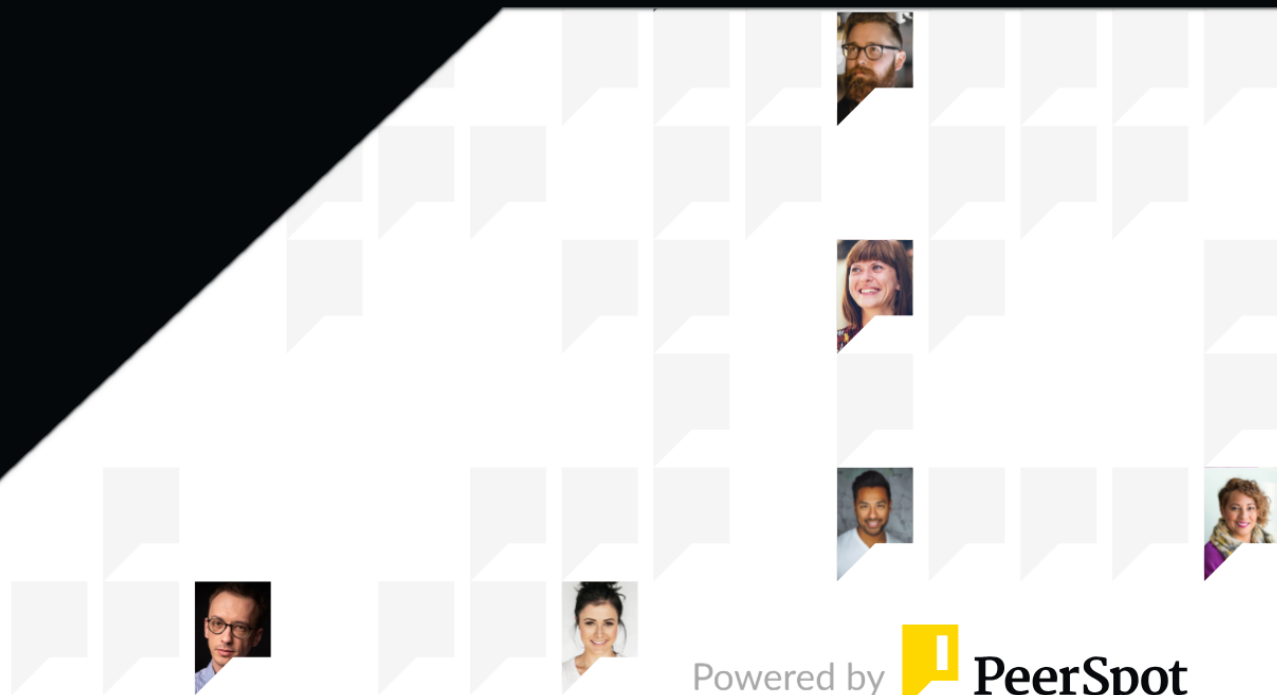




Cisco Duo

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 16

ROI..... 17 - 20

Use Case..... 21 - 25

Setup..... 26 - 28

Customer Service and Support..... 29 - 32

Other Advice..... 33 - 39

Trends..... 40 - 41

About PeerSpot..... 42 - 43

Product Recap



Cisco Duo

Cisco Duo Recap

Cisco Duo is a cloud-based identity security platform safeguarding critical resources for any user and device worldwide. Known for its ease of use, Duo offers seamless protection across multi-cloud, hybrid, and on-premises environments.

Cisco Duo is designed to secure access with identity-first protection and provides extensive visibility throughout an organization's identity ecosystem. Offering multi-factor authentication, Duo facilitates easy integration and management, allowing teams to protect data effectively on VPNs, applications, and networks. Its single-pane management improves security processes while enhancing trust, making it suitable for diverse IT infrastructures.

What are the key features of Cisco Duo?

- **Multi-factor Authentication:** Strengthens user verification with multiple methods.
- **Push Notifications:** Simplifies authentication with quick approvals.
- **Single Sign-On:** Enhances convenience by allowing one set of credentials.
- **VPN Access:** Secures remote connections with reliable authentication.
- **User Activity Visibility:** Offers comprehensive insights into access patterns.

Which benefits and ROI should users consider?

- **Quick Deployment:** Facilitates rapid integration within existing systems.
- **Effective Management:** Streamlines IT operations with centralized control.
- **Regulatory Compliance:** Aids in meeting industry standards for data protection.
- **Enhanced Trust:** Strengthens security posture across networks.
- **User-friendly Approach:** Simplifies authentication for non-technical users.

In industries like education and finance, Cisco Duo is widely employed to secure multi-factor authentication across platforms such as email, databases, and servers. Its integration capabilities with Microsoft 365, Active Directory, and VPNs like AnyConnect are instrumental in verifying user identities using mobile apps or OTPs, catering effectively to both remote and on-premise environments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Cisco Duo seems very scalable; in my experience, I started with a small-medium business, and in my last contracting position, it was a large one for a major worldwide airline that had hundreds of thousands of devices that could use Cisco Duo, and it scaled very well.”



Charles Slaustas

Information Technology Contractor at Insight global

- ✓ “Since we onboarded it, since we started using Cisco Duo, we have never had any operational glitch.”



Johnson Nejo

Technical Support Analyst at FBC Farm and Small Business Tax Consultants

- ✓ “The product is really amazing, and I think it is one of the best documentation sets I have ever seen.”



Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG



“In terms of operational efficiency, Cisco Duo has improved our security workflow significantly.”



Zeb Ramey

Director, Information Technology Technical Services at MOBILE INFIRMARY ASSOCIATION



“For one of my clients, the ROI was somewhere between 25 to 27 percent in year one.”



Tejas Jain

Principle Cloud Architect at a tech services company with 11-50 employees



“I appreciate the features that Cisco Duo offers.”



Syed Mohammed Ghouse

Network Security Engineer at a consultancy with 11-50 employees



“Cisco Duo has improved my operational efficiency and reduced costs in areas such as authentication, IT support, and security operations.”



Daniel Tsao

Cybersecurity Analyst at Broward County

What users had to say about valuable features:

“The assessment feature, also called posture, is what I find good. It performs checks on cell phones for new updates, patches, and so on. I think that is an interesting solution..”

Alexander-Rudenko

Technical Advisor at WM Group

[Read full review](#) 

“My experience with Cisco Duo's strong security authentication system has benefited my organization; it is quite simple. It helps to manage potential threats because there are many things; if you have connected any network equipment and someone has used any third-party equipment, it will alert immediately, detecting many things which are bypassing the network equipment very well.

“There is much that is helpful in having a complete passwordless environment with Cisco Duo; previously, we had a lot of password handling and saving, with people forgetting passwords, but now we do not face those problems anymore..”

ArjunAlva

IT Manager at KONGSBERG

[Read full review](#) 

“The specific features of Cisco Duo that stand out most to me are the strong multi-factor authentication, ease of use, and access control capabilities. Duo makes it straightforward for users to verify their identity while giving admins better control over who can access company resources. I also find the authentication visibility and security policies useful for managing remote and cloud-based access.

“Another valuable feature I find in Cisco Duo is the balance between security and user convenience. Duo provides strong MFA and access control while keeping the authentication experience simple for end users. The visibility and policy options also make it easier to monitor access and respond to potential security issues.

“Cisco Duo has positively impacted our organization by improving our overall access security by adding an extra layer of protection beyond passwords. MFA helps reduce the risk of unauthorized access from compromised credentials, especially for remote users. It has also made it easier for admins to apply consistent authentication policies while keeping the login experience relatively simple for users..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“The advantages of Cisco Duo include three categories: Essential, Premium, and Advantage. All these features may vary depending on these license SKUs. MFA is the primary use case for Cisco Duo. Phishing-resistant authentication based on the end-use, end-device profile is another use case, and obviously, ZTNA, or zero-trust security, addresses user identity, device health, and location. All those aspects are another advantage or another use case.

“Cisco Duo improves the visibility into identity-based risks, especially with the report for failed logins and authentication attempts. That provides more insight about our network and the users and how they are using our network. These are the two major features when we discuss the visibility part on Cisco Duo. Then obviously there is device compliance and user activity, but especially authentication attempts and failures and logins will give more insight to the IT team to secure their devices and their IT infrastructure.

“In terms of operational efficiency, using Cisco Duo helps organizations or management secure their workload. Also, they can reduce security threats, which will help them protect their financial partners..”

SreejeshSoman

Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

[Read full review](#) 

“I find Cisco Duo to be easy to use for multi-factor authentication compared to other authenticators that I have used. Cisco Duo is comparatively much simpler to use than others, so intuitiveness is something that I really appreciate.

“The interface is definitely easier to understand and the workflow is straightforward. Multi-factor authentication can be so challenging depending upon what authenticator you are using, as sometimes they make life unnecessarily difficult. Given that multi-factor authentication is an extra process, using other authenticators can feel much more burdensome than it should. Cisco Duo's process makes authentication much simpler. For example, even during setup, the process is really easy, and once you are set up, you do not have to battle with other authentication issues. It is just as simple as receiving a push, approving it, and that is it.

“I definitely feel more secure with Cisco Duo. Based on my talks with other people and my own reflection, I feel more secure knowing I have multi-factor authentication in place. I actually feel good about using Cisco Duo rather than others. I have other authentication apps on my phone, and Cisco Duo is by far the easiest. I feel that I am using a good product that not only secures my accounts but also will not be a headache to use. When I sign into other accounts that use other authenticators, I usually experience stress or anxiety that I will have difficulty authenticating. With Cisco Duo, the process is straightforward. I log into my accounts many different times, as I am a professor and must log in repeatedly when going to different classes. It does not give me a hard time. If I cannot approve the push due to internet connectivity issues, they can send me a code, and I know there are several other options available to get authenticated. That is another good point about Cisco Duo.

“Logging in with Cisco Duo's strong security authentication system has been easy for all the reasons I have explained. Definitely, having multi-factor authentication helps with phishing, and everyone uses Cisco Duo for multi-factor authentication in my organization. Having Cisco Duo helps with multi-factor authentication, which in turn helps prevent phishing emails, so there is a direct relevance there..”

Validated user[Read full review](#) 

Assistant Professor of Cybersecurity at a university with 1,001-5,000 employees

“The licensing model for Cisco Duo is really amazing because it is based on the number of users. When you buy Cisco Duo, you pay for the number of users and it does not matter how many applications you want to protect. It can be any number of web applications, any number of devices, anything. This allows us to make great deployments.

“When the customer is satisfied with Cisco Duo, they can become addicted to it in a good sense because we can cover pretty much everything. I love the fact that it tries to play the role of integrating multiple identities. I think that is where they are going, and I think that makes sense.

“Whenever a customer has multiple IDPs, for example, they have some LDAP servers, Active Directory, or RADIUS servers, Cisco Duo integrates it all. This is a lot harder with Microsoft or with other platforms. In general, the whole UI experience for an admin and also for users is very straightforward. They have integrated recently an AI assistant that is good. It can be better, but it helps you to configure things and to troubleshoot things. I really like the whole user experience of Cisco Duo, including the configuration experience, documentation, and support is great.

“Cisco Identity Intelligence, which is part of Cisco Duo, is a great feature that performs a lot of security checks on all accounts, including machine accounts and agentic users. Depending on those checks, administrators get notifications and based on those notifications, they can act.

“This is kind of a SOC CDC story. The admins managing Cisco Duo are not responsible for processing those monitoring or detections. Identity Intelligence is a great, amazing, and fantastic source of information that is absolutely relevant for the use cases that SOC CDC colleagues do for investigations that they run. They heavily rely on this and really consider it very much. They also integrate Microsoft similarly. For our managed service customers where we do SIM, CM, SOC, and CDC services kind of managed detection response, they use it a lot, so I think Identity Intelligence is a great tool.

“When it comes to agentic things, we are quite at the beginning of the whole cycle. We do not see yet that big organizations really deploy those agentic agents. Of

course, there are service accounts and those service accounts have been monitored, which is again a great tool. However, they are really afraid to create some AI tools that are just talking to each other because nobody has an overview about that. The organization security policy does not allow it for many customers, so it is not really a topic that we see right now. However, I think it will come at some point.

“Visibility is great, and you get all the possible logs and all the possible security posture results in Cisco Duo. First of all, administrators and organizations get a lot more visibility and understanding of what is happening in their network and which identities they have.

“With Cisco Identity Intelligence, you get a great overview of all possible accounts, including service accounts and user accounts. A lot of people start with the cleanup of those accounts because a lot of them are dormant, probably have been compromised, or have permissions that they do not need to have.

“Cisco also has a partnership with BloodHound Enterprise, which is a great tool to discover attack paths on the active directory, which is an identity access management relevant topic. This has helped a lot. However, I must admit that we should do a better job in there because unfortunately, many customers managing Cisco Duo are firewall or network admins, and they are not really security oriented. Sometimes this teamwork is missing between those firewalling Cisco Duo management teams and the security SOC at the customer where they can really exchange information. Unfortunately, this conversation sometimes is missing, and sometimes it is just political decisions. It is really hard to affect how people work between themselves and between different teams. However, we are trying, and I think Cisco Duo has all the capabilities to improve and answer those needs. It can help a lot already to many, but it can help more. We are trying to do good work there, but people are people and unfortunately, some people do not really work the best with each other..”

Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG

[Read full review](#) 

Other Solutions Considered

“A huge competitor in our market, especially in the Ukrainian market, is an HID product. The biggest difference between Cisco Duo and competitors is that they have an on-premise solution. That is the only difference, I believe..”

Alexander-Rudenko

Technical Advisor at WM Group

[Read full review](#) 

“Before implementing Cisco Duo, my clients were particularly concerned about phishing or credential-based attacks, typically involving user password theft or fake logins and credential stuffing.

“As far as I understand from our conversation, my clients usually choose Cisco Duo as a comprehensive identity security platform, not only as a standalone MFA..”

SreejeshSoman

Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

[Read full review](#) 

“Before Cisco Duo, our authentication environment relied more heavily on traditional username and password authentication and existing MFA capabilities. We moved towards Duo because we wanted a more consistent and security-focused MFA solution for remote users and cloud applications. Our main reasons were strong protection against compromised credentials, easier centralized administration, better visibility into authentication activity, and support for a broader range of access scenarios. Duo also provided a relatively straightforward user experience, which made it easier to encourage adoption of stronger authentication practices..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“Since we are using the same product only, we have stopped using SolarWinds.

“Approximately three months ago, we started using Datadog.

“We are using Cisco Duo and ThousandEyes as well..”

Charles A

Deputy Director at a healthcare company with 5,001-10,000 employees

[Read full review](#) 

“We considered other MFA and identity security solutions before choosing Cisco Duo. The main alternatives were solutions from established IAM and security vendors that offer MFA, conditional access, and remote access protection. Our evaluation focused on security capabilities and ease of deployment and user experience, integration with existing applications, administrative controls, and overall licensing cost. Duo stood out because of its strong MFA capabilities, a relatively simple user experience, broad integration options, and centralized administration. These factors made it a good fit for our security, remote, and cloud-based access..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“Cisco Duo is trying to be cloud only with SaaS deployment. It would be great if they did it on-premises. Here in Europe, there are plenty of customers that would benefit greatly from Cisco Duo, but they do not want it because it is SaaS only. I am not saying that they should do the whole on-prem version, but they could maybe do a data plane on site, and the control plane could reside in the cloud as SaaS. However, the data plane could reside on-prem, and for many customers, that would be already enough to consider it. Sometimes it is really a security policy. They hear cloud and they say no.

“Another thing that I am really looking forward to happening is integration with the Cisco Secure Firewall. That is in terms of identity intelligence, and those kinds of risks that are dynamically assessed by Cisco Identity Intelligence, which is part of Cisco Duo, could be shared with the secure firewall. However, the identities themselves and the mappings of which users are coming from where could be used, and that would also be fantastic. They do something similar with Secure Access. Cisco Duo integrates with Secure Access. However, there is room for improvement in there. I just do not know if they go that direction. I know a lot of people at Cisco because I work a lot with them. I know that they discuss it, and they want to integrate Cisco Duo more and more with Secure Access. I do not know if they plan for Secure Firewall. I hope they plan. It would be great to see more integrations in that area..”

Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG

[Read full review](#) 

ROI

Real user quotes about their ROI:

“The technology is evolving, and we need to adopt the technology, otherwise we are outdated. This technology started now, and while it will not completely replace human efforts, it has reduced about 50% of the workload..”

Charles A

Deputy Director at a healthcare company with 5,001-10,000 employees

[Read full review](#) 

“Regarding return on investment for Cisco Duo, it is possible to observe a good ROI because, from a security standpoint, Cisco Duo provides more ROI since its rich features help customers avoid using multiple agents. The single agent could secure their entire endpoints..”

SreejeshSoman

Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

[Read full review](#) 

“Cisco Duo's visibility into identity-based risk has been really good. We conducted a practice scenario with something similar to spamming, where you get one request and then another one immediately. You assume it's legitimate, but it's not, and you pass it anyways. You could have been lazy about it..”

Karrie Westmoreland

Senior Security Engineer at a consultancy with 11-50 employees

[Read full review](#) 

“I do not have the metrics, but regarding return on investment, I would say just by working in this field, I can honestly say that Cisco Duo has provided a return on investment based on security. We have definitely had that return because nowadays, the education domain is really targeted by malicious actors. Especially for students, who are not really concerned about security, Cisco Duo provides a layer of security, particularly for student accounts and many other users who are not explicitly concerned about security..”

Validated user

Assistant Professor of Cybersecurity at a university with 1,001-5,000 employees

[Read full review](#) 

“We have seen a positive return on investment mainly through improved security and reduced risk rather than through specific measured cost savings. Cisco Duo helps reduce the likelihood of account compromise by adding MFA, which can potentially prevent the much higher costs associated with security incidents. It has also helped streamline authentication and access management. Having a consistent MFA process makes it easier for the IT team to support users and troubleshoot authentication issues. While we have not calculated a specific dollar amount or percentage reduction in support tickets, the main ROI for us is the combination of strong account security, better control over remote access, and a more manageable authentication process..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“It is hard to calculate, but one of the features that has really affected operational costs is the fact that Cisco Duo can be integrated pretty well with any SIEM solution, also Splunk, which belongs to Cisco.

“SOC CDC teams that are doing security investigations rely on identities. Normally, it is relatively hard for them to get all of the possible identity logs. Sometimes it is just an IP address or the hostname. They get those logs from other systems or from the firewall. Cisco Duo adds this layer of identities. I know that SOC CDC colleagues spend a lot less time finding those identities and therefore reduce the whole operational cost. They would need less time finding out the identities and they can focus on other things. However, it is really hard to calculate because you need to take each individual customer, how many investigations that customer has, and how many it was without Cisco Duo and with Cisco Duo.

“I think it did improve a lot of things. From the configuration perspective, they have added an AI assistant recently, like some months ago. I think that is also great. That helps some people that are starting to work with Cisco Duo to do those configurations faster.

“The UI itself has developed a lot. There are a lot of explanations when you click on a button and when you see a feature, it explains it very well. That also helps to minimize the cost of configuration because some customers do not need to contact partners or somebody else more experienced. They can do a lot of things themselves, and I think they can do everything themselves. It is just that you have to read a bit, but it is not hard at all. Cisco is doing a great job in there..”

Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG

[Read full review](#) 

Use Case

“I use Cisco Duo for device management and logging in. We also use it for applications and single sign-on, and we have Duo Central for logging into our applications..”

Karrie Westmoreland

Senior Security Engineer at a consultancy with 11-50 employees

[Read full review](#) 

“The major use case for Cisco Duo is remote access VPN, which I believe is the widespread solution for remote access. I use it in combination with Cisco AnyConnect, Cisco Firepower, and Cisco Duo as an MFA solution..”

Alexander-Rudenko

Technical Advisor at WM Group

[Read full review](#) 

“My main use case for Cisco Duo is multi-factor authentication. Whenever I am trying to log in to a service, Cisco Duo sends me a push notification. I use it for different services including several of my work emails, Instagram, and many different applications. Whenever I am logging in, to ensure that it is really me logging in, I have to go to Cisco Duo and approve the push that was sent, or sometimes enter the code that has been given by the application. This ensures the security of my account..”

Validated user

Assistant Professor of Cybersecurity at a university with 1,001-5,000 employees

[Read full review](#) 

“My main use case for Cisco Duo is to address the issue of MFA and secure access for users, particularly protecting remote access and cloud applications from unauthorized access.

“A specific example of how I use Cisco Duo in my daily work is that we use it mainly to add an extra layer of security for remote access and cloud applications. A typical scenario is when a user tries to access a protected application or remote resource from outside the corporate network, Duo verifies their identity through MFA after the initial username and password. This helps ensure that even if a password is compromised, an unauthorized person cannot easily access company resources. We also use the MFA prompt and access control to improve our overall security for remote users.

“The main use case of Cisco Duo we use is that it provides an extra layer of protection for remote users without significantly changing their normal login experience. I primarily value it for strengthening MFA, reducing the risk of compromised credentials, and improving security when users access a cloud application or company resources remotely..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“I have completed a couple of installations for SSO or MFA using Cisco Duo, and it is possible. I have been working with Cisco Duo for nearly three years. Mostly, I have implemented it for MFA or SSO use cases, along with all these secure platform or user platform, especially for email security platform or user company or organization access security platform.

“Cisco Duo mainly serves as a security layer and a central control point, integrating with other security products. It is mostly integrated with other security products, especially Cisco Duo along with the Cisco security platform or Cisco fabric. Obviously, seamless integration will be possible. However, I am not sure about Cisco Duo's integration with other platforms as I have not done any integration of Cisco Duo with other platforms.

“In terms of deployment, I would say Cisco Duo is straightforward for the Cisco workload, with easy deployment. However, for other use cases, I do not think it will be that much easy, but I do not have personal experience; that is based on normal readings of marketing information.

“As for the deployment model, Cisco Duo works for hybrid, on-prem, or cloud platforms. Use cases and customer setups, like customer IT infrastructure, do not matter; the exact use case will be served if we evaluate it the right way..”

SreejeshSoman

Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

[Read full review](#) 

“Cisco Duo serves as an MFA platform with various primary use cases. The first use case is remote access VPN MFA, which protects VPN access for users. Integration with Windows RDP and device admin management use cases are also configured frequently. When administrators need to access network devices, switches, firewalls, routers, and remote desktop environments, these systems are protected with MFA.

“Cisco Duo is mainly an MFA platform, though Cisco positions it as much more. Once a customer has Cisco Duo, we can go into details and use all of the security assessment policies that they have, or a new solution that was recently integrated is the Identity Intelligence platform, which is a kind of ITDR focusing on identity threats monitoring and posturing. However, it all starts with the MFA.

“The product is really amazing, and I think it is one of the best documentation sets I have ever seen. The development platform has improved much. However, it is really hard to position against Microsoft because a lot of customers have Microsoft or Entra ID. Microsoft sells it for free, so they have similar MFA use cases and conditional access policies, and about 90% of customers have it for free. Cisco Duo shines in environments where there are multiple identity providers being used. However, that may only be relevant for really big customers. For smaller customers or medium enterprise customers that mainly rely on Microsoft IDP, Entra, and Active Directory, we have troubles because they prefer Microsoft since it comes for free and is also a great tool..”

Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG

[Read full review](#) 

Setup

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

“Setup is really easy, and once you are set up, you do not have to battle with other authentication issues. It is just as simple as receiving a push and approving it..”

Validated user

[Read full review](#) 

Assistant Professor of Cybersecurity at a university with 1,001-5,000 employees

“Since the product is only deployed on the cloud, installation is really easy. It is really easy to deploy. In a few hours, you will have access to the cloud GUI, and a few hours are needed to complete the integration process. It is absolutely easy..”

Alexander-Rudenko

[Read full review](#) 

Technical Advisor at WM Group

“My experience with deployments was that I deployed this as an end user and it was seamlessly available on the App Store and any type of store. There was no problem with the deployment or initiating Cisco Duo on the phone..”

Validated user

[Read full review](#) 

IT at a tech vendor with 10,001+ employees

“The initial deployment of Cisco Duo was difficult because setting up the original single sign-on was challenging.

It took me several hours across several days to deploy Cisco Duo for the first time because I kept giving up on the single sign-on. It was frustrating..”

Karrie Westmoreland

[Read full review](#) 

Senior Security Engineer at a consultancy with 11-50 employees

“Deployment of Cisco Duo was, at the beginning, a little bit tricky with the designing and all the considerations, then after that, it is very convenient to handle.

“For a non-prepared, non-technical user, it could be tricky and quite complex. The implementation part is not simple as it requires many things to be taken care of before it is a stable solution..”

ArjunAlva

IT Manager at KONGSBERG

[Read full review](#) 

“I think the setup for Cisco Duo is very straightforward. You have to understand the whole topic a bit, like what is possible and what is achievable. Cisco Duo is not only MFA; it is a real identity access management platform with a lot of security features in there.

“It takes some time to explain all of those capabilities, but the setup itself is very straightforward. However, in most cases, this topic does not land on the side of Windows or Active Directory admins that already know a lot about identities. Most of the time, the MFA topic lands on the firewall team because they start by securing remote access VPN and securing access to devices like switches. They do not know that much about identity, so it takes some time to explain how it works. I would say it is just more of a positioning thing, but the setup itself is very easy. If it lands on a person that knows about identities because they worked with identities before, that is very self-explanatory..”

Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG

[Read full review](#) 

Customer Service and Support

“I do not use customer service or tech support because I do not need it; the product works well. I would rate the support a ten out of ten because the product is reliable..”

Validated user

Supervisor, Network at a transportation company with 201-500 employees

[Read full review](#) 

“My experience with Cisco Duo's customer support and technical support has been great. Anytime we have run into a hurdle where we cannot figure it out, technical support is right there and very quick. I rarely rate things at ten, so I give it a nine because I always see there is room for improvement..”

Validated user

Network Administrator at a university with 10,001+ employees

[Read full review](#) 

“Cisco technical support is absolutely helpful because I have very good communication with the local Cisco office in Ukraine. The first line of support, Cisco TAC, is absolutely good with no problems or issues. In the case of emergency situations, such as P1 cases, I have the ability to contact our local colleagues in the Kyiv office to escalate our issues. Support from Cisco is absolutely good with no issues or problems..”

Alexander-Rudenko

Technical Advisor at WM Group

[Read full review](#) 

“Like any other support team, there are certain things that they can improve. One area that could be improved is response time for more complicated technical cases. It would also be helpful to have more detailed troubleshooting guidance for integration-specific issues so administrators can resolve common problems without always needing to contact support. The support is reliable, and the combination of documentation, self-service resources, and technical support provides a good experience..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“I'm sure Cisco Duo's customer service and technical support are great, but I haven't had to call them, which is a good thing.

“On a scale from one to 10, I would rate Cisco Duo's customer service and technical support a 10 just because I haven't had to use them, but I'm sure they are top-notch because they are a Cisco-based company..”

Validated user

Bdm at a tech vendor with 1,001-5,000 employees

[Read full review](#) 

“Depending on the customer, if we have implemented Cisco Duo correctly or if my organization heavily relies on Cisco Duo, it cannot be gone in a minute because we rely on that. If we cannot have Cisco Duo anymore for some reason, we would need to migrate to another solution, and that would take a lot of effort.

“There are solutions that can cover use cases of Cisco Duo, such as maybe Okta, though maybe not all of the use cases. Most of them can be covered, and the other use cases may be covered somehow elsewhere, but somewhat differently. That would be a big, massive effort to migrate from Cisco Duo.

“Cisco Duo cannot be easily replaced. If you configure it correctly and it is a primary authentication source, then you federate with an IDP, for example, and you need to federate other things. The federation itself is a real, global, major change. That is a complete traffic outage of the whole company. That is really hard if you go this way of relying on Cisco Duo as a primary authentication source. Not every company does it. For some of them, it is a lot easier to replace Cisco Duo, depending on how many applications they secure. However, for some customers, that is practically possible, but it is a massive effort..”

Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG

[Read full review](#) 

Other Advice

“I chose a rating of nine out of ten for all the reasons I have told you before. I think I would say just set it up correctly and let Cisco Duo do its job. My overall review rating for Cisco Duo is nine out of ten..”

Validated user

Assistant Professor of Cybersecurity at a university with 1,001-5,000 employees

[Read full review](#) 

“I do make use of advanced identity threat detection and response features.

“I am not much of a user, but we have a team to handle those things, which are the advantages of Cisco Duo.

“In the past one year, we have not upgraded to any new features.

“I am not much aware about Cisco Identity Intelligence, but my team looks at those things; I have very little information on that.

“My overall rating for this product is seven..”

ArjunAlva

IT Manager at KONGSBERG

[Read full review](#) 

“Regarding the impression of Cisco Duo's Identity Intelligence capability, I do not have much experience with the capability at this time, but it provides really good visibility for information purposes. Unfortunately, I do not have enough

experience with the capability to comment further.

“Regarding whether a complete passwordless environment is beneficial, the major point is that you do not need to track all passwords. You need to track different passwords for different applications and solutions. You do not need to use third-party password management tools. It is really simple to provide and obtain secure access where you need it. That is the most advantageous feature of the passwordless solution.

“If asked to subjectively rate support from zero to ten points, I would give it eight or nine points.

“My overall rating of Cisco Duo on a scale from zero to ten is 8.5, as it is close to nine..”

Alexander-Rudenko

Technical Advisor at WM Group

[Read full review](#) 

“Cisco Duo is only a SaaS solution. There is nothing else.

“Cisco Duo is still kind of an island in Cisco. It is another team and kind of another company in a company. I would say they are really good, and I have really great experience with those people. They are always helpful. In general, for customer experience, they are always trying to reach out to ask for feedback, and I see that they consider those feedbacks. I would rate them as a nine. Not a ten because it is hard to be everything ten.

“Cisco Identity Intelligence, which is part of Cisco Duo, is a great feature that does a lot of security checks on all accounts, including machine accounts and agentic users. Depending on those checks, administrators get notifications, and based on those notifications, they can act.

“I would rate Cisco Duo a nine because they can improve in some cases like everybody. However, I think it is a really good tool. They are trying now to really promote it. You get it kind of almost for free with some products. With Secure Access, you get it, and sometimes with a great discount. However, the whole story of Microsoft is really hard to compete with in general. If it was Okta, I am sure that Okta is also struggling to compete with Microsoft because they just come in, and everybody realizes that they give the authenticator capabilities for free. That is a hard conversation to have. The overall review rating for Cisco Duo is nine out of ten..”

Yahor Charkasau

Security Systems Engineer at NTS Netzwerk Telekom Service AG

[Read full review](#) 

“I have never worked with [AWS Marketplace](#) and do not have experience with their marketplace.

“Regarding AI integration in Cisco Duo, I did not go through the AI part of Cisco Duo, but as per my theoretical knowledge, it will help us to get protection. Cisco

Duo will help us with some sort of AI security part as well.

“As previously mentioned for [Cisco Secure Access](#), my clients using Cisco Duo do utilize [AWS](#) as the main cloud provider.

“Cisco Duo contributes to clients becoming more resistant to phishing attacks because its device health check before authorizing to the network helps us ensure clean device access to our network. If that device is compromised, it will obviously be quarantined and will resist connecting to our network. That will help us.

“I would say Cisco Duo helps to evolve the [IAM](#) strategy from simple authentication to a more comprehensive identity security platform, as mostly all these SSO or MFA is for protecting from these simple authentication parts. Cisco Duo integrates well into the environment, acting not only as a security layer but also as a central control point that integrates with various other products.

“I give this review an overall rating of ten out of ten..”

SreejeshSoman

Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

[Read full review](#) 

“On a scale of one to ten, I would rate Cisco Duo an eight out of ten. It offers strong MFA, good ease of use, and solid access control with some room for improvement in administration and reporting.

“I chose eight out of ten because there is room for improvements, primarily in administration, reporting, and troubleshooting. These are the few areas where it can improve.

“Regarding Cisco Duo's AI capabilities, I think it takes a security-focused approach to its AI features. From a governance perspective, the AI features operate within clearly defined access control and security policies, particularly when dealing with identity and authentication data. I value transparency around how AI features use data, what information it retains, and how administration can control or configure

those capabilities. Strong privacy protections, access control, auditing, and clearer governance policies are important for building confidence in AI within an enterprise security environment. Overall, I see AI as a useful addition to Duo, but security, privacy, transparency, and administrative control should remain the priority.

“I find that Cisco Duo's AI capabilities appear useful for improving security visibility and helping administrators identify and understand potential security issues. The output is generally helpful when used as an additional source of information rather than the sole basis for security decisions. One area that could be improved is providing more context behind AI-generated recommendations, including why a particular conclusion was reached and what data contributed to it. Clearer explanations and context would make the output easier for security teams to use. I consider the AI capabilities a useful part of the solution, and this can inform security decisions.

“Cisco Duo is deployed in our organization primarily as a public cloud SaaS solution. This makes it convenient to protect users accessing cloud applications and remote resources without requiring us to maintain a separate on-premises MFA infrastructure. The deployment model also makes it straightforward to scale the number of users and applications as we grow. We can manage authentication policies centrally while enabling users to authenticate securely from different locations and devices.

“We use Cisco Duo as a Cisco-hosted SaaS solution, so we do not directly select or manage the underlying cloud provider. The service is hosted and managed by Cisco, while we manage our Duo configuration, user authentication policies, and integrations.

“I have not used Duo's conversational AI interface extensively for administration tasks yet, but my experience has primarily been with the core MFA, access policies, and administrative features. However, I see that a conversational AI interface could be useful for quickly finding configuration options, underlying authentication issues, and guiding administrators through troubleshooting steps. I view it as useful assistance while still validating any recommended configuration changes before applying them.

“We have not extensively used the Advanced Identity Threat Detection and response capabilities in Cisco Duo, so I would not want to overstate our experience with the feature. Our primary focus has been on MFA, access control, and securing remote and cloud application access. However, the capabilities are valuable from a threat management perspective because detecting risky identity behavior can help security teams identify suspicious authentication activity earlier and prioritize potential threats to take appropriate action before compromised credentials result in unauthorized access.

“I evaluate the benefit of having a complete passwordless environment in my organization as providing significant security benefits because it reduces the risks associated with weak, reused, or compromised passwords. It can also improve the user experience by reducing password resets and making authentication simpler with methods such as security keys or biometrics. The main challenges involve adoption compatibility. Some legacy applications may still depend on passwords, and users may need time to become comfortable with the new authentication methods. There also needs to be a reliable recovery process for situations such as lost or replaced devices. Overall, I see passwordless authentication as a strong long-term direction, particularly with MFA, device trust, and risk-based access control. A gradual rollout is usually more practical than eliminating passwords immediately.

“My experience with Cisco Duo's strong security authentication system has generally been straightforward and easy. Once the initial setup is completed, the MFA process adds only a small step to the normal login experience. The push notification and other authentication options make it convenient for users to verify their identity quickly. The main challenges can occur when a user changes or loses their phone, as connectivity issues or the need to re-enroll the device may arise. In those situations, administrator assistance may be required. Overall, the additional security provided by Duo is worth the small amount of extra effort during login.

“Recently, our focus has mainly been on strengthening MFA and improving access control rather than rolling out completely new Duo features. We have been making better use of Duo's authentication policies and administrative visibility to improve how we manage remote and cloud-based access. These capabilities have helped us

apply more consistent security controls, monitor authentication activity, and respond more effectively when users experience access or authentication issues. We are also interested in newer capabilities around risk-based authentication and identity threat detection as potential next steps for improving our security posture.

“Our organization has taken a layered approach to become more resistant to phishing attacks. This includes strengthening MFA, educating users about suspicious emails and links, and enforcing stronger authentication policies and monitoring unusual login activity. We also encourage users to report suspicious messages and provide guidance on common phishing techniques. Cisco Duo contributes by adding an extra authentication layer beyond the username and password. Even if a user's credentials are compromised through phishing, MFA makes it more difficult for an attacker to gain access to protected application resources. Duo's authentication visibility and access policies help administrators identify suspicious behavior and strengthen controls for remote users.

“My advice for others looking into using Cisco Duo would be to clearly define your MFA and access security requirements before choosing a Duo plan. Start with the applications and user groups that need the most protection, especially remote users and critical cloud applications, and then expand gradually. I would also recommend planning the user enrollment and device recovery process in advance. Good communication and user training can make adoption much smoother. During the evaluation, pay attention to not only the MFA features but also to the integration, policy management, administrative experience, and security. Cisco Duo is a strong choice for strengthening identity and security, making authentication less complicated for users.

“It is a pretty good platform for authentication, reliable, and it can be a valuable security platform for your MFA needs. I rated Cisco Duo an eight out of ten overall..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

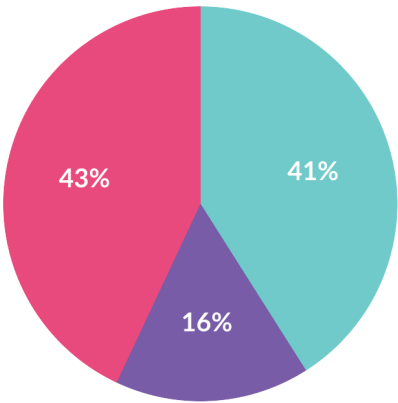
Top Industries

by visitors reading reviews

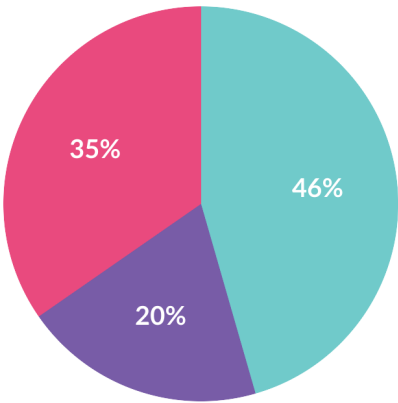


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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