aws marketplace

Nucleus Security

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Nucleus Security

Nucleus Security Recap

Nucleus Security offers a scalable vulnerability management platform designed for effective risk reduction. By integrating with existing IT infrastructure, it enhances security measures and improves agility.

As a comprehensive security tool, Nucleus Security provides customizable vulnerability assessment, streamlined workflows, and integration capabilities with security tools to enhance threat detection and response. It's tailored for enterprises seeking an intuitive management platform that delivers actionable insights and increases efficiency. By leveraging robust automation and advanced analytics, the platform aids organizations in optimizing their cybersecurity posture.

What are the key features of Nucleus Security?

- Customizable Dashboards: Offers personalized views for better visibility and control.
- Automated Workflows: Reduces manual tasks, allowing for quicker incident response.
- Extensive Integrations: Connects with major security tools to unify threat data.
- Risk Prioritization: Analyzes threats to focus on the most critical vulnerabilities.

What benefits can users expect from Nucleus Security?

- Increased Efficiency: Streamlined processes lead to faster threat resolution.
- Enhanced Data Visibility: Comprehensive data access improves decision-making capabilities.
- Cost Reduction: Automation reduces labor costs and minimizes resource expenditure.
- Improved Compliance: Facilitates adherence to regulatory standards and policies.

In industries like healthcare, finance, and technology, Nucleus Security is implemented to address specific risks and compliance needs. It provides tailored solutions to safeguard sensitive data, manage regulatory pressures, and ensure robust threat detection. Industries benefit from its ability to adapt to sector-specific challenges while maintaining high security standards.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Nucleus Security has impacted my organization positively by providing a single pane view of vulnerabilities from different connectors and enabling the automation of reporting and alerting on findings that are out of due date or out of SLA."

Verified user

Vulnerability And Compliance Manager at a insurance company with 5,001-10,000 employees

- "Nucleus Security has fundamentally changed how we manage our vulnerability lifecycle and made our entire incident response process much more proactive, organized, and reliable."

Venkata Kaza

manager at a computer software company with 201-500 employees

- "The best features that Nucleus Security offers in my experience are the unified integrations with all of the different vulnerability management platforms."

Verified user

Cyber Security Architect at a retailer with 10,001+ employees

"The best features Nucleus Security offers, in my opinion, are that it is really great in showcasing things and providing centralized vulnerability management."

Verified user

Head of Security at a consultancy with 51-200 employees

What users had to say about valuable features:

"The best features that Nucleus Security offers in my experience are the unified integrations with all of the different vulnerability management platforms. It is helping quite a lot to unify all of that. It also offers good prioritization based on the EPSS or the CVSS score, as well as different other factors including Mandiant threat intelligence and similar aspects. It helps bring it all into one big picture instead of different silos of vulnerabilities.

The integrations make my job easier because I can connect my other tools, which is the most important part of this tool to bring in all the vulnerabilities from the different other tools. The prioritization changed it from chasing vulnerabilities or pushing colleagues to patch vulnerabilities to providing colleagues with their vulnerabilities and requesting remediation and patching.

Nucleus Security positively impacts my organization by bringing awareness to vulnerability management since we can actually determine how many vulnerabilities we have and how critical the risk is, or we can quantify the risk overall for the company.."

Verified user

Cyber Security Architect at a retailer with 10,001+ employees

Read full review

"The best features Nucleus Security offers, in my opinion, are that it is really great in showcasing things and providing centralized vulnerability management. It also has risk-based prioritization.

"The risk-based prioritization has helped my team focus on the most critical vulnerabilities by considering severity, asset context, and the remediation priorities, rather than just looking at the raw vulnerability counts.

"Nucleus Security's ability to aggregate, normalize, and organize vulnerability data from different sources into a central, manageable view is also a significant advantage.

"I have used the risk reduction measurement feature in Nucleus Security, and it is valuable because it helps translate vulnerability remediation activities into a clearer view of overall security improvement rather than only reporting the number of vulnerabilities closed. It helps the team track reduction in overall exposure all the time and progress against remediation goals.."

Verified user

Head of Security at a consultancy with 51-200 employees

Read full review

"One of the main benefits of Nucleus Security is having built-in capability or connectors into multiple threat intelligence or vulnerability scanning tools, which enables me to interpret this data with a single connector click without having to do any of that work myself.

"The best features Nucleus Security offers are its automation capabilities and the ability to alert application or system owners on their vulnerability posture, letting them know when things are out of SLA and alerting them when things are fixed. It closes the communication cycle, and the most important capabilities are the commentary features, which give visibility of the movement on certain items and the status features. Many vulnerabilities do not get remediated, some are false positives, while others require risk acceptance. The capability to have full control and visibility of the movement of vulnerabilities, whether active or not, is crucial.

"The automation and commentary features have changed the way my team works day-to-day. Having a system owner comment on why something has been delayed or when it may be going into production provides context to the vulnerability findings and potential movement.."

Verified user

Vulnerability And Compliance Manager at a insurance company with 5,001-10,000 employees

Read full review

"For me, the absolute best feature of Nucleus Security is its ability to aggregate and deduplicate data from all our different scanning tools into a single pane of glass. Instead of having our teams dig through separate massive reports from network scanners, cloud tools, and application tests, Nucleus Security normalizes all that data into one place and saves us an incredible amount of manual effort. Another massive standout is the automation engine, which allows us to set up custom triage rules that instantly route high severity vulnerabilities to the right teams or automatically assign due dates based on SLA policies, taking a huge operational burden off our shoulders.

"The out-of-the-box API connectors and integrations make it incredibly easy to hook into existing tools without requiring massive custom development. It works smoothly with whatever scanning tools or ticketing platforms we already have in place, which made the initial rollout much less painful.

"The biggest positive impact of Nucleus Security has been a massive reduction in our time to remediation. Before using the platform, our technical team spent too many hours trying to sort through conflicting scan data and figure out who was responsible for patching what. By centralizing everything, Nucleus Security has completely eliminated that friction and dramatically cut down on alert fatigue across our infrastructure and support teams because the platform prioritizes risk based on real-world threat intelligence. We are no longer wasting time chasing minor internal issues as if they were major fires. We can instantly pinpoint what is actually critical, assign it to the right teams automatically, and track it through to completion. Nucleus Security has fundamentally changed how we manage our vulnerability lifecycle and made our entire incident response process much more proactive, organized, and reliable.."

Venkata Kaza
manager at a computer software company with 201-500 employees

Read full review

Other Solutions Considered

"I did not previously use a different solution; the topic of unified vulnerability management is rather new, so I did not have any solution before that.."

Verified user
Cyber Security Architect at a retailer with 10,001+ employees

Read full review

"This is the first vulnerability management solution that I have tried out, and it worked well for us. I did not get to evaluate other options as this was suggested by our client to see how it would work for us, and it definitely made our day easier and our task easier as well.."

Venkata Kaza
manager at a computer software company with 201-500 employees

Read full review

"Before choosing Nucleus Security, I evaluated other options and looked into all the other solutions, but at that point in time, Nucleus Security was the main company offering something like this, making it clear that Nucleus Security would be the company to go with.."

Verified user
Cyber Security Architect at a retailer with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

"I have seen a return on investment. With security, it is always hard to quantify, and we did not really save money, but we used time more effectively and changed our way of working. I would say time saved is the primary benefit.."

Verified user
Cyber Security Architect at a retailer with 10,001+ employees

Read full review

"I have not seen a return on investment in terms of metrics involving fewer employees or money saved, but Nucleus Security saves time. While any deployment requires initial time and effort, once it is set up, the value stream is substantial. Automation handles reporting on a scheduled basis and alerts system owners about their posture each week. In terms of employees, we still need the same number to remediate findings.."

Verified user
Vulnerability And Compliance Manager at a insurance company with 5,001-10,000 employees

Read full review

"We have seen an absolutely clear return on investment in Nucleus Security, and it primarily shows up in massive time savings and vastly improved resource utilization. Rather than reducing our headcount or needing fewer employees, it has been about reclaiming engineering hours. Before implementing the platform, our core technical teams were spending roughly fifteen to twenty hours a week just manually aggregating spreadsheets, trying to deduplicate scanning data, and routing tickets to the right infrastructure owners.."

Venkata Kaza

manager at a computer software company with 201-500 employees

Read full review

Use Case

"My main use case for Nucleus Security is vulnerability management, along with audit trail commentary and a single pane view.

"I can provide a specific example of how I use Nucleus Security for meeting management or audit trails. Nucleus Security filled a gap within the vulnerability management landscape. Multiple tools available did not provide the opportunity to comment against vulnerabilities and assign vulnerabilities automatically. Nucleus Security were pioneers in bringing threat intelligence, EPSS scoring, and threat intelligence Mandiant ratings at the time. It was an opportunity to review and prioritize vulnerabilities differently, but it provides management oversight and capability that did not exist before. The allocation of vulnerabilities, setting due dates, and commentaries were the start of what made Nucleus Security great.."

Verified user

Vulnerability And Compliance Manager at a insurance company with 5,001-10,000 employees

Read full review

"I have been using Nucleus Security for a year.

"My main use case for Nucleus Security is primarily for vulnerability management. I can give you a quick, specific example of how I use it for vulnerability management in my organization: we connect that with our public clouds such as Azure. It connects to Azure. For example, if Azure has Defender for Cloud enabled and the vulnerabilities on Azure are being replicated into Nucleus Security, with Nucleus Security, we have asset groups, and we can make sure that we provide good visibility to the required teams.

"I have something else to add about how I use Nucleus Security: we have many subscriptions as an example. If we take Azure, we have many Azure subscriptions and all these subscriptions are being looked at by different teams, but the portfolios and the leadership that they report to are almost the same. With Nucleus Security, we have a centralized dashboard for the leadership as well as the teams. We can make sure that role-based access could be granted, so that they can only see the vulnerabilities relevant to them.."

Verified user

Head of Security at a consultancy with 51-200 employees

Read full review

"In the initial phase when we first brought Nucleus Security into our environment, instead of immediately pushing it into full production, I spent some time exploring the interface, connecting a few test data sources, and seeing how the platform aggregates vulnerabilities in real time. Specifically, I was testing how well it ingested scan data from different tools we use and seeing how the automation rules reacted to those findings. It was basically a hands-on trial period to see how the platform prioritizes the risks and handles asset grouping before we fully integrated it into our daily monitoring and incident response workflows.

"I was specifically focusing on setting up automation rules for vulnerability ticketing and risk scoring. In our line of work, we get flooded with scan data from multiple scanners. I wanted to see how intelligently the platform could aggregate those duplicates into a single actionable record. I spent some time setting up the criteria to automatically route high priority vulnerabilities to the right technical teams and tracking how well the tool managed the lifecycle of an incident from discovery to remediation.

"In our organization, Nucleus Security is deployed using a hybrid cloud approach. Nucleus Security itself operates as a secure SaaS platform, which makes it incredibly easy to manage without us having to worry about hosting the infrastructure or managing server updates ourselves. However, because our organization manages a complex infrastructure including internal data centers, private cloud environments, and public cloud services, the platform is integrated across all of them. We use their secure connectors and APIs to safely pull vulnerability data from our infrastructure and centralize everything into their cloud interface. This gives us the best of both worlds: a low-maintenance SaaS tool that still has full visibility into our entire hybrid estate.

"We use AWS the most within Nucleus Security. A massive chunk of our core cloud infrastructure and workloads live there, so it is naturally our primary data source. We heavily rely on Nucleus Security to ingest and centralize everything coming out of our native AWS security tools, such as Amazon GuardDuty, Inspector, and AWS Security Hub, alongside our standard network and application scanners. The platform is especially useful here because it handles cloud-native vulnerabilities really well, particularly when it comes to tracking ephemeral or short-lived assets

and automatically organizing them based on our existing AWS resource tags.

“We purchased Nucleus Security directly through the AWS Marketplace. It made the entire procurement and billing process much smoother since we could consolidate the subscription cost right into our existing enterprise AWS billing agreement..”

Venkata Kaza
manager at a computer software company with 201-500 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.

"The ease of using natural queries or advanced logic with NQL to identify vulnerabilities is fairly simple; it gives an idea of how to build queries and is relatively easy to use.."

Verified user

Vulnerability And Compliance Manager at a insurance company with 5,001-10,000 employees

Read full review

"I would advise starting with Nucleus Security from scratch and then making use of all the tools in place so that it would give a better understanding of things. My biggest piece of advice would be to map out your existing vulnerability management and incident response workflows before starting to build out your rules in the platform.."

Venkata Kaza

manager at a computer software company with 201-500 employees

Read full review

Customer Service and Support

"I would describe Nucleus Security's customer support as absolutely fantastic. I would rate the customer support of Nucleus Security at a ten on a scale of one to ten.."

Venkata Kaza
manager at a computer software company with 201-500 employees

Read full review

"Customer support has met our expectations. While faster response times would enhance the experience, the support provided has been reliable and effective.."

Verified user
Cyber Security Architect at a retailer with 10,001+ employees

Read full review

"Customer support is great; I have always had communication with executive leaders, been able to have roadmap calls, and talk with support. They are fairly responsive with no issues.."

Verified user
Vulnerability And Compliance Manager at a insurance company with 5,001-10,000 employees

Read full review

Other Advice

“I do not have anything else to add about the features.

“I have not really needed to use the customizable risk model feature since we rely on the out-of-the-box capabilities.

“I rate Nucleus Security a seven out of ten. I rate customer support an eight out of ten.

“I would advise others looking into using Nucleus Security to consider the value offering, especially if they have multiple tools and need a single pane view. While Nucleus Security is great, it is debatable whether it will be the best tool or provide the best value in 2026, as many competitors have moved into the Continuous Threat Exposure Management space. I would recommend assessing existing vulnerability management solutions first before exploring Nucleus Security, as it can be a difficult investment when you have solutions that already meet your needs..”

Verified user
Vulnerability And Compliance Manager at a insurance company with 5,001-10,000 employees

Read full review

“I assess Nucleus Security's feature of providing unified exposure visibility across all tools I use as great because I can use all of the data and get all the vulnerabilities in one central place. It has a lot of capabilities, and this is the strongest feature of Nucleus Security. Providing this unified exposure visibility is doing a good job. The integrations could be easier, but the rest is working rather well. I have to work a lot with asset rule lists, so I have to do a lot of automation or processing of the data in Nucleus Security, but at the end of the day, as soon as I set up those rules, I am good to go.

Risk-based prioritization is crucial for addressing vulnerabilities in my organization because I cannot fix all the vulnerabilities; I have to know what I need to handle, how big the risk is, and what the highest risk is that I need to tackle. That is exactly what Nucleus Security is offering.

I did not use the risk reduction measurement feature in Nucleus Security, as risk reduction measurement is not something I am familiar with, but I have used the metrics and trends from Nucleus Security to assess how we are developing, especially regarding the remediation performance.

My advice for others looking into using Nucleus Security is to think about your processes as well. You need to consider where you want to go and think a lot about how you want to use and work with vulnerabilities in the future. I have given this review a rating of eight out of ten.."

Verified user
Cyber Security Architect at a retailer with 10,001+ employees

Read full review

"On a scale of one to ten, I would rate Nucleus Security overall a six.

"I chose six out of ten because vulnerability management alone is not enough when it comes to security operations. I think if Nucleus Security could provide more features across various other areas, it will be better.

"Regarding Nucleus Security's AI capabilities, I do not have any concerns about its governance and security because we reviewed the data classification and all, so we are happy with how they are operating currently.

"Regarding Nucleus Security's AI capabilities, in general, it does a good job regarding its accuracy and reliability of output.

"I did not purchase Nucleus Security through the AWS Marketplace.

“I elaborated on Nucleus Security's feature of providing unified exposure visibility across all tools I use earlier regarding the SentinelOne example.

“Risk-based prioritization is very crucial for addressing vulnerabilities in my organization, and I think it helps the team focus on the most critical vulnerabilities.

“The integration flexibility with ticketing systems and existing tools has affected my deployment process with Nucleus Security because we were able to do this with Jira workflows very easily.

“The advice I would give to others looking into using Nucleus Security is that it is a good tool and covers many areas and tools.

“My overall rating for Nucleus Security is six out of ten..”

Verified user
Head of Security at a consultancy with 51-200 employees

Read full review

Top Industries

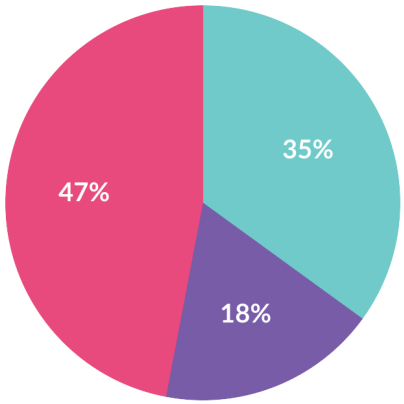
by visitors reading reviews

Computer Software Company	13%
Financial Services Firm	12%
Construction Company	8%
Healthcare 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 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