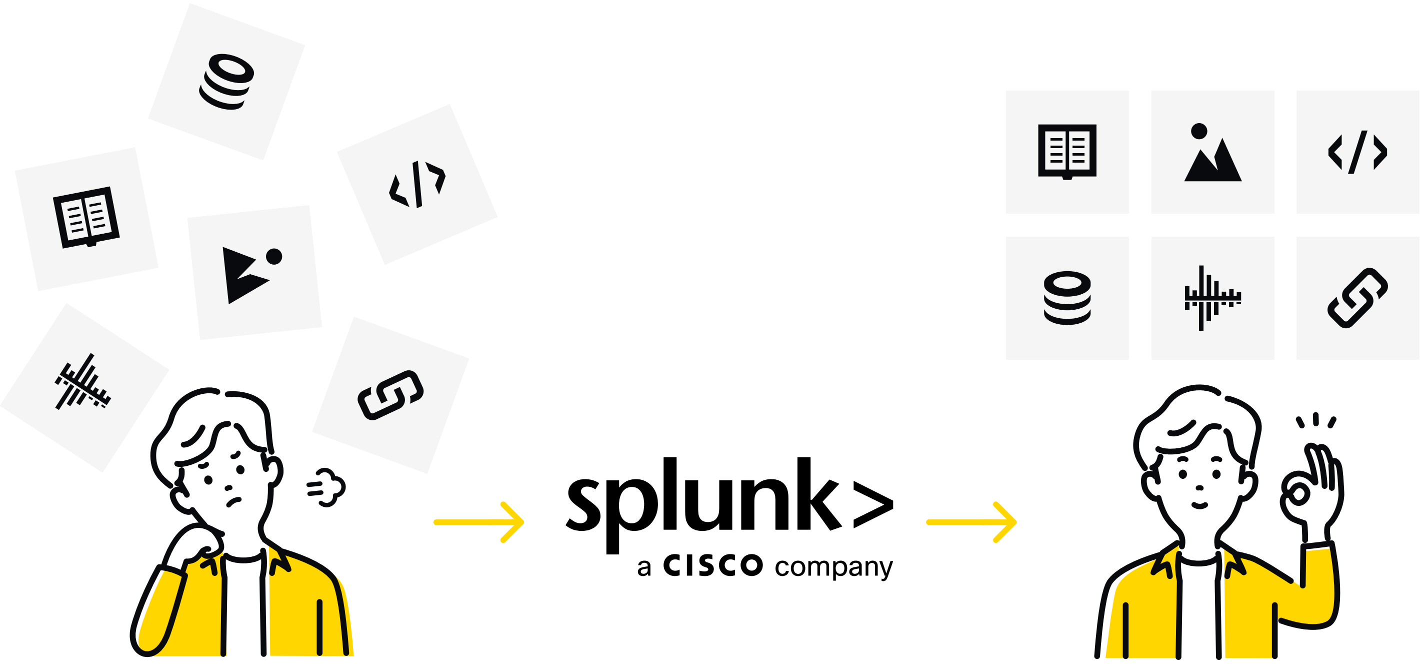
Page 15. Rapid Incident Response

Page 17. Unify and Automate Threat Detection, Investigation, and Response

Page 20. **Conclusion**

# It’s a Jungle Out There

As organizations migrate more of their operations to the cloud, security teams are facing the growing challenge of trying to stay on top of the multi-platform nature of business assets. Overwhelmed by vast amounts of data from security and IT sources, security analysts struggle to gain visibility across hybrid, cloud, and on-premises environments. As a result, teams are often unable to distinguish the signal from the noise and often struggle to gain contextual understanding of security incidents as they unfold. Lack of context makes threat detection, investigation, and response especially arduous and time-consuming, leaving analysts very little time for much else.



On average, 41% of daily cybersecurity alerts are ignored because analysts simply don't have the time or resources to address every alert every day.

Security teams are also burdened with managing as many as 25 security tools on average, each performing different functions with respect to detection, investigation and response, often requiring manual implementation, which drastically increases investigation times and overburdens security analysts with monotonous grunt work.

Solving these problems is the remit of SIEM solutions, but many traditional products lack the capabilities necessary to alleviate these issues. SOC managers are therefore turning to more sophisticated SIEM solutions such as Splunk Enterprise Security, which addresses the issues faced by SOC teams and provides a comprehensive, unified solution.

**Shakti K.**
Senior Engineering Managerat
Happiest Minds Technologies

★★★★½

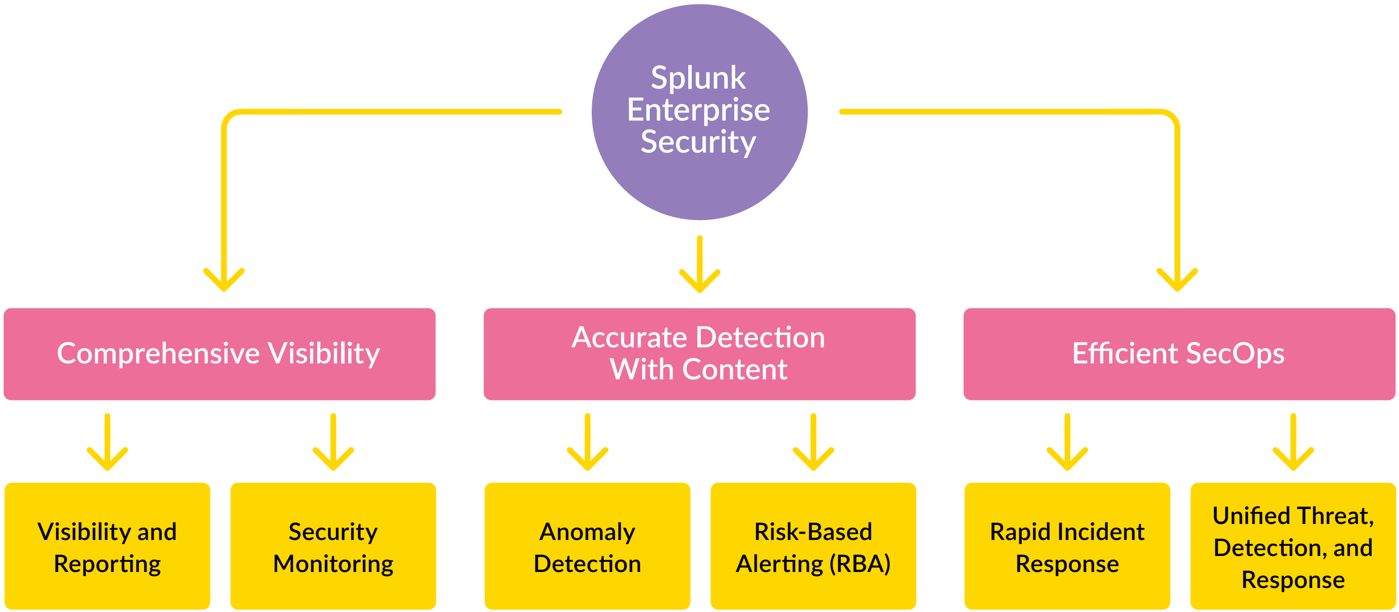
> "Splunk Enterprise Security has helped us reduce our alert volume. The SOAR tool detects and automatically manages repetitive and generic alerts proactively."

**Read review »**

# Core Benefits of Using a Best-of-Breed SIEM

Security teams that use Splunk Enterprise Security as their SIEM have reported benefits that align to 3 primary categories:

- **Comprehensive Visibility** - Splunk Enterprise Security provides comprehensive visibility by seamlessly ingesting, normalizing, and analyzing data from any source - at scale.
- **Accurate Detection with Context** - Detect accurately, rapidly assess risk, and gain contextual understanding of attacks and threats by leveraging risk-based alerting and the latest curated threat detections.
- **Efficient SecOps** - Centralize workflows and unify processes across detection, investigation, and response to fuel SOC operational efficiency and stop breaches.



Comprehensive Visibility

Let’s take a closer look at each of these benefits and how they can transform your SOC.

## Comprehensive Visibility

Security teams are struggling to gain visibility across on-premises, cloud and hybrid environments, all while being bombarded by overwhelming amounts of data from different security, IT and other business sources. They’re trying desperately to filter out the signal from the noise, and then act on it quickly to protect the organization.

With Splunk Enterprise Security, data is monitored across all ecosystems–on-premises, in the cloud or hybrid–to provide real-time, holistic visibility across the organization and uncover stealthy threats. Splunk Enterprise Security vigorously analyzes data wherever it resides to generate actionable insights for the SOC to facilitate faster investigation and response.

**Praveen K.**
Senior Consultant at
Ernst & Young

**“The threat topology and MITRE ATT&CK features are integrated, allowing us to obtain the tactics, techniques, and processes necessary to solve any remediation process.”**

**Read review »**

## Visualization and Reporting

The comprehensive visibility that Splunk Enterprise Security brings to the SOC is delivered through various visualizations and reports. These visualizations and reports provide analysts with much needed context around security events, and help to facilitate investigations and accelerate incident response.

Two data visualization features in Splunk Enterprise Security are the MITRE ATT&CK Framework visualization and the Threat Topology visualization. Cyber Security Analyst Maaz Khalid uses both of these features to visualize the threat risks his SOC is facing: “We utilize the Threat Topology and MITRE ATT&CK Framework features to enhance our understanding of threats. These features offer micro-mapping visibility, allowing us to align identified needs with specific techniques”

Praveen-Kadali, a Senior Consultant at Ernst & Young, agrees that these visualization features aid his team’s investigation and response workflows, saying, “The threat topology and MITRE ATT&CK features are integrated, allowing us to obtain the tactics, techniques, and processes necessary to solve any remediation process.”

A cybersecurity engineer at a large university also states: “Splunk’s threat topology and MITRE ATT&CK framework cover everything, including endpoints and application security from Layer 3 to Layer 7. Most queries are available out of the box.”

Information Security Analyst Kent Yan has found that Splunk Enterprise Security provides end-to-end visibility that gives him and his team a clearer, comprehensive picture of their security posture: "Splunk Enterprise Security provides end-to-end visibility into the environment. It is very important for our organization to be able to see the threats, understand the threats, and figure out how to stop those threats. We are able to see the logs of multiple systems, the logs of the firewall, and the logs of the DNS and the Windows servers. It is able to bring all of that together and give a nice, solid picture of what is happening. We can read those logs faster."

Generating an accurate report quickly and efficiently has not always been straightforward for SecOps, and by switching to Splunk Enterprise Security, users are noticing a dramatic change in the level and speed of reporting. For example, a Senior Cybersecurity Engineer at a large utilities company revealed, "I used to do incident response when I first joined the SOC, and there were times when I used to sit down and run a search right at the start of my shift, which is at 7 AM, and I used to hope that it would be run by the end of the shift at 7 PM. I used to hope that it would run in 12 hours and not time out. When we got Splunk, it was a game changer. It took seconds to a minute depending on how intense the search was."

Kiran Kumar, lead administrator at Wipro Ltd, appreciates the ability to generate customizable reports: “Splunk has a wide range of features that customers use to find and analyze all kinds of logs. Additionally, they can create dashboards to visualize and filter their data, and to create real-time alerts when thresholds are exceeded.”

Girish B, Security Engineer at Softtek, also appreciates the dashboards available in Splunk Enterprise Security, noting, “Splunk Enterprise Security offers a variety of dashboards, including real-time dashboards that update continuously. These dashboards complement Splunk’s real-time alerts by providing a visual overview of our system’s health.”

## Security Monitoring

Splunk Enterprise Security provides continuous security monitoring. Security analysts can search and correlate across multi-cloud, on-premises, or hybrid data sources so maximum attack-surface coverage is achieved. SOCs can investigate and analyze with a comprehensive viewpoint across all data sources for faster detection.

**Continuous Security Monitoring**

**Alam M.**
System Administrator at
Nournet communications

★★★★⯪

**"Splunk Enterprise Security helped us analyze malicious activities and detect breaches between 50 to 90 percent faster."**

**Read review** »

SOC Manager Manish Choudary explains how his SecOps team have improved the level of threat monitoring and detection using Splunk Enterprise Security: "Splunk Enterprise Security can help us detect threats faster when it is properly configured. We have implemented over 400 use cases for specific types of malware and other threat detection. In over 70 percent of environments, Splunk is able to detect threats faster than other solutions."

Valarie, SOC Technical Lead in an educational organization, explains that the information they need is at their fingertips because of Splunk Enterprise Security: "We have a wide range of tools in our shop. We are able to stop at one spot and look at all the data. All the data is able to come through, and we can then jump from source to source or index to index. We can dig deep whenever we need to and get a good high-level understanding."

MS Alam, System Administrator at Nournet communications is impressed with Splunk's ability to provide the data that helps his SOC team monitor threats and detect them faster: "Splunk Enterprise Security helped us analyze malicious activities and detect breaches between 50 to 90 percent faster."

## Accurate Detection With Context

Security leaders often struggle to discern high-priority threats amidst the noise. This is compounded by a pervasive lack of context when investigating threat events or trying to understand the nature and scope of attacks. A survey by the SANS Institute found that respondents named “lack of context related to what we are seeing” as the number one barrier to SOC success.

To combat this, the SOC requires the most up-to-date detections to establish a consistent understanding of security incident context. They also require a way to reduce the sheer volume of noisy alerts received each day and build confidence in the alerts they do receive. Splunk Enterprise Security users testify that the technology provides contextual visibility into threat events, reduces the volume of alerts, and captures the signal amidst the noise.

### Anomaly Detection

Anomaly detection in Splunk Enterprise Security is fueled by event-based detections, finding-based detections, and curated detections. Event-based detections provide the necessary context to respond to threats. Finding-based detections are based on specific details or analytics observed. Curated detections are produced by the Splunk Threat Research Team and can be utilized for specific security use cases out-of-the-box. But how do these detection capabilities solve problems for customers?

**Detect Insider Threats**

**Azita Z.**
System Engineer
at Tara

★★★★★

> “Splunk Enterprise Security is excellent for analyzing malicious activities and detecting breaches. We can see, step by step, what happened.”
>
> **Read review »**

Chief cybersecurity architect Anat Garty claims that these detection mechanisms in Splunk Enterprise Security are helping her team to uncover and detect unknown threats. “Its insider threat detection capabilities for helping our organization find unknown threats and anomalous user behavior are great. They have a lot of built-in capabilities for analytics, and they can provide a lot of visualizations and insights into whatever is being brought into it.”

Azita Zoughi, System Engineer at Tara, appreciates that Splunk Enterprise Security provides accurate detection with context: “Splunk Enterprise Security is excellent for analyzing malicious activities and detecting breaches. We can see, step by step, what happened.”

Threat detection in Splunk Enterprise Security is not only more accurate, but faster, according to this security architect: “We’ve been able to help customers detect threats faster. It might be 5% to 10% faster in some cases. And since we can analyze large volumes of data, we’re not missing any particular data point or data set. That gives us an advantage.”

Splunk Enterprise Security includes over 1,700 out-of-the-box detections which have been researched and engineered by the Splunk team, which align with MITRE ATT&CK and other industry frameworks. This is why Surya Teja, Information Security Analyst at APCFSS, has high confidence in Splunk's threat detection abilities: "Splunk uses the MITRE ATT&CK framework, giving us new tactics and techniques based on issues observed in other businesses and industries and helping us to address novel threats to our network. MITRE ATT&CK is highly useful."

Splunk Enterprise Security can also detect the ever-illusive insider threats, as software company Infrasec owner Viktor Nagy explains: "Splunk's capabilities in insider threat detection are highly effective in assisting organizations in identifying unknown threats and anonymous user behavior. The sophistication of these features is notable, making them suitable and beneficial across a range of organizational sizes, from small businesses to large enterprises... Splunk Enterprise Security's insider threat detection capabilities enable us to effortlessly identify unknown threats and anonymous user behavior."

Nagendra N., Senior Manager ICT at Bangalore International Airport Limited, perhaps said it in the simplest of terms, "Splunk Enterprise Security helps us detect threats two to three hours faster."

**Viktor N.**
Owner at Infrasec

★★★★½

**"Splunk's capabilities in insider threat detection are highly effective in assisting organizations in identifying unknown threats and anonymous user behavior."**

**Read review »**

Reduces Alerts

## Risk-Based Alerting (RBA)

SOC managers often report that they struggle to keep up with the volume of security alerts across their network. Risk-based alerting (RBA) is a feature and framework in Splunk Enterprise Security that helps security analysts increase alert fidelity, prioritize the alerts that matter most, and in doing so, reduce overall alert volumes. RBA allows you to alert based on combinations of observations about a user or system. It acts like a layer between observation and alerting by building risk scores that only trigger when the observations and metadata associated with that user or system reach a certain threshold. This process transforms traditional alerts into potentially interesting observations which correlate into a high-fidelity security story for analysts to investigate.

Users report that RBA dramatically reduced their overall alert volume, producing higher-fidelity alerts. Users have also seen improved detection of low-and-slow threats from sophisticated attackers, improved investigation times, an ability to meet and exceed many security audit requirements, and more time for the SOC to pursue high-value activities like threat hunting and content engineering.

A Senior Analyst user at a software company found that risk-based alerts reduce their overall alert volume: "Splunk helped us reduce our alert volume because we could optimize our risk-based user analytics. I estimate that we decreased alerts by around 20 percent."

Another user, a Senior Security Engineer at a large insurance company, also saw a big improvement for his SecOps team due to risk-based alerting: "With risk-based alerting, we are now getting the right context for investigations. It definitely helps and speeds up the investigation. With risk-based alerting, I can see the chain of events. I can see what caused this to occur. I do not have a percentage, but I know my analysts are not getting the alerts that they have not completed by the end of the shift. Previously, that was not the case, so I am pretty pleased."

Other users, including this one, a Cyber Security Engineer at a large university, report similar experiences in terms of reduced alerts, which translates to faster resolution times: "The solution's analytical features helped us reduce our alert volume by 30 to 40 percent. Splunk significantly speeds up our security investigations."

**Sr Security Engineer**
at Insurance Company with
5,001-10,000 Employees

★★★★★

"With risk-based alerting, we are now getting the right context for investigations. It definitely helps and speeds up the investigation."

**Read review »**

Accurate alerts are essential for saving time and enabling a speedy response. Risk-based alerting streamlines this process. Manish Choudary, SOC manager for a large tech vendor, explains: “We have reduced our alert volume by around 50 percent with Splunk. When we first started creating and using Splunk use cases, we received around 700 alerts. Splunk can merge different sources of use cases into one to identify false positives, which has been very helpful for us.”

**Streamlines SecOps**

## Efficient SecOps

SecOps teams are overwhelmed by data volume, alert storms, and manual tasks. They need to act fast on incidents but might be juggling more than 25 different security tools that perform actions across detection, investigation and response. By unifying security analytics with automation, SecOps teams can streamline security operations to increase the speed and efficiency of response. Splunk Enterprise Security is natively integrated with additional tools to improve SOC performance and increase your level of protection against cyber threats.

## Rapid Incident Response

Splunk Enterprise Security enables the SOC to respond to incidents rapidly. Users often cite the benefits of Mission Control – a feature within Splunk Enterprise Security that delivers a single unified work surface – to help them rapidly detect, investigate and respond to incidents. A feature called “Response Plans” are also utilized by analysts to collaborate and execute incident response workflows for common security use cases. Response Plan templates allow users to see each phase of an incident response plan, assign key stakeholders to specific phases, and apply simple automation playbooks and workflows to tasks for quicker, more efficient remediation efforts. Analysts can access a defined and organized response process directly within Splunk Enterprise Security without spending extra time pivoting between other tools. The ability to collaborate and assign owners to each phase of the incident response process helps expedite the whole process, further simplifying an analyst’s workflow.

These features enable Splunk Enterprise Security users to more efficiently and effectively manage incidents and reduce mean time to investigate and respond (MTTR) to incidents. Users often cite “the gift of time” that Splunk Enterprise Security affords their team.

**Saves Time**

**Nagendra N.**
Senior Manager ICT at Bangalore International Airport Limited

★★★★☆

> "Splunk Enterprise Security has saved us two hours per day of investigation time."
>
> **Read review** »

Nagendra N, Senior Manager ICT at Bangalore International Airport Limited, says, "Splunk Enterprise Security has saved us two hours per day of investigation time." Similarly, Avinash G, Associate VP & Cyber Security Specialist at US Bank, explains, "Splunk Enterprise Security facilitates the acceleration of our security investigations, reducing the required time from one week to one day."

Sharan P., SOC Analyst at Topcon Omni Systems, Inc., cites a significant reduction in investigation time by using a few specific features in Splunk Enterprise Security. Sharan explains, "Splunk Enterprise Security helped reduce our mean time to resolve. Using the identity investigator and asset investigator applications definitely reduces the mean time for an investigation... It reduces investigation time by about 60 to 75%."

Raheel Asim, SOC analyst at Nera Philippines Inc., has seen a marked improvement in incident response times: "Splunk Enterprise Security helped speed up our security investigations. We now have an in-depth insight into endpoint usage. We've saved about 60% of our time if you compare Splunk to how we were operating before in terms of monitoring."

**Raheel A.**
Security Operation Centre (SOC)
Analyst at Nera Philippines Inc.

★★★★☆

> **“We now have an in-depth insight into endpoint usage. We’ve saved about 60% of our time if you compare Splunk to how we were operating before in terms of monitoring.”**
>
> **Read review »**

According to Saravana Kumar, a consultant at Fourth Dimension Technologies, the time savings are considerable: “It speeds up security investigations. It helps us detect threats faster. Everything is faster.”

Sneha Golhar, Senior Engineer at tech firm Wipro Limited points out how time savings translates into tangible financial savings: “By automating our monitoring and alerting with Splunk Enterprise Security, we’ve achieved a significant return on investment. This has freed up over 190 days of manual monitoring effort by our team, resulting in overall cost savings of around 30 million dollars.”

## Unify and Automate Threat Detection, Investigation, and Response

Splunk Enterprise Security fuels operational efficiency by unifying threat detection, investigation, and response security workflows. While Splunk Enterprise Security generates detection events and aids in security investigations, a native integration with Splunk SOAR (Splunk’s security orchestration, automation and response tool) allows analysts to automate the investigative and response tasks required to resolve security incidents. With a Splunk SOAR and Splunk Enterprise Security subscription, SOCs can seamlessly automate security tasks and processes to free up analyst time, investigate incidents more holistically, and respond to threats faster.

## Provides Actionable Intelligence

Senior engineering manager, Shakti Kumar, has been impressed with Splunk SOAR and its integration with Splunk Enterprise Security. Splunk SOAR has been leveraged to take care of the majority of security grunt work his analysts perform each day. “We use Splunk Enterprise Security because we have to manage a big infrastructure and may have many security vulnerabilities... Splunk Enterprise Security has helped us reduce our alert volume. The SOAR tool detects and automatically manages repetitive and generic alerts proactively.”

Venkatesh, a tech company security analyst, particularly values the time saving which is made possible by Splunk’s automated processes: “The solution has helped to speed up our security investigations. Once again, the automation will speed up the process of investigation. It saves a lot of time for analysts as it allows them to see the initial data... Splunk does the initial investigation for analysts and will escalate to analysts as needed. It might have reduced security investigations by 80% compared to earlier versions.”

Users cite the Mission Control feature as a mechanism for unifying across security workflows for easier incident management. A regional sales manager at Redington Ltd notes, "The Mission Control feature… provides a unified and simplified security operations experience for SOC analysts."

Other users have reported a considerable increase in overall efficiency due to the unified nature of Splunk Enterprise Security, such as this user, a Cyber Security Analyst at a large manufacturing firm: "We're at least twice as efficient with Splunk Enterprise Security at identifying risk, following up, tracing it throughout the chain, and resolving it."

SOC Manager Manish Choudhary has found that bringing all of the security data into one location means that his SecOps team are able to make even better use of the information: "Splunk is one of the easiest solutions for analyzing malicious activities and detecting breaches. It is flexible enough to work with small teams, and it provides a broad view of the data, allowing us to segregate and fine-tune the analysis based on the customer's requirements."

Splunk Enterprise Security also includes native capabilities for threat intelligence management. The security team at ATSS, led by Riaz Ahmmed, appreciates the integrated aspect of Splunk Enterprise Security, which embeds threat intelligence into investigations: "The actionable intelligence provided by the threat intelligence management feature is effective. The solutions are integrated into the platform."

**Manish C.**
SOC manager at a Tech Vendor
with 10,001+ Employees

**"Splunk is one of the easiest solutions for analyzing malicious activities and detecting breaches. It is flexible enough to work with small teams, and it provides a broad view of the data."**

**Read review »**

# Conclusion

Splunk Enterprise Security is a SIEM and security analytics solution trusted by SOCs around the globe. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context, and fuel operational efficiency.

- ✓ **Comprehensive Visibility** - Customers report that Splunk Enterprise Security delivers end-to-end security visibility with robust dashboards and visualizations, customizable reports, features like MITRE ATT&CK Framework and Threat Topology visualizations, and the ability to search and correlate across multi-cloud, on-premises, or hybrid data sources so maximum attack-surface coverage is achieved.
- ✓ **Accurate Detection with Context** - Customers report that Splunk Enterprise Security helps them to detect threats accurately, rapidly assess risk, and gain contextual understanding of attacks and threats using features like risk-based alerting (RBA), event-based detections, finding-based detections, and curated detections.
- ✓ **Efficient SecOps** - Customers report that Splunk Enterprise Security utilizes features like Mission Control and a native integration with an orchestration, automation and response tool, Splunk SOAR, to unify and automate workflows across detection, investigation, and response to fuel SOC operational efficiency.

In summary, Splunk Enterprise Security enhances the operational effectiveness of security teams and provides a robust, scalable solution. As a platform powered by AI capabilities, it ensures analytics at scale for continuous security monitoring and helps ensure cost-effective data optimization by detecting what matters, investigating holistically, and responding rapidly.

# About PeerSpot

PeerSpot is the authority on enterprise technology buying intelligence. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

PeerSpot does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, PeerSpot websites, and PeerSpot materials do not reflect the opinions of PeerSpot.

# About Vendor

Splunk Enterprise Security is the market-leading SIEM and security analytics solution trusted by SOCs around the globe. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context, and fuel operational efficiency. A platform powered by AI capabilities delivers analytics at scale for continuous security monitoring and helps ensure cost-effective data optimization. This foundation enables you to detect what matters, investigate holistically, and respond rapidly.

To learn more, visit splunk.com/es