aws marketplace

Cisco XDR

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

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 SISA

- "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

"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

"My advice for other organizations considering Cisco XDR is that it offers proactive security measures that are really very helpful."

AjenthanAiyathurai

Manager IT at NVCL Group

"Before using Cisco XDR, I sometimes did not detect malicious activities in my client's environment, but since implementing this solution, my mean time to detect has reduced and my mean time to respond has fallen within the acceptable threshold, positively impacting my organization as I can detect and respond to threats in time."

Bolaji Kazeem

Cybersecurity Analyst at a outsourcing company with 51-200 employees

"The features of Cisco XDR benefit my company since time is money. When outages happen and when a customer can't reach the internet, they get agitated. Therefore, the quicker we can mitigate an issue, our customers get happier in a quicker fashion."

Matthew Dean

Network Engineer at BTC Broadband

What users had to say about valuable features:

"Cisco XDR is one of the most matured systems available. It is quite user-friendly. The system has been very effective, and our customers receive sufficient reports demonstrating visible benefits. This helps maintain customer confidence, particularly in secure data center implementations. With the implementation we have deployed, our customers gain confidence in having their data center secure. The reporting capabilities are pretty extensive. Cisco XDR is keeping our customers protected.."

Ananda Deb

Technical Manager at Ledorbis Solutions

Read full review

"The best feature of Cisco XDR, on which I based my decision to purchase it, is that Cisco XDR does not require an endpoint from Cisco. It can work with any endpoint. In my situation, I have an endpoint from Kaspersky, and Cisco XDR can integrate with it. It has predefined integrations based on the licensing model, so there is no need to have a Cisco endpoint to use Cisco XDR. This is not the typical use case for other XDR solutions like Trend Micro or Palo Alto Cortex, where you must obtain the endpoint from the same vendor.

In just four months, I have seen a good return on investment with Cisco XDR. I have reduced incidents and saved time because previously, if I encountered any incident, I would have spent considerably more time and effort reaching out to every security control on my network and checking logs across multiple systems. With Cisco XDR, I gain visibility on one dashboard where I can see extensive logs, resulting in time saved and reduced security incidents, which provides a strong return on my investment.."

Mohamed Fouad
Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

Read full review

“I find Cisco XDR really useful and interesting, and I believe that with time, it is going to get even better.

I appreciate the fact that Cisco XDR detects malicious activity as fast as it can and notifies me when suspicious executable files are downloaded in the client's environment, providing all the information needed for investigation, which is a feature I really enjoy.

When the alerts come in, they bring context, which is helpful. The alert comes in with context such as the file hash, sometimes with the source IP address or the destination IP address, and this context helps bring a suspicious activity to resolution quickly.

Before using Cisco XDR, I sometimes did not detect malicious activities in my client's environment, but since implementing this solution, my mean time to detect has actually reduced, and my mean time to respond has fallen within the acceptable threshold, positively impacting my organization as I can detect and respond to threats in time..”

Bolaji Kazeem
Cybersecurity Analyst at a outsourcing company with 51-200 employees

Read full review

"The investigative ability of Cisco XDR is amazing to me. Once all the data is in Cisco XDR and it flags an incident when it sees something that is notable, important, and of concern, it will raise an incident. The ability to look at one screen about this incident and get data from multiple different sources is a very great capability for incident responders to obtain the information they need. Cisco has AI built into the product where it actually translates some of this log data. Professionals typically have to spend a huge amount of time looking through logs trying to figure out what the log data means, and this is done for you automatically.

The number one thing was getting visibility from customer environments into one console. Customers would have network telemetry from NetFlow, Secure Network Analytics, or the Cisco Telemetry Broker. They would have an endpoint product, a firewall product, and cloud resources, but they needed to correlate all of that data into one location and be able to respond to it instead of having to go into all of these separate security products. By integrating all of these products with Cisco XDR, this allowed them to have a single pane of glass and respond more effectively and quickly to security threats and know what they needed to respond to with that intelligence.."

Fred Parks
Senior Systems Consultant at W.C. Bradley Co.

Read full review

“From the malware detection perspective, Cisco XDR can actually find out if there is any malware present, and we can lock down the system as well, which we call isolation. That is a great add-on for me.

From the SOC perspective, the best features Cisco XDR offers are the ease of use and the ability to understand the logs and log aggregation. It is one of a kind. What stands out for me about the log analysis and the user interface in Cisco XDR is that Cisco has an AI assistant that we can utilize to understand the correlation. The main intent of the integration architecture allows us to integrate easily without any cumbersome processes. We can simply specify what should be integrated with what. They have an open integration architecture already present with third-party tools such as CrowdStrike, Palo Alto Networks, and AWS. Additionally, the automated response workflow can actually automate the flows and tell me the response automatically, indicating whether something is an issue or not. All these features make my daily work and log analysis easier.

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. The mean time to respond has improved for the company, and we have automated many processes. A severe incident would typically take my engineer one or two days to solve, but Cisco XDR would have already completed almost half of that work. The engineer can then review the incident and understand whatever analysis has already been provided.

The features of Cisco XDR are a great add-on for the SOC team, and the security has increased by using Cisco XDR. .”

KarthikB

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

Read full review

"Cisco XDR offers a wide range of integrations and connectors where we can integrate a whole range of devices available in our on-premises environment as well as cloud sources which we have primarily on AWS and Azure. Those environment log sources are integrated with Cisco XDR and it helps provide a single pane of glass view in terms of our security posture, giving us visibility within a single platform rather than focusing on individual security devices such as firewalls or EDRs which would typically be working in silos.

"These integrations are straightforward. Cloud workloads are easier to integrate compared to on-premises devices, primarily because the cloud workloads have readymade connectors and integration standard operating procedures for us to integrate with Cisco XDR. We have typically not faced challenges with integrations with Cisco XDR. There may be certain OEMs which are not well known and cannot be directly integrated without the help of vendor support or OEM support, which we were able to connect with and ensure they are integrated with Cisco XDR.

"From the reporting perspective, the dashboards offer quite a lot of predefined and useful options which help with live threat monitoring and provide a high-level view of the current threats, incident reporting metrics, mean time to detect, and mean time to respond. These sorts of dashboards are available on the platform and help provide a good view even for someone at the leadership level.

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

"Cisco XDR has definitely reduced our mean time to respond. Previously it used to be more than 24 hours, but we have been able to reduce it to less than 16 hours due to all the various integrations and automation capabilities.

"Cisco XDR has been useful for us to gain visibility into gaps in our security posture and how those can be improved by conducting analysis on the platform itself. We have utilized the platform to improve our security posture and reduce blind spots.."

Pranav Salian
Head of Business Operations at SISA

Read full review

Other Solutions Considered

"Before choosing Cisco XDR, we evaluated Splunk, IBM QRadar which was already existing in the environment, and Microsoft Sentinel. Cisco XDR was the best option in terms of overall feature capabilities and pricing.."

Pranav Salian
Head of Business Operations at SISA

Read full review

"We used IBM QRadar before we switched to Cisco XDR primarily because IBM QRadar was more a legacy system and customizations, connector building, parser building, and integrations were taking a long time where we had to reach out to IBM for support. With Cisco XDR, we found a quicker turnaround time.."

Pranav Salian
Head of Business Operations at SISA

Read full review

"For this specific client, they have not used an XDR before, so Cisco XDR is the first one they are using in their environment.

They were convinced to try Cisco XDR due to the value they received from other Cisco products, such as Cisco ISE and Cisco ASA Firewall.."

Bolaji Kazeem
Cybersecurity Analyst at a outsourcing company with 51-200 employees

Read full review

"I believe Cisco XDR compares favorably with other XDR solutions such as Cortex XDR and Trend Micro Vision One. The best feature, as I mentioned earlier, is that Cisco XDR does not require its own endpoint. I have a Kaspersky endpoint, and I did not need an endpoint from Cisco to use Cisco XDR. In contrast, with other vendors such as Cortex or Trend Micro, you must obtain the same vendor endpoint.."

Mohamed Fouad
Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

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

"I never saw a false positive. I think it is very accurate. There were some times where it actually flagged some behavior that would have been malicious if I had not known very specific things about it. For example, it was custom code that was written by developers that did not use very good coding methodologies, so it was doing crazy things, but in this exact instance, it was not malicious. However, if I had not had that special knowledge already, I would need to respond to that. It identified that they do not need to be doing this in the first place, so that required a code change. I would say it is highly accurate. It runs everything through the MITRE Framework and it uses Cisco's intelligence where they are getting threat intelligence from Talos and all of the products that people have deployed, even if they do not have Cisco XDR. If you have Cisco security products deployed out in the world, all that data is feeding the back end. Therefore, you are taking advantage of the millions of customers out there and the environments that are running Cisco. Even if they do not have Cisco XDR, they are feeding data into your Cisco XDR solution and it is making it more intelligent.."

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

"I find it does bring a return on investment, but that will take a long period. I would say it is not in a short span; probably two to three years or more.."

AjenthanAiyathurai
Manager IT at NVCL Group

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

"In just four months, I have seen a good return on investment with Cisco XDR. I have reduced incidents and saved time because previously, if I encountered any incident, I would have spent considerably more time and effort reaching out to every security control on my network and checking logs across multiple systems. With Cisco XDR, I gain visibility on one dashboard where I can see extensive logs, resulting in time saved and reduced security incidents, which provides a strong return on my investment.."

Mohamed Fouad
Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

Read full review

"We have experienced return on investment since we have been utilizing this platform for the last five years. Over time as the platform has evolved and more automations have been put in place, the number of human resources required has drastically reduced. Previously, we used to require four people in each shift to manage all of the incidents and workloads, which would essentially be about twelve people per day. We have been able to cut them down to six people per day, which is roughly half the team size required as of now. This helps in saving cost and time.."

Pranav Salian
Head of Business Operations at SISA

Read full review

"I have expanded the usage of Cisco XDR. The process of expanding usage has been smooth and easy. Since we frequently work with Cisco, it makes it hassle-free to justify needing more and explaining why.

Having proven its value and capability to quickly ramp up our operations has simplified expanding licensing and replacing systems. I know of several incidents that demonstrate Cisco XDR's return on investment (ROI). Two customers faced a network breach and a bad configuration incident, but unlike in the past where recovery took days, they managed to shut down access points quickly. Their ability to divert a crypto attack within 30 minutes saved them from a multi-day outage that previously had entire staff doing nothing but recovering systems.

Within our teams, I absolutely see the ROI with Cisco XDR. We have effectively identified gaps in our incident response processes and what information we need. Security is one of the most cost-effective insurance policies, and Cisco XDR serves as our magnifying glass to understand our security contract better. It has provided us with a tool that enhances visibility and interactivity among our teams.."

Joseph Houghes
Cloud Architect at Pure Storage

Read full review

Use Case

"Cisco XDR is used for endpoint security, data protection across endpoints, network protection, advanced persistent threat (APT) detection, ransomware attack mitigation, and advanced threat detection. We use Data Loss Prevention (DLP) because it integrates with Cisco Secure Access and Cisco Umbrella, helping to protect sensitive data. Cisco XDR is the extended detection and response solution we have implemented.."

Sanjay Gaiswal
Technical Presales at Vcom Technologies

Read full review

"We are system integrators working in a consultancy mode with a team of implementation engineers. Over the last two years, we have worked on several Cisco XDR cases. In data centers, Cisco XDR is definitely the primary requirement. Our first choice is always Cisco, and while one or two other solutions have come our way, Cisco cases primarily come to us. In a certain segment, Cisco XDR is definitely the first priority. I would say that about 80% of my customer base relies on Cisco XDR. We are partners of Cisco and we focus particularly on the implementation aspect, while also taking care of services.."

Ananda Deb
Technical Manager at Ledorbis Solutions

Read full review

"My main use case for Cisco XDR is to collect all the logs from the use cases of how users try to explore and perform their tasks. We are threat hunting to prevent, detect, and respond to threats, collecting from different systems such as M365 and others, correlating them into one central location, and trying to correlate between different kinds of logs to provide whether the alert is a true positive or not.

A simple example of how I used Cisco XDR to connect all these logs and coordinate between different systems is that we have M365 connected to Cisco XDR, as well as browser security connected. Many users use client applications including Outlook, but many use cases go wrong when they are using it via a browser. So what we did was correlate all the source logs from the browser and XDR and try to correlate them with the user's reactions as well as their daily usage. This helps us understand their daily perspective of how they are behaving. Behavioral analysis was easier when we connected all these systems. ."

KarthikB

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

Read full review

"Cisco XDR serves as the main platform for threat detection and threat response in my organization.

"We have integrated all of our internal devices including firewalls, servers, EDRs, and endpoints into Cisco XDR. In typical scenarios, we find blacklisted IP communication detected by our firewall, and Cisco XDR blocks these particular attempts made by blacklisted IPs, thereby helping us secure our environment from potential cyber threats.

"We focus on the alerts generated by Cisco XDR and the threat intelligence reports available on the platform. Our security team reads through those reports and proactively blocks those IPs and the IOCs on our firewall rather than waiting for Cisco XDR to raise an alert about a particular IP or IOC attempting to communicate with the environment. The threat intelligence information available on the platform is quite useful for us to proactively take actions to better secure our environment and reduce our attack surface for potential cyber threats.."

Pranav Salian
Head of Business Operations at SISA

Read full review

“I have used Cisco XDR to detect and respond to malicious activities on my client's endpoint. For instance, the last time I used it was when a client downloaded a malicious executable file, and when the endpoint picked it up as suspicious activity, I investigated and discovered using a threat intelligence platform, VirusTotal, that the hash of the executable file is malicious. I quarantined the endpoint and deleted the malicious executable file afterward, using it to block the malware.

It has positively affected our incident management process because Cisco XDR helps with early detection and does not allow room for escalation of malicious activities before remediation starts.

One function that Cisco XDR streamlines incident response through is its containment feature, which speeds up response time and demonstrates how it is useful in incident response.

For data loss prevention, I find it really helpful because it monitors email activities for some clients and reports suspicious data exfiltration activities, capturing and reporting instances when there is communication to a public IP suspicious for data exfiltration, allowing me to verify legitimacy with the client..”

Bolaji Kazeem
Cybersecurity Analyst at a outsourcing company with 51-200 employees

Read full review

"I use Cisco XDR for detection and response. I have an Insight license from Cisco XDR, which provides me with a powerful GUI on the cloud where I can see comprehensive insights from my machines. I also have an MDR service license from Cisco.

I use Cisco XDR for prioritizing incidents across multiple security controls. The second-best technical feature is incident correlation, which provides me centralized visibility and a single place to review incidents and investigate IPs, URLs, and domains. All log data is visible on one dashboard for managing incidents and taking actions with integrations and connectors to other products in my organization.

I have not yet run the DLP feature in Cisco XDR, but the XDR forensics capability provides evidence collection and forensics visibility, which works very well with incident correlation. Regarding DLP, I run an endpoint from Kaspersky, not Cisco. The integrations are strong, and I have purchased integrations from Cisco.

I have used the automation feature in Cisco XDR to improve workflows. I have connectors and direct integrations that allow Cisco to integrate with my firewalls using predefined integrations. I enable collectors and have connected firewalls, endpoints, and email systems, which allows me to take actions. For example, during a phishing incident, I run automations to investigate domains that trigger a phishing email, and I can block this domain on my email system through integration with Cisco XDR.

Cisco XDR has helped expose gaps in my security coverage. Since implementing it, I did not have NDR, and I opened a conversation with Cisco to implement the Cisco NDR module, which will be very useful to integrate with Cisco XDR. I receive detailed reports on traffic flow, so I can see on the Cisco XDR dashboard when user X attempts to connect to a malicious domain, for example.."

Mohamed Fouad
Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

The initial setup is not difficult and is very easy to command. We can easily find all the guidelines and necessary documentation online or from the Cisco site.

Aruna Udawatte

Director -Digital Transformation at Convergence

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

"My experience with the deployment of Cisco XDR was that it was simple. During the proof of concept, the setup was straightforward, and for the most part, we provided systems access to the security team, allowing them to tie everything together without needing additional help.."

Joseph Houghes

Cloud Architect at Pure Storage

Read full review

"Deployment went fine, but when it came to integration with tools, I was definitely the test guinea pig in terms of system failures. For two months, my Cisco XDR did not work because I was the one who found the observable issue and reported it to Cisco. There were multiple meetings and constant back and forth with engineers, telling them the things they were telling me to do were not working. They were not able to understand that I could not even log in to the application without it freezing. So, the deployment went well, but for the next two months, we had issues, which is normal with a new tool. We got it as soon as it hit the market, so we knew that there were going to be some complications.

I wouldn't say we have it fully set up right now. We're still integrating tools and workflows into it. We have it in working condition where we're able to do investigations in it, so we have it 95% set up now.."

Colin Oxendine

SOC Analyst at a educational organization with 501-1,000 employees

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

Senior Systems Consultant at W.C. Bradley Co.

Read full review

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

"I would rate Cisco technical support as extended, but their service is very unresponsive. It is very difficult to get in touch with them, so I would rate it a four out of ten.."

AjenthanAiyathurai
Manager IT at NVCL Group

Read full review

"I would rate technical support as a seven to eight because it is very great in current times. If I had to decide between seven or eight, I would say a seven.."

Shourya TejReddy KSS
Cybersecurity Consultant | Managed Infrastructure Services Head | Business Apps and DevOps Head at Blueberry Tech Solutions India Pvt Ltd

Read full review

"The technical support has been very helpful. During implementation, we receive assistance from the technical support team and have obtained proper support from their side.."

Ananda Deb
Technical Manager at Ledorbis Solutions

Read full review

"The customer support has been quite good. When we raise a ticket on technical support, they reach out to us within a couple of hours to listen to our issue and provide us with solutions. I would rate customer support at nine out of ten.."

Pranav Salian
Head of Business Operations at SISA

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

Other Advice

"With the functionality and support Cisco XDR provides, I advise others to go for Cisco XDR, whether for a small company or a large company. I rate this product 7 out of 10.."

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

Read full review

"My advice for other organizations considering Cisco XDR is that it offers proactive security measures that are really very helpful. It is also a unified control system where all emails and endpoints are visible on one dashboard, making it easy to understand, even for a non-technical person to quickly grab information by just seeing that. I would rate Cisco XDR as a product an eight out of ten overall.."

AjenthanAiyathurai
Manager IT at NVCL Group

Read full review

"Based on feedback from my client, they seem very satisfied with the output of Cisco XDR solution, so I assume they are content.

I recommend Cisco XDR to any client that may be interested because I have used a number of Cisco products and have no negative reservations at this point.

I would rate this product an 8 out of 10.."

Bolaji Kazeem
Cybersecurity Analyst at a outsourcing company with 51-200 employees

Read full review

"My advice for others looking to implement Cisco XDR is to establish licensing agreements beforehand and list your products for integration with Cisco XDR. You need to know which email systems, DLP solutions, firewalls, and vendors you will use, as this helps identify the best licensing for your needs.

Regarding how many people use the solution, I can say that we are running it on our SOC, which has multiple shifts and approximately eight SOC analysts.

Cisco XDR does not require any maintenance, as this is provided by Cisco. My overall rating for Cisco XDR is ten out of ten.."

Mohamed Fouad
Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

Read full review

"It is difficult to say because it depends on how many products a customer would have. But if they had an endpoint product, a firewall product, a network product,

and a cloud product, and they had an incident, they would have to get into each one of those and then do research, potentially an hour per product. Whereas now, they are in Cisco XDR and they are able to get the answer to this in less than thirty minutes. This is a huge time savings to me personally.

Getting the endpoint data is absolutely critical and Cisco XDR does a great job. Getting endpoint data from something such as CrowdStrike or from Cisco Secure Endpoint and then taking in data from the network with NetFlow logs or data from Secure Network Analytics or something that does IPFIX, and then the cloud logs and then also being able to do email integration for email threats, all of that data is available to investigate, to make decisions, and to see if one host ever talked to another host. When investigating an incident, that is extremely beneficial. The integration of that data and merging it into one screen where I do not have to look at different solutions is a great benefit. The merging of all of that data into one display is probably the best benefit of Cisco XDR.

There is the concept of playbooks where, if an incident is raised and there is a problem, it allows companies to build out how they want their incident response staff to operate. What is the first step? What is the second step? What do we investigate first? Who do we notify about this? It allows them to customize that response process to align with the company's own written IT security policy. This helps focus incident responders on the tasks that they need to do for that specific environment and focus on the things that are important to them, not just what Cisco thinks.

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

Fred Parks
Senior Systems Consultant at W.C. Bradley Co.

Read full review

"In terms of DLP, Cisco XDR is quite useful. We are using a different DLP as well

within our organization, so we are not extensively relying upon Cisco XDR for DLP, but it is a good solution to fall back upon. In terms of pricing, it is not the cheapest but it is also not the most expensive compared to other products we have experienced in the past.

“Cisco XDR is hosted on private cloud.

“We are typically deployed on AWS and have utilized automation workflows to improve our mean time to respond, reducing it from over 24 hours to less than 16 hours.

“We prioritize incidents based on its criticality in terms of which devices or environments are affected that we have integrated with this platform. This has definitely helped in prioritizing incidents and ensuring that we have good coverage twenty-four hours a day, seven days a week across business hours and non-business hours by looking at the trend of what incident types occur and how often they occur, as well as what kind of team support is required across multiple shifts during the day and night.

“The platform helps our SOC team access the platform across the entire shifts. We follow three shifts, and it helps with the shift handover when we transition from the morning shift to the afternoon shift or from the afternoon shift to the night shift. The platform helps seamlessly hand over from the previous analyst in the previous shift to the new analyst in the next shift.

“My advice to other potential buyers of Cisco XDR would be to always conduct an evaluation or a proof of concept before actually purchasing because each environment is different and while Cisco XDR may be useful in most environments, there are potentially some environments where it may not be useful. It is always good to try before you buy. I would rate this product an eight out of ten..”

Pranav Salian
Head of Business Operations at SISA

Read full review

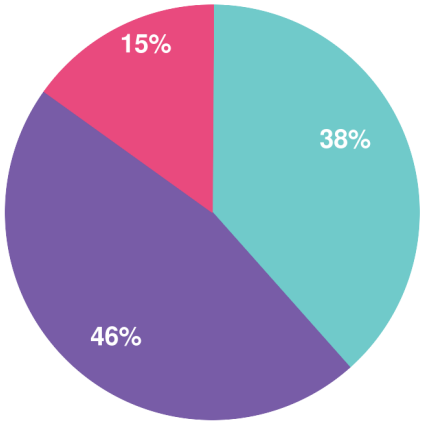
Top Industries

by visitors reading reviews

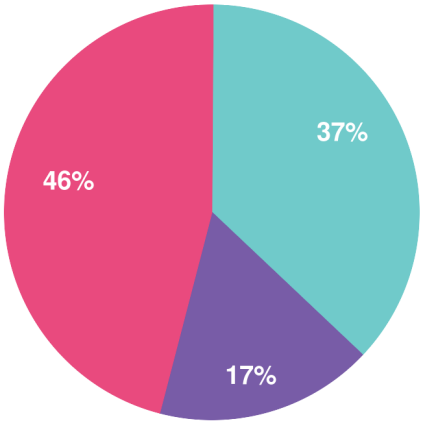
Computer Software Company	11%
Government	10%
Manufacturing Company	9%
Comms Service Provider	7%

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944