

Fast forward to a brighter future

With the Cisco Duo MSP Program





Introduction

Welcome to the Duo MSP Program

It's time to move forward and share a brighter future with your customers via the Duo MSP Program.

A future that improves security by:

- **Protecting identity and helping to prevent cyberattacks**
- **Boosting productivity by frustrating attackers, not users**
- **Adding value through streamlined authentication**

Duo MSP is a program designed to build your pipeline, create new opportunities, and deliver improved security and better business outcomes for your customers. With Duo, you can empower those customers to verify user identity, ensure that every device accessing applications meets pre-defined security requirements, and provide a secure connection to their organization's networks and applications. It's easy to set up, easy to scale, and always improving to protect against whatever threat comes next.

The Duo MSP Program offers a range of tools to help you share this good news — and build long-term relationships so you retain their business too. This playbook is one of the most important of these tools.

In the following pages, you can quickly and easily find out more about our solution — including product updates, a summary of the advantages that Duo delivers, and the key messages that will convey the value all of this represents for your customers.



Table of contents

Section 1	
How to Solve Customer Challenges	6
Section 2	
Cisco Duo 101	9
Section 2.5	
At-a-Glance Sales Play	12
Section 3	
Duo’s Security Innovations	15
Section 4	
Real Customer Stories	20
Section 5	
The Duo MSP Partner Program	24

When you hear customers ask questions like these, Duo will provide many of the answers they need. This playbook will be the place where you can find those answers.

01 “How can we protect ourselves against increasingly sophisticated phishing attacks?”

It's true: phishing tactics continue to evolve, outsmarting what once were adequate multi-factor authentication (MFA) solutions. MFA fatigue, push, and adversary-in-the-middle (AITM) attacks challenge your perimeter in new ways and require a more rigorous response. The difference with Duo? It's deliberately designed for this world of evolving threats.

An MFA and access management innovator, Cisco Duo continues to pioneer new approaches that keep your business a step ahead of the next threat.

[7 Steps to Advanced Anomaly Detection | Duo MSP Brandfolder \(Infographic\)](#)

02 “How can we balance security with productivity?”

Duo can help you achieve your organization's security objectives while keeping your employees productive. That's true in a wide range of scenarios including continuing the zero trust journey, implementing the BeyondCorp model for remote access, enforcing least privilege access for users and devices, meeting security controls for compliance requirements, and lowering operational costs through vendor consolidation.

[Duo Risk-Based Authentication | Duo.com](#)

[Duo vs. Traditional Two-Factor | Duo.com](#)

03 “Why Duo, why now?”

Cybercriminals are increasingly targeting weak MFA implementations. Duo is actively responding and improving. Over the last year, Duo has introduced 20+ security-oriented innovations such as passwordless and risk-based authentication, and improvements to single sign-on (SSO) - all of which directly combat these attacks.

[Duo MSP Solution Overview | Duo MSP Brandfolder \(PDF\)](#)

04

“Our IT team is already stretched and we’re struggling to recruit. Will deploying Duo push the team over the edge?”

With the Duo MSP team to support you, you can help your customers protect critical applications quickly and smoothly, putting enrollment and remediation in the hands of users so security experts are free to focus on more strategic tasks and deploy securely in days – not weeks or months.

[Customer Deployment in 60 Minutes | Duo MSP Brandfolder \(Webinar\)](#)

05

“Other vendors offer MFA for free. Why should I pay for Duo?”

Customers deserve to know that they are usually not comparing apples with apples in this situation. Duo pricing is comprehensive and transparent, and customers are not obliged to buy our solution as part of a bundle. Naturally, customers are also able to use a “free” solution side-by-side with Duo to get the best of both worlds and be confident that all options are covered if that is their preference. But while such free or low-cost MFA can be helpful for some organizations with limited use cases and narrow security needs, many organizations find themselves in need of a more robust solution to fully secure their workforce. There are at least five good reasons why. Read about them in more detail:

[5 Reasons to Choose Duo Over Free Multi-Factor Authentication | Duo Blog](#)
[Cisco Duo Vendor Agnostic Comparison Infographic | Duo MSP Brandfolder](#)



Section 1

A brighter future

Solving customer challenges. Building a better business.

What does a brighter future look like for MSPs? In our view, it looks like more security for your customers, and better business for you. That's exactly the vision driving the Duo MSP Program.

If you see that as the way forward for your business, start by talking to customers and prospects about the most pressing security challenges they're facing right now. We've identified some of the current pain points you're most likely to hear, along with quick and simple replies on how Duo can make things better.

These are great ways to start productive conversations:

Challenge 1

"Other vendors offer MFA for free. Why should I pay for Duo?"

"Threats are increasing and we need a way to react and stay protected."

Further reading:

- [Cyber Liability Insurance for Small and Medium Businesses Duo Security \(EBook\)](#)
- [Duo for Cyber Liability Insurance Duo MSP Brandfolder \(PDF\)](#)
- [Cyber Liability Insurance What You Need To Know Duo MSP Brandfolder \(EBook\)](#)

How to respond:

Enhanced Multi-Factor Authentication (MFA)

It's clear that weaker MFA implementations are under attack as bad actors invest significant time, energy, and focus exploiting weak implementations with "ransomware-as-a-service" attack kits equipped with support contracts and fully staffed call centers. In addition to the security threat, this creates additional pain for enterprise customers as insurers increase premiums while reducing coverage. That's why Duo is bringing protection previously available only in our most advanced edition to every Duo customer.

All Duo paid edition customers can now block access from unknown devices and only allow trusted devices to gain access to resources. In other words, even if an attacker tried to use stolen credentials for access, their device (unknown to the system) should give them away.

Over the last year, Duo has introduced 20+ security-oriented innovations such as passwordless, risk-based authentication, and improvements to single sign-on (SSO) — all of which are designed to directly combat these attacks and extend protection well beyond standard MFA implementations. We also recognize how important speed of response can be. That's why Duo deploys in minutes to protect your client organizations.

Challenge 2

“Hybrid working is a fact of life for us now. How can we keep it secure?”

“What is the best way to protect our network, data, and applications – wherever and whenever our people choose to work?”

How to respond:

Duo’s risk-based authentication helps organizations build a zero trust framework that can meet the challenges of an evolving, complex security landscape and reduce the risks that come with hybrid working. At each login attempt, Duo verifies user identity, validates device compliance, and ensures least privilege access to specific applications. Never trust, always verify.

Duo’s zero trust model establishes trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application. For your hybrid workers, that means a seamless experience as you unify security and connections at scale.

Further reading:

- [From MFA to Zero Trust | Brandfolder \(Ebook\)](#)

Challenge 3

“We’re an Office 365 House. What’s the best way of keeping ourselves secure?”

“We need security that works without a problem for our Microsoft apps.”

How to respond:

Duo has you covered. Cisco Duo is the only solution to offer native multi-factor authentication support for Azure Active Directory, allowing you to securely access all your cloud and on-premises applications with a consistent and simple log-in experience. Whether you’re accessing Office 365, WinLogon & RDP, or any Microsoft application, Duo gives you enhanced visibility into every user and device. Confidently protect access to your entire Microsoft infrastructure when you choose Duo – over 30,000 organizations already do.

Further reading:

- [Duo for WinLogon & RDP | Duo MSP Brandfolder \(PDF\)](#)
- [Duo for Microsoft | Duo MSP Brandfolder \(PDF\)](#)



Challenge 4

“Our compliance workload just seems to get bigger all the time. How can we make it more manageable?”

“Our resources are already stretched so we could definitely do without the additional workload of managing a growing regulatory burden.”

How to respond:

Meeting the standards of the security industry is a priority for Duo. We have a team of independent third-party auditors regularly auditing and reviewing our infrastructure and operations to ensure we’re secure enough to support our customers. That’s how you can be confident that our solutions cover you for a range of legislative requirements across different jurisdictions including SOC2, FIPS CAVP, FEDRamp, EPCS, NIST SP 800-63-3, ISO 27001, 27017 and 27018, FIPS 140-2, IRAP (including Essential Eight), General Data Protection Regulation (GDPR), and Cloud Computing Compliance Controls Catalog (C5).

Further reading:

- [Industry and International Compliance | Duo Security \(Duo.com\)](#)
- [Duo for Compliance | Duo MSP Brandfolder \(Infographic\)](#)

Challenge 5

“Frankly, security is the last thing we want to be thinking about. Our focus is on building a productive, efficient and successful organization. How can we get the security problem off our desk and focus on doing the work?”

How to respond:

Security is never quite a “one and done” proposition but Duo does its best to let you focus on the business outcomes you want. We focus on security so you can focus on your business. We play our part by consistently protecting against breaches with a best-in-class access management suite that provides strong multi-layered defenses and innovative capabilities. That means you can be confident you’re letting legitimate users in – and keeping bad actors out.

Further reading:

- [Duo Helps Protect La-Z-Boy from Ransomware, Malware, and Phishing | Duo Security](#)



Section 2

Fast forward to security

“Duo protects against breaches with a leading access management suite that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out.”

What is Cisco Duo?

Covering any user, any application, and any device, Duo is a compelling opportunity for you to protect your customers and build your security practice.

Duo helps protect organizations against breaches through features that help create a cloud-based zero trust security platform. These include multi-factor authentication (MFA), device health check, insight dashboard, Duo single sign-on (SSO), mobile and endpoint security, and user and entity behavior analytics.

How can Duo help my customers?

By making them more secure in more ways than one. Duo's seamless access management solution verifies users' identities with strong multi-factor authentication before granting access to the applications they need. More than just an extra step, Duo verifies user trust, establishes device trust, and provides secure access to apps and networks — from wherever users are logging in.



How does Duo work?

When a user logs in – whether from their home office, the corporate office, or another remote location – Duo automatically uses a zero trust approach to security. That means you can offer customers great peace of mind. Why? Because, before granting access, Duo will:

- **Verify user trust.** Prevent attackers from bypassing MFA using phishing-resistant FIDO2 authenticators or Verified Duo Push. Duo can also help enable organizations to securely log in without a password using Duo Mobile or FIDO2 authenticators.
- **Establish device trust.** Once access is granted, Duo enables the customer's organization to check device security and easily monitor device health and desired security requirements including, for example, checking that the device is password-protected or jailbroken.
- **Enforce granular, adaptive policies.** IT admins can set personalized access levels based on role, device, location, and other relevant factors. That's a big plus for customers who need to onboard contractors easily, quickly change access permission, or react quickly to protect particularly sensitive information.
- **Grant secure access to users.** Customers can continuously verify the identities of users no matter where they choose to log in. Ongoing attack attempts can be detected using the machine-learning capabilities of Duo Trust Monitor. Based on the risk level posed by the user and their device throughout an active session, access can be granted or denied, or additional or stronger verification can automatically be requested.
- **Grant secure access to apps.** Provide users with single sign-on (SSO) for a consistently easy login experience. A user-friendly dashboard provides streamlined access to company apps. Implement the zero trust principle of "least privilege" by ensuring that only the right users with the right devices are accessing the right applications.

Confidently build your security credentials

Discuss these security topics with your customers, open the door to more sales of Cisco Duo, and build your security practice. Today.



Multi-factor Authentication

MFA is a security access management solution that verifies a user's identity at login with two or more verification factors. By providing a layer of protection to a user or company's data, MFA helps to minimize malware, phishing, and ransomware attacks. Prevent attackers from bypassing MFA using phishing-resistant FIDO2 authenticators or Verified Duo Push. With Cisco Duo, MFA is easier than ever to integrate, implement, and use as well as continually improving to counter evolving threats.



Single sign-on

Hundreds of workforce applications. Multiple usernames. Many, many passwords. This is the pain your customers (and their users) feel as they move to cloud-based apps. Single sign-on (SSO) provides an easy and consistent login experience for any application, whether it is on-premises or cloud-based.

Less pain – more productivity.



Passwordless Authentication

Passwordless authentication is the term used to describe a group of identity verification methods that don't rely on passwords. Examples of passwordless authentication include biometrics, security keys, and specialized mobile apps. With strong MFA, SSO, adaptive access policies, and device trust capabilities, Duo can help lay the foundation for a passwordless experience today.



At-a-glance sales play

01 Talk to the right people

Identify the target market

Large numbers of contractors/Bring Your Own Device (BYOD)/remote workers. This is potentially low-hanging fruit: customers may have an urgent need for protection and Duo can deploy in days, not weeks or months.

Organizations that have a complex environment, such as a hybrid mix of cloud, on-premise and custom applications; multiple IdPs or VPNs; a geographically distributed workforce; or even just using macOS.

Want to keep robust security but reduce friction for their end users and decrease helpdesk tickets.

Need a way to ensure all devices that access applications are updated and healthy.

Need more granular policies with least privilege access for admins and applications.

Those who want to minimize MFA-targeting and push phishing risk.

Need stronger access management security like SSO, Passwordless, or checking if a device is managed or unmanaged (Trusted Endpoints) without driving up costs.

02 Unpack the benefits

Show them what a brighter future looks like

1. Phishing-resistant MFA	Help customers counter the current wave of sophisticated cyber threats with phishing-resistant MFA measures that rely on credentials that attackers cannot trick them into sharing. Duo protects through phishing-resistant FIDO2 authenticators or Verified Duo Push.
2. Broader Coverage	Help customers eliminate the gaps in their perimeter like never before, with a solution that offers easy-to-use integrations bringing all applications and operations under one secure roof. Unlike some competitive solutions, Duo offers vendor-agnostic integrations, broad coverage including Radius/VPN/SSH (legacy applications) coverage for varied environments, including complex, hybrid and legacy environments with diverse user groups (e.g., contractors), and supports the broadest range of OS.
3. Protection & Productivity	Give customers the tools they need to protect their environments while empowering the workforce to operate from anywhere and on any device. Users are empowered through several authentication methods and self-service. Admins can create comprehensive, conditional access policies with a few clicks.
4. Speed to Security	Let your customers know that you can protect critical applications quickly and smoothly for them without burning through their IT team or budget. Put enrollment and remediation in the hands of users so the customer's security experts can concentrate on more strategic priorities.
5. Zero Trust	<u>96% of security executives</u> consider security resilience as “highly important.” Data and applications aren’t located behind the network perimeter and a firewall, and users connect directly to company networks with personal devices. In a recent study, organizations with a mature zero trust implementation scored 30% higher in security resiliency than organizations without a zero trust strategy. Seamlessly start on a successful zero trust journey with Duo by securing workforce identities and verifying their devices at every login before granting access to corporate resources. <u>See a 5-phase ZT journey with Duo</u>



03 Open to close

Fast forward the sales conversation with questions that lead to a close

“What applications are you looking to protect, and what devices are your users logging in from?”

“How do you think you would fare against a ransomware or MFA targeting attack like push-phishing?”

“How are you enabling and securing a hybrid, distributed, or third-party work environment?”

“Does your organization have BYOD or non-managed devices that need to access applications?”

“What are some of your authentication requirements for compliance or cyber liability insurance?”

“Can you continuously evaluate risk at the point of login and adjust accordingly?”

“How do you block unknown or unmanaged devices from accessing key applications?”

“To what extent do your teams keep adding on more security tools rather than consolidating?”

“How many different tools or processes do your teams have to rely on to monitor, investigate problems, and take action to resolve them?”

“What is your access policy across the different devices connecting to your environment? How are you assessing risk, providing control, and gaining visibility?”

“What kinds of challenges do you have sharing insights and critical data across teams?”

“How easy do you think it might be to start building towards a zero trust security environment for your teams?”



Section 3

Raise the bar:

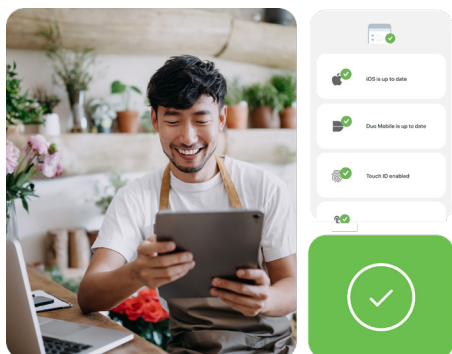
Continuous innovation for customers, continuing opportunities for you.

Cisco Duo is a dynamic cloud-based zero trust security platform, always evolving to counter the changing nature of threats. That's good news for our customers and great news for MSPs like you. The growth of cloud services, mobile, and the consumerization of identity and authentication are megatrends that customers cannot afford to ignore if they want to stay competitive. They bring huge commercial opportunities — and significant security risks.

Let your customers know: the security technologies underpinning Duo can help them maximize their commercial opportunities and minimize their security risks.

Here are some ways we're working to keep Duo two steps ahead of bad actors — as well as offering your customers and their users new ways to stay securely competitive and productive.

When the bad actors raise the stakes, we raise the bar to empower our MSPs and protect our customers.



Multi-Factor Authentication (MFA)

Duo has always made MFA easy to integrate, implement, and use. Because MFA is now such a common solution to protect logins, cybercriminals are targeting it with new and creative ways to gain fraudulent access. There's not one silver bullet that can stop all types of MFA attacks, but we can work together to help customers move towards more advanced forms of authentication that shut down typical MFA attack methods, like Verified Duo Push or FIDO2-compliant security keys. We can also work together to help customers upgrade to Duo's Universal Prompt: our next-generation authentication experience that delivers an easier, more secure, and more accessible authentication experience for every user and opens the way to benefiting from Duo's new solutions.

In addition, amongst many other advantages, Duo's Risk-Based Authentication continuously adapts its understanding of normal user behavior and identifies patterns of behavior consistent with an attack. Required authentication can stay the same or be stepped up in line with the level of risk, but in either case, there is no impact on productivity for an authorized user despite the enhanced level of security for the organization. Adding a further layer of protection, Duo's Trusted Endpoints feature can exclude risky devices by distinguishing between unmanaged endpoints and managed endpoints that access your browser-based applications.

Supported Authenticators



Duo Push



SMS Passcodes



Phone Callback



Security Keys



Mobile Passcode



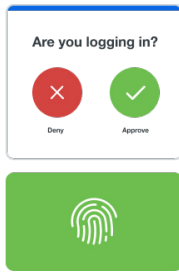
WebAuthn



Passwordless



Verified Duo Push



Put simply, there are more sales out there for you when you champion Duo SSO.

Duo Single Sign-On (SSO)

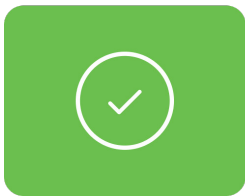
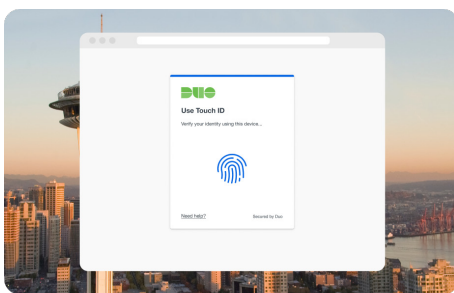
Duo SSO, included in each Duo edition, lets users access any application with a single login experience, protected by Duo's strong authentication and granular access policies and without the need to remember or enter multiple login credentials. Applications can be accessed in one location via Duo Central – cutting down the risk of accidentally going to the wrong site.

A rapidly growing number of customers adopt Duo SSO because it enables seamless, secure access to the broadest range of cloud and on-premises apps. This includes those built on SAML 2.0 and OpenID Connect (OIDC) standards that offer organizations of all sizes the right levels of improved user experience, increased productivity, and enhanced security for their needs.

Customers quickly realize the value of SSO for productivity as well as security, making it a remarkably 'sticky' solution for our MSPs to sell. Duo SSO not only dramatically reduces reliance on passwords, but also lays the foundation to begin adopting passwordless authentication methods.

Further reading:

- [Five Key Factors for Simpler, More Secure SSO](#)
- [Duo MSP Brandfolder \(PDF + Workshop\)](#)
- [The Value of Single Sign On | Duo MSP Brandfolder \(PPT\)](#)
- [Why MFA Demands Single Sign-On | Duo Security \(Ebook\)](#)



Duo Passwordless means you can offer security, convenience, and productivity to more customers than ever before.

Passwordless

20-50% of all IT help desk tickets each year are for password resets. Each year, U.S.-based enterprises allocate over \$1 million to password-related support costs. Duo supports password-free open standards, such as WebAuthn, as MFA methods for SAML applications. This functionality lets organizations establish a passwordless login workflow for cloud apps, without ripping and replacing existing infrastructures, reducing the risk surface and administrative burden associated with passwords while improving the user experience. Duo Passwordless makes it simple as it works with existing identity provider (IdP) or SSO solutions. Moreover, Duo makes it easy to roll out passwordless to subsets of users first, to make sure users and the helpdesk are comfortable with the transition before expanding to the full workforce. IT admins have peace of mind that users no longer have to remember or type long, complex passwords. Instead, they can log in securely with a single gesture that provides the security of two authentication factors.

In terms of the potential for scalability, Cisco IT has enabled Passwordless in its global policy and made it available to 150K users at Cisco. A lot of customers are showing interest in passwordless, recognizing its value in security, user productivity and reducing help desk costs.

Are those benefits your customers might buy into?

Further reading:

- [Passwordless: The Future of Authentication | Duo Security \(Ebook\)](#)
- [The Value of Passwordless with Duo MSP Business Development | Duo MSP Brandfolder \(PPT\)](#)



Device Trust & Trusted Endpoints

Previously available in only the highest edition, Duo Trusted Endpoints is now accessible for all paying tiers of Duo. Duo enables you to define trust for the endpoints accessing Duo-protected resources on your network, whether they're company-issued and registered or unmanaged and unregistered personal devices, and allow or block access based on policy—without having to install any endpoint agents or mobile device management tools (MDM).

Identify risky devices, enforce contextual access policies, and report on device health using an agentless approach or by integrating with your device management tools.

- Get granular insights with device visibility and maintain an inventory of access devices to gain a deeper understanding of your security environment.
- Assess Device Health posture in real time to check for corporate device policies like OS version, disk encryption, and management status. Non-compliant devices are blocked at authentication, and self-remediation keeps the helpdesk tickets at bay.
- With device and user access policies, full-time employees, short-term contractors, and vendors alike can all get up and running with Duo quickly and easily—each with customizable access controls for role-specific permissions.

Further reading:

- [Duo for Device Trust | Duo MSP Brandfolder \(PDF\)](#)
- [Healthy Device? Check with Duo Desktop Before Granting Access | Duo Blog](#)
- [Duo Trusted Endpoints At-A-Glance | Duo Security \(PDF\)](#)
- [Trusted Endpoints Unleashed – Deliver Added Value | Duo MSP Brandfolder \(PPT + Webinar\)](#)

Section 4

Fast forward together

What Customers and MSPs like you think about Cisco Duo.

Cisco Duo is a dynamic cloud-based zero trust security platform, always evolving to counter the changing nature of threats. That's good news for our customers and great news for MSPs like you. The growth of cloud services, mobile, and the consumerization of identity and authentication are megatrends that customers cannot afford to ignore if they want to stay competitive. They bring huge commercial opportunities – and significant security risks.

Room&Board

Room & Board

Room & Board is a modern furniture and home décor retailer with over 20 stores across the United States. To secure their complex and distributed workforce, they deployed Duo.

“We’re a multi-platform environment. We’ve got Windows PCs. We’ve got iPads. We’ve got some Androids living out there. Staff even needed access via their own personal devices. So, we have a very mixed environment. How do you square that circle?”

“Historically at Room & Board, application rollouts have been a lengthy process with lots of training. The Duo rollout took maybe four weeks from start to finish. All the training and onboarding material was right there. We just downloaded it, added our banner, and sent it to our users. We had roughly one thousand employees onboarded, registered, and using the product in less than 30 days. It was one of our fastest rollouts.”

“One of the reasons we continue to invest and further our implementation with Duo is because it isn’t just an MFA tool. The risk-based challenges are something we enabled very early on to get ahead of the MFA fatigue attacks that we were seeing.”

[Find out the whole story](#)



CommSec

This Dublin-based managed service provider uses Duo to protect workers and data through a zero trust security approach. For customers working with CommSec, a key concern is knowing where to begin. CommSec offers a wide range of services including threat hunting, digital forensics, vulnerability management, anti-virus, endpoint protection, email protection, and more. Typically, the customer journey begins with a security audit in order to find potential gaps or vulnerabilities. That's where Duo comes in.

"Duo was the first vendor that put the zero trust model into practice with multi-factor authentication. It not only looks after MFA, it sees who the user is, what device they're using, and establishes whether it's a trusted device. Duo ties it all together in one product, especially for MSPs, and it makes it easy to manage customers of different sizes."

"The support given by Duo is above par. They're quick to get back, very helpful, and detail-oriented."

[Find out the whole story](#)



Arraya Solutions

Duo's MSP offering helps Arraya reduce their TCO and help desk ticket volume while providing a subscription model that scales with their clients' growth.

"I was blown away with the simplicity of Duo's MSP program. They removed all the upfront expenses and commitments that prohibit newer MSPs from partnering with a vendor. Duo's product is so easy to use that it didn't require a large engineering investment to get up to speed."

"Duo's simplistic, straightforward approach makes them very easy to partner with. They removed all the unnecessary barriers and made it easy for us to help protect our clients."

[Find out the whole story](#)



Member Driven Technologies

Member Driven Technologies (MDT) provides credit unions with a secure, private cloud alternative for core banking and IT needs. Their need: to secure SSL VPN remote access by devaluing credentials, so if an intruder compromised credentials, it could not be exploited.

“We chose Duo over the other two-factor competitors because of the simplification, the ease of use, the multi-tenancy, and the scope and coverage of applications covered under two-factor.”

“The proof of concept was a home run. It was incredibly simple to onboard users, it was effortless to protect our applications, and being a cloud service, we were able to accelerate the adoption and integration immediately,”

[Find out the whole story](#)



MNX Solutions

The team at MNX Solutions manages the critical systems and applications for companies within all types of industries, ranging from online commerce to financial services. Not only do they have to maintain hundreds of systems for different customers, but they also must help secure those customers from potential threats. MNX settled on Duo Security for the ease of integration and affordable cost. It's a choice that's stood the test of time.

After over four years as a Duo customer, MNX Solutions is still deploying Duo Security whenever possible and continues to appreciate the easy integrations and flexible two-factor methods that Duo provides, especially Duo Push. Through consistent usage of Duo Security, MNX Solutions has yet to see a single account get compromised on a Duo-secured server.

[Find out the whole story](#)

[Read all Duo Customer Studies Here](#)



What Cisco Duo thinks about MSPs like you

“The MSP team at Duo never loses sight of just how important managed services providers are to our overall business. They are strategic allies, and their contribution is immensely valued. We are continually looking for improved opportunities to move forward together for mutual benefit.”

Esther Kho, Strategy & Planning Manager
Cisco Duo



Section 5

More value for MSPs – with as little administrative overhead as possible.

A better MSP program

that ticks more boxes.

Cisco Duo’s modern approach to security deserves a modern program approach for our managed service providers (MSPs). That’s why we’ve designed a program that makes Duo Security deployments easy to buy, easy to manage, and easy to grow so that your business can enjoy better support, better sales, and – most importantly – a brighter future in partnership with Duo.

The top 6 ways Cisco Duo and our MSPs work better together.

What we offer	How you benefit
 1. No minimums or commitments	Enjoy the freedom and agility to move fast and start building your security practice with Duo.
 2. No certifications or costs to enroll	Keep more of the money you earn. We’re here to do business together, not add to your overheads unnecessarily.
 3. Flexible billing	Take the opportunity to pay month to month, and only for what you use. We respect your cash flow!
 4. Unified view and management of all customers	Improve your productivity and save time and resources managing your Duo customers.
 5. End-to-end business support	Improve your productivity and save time and resources managing your Duo customers.
 6. Deploy without quotes, order or renewals	Free up your time and move to serve your customers more quickly with no need for cumbersome admin.

Fast forward to a brighter future today.
Become a Partner | Duo Security