aws marketplace

Cisco Security Cloud Control

# Reviews, tips, and advice from real users






Powered by PeerSpot

# Contents

# Product Recap

Cisco Security Cloud Control

# Cisco Security Cloud Control Recap

Cisco Defense Orchestrator (CDO) is a cloud-based management solution designed to ensure streamlined and consistent security policies across the Cisco security portfolio. Specifically tailored to manage all Cisco Secure Firewall form factors (running either ASA or Firepower Threat Defense (FTD) software), CDO offers real-time visibility and troubleshooting capabilities, effectively enhancing overall network security.

CDO addresses the challenges of migration, supporting transitions from on-premises to cloud environments and facilitating the shift from ASA to FTD configurations. As organizations embark on their cloud adoption journey, CDO simplifies provisioning workflows for remote branches, reduces operational expenditures related to inventory management, and offers scalability for multi-cloud deployments.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The most valuable feature is the automation, as it reduces user intervention and allows us to focus on other tasks."

Francisco Delos Santos
Security Engineer at Metrobank

- "We use a lot of image upgrades. We take some 20 devices and then we update everything at once, including the policies. We apply policies for groups. For certain groups, like anti-viruses, we send out policies and apply them to every single device. It's really easy and simple."

Jairo Mendes
Network and Security Specialist at CONNECTED TECHNOLOGY

- "If we have a firewall go down, I can hop into CDO, pull the latest configuration off and apply it. That's really good. It helps save time."

Dave Klunk
Network Security Engineer at a manufacturing company with 10,001+ employees

"There are a lot of templates that are already built-in. They give you quick-to-create and quick-to-apply policies that are typically a little more complicated for people."

Todd Ellis

CTO at SECURE NETWORKERS LLC

"Cisco Defense Orchestrator has useful guides for the steps that need to follow by users."

Vivek Balaji

Technical Director - Cyber Security at a comms service provider with 1-10 employees

"The most valuable feature is the Intrusion prevention."

Verified user

Cyber Security Pre-Sales Consultant at a tech services company with 51-200 employees

"With Cisco Defense Orchestrator, we can manage the complete Cisco Security solution. It provides a simple and centralized way to manage all products."

BinhNguyen1

Product Consultant at a tech services company with 501-1,000 employees

## What users had to say about valuable features:

"The most valuable feature is the automation, as it reduces user intervention and allows us to focus on other tasks. Since the system is automated, response times for resolving security issues are fast, providing quick prevention of threats and making us more secure against zero-day attacks.."

**Francisco Delos Santos**
Security Engineer at Metrobank

Read full review

"The most valuable feature of this solution is the centralization of device control. This helps to ensure that transactions between us and other companies are all secure. After we installed the firewalls we get reports for a safety check on a daily basis. Executive reports, custom reports, and penetration testing reports are all very valuable.."

**Verified user**
I.T. Manager at Egypt Foods group

Read full review

“The rule usage is a nice feature.

The ability to see the uptimes on the different VPNs that we have configured for site-to-site.

The overarching policy as far as the rules go and the assessment that it can do with the rule base.

The GUI on it was decently put together..”

**Verified user**
Network Engineer at a healthcare company with 10,001+ employees

Read full review

“I like the upgrade feature. That is pretty valuable to me because I have dual ASAs and when I go through CDO it does it for me pretty well. It's all done in the back-end and I don't really have to be involved. I just initiate, pick the image, and I pick when I want it done and it just does it, whether I have a single ASA or have a dual ASA. If I have a dual ASA and the primary is not active, the secondary wants me to make the primary active. It tells me that, but it's not a big deal.

I like the solution’s ability to make bulk changes across image upgrades.

For configuration changes, every time there's a change in the firewall, it records it in the cloud. If not, I have to go there and manually make sure it is sent. But it does have a configuration in the cloud.

In terms of firewall builds and daily management of existing firewalls, I use it for a rule-change or to add a rule to a single firewall..”

**Hamed Khakipour**
Sr. Network Engineer at Vocera

Read full review

“The most valuable feature is the restore history. For any changes that you have backed up, if something goes wrong, then the system will automatically prevent the system from crashing or from loss of the client's connection. When you start programming any ASA or device connected to CDO, if you make a mistake, you have the option to restore the previous configuration. You will not lose connection with the device and the client will continue working without problems.

We use a lot of image upgrades. We take some 20 devices and then we update everything at once, including the policies. We apply policies for groups. For certain groups, like anti-viruses, we send out policies and apply them to every single device. It's really easy and simple.

The solution’s security features for storing firewall configurations in the cloud are pretty secure. I don't see any problems with it. They have two-factor authentication. From what I see, it's working properly. I don't feel there is any gap there..”

**Jairo Mendes**
Network and Security Specialist at CONNECTED TECHNOLOGY

Read full review

“The most valuable feature is being able to do centralized upgrades on the ASAs. We can literally go in and tick a bunch of ASAs - we have them grouped within their business uses. We can select all of those ASAs, and say, "Upgrade these ASAs at this scheduled time." It will copy down the ASA image, ASDM image, and then do the upgrade and failovers, and then put it all back into service as required at a scheduled time. It automates that process for us.

We use the command-line tool quite a lot to push out bulk commands and changes to ASAs. That saves us a considerable amount of time. We have firewalls that are used for guest WiFi access. We try and maintain them as a standard policy. We can do that centrally and push that out.

As for its security features around storing our firewall configurations in the cloud, I take it that it's secure, from conversations I had at the time. It's all encrypted on REST and in transit. That goes through our security team, who respond with that information. It doesn't concern me particularly because I know it's all encrypted. We also use two-factor authentication to be able to log in to the solution as well. Obviously, you need the user name and password, and you need the multifactor authentication key. That's built-in, we use the one that's provided by CDO, which is OneProtect. That works for rules.

Everybody has their own login and I've got a full, change-management log view, so I can see who's done what changes. The other advantage we get from that is, if somebody makes a change and there happens to be an out-of-hours issue, the users can log back in and they can look at the changes that were made on that firewall, and they can roll it back by clicking a button..”

**Verified user**

Network and Data Centre Platform Manager at a manufacturing company with 1,001-5,000 employees

Read full review

# Other Solutions Considered

“I didn't use anything prior to CDO. I went to CDO for better management, central management. CDO was suggested to me and they gave me a free trial for a couple of devices. We eventually signed the agreement for security, which is included..”

**Hamed Khakipour**
Sr. Network Engineer at Vocera

Read full review

“We have something different, but at this point we are mostly using CDO. We use Cyberhub only to monitor vulnerabilities. That's all it does. With CDO we try to do SSH and all the language. But CDO doesn't have vulnerability monitors. That is something that they definitely need to improve on..”

**Jairo Mendes**
Network and Security Specialist at CONNECTED TECHNOLOGY

Read full review

"We did a few tests but I don't remember the names of the other products. What made CDO stand out is that you can do different devices at once. The other companies offered only one system. There was no way we could do updates on all the devices. That's really the strong point of CDO.."

**Jairo Mendes**
Network and Security Specialist at CONNECTED TECHNOLOGY

Read full review

"I didn't assess any other options at the time but I'm familiar with a couple of them. I tried Tufin, but that's just an auditing tool.

Another one was FireMon, but I haven't tested it out. That may be pricey, although I'm not sure. It seemed like it was an overlay on the ASAs, on the firewalls, so you could manage everything. What you could do in ASA you could do there. And the monitoring was pretty good too. But that was a few years back. I haven't looked at it recently. That tool was much better than CDO, when I think back.."

**Hamed Khakipour**
Sr. Network Engineer at Vocera

Read full review

“We actually got it before we decided to buy it. I heard about it at Cisco Live about three years ago and brought it back here. We decided to try it out. We thought, "Man, it looks pretty good. Let's buy it." And we bought it.

We didn't have a competitor's solution before CDO and that was another big reason to buy this. If nothing else it was, one of the things we were happy about, and that we feel justified the spend, was having the configurations kept in a central spot, where we can go really quickly and pull them down as need be. Without CDO, we had a problem with that a lot. A firewall would go offline and maybe our on-call didn't have the config, or the config was six months old, and changes had been made. With CDO, it is right up-to-date. It's so much easier.

We just kept tape backups all the time. With that many firewalls, it's hard for one person to do that and have an up-to-date configuration for all the firewalls. It was near impossible. This makes it possible..”

**Dave Klunk**

Network Security Engineer at a manufacturing company with 10,001+ employees

Read full review

“We are still using FireMon as our firewall manager right now. FireMon is definitely a little more feature-rich. It definitely could get further into the rule base of it. We didn't use FireMon to deploy anything, so it was more or less just to validate configuration, put a source and destination, and have it spit out what firewalls it would hit. We never really tried to sit down and do a comparison between the two. The UI within FireMon has probably a little more security-centric viewpoint.

I don't always spend a lot of time in either FireMon or CDO. These are for the security team who have ability to look and see policy, and if they want to make any changes or remove anything of that nature.

We are moving away from FireMon and starting to look more at a RedSeal approach right now. Some other members of my team have looked pretty closely into it. Our security team really liked it. I think they've actually issued a PO for it.

We will probably not be increasing usage of the product because we are moving over to Palo Alto firewalls. Eventually, a lot of ASAs that we have will be phased out..”

**Verified user**

Network Engineer at a healthcare company with 10,001+ employees

Read full review

# ROI

Real user quotes about their ROI:

"The biggest thing that we were looking at it for was the ability to push out a mass firewall change, if we needed it to. We just never got to a point of testing that feature and setting that up.."

**Verified user**
Network Engineer at a healthcare company with 10,001+ employees

Read full review

"I don't measure ROI, but for me, the return of investment would be the amount of time saved, versus doing it manually. The upgrades of the ASAs would be where the biggest time savings are for us.."

**Verified user**
Network and Data Centre Platform Manager at a manufacturing company with 1,001-5,000 employees

Read full review

“Once we had CDO up and running, after first implementing it, it took about six months to see value from the solution.

The ROI comes from the fact that, before CDO we had different teams in charge of different companies. They were responsible for updates, checking for vulnerabilities, making sure the devices follow protocols and have all the policies necessary in those companies. For the most part, the companies share the same policies. We try to leave everything standard. We had teams in charge of that, but now we have one person who is in charge of it. That is saving a lot of money for our company and time for the clients. CDO has made our security team more productive. We're saving all that time. Again, it's just one person who can now take care of that..”

**Jairo Mendes**
Network and Security Specialist at CONNECTED TECHNOLOGY

Read full review

“Once up and running, we see value from it right away. The impact is immediate. The biggest problem I have now is that something that gets forgotten is how bad things were before the implementation. C-level people tend to forget that.

The biggest part of ROI is the improvement to the operations. Our clients with CDO are having fewer issues. Things are just not going down. People are more productive. I don't know if any of the organizations that I've been with have done a study, but from an IT ticketing standpoint, tickets are down to one-tenth of what they were. People are able to bring in new projects and think about new things. From a staff being overtaxed due to remediation, because so-and-so clicked on an email or there was an issue with some type of a compromise, now it's eerily quiet..”

**Todd Ellis**
CTO at SECURE NETWORKERS LLC

Read full review

“The main return on investment is time. If a firewall goes down, the site goes down. We need to get the backup config for it and get it applied as soon as possible. If we don't have a decent enough backup config, we have to put a config on there that is supposed to be okay, but there can still be issues. Now, we get the site back up with the config they were running when it went offline. Some of these sites are our major mills. They do process control, handle large machines, they make paper and boxes, etc. Getting them back up the way there were saves time.

I'm sure somebody could put a monetary value on it. And the first time that happened, the savings probably exceeded what CDO costs. That would be a definite return on investment. I don't have a way to quantify, but I definitely believe it is worth the price we're paying for it, just in that respect alone.

The more Cisco keeps adding to CDO, the more capabilities, the better it's going to be..”

**Dave Klunk**

Network Security Engineer at a manufacturing company with 10,001+ employees

Read full review

# Use Case

"I use it to manage my group of firewalls, and I make some configuration changes with it. If I have to update multiple devices at one time I will use it as well.."

**Isiac Sullivan**
Network Administrator at Texas Hydraulics, Inc.

Read full review

"We provide consultation for all Cisco solutions. We give consultations to customers for buying a preventive solution like Cisco Email Security, Cisco IronPort, Cisco Security, Cisco Web Security. ."

**BinhNguyen1**
Product Consultant at a tech services company with 501-1,000 employees

Read full review

"We are using this solution for filtering and blocking some websites. It's a firewall.

This is the main tool for network segmentation and intrusion prevention. It blocks malware and malicious activity.."

**Verified user**
Cyber Security Pre-Sales Consultant at a tech services company with 51-200 employees

Read full review

"What I take primarily take advantage of are ASA upgrades. I also use it, sometimes, to see other backups, because each time there's a configuration change, it creates a backup for it. I also check out conflicts or unused rules. But I mostly use it for ASA, for management. ."

**Hamed Khakipour**
Sr. Network Engineer at Vocera

Read full review

"This is part of our network orchestration solution. It allows us to optimize our network. For example, if I want to communicate with a laptop, this solution gives us a way to route the communication.

We have a public cloud deployment using Microsoft Azure.."

**Hasnae Lamrani Alaoui**
Presales Engineer at DataProtect

Read full review

"We have it set up to test to look at policy from an overarching perspective. Then, we are hoping to use it for policy push, such as making both changes across different firewalls, but we haven't gotten to that point yet.

We have the on-prem relay, and then that connects into the cloud for Cisco Defense Orchestrator (CDO),

We deployed the most recent version about a year ago.

We don't use it on a day-to-day basis. It's not something that we really spend a lot of time reviewing. I just haven't had time to sit down with it.."

**Verified user**

Network Engineer at a healthcare company with 10,001+ 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 initial setup was pretty straightforward. I had one of the guys from Cisco show me how to onboard one device, and I was able to get the others onboard within about five minutes. There wasn't really an implementation strategy. He just showed me how to do one device at a time..”

**Isiac Sullivan**

Network Administrator at Texas Hydraulics, Inc.

Read full review

“The initial setup is straightforward.

It can take up to five hours to deploy.

We have a team of five who are mainly engineers to maintain this solution..”

**Verified user**

Cyber Security Pre-Sales Consultant at a tech services company with 51-200 employees

Read full review

"The initial setup of this solution is of medium difficulty. The deployment took one day, although for a larger infrastructure I think it will take more than one day.

One person is suitable for deployment. In terms of maintenance, two people including the administrator are sufficient.."

**Hasnae Lamrani Alaoui**

Presales Engineer at DataProtect

Read full review

"The initial setup was straightforward. We spun up the VM onsite. We generated the key that it needed to talk to the Cloud Orchestrator. After that, as I started adding devices, it was relatively quick and easy.

Provided that you can get the VM spun up without politics involved, it takes a couple hours to a day to set up.."

**Verified user**

Network Engineer at a healthcare company with 10,001+ employees

Read full review

“The initial setup was really straightforward. If the person setting this up has knowledge of firewalls and switches, it's pretty simple. It took about two hours for us to deploy. It depends on the company. It could be a company has only five ASAs, and that could take 20 minutes to one hour. All companies are different, so it depends on how many ASAs they have.

In terms of an implementation strategy, we used SSH first and then did the connections.

Deployment of the whole system can be done by one person. And similarly, it takes one person to maintain it..”

**Jairo Mendes**

Network and Security Specialist at CONNECTED TECHNOLOGY

Read full review

“I didn't actually deal with the server-build, but that seemed to go fine. We didn't hear any issues from the server team on that. The Secure Device Connector which is liaising with the web, we haven't had any issues with it. It was pretty straightforward. We did have a little bit of help when we first bought it. They had a couple of WebEx's to show us how to do some basic stuff. It seemed to progress, so we learned, researched, and have asked questions about it.

I don't remember how long the deployment took but it didn't stick in my mind as being overly cumbersome or painful, so it couldn't have been that bad. Otherwise, I'd probably remember it.

From my group, one person was involved in the deployment. She was handling it at the time. She worked with our server team to build the virtual server for the Secure Device Connector. There were probably one or two people on that team, at the most.

For maintenance, it's just me who gets into it and uses it. We don't really have anybody else on our team that does VPN/firewall. That's my luck of the draw..”

**Dave Klunk**

Network Security Engineer at a manufacturing company with 10,001+ employees

Read full review

# Customer Service and Support

“The customer service is helping us out and giving us great support when we need it. The Cisco team is helpful and knowledgeable when we put in queries or tickets. They consistently respond very fast to our issues and that helps us maintain productivity..”

**Verified user**
I.T. Manager at Egypt Foods group

Read full review

“Every time we've had a question, they've been johnny-on-the-spot. They answer really quickly, get emails back to us, and help as needed. We've had no issues with them whatsoever. It's like anything with Cisco. If you get ahold of Cisco and say, "We have a problem," they're right on it..”

**Dave Klunk**
Network Security Engineer at a manufacturing company with 10,001+ employees

Read full review

"I used the technical support once. It was to get a username reset. The experience was okay.

We use the solution support for our ASA devices. We also have Firepower, and at the time, it only does FTEs. Therefore, everything we deploy is in an FMC manner. We never could get that in there.."

**Verified user**
Network Engineer at a healthcare company with 10,001+ employees

Read full review

"Tech support is pretty good. Since day one I have received support. Anytime I have a question, I still reach out to my product manager and he and his teammates help me out.

I may have opened a TAC case once or twice and that was because of something that happened when adding a user. One thing I would like to see is more control when it comes to user setup. I don't have that. I cannot go ahead and set up a user. I have to open a case. It's time-consuming. Granted, it was fast, but I still had to send an email, wait, and go back and forth. That's something that I'd like to see changed. I don't know what the reason behind it is.."

**Hamed Khakipour**
Sr. Network Engineer at Vocera

Read full review

"On a scale of one to ten, tech support would be about a seven.

We definitely have to escalate the issues. The first tier is always complicated. We, ourselves, are basically second-tier here, so the guys don't often call support. We try to resolve problems here. I do recall that about eight months that ago we had a situation, a specific problem, but it was something out scope so the system was not supporting those devices. It took about a week to resolve it because we could never get the right person. We tried to explain what's going on and it was a little confusing. It had to do with CDO but not everybody at Cisco has knowledge of CDO.."

**Jairo Mendes**
Network and Security Specialist at CONNECTED TECHNOLOGY

Read full review

"Tech support has been very good. They've always answered the questions very quickly and resolved the issues very quickly. The last issue they did for me was a new user account.

The CDO team has been really good with us. They've been really helpful and they're always open to new ideas and improvements to the application. It's very good because, with a company the size of Cisco, quite often you don't get to give that type of feedback. But I've had quite a lot of conversations with Derek around bits that could be improved or bits that are not quite there but need to be. They've taken them away and worked on them and then you start seeing all the new features coming through.."

**Verified user**
Network and Data Centre Platform Manager at a manufacturing company with 1,001-5,000 employees

Read full review

# Other Advice

Cisco Defense Orchestrator is a solution that does not have a lot of competition, it is unique. However, the next similar solution would be Palo Alto Demisto.

I rate Cisco Defense Orchestrator a seven out of ten."

**Vivek Balaji**
Technical Director - Cyber Security at a comms service provider with 1-10 employees

Read full review

"Those who want to use Cisco Defense Orchestrator should build their own use case and see if it fits their environment. The most significant benefit for us is the response time because it automates our playbooks.

I would rate the overall solution as eight out of ten.."

**Francisco Delos Santos**
Security Engineer at Metrobank

Read full review

"I would recommend Cisco Defense Orchestrator. Cisco is a very good company and has a reputation. They can provide a comprehensive solution to customers. They have a lot of defense solutions for the network and endpoint security.

Cisco buys a lot of solutions and has a lot of acquisitions. When they combine them into one central management, the setup can be quite complex.

I would rate Cisco Defense Orchestrator an eight out of ten.."

**BinhNguyen1**
Product Consultant at a tech services company with 501-1,000 employees

Read full review

"My advice for anybody who is researching this solution is to consider the advantages that it provides in terms of infrastructure.

It is easy to configure administrators and other users who can generate reports and check the dashboard. For the moment, this solution meets our needs and I cannot think of any additional features that should be added.

I would rate this solution an eight out of ten.."

**Hasnae Lamrani Alaoui**
Presales Engineer at DataProtect

Read full review

"It's just a good product to have.

In terms of CDO's security features around storing firewall configurations in the

cloud, I haven't delved into that yet. I plan to get into it this month, but I haven't logged into it yet. I still use the ASDM a lot of times. I also have a FirePOWER which most of the firewalls are in and I will the FirePOWER Management Center for that because Orchestrator doesn't manage it quite as well. For firewall builds and daily management of existing firewalls, I normally use FirePOWER, as far as monitoring goes..”

**Isiac Sullivan**
Network Administrator at Texas Hydraulics, Inc.

Read full review

“My advice is to try to gain more knowledge of SSH. CDO needs to improve monitoring and reporting.

Every six months, we go in deep. We check the devices to make sure everything is working correctly. We have another system, not related to CDO, which is alerting us if something is not working correctly. It runs daily. For example, if we find any ASAs with vulnerabilities, we take the information from that third-party software and go to CDO and again do the update for all the devices that are affected.

We're not using CDO for firewall builds or daily management of existing files. It is not as strong in that.

Overall, I would rate the solution at seven out of ten. .”

**Jairo Mendes**
Network and Security Specialist at CONNECTED TECHNOLOGY

Read full review

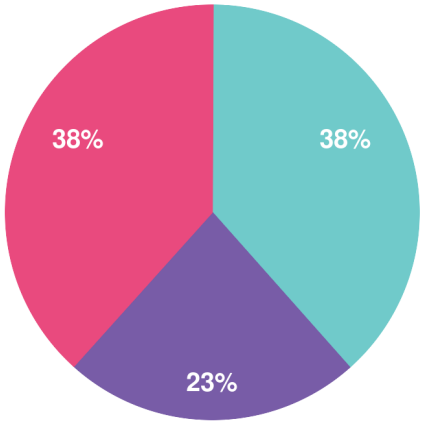
# Top Industries

by visitors reading reviews

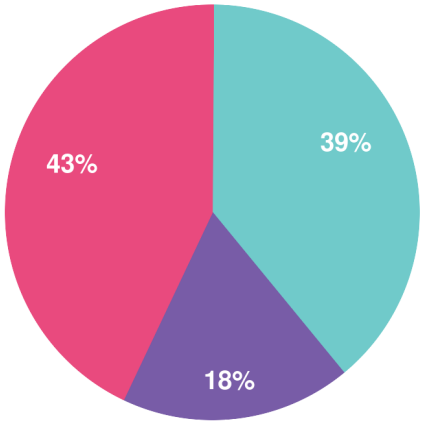
| | |
|---|---|
| Manufacturing Company | 11% |
| Computer Software Company | 10% |
| Financial Services Firm | 8% |
| Outsourcing Company | 7% |

# Company Size

by reviewers




by visitors reading reviews




Large Enterprise  Midsize Enterprise  Small Business

# About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

# Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

# About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

## PeerSpot

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

reports@peerspot.com

+1 646.328.1944