aws marketplace

NetWitness Platform

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

NetWitness Platform

NetWitness Platform Recap

NetWitness Platform provides seamless threat intelligence integration and robust log/packet ingestion. It enhances network visibility and incident management through automated threat detection, ideal for enterprises seeking scalability and security intelligence.

NetWitness Platform offers a comprehensive suite of tools designed to tackle security challenges within Security Operations Centers. It integrates data from endpoints, networks, and other sources, ensuring in-depth security analysis. By supporting features like XDR and UEBA, it grants a unified view of security events. Its capabilities extend to threat hunting, malware analysis, and network forensics, assisting organizations in managing incidents, ensuring compliance with regulations like GDPR, and detecting cyber threats. Users appreciate its ease of deployment, flexibility, and threat prediction capabilities, although improvements in integration, documentation, and AI are desired.

What are the key features of NetWitness Platform?

- User-friendly Interface: Simplifies security monitoring and management.
- Threat Intelligence Integration: Provides seamless access to threat data.
- Log/Packet Ingestion and Alerting: Enhances detection and response.
- Network Visibility: Improves threat detection across networks.
- Incident Management: Streamlines response to security incidents.
- Automated Threat Detection: Facilitates quick identification of threats.
- Custom Connectors: Allows for tailored integrations.
- Advanced Dashboarding and Reporting: Offers detailed insights.
- Packet/Incident Correlation: Enhances understanding of threats.

What benefits can users expect when evaluating NetWitness Platform?

- Threat Prediction: Anticipates potential vulnerabilities.
- Ease of Use: Streamlines user experience.
- Deployment Flexibility: Adapts to organizational structure.
- Scalability: Supports growing security infrastructure needs.
- Security Intelligence: Enhances awareness and response capabilities.

In finance and health sectors, NetWitness Platform aids significantly by providing comprehensive threat analysis, ensuring compliance, and facilitating rapid incident management. Enterprises in these industries benefit by maintaining robust security postures and meeting regulatory demands.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- “NetWitness Platform is valuable for creating rules that the solution must detect.”

Verified user

Head of Information Security, Cyber Defense and IT Risk Management at HCT. at a transportation company with 201-500 employees

- “The product's initial setup phase was not at all difficult.”

Verified user

Information Technology Security and Infrastructure Expert at a government with 201-500 employees

- “The product has a user-friendly interface and a valuable feature for threat intelligence integration.”

Suri Shahar

Security Analyst at HeiTech Padu Berhad

"Incident management is its most valuable feature."

MOTASHIM Al Razi

CISO at One Bank Limited

"I can have enterprise security, email security, next generation firewall security log, HIDS and NIDS logs, etc. all on the same dashboard. It makes it easy to pinpoint or correlate our server to this. I can find out if there is lateral movement. This is the biggest advantage of this solution."

Verified user

Senior Assistant Vice President at a financial services firm with 1,001-5,000 employees

"The most valuable feature of RSA NetWitness Logs and Packets are the alerts and correlations tools."

Verified user

Manager at a comms service provider with 10,001+ employees

"It gives the capability for the incident response team to correlate logs to identify any kind of problem like malware and incidents in a general sense, both for logs and packets."

Verified user

Presales Manager at a tech services company with 51-200 employees

What users had to say about valuable features:

"The development of use cases on the SSA console is quite user friendly. This means that the security analyst or the researcher does not have to learn another language.."

Raul Rawat
Senior consultant Cybersecurity

Read full review

NetWitness Platform offers flexibility for deployment and robust integration capabilities. It excels in research events, analytics data, and reporting. It is particularly beneficial for reporting purposes, offering efficient solutions.

Luis Agapito
Computer Security Consultant at SECURE SOFT

Read full review

"In my opinion, the solution's most valuable feature is its capacity to monitor network traffic, logs from devices within the network, and network captures.

This capability extends beyond logs to include full network capturing.."

Salah Sabouni
Director at ST

Read full review

"I don't really see any valuable features in the product. I feel that it is time to move away from NetWitness Platform. All SIEM tools have to deal with advanced use cases, and many of them are getting upgrades, but this is not the case with NetWitness Platform. NetWitness Platform has remained the same for almost four to five years. The support and RMAs offered by the product in our region have also become very bad.."

Verified user

Information Technology Security and Infrastructure Expert at a government with 201-500 employees

Read full review

"The most valuable feature of the NetWitness Platform, as I've found through occasional engagements, is its Total Customer Ownership (TOC) approach. It encompasses having a unified engine and database where all collected information, including logs, network traffic, and endpoint data, is correlated and analyzed. This centralized database enables efficient analysis and correlation of security events aided by artificial intelligence algorithms. Additionally, customers can develop custom parsers to integrate new data sources into the database, enhancing its speed and reliability.."

Rafał Popielski

Solution Architect at NASK

Read full review

"It gives the capability for the incident response team to correlate logs to identify any kind of problem like malware and incidents in a general sense, both for logs and packets. I think the most important thing was that it gives the customer the capability to discover and respond to an incident. It gives customers visibility about their most important servers and devices.

Regarding the packet model, the most important thing is how easy it is to rebuild the raw data. Through one click, you can see an email that was sent even without accessing the mailbox from the user. It's easy to rebuild the raw data, especially the packet.."

Verified user

Presales Manager at a tech services company with 51-200 employees

Read full review

Other Solutions Considered

"I have worked with ArcSight from Micro Focus. One thing to be improved in NetWitness is the capability to correlate event logs in a general sense. We have less resources in the NetWitness correlation engine compared with ArcSight.."

Verified user
Presales Manager at a tech services company with 51-200 employees

Read full review

"In this company, they did not use a similar solution prior to this one. Personally, I used Splunk in my previous organization. Definitely, I prefer to use Splunk because there is more functionality, visibility, and options. You can do whatever you want with Splunk.."

Verified user
Associate Manager Human Resources at a financial services firm with 1,001-5,000 employees

Read full review

"My company has a hybrid environment. I have looked at other products like Splunk and Sentinel. I am still looking around for other solutions in the market. In my company, we are having discussions to move to some other solution.."

Verified user
Information Technology Security and Infrastructure Expert at a government with 201-500 employees

Read full review

"Integration is exceedingly minimal, since its project development is much easier than that of LogRythm or IBM. This means that the solution is significantly more flexible for the customer and requires less training.."

Verified user
IT manager at a agriculture with 10,001+ employees

Read full review

"I have worked with Zscaler and Cisco for four or five years.

I am familiar with Elasticsearch, but I prefer NetWitness Platform as it is specifically designed as a security solution for logs, packets, and endpoints rather than a SIEM-only only tool.."

Salah Sabouni
Director at ST

Read full review

“I previously prepared comparisons between solutions such as IBM QRadar and RSA NetWitness. Having worked for several large vendors, including IBM, I have insights into various security platforms. IBM QRadar, while mature and feature-rich, was behind RSA NetWitness in certain aspects. RSA was among the first to collect data from multiple sources, including live network traffic, endpoints, and logs, offering a more comprehensive approach to threat detection. Both vendors eventually incorporated Extended Detection and Response (XDR) capabilities into their solutions, but RSA was an early adopter. Nowadays, it's challenging to pinpoint significant differences in functionalities among various vendors, as most deliver similar capabilities. Performance and cost considerations may vary depending on the specific use case and hardware infrastructure. Thus, a thorough evaluation is essential when choosing a security platform..”

Rafał Popielski
Solution Architect at NASK

Read full review

Use Case

"Primarily, I use this solution to integrate with applications and systems like firewalls and routers. For example, if somebody is trying to log on from two different locations simultaneously, we can catch that.."

Nilesh Bhate
Delivery Partner APAC and MEA at Tata Consultancy

Read full review

"It's a log management solution where we have logs from different sources, like network devices, firewalls, load balancers, IT, application servers, and database servers. We also use it for compliance and governance. Our cyber security team uses it to monitor malicious activity across our IT infrastructure.."

Raul Rawat
Senior consultant Cybersecurity

Read full review

"We have two customers using this solution and one of them is a banking business. We are collecting some of the security log sources. In the main use case, we are correlating rules and we are using the endpoint detection capabilities. We are utilizing RSA NetWitness Logs and Packets, to have more insights on an endpoint level.."

Verified user

Security Operations Manager at a computer software company with 1,001-5,000 employees

Read full review

"We provide NetWitness along with Archer, and multiple sites. We are managing their security operations using this other station and Archer. A collector can work in two different ways. It can collect the logs, and it can aggregate the traffic tools from different net flow logs. When I saying "logs," I mean a log collector and when I say "packet," that means the packet or log connector. ."

Sandeep Sehrawat

Information Technology Security Consultant at Sify Technologies

Read full review

"The primary use case for the NetWitness Platform is within large companies, particularly in their internal security operation centers (SOCs). They utilize the platform for block collections from the entire company, including subsidiaries, enabling comprehensive security monitoring and analysis. It supports functions such as collections and correlation. Additionally, some licenses may include XDR capabilities. NetWitness stood out for many customers as it was one of the first solutions to collect blocks from endpoints, networks, and logs simultaneously, providing a unified view of security events.."

Rafał Popielski
Solution Architect at NASK

Read full review

"Our solution is utilized by customers to monitor security alerts by ingesting logs from all their assets.

They create correlation rules to identify any potential breaches or hacking attempts and receive notifications through the dashboard.

Customers can use additional features to investigate the incident and take the necessary actions.."

Salah Sabouni
Director at ST

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.

"Using the software is straightforward, but configuring it is complex. To achieve the best results, we need to set up the log system. We have an RSA team to integrate the log system with the SIEM.."

Francesco Ritrovato

Security Analyst at Sogei

Read full review

"Implementation is quite easy, and it takes about a week to deploy the solution. On a scale from one to five, with one being the worst and five being the best, I would give the setup process a four.."

Raul Rawat

Senior consultant Cybersecurity

Read full review

“The product's initial setup phase was not at all difficult. The tool's upgrades and moving from old hardware to new hardware are difficult and time-consuming. If you have any hardware failures, as per the RMA offered by the tool, it takes a very long time to get some after-service. The product has not been working well in my region recently..”

Verified user

Information Technology Security and Infrastructure Expert at a government with 201-500 employees

Read full review

“The solution's initial setup takes work. We have to organize multiple paths and many features.

The deployment process takes less than a week. But it takes a month to complete if we want to make the solution smarter by integrating it with various devices. I rate the process as a six out of ten..”

MOTASHIM Al Razi

CISO at One Bank Limited

Read full review

“I rate the initial setup a five out of ten since the solution had to be implemented twice. It took more than half a year to deploy the solution. Some of the processes were set up with the first implementation very fast. However, the implementation was insufficient to use the solution with all the needed coverage. All the customizations and integrations can take a few months, and it's a long process.

The steps taken to deploy NetWitness Platform are like with any other product. We had to plan whether it was a low-level or high-level design. We had to see the scope of work for implementation, including all the integration processes and data connections..”

Verified user

Read full review

Head of Information Security, Cyber Defense and IT Risk Management at HCT. at a transportation company with 201-500 employees

“The initial setup is complex. It requires some knowledge in order to set it up.

If one is the most difficult and ten is the easiest, I would rate it a three out of ten. It's quite complex.

Initially, we need to prepare the hardware boxes, whether they are physical or virtual or offered as a service. This involves imaging them with the appropriate functions for the module. Then, for network packet capture, the mirror ports must be connected to the packet capture box. Regarding logs, the configuration process involves making NetWitness boxes communicate with each other through the appropriate protocols and ports.

Following this, the next step involves configuring the log sources to send logs to the log box. This process requires the appropriate rules to be configured to initiate log transmission and generate metadata by appropriate parsers on NetWitness. After the setup, the focus shifts to building correlation rules, alerts, and other monitoring activities. These rules and alerts are crucial components for effective monitoring.

The deployment process can vary based on the specific environment and requirements, but typically it takes about one to two weeks to complete.

Maintaining the solution doesn't require a large number of resources. Typically, one or two capable resources are sufficient to maintain the solution effectively.

It's important to continuously monitor and ensure the health and proper functioning of the solution. This involves regularly checking the log sources to ensure that the logs are being ingested correctly and there are no issues such as overutilization or spikes in network traffic..”

Salah Sabouni

Director at ST

Read full review

Customer Service and Support

“We have contacted technical support. They are available. They have around-the-clock support, and they're very helpful.

I would rate them a nine out of ten. There is always room for improvement..”

Salah Sabouni
Director at ST

Read full review

“When we have any critical issues we escalate them to the support of RSA NetWitness Logs and Packets.

I rate the support from RSA NetWitness Logs and Packets a four out of five..”

Verified user
Manager at a comms service provider with 10,001+ employees

Read full review

"Technical support staff were responsive, but they were not always knowledgeable about the project. They didn't have the expertise. They need to be more knowledgeable about their products. Because of this, I would rate technical support at six on a scale from one to ten.."

Raul Rawat
Senior consultant Cybersecurity

Read full review

"The technical support is responsive. Professional service when it is required is expensive. I wasn't able to compare with other professional services, because we have only one tool we are using at the moment. I am not able to tell you how much other OEM professional services cost. We have heard from the support that it is expensive.."

Verified user
Security Operations Manager at a computer software company with 1,001-5,000 employees

Read full review

"My experience with customer service and support for RSA NetWitness has been positive overall. I know individuals who are specialists in the field and attend meetings organized by RSA. These specialists support customers, including those whose partners or companies sell and implement NetWitness at their sites. Despite the cost, it has a strong reputation. I have received helpful assistance from technical support when needed, such as accessing restricted areas on their website or technology database. Even in complex cases, the support team has been attentive and supportive, ensuring I am not left alone with any issues.."

Rafał Popielski
Solution Architect at NASK

Read full review

"Technical support is not available locally in Israel. We're using support from outside. It's global technical support from the vendor and is available 24 hours a day. However, the escalation is very slow. It's dependent on the kind of situation we're in. If it's a full dimension where we have malfunctions that stop processes, the issue can be escalated very fast. We can get support immediately with the service-level agreement we have. But if we have any questions about using the technical support for systems for feature requests or some knowledge. It can take a lot of time, and It's not something we can get from the vendor.."

Verified user
Head of Information Security, Cyber Defense and IT Risk Management at HCT. at a transportation company with 201-500 employees

Read full review

Other Advice

“I would advise taking your time to understand the architecture of the solution, including how the modules communicate with each other and the role of each module. It is recommended to start slowly after gaining this understanding.

I would rate NetWitness Platform an eight out of ten..”

Salah Sabouni
Director at ST

Read full review

“For small to medium-sized organizations, NetWitness Platform will be a suitable option. Most enterprises or larger organizations will likely choose a different platform because NetWitness Platform is no longer listed in Gartner. Additionally, the pricing is too high and is not competitive with Splunk and other products. It is relevant, but they need to set up or hire someone to help them compete with similar products like Slack, QRadar, or Palo Alto. Overall, I rate it a seven out of ten..”

Suri Shahar
Security Analyst at HeiTech Padu Berhad

Read full review

“I've been using Sentinel and IBM QRadar. They are far better than RSA SIEM from a graphic user point of view and in terms of log integration. Everything is enhanced in these solutions compared to that in RSA.

RSA NetWitness Logs and Packets is far behind the competition. Initially, RSA was the only company focusing on decentralization and automation, but now, Microsoft and Google are also in the picture and are investing a lot of money to make their product user friendly and good for the customers from a cybersecurity point of view.

Overall, I would rate RSA NetWitness Logs and Packets (RSA SIEM) at six on a scale from one to ten.."

Raul Rawat
Senior consultant Cybersecurity

Read full review

"NetWitness can be highly beneficial for incident detection and response. RSA has incorporated Extended Detection and Response (XDR) functionality through collaborations and licensing agreements with other companies.

It integrates well with other tools, boasting over 600 integrations on its website. The list is continuously updated and readily accessible.

Security improvements will vary depending on the combination of integrations. It's essential to carefully assess both the list of available integrations and each customer's specific needs.

I rate it a ten out of ten.."

Rafał Popielski
Solution Architect at NASK

Read full review

“My company has had many benefits from the use of the product in the last eight years.

The tool has streamlined our company's incident response process since it serves as a log repository, which allows us to correlate events and access different technology stacks. In our company, we were able to actually find some potential attacks, so it has been very helpful.

The tool's integration capability isn't so great. In my company, we managed to integrate it with our Microsoft Azure Subscription, after which we managed to integrate it with other tools. You will face a lot of difficulties if you want to integrate it with your database monitoring tool, PAM solutions, or IAM products.

The product has done well overall for my company's teams to deal with their workflow efficiency.

I would not recommend the product to others.

I rate the tool a seven out of ten..”

Verified user
Information Technology Security and Infrastructure Expert at a government with 201-500 employees

Read full review

“NetWitness is a part of the cybersecurity solutions we use today, but it's not the only one. We use many different solutions, such as Splunk and QRadar. The product is an SIEM solution, and we use SIEM solutions from different vendors for different needs on different sites.

We don't have all the features we thought were a part of the solution. We need to do many things manually to customize the solution for the customer's needs. By the book, we don't have enough to connect the product to all the systems with some inputs based on machine learning or all the new algorithms like artificial intelligence. The customer must know all these before installing this product. We

need community knowledge for new products that tell us what has to be added after a few installations. The setup, then, can be very fast, and all the knowledge for integration with other components and the company's infrastructure can also be very fast because the solution is best-of-breed and third-party. It's not proprietary for special companies and corporations. In the context of product implementation, everything is very slow and must be done manually and not integrated automatically into the product. We need to know what we will do, how we will monitor the overall system, what kind of events we want to collect from the system, and what type of layout we want to provide through the system to alert about incidents or some type of situation. The customer manually processes all this. It's not like we deploy the product and get all this information and all these capabilities in one coverage of the solution.

Before choosing the NetWitness Platform, find the best integrators with professional experience implementing and deploying this product in other companies. The product has many features and coverage but needs professional integration and implementation.

I would rate NetWitness Platform an eight, but since it depends on the installation, I rate the solution a seven out of ten.."

Verified user
Head of Information Security, Cyber Defense and IT Risk Management at HCT. at a transportation company with 201-500 employees

Read full review

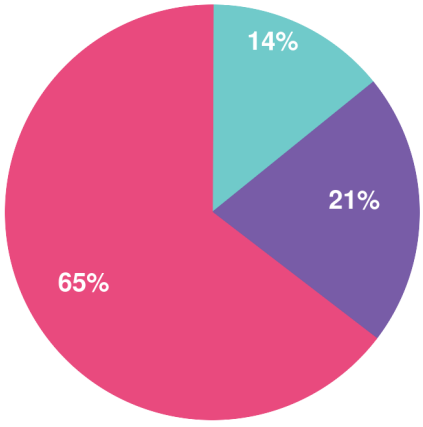
Top Industries

by visitors reading reviews

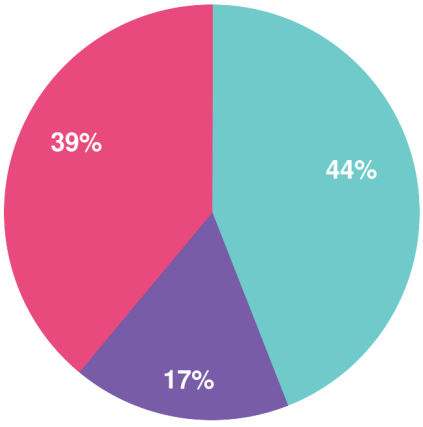
Financial Services Firm	11%
Comms Service Provider	10%
Construction Company	9%
Performing Arts	7%

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