aws marketplace

Dragos

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Dragos

Dragos Recap

Dragos offers a comprehensive cybersecurity platform specializing in industrial control systems. It provides advanced threat detection and response capabilities tailored for sectors like energy, manufacturing, and water.

Dragos enhances security by providing specialized solutions that address the unique vulnerabilities present in industrial environments. With a robust framework, it monitors networks for threats, offers advanced analytics, and delivers actionable insights. This makes it essential for maintaining operational integrity and ensuring system protection against cyber threats.

What are the valuable features of Dragos?

- Threat Detection: Identifies risks specific to industrial control systems.
- Incident Response: Facilitates quick and effective handling of security breaches.
- Network Monitoring: Provides continuous oversight of industrial networks for threats.
- Intelligent Analytics: Offers insights through advanced data analysis.
- Threat Intelligence: Delivers focused, up-to-date information on security threats.

What benefits or ROI can be expected from Dragos?

- Enhanced Security: Protects critical infrastructure from cyber threats.
- Operational Efficiency: Reduces downtime through rapid threat detection and response.
- Cost-effective Protection: Minimizes financial impact of breaches through effective defense mechanisms.
- Strategic Insights: Boosts decision-making with comprehensive analytics and reporting.

Dragos is implemented across industries such as energy, manufacturing, and water to offer tailored solutions that improve cyber resilience. By integrating industry-specific knowledge and cybersecurity practices, it supports safeguarding critical infrastructure assets effectively.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Dragos especially ensures systems recover quickly, providing resilience, and it handles all the operational resilience in banking with metrics of 99.9% uptime, 30 minutes recovery time, and 99% transaction accuracy."

Rajesh Podishetty

Manager at a tech vendor with 51-200 employees

- "Dragos has positively impacted my organization by aiding us to compensate our time."

AhmedSherif

Cybersecurity engineer at Schneider electric

- "Dragos' best features are that they are more focused towards Incident Response, so they have a dedicated playbook in their platform, making it easier for anyone investigating any incidents to investigate the alerts."

Jehin Nadar

OT Cybersecurity Engineer at Nadar

"Dragos is more expensive than other vendors, probably about fifteen to twenty percent more, but it is generally worth the investment."

MarkLopez

Director of IT at a tech services company with 1,001-5,000 employees

What users had to say about valuable features:

Dragos offers several valuable features, including the capability to manage IoT devices on a centralized platform. It allows for updates to devices and uniform management counsel, enabling updates to all devices. Another key feature is its ability to manage cybersecurity aspects of devices, such as updating or isolating devices found to have vulnerabilities. It includes features for automatic discovery of devices and inventory management of devices, and it facilitates incident response by allowing for isolation or shutdown of devices in case of critical vulnerabilities.

MarkLopez

Director of IT at a tech services company with 1,001-5,000 employees

Read full review

“The best features Dragos offers are its capabilities for vulnerability management and asset inventory building, and the sensor can detect a lot of assets.

“What stands out to me about the inventory building and asset detection is the simplicity of detecting the assets and building tables that contain all the assets that I need to collect. Dragos has positively impacted my organization by aiding us to compensate our time. It is useful to have less manpower, so we do not have to use a lot of time to collect our assets and make an organized sheet manually. Dragos makes this automatically. It has already reduced our time and manual work since using Dragos, but I cannot share specific details because they are confidential..”

AhmedSherif
Cybersecurity engineer at Schneider electric

Read full review

“Dragos' best features are that they are more focused towards Incident Response, so they have a dedicated playbook in their platform, making it easier for anyone investigating any incidents to investigate the alerts. One of the main features of Dragos is that they have a dedicated Incident Response team, so if clients need any help, they are there to help.

“Dragos does real-time monitoring as well, collecting mirror traffic from the span port of the switch, and as soon as it gets the traffic, it analyzes it in real time and shows what's going on in the networks, which relates to the real-time visibility feature for ICS networks..”

Jehin Nadar
OT Cybersecurity Engineer at Nadar

Read full review

"The best features that Dragos offers include a really appreciated dashboard and especially the way the sensors are integrated, which allows any field engineer to perform the integration and see all the traffic that is going through. The only critical part is enabling Port Mirror to truly see all the traffic passing, which often causes problems or concern about losing information.

Dragos positively impacted the organization by providing visibility of all their components, although I do not know the current status since it has been almost a year since I left the company where Dragos was implemented.

I noticed specific improvements in security processes and team responses to incidents due to the visibility Dragos provided, especially when I got certified as an implementer and began to see more information until the operation of the dashboard was taken away from me, limiting my time to keep investigating and discovering more findings. ."

Cesar Agustin

Arquitecto De Seguridad at a tech vendor with 10,001+ employees

Read full review

"Risk detection while using Dragos helps identify that incident response planning is one of the options in risk detection. I have reduced it from 40% to 18.5%, and ICS visibility has also contributed to a 60% improvement overall.

"Dragos includes features like automated asset discovery, protocol-aware detection, incident response playbooks, and threat intelligence reports. Dragos supports monitoring of hundreds of thousands of assets and has positive false positive reduction.

"Governance alignment with formats like NERC, CIP, IEC, and others, broad-level reporting, and operational resilience are some of the best governance features providing the right guidelines and policies.."

Rajesh Podishetty
Manager at a tech vendor with 51-200 employees

Read full review

Other Solutions Considered

"My experience with integrating Dragos with other tools or systems was that no additional tools were integrated, as it was the first tool put in place and, to the best of my knowledge, it is still in use today unless it has been removed for some reason.."

Cesar Agustin
Arquitecto De Seguridad at a tech vendor with 10,001+ employees

Read full review

"I have not used any other tool, but there is one more tool called Nozomi Networks. That is another option I had considered, but I always use Dragos. Dragos was the very first option I used.."

Rajesh Podishetty
Manager at a tech vendor with 51-200 employees

Read full review

ROI

Real user quotes about their ROI:

Security does not provide direct ROI as it is not related to our products but is critical for maintaining operations. It is more of an insurance policy.

MarkLopez Read full review
Director of IT at a tech services company with 1,001-5,000 employees

"The return on investment is more about time saved. Dragos saves time compared to other tools, especially for employees. Together, I achieve reliability and accuracy at 99.9% uptime. The time saved has been significant compared to other tools in the market. It has really helped in achieving cloud data integration with different tools, saving time. It gives access to valid users, allowing me to know the transactions of different customers. Banking sectors can recover various banking sector operations in no time. Transactions and everything are covered in very little time. The time saved is a good example compared to other things.."

Rajesh Podishetty Read full review
Manager at a tech vendor with 51-200 employees

Use Case

We use Dragos specifically for managing IoT devices in the industrial sector within our manufacturing ecosystem. It provides a platform to manage, update, and keep track of all network information related to IoT devices. It allows centralized management of industrial IoT devices.

MarkLopez
Director of IT at a tech services company with 1,001-5,000 employees

Read full review

"My main use case for Dragos is for vulnerability management, which I rely on day-to-day. A quick specific example of how I use Dragos for vulnerability management in my daily work is that I made an asset inventory with Dragos sensors.

"If I am following the right procedure, it is good to go with good procedure. If we do not have the step-by-step procedure or the guidance, it may not be very simple to use.."

AhmedSherif
Cybersecurity engineer at Schneider electric

Read full review

"I am an engineer in a service provider company where we help clients choose and implement security solutions, and I'm still looking for a new solution.

"I am certified in Dragos, but I have not deployed it in client sites.

"I used Nozomi a few years ago for two years, and now I'm getting trained in it so that I can help clients implement the tool. My customers are still using it.."

Jehin Nadar
OT Cybersecurity Engineer at Nadar

Read full review

"The main use case I had for Dragos during that period was for infrastructure monitoring and to begin detecting any incidents or problems that could arise, especially configuration failures, such as unauthorized accesses or RDP sessions, mainly for an assessment of the OT infrastructure that existed at that time in the gas industry in Colombia.

A specific example of an incident or relevant finding that Dragos helped identify during that assessment occurred during installations when the switches were not being correctly set to monitor mode. Once we started to receive some initial traffic, it was detected that RDP sessions existed to devices on the OT network that should not have had them, which raised an incident that proved very significant because people thought RDP was never used, and it turned out that it was being used. ."

Cesar Agustin
Arquitecto De Seguridad at a tech vendor with 10,001+ employees

Read full review

"Dragos is a tool that is very specialized in OT and ICS cybersecurity platforms. Dragos is very stable and widely used in critical infrastructure sectors, mainly in banking, education, and insurance sectors. It provides excellent detection visibility, threat detection, governance alignment, and incident response capabilities. In a real-time banking security operation, Dragos is a very strong choice.

"In real-time banking environments, I use Dragos for fraud and transaction monitoring. Dragos integrates with other SOC systems to monitor OT and ICS systems in banking data centers as well as ATM networks. It integrates with all the different machines to identify any fraud or transaction issues that may be happening, such as incorrect deposits or withdrawals for particular customers. All of these things are monitored through fraud and transaction monitoring, which is one of the best real-time examples.

"Dragos also has asset visibility capabilities where it identifies and maps critical banking infrastructure assets like servers, ATMs, and payment gateways. Asset visibility helps understand what type of ATM and what type of servers are being used, who is accessing them, who is withdrawing funds, who is depositing funds, and who is using different features.

"Threat detection is another important capability where Dragos detects protocol anomalies and threats in real time while reducing false positives compared to IT-centric tools. If someone tries to detect the tool with improper options, tries to break down machines, or commits fraud, threat detection helps identify who that person is and what they have done.

"Dragos integrates with SOC systems, especially OT and ICS systems, to give a clear picture of a particular customer who has been using a specific ATM at a center. If a customer goes to a bank and tries to use different options such as depositing, making fixed deposits, withdrawing, or conducting any kind of transaction or fraud, the fraud and transaction monitor helps identify which bank the customer visited, which data center was used, what servers are in it, and what ATM networks are across it. It tries to identify each piece of information related to that customer and helps understand whether proper or improper things have taken place. It is more of monitoring and transaction control, and it is very

transparent toward any customer..”

Rajesh Podishetty
Manager at a tech vendor with 51-200 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 main challenges I faced during the implementation of Dragos were getting people to correctly implement Port Mirror, but beyond that, I did not encounter problems executing the commands since I have extensive experience working with switches and Linux.."

Cesar Agustin

Arquitecto De Seguridad at a tech vendor with 10,001+ employees

Read full review

Customer Service and Support

Customer service and support have been generally good. Support requests typically do not exceed twenty-four hours for resolution, and the cybersecurity support has been helpful. The platform's ease of use and device discovery ease are notable.

MarkLopez
Director of IT at a tech services company with 1,001-5,000 employees

Read full review

"My experience with Dragos technical support was non-existent since I had no need to contact them; I was certified to carry out the implementation, thus not requiring support.."

Cesar Agustin
Arquitecto De Seguridad at a tech vendor with 10,001+ employees

Read full review

"Customer support is good. I could rate it a 10 out of eight. They are very good in customer support. If someone is looking for Dragos, especially who are into specialized handling of cybersecurity platforms in a very high scalable manner, maybe toward any banking sector, and if they want to provide any asset visibility, threat detection, and governance alignment with incident response capabilities, I think when all of these come into picture, Dragos is a strong choice. There are other tools available, but Dragos is a very strong tool when comparing all its metrics, scalability, and governance.."

Rajesh Podishetty
Manager at a tech vendor with 51-200 employees

Read full review

Other Advice

“Dragos basically helped us get to know the entire infrastructure because there were many devices that not even the client themselves knew existed or that were still active, making it a very good tool; however, it requires a lot of hardware and knowledge, especially expertise from people who have worked in the industry and know security, which was lacking in the company where it was implemented, leading to lucky hits but ultimately prompting my decision to change companies.

My advice to companies considering implementing Dragos is to evaluate the tool but ensure they have a person who truly understands the industry, what operates within their OT infrastructure, and cybersecurity expertise, rather than someone who has simply taken a course or has a casual connection selling them the product..”

Cesar Agustin
Arquitecto De Seguridad at a tech vendor with 10,001+ employees

Read full review

“I have experience managing the tools Clarity, Nozomi, Dragos, Sangfor, and I am familiar with these products.

“My customers are already working with Devo, Dragos, Nozomi, Clarity, and these are locally deployed in the client sites, not bought on the AWS Marketplace.

“I have not used Devo, but I have used Nozomi and Dragos, so I do have experience with those products.

“I completed my certification in Dragos and recommend it to my customers already, and I have been dealing with Dragos for a while now.

“Dragos offers a threat intelligence subscription called worldview, so if a customer

subscribes to that, they will get regular threat intelligence.

“I have not used much of the detailed analytics and reporting functionalities of Dragos.

“Dragos is a good option to choose, as it performs well in the market.

“Dragos is a big name, and there is room for Dragos in the India market, and they should promote it more.

“The company that I'm working for is a partner with Dragos. I also have partnerships with other vendors including Clarity, Nozomi, and Fortinet.

“I was learning FortiSIEM three months back, but I am not certified in it, so I have been dealing with Fortinet products in a somewhat limited manner. FortiGate is what I mostly deal with from Fortinet.

“On a scale of 1-10, I would rate this solution a 6 or 6.5..”

Jehin Nadar
OT Cybersecurity Engineer at Nadar

Read full review

“Risk detection is something where I identify that incident response planning is one of the options in risk detection, which has reduced to 18.5% from 40%. Using ICS visibility has helped a lot, and a 60% improvement has been done overall.

“There are some features like automated asset discovery where I have proper visibility of the vendor and model context, determining what is automated to that particular option or for banking usage. Protocol-aware detection tunes to iOS or IoT OT environments, knowing what protocols and what aware detections exist. If any improper detection happens, the protocol gives awareness that something is going wrong. Incident response playbooks guide investigations of what is happening across banking systems, especially servers and databases.

“Scalability is another important feature. It supports monitoring of hundreds of

thousands of assets across multiple sites. More customers or different users who come and access different monitors, especially banking systems, have been enabled through this scalability. False positive reduction is another feature that understands behavior analytics tuned to OT protocols, minimizing alert fatigue. If false positive reductions or any deductions happen, they are tracked.

"Governance alignment has been very much improved in my organization by using Dragos. It supports formats like NERC, CIP, IEC, and standards called NIST and CFC compliances. These are government and governance compliance according to banking sector requirements based on unique identifiers and are always valid toward any system. Broad-level reporting provides risk scoring and incident records for audits. If any risk happens, I know what should be improved next time. If anything changes, I know what needs improvement. The reporting level, especially at board level in a high-level capacity controlling branches, especially from headquarters, is one of the benefits Dragos has provided. Operational resilience is another benefit where continuous monitoring of Dragos ensures reduced downtime and financial risk.

"Operational resilience is continuous monitoring. Metrics-wise, it helped me achieve downtime reduction of less than two hours of downtime per year for critical banking services. The Reserve Bank of India guidelines require banks to set impact tolerances for critical operations like payment processing. Recovery time objective helped me achieve under 30 minutes for core banking systems. Earlier it was around 3-4 hours and now it has reduced to 30 minutes.

"Dragos should be improved in deployment complexity as it requires OT engineering coordination. One needs to have proper engineering coordination to understand the system, deploy it, integrate it, and make all the complex things into one system. This is very challenging, and one should be really skillful and have experience to do that. Cost is another area for improvement as it is higher due to site-based licensing and expert services. The licensing is very heavy, and expert services are required. Integration needs alignment with IT security systems and compliance frameworks where controlling cybersecurity to prevent fraudulent persons or third parties from accessing the system is complex.

"Accuracy and dependency-wise, the tool is very accurate. The percentage of

error-free transactions processed in banking achieving 99% is one of the most important metrics for millions of daily transactions. Fraud detection accuracy is another metric where AI-driven fraud helps identify and especially 95% of detection happens through this accuracy. Data accuracy, especially in KYC, helps banks identify what type of KYC information like ID proofs is present, avoiding regulatory penalties at 99% accuracy. Reliability-wise, the core banking system is always at 99.9% uptime and gives the right measures toward any customer. Mean time between failure (MTBF) is another metric where ATM networks achieve more than 5,000 plus hours.

“I use AWS cloud for my hybrid deployment and have purchased Dragos from the AWS marketplace.

“Dragos especially ensures systems recover quickly, providing resilience. It handles all the operational resilience in banking, with metrics of 99.9% uptime, 30 minutes recovery time, and 99% transaction accuracy.

“I would rate this review an 8 out of 10 overall..”

Rajesh Podishetty
Manager at a tech vendor with 51-200 employees

Read full review

Top Industries

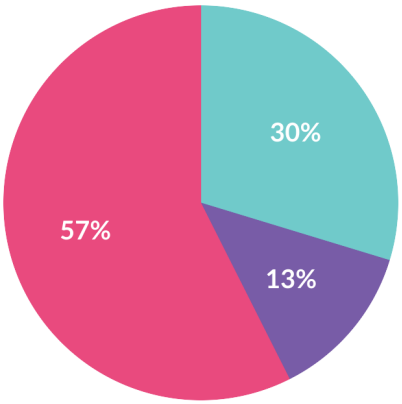
by visitors reading reviews

Energy/Utilities Company	16%
Manufacturing Company	12%
Outsourcing Company	6%
Healthcare Company	5%

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