

aws marketplace

Cisco XDR

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16 - 18

Use Case..... 19 - 22

Setup..... 23 - 25

Customer Service and Support..... 26 - 28

Other Advice..... 29 - 32

Trends..... 33 - 34

About PeerSpot..... 35 - 36

Product Recap



Cisco XDR

Cisco XDR Recap

Cisco XDR delivers an advanced threat detection and response experience through integration with Cisco's security suite, offering enhanced visibility, intelligence, and automation for network protection and system evaluations.

Cisco XDR integrates with Cisco Meraki and Splunk, excelling in threat intelligence and zero-day attack detection. Its automated response features provide crucial support in managing extensive networks, while the comprehensive log management facilitates detailed troubleshooting. Dashboards assist in system evaluation for effective gap mitigation. Despite its licensing complexity and upfront costs, it remains a key tool for Security Operations Center analysts and internet service providers, helping isolate threats and ensuring consistent security monitoring.

What features make Cisco XDR stand out?

- **Threat Intelligence:** Offers robust insights to identify and manage threats.
- **Integration:** Seamlessly works with Cisco Meraki and Splunk.
- **Zero-Day Detection:** Protects against unknown threats with innovative technology.
- **Automated Response:** Automates tasks such as phishing email handling.
- **Comprehensive Log Management:** Supports detailed troubleshooting and network visibility.

Which benefits should users look for?

- **Enhanced Network Visibility:** Allows for better monitoring and protection.
- **Reduced Downtime:** Reliable performance ensures minimal interruptions.
- **Ease of Training:** Intuitive tools facilitate rapid adoption.
- **Gap Mitigation:** Dashboards provide insights to strengthen system security.

Cisco XDR is widely implemented in sectors requiring robust network management and monitoring. Organizations use it alongside Cisco Firepower Threat Defense and Meraki for comprehensive security measures, benefiting global customers and internet service providers for traffic and routing insights across devices and data centers.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“The merging of all of that data into one display is probably the best benefit of Cisco XDR.”



Fred Parks

Senior Systems Consultant at W.C. Bradley Co.



“Cisco XDR has definitely improved our security posture and our visualization, ensuring that we are protected and providing greater visibility for our SOC team.”



Pranav Salian

Head of Business Operations at a manufacturing company with 501-1,000 employees



“The feature I appreciate the most about Cisco XDR is the flexibility for a user to be able to create their own reporting and dashboards, ingest all the analytics, and make it something meaningful to their business to actually get real, purposeful information out of just a swamp of data.”



Joseph Houghes

Cloud Architect at Pure Storage

- ✓ “Overall, the platform has strengthened our cybersecurity posture and increased operational efficiency for the security team.”



Sufiyan Shaikh

Senior Technical Support Executive at digital track

- ✓ “Since implementing Cisco XDR, our organization has improved its incident response process and overall SOC visibility.”



Sohan Hadke

Cyber Security Analyst at Digitaltrack

- ✓ “I have seen a measurable ROI after implementing Cisco XDR, as my SOC team reduced manual investigation and triage effort by nearly 40 to 50%, which significantly improved analyst productivity and reduced response time for critical incidents.”



Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

- ✓ “Cisco XDR has positively impacted my organization because instead of ten people working on one event, Cisco XDR can do many things an analyst can do, reducing the human effort required and coordinating everything.”



KarthikB

Engineering Security Manager at a recreational facilities/services company with 201-500 employees

What users had to say about valuable features:

“Cisco XDR helps to detect the threats in my organization. It prioritizes most of the critical incidents and responds to them faster as well.

“Cisco XDR generates the alerts and reduces the false positive reports. It prioritizes automatically the risk and the impact which will be happening on my organization. It also helps the SOC team to act faster due to the automation.

“The best features Cisco XDR offers are threat detection, incident response, automated investigation, and integration. There are many third-party tools which I can integrate with Cisco XDR..”

Evans Vasavan

Security Engineer at GlobeSecure Technologies Pvt Ltd

[Read full review](#) 

“The best features Cisco XDR offers are its ability to correlate alerts from different security tools into a single incident view. I also found the automated investigation workflows and real-time visibility very useful for reducing the response time and analysis workload.

“The automated investigation workflows in Cisco XDR have helped my team prioritize high-risk alerts by automatically enriching the incidents with related telemetry and threat intelligence. The real-time visibility across endpoints, email, and network activity made it easier to identify affected systems quickly and respond before the issue spread further.

“Another feature I value in Cisco XDR is its integration with multiple Cisco and third-party security products. It gives a more unified security view and helps analysts work more efficiently without constantly switching between different consoles.

“Cisco XDR has positively impacted my organization by improving our incident response efficiency by reducing investigation time and simplifying alert management. It also helped our SOC team gain better visibility across the environment, leading to faster detection and remediation of threats..”

Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

[Read full review](#) 

“The best features Cisco XDR offers that stand out the most for us are alert collection, centralized visibility, automated investigation workflow, and integration with multiple security tools. Cisco XDR helps our analysts investigate incidents much faster because related alerts from endpoints, email, network, and identity tools are automatically correlated into a single incident.

“The automated investigation workflow in Cisco XDR has reduced a considerable amount of manual effort for our SOC team. Previously, analysts had to manually collect logs and check multiple tools separately. Now, Cisco XDR automatically brings related alerts, user activity, device details, and threat intelligence together.

“I also appreciate the threat intelligence integration and unified dashboard because they provide better context during investigation and help us handle incidents more effectively. Since implementing Cisco XDR, our organization has improved its incident response process and overall SOC visibility. Our analysts can investigate threats faster, alert fatigue has been reduced, and the team spends less time switching between different tools. It also improved coordination during security incidents because all relevant information is available on one platform..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“Recently, a phishing email triggered an alert in Cisco XDR through email security, while the endpoint detected suspicious execution. The firewall logged unusual traffic, and Cisco XDR correlated all signals into a single incident, showing the full attack chain.

“The best features Cisco XDR offers are cross-domain visibility, encompassing endpoint, network, and email in one place, and incident prioritization, which highlights high-risk events.

“The threat correlation that links related alerts automatically is the feature I rely on the most because it converts multiple alerts into one actionable incident, which has significantly reduced investigation time.

“Cisco XDR has positively impacted our organization by providing faster detection of complex threats, reducing alert fatigue, and giving us better visibility..”

Suraj Varma

Senior Network Security Engineer at DigitalTrack Solutions Pvt Ltd

[Read full review](#) 

“The best features of Cisco XDR are its centralized visibility, intelligent alert correlation, and automated incident response capability. It brings together data from endpoint, network, email, cloud, and other security tools into a single platform, making investigation much faster and more efficient. The AI-driven analytics and threat intelligence help to reduce false positives and prioritize the real threats for the SOC team. We also find the integration with third-party security tools and automation workflow very useful for streamlining daily security operation and improving response times.

The centralized visibility and alert correlation make the biggest day-to-day difference for our team using Cisco XDR. Cisco XDR brings alerts and telemetry from multiple security tools into a single dashboard, which greatly reduces the time spent switching between platforms. It helps our team quickly understand the full context of an incident and prioritize the genuine threats more efficiently. This has improved investigation speed, reduced alert fatigue, and made overall security operations much smoother.

The feature set in Cisco XDR has been very helpful for improving operational efficiency and security visibility. We especially appreciate how it simplifies complex investigations and helps the team respond to potential threats more confidently and quickly.

Cisco XDR has positively impacted our organization by improving overall threat visibility, reducing incident response time, and simplifying security operations. The centralized dashboard and alert correlation capabilities help our team to investigate security events more efficiently and focus on high-priority threats first. It has also reduced the manual effort by streamlining workflows and improving coordination across different security tools. Overall, the platform has strengthened our cybersecurity posture and increased operational efficiency for the security team..”

Sufiyan Shaikh

Senior Technical Support Executive at digital track

[Read full review](#) 

“One significant benefit of Cisco XDR is the automatically alert correlation instead of manually piecing together endpoint, firewall, and email events from different consoles. The platform links them into a single incident timeline, which noticeably speeds up triage during phishing or lateral movement investigations.

It also helped reduce alert fatigue significantly by spending less time chasing isolated low-value alerts and more time focusing on incidents that actually have a correlated risk behind them.

The best feature of Cisco XDR for me is the cross-tool alert correlation. It pulls signals from endpoint, network, email, and identity tools into one investigation flow instead of requiring analysts to jump across multiple dashboards. The automated incident prioritization and attack chain visibility also stand out because they reduce a significant amount of manual triage work.

Cisco XDR does a good job grouping related alerts into single incidents and assigning alerts based on how the event connects. The SOC team is not treating every alert equally, which helps us cut down on investigation time because analysts can focus on high-confidence incidents first instead of manually sorting through hundreds of disconnected alerts.

The integrations are probably another standout. Cisco XDR works especially well if you already have Cisco security products in your environment, and the built-in automation playbook capabilities help reduce repetitive SOC tasks.

Cisco XDR improved our incident response workflow considerably. Investigations became faster, alert fatigue dropped, and the analysts had much better visibility across endpoint, network, email, and identity activity from a single console..”

Manik Singh

Penetration Tester at Essen Vision Software

[Read full review](#) 

Other Solutions Considered

“Before Cisco XDR, we were relying on a separate SIEM, EDR, and email security console with a lot of manual correlation between tools. We switched because the investigation workflow was too fragmented and Cisco XDR gave us a more unified incident view with better automation and cross-tool visibility..”

Manik Singh

Penetration Tester at Essen Vision Software

[Read full review](#) 

“Before Cisco XDR, we mainly relied on a combination of traditional SIEM monitoring and separate security tools for endpoint, email, and network visibility. We switched because investigations were taking too long and analysts had to manually correlate alerts from different platforms. Cisco XDR gave us a more centralized and automated approach for threat detection and incident response..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“Before finalizing Cisco XDR, I evaluated platforms like Microsoft Defender XDR and Palo Alto Cortex XDR. I chose Cisco XDR because of its strong integration with our existing Cisco security ecosystem, centralized investigation capabilities, and easier cross-platform visibility for the SOC team..”

Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

[Read full review](#) 

“Before implementing Cisco XDR, we relied on separate security tools for endpoint protection, email security, and network monitoring with limited centralized correlation. As our environment grew, managing alerts across multiple platforms became time-consuming and increased investigation complexity. We moved to Cisco XDR to gain better visibility, centralized threat detection, and faster incident response through a unified portal. The improved integration capabilities and automated correlation features were key reasons for the switch..”

Sufiyan Shaikh

Senior Technical Support Executive at digital track

[Read full review](#) 

“Before selecting Cisco XDR, we evaluated some other options like Microsoft Defender XDR, CrowdStrike Falcon, and Palo Alto. We compared them based on integration capabilities, threat visibility, ease of management, and overall fit for our hybrid environment. Cisco XDR stood out because of its strong integration with our existing infrastructure, centralized visibility, and efficient alert correlation capabilities..”

Sufiyan Shaikh

Senior Technical Support Executive at digital track

[Read full review](#) 

“Cisco XDR totally supports third-party integrations and it works as long as the third party already has an API. If they have an API that allows changes to be made and data to be written, then it typically works really well. If it is a closed-off system, it is not going to work well. The cloud integrations work really well getting data from AWS and getting data from Azure, and getting that network data. This is a great part of it and it does not really require much of an integration. It is just reading that data that is already there. However, it kind of depends on the third party, but it does work. When I have done it before, it has worked well..”

Fred Parks

Senior Systems Consultant at W.C. Bradley Co.

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have seen a return on investment with Cisco XDR. I can share that I save time and people. For money saved, I do not see much improvement, but time saved is significant..”

KarthikB

Engineering Security Manager at a recreational facilities/services company with 201-500 employees

[Read full review](#) 

“The biggest ROI from Cisco XDR was time savings in the SOC. We saw triage and investigation time drop by roughly 40 to 50 percent for common incidents because analysts were not manually coordinating alerts across multiple tools anymore. It also helped reduce alert fatigue and duplicate investigations, so the existing team could handle more incidents without needing to scale headcount at the same pace..”

Manik Singh

Penetration Tester at Essen Vision Software

[Read full review](#) 

“I have seen a measurable ROI after implementing Cisco XDR. My SOC team reduced manual investigation and triage effort by nearly 40 to 50%, which significantly improved analyst productivity and reduced response time for critical incidents. Cisco also highlights that Cisco XDR can reduce investigation workflows from hours to minutes through automation and centralized visibility..”

Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

[Read full review](#) 

“Cisco XDR absolutely can provide ROI. It has some default tasks that it thinks probably everybody should use, but then you can make those work. For example, if you do not have this type of product, you can take that out and not focus your time on incident response on that. You can focus your time on incident response on your email, endpoint security, and cloud..”

Fred Parks

Senior Systems Consultant at W.C. Bradley Co.

[Read full review](#) 

“We have seen a positive return on the investment from using Cisco XDR, mainly through improved operational efficiency and faster incident handling. Our security team spends significantly less time investigating alerts because the platform correlates data from multiple tools into a single view, which has reduced manual effort and improved response time. Overall, the automation and centralized visibility have helped improve productivity without needing to significantly increase security staffing..”

Sufiyan Shaikh

Senior Technical Support Executive at digital track

[Read full review](#) 

“We have definitely seen a return on investment with Cisco XDR. The biggest benefit has been time savings for our SOC team. Investigation and response time improved by around forty to fifty percent, and analysts spend considerably less time manually correlating alerts from different tools. It also helps us manage increasing alert volumes without needing to significantly expand the SOC team, which improves operational efficiency and reduces overall security management efforts..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

Use Case

“We mainly use Cisco XDR for centralized threat detection and incident investigation, especially for correlating endpoints, emails, firewall, and identity alerts in one place, so the SOC team can respond faster..”

Manik Singh

Penetration Tester at Essen Vision Software

[Read full review](#) 

“Our main use case for Cisco XDR is to centralize security telemetry and correlated events across endpoints, the network, and email security tools. This solution helps us detect threats faster, reduce alert noise, and improve investigation efficiency..”

Suraj Varma

Senior Network Security Engineer at DigitalTrack Solutions Pvt Ltd

[Read full review](#) 

“I use Cisco XDR to automate all the threats which are coming in. It automatically isolates the particular endpoints, whether it's a laptop or a server. That helps and provides a good quality report which helps us to identify and then analyze according to it.

“I have SIEM tools of CrowdStrike. I have third-party tools such as endpoints of Trellix endpoints and SentinelOne as well. I integrate this from this integration to Cisco XDR, and I can see all the reports on a single dashboard..”

Evans Vasavan

Security Engineer at GlobeSecure Technologies Pvt Ltd

[Read full review](#) 

“Our main use case for Cisco XDR is centralized threat detection and incident investigation. On a daily basis, our SOC team uses Cisco XDR to monitor alerts, collect events from multiple security tools, investigate suspicious activities, and respond to incidents faster from a single dashboard.

“Recently, our team used Cisco XDR when we received multiple suspicious login and endpoint alerts from different tools. Cisco XDR automatically correlated those alerts into a single incident, which helped our SOC team quickly identify a potential compromised user account and isolate the affected endpoints, much faster than our previous workflow..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“My main use case for Cisco XDR is centralized threat detection, security monitoring, and incident response across our infrastructure. It helps us correlate alerts from multiple security tools into a single dashboard, improving visibility and reducing investigation time. The platform has been useful in identifying suspicious activities quickly and streamlining the security operations.

In one instance, Cisco XDR helped us identify unusual login attempts and suspicious endpoint activity across multiple systems. The platform correlated alerts from endpoint protection and network security tools, allowing our team to quickly investigate the issue from a single console. Using the automated insights and response recommendations, we were able to isolate the affected device and prevent further impact. This significantly reduced the investigation time and improved our incident response efficiency.

Overall, Cisco XDR has helped improve visibility across our security environment and made the threat investigation more efficient. The centralized monitoring and alert correlation features save valuable time for the security team and simplify the daily operations..”

Sufiyan Shaikh

Senior Technical Support Executive at digital track

[Read full review](#) 

“My main use case for Cisco XDR is for centralized threat detection and faster investigation across multiple security tools. It helps correlate alerts automatically, reducing manual analysis time for the SOC team.

“One specific example of how I used Cisco XDR for a centralized investigation is related to a phishing alert, where Cisco XDR correlated email, endpoint, and network telemetry into a single incident view. It helped our SOC quickly trace the compromised device, isolate it, and reduce investigation time significantly compared to the manual log analysis.

“Cisco XDR has helped improve visibility across our environment by bringing multiple security alerts into one platform. The automated correlation and investigation features have made incident response faster and reduced alert fatigue for the team..”

Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

[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.

“Setup was faster than expected because a lot of integrations were already native. Licensing was still enterprise style but easier to justify once we saw the reduction in manual SOC workload..”

Manik Singh

Penetration Tester at Essen Vision Software

[Read full review](#) 

“The deployment of Cisco XDR is very simple and straightforward. I access the service, check the service, configure it, and I obtain the dashboard to begin configuring integrations. I receive logs and can take actions based on incidents easily..”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

“The deployment aspect of Cisco XDR is smooth. Since I was new to this product, I did not do it in-house; I had a third party do it for me. My contribution was about 40 percent, and they did 60 percent of the work, so it went smoothly..”

Ajenthanaiyathurai

Manager IT at NVCL Group

[Read full review](#) 

“Our experience with pricing and licensing for Cisco XDR has been positive overall. The initial setup was relatively straightforward because we already had some Cisco security products in our environment, which made integration easy. The licensing is flexible and based on the features and scale required..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“Our experience with pricing and licensing for Cisco XDR was generally positive, especially since the AWS Marketplace simplified subscription management and deployment. The setup was straightforward, but licensing can become complex when integrating multiple third-party products or advanced modules..”

Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

[Read full review](#) 

“It is all about getting the data into the product because technically there is not really anything to install in the environment. It is about connecting what is in the environment out to Cisco XDR. I would always focus on the network traffic, getting either Secure Network Analytics data out there or deploying the Cisco Telemetry Broker to get network data. We need network telemetry and then focus on the endpoint. The endpoint is probably one of the more difficult ones because it does touch all of the hosts in that customer, so they are typically more concerned with changes because they do not want to affect that environment. So we are integrating that, network, endpoint telemetry, email integration, and then cloud. If we can get the cloud data, that is typically what we would do. I have not had any issues on the Cisco XDR side. It is typically things in the customer environment that are already not working correctly and therefore we have to fix it to get the data out. However, it is typically a straightforward process as long as the underlying products are in good shape. That is where you really run into a problem, but those are not part of a Cisco XDR problem. They are just normal life in IT..”

Fred Parks

[Read full review](#) 

Senior Systems Consultant at W.C. Bradley Co.

Customer Service and Support

“The customer support for Cisco XDR is fantastic. I have not had a reason to call them, but based on client information, they seem readily available whenever needed..”

Bolaji Kazeem

Cybersecurity Analyst at a outsourcing company with 51-200 employees

[Read full review](#) 

“Customer support is excellent. I have had the experience of needing to resolve my ticket as soon as possible, and they are really helpful and very seamless with that process. They also resolved my ticket before I was expecting..”

Manik Singh

Penetration Tester at Essen Vision Software

[Read full review](#) 

“Overall, the customer support for Cisco XDR is very useful, and our experience has been positive. The support engineers are very knowledgeable and helped us resolve issues in a reasonable time. My experience was positive overall..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“Customer support for Cisco XDR has generally been responsive and helpful in my experience, especially for deployment and integration-related issues. The TAC team usually provides good technical guidance, although response quality can sometimes vary depending on the complexity of the issue and the assigned engineer..”

Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

[Read full review](#) 

“I occasionally contact customer service, though not too often. I would say probably in the earlier days there were more support cases because Cisco XDR came into existence later in 2024 and the product was evolving a lot in the early days. Later on, it has gotten a lot better, and I have not had to open up much support cases..”

Fred Parks

Senior Systems Consultant at W.C. Bradley Co.

[Read full review](#) 

“Our experience with customer support for Cisco XDR is generally good. The support team is knowledgeable, responsive, and helpful during troubleshooting, deployment, guidance, and integration-related queries. In critical situations, we have received timely responses, assistance, and useful technical recommendations that helped to resolve our issues significantly..”

Sufiyan Shaikh

Senior Technical Support Executive at digital track

[Read full review](#) 

Other Advice

“If you are considering Cisco XDR, it really delivers the most value when you already have a decent security ecosystem and want centralized visibility plus faster investigations, especially if you are already using Cisco security products. I would rate this product an 8 out of 10..”

Manik Singh

Penetration Tester at Essen Vision Software

[Read full review](#) 

“I highly recommend Cisco XDR, and my advice would be to deploy this solution by integrating the maximum number of security tools for full visibility and to start with key use cases. It is important to train your SOC team so that they can effectively handle this solution. I am providing this review with a rating of eight out of ten..”

Suraj Varma

Senior Network Security Engineer at DigitalTrack Solutions Pvt Ltd

[Read full review](#) 

“I believe Cisco XDR is good and I think I can also recommend it to most of the companies to just try it out once to have a POC, just to make sure all the things get under control in a single dashboard. You have to try it once. So far, everything is going well. I gave this product a rating of nine out of ten..”

Evans Vasavan

Security Engineer at GlobeSecure Technologies Pvt Ltd

[Read full review](#) 

“One specific example of how I used Cisco XDR for a centralized investigation is related to a phishing alert, where Cisco XDR correlated email, endpoint, and network telemetry into a single incident view. It helped our SOC quickly trace the compromised device, isolate it, and reduce investigation time significantly compared to the manual log analysis.

“My advice for considering Cisco XDR is to spend the time planning integration and alert tuning during the initial deployment phase. Organizations already using Cisco security products will gain the most value, especially from the centralized visibility and automated investigation capabilities.

“I would rate this product a 9 overall..”

Abhijeet Chaskar

Cybersecurity Analyst at DigitalTrack solution pvt ltd

[Read full review](#) 

“My advice would be to first understand your existing security stack and integration requirements before deployment. I would also recommend starting with a phased rollout and spending time on alert tuning for overall effectiveness and best performance.

“We use Cisco XDR in a hybrid cloud deployment. Most of the security monitoring is cloud-based, but it also integrates with our on-premises infrastructure and internal security tools.

“I rate Cisco XDR an eight out of ten overall because it has improved our SOC visibility and incident response significantly, while still having some room for improvement in usability and customization. I chose eight because the platform delivers strong threat detection, visibility, and investigation capabilities. However, some areas concerning dashboard customization, reporting, and ease of onboarding for new analysts could still be improved. If the interface became more intuitive and third-party integrations became simpler to manage, it would be closer to a ten for us..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“My experience with pricing and licensing for Cisco XDR has been generally positive, especially considering the security visibility and response capability it provides. The licensing model is flexible with different tiers like Essential, Advance, and Premier, which help organizations choose based on their requirements and budget. Once configured, the platform delivers good operational value and centralized management. We do feel that the licensing structure could be improved, and some components and integrations can be a bit complex to understand initially.

My advice would be to clearly evaluate your existing security ecosystem and integration requirements before implementing Cisco XDR. The platform delivers the most value when it is properly integrated with endpoint, network, email, and cloud security tools to provide full visibility and effective alert correlation. It is also important to plan the deployment and onboarding process carefully, especially in hybrid environments, to ensure the policies, integration, and workflows are configured correctly. Providing proper training for the security team will also help maximize the platform capabilities and overall return on the investment.

Overall, Cisco XDR has been a valuable addition to our security operations. It has helped improve threat visibility, streamlined investigations, and enhanced incident response across our hybrid environment. The centralized approach to monitoring and alert correlation has made daily security operations more efficient and manageable for the team. I would rate my overall experience with Cisco XDR a nine out of ten..”

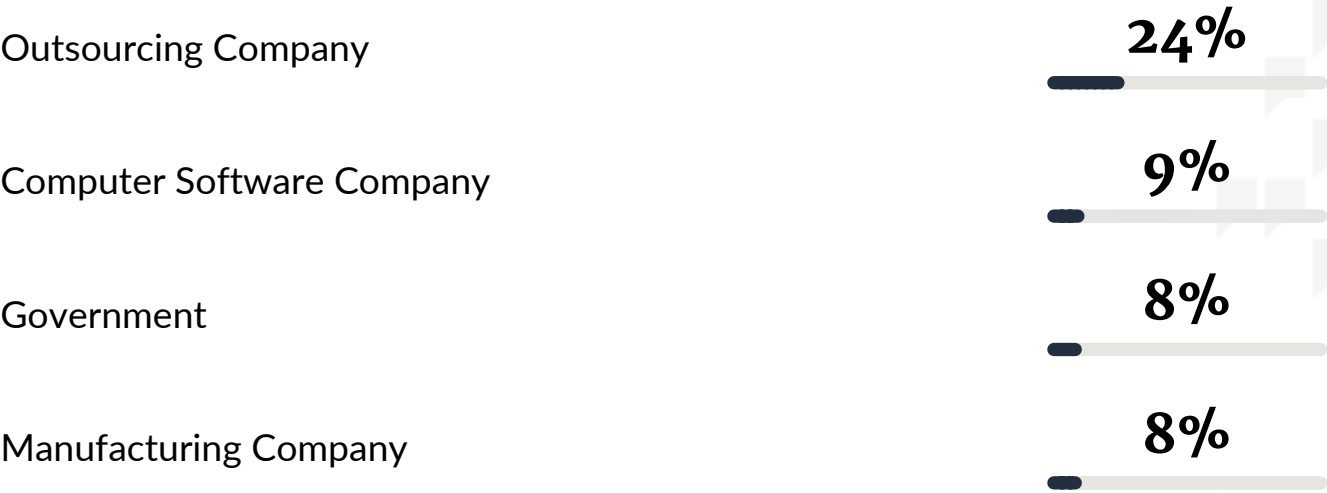
Sufiyan Shaikh

Senior Technical Support Executive at digital track

[Read full review](#) 

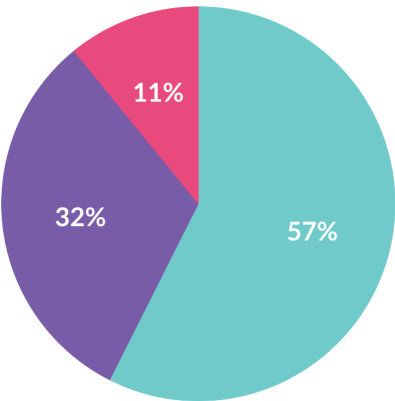
Top Industries

by visitors reading reviews

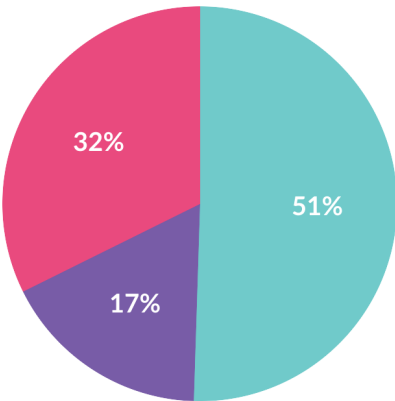


Company Size

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