



**Lacework FortiCNAPP**

# Reviews, tips, and advice from real users



Powered by  **PeerSpot**

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 13

Other Solutions Considered..... 14 - 16

ROI..... 17 - 18

Use Case..... 19 - 21

Setup..... 22 - 25

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

Other Advice..... 30 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

# Product Recap



Lacework FortiCNAPP

# Lacework FortiCNAPP Recap

Lacework FortiCNAPP provides robust cloud security, combining vulnerability management and multi-cloud insight with user-friendly controls, machine learning detection, and compliance support.

Lacework FortiCNAPP specializes in cloud security by merging machine learning anomaly detection with agent-based vulnerability management to offer detailed alerts and compliance reports. Its comprehensive approach allows continuous monitoring across AWS and Kubernetes, providing insights from an attacker's perspective. The platform offers automation and seamless Slack integration, facilitating collaborative and efficient cloud security management. Users value its ability to handle multi-cloud environments and scan IAC scripts, configurations, and compute nodes across AWS and GCP.

## What are the key features?

- Machine Learning Detection: Identifies anomalies effectively.
- Compliance Reports: Provides precise compliance documentation.
- Vulnerability Management: Supports agent-based vulnerability assessments.
- Multi-Cloud Support: Manages and secures across multiple cloud providers.
- Automation and Collaboration: Enables integration with Slack for streamlined communication.
- Custom Alerts: Allows creation of personalized alerts for better focus.

## What benefits do users expect?

- Reduced Alert Noise: Minimizes distractions with filtered alerts.
- Efficient Cloud Security: Automates processes for enhanced security management.
- Collaboration Support: Integrates with tools like Slack.
- Insightful Perspective: Provides insight from an attacker's viewpoint.

Organizations across sectors leverage Lacework FortiCNAPP for cloud security, focusing on compliance, security posture, and vulnerability management. It is widely used for monitoring AWS and Kubernetes environments, scanning IAC scripts, configurations, and securing compute nodes. It supports multi-cloud security posture management and log ingestion, enabling companies to maintain strong cloud infrastructures without dedicated security layers.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Lacework is helping a lot in reducing the noise of the alerts. Usually, whenever you have a tool in place, you have a lot of noise in terms of alerts, but the time for an engineer to look into those alerts is limited. Lacework is helping us to consolidate the information that we are getting from the agents and other sources. We are able to focus only on the things that matter, which is the most valuable thing for us. It saves time, and for investigations, we have the right context to take action.”



**Carlos Vitrano**

Cloud security director at Medallia

- ✓ “For the most part, out-of-the-box, it tells you right away about the things you need to work on. I like the fact that it prioritizes alerts based on severity, so that you can focus your efforts on anything that would be critical/high first, moderate second, and work your way down, trying to continue to improve your security posture.”



**Jim Shank**

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



“The compliance reports are definitely most valuable because they save time and are accurate. So, instead of relying on a human going through and checking or providing me with a report, I could just log into Lacework and see for myself.”



**Konnor Willisobn**

Director of Engineering at DeepSee.ai



“Polygraph compliance is a valuable feature. In our perspective, it delivers significant benefits. The clarity it offers, along with the ability to identify and address misconfigurations, is invaluable. When such issues arise, we promptly acknowledge and take action, effectively collaborating with our teams and the responsible parties for those assets. This enables us to promptly manage problems as soon as they arise.”



**Russell**

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



“The most valuable feature, from a compliance perspective, is the ability to use Lacework as a platform for multiple compliance standards. We have to meet multiple standards like PCI, SOC 2, CIS, and whatever else is out there. The ability to have reports generated, per security standard, is one of the best features for me.”



**Daniel Vukadinovic**

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

- ✓ “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.”



**Verified user**

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

- ✓ “The most valuable feature is Lacework's ability to distill all the security and audit logs. I recommend it to my customers. Normally, when I consult for other customers that are getting into the cloud, we use native security tools. It's more of a rule-based engine.”



**Robert Croteau**

Director of Enablement at Avesha

## What users had to say about valuable features:

“The most valuable feature is Lacework's ability to distill all the security and audit logs. I recommend it to my customers. Normally, when I consult for other customers that are getting into the cloud, we use native security tools. It's more of a rule-based engine.

They have to go in and put their policies in place. It's hard for them to implement that, especially if they don't have a real security team. The team's policymakers don't do anything. Lacework takes out all the noise and gives them bits of things that actually matter with the application after it learns the behavior..”

**Robert Croteau**

Director of Enablement at Avesha

[Read full review](#) 



“The most valuable aspects are

- identifying vulnerabilities, things that are out there that we aren't aware of
- finding what path of access attackers could use
- being able to see open SSL or S3 buckets and the like.

For detecting anomalous activities, as well as known threats, it's good. It is definitely a decent platform for doing that. It is also good for helping us see our environment from an attacker's perspective.

It also does a good job of continuously monitoring configurations. You can set up alerts around that monitoring and know whether or not there have been any kinds of changes. It's good, especially with automation. The way that things are happening in the cloud, there is a need for security teams to see vulnerabilities as they come up and address them as quickly as possible..”

**Verified user**

Senior Manager at a educational organization with 10,001+ 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](#) 

“There are many valuable features that I use in my daily work. The first are alerts and the event dossier that it generates, based on the severity. That is very insightful and helps me to have a security cap in our infrastructure.

The second thing I like is the agent-based vulnerability management, which is the most accurate information. It helps us to know what the security gaps or weaknesses are in the systems and to patch them. Finding a critical weak spot is one of the best features, with the agent-based scanner. We can check it out, based on a filter of the host or container, get the vulnerability report for that particular host, and just share it with the DevOps team to patch.

For anomalous activities, Lacework has a good set of rules for detection and it gives super-informative alert information. For example, when an issue is detected that results in an alert, it doesn't just give the details. It also explains clearly what is happening, with "WH" questions. In the alert, if you click on "Why this alert has been detected," there is a clear explanation for it. Next, you can click on, "When," and it gives the time range of the detection time. The next is "What has been impacted?" That kind of accurate information means we don't have to look around or worry about the source of the information or the legitimacy of the alert..”

**Srinivas Shankar**

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

[Read full review](#) 

“The most valuable feature, from a compliance perspective, is the ability to use Lacework as a platform for multiple compliance standards. We have to meet multiple standards like PCI, SOC 2, CIS, and whatever else is out there. The ability to have reports generated, per security standard, is one of the best features for me. In the portal, you can go to reports and pick any security framework, any standard, like PCI DSS, for example. It will automatically generate a report on your security posture for your entire infrastructure, based on that security framework, which is really useful. Otherwise, I would have to do all that manually. It has definitely helped save time.

And one of the reasons we adopted Lacework was the continuous monitoring of our configurations, as well as the ability to adapt and the scalability that it offers. The continuous monitoring is one of the major things that alleviates some of the pressure on our team. It's one of the most useful features. It's essential and, without it, it wouldn't be of much use to us in the context of compliance. It needs to continuously monitor all the changes, and that is what it is doing quite well.

It does so much in terms of security assessments that would require a lot of effort, with multiple other tools that are available on the market, to compensate for what Lacework offers. It does a lot and offers a lot of features packaged into one solution.

We use it in the public cloud, on GCP and Microsoft Azure. That's another aspect that is really good, that you can so easily integrate it into a multi-cloud environment..”

**Daniel Vukadinovic**

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

[Read full review](#) 

“The most valuable features are the anomaly detection and security compliance, both, that the product does pretty well.

For anomaly detection, it parses things using a severity scale of low, moderate, and high, and that helps provide context to the urgency and prioritization of the alerts that you get in the tool. And on the compliance side, it supports several benchmarks, including CIS, NIST 800-53, as well as other security standards. It will give you insights into compliance against those standards so you can see how your product is configured and if it complies with the best security practices of those standards.

Where it really shines is in helping you detect anomalous activities and known threats, assuming that you have it properly configured. Out-of-the-box, it's not difficult to configure. You do need to do some minor configuration work depending on how you deployed your application. But for the most part, out-of-the-box, it tells you right away about the things you need to work on. I like the fact that it prioritizes alerts based on severity, so that you can focus your efforts on anything that would be critical/high first, moderate second, and work your way down, trying to continue to improve your security posture. That part works very well.

Also, to the extent that attackers are trying to take advantage of vulnerabilities that you may have in your system, Lacework is very good at giving you a view of your environment from an attacker's perspective. It provides context to help understand how easy or difficult, and how likely or unlikely, it is for an adversary to exploit the vulnerabilities that you may have.

In addition, it's really good at continuously monitoring, 24/7, 365. It's designed to do that. It's constantly working in the background to protect our AWS workloads, and I feel good about that. It's very important because it's one of the things we rely upon the most to give us insights into our security posture at any given point in time.

I also like a lot of the dashboards and reports. They're fairly user-friendly and easy to understand..”

# 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 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](#) 

“As a consultant, I've seen all the products, and I was working with Lacework when it came out. They only supported AWS at the time, so I didn't what they could do. I recommend Lacework to other customers because I have customers who generate 30,000 alerts daily on GCP. I recommended Lacework, and we ripped out Security Command Center. With Lacework, they were getting maybe 15 alerts instead of 25,000..”

**Robert Croteau**

Director of Enablement at Avesha

[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**

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

[Read full review](#) 



# ROI

Real user quotes about their ROI:

“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**

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

[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

“Lacework is a cloud security platform. We have multiple cloud providers, and we're ingesting the logs from each. About six people at my company use Lacework. .”

**Robert Croteau**

Director of Enablement at Avesha

[Read full review](#) 

---

“The biggest draw was being able to have a report that would tell me if my AWS cloud environment was in compliance or not. So, the biggest use case was that I needed something that I could just plug in, and it would go through all of my resources in AWS and find all those nooks and crannies, every little thing, and tell me if I'm in compliance or not..”

**Konnor Willisobn**

Director of Engineering at DeepSee.ai

[Read full review](#) 

“We are covering cloud security posture management and run-time detection as well, so there are two flavors. It is also used for inventory purposes. We are probably using all the capacity of the tool. We have the agents deployed in our environment, and we are also covering all of the cloud environments with the Cloud Security Posture Management version..”

**Carlos Vitrano**

Cloud security director at Medallia

[Read full review](#) 

---

“Lacework is a sales platform.

Because Kubernetes had a number of important processes that used EKS, we needed Lacework to protect the cloud environment in general and Kubernetes in particular. We required it to defend both the overall cloud posture and to offer protection. And then our container environment's detecting capabilities..”

**Yuri Livshitz**

Chief Information Security Officer at a tech services company with 201-500 employees

[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**

[Read full review](#) 

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

---

“We use it mainly for detection and response purposes. We have also started using Lacework as our vulnerability management tool, which is most important for our organization. We don't have any kind of security layer for all our cloud infrastructure so we are using Lacework as a security product for our cloud infrastructure..”

**Srinivas Shankar**


[Read full review](#) 

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

# 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 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

---

“Setting up Lacework was straightforward. I've deployed it both ways. I did it manually, which took a little time to go through the documentation. I used Terraform scripts the second time. Deployment took me 15 minutes. It's on the cloud. I'm using Google and AWS. .”

**Robert Croteau**[Read full review](#) 

Director of Enablement at Avesha

---

“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

---

“I and another person on my team set it up. Its initial setup was very straightforward. If you're familiar with containers, it's a walk in the park.

In terms of maintenance, it doesn't need any maintenance. There was a large security vulnerability. I forgot what it was exactly, but with how we were using Lacework, it didn't impact us at all. We haven't done any sort of maintenance on it at all since we implemented it..”

**Konnor Willisobn**

[Read full review](#) 

Director of Engineering at DeepSee.ai

---

“We have a separate DevOps that takes care of Lacework deployment, uploading and installing the agent. My job is to make sure that we have visibility into all our containers and host-based cloud infrastructure. Lacework has a feature called resource that completely shows how many containers or instances are running with Lacework and without Lacework. I just pull that data and give it to the DevOps team. They go in and do the config of hosts that don't have a Lacework agent.

There is some maintenance involved with Lacework, but in most scenarios it isn't a problem. We always want to have visibility into everything, so we need to make sure that things are working fine..”

**Srinivas Shankar**

[Read full review](#) 

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

Cloud security director at Medallia

[Read full review](#) 

# Customer Service and Support

“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](#) 

---

“The support is quite good. We encountered an issue when attempting to integrate Alerting Channels. Specifically, we aimed to send alerts to our communication platform, but encountered an issue that hindered this process. I submitted a request, and the response was swift. The support team addressed the matter promptly, resulting in an immediate resolution. .”

**Russell**

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

[Read full review](#) 

“I contacted their support in the first week of January when we had that issue with the API, and that was sorted out fairly quickly. They're very responsive and quite good when it comes to technical help.

We have monthly catch-up meetings. They're quite good in the sense that they offer a lot of advice and suggestions, and they're quite responsive when you need help. They're always happy to help, which I appreciate a lot. Anytime I have doubts about alerts, or have a question, I can contact them. Or, if they proactively have a suggestion for us, they will reach out and we'll just get it sorted. We constantly work on updating our alert and policy strategies..”

**Daniel Vukadinovic**

[Read full review](#) 

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

---

“We have contacted their tech support on multiple occasions. They're very good, very timely in terms of responding. Generally speaking, they give us good feedback and help us work through most of our problems. There have been a couple of stickier and more challenging problems that have taken some more time to work through, but generally speaking, they've been pretty good about working through issues in a timely manner.

They have a method of escalating when an issue doesn't get resolved in a timely manner, which is good. Sometimes, it takes a little bit longer to engage the supplemental support, get them up to speed on a problem, and get them engaged because that may not be their primary responsibility. But they do help get you through an issue if you give them enough time..”

**Jim Shank**

[Read full review](#) 

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

---

“Even though here and there there are some problems with the solution, whenever we address the issues with the Lacework team, they're always ahead of it in their response and they always are supportive.

We have a community channel as well. CSP is partnered with us and we have frequent communications with them. We have a conversation with them on a day-to-day basis on a Slack channel. Their technical team is connected all the time. The moment we post a question on that channel, we will get a response within five or 10 minutes. That is a much faster resolution than any other solution that I have used..”

**Srinivas Shankar**

[Read full review](#) 

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

---

“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

“Evaluate all other options to know what you are looking for, and you should already have a process in place to take findings from a particular platform and put them into actionable changes..”

---

### Verified user

Senior Manager at a educational organization with 10,001+ employees

[Read full review](#) 

“To those evaluating this solution, I would advise identifying the requirements of the company and having a clear understanding of the success criteria and the use cases that they want to cover. After that, they can do a PoC. Identify the right number of systems that you want to go over the cloud environments and then move to production. Take Lacework's support for production deployment. It is important.

I would rate Lacework a nine out of ten..”

---

### Carlos Vitrano

Cloud security director at Medallia

[Read full review](#) 

“The overall solution can be rated 10 out of 10.

I would recommend that while utilizing the product, it's vital to actively engage in configuring your environment appropriately and adopting the right procedures, both technical and administrative. This approach ensures the realization of value from Lacework or any security solution.

.”

**Russell**

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

---

[Read full review](#) 

“The security team is the most important part of any organization because they are the people who help protect your organization. For them to protect you, they need better visibility into the environment and infrastructure and certain tools to help do their jobs more easily. As an analyst, I think Lacework is much better.

When an analyst gets an alert, time becomes very crucial. His response time should be 30 minutes. In the first 15 minutes, he should be able to understand what type of attack it is, exactly what is happening, and how to stop it. And he also should come to a method of remediation to stop the attack for the short term. For all these aspects, Lacework is really much better. Any analyst, when working on an alert, will initially have the five questions: why, when, what, how, and where. That's what Lacework provides. These questions are the template for any analyst and with them, it takes me about 15 minutes to understand an alert. In the next 15 minutes, I will work on contacting the team, et cetera. From a time perspective, Lacework is much better.

Give Lacework a try. It's one of the best tools in the market that I have used so far. Except for the RTR response, the rest is fine. It is really doing a pretty good job. It will never disappoint you..”

**Srinivas Shankar**

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

[Read full review](#) 

---

“My advice is that it's very important to understand what you have and where you want to get to. You can use Lacework in many ways, and one of the ways you can use it is to assess the security posture of your infrastructure. If you understand what your security requirements are, you will better understand how to get the most out of Lacework.

Lacework provides insight, to some extent, for viewing our environment from an attacker's perspective, because every alert is broken down into the steps someone



took to get to the point where it generated the alert. That way, you get some insight into how someone would approach hacking the infrastructure. But it obviously doesn't offer as much detail as a pen test would.

Because of the way we use Lacework, integrated with public cloud providers, every time we create an environment in the public cloud, we have to create an integration with Lacework. We do that through Terraform, using the principle of infrastructure as code. The maintenance comes in when Lacework makes API changes on their end. If the API changes in such a way that it's not compatible with our code, then we have to update it. But that happens rarely. It has only happened once in the last six months.

Overall, I rate Lacework at 10 out of 10. I've been really happy with it..”

---

**Daniel Vukadinovic**

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

[Read full review](#) 

“My advice is to understand what it's going to do for you and what it's not going to do for you. It's very good at highlighting vulnerabilities in your architecture or your system, and it's very good at identifying non-compliance and anomalies. It's not going to do anything outside of that. Those are the things it's intended to do and that it focuses on.

In terms of our time and effort spent on security incidents and threat-hunting, the reduced alerting that has resulted from using Lacework is a mixed bag. I look at Lacework as being part of an overall suite of tools that help us look at the environment. I wouldn't rely upon it too much for threat intelligence. That's not its primary wheelhouse. But, as I mentioned, it does offer us a whole lot in terms of looking at our security posture at a point in time.

We need to be more careful when we roll out new services because we often don't

have them properly vetted. Sometimes, when we do that, Lacework will tell us there are a lot of issues with them. But if you use the tool for monitoring those things in a development or staging environment, and it tells you that you have those issues, it will be very helpful in identifying the vulnerabilities and bringing focus to clearing them before you roll something out into production.

The only thing that we do from a maintenance perspective is that we periodically review alerts that are suppressed. Sometimes, you'll run across alerts that don't have value or context in your architecture, based on how you're designed. We will look at those and validate that they should continue to be suppressed, based on our architecture or a similar valid reason for suppressing them. That's pretty much the extent of the maintenance..”

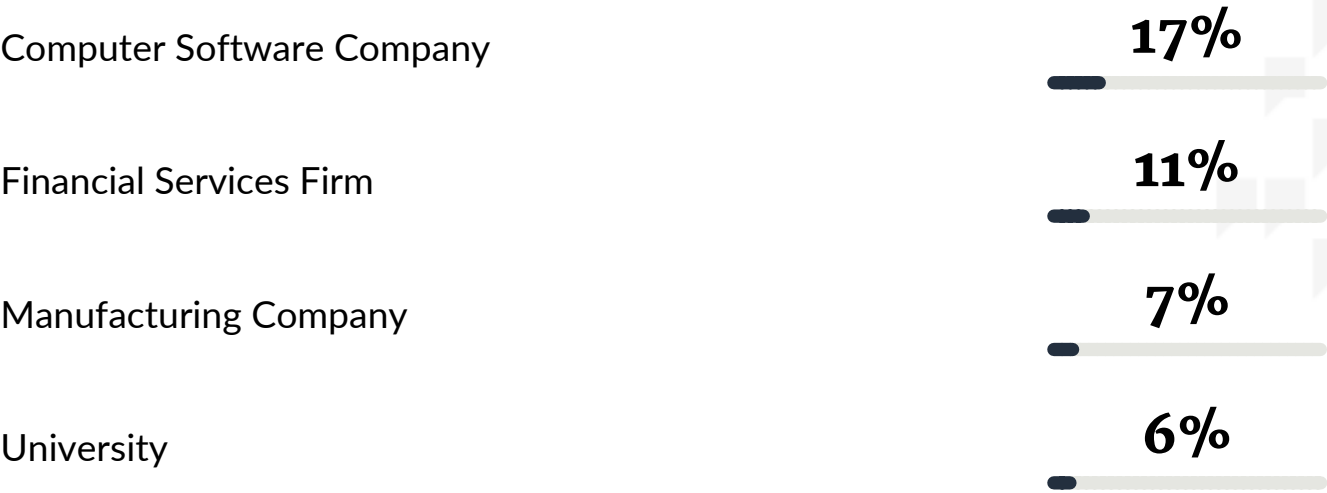
**Jim Shank**

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

[Read full review](#) 

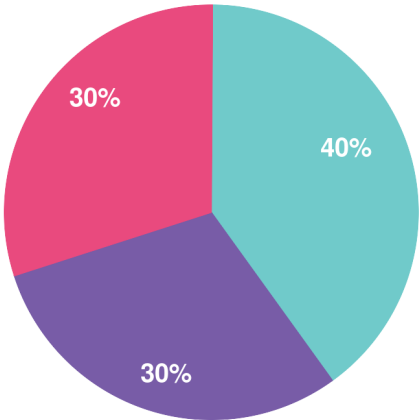
# Top Industries

by visitors reading reviews

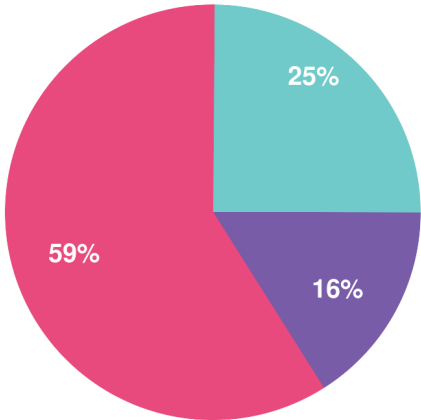


# Company Size

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 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](https://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944