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:

- "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 initial setup was straightforward."

Drake Scott

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

"It's a complete solution package."

Balakrishna Mysore

Senior Manager, Services at International Turnkey Systems - ITS

What users had to say about valuable features:

"I appreciate that they introduced the NDR feature and zero-day protection in this product.

"The running interface is good enough; I can see the web traffic, web monitor, and application monitor traffic here, so it is adequate for now.."

Mohammad Talha Talkin Alam
Assistant Manager IT at PDS Multinational

Read full review

"I think the best features of Secureworks Taegis XDR simplify the triaging method for SOC analysts. The SOC analyst can check whether the alert is low, high, or critical. Secureworks Taegis XDR auto-triages the specific alerts, and that is the best feature.

"The auto-triage feature of Secureworks Taegis XDR makes my workflow easier and efficient. It helped me to shorten the time of responding to every alert and also make my activities productive. I can manage everything that I need to check every alert and detection. This shortens my time of triaging and investigating numerous alerts.

"Following the SLA or Service Level Agreement with the clients, we have plenty of time to deeply investigate or analyze the specific alert since using Secureworks Taegis XDR. Since the triaging reduced or the time of investigating is reduced because of the auto-triage of Secureworks Taegis XDR, this positively changes our point of view of investigating alerts and makes our investigation faster.

"We manage a lot of alerts and with Secureworks Taegis XDR, we can scrub and triage or decide if the alerts are false positive or true positive in a faster way.."

Verified user

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

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

Other Solutions Considered

“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

Use Case

"I use Secureworks Taegis XDR within my organization primarily to secure our network infrastructure so that none can access our servers and our devices in the LAN portion.."

Mohammad Talha Talkin Alam
Assistant Manager IT at PDS Multinational

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

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.

"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

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

Read full review

"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

"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

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 have not used the threat hunting feature of Secureworks Taegis XDR.

"I have not used customizable workflows in Secureworks Taegis XDR.

"My overall review rating for this product is 8.5.."

Mohammad Talha Talkin Alam
Assistant Manager IT at PDS Multinational

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

Top Industries

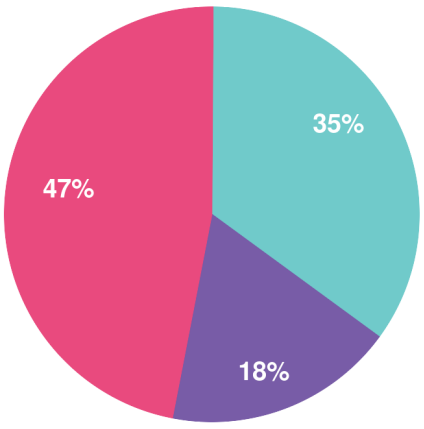
by visitors reading reviews

Financial Services Firm	15%
Manufacturing Company	13%
Computer Software Company	9%
Comms Service Provider	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