aws marketplace

Fortinet FortiSIEM

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Fortinet FortiSIEM

Fortinet FortiSIEM Recap

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 detection
- Alleviating compliance mandate concerns for PCI, HIPAA and SOX
- Managing “alert overload”
- Handling the “too many tools” reporting issue
- Addressing the MSPs/MSSPs pain of meeting service level agreements

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "These aspects make Fortinet FortiSIEM a valuable choice."

SaurabhYadav5

Network Engineer at Ogma Consulting

- "The most fascinating aspect of FortiSIEM is its integration with the MITRE ATT&CK framework."

Muhammad Tayyab

IT Solutions Product Manager at a computer software company with 11-50 employees

- "It provides extensive logging and record-keeping for internal networks, cloud applications, and services as well as perimeter physical network security."

Oliver Jackson

Network Engineer at Laminar Communications Pty Ltd

"FortiSIEM allows you to match IPs with threat intelligence feeds from sources like Kaspersky or Anomali, adding valuable context."

LENIN RAMIREZ

SIEM MANAGER at a comms service provider with 1,001-5,000 employees

"The most valuable feature is the ability to view all the network events on a single pane and find the point of contact or point of the incident."

Vishwajeet Pandey

senior technical administrator at Ogma Consulting

"We have many application systems, and I can set up Fortinet FortiSIEM for users to monitor their systems."

Haiyang Lu

System Engineer - Security at a educational organization with 1,001-5,000 employees

"It's easy to manage. There's a web interface and a command line, depending on what the user is comfortable with. There's a large knowledge base available, and the support is timely."

Cletus Okolie

Senior Network Associate at AMCON, Inc.

What users had to say about valuable features:

"The tool's most valuable feature stems from the fact that I can see a complete analysis, like all the incidents that have happened, and it detects everything in real-time. It lets you know of the attack in real-time. The tool sends alerts and reports, so I think it is a useful tool.."

Verified user
Network administrator at a manufacturing company with 51-200 employees

Read full review

I use Fortinet FortiSIEM for complete infrastructure monitoring for security events. It supports a number of compliance rules that cater to different requirements. I find the real-time monitoring and correlation capabilities effective for security alerts. Fortinet FortiSIEM provides pre-built rules, with more than three thousand rules supplied, eliminating the need to define them from scratch. These aspects make Fortinet FortiSIEM a valuable choice.

SaurabhYadav5
Network Engineer at Ogma Consulting

Read full review

"The most valuable features of the solution is its integration with other technologies, especially its ability to collect logs from Cisco and Aruba devices along with Fortinet products. The tool has an endless number of templates, so based on a customer's use case, we can choose the templates, create the report as per compliance, and submit it to management for higher visibility.."

SreejeshSoman
Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

Read full review

"Fortinet FortiSIEM is valuable mainly for its features around firewall monitoring, intrusion detection, and authentication. It provides extensive logging and record-keeping for internal networks, cloud applications, and services as well as perimeter physical network security. Compliance management capabilities, although limited, are utilized by mature customers for reporting.."

Oliver Jackson
Network Engineer at Laminar Communications Pty Ltd

Read full review

"The most fascinating aspect of FortiSIEM is its integration with the MITRE ATT&CK framework. It maps threat vectors and IOCs on the MITRE framework to identify the kind and magnitude of a threat and the techniques used. This allows us to take requisite measures using the SOAR solution or by involving our team of SOC analysts and incident responders.."

Muhammad Tayyab

IT Solutions Product Manager at a computer software company with 11-50 employees

Read full review

"Fortinet FortiSIEM is really user-friendly. You can filter easily, find rules, and even create new rules. I appreciate Fortinet FortiSIEM the most because it is easy to search, filter, make rules, and look for correlations and events.

"For Fortinet FortiGate, it is easy to navigate through the tool itself, make policies, and look at events and logs. It is very easy to monitor on Fortinet FortiGate. I really appreciate it and believe anyone in the field can work with it easily.

"For FortiSOAR, it is easy to work with playbooks and rules for approvals, and everything there is straightforward. Fortinet FortiSIEM pulls the events from FortiSOAR, processes them, and applies the playbooks. It is simple in its functions, has correlations, and offers everything needed.

"I can find everything I need on Fortinet FortiSIEM. The filters, trends, and dashboard make it easy to use. The database, alerts, and customer service are excellent as well.."

Verified user

SOC Analyst at a tech vendor with 1-10 employees

Read full review

Other Solutions Considered

"I have used ArcSight. Fortinet stands out because it supports a broader range of technologies, allowing for greater integration within a system. Another key advantage is its robust analytics, making it easier to obtain specific information consistently.."

LENIN RAMIREZ
SIEM MANAGER at a comms service provider with 1,001-5,000 employees

Read full review

"I am using only Fortinet and Wazuh currently. I have worked with AlienVault and IBM QRadar in a different organization. The products have their own unique space in the market. SolarWinds has a logging engine. IBM is huge.."

Verified user
CISO at a financial services firm with 501-1,000 employees

Read full review

"Other vendors like IBM QRadar are more effective than FortiSIEM for a SOC use case because they specialize in that area. I would recommend that if you are trying to build a large SOC team. ."

HamedWasel
Senior Network Security Engineer at Orange

Read full review

"I like Azure Sentinel more than Fortinet FortiSIEM because it has a lot of documentation, information, and training material. The problem with Microsoft is that they keep changing things regularly and you need to be updated about their changes. For usability, Azure Sentinel is much better than Fortinet FortiSIEM.."

Haiyang Lu

System Engineer - Security at a educational organization with 1,001-5,000 employees

Read full review

"We implemented Fortinet FortiSIEM for our own use, and then we have been exploring the idea of using it for a customer-facing or a managed service provider multi-tenant SIEM. We offer managed SIEM services to our customers, and we've come to the conclusion that it is not well suited for that purpose. We are in the process of installing Microsoft Sentinel and Azure Lighthouse for a new service. ."

Verified user

Director, Infrastructure and Operations at a comms service provider with 11-50 employees

Read full review

“We were using Check Point before we migrated to FortiSIEM. We used Check Point for about ten years before we moved to FortiGate.

So, we switched to Fortinet from Check Point. There were two main reasons. First, we weren't getting the support we needed from Check Point. Second, the cost of renewing support for our end-of-life devices was too high. We had a limited budget, so we looked for a solution that could give us the same features and capacity as Check Point at a more competitive price. We opted for FortiSIEM because it met both of our requirements..”

Cletus Okolie
Senior Network Associate at AMCON, Inc.

Read full review

ROI

Real user quotes about their ROI:

"Many of my customers are happy and have provided positive reviews about their experiences. They continue to pay for services and see value in the investment.."

Oliver Jackson
Network Engineer at Laminar Communications Pty Ltd

Read full review

Use Case

Our primary use case for Fortinet FortiSIEM is mostly in government offices. We fully rely on vendors for implementation, and we generally review and approve the recommendations made by the implementation partners.

SaurabhYadav5
Network Engineer at Ogma Consulting

Read full review

"FortiSIEM is primarily used as a monitoring tool that can monitor all the incidents and events occurring in the network. The main concern of the customer is to view all the events and incidents on a single pane where everything can be managed.."

Vishwajeet Pandey
senior technical administrator at Ogma Consulting

Read full review

"Mainly, we are configuring various correlation rules in FortiSIEM to detect various types of cyber threats and cybersecurity attacks, particularly brute force attacks, denial of service attacks, and distributed denial. We are using it to identify suspicious activities by internal staff as well as outsiders, for any type of intrusion.."

Muhammad Tayyab

IT Solutions Product Manager at a computer software company with 11-50 employees

Read full review

"My primary use case for Fortinet FortiSIEM is systems monitoring and alerting. I use it for standard functions like log monitoring, incident detection, and notification.

My customers are mostly medium-sized enterprises ranging from engineering companies, mining companies, independent schools, and government departments to agencies.."

Oliver Jackson

Network Engineer at Laminar Communications Pty Ltd

Read full review

"I normally use the solution in my company as part of SOC. The tool is implemented to collect logs from all networks, perimeter devices, and security devices. We are using all kinds of SIEM tools to collect logs, especially security logs from all network devices, and analyze all those logs. Fortinet FortiSIEM works for enterprise and banking customers and BFSI customers, as most of them use Fortinet FortiGate devices for the security of the perimeter devices.."

SreejeshSoman
Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

Read full review

"I have a lot of experience working with solutions such as Fortinet FortiSIEM, FortiSOAR, and FortiGate. I have also worked with ImmuniWeb. However, I did not have the credentials or the software to work with ImmuniWeb, which is why I was searching for more information on the website to learn more about the tool.

"In the company I work for, we have a partnership with Fortinet.

"In my organization, I work on Fortinet FortiSIEM in the cloud.."

Verified user
SOC Analyst at a tech vendor with 1-10 employees

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"From a new user's perspective, setting up Fortinet FortiSIEM could be rated as a five or six out of ten. However, with my four years of experience, I would rate the setup an eight out of ten.."

Oliver Jackson

Network Engineer at Laminar Communications Pty Ltd

Read full review

"The initial installation requires some tech knowledge. You should have prior understanding of modules, collectors, workers, supervisors, and databases. However, after installation, it's really easy to operate.."

Muhammad Tayyab

IT Solutions Product Manager at a computer software company with 11-50 employees

Read full review

"The initial setup can vary from being easy to moderate depending on the network size. If the network is small, it might be easy. That said, if it's semi-small or semi-large, it's a moderate setup.."

Vishwajeet Pandey
senior technical administrator at Ogma Consulting

Read full review

"The initial setup is easy. If you want to deploy FortiSIEM on-premise, you need to purchase a specific appliance or install it on your hardware. I have deployed FortiSIEM both on-premise and in the cloud, managing both environments effectively.

Deployment depends on the architecture since FortiSIEM uses various components, such as the supervisor, event collector, and worker. It can be set up in just one day if you're deploying it as an all-in-one solution.."

LENIN RAMIREZ
SIEM MANAGER at a comms service provider with 1,001-5,000 employees

Read full review

“At the beginning the product's initial setup phase was complex. Lately, since I have started to understand the tool, the setup phase has become easy.

The solution is deployed on an on-premises model with VMs in a local data center.

The solution can be deployed in four days. One day is for installing the VMs, one day is for understanding the tool's dashboard and its rules, one day is for installing the agents and adding the equipment, and one day is for seeing what the clients want exactly..”

Verified user

Read full review

Network administrator at a manufacturing company with 51-200 employees

“If one is difficult and ten is easy to set up, I rate the product's initial setup phase a nine out of ten. It is not very complicated, but a tech person who has the expertise to install and scale implement all these features would be required to implement the tool.

The product's installation model depends on the company's compliance and IT policies. Most customers prefer implementing an on-premises model. When considering commercial and upfront investment, customers are ready to go for cloud solutions as well. But in my experience, most customers prefer to implement an on-premises model.

The time required to deploy the solution depends on how big your network is currently. It might take two days to up to two weeks, so that is the normal project implementation time. It is always based on how big our network is and how we know our network. If customers have good visibility and understanding of their network, good access, and all the authentication paths, the integration will be much easier. In some cases, it might take more than two weeks. On average, I think it will take one to two weeks to complete installation.

The deployment of the tool is always for the SOC part of a company. It is used for real-time network analytics.

For the deployment, we discuss all the requests or use cases with the customer and understand their network topology. Most of the time, we access their platform for installation, and so we deal with virtualization platforms, like VMware ESXi, and based on that, we will download the SIEM pack from Fortinet. Once the installation has been completed, we try to find all the devices in the network that we need to monitor so we can enable all those processes. It is the normal deployment procedure we are following for implementation. Once the primary implementation has been completed based on customer use cases or complaints, we might create those dashboards and templates for reporting..”

SreejeshSoman

Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

Read full review

Customer Service and Support

Fortinet's customer support is okay, but not very good. They take some time to respond because they need logs and investigations, which delays the response time. I expect faster responses for the issues raised.

SaurabhYadav5
Network Engineer at Ogma Consulting

Read full review

"The customer support from Fortinet is good. There is a knowledgeable, though small, team of support engineers around the world. I have come to know them all by name.."

Oliver Jackson
Network Engineer at Laminar Communications Pty Ltd

Read full review

"We have expertise with the product, so we don't use technical support often. We only require support for the error mark, and the support is quick and fast for that.."

Drissa DOUMBIA
Network Security Engineer at Technicom Mali

Read full review

"The solution's technical support didn't help our company a lot. When it came to Fortinet FortiSIEM, we added the devices, and started making rules, but when we asked a question to the tool's support team, it took them a long time to answer. I rate the technical support a five out of ten.."

Verified user
Network administrator at a manufacturing company with 51-200 employees

Read full review

"With technical support, I often direct tickets to them in terms of licensing, and within a maximum of two to three hours, the license will be active. They are very helpful. They are very responsive. They are always responding to the tickets and assisting us. You can show your customer their level of engagement. It's very impressive. Customers are happy.."

ZaidoonAbuhanak
SALES PRODUCT MANAGER at NOURNET

Read full review

"Technical support in my city, specifically in Islamabad or Rawalpindi, is decent. I would rate it seven out of ten.

Local tech support is available, however, for more critical or technical issues, we depend on the OEM directly, especially when it comes to on-prem solutions.."

Muhammad Tayyab
IT Solutions Product Manager at a computer software company with 11-50 employees

Read full review

Other Advice

If planning to use Fortinet FortiSIEM, it is important to know that it provides pre-built rules, which is a significant advantage. It is suitable for medium to enterprise customers. Overall, I would rate Fortinet FortiSIEM seven out of ten.

SaurabhYadav5
Network Engineer at Ogma Consulting

Read full review

"I would rate FortiSIEM eight out of ten. It's a nice product and is used by major governmental infrastructures and organizations. I would definitely recommend it to other users.."

Muhammad Tayyab
IT Solutions Product Manager at a computer software company with 11-50 employees

Read full review

"If you want to set it up yourself, seek expert support before starting. If considering a service, contact Fortinet for a recommended service provider in the FortiSIEM space.

I'd rate the solution eight out of ten.."

Oliver Jackson
Network Engineer at Laminar Communications Pty Ltd

Read full review

"I can recommend FortiSIEM, but it depends on customer needs, network size, and preferences. Customers can also consider replacing a physical SOC team with FortiSIEM.

I'd rate the solution eight out of ten.."

Vishwajeet Pandey
senior technical administrator at Ogma Consulting

Read full review

"I wish to remain anonymous, with no names for my company or myself. I prefer written communication rather than voice-based.

"Based on my experience, I would rate this solution 9 or 10 out of 10.."

Verified user
SOC Analyst at a tech vendor with 1-10 employees

Read full review

"For threat detection, some AI-based analytics tools are there, and it is one of the latest features in the product. The AI helps mitigate threats.

In terms of the tool's ability to streamline customer security workflow, the product normally searches events in real-time, so customers will get alerts of the event in real-time. Compared to other products like Splunk or Oracle, I think Fortinet FortiSIEM is more reliable in real-time.

If there is proper support and better technical capabilities, it can become a good solution.

I rate the tool an eight out of ten.."

SreejeshSoman
Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

Read full review

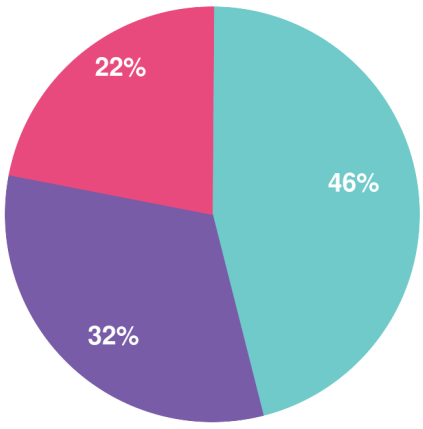
Top Industries

by visitors reading reviews

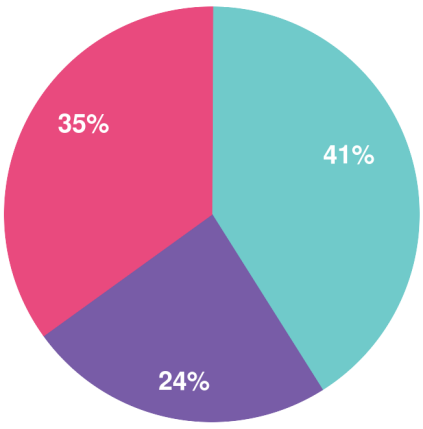
Financial Services Firm	10%
Comms Service Provider	9%
Computer Software Company	9%
Manufacturing Company	6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

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