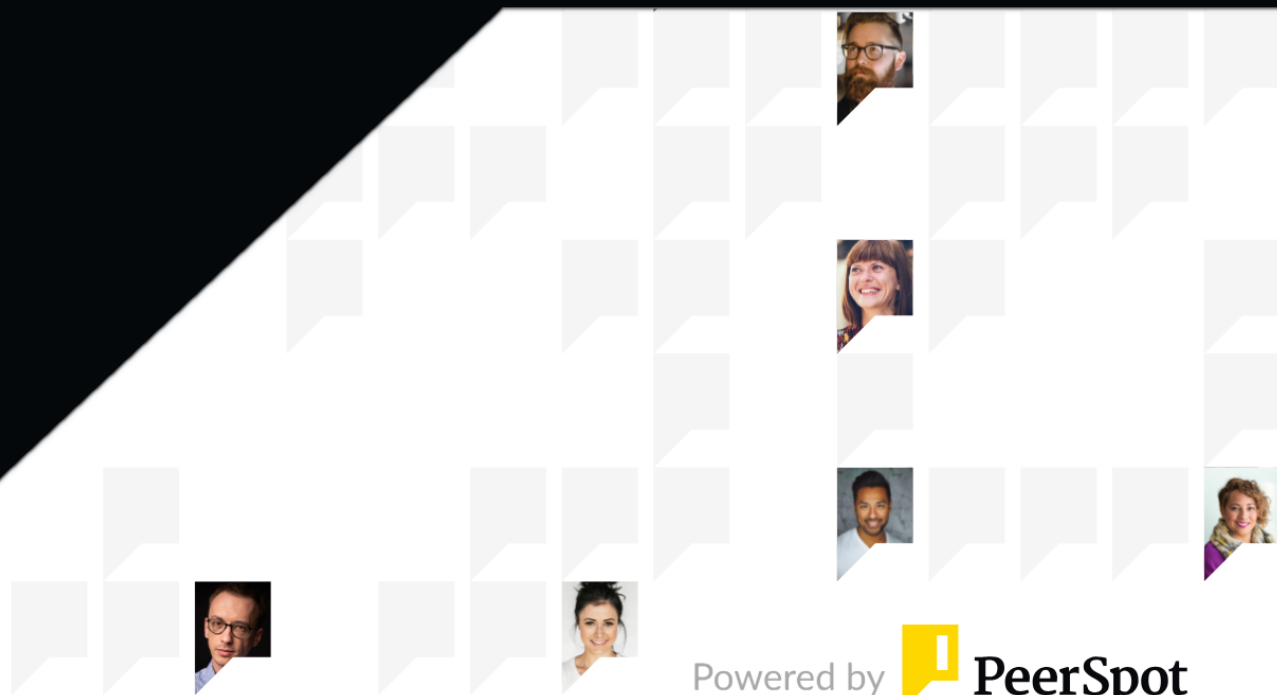


aws marketplace

FortiCNAPP

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 15

ROI..... 16 - 18

Use Case..... 19 - 22

Setup..... 23 - 25

Customer Service and Support..... 26 - 29

Other Advice..... 30 - 33

Trends..... 34 - 35

About PeerSpot..... 36 - 37

Product Recap



FortiCNAPP

FortiCNAPP Recap

FortiCNAPP is a comprehensive cloud security platform focusing on ease of use and machine learning-driven anomaly detection. It offers robust compliance reporting, seamless integration, and continuous monitoring, making it an essential tool for organizations managing multi-cloud environments and security configurations.

FortiCNAPP provides significant capabilities in cloud security, compliance, and vulnerability management. Designed for organizations needing efficient monitoring, it enables detection of anomalies across cloud infrastructures while optimizing security posture and ensuring compliance with environments like AWS and GCP. The platform offers in-depth insights through scanning of IAC scripts, host systems, and cloud configurations. Recognized for effectively managing security posture, it safeguards Kubernetes and container environments, providing comprehensive threat detection and response. However, some areas like visibility, IAM security controls, and compliance metrics need improvement. Users face challenges with alert setup and lack intuitive design, alongside issues like FedRAMP authorization absence and complexity in the data model.

What are the key features of FortiCNAPP?

- **Ease of Use:** FortiCNAPP simplifies security management for cloud environments.
- **Machine Learning Anomaly Detection:** Automatically identifies and prioritizes threats.
- **Compliance Reporting:** Streamlines compliance procedures and reporting.
- **Seamless Integration:** Ensures smooth operation across multi-cloud environments.
- **Continuous Monitoring:** Provides ongoing oversight of security vulnerabilities.
- **Multi-Cloud Integration:** Enables swift response to misconfigurations and vulnerabilities.

What benefits should users expect when evaluating FortiCNAPP?

- **Time Efficiency:** Reduces time spent on compliance and threat management.
- **Improved Security Posture:** Enhances protection for cloud and container environments.
- **Valuable Security Insights:** Provides in-depth analysis for proactive threat response.
- **Noise Reduction:** Distills security logs to minimize alert fatigue.
- **Operational Effectiveness:** Facilitates seamless multi-cloud security management.

FortiCNAPP is implemented extensively by industries needing reliable cloud security, such as finance, healthcare, and technology sectors. It supports organizations in enhancing cloud infrastructure protection, ensuring compliance, and strengthening vulnerability management. By integrating with platforms like AWS and GCP, businesses can optimize security posture in their cloud deployments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“If you want to turn your cloud findings into actionable security work, FortiCNAPP is the way to go.”



Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees



“FortiCNAPP is a competitive and robust solution, the only one in the IT sphere that addresses all quadrants in the Gartner Quadrants.”



Mark Freeborough

Client Manager at MLL Telecom Ltd



“FortiCNAPP has positively impacted my organization by providing centralized visibility and consolidating our cloud security posture management, helping us identify misconfigurations and public accessibility issues, which allowed us to enhance IAM governance and visibility on vulnerabilities.”



Pranav Telang

DGM at Airtel Digital



“The machine learning capability in Lacework FortiCNAPP is used for threat detection, and automated policy recommendation helps to improve my security measures in general.”



Sai Tharun Kumar

Software Engineer at a university with 5,001-10,000 employees



“The automated policy recommendations when pushing any firewall policies using Fortinet were really good and performed their job effectively.”



Sudarson Prabhu

Security Consultant at Payatu



“FortiCNAPP definitely brings time-saving benefits, and security is the main concern for the company.”



Munjal Bhargama

Owner at IT CARE



“What I personally appreciate about FortiCNAPP is that I think it is a good product and a good firewall because it usually offers many options for the company.”



José Manuel Viejo

Senior Sales Account Manager at Hard2bit Cybersecurity

What users had to say about valuable features:

“The best features FortiCNAPP offers, in my opinion, include compliance and audit capabilities, IAM identity management, and security rectification in configurations, along with vulnerability management, which helped us rectify thousands of overwhelmingly security vulnerabilities. I find myself relying on all of them day-to-day, including threat detection, which is really good..”

Pranav Telang

DGM at Airtel Digital

[Read full review](#) 

“Regarding the firewalls, I think it is good to have a comprehensive security software in place, and I believe they provide crucial protection for our network.

“What I personally appreciate about FortiCNAPP is that I think it is a good product and a good firewall because it usually offers many options for the company. I believe my partners, who are technicians, often prefer this kind of product because it is better for the end-user.

“Automated policy recommendations with this solution do help to improve security..”

José Manuel Viejo

Senior Sales Account Manager at Hard2bit Cybersecurity

[Read full review](#) 

The most valuable features in FortiCNAPP include robust network segmentation and restricting access to network assets. It also supports security measures by leveraging security fabrics for better enforcement and policy enforcement. FortiCNAPP integrates with SIEM solutions, and we offer different SIEM options that work with Fortinet and AlienVault, among others, providing multiple scenarios.

FortiCNAPP's automated policy recommendations significantly help improve security measures as part of an overall service wrap. When deploying a Fortinet SD-WAN or network, these tools provide greater visibility to vulnerabilities and enhanced security on the network. It functions as a proactive tool, enabling me to identify threats quickly and automate responses..”

Mark Freeborough

Client Manager at MLL Telecom Ltd

[Read full review](#) 

“The machine learning capability in Lacework FortiCNAPP is used for threat detection.

“Automated policy recommendation helps to improve my security measures in general.

“I usually use certain policies in my workspace, like if there are some alerts or something.

“Continuous compliance and security monitoring are good, but they need more improvement in the vulnerabilities part..”

Sai Tharun Kumar

Software Engineer at a university with 5,001-10,000 employees

[Read full review](#) 

“FortiCNAPP offers features that stand out to my clients and to me as a reseller. It is not just a reporting tool; it gives you the actual context around cloud risk in a way that helps with prioritization, investigation, and compliance tracking, taking away a lot of your time and saving your resources to focus on what's important. The vulnerability and workload risk detection with severity-based prioritization is a key player, compliance reporting that supports frameworks such as PCI, SOC 2, and CIS is a game changer, and noise reduction by consolidating and prioritizing alerts saves a lot of time.

I can tell you more about how the compliance reporting helps my clients. I have not had feedback from them regarding how it made it easier, but I have had showcases where I can demonstrate from a PCI perspective as well as a SOC 2 that it is a requirement and how it addresses that compliance framework.

FortiCNAPP has impacted my clients positively. The strong visibility into the cloud security posture and operational risk is a massive impact for clients. From a compliance reporting perspective, it is valuable when they need evidence for audit and control testing, fitting well into security operations models where cloud findings need to be handled alongside broader SOC activity..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

“ I find the cloud configuration compliance scanning mature. It generates a lot of data and supports major frameworks like ISO 27001 or SOC 2, providing reports and datasets. Another feature I appreciate is setting custom alerts for specific events. Additionally, I value the agent-based monitoring and scanning for compute nodes. It gives us deeper insights into our workloads and helps identify vulnerabilities across our deployed assets.

One key aspect of the agent that stands out is its capability to distinguish between active and inactive packages on compute nodes. This feature reduces the number of actionable vulnerabilities by focusing on packages actively running in the environment rather than all installed packages.

I noticed that it was quite noisy, with many alerts about things I wasn't particularly concerned about. However, over time, Lacework's anomaly detection improved by establishing baselines of normal activity. It now alerts us only when there are deviations from these baselines. Integrating with Slack was especially beneficial—I set up a dedicated Slack channel just for Lacework alerts. This allowed me to focus on the alerts that required attention..”

Verified user

Director of Security Operations at a insurance company with 51-200 employees

[Read full review](#) 

Other Solutions Considered

“There are very few solutions out there for cloud infrastructure. When it comes to physical infrastructure, there are already many tools. But the cloud industry is just beginning. I have worked with a few of the cloud solutions and I found Lacework is the most useful one because it has various categories of alerts..”

Srinivas Shankar

Infosec Engineer - Lead at a tech vendor with 1,001-5,000 employees

[Read full review](#) 

“I see some big differences between Lacework FortiCNAPP and Microsoft.

“The ease of access is better with Lacework FortiCNAPP, while Microsoft is more complex..”

Sai Tharun Kumar

Software Engineer at a university with 5,001-10,000 employees

[Read full review](#) 

“I have not seen many other similar solutions. I have a genuine appreciation for Lacework. Comparing it to other products wouldn't be equitable, as my experience with those alternatives is limited. Thus, it wouldn't be justifiable to make a definitive judgment about one product being superior to Lacework or vice versa. I can affirm, however, that Lacework is highly commendable and is delivering substantial benefits for our needs..”

Russell

Information Security Engineer at a insurance company with 501-1,000 employees

[Read full review](#) 

“Lacework is pretty good at ingesting data to correlate workloads and account behaviors. As long as you have the tool properly configured, it will give you correlation information. It's not as much information as you might get out of some other products, potentially, but it does give you good correlation information against some of those standards that I mentioned. To the extent that there's overlap in those standards, we do see the same kind of compliance or other issues pop up more than once..”

Jim Shank

VP of Engineering Security at a tech services company with 201-500 employees

[Read full review](#) 

“We have used a lot of solutions. We had Sysdig. We had something from Rapid7. We had Prisma Cloud as well. Lacework stands out in reducing the alert noise, having the right context for investigations, and saving time. That was the main driver for us to switch to Lacework.

If I have to compare Lacework with other tools, it covers the basis, but from the detection perspective, when you combine different portions of the data that you are receiving and create a comprehensive alert for your analysis, that is the advantage that we have from Lacework against others. That is great because we are only focused on the things that we need to fix..”

Carlos Vitrano

Cloud security director at Medallia

[Read full review](#) 

“Lacework's advantage is its ability to differentiate between active and inactive packages through the agent. Most other CNAPP solutions don't offer this capability, and competitors like Wiz don't implement it as effectively.

I've used several other platforms, such as Wiz and Prisma, and they all cover similar functionalities, such as scanning for misconfigurations in the cloud against compliance standards, monitoring IAM configurations for risks, logging and anomaly detection, host-based vulnerability scanning, and IAC code scanning. Wiz offers better reporting and ease of data extraction from datasets.

Lacework, on the other hand, is generally more cost-effective and becomes user-friendly once you're accustomed to its UI conventions. However, extracting specific data from Lacework can sometimes be challenging..”

Verified user

[Read full review](#) 

Director of Security Operations at a insurance company with 51-200 employees

ROI

Real user quotes about their ROI:

“I have seen a return on investment for my clients. They need fewer employees from a SOC perspective where people are deployed in their SOC, as well as significant time saved. When you save time, you save money..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

“We have seen an ROI. It has been three to four years since we have been using the tool. If we had gone to another tool in the past, we would have been spending a lot of money and resources as well..”

Carlos Vitrano

Cloud security director at Medallia

[Read full review](#) 

“From my perspective, there's an immediate return on investment because, as I mentioned, you would need a team of people to deal with these sorts of things, whereas Lacework does most of the hard labor for you. Just by adopting Lacework as a solution, you eliminate the need for having a team of people. One person can do it..”

Daniel Vukadinovic

Techology Operations Lead at a computer software company with 11-50 employees

[Read full review](#) 

My experience with FortiCNAPP's pricing demonstrates that we conduct extensive work with Fortinet and minimal work elsewhere. We focus on selling the value of the solution, which I find to be highly competitive within the Fortinet world. Overall total cost of ownership is critical; we demonstrate ROI by showing how it saves time and optimizes roles for staff to focus on more important tasks. The pricing is competitive, further supported by special pricing based on our engagement level with Fortinet, which is advantageous. FortiCNAPP is a competitive and robust solution, the only one in the IT sphere that addresses all quadrants in the Gartner Quadrants.

Mark Freeborough

Client Manager at MLL Telecom Ltd

[Read full review](#) 

“I believe that quantifying the tangible gains from deploying a security solution is a challenge. Especially in the realm of security, the implemented solutions work to avert potential significant losses that might be hard to measure. The return on investment is evident in the form of enhanced security and prevention of major security incidents. While the value gained isn't easily quantifiable in a monetary sense, it's clear that the expense is justified. Essentially, purchasing and implementing such solutions incurs a cost without direct monetary returns. However, if we were without such solutions, the alternative would involve hiring additional staff, particularly SOC engineers, to manage anomalies, issue investigations, and alert correlation. .”

Russell[Read full review](#) 

Information Security Engineer at a insurance company with 501-1,000 employees

“We have definitely seen ROI with Lacework. We used to have more people monitoring things in a more manual way. Lacework has reduced the amount of effort and time applied to monitoring.

We've also leveraged some of the integrations, for example with Jira, so that when an anomaly or alert comes in, we automatically generate a Jira record, which somebody then has an assigned action to go look at. Those are examples of where it's really saved some time. Instead of having someone say, "Yep, there's an alert. I need to create a ticket," it automatically creates a ticket, assigns it to someone on our team, and then they look at it, investigate, and disposition it accordingly..”

Jim Shank[Read full review](#) 

VP of Engineering Security at a tech services company with 201-500 employees

Use Case

“The primary focus of Fortinet for us is to monitor firewall traffic, create firewall rules, and manage the IDS and IPS for the firewall. We obtained a tool called FortiAnalyzer for monitoring and threat detection..”

Sudarson Prabhu

Security Consultant at Payatu

[Read full review](#) 

“FortiCNAPP is mainly used from a security point of view. Some VPNs charge for their solutions, but Fortinet provides a free-of-cost VPN solution, making it more reliable and cost-effective for clients..”

Munjal Bhargava

Owner at IT CARE

[Read full review](#) 

FortiCNAPP is typically used for network access control. The standard use cases for FortiCNAPP center around reporting and automated responses, particularly in IoT environments and workflow automation. Various environments require these tools, and SOC users may utilize them as well. FortiCNAPP serves as a gateway to numerous other products and services in the Fortinet portfolio.

Mark Freeborough

Client Manager at MLL Telecom Ltd

[Read full review](#) 

“We use the tool for two main purposes: vulnerability management and monitoring. We utilize it to scan all of our IAC scripts and configurations across our AWS and GCP environments. Additionally, we employ its agent to scan our compute nodes. This covers three main areas: cloud configuration, host systems, and IAC code, all essential for vulnerability management. We primarily focus on monitoring AWS CloudTrail to detect anomalous activities and risky behavior..”

Verified user

Director of Security Operations at a insurance company with 51-200 employees

[Read full review](#) 

“My main use case for FortiCNAPP, from my previous experience distributing it or now as a reseller, is for anyone who's looking for a strong cloud security platform and gaining visibility into risk, malicious configurations, any vulnerabilities, as well as your workload behavior across cloud environments.

The fact that it is built as a cloud native application protection platform means it is aimed at helping security teams manage their cloud posture, the workload protection, identity risk, and compliance from a central place. When you consider it as a solution that someone can use in their SOC, it is most valuable when you need clearer visibility across multi-cloud environments, which is a challenge in today's environment. If you want to turn your cloud findings into actionable security work, FortiCNAPP is the way to go..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

“My main use case for FortiCNAPP is majorly for AWS, specifically for security posture management and auditing so that the user and whoever is using this can capture what is necessary.

“A specific example of how I use FortiCNAPP for AWS security posture management is that we created resources manually, which sometimes led to misconfigurations in the customer requirements, and we have used FortiCNAPP to detect services that are publicly exposed and security groups with wide ranges of open IPs for ingress or egress, along with checking unencrypted databases and tightening IAM permissions.

“I also have a unique use case of FortiCNAPP for one of Asia's largest growing country government projects where we identified users with excessive permissions not required by them, due to many users being onboarded in the government sector, so we used FortiCNAPP to identify all cloud identities and recommended the right permission sets for them..”

Pranav Telang

DGM at Airtel Digital

[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.

“The deployment time for the solution usually depends on the specific requirements. I would estimate it might take one day or two to four hours depending on those requirements..”

José Manuel Viejo

Senior Sales Account Manager at Hard2bit Cybersecurity

[Read full review](#) 

“The installation of Lacework FortiCNAPP is quite complicated, especially regarding the settings.

“We face some issues with troubleshooting the settings..”

Sai Tharun Kumar

Software Engineer at a university with 5,001-10,000 employees

[Read full review](#) 

“My experience with pricing, setup cost, and licensing for FortiCNAPP revolves around Fortinet being an enterprise vendor. Pricing is always a discussion point. FortiCNAPP is not a cheap solution, and licensing around it can become very expensive for specific customers. However, if the use case is there and the need is a demand, then pricing is the last thing that will be the focus..”

Charl Pinches

[Read full review](#) 

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

“It is deployed on the cloud. Regarding maintenance, certain tasks must be done, including policy maintenance and alert review. However, beyond these responsibilities, there's not much to manage, given its complete Software as a Service (SaaS) nature. There's no need for involvement in tasks like storage management or endpoint maintenance.

.”

Russell

[Read full review](#) 

Information Security Engineer at a insurance company with 501-1,000 employees

“The product is very straightforward to deploy across an entire AWS or GCP organization. They offer automation via Terraform and CloudFormation templates, which allow deployment across all accounts with the appropriate permissions. As for Azure, I'm unsure about its compatibility..”

Verified user[Read full review](#) 

Director of Security Operations at a insurance company with 51-200 employees

“It is a cloud solution. I was involved in its deployment from the beginning. I started with the definitions of the success criteria that I was going to use with the team. I had the team implement it, and I was supervising. I was practically aware of every single aspect of this work.

Its initial deployment was super straightforward. It was super easy. It also depends on how your infrastructure is managed. In our case, it was easy to deploy the agents. For the entire environment, it took us four days. There were three to four people involved.

In terms of maintenance, from our side, only the agents need to be maintained. It requires us to download the new version of the agent and deploy it. Cloud Security Posture Management does not require any maintenance from our side. They are doing that by themselves..”

Carlos Vitrano[Read full review](#) 

Cloud security director at Medallia

Customer Service and Support

“Fortinet's technical support is definitely helpful and responsive. The response time for solutions or support is quick compared to other UTM's, which is beneficial..”

Munjal Bhargava

Owner at IT CARE

[Read full review](#) 

“The customer support for FortiCNAPP is pretty good from a South African perspective. Most support runs via the distribution channel, and only once it gets to layer two or tier two does it get pushed through to your Fortinet system engineers, where support is very quick..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

“Their technical support is good. We have a Slack channel. We have monthly meetings. We have a dedicated customer success manager. He is taking care of all of the tickets that we are creating. We have probably opened five cases so far, and they were able to resolve them all. It might not have been at the pace that we were expecting, but in the end, they are supportive. I would rate them an eight out of ten..”

Carlos Vitrano

Cloud security director at Medallia

[Read full review](#) 

“I had a local vendor providing Fortinet support, and their support was very quick and responsive. In comparison, Wazuh offers clear technical requirements and FAQs on their website, but understanding problems required technical expertise to navigate the documentation effectively.

“Since Fortinet support is provided by the local vendor and is always available and quick, I would rate them a 10..”

Sudarson Prabhu

Security Consultant at Payatu

[Read full review](#) 

I provide deployment services, supplying, installing, and maintaining the entire service.

Some of my colleagues may utilize FortiCNAPP's integration with DevOps tools, though I am not extensively familiar with this capability. My technical teams do utilize integration with DevOps tools, as it performs significantly with automation regarding sophisticated challenges. We have an in-house development team that works on this, focusing on how it integrates primarily with the security fabric. Fortinet has their own developer networks, and we also explore what they may have accomplished previously. In terms of integration, FortiCNAPP performs substantially with DevOps tools, though this would depend on what our teams choose to implement..”

Mark Freeborough

Client Manager at MLL Telecom Ltd

[Read full review](#) 

“One thing I appreciated about Lacework was the support I received from their team. I regularly met with them to provide feedback on what worked well and what didn't in their modules. They took my feedback seriously, often implementing it into features, hotfixes, and interface changes. Part of the reason for this was my clear and detailed communication style.

While some customers might say, "This sucks," I made sure to explain exactly why and how I would suggest fixing it. This approach was well-received by their product managers, who valued my input. As a premium customer, I have access to account managers. Its support is very good.

Sometimes, the support process was quite slow. While they acknowledged my tickets promptly, resolving issues could take weeks as they liaised back and forth with engineering to diagnose and determine solutions. However, the support I received from my account management and technical account management teams was very good. .”

Verified user[Read full review](#) 

Director of Security Operations at a insurance company with 51-200 employees

Other Advice

Some of my colleagues may utilize FortiCNAPP's integration with DevOps tools, though I am not extensively familiar with this capability. I would rate this review as a nine out of ten.

Mark Freeborough

Client Manager at MLL Telecom Ltd

[Read full review](#) 

“For others looking into FortiCNAPP, I recommend it for tightening security in public clouds as it has worked well for us compared to other options such as Palo Alto Prisma and CrowdStrike. I would rate this product 8.5 out of 10..”

Pranav Telang

DGM at Airtel Digital

[Read full review](#) 

“We are a partner of FortiGate, but we have to buy from a distributor to acquire FortiGate products. This is necessary for us, and I think this process is probably the same in England, but I am not certain.

“I think it is easy to integrate FortiCNAPP with other tools, including DevOps tools and products such as Cisco and Palo Alto.

“I would rate this review an eight overall..”

José Manuel Viejo

Senior Sales Account Manager at Hard2bit Cybersecurity

[Read full review](#) 

“Policy implementation is one part of the solution; every customer needs particular policies for groups or department-wise needs, which takes time. I am not currently using FortiCNAPP's integration with DevOps tools; some inquiries are running, but it will take time to close, and I hope it will be done in the future.

The time for implementation of this product depends on the network and users; it varies based on how many users and networks are involved, as well as what downtimes are allowed. The maximum number of users I have encountered is approximately 300 or 400.

It took me weeks to deploy, gradually applying the policies and all of that, and it depends on the circumstances. FortiCNAPP's continuous compliance and security monitoring are gradually upgraded, which is why the solutions also get upgraded, and it depends on the UTMs.

I would rate this product 9 out of 10..”

Munjal Bhargava

Owner at IT CARE

[Read full review](#) 

“I must ensure that you understand the interface and the model that you want to expect from it. I believe it is flexible enough to get the right interface or data that you want to see from a CNAP perspective.

From a feature perspective, I wish more people knew about the integration potential with the broader Fortinet ecosystem, which is a massive game changer. If you are already invested in a Fortinet ecosystem, it is a no-brainer to go for FortiCNAPP to look after your cloud platform.

Integration depth can matter a lot for FortiCNAPP. Value can be improved significantly when it is connected into an existing SOC stack. However, if you are not running any form of a Fortinet estate, it can become complex.

I rate FortiCNAPP an eight because, from my experience, it is best viewed as a platform that helps a SOC make cloud risk visible, understandable, and actionable, which is exactly what I prefer using it for or positioning it to customers. However, as a stand-alone product, if you do not have the experience from an existing cloud or understanding of how to manage cloud security at scale, then there might be a bit of a challenge. FortiCNAPP is a credible solution that adds real value when you properly integrate it with your existing security operations..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

“I am familiar with [FortiCNAPP](#), as it is a vulnerability management tool that I have worked with before.

“I confirm that FortiCNAPP is also an on-premises solution.

“I do not know how many people were involved in the deployment because it occurred before I joined the organization.

“I did not use FortiCNAPP's machine learning for threat detection at that time

because artificial intelligence and machine learning were not popular on every product in 2022, and the feature was not available.

“I did not use FortiCNAPP's integration with DevOps tools because the organization I worked for was a service-based entity focused on e-book publishing, not a product-based one.

“Using the MITRE ATT&CK framework with FortiAnalyzer helps us identify tactics and techniques indicating compromise, allowing us to check for false positives and move forward with incident management if it is a true event.

“I am not fully satisfied with FortiCNAPP because the product has limited functions and it requires the use of other Fortinet tools for complete capabilities.

“Considering my experience with FortiCNAPP, I can give it a rating of six to seven because the job it is assigned to perform is good, but the capabilities and improvements we sought were not achieved. My overall review rating for this product is six..”

Sudarson Prabhu

Security Consultant at Payatu

[Read full review](#) 

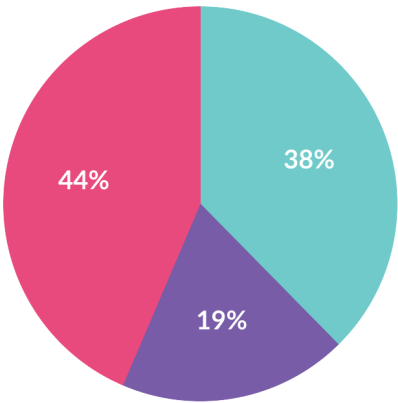
Top Industries

by visitors reading reviews

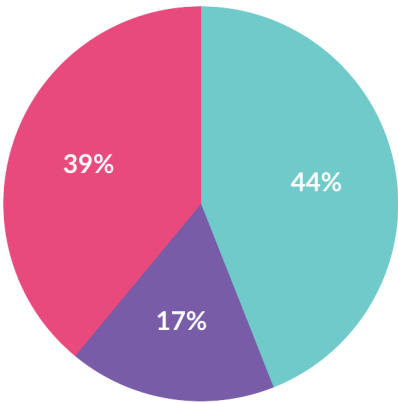


Company Size

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 cloud, AI, and business software. 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