aws marketplace

Securonix Next-Gen SIEM

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Securonix Next-Gen SIEM

Securonix Next-Gen SIEM Recap

Securonix Next-Gen SIEM is a security information and event management solution designed to provide advanced threat detection, response, and compliance capabilities. It leverages machine learning and big data analytics to offer a comprehensive security platform for modern enterprises.

Securonix Next-Gen SIEM utilizes advanced analytics and machine learning to detect complex threats that traditional SIEM solutions might miss. Its architecture is built on Hadoop, enabling scalability and the processing of large volumes of data in real-time. This allows organizations to gain deep insights into security incidents, prioritize threats, and automate response actions. The solution also includes behavior analytics to detect insider threats and unknown attacks, integrating seamlessly with existing IT infrastructure.

What are the critical features of Securonix Next-Gen SIEM?

- **Advanced Threat Detection**: Uses machine learning algorithms to identify sophisticated threats and reduce false positives.
- **Behavior Analytics**: Analyzes user and entity behavior to detect insider threats and anomalies.
- **Scalable Architecture**: Built on Hadoop, it scales to handle large data volumes, providing real-time analytics.
- **Automated Response**: Automates incident response to mitigate threats quickly and efficiently.
- **Integration Capabilities**: Easily integrates with various IT and security tools for comprehensive coverage.

What is the ROI expectations?

- **Improved Threat Detection**: Enhanced ability to detect and respond to advanced threats, reducing risk.
- **Operational Efficiency**: Automation of repetitive tasks allows security teams to focus on more critical activities.
- **Cost Savings**: Scalability and efficient data processing reduce the need for additional hardware and resources.
- **Compliance Support**: Helps in meeting regulatory compliance requirements through detailed reporting and monitoring.

Securonix Next-Gen SIEM is implemented across various industries, including finance, healthcare, and retail. Its flexibility and advanced analytics capabilities make it suitable for environments with complex security needs. In finance, it helps detect fraud, while in healthcare, it ensures patient data security. In retail, it protects against data breaches and payment fraud.

In summary, Securonix Next-Gen SIEM offers advanced threat detection, scalability, and integration capabilities, making it a robust solution for modern enterprises.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The reporting in the Securonix Next-Gen SIEM is very good, and the dashboard is great."

Verified user

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

- "One of the valuable features of Securonix is the auto-incident creation, which was not available two or three years ago."

Verified user

Works

- "They are very updated. Their customer responses are great, and they keep using the new AI tools to keep themselves at the edge of the game."

Verified user

VP International Business and Alliances at a tech services company with 51-200 employees

"The AI capabilities enhance threat detection."

Bavan Balakrishnan

Senior SOC Developer at XVE Security

"We ingest billions of logs without worrying about resource allocation."

Mohammed Nadeem Rais

Lead - Cyber Security at NMC Healthcare

"The software includes user behavior interactions, dashboards, and training capabilities."

Yoganantham Theerthagiri

Regional Channel Manager at i2sBusiness Solutions

"I rate the technical support a nine out of ten. They're friendly. Whenever we have a P1 issue, we write an email and our issue is resolved in one or two hours."

Pavan Lingam

Cyber Security - Consultant at LTI - Larsen & Toubro Infotech

What users had to say about valuable features:

"The most beneficial feature is the option for a resource group name. We don't have to type the query specifically. We can select the resource group name or functionality directly of which type of security tool logs we want. We don't need to write the query for that; we just have to select.."

Verified user
Security Specialist at a tech vendor with 10,001+ employees

Read full review

"One of the valuable features of Securonix is the auto-incident creation, which was not available two or three years ago. Previously, we had to create incidents manually when a violation was triggered. Now, the process is automatic, reducing our workload. Additionally, behavioral analytics is a useful function, even though it sometimes triggers due to legitimate actions. It requires fine-tuning but correctly detects abnormal behavior.."

Verified user
Works

Read full review

"Securonix Next-Gen SIEM has effective features for threat detection, such as models and custom trap models which are useful. Its integration capabilities are good and comprehensive, allowing us to connect with various necessary components.

Additionally, the AI capabilities enhance threat detection, although they were relatively new at the time. Finally, the solution has shown to be time-saving in the long run.."

Bavan Balakrishnan
Senior SOC Developer at XVE Security

Read full review

"The most valuable feature of Securonix Next-Gen SIEM is its advance analytics, flexibility and scalability. We ingest billions of logs without worrying about resource allocation. This makes it a robust and cost-effective solution for our needs. Its user entity and behavior analytics (UEBA) are also integral for detecting insider threats and lateral movements within the organization. These features help organizations strengthen their security posture, protect sensitive data, and maintain compliance with strict regulatory requirements.."

Mohammed Nadeem Rais
Lead - Cyber Security at NMC Healthcare

Read full review

“They are very updated. Their customer responses are great, and they keep using the new AI tools to keep themselves at the edge of the game.

“This is very helpful because there are many false positives which keep cropping up, and one of the things that Securonix Next-Gen SIEM does very well is ensuring they don't give attention to false positives. They don't take attention away from the real problems and reduce a lot of noise.

“We look forward to more developments from Securonix Next-Gen SIEM in terms of their service turnaround times and staying connected with customers..”

Verified user

VP International Business and Alliances at a tech services company with 51-200 employees

Read full review

"The other SIEM solutions lack an option for big data analysis, whereas in the Securonix Next-Gen SIEM, we have this option, so considering the scope of the project we planned, we chose Securonix Next-Gen SIEM over other vendors.

"We utilize user and entity behavior analytics in the Securonix Next-Gen SIEM.

"The reporting in the Securonix Next-Gen SIEM is very good, and the dashboard is great.

"We have a separate dashboard for MTTD and MTTR. Compared to the previous solution we used, Securonix Next-Gen SIEM has many advantages on the MTTR part, as the containment and alerts automations are feasible from the response point of view.."

Verified user

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

Other Solutions Considered

"Previously, we used Splunk. We switched to Securonix Next-Gen SIEM since Splunk required a lot of hand-holding in terms of creating rules and models. We needed a solution out of the box as we have a small team.."

Bavan Balakrishnan
Senior SOC Developer at XVE Security

Read full review

"The choice depends on the posture that the particular company would take. If they are more mobile intensive with more endpoints, they would go for solutions from companies such as CrowdStrike. It also depends on which tool the CISO and the rest of their team is more comfortable dealing with.."

Verified user
VP International Business and Alliances at a tech services company with 51-200 employees

Read full review

"Prior to Securonix, we evaluated LogRhythm and IBM QRadar. Based on our company's requirements, reduced operational overhead, lower TCO and improved threat detection Securonix Next-Gen SIEM was the best fit.."

Mohammed Nadeem Rais
Lead - Cyber Security at NMC Healthcare

Read full review

"Before choosing Securonix, we evaluated LogRhythm and IBM QRadar. Based on our requirements need for more advanced analytics, scalability, better cloud integration, and automated threat detection., Securonix Next-Gen SIEM was found to be the best fit.."

Mohammed Nadeem Rais
Lead - Cyber Security at NMC Healthcare

Read full review

"We validated ArcSight, Securonix Next-Gen SIEM, and Splunk while considering suitable SIEM solutions. Before using Securonix Next-Gen SIEM, we used ArcSight, where the integration created many issues, particularly data integration, because most end-of-life service systems are not supported in ArcSight, and regular content updates are not up to the mark. Securonix Next-Gen SIEM provides both options, which made us switch from ArcSight.

"We also considered Splunk, and we noticed the customization in our organization is not at the level we need. We tried providing some applications to develop a custom parser, but we do not think Splunk is capable of handling such complexities.."

Verified user

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

“In my market and environment, I compete with Splunk, QRadar, and IBM. I've also heard about Hexabeam, but it's not a major competitor here in Brazil. Another one we're considering, which has posed some challenges, is Google Chronicle. However, the two biggest competitors for me are Splunk and QRadar.

When comparing Securonix to Splunk, one issue is the pricing; I believe even Securonix is on the higher side. However, in terms of working with cloud environments, Securonix has an advantage as it performs exceptionally well in the cloud. Unlike Splunk, which struggles in cloud setups, Securonix handles it perfectly. Additionally, in terms of crunching work in the database (DB), Securonix performs better and more efficiently than Splunk, making it a better choice for such tasks.Other products seem to have a more established market presence, and people are familiar with them, but they might not be as acquainted with Securonix. However, I am confident about the quality of Securonix, and when I get the chance to demonstrate how it works, people tend to like it.Furthermore, in comparison to IBM, I don't encounter any technical problems with Securonix. The quality of Securonix is solid, and I have no issues discussing its capabilities. When it comes to pricing, Securonix offers a more competitive solution. Even if it's only ten percent better than Splunk in some aspects, the overall value makes it a better option in the end. If the price difference is not as significant, it's more likely that customers will choose Securonix over other options..”

NELSON COIMBRA DA SILVA

Cyber Security Sales Engineer Manager at a comms service provider with 501-1,000 employees

Read full review

ROI

Real user quotes about their ROI:

"Our company is already trying to sell Securonix services, although it is a fairly new solution in the company. First, it is being handled internally, but they are already beginning the process of selling the service. That is the best return on investment.."

Andres Fuentes
SOC Analyst at ComWare S.A

Read full review

"Where we see our best return on investment is in the time and manpower we save. Before Securonix, our staff had to investigate events constantly. Now, one engineer with some expertise is enough to speed things up and give the rest of the admins time to do other things.."

Jeanpierre Soto Salvatierra
Head of Cybersecurity at a tech services company with 11-50 employees

Read full review

"We have surely seen an ROI when we look at multiple threats that we have been able to prevent.

It improves analysts' efficiency to do more with less time. By using the contextual information that it provides, we can be more accurate in our investigation. It has saved about 30% time.."

Rafael-Barrios
Cybersecurity SE at a tech vendor with 10,001+ employees

Read full review

"From a business point of view, it can be assessed in both quantitative and qualitative terms. The ROI may vary depending on the organization's size, security needs, and how well the platform is utilized and is highly positive in environments with high compliance requirements, frequent security incidents, or large amounts of data to process. By reducing incidents, improving operational efficiency, and simplifying compliance, the cost savings and protection against expensive breaches can quickly outweigh the initial investment.."

Mohammed Nadeem Rais
Lead - Cyber Security at NMC Healthcare

Read full review

"We most probably did see an ROI. I was working only at the analyst level. I do not have the numbers, but it did improve the efficiency to do more in less time. In the beginning, we were hesitant to use a new tool, but it soon became our go-to tool for checking and verifying any issues. We started engaging with the tool quite a lot, and it probably saved four to five hours a day. Documentation and ticketing were the biggest challenges, and it helped in having everything in one place. We could just click on a ticket and see everything.."

Verified user

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

Read full review

"The Securonix cloud-native platform helps minimize infrastructure management. We don't need that much manpower. If there is infrastructure to maintain, I need an engineer to maintain infrastructure, a software engineer who will look for the application, a security unit who will look for the threats and attacks, and a response person. Now, I don't need a software engineer or infrastructure engineer. That has gone away. Currently, I need only a security engineer and response person, which one person can do. We can also hire two people to do the different jobs. That is no problem.

We don't have to put more focus on infrastructure, which helps. There is a little bit of an infrastructure included, but that is a one-time setup thing. You don't need to go and maintain it again and again.

Securonix Security Analytics adds contextual information into security events. For example, on a generic system, if I used to put in an hour, now I'm putting in 35 to 40 minutes on this. So, it's saving me about 20 minutes of time.."

Verified user

Lead Security Engineer at a tech services company with 1-10 employees

Read full review

Use Case

“We work with CrowdStrike, Securonix Next-Gen SIEM, and other cybersecurity products such as Gurucul. We are a service provider and partner of Securonix Next-Gen SIEM. We operate as a reseller of Securonix Next-Gen SIEM for their customers' cybersecurity as their primary defense mechanism..”

Verified user

VP International Business and Alliances at a tech services company with 51-200 employees

Read full review

“We use Securonix for alert generation by feeding events from different data sources and creating policies. Based on policy violations, we manage alerts. It's essentially a SIEM system for what we do with Securonix..”

Verified user

Works

Read full review

"We use Securonix Next-Gen SIEM to provide managed security services. We have an MSSP delivery model using the Securonix asset platform tool that delivers the solution to multiple customers using their multi-tenant approach. It is a shared service delivery model, and we have close to five customers using the tool in our MSSP model.."

Balamurali Vellalath
Practice Head-CyberSecurity at ALTEN calsoft Labs

Read full review

"We have created correlation rules. When the condition matches, we get the alerts. We start analyzing the alerts and then create tickets for it in ServiceNow. We have also created dashboards in Securonix. If any breaches of data or unpredictable work is detected, it will show in the dashboard.."

Verified user
Security Specialist at a tech vendor with 10,001+ employees

Read full review

"We use Securonix Next-Gen SIEM primarily for managed SOC, focusing on threat detection, baselining, and ensuring the maturity of our SOC security operations.

It is integrated with threat intelligence and utilizes frameworks like MITRE ATT&CK and the Cyber Kill Chain.

The solution helps in threat detection, especially with use cases like brute force attacks, port scans (both horizontal and vertical), other insider threat activities, Privileged access abuse, Ransomware detection and Data exfiltration prevention. We also customize and fine-tune these use cases based on our requirements.."

Mohammed Nadeem Rais
Lead - Cyber Security at NMC Healthcare

Read full review

"We have actually used our company, which is a large one, and we are using multiple Securonix Next-Gen SIEM technologies. For the on-premises environment, we are using Securonix Next-Gen SIEM, and for cloud, we are using Sentinel.

"We primarily use Securonix Next-Gen SIEM to detect policy violations, firewall detection, and other basic parts for the on-premises system, but we primarily focus on the cloud solution because cloud is the scope of our work and we are moving to cloud slowly.."

Verified user
Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 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 initial setup includes evaluating technology that fits our organizational needs, signing NDAs, scoping, providing inventory, and EPS calculation. Once we procure the licenses, there is an expectation setting for onboarding, followed by workflows for exchanging guides, documents, and prerequisites. After the environment is ready, we proceed with onboarding.."

Mohammed Nadeem Rais

Lead - Cyber Security at NMC Healthcare

Read full review

"As per our technical team, the initial setup was fine. It wasn't really difficult.

I am from the sales department, so I don't get involved in the implementation.

The solution is deployed on-premises.."

Mohamad Ammar

Services Sales Consultant at Alpha

Read full review

“The initial setup is easy. I don't see that as a challenge. All the features are user-friendly, and anyone with basic training should be able to install and get it started.

Generally, government clients or large enterprises prefer the product on-premises. Around 20 to 30% of our clients prefer to have it on the cloud. Most of our clients have installed it on-premises because they are very large companies. Fortune 500 companies would prefer to have it in their own environment and not on the cloud. However, Fortune 2000 or Fortune 5000 companies would be more interested in a cloud environment..”

RajivSingh

Read full review

Sr.Vice President & Head - Global Cybersecurity Business at Tech Mahindra Limited

“I was involved in a certain part of the implementation that focused on the RING installation. The implementation was simple. They shared an interactive manual with us and there were no problems. Onboarding the sources was not such a complicated process. We needed three to five employees for the implementation.

They also provided guided training in which a representative from Securonix helped us with the queries we had.

Maintenance is mostly managed by Securonix. We are hardly involved in it..”

Francesco Andre Castro Montoya

Read full review

Security Developer at a tech consulting company with 201-500 employees

"First, we saw how many events we had in the past SIEM. Under that same report, the infrastructure was made in Securonix, the RING was built, the platforms were connected, and then we let Securonix enrich in the system while the platform was configured. After that, the monitoring started.

There were particularities. The implementation of the infrastructure was simple, but the integration was complex due to integration issues in one of the solutions.

It took approximately three weeks until we implemented everything. In terms of staff from our side, there were two technicians, one who was in charge of integrations and another in charge of configurations in the SIEM. My responsibility was more on the strategic approach. Additionally, two integration managers from the Securonix team were involved.

Securonix notifies us when it needs to do maintenance. We only have to take care of the RING since it is local and not part of the SaaS infrastructure.."

Sebastian Velazquez

Cyber Intelligence Supervisor at a tech services company with 201-500 employees

Read full review

"Securonix is in the cloud. We have a virtual machine that stores certain platform configuration information, and since it is in the cloud, we can manage the platform from anywhere. The cloud-native platform helps minimize infrastructure management. Having everything integrated into one place makes things much easier for us.

I was only involved a little in the implementation of Securonix, but from what I heard, their team was helping our entire company, day and night, to get the implementation out as soon as possible. There may have been some problems in integration, but support cases were created and their team was always there with updates and new ways to connect our sources with their platform. Overall, it was not that complicated.

On our side, we had specialists involved from each department that wanted to be integrated with the platform, such as Windows, networking, security, et cetera. The Securonix staff was always present.

Securonix has provided us with a consultant here in Colombia. We are in contact regarding configuration of the platform to rule out possible false positives and help us focus on events that we must take into account.

It took us four months to incorporate all the sources.

There are no maintenance requirements on our part. They are constantly notifying us of updates and, before making changes, they let us know if there are going to be any interruptions in the service. ."

Andres Fuentes

SOC Analyst at ComWare S.A

Read full review

Customer Service and Support

"They excel in response times and quick reactions when there's an actual threat. We work with a particular team which is regionally based out of the Middle East, and they have been very responsive, so we don't want to make any changes.."

Verified user
VP International Business and Alliances at a tech services company with 51-200 employees

Read full review

"The technical support from Securonix is good. If I raise a ticket, it initially goes to the L1 team, but the next level of escalation is really effective. Response times are satisfactory and meet deadlines.."

Verified user
Works

Read full review

"Customer support is rated around seven to eight out of ten. The support system requires creating support requests, and there is no UK-based support, which leads to delays in waiting for US support.."

Bavan Balakrishnan
Senior SOC Developer at XVE Security

Read full review

"For technical support, I can rate it as seven. They also have the same issues other vendors are facing. They are good at resolving issues but not all of them. When we reach out to someone, we often wait for the right person with the right skills to come and fix the solution, which is the major challenge.."

Verified user

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

"Since I work in the sales team, I didn't need technical support. My role is mainly focused on discussing and selling the product to customers, highlighting its advantages.

So, if any technical assistance is required, it would be handled by the partner or someone else in the client-facing team. I have mostly been involved in the sales process, and I haven't had the need to engage with the technical support team.."

NELSON COIMBRA DA SILVA

Cyber Security Sales Engineer Manager at a comms service provider with 501-1,000 employees

Read full review

"Securonix is generally regarded for its **strong customer service and support**, which is a critical factor in ensuring the success of complex security solutions like SIEM. Overall, Securonix offers **solid and responsive support** with a team that is technically proficient and helpful, especially in complex deployments. The proactive guidance, customization support, and strong documentation make it easier for organizations to implement and maintain their SIEM effectively. However, for critical issues, it's advisable to escalate promptly and ensure you're engaging the appropriate level of support for your organization's needs. ."

Mohammed Nadeem Rais
Lead - Cyber Security at NMC Healthcare

Read full review

Other Advice

“My rating for the solution would be around eight out of ten.

If organizations are on a journey to move to cloud, I recommend transitioning to Securonix over an on-premise solution due to its ease of deployment in cloud..”

Yoganantham Theerthagiri
Regional Channel Manager at i2sBusiness Solutions

Read full review

“I would recommend Securonix Next-Gen SIEM depending on the use case. For a small team that wants to get things done without much additional work, it is suitable.

Overall, I would rate the solution at eight point five..”

Bavan Balakrishnan
Senior SOC Developer at XVE Security

Read full review

"For new users, it is good to use. For experienced users, they need fast query resolution; otherwise, it will be difficult for them to use. It does not require much maintenance.

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

Verified user
Security Specialist at a tech vendor with 10,001+ employees

Read full review

"My recommendation would be to evaluate the solution precisely based on the company's requirements to avoid scalability issues in the future. Careful calculation of the EPS during initial sizing is crucial as it can become costly to procure additional EPS licenses later.

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

Mohammed Nadeem Rais
Lead - Cyber Security at NMC Healthcare

Read full review

"I would rate Securonix Next-Gen SIEM as six to seven out of ten.

"From my perspective, it changes based on the organization using it. If your scope focuses on big data, I recommend going with Securonix Next-Gen SIEM. If you plan to maintain the same level of scope in the on-premises environment without any advanced technology, then I would suggest going with better SIEM solutions.."

Verified user
Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

"Automated threat hunting is an evolving space because you can only hunt so many threats, but there are always some that go completely unnoticed. You only know what you know.

"The system is pretty robust because it covers all applications and the entire spectrum. There are cycles that you keep going through and review periodically.

"Whatever feedback we provide to the Securonix Next-Gen SIEM team, they have been very forthcoming.

"I rate Securonix Next-Gen SIEM a 9 out of 10.."

Verified user
VP International Business and Alliances at a tech services company with 51-200 employees

Read full review

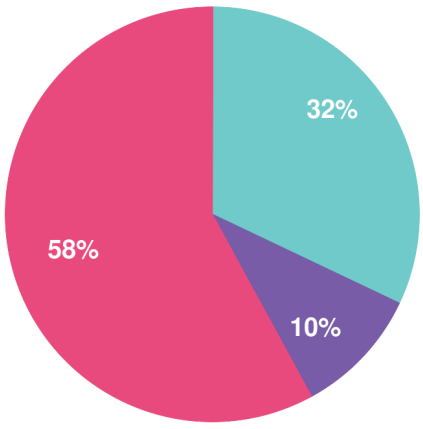
Top Industries

by visitors reading reviews

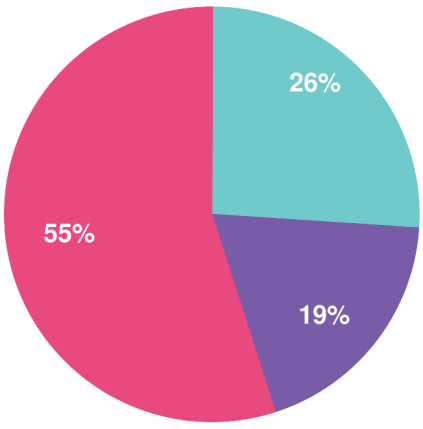
Computer Software Company	17%
Financial Services Firm	11%
Healthcare Company	6%
Manufacturing Company	6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944