aws marketplace

Secureworks Taegis XDR

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Secureworks Taegis XDR

Secureworks Taegis XDR Recap

Secureworks Taegis XDR offers cutting-edge extended detection and response capabilities to enhance cybersecurity efforts. It effectively integrates and analyzes comprehensive data to provide actionable insights for threat identification and mitigation.

Secureworks Taegis XDR consolidates security data, thus enabling organizations to detect and respond to threats more efficiently. Its integrated approach allows for seamless correlation across data sources, enhancing the ability to identify threats quickly and accurately. Best suited for enterprises seeking comprehensive threat detection and response, it helps in simplifying and strengthening security operations by broadening the coverage and context of threats.

What are the key features of Secureworks Taegis XDR?

- Advanced Threat Detection: Utilizes sophisticated algorithms to identify threats in real-time.
- Automated Response: Enables instant mitigation actions to minimize potential impact.
- Data Integration: Provides seamless data aggregation from multiple sources.
- Continuous Monitoring: Ensures round-the-clock vigilance through persistent monitoring capabilities.
- Scalability: Easily adapts to the growing security needs of an organization.

What benefits should users expect from Secureworks Taegis XDR?

- Improved Security Posture: Strengthens overall security defenses through proactive threat identification.
- Operational Efficiency: Reduces manual intervention with automated threat responses.
- Cost-Effectiveness: Optimizes resource usage and reduces incident response costs.
- Enhanced Visibility: Provides a centralized view of security events across platforms.

In industries such as finance, healthcare, and technology, Secureworks Taegis XDR is implemented to address sector-specific cybersecurity challenges. Its tailored solutions cater to the dynamic and sensitive nature of data protection in these fields, ensuring compliance while providing robust threat defense mechanisms.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Threat hunting and SOC augmentation represent the most special features about Secureworks Taegis XDR, where some of the best people in cybersecurity proactively search, provide reports, and deliver indicators of compromise for any activity in your network."

Mohammad Jundiah

Solutions Architect at Qatar Datamation Systems

- "Definitely, Secureworks Taegis XDR is cost effective for the long run since the product is at a lower cost rather than other brands."

Mohammad Talha Talkin Alam

Assistant Manager IT at PDS Multinational

- "Secureworks Taegis XDR has positively impacted our organization by improving detection rates and reducing our time; as I mentioned, it saves us from manually going through all the logs, which is not practical."

ASUDHARSAN

Cyber Security Analyst at a financial services firm with 11-50 employees

"The auto-triage feature of Secureworks Taegis XDR makes my workflow easier and efficient, helping me shorten the time of responding to every alert, make my activities productive, and manage everything that I need to check every alert and detection."

Verified user

SOC Analyst at a consultancy with 1,001-5,000 employees

"The features I find most valuable are the fact that Secureworks Taegis XDR runs itself without any form of intervention."

Daniel Wakori

Technical Sales Specialist at a comms service provider with 1,001-5,000 employees

"The price for Secureworks Taegis XDR is very competitive."

Ligor Medina

Technology Solutions Head at a tech services company with 11-50 employees

"Sophos is a good XDR, and I recommend it for large companies since they have approximately 2,000 or 3,000 devices and can implement it as it is the best XDR."

Abhishek-Roy

Security Engineer at Corsearch

What users had to say about valuable features:

"If your organization is experiencing a malware attack while using Secureworks Taegis XDR, you can directly block the malware from the console. The threat hunting feature was also beneficial.."

Abhishek-Roy
Security Engineer at Corsearch

Read full review

"The capability of Intercept X with XDR to integrate with third-party tools has usually helped my customers' security operations. We usually advocate for an agnostic setup where if you are running Secureworks Taegis XDR, to have it on almost every level. However, we do have instances where you find a customer running a FortiGate firewall and perhaps they are on Microsoft 365 or something similar. The integration with third-party tools is quite good. I know they have significant add-ons that can facilitate and ingest information from almost all known third parties. That is a plus as well.."

Daniel Wakori
Technical Sales Specialist at a comms service provider with 1,001-5,000 employees

Read full review

"The analysis tools in Secureworks Taegis XDR that are most useful from my perspective are important to note. To be frank, I am not a security person. I am more of an infrastructure person. The reason why this solution is only involved or I was exposed to this is because I always bundle a security solution on every unit that we supply to our customers.

"I talk about on-premises solutions. It is always on-premises or installed on endpoints.."

Ligor Medina

Technology Solutions Head at a tech services company with 11-50 employees

Read full review

"We use the Threat Hunting feature of Secureworks Taegis XDR. Once we deploy this solution, we get visibility on a dashboard and we come to know what the challenges are in the customer's network. If there is any lateral movement about to happen, we can figure it out and catch it as well. The threat hunting part helps significantly with this capability.

"Using Secureworks Taegis XDR has positively impacted our organization overall. It is quite competitive from a price perspective. Price is one of the advantages, and the second advantage is that it has a user-friendly GUI. The rules are very easy to set up and the dashboard is also very good.."

Vishal Khedekar

Techinal Lead at Orient Technologies Pvt. Ltd.

Read full review

"In my experience, the best features Secureworks Taegis XDR offers include advanced analytics, which provides an in-depth overview of incidents or events. In case an incident happens, we can go to Secureworks Taegis XDR, check all the logs, as it ingests and correlates all logs and gives us recommendations. It now has AI, which helps with recommended steps we need to take regarding incidents, and the Dell team is always available to look into and investigate incidents when we are unavailable or it's out of office hours.

"Regarding features, integration stands out; Secureworks Taegis XDR is integrated with major antivirus security platforms such as CrowdStrike, so it ingests every log from CrowdStrike. If CrowdStrike misses anything, we're confident that Secureworks Taegis XDR will pick it up, automatically creating a ticket and informing us. In critical situations or out of office hours, we get notified or receive a call from the Secureworks Taegis XDR team. It's a very popular and helpful platform for reviewing logs, significantly reducing manpower. Going through all the logs to find abnormalities is very time-consuming, but Secureworks Taegis XDR does it for us, which is the main advantage.

"Secureworks Taegis XDR has positively impacted our organization by improving detection rates and reducing our time; as I mentioned, it saves us from manually going through all the logs, which is not practical. Instead, Secureworks Taegis XDR correlates logs from the different security vendors we use, makes recommendations, and detects any abnormalities in events or issues; this is very time-saving for us.

"Since using Secureworks Taegis XDR, our organization has definitely saved time; initially, we were manually going through logs to find abnormalities in events, and if we found any, we had to conduct an in-depth investigation through all platforms. With Secureworks Taegis XDR, all logs are in one place, so we just have to look into it and see what went wrong; it saves a lot of time.."

ASUDHARSAN

Cyber Security Analyst at a financial services firm with 11-50 employees

Read full review

“Threat hunting and SOC augmentation represent the most special features about Secureworks Taegis XDR, where some of the best people in cybersecurity proactively search, provide reports, and deliver indicators of compromise for any activity in your network. This monitoring and reporting can be conducted weekly or monthly.

“Centralized security monitoring and reporting is one of the most valuable aspects, as security fundamentally revolves around compliance. Having a centralized security monitoring platform that detects endpoints, networks, and cloud environments, including servers and switches, is essential. Secureworks Taegis XDR's architecture involves a collector device that collects all your data, even from small laptops, and allows you to monitor everything in one platform. This centralized system provides compliance and security visibility, ensuring evidence and visibility for your security and any compliance requirements you have.

“Analytics with Secureworks Taegis XDR give you a full preview of everything on your device. It takes all the inputs and outputs of your infrastructure; for example, if it is a firewall, it scans all of the traffic. While it is not a SIEM, it is an open XDR, which excels at conducting analytics. This represents one of its best features because Secureworks has implemented a machine learning model that can detect and analyze everything independently, providing AI-driven features.

“Integration with third-party tools is quite seamless. Secureworks Taegis XDR can integrate with virtually anything. One of the best features of this product is its integration capabilities with multiple sources of EDRs and any operating system, whether protecting Linux or Windows servers. It boasts very good integration, and if a specific integration is not available, you can raise a ticket to Secureworks, and they will work on your integration, whatever it is, even if it is custom-built software.

“Secureworks Taegis XDR absolutely aids in efficiency. SOC augmentation extends an organization's existing SOC, which helps reduce alert fatigue significantly. It provides additional threat intelligence and expert investigation, making it very useful for organizations that have a security team but lack twenty-four seven coverage..”

Mohammad Jundian
Solutions Architect at Qatar Datamation Systems

Other Solutions Considered

"CrowdStrike is a good product, but I do not think it has any advantages over Secureworks Taegis XDR. Both Secureworks Taegis XDR and CrowdStrike are the same.."

Abhishek-Roy
Security Engineer at Corsearch

Read full review

"At the moment I do not have alternate solutions, but where I was previously, I was reselling SentinelOne, Comodo, or other products from other vendors as well.."

Daniel Wakori
Technical Sales Specialist at a comms service provider with 1,001-5,000 employees

Read full review

"Before working with Secureworks Taegis XDR, we considered other vendors like SentinelOne and CrowdStrike, which are competitors for Secureworks Taegis XDR and are also providing the same solution in the market.."

Vishal Khedekar
Techinal Lead at Orient Technologies Pvt. Ltd.

Read full review

"I have been working only with Comodo, and we dropped it. The moment there was a massive price hike on the licenses and our market is quite price-sensitive. It is a good solution and does a lot, but it all boils down to the costings, unfortunately, here in Kenya.."

Daniel Wakori
Technical Sales Specialist at a comms service provider with 1,001-5,000 employees

Read full review

"I would not say there is anything that provides a one-to-one comparison with Secureworks Taegis XDR, but I think vendors like CrowdStrike, Fortinet, Palo Alto, and Trend Micro have their own open XDR solutions.."

Mohammad Jundiah
Solutions Architect at Qatar Datamation Systems

Read full review

"I used Trend Micro XDR before using Secureworks Taegis XDR.

"I did not really switch from Trend Micro XDR to Secureworks Taegis XDR. I just had the opportunity to go to another company where they use an XDR platform.."

Verified user
SOC Analyst at a consultancy with 1,001-5,000 employees

Read full review

ROI

Real user quotes about their ROI:

"I would not know the exact metrics they use to assess the effectiveness of Intercept X with XDR in reducing incident management time, but I would say it significantly reduces any form of incident response. I do know it has AI capabilities, so it does intervene and assist with significantly reducing the incident response time.."

Daniel Wakori
Technical Sales Specialist at a comms service provider with 1,001-5,000 employees

Read full review

"I see a return on investment despite the price being relatively high. It is costly, but it delivers whatever you ask for. Some people perceive advantages and disadvantages here; it can be complex if you want to integrate and tune multiple data sources based on your requirements. While some users find it complicated due to the numerous integrations in their environment, others find it very simple, as it allows for a plug-and-play setup where everything can be read seamlessly, and reports are generated easily.."

Mohammad Jundiah
Solutions Architect at Qatar Datamation Systems

Read full review

Use Case

"Secureworks Taegis XDR is designed for customers looking for next-generation antivirus or those who want to protect their systems from ransomware attacks or next-generation attacks. Customers seeking this type of solution primarily look for comprehensive threat protection capabilities.."

Vishal Khedekar
Techinal Lead at Orient Technologies Pvt. Ltd.

Read full review

"Clients are primarily using Secureworks Taegis XDR for securing endpoints, networks, and extending to cloud, identity management, and email protection. It functions as an antivirus in enterprise terms, known for being an EDR, MDR, and XDR. For organizations looking for ransomware protection, threat detection, and incident response, it works as cloud security monitoring as well, monitoring cloud environments for any suspicious activity and detecting threats.."

Mohammad Jundiah
Solutions Architect at Qatar Datamation Systems

Read full review

“My main use case for Secureworks Taegis XDR is ingesting logs from all our resources, so we're using it as a SOC.

“For example, in our SOC operations, we ingest logs from all our security providers; let's take an example of a firewall using Fortinet. We ingest all the firewall logs to Secureworks Taegis XDR, which then reviews these logs, picks up any malicious activity or abnormalities in the events, and notifies us.

“The main purpose of using Secureworks Taegis XDR is as a SOC, and we have playbooks and connectors that help us with remediating risks with the endpoints; it also integrates with the antivirus, which is CrowdStrike. Secureworks Taegis XDR helps us to detect and remediate any vulnerabilities..”

ASUDHARSAN
Cyber Security Analyst at a financial services firm with 11-50 employees

Read full review

"The main use for Secureworks Taegis XDR is to triage alerts from low to critical alerts and analyze and investigate different kinds of alerts from the platform. As a SOC analyst, Secureworks Taegis XDR is helpful to check every detection from the client's environment. It helps the SOC analyst to analyze the specific alert and provide more specific or comprehensive investigation or technical reports to clients.

"I investigated a case wherein there was an impossible travel of a user or an account while using Secureworks Taegis XDR. The user logged in from different countries, then another country for the second time of his login. Secureworks Taegis XDR helped me to check which countries the user had logged in from and provided more details such as the time of login, the IP address that the user used, and more.

"Secureworks Taegis XDR allows us to check or monitor every data collector we are managing and also the users or the endpoints that we are managing in that platform. We can verify if the endpoints or computers of the company have endpoint sensors installed in their endpoints so that we can ensure that their computers are in a managed asset.."

Verified user

SOC Analyst at a consultancy with 1,001-5,000 employees

Read full review

"I have known Secureworks Taegis XDR for about three or four years when I forgot about this solution that Broadcom has acquired. They have their security and then I think that was the time that Sophos also introduced their solutions. Most of the products are also in line with each other. If Trend Micro introduced this, of course, CrowdStrike introduced it, and Sophos as well will also introduce a solution like that.

"Secureworks Taegis XDR is easy to deploy, although there may be some challenges. Most of the customers have their own IT team and will just ask for the license and they can do it by themselves.

"I stand more as a reseller, but not as an integrator. It is more of a delivery and supply of this solution.

"I am dealing with universities. The units have been distributed to all the faculty members, the teachers, and some of the admin staff. If someone claims a unit or it is not distributed as one distribution, we supply to them and they store it in their own storage area or storeroom. Then a faculty member claims it and they will provide some installation or initiation of the configuration of the laptop. I think it takes less than two hours to install everything, including the other applications. Of course, they provide buffer time. It is pretty much fast.."

Ligor Medina

Technology Solutions Head at a tech services company with 11-50 employees

Read full review

"I am working with Trend Micro Vision One, mostly MCC Vision One, for smaller customers. I see a lot of customers opting for known brands such as ESET and Kaspersky. On Trend Micro, Vision One is what we see being pushed a lot here.

"On Fortinet, we deal a lot with FortiEDR and their other products: FortiSIEM, FortiNAC, and FortiWAF. We are not yet on FortiCNP, as most of our native cloud customers opt to rely on the platform for vulnerability management and identification. Cloud specialists can advise more on that end, though I am more focused on generic security as opposed to cloud security.

"With Sophos, we do everything: XDR, MDR, and Sophos EDR. Regarding the threat hunting features, we do not consume the product ourselves; we resell it to customers. From feedback I have received, the threat hunting is very impactful and requires almost no intervention. If you set it up well, you can leave it to run itself with minimal oversight. The identity threat and detection response of the XDR is quite phenomenal.."

Daniel Wakori

Technical Sales Specialist at a comms service provider 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 implementation is straightforward. It is a centralized deployment with Secureworks Taegis XDR, so you can deploy it through the centralized unit and it will automatically deploy on all those devices.."

Abhishek-Roy

Security Engineer at Corsearch

Read full review

"I do not know how much time implementation may require, but I think it is pretty much fast because they are doing it on a per-unit basis. For example, they have their storage, we supply the units, the laptops and the desktops, and once the user claims it, most of the customers that we are dealing with are universities.."

Ligor Medina

Technology Solutions Head at a tech services company with 11-50 employees

Read full review

"My advice for others looking into using Secureworks Taegis XDR is that it's very much reliable; you can run it on a public cloud, private cloud, or, as we do, on-premises. It's easy to install and deploy the collectors, and once we start using it, not much maintenance is needed, as all collector updates are managed by the Secureworks Taegis XDR team. We only need to log in, check the logs, and it flags anything wrong or malicious by giving severity ratings to each event or incident, which allows us to prioritize our investigations.."

ASUDHARSAN

Read full review

Cyber Security Analyst at a financial services firm with 11-50 employees

"The deployment of Secureworks Taegis XDR is quite simple. We have proper training for that and we have trained our engineers.

"In a couple of hours, we are able to deploy Secureworks Taegis XDR. Only the agent deployment takes some time because it is dependent on the customer's number of users and the users' availability.."

Vishal Khedekar

Read full review

Techinal Lead at Orient Technologies Pvt. Ltd.

"I say it is easy to deploy Secureworks Taegis XDR.

"Two people should be good to complete the implementation.

"It requires a couple of days to configure it, then a couple of days to test the scenario, such as what will be the outcome if I deploy the firewall in a running environment and running infrastructure, what will be the output?

"The entire deployment took that long.."

Mohammad Talha Talkin Alam

Assistant Manager IT at PDS Multinational

Read full review

Customer Service and Support

"I had a good experience with Secureworks Taegis XDR customer support. They are reachable and they reply in a prompt manner. I have no problem with them.."

Verified user
SOC Analyst at a consultancy with 1,001-5,000 employees

Read full review

"Their technical support typically responded promptly, especially when using the live chat function. They generally met our expectations and provided good incident response timelines.."

Drake Scott
WPS Security Engineer at a tech services company with 201-500 employees

Read full review

"Sophos support is good and helpful. We always seek support or help from a distributor and they are very accommodating.

"I would rate the support from Sophos at an eight out of ten.."

Ligor Medina
Technology Solutions Head at a tech services company with 11-50 employees

Read full review

"They are very helpful regarding technical support of Sophos.

"I can definitely give a rating of 10 for the support because I always receive prompt service from them.."

Mohammad Talha Talkin Alam
Assistant Manager IT at PDS Multinational

Read full review

"The customer service from Secureworks is quite helpful. The best aspect of this is the support window; you can click on the support link, and you will connect with a real person, not an AI, who will assist you. Given the high cost of the product, you would expect high-quality support, and security being a critical aspect elevates this expectation. I would rate the support a ten out of ten.."

Mohammad Jundiah
Solutions Architect at Qatar Datamation Systems

Read full review

Other Advice

"Regarding the accuracy and reliability of Secureworks Taegis XDR's AI capabilities, accuracy is above 90-95 percent, and it is very much reliable. I would rate this review a 9 out of 10.."

ASUDHARSAN
Cyber Security Analyst at a financial services firm with 11-50 employees

Read full review

"I do have feedback about the customizable workflows. I have a customer who has pretty much loaded the XDR agents on his critical assets, the servers. Once we got it up and running and everything in place, he does not even touch the solution; it does everything for him. When we are talking about workloads and everything, I would say it is pretty much a plug-and-play solution with almost no intervention on what it does. It does pretty much everything for you.

"You do need agents on your assets, of course your devices, but all the interfaces are on cloud. There is no need for local storage for your alerts or anything. I would rate this solution an eight overall.."

Daniel Wakori
Technical Sales Specialist at a comms service provider with 1,001-5,000 employees

Read full review

"We purchased Secureworks Taegis XDR through a distributor. We place the order on the distributor and the distributor places the order to Secureworks Taegis XDR.

"The integration part with third-party tools is easy and is not a challenge.

"As of now, we have not worked with customizable workflows in Secureworks Taegis XDR.

"I would rate this review as a 9.."

Vishal Khedekar
Techinal Lead at Orient Technologies Pvt. Ltd.

Read full review

"One of the best features of this product is its integration capabilities with multiple sources of EDRs and any operating system, whether protecting Linux or Windows servers. Secureworks Taegis XDR boasts very good integration, and if you do not have that integration, you can raise a ticket to Secureworks, and they will work on your integration, whatever it is, even if it is custom-built software.

"The model clients usually use is a hybrid approach, as it can stretch to the cloud. I believe they utilize various cloud providers, including AWS, GCP, and Azure.

"I rate this product a nine out of ten overall.."

Mohammad Jundiah
Solutions Architect at Qatar Datamation Systems

Read full review

"Secureworks Taegis XDR has been dependable for me regarding its AI capabilities in terms of accuracy and reliability of its output.

"The Taegis XDR AI is helpful to analysts such as myself to check and to be more comprehensive of every detection and alert.

"It stands out because it is very comprehensive for users or analysts to learn or to analyze the specific alerts. It is also user-friendly or newbie-friendly. New

analysts can understand faster how the triaging and investigating an incident is conducted. What keeps it from being a perfect 10 is the occasional lag issues on the platform.

“You can also first try to check their certifications regarding Secureworks Taegis XDR.

“My overall review rating for Secureworks Taegis XDR is 9 out of 10..”

Verified user
SOC Analyst at a consultancy with 1,001-5,000 employees

Read full review

“I am familiar with Sophos solutions. Secureworks Taegis XDR is the solution being discussed, which is a Network Detection and Response product.

“I do not know if our customers use the threat hunting feature of Secureworks Taegis XDR. I am not sure because whatever is included in the license that we provide, I do not know if they utilize it much.

“Customizable workflows in Secureworks Taegis XDR help to consolidate all of the processes. When it comes to Sophos specifically, there is not much complex activities that we have done with our customer. It is more of a direct installation or standalone installation of the solution.

“The price for Secureworks Taegis XDR is very competitive. The good thing with Sophos is that it is very competitive with other solutions. In terms of support, they are all the same, but the price is very competitive compared to the other solutions. I would rate this review as a seven out of ten..”

Ligor Medina
Technology Solutions Head at a tech services company with 11-50 employees

Read full review

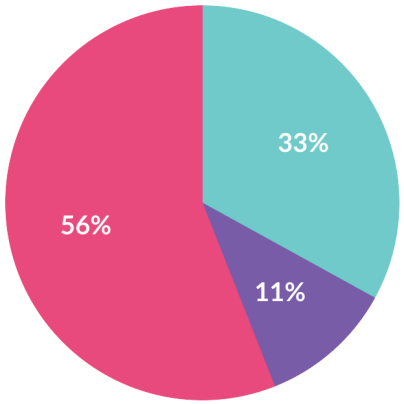
Top Industries

by visitors reading reviews

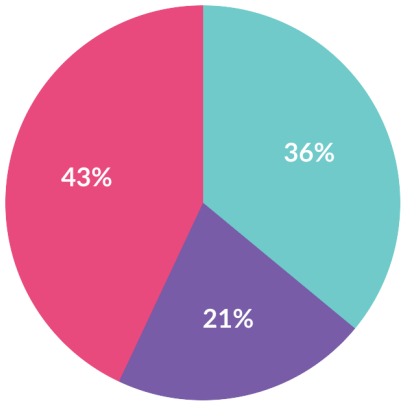
Financial Services Firm	16%
Manufacturing Company	12%
Comms Service Provider	9%
Construction Company	7%

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