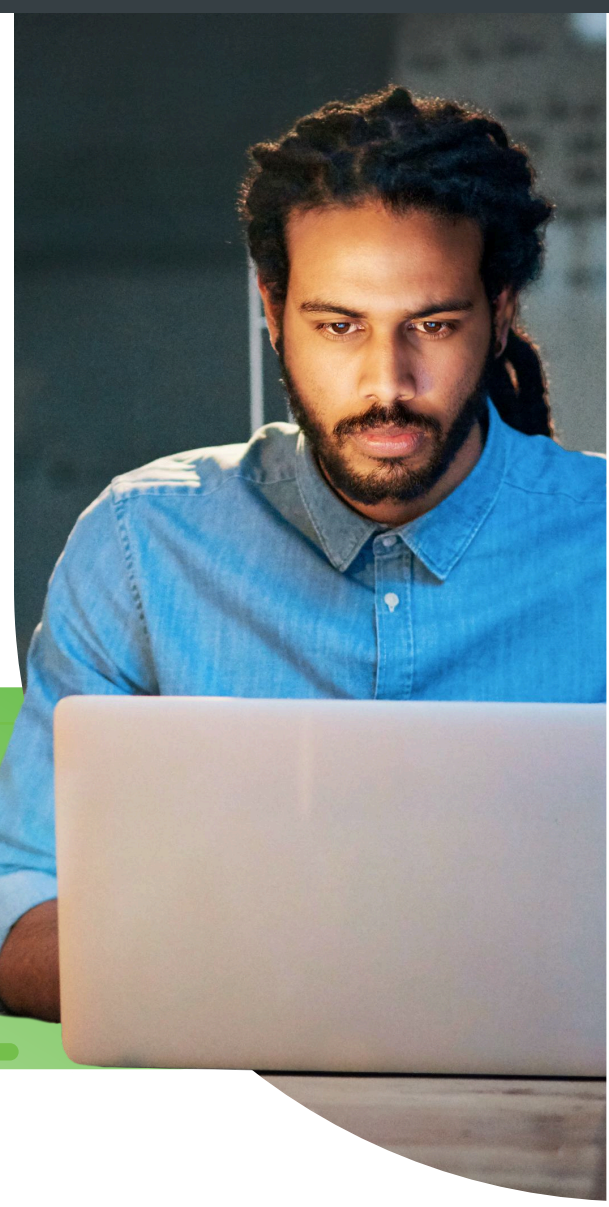
CISCO DUO

The Ultimate Guide to MSP Operations

The only guide you need to anticipate and meet your clients' identity security needs.

Table of Contents



SECTION ONE

A Need For Speed

The Managed Services Provider (MSP) model demands efficiency. Dedicated to customers' IT and security needs, MSPs are tasked with providing strong, scalable solutions across their clientele. However, time and resource constraints inevitably prevent MSPs from operating as separate outsourced IT departments for each customer. A completely bespoke experience poses a challenge for sustainability and scalability.

When striving for operational efficiency, streamlining is key: ensuring that processes and technologies work together to achieve most clients' security goals in a time and resource-effective manner.

This is especially important in a field when things change frequently – new attack methods are identified, customers need new technology to support their work, and increasing compliance requirements demand improvements to identity security. How can MSPs get ahead of the curve when it comes to client needs?

3 Considerations for MSP Efficiency

What MSPs need to know to stay on top of common client concerns.

Strong security.

We live in an active attack landscape. Clients place their trust in MSPs to minimize security risks and expect comprehensive protections that rise to meet changing working norms like remote and hybrid work. This requires MSPs to stay on top of new compliance requirements and novel attack methods and assess the solutions that crop up to address them.

Flexible solutions.

Rarely, if ever, does a business approach an MSP with no existing IT infrastructure. When they do, they will bring with them the technologies they have used until now – plus the workarounds and kludges they have used to keep everything running. No two customers are the same, requiring MSPs to stay flexible, find integrations, and take any existing IT environment in stride.

Straightforward management.

Maintaining security solutions efficiently is top-of-mind for MSPs who want to scale and grow. Easy methods of reporting outcomes can help in directly articulating the value of security solutions.

Inefficiencies are expensive, and their impact can be hidden by overall success. Even if an MSP is profitable, a lack of operational efficiencies can cost time and money that could be spent on growing the business. Free resources could be spent acquiring new skills, evaluating new services and tools – or even simply creating the room to take on new customers.

SECTION TWO

Keeping Tabs on the Security Landscape

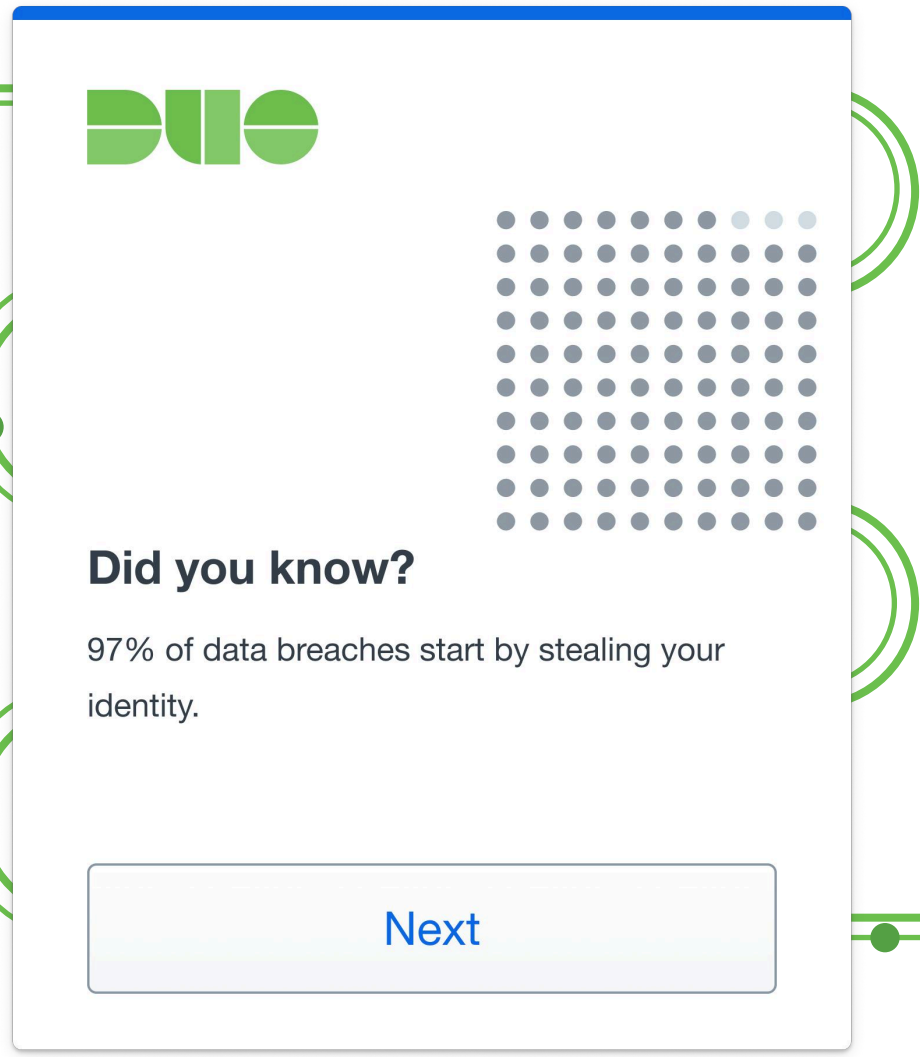
Keeping up with rapid growth is challenging. Over the last few years, the move to hybrid working and security concerns have seen many MSPs grow rapidly and take on new business. Prioritizing the needs of multiple clients can sometimes introduce risk through fragmented processes and other inefficiencies. To add complexity, the attack landscape of today is constantly in flux.

According to the **IDS Alliance**, identity-related security attacks are endemic. Only one in 10 businesses could claim no identity-related incidents in the last year.

Every other business suffered some kind of attack, including phishing, credential stuffing, and socially engineered password attacks. Businesses are in dire need of help and are looking to their suppliers for better protection.

Luckily, it's clear some protective measures are becoming more common. MFA is the best defense against identity-based breaches, preventing over 99% of account compromise attacks. However, it's not a "set-it-and-forget-it" solution. Identity-based attacks are frequently evolving.

Duo provides must-have protection against identity attacks with advanced tools to protect against evolving threats, including single sign-on, risk-based authentication and device health checks. Easily manage accounts with adaptive access policies, and machine-learning driven threat detection. These and other features make Duo an essential part of a layered security strategy, designed to protect your clients against sophisticated attacks.



SECTION TWO

Straightforward Insurance & Compliance Conversations

Oftentimes, clients come to MSPs with clear needs: cyber insurance qualifications, industry standards, or federal mandates. Understanding common drivers and how to address them, coupled with technology providers who stay on top of changing requirements, leads to simpler conversations with customers. **Common security compliance drivers include:**

- **PCI DSS**
  Security standards for anyone processing payment card details, including merchants that outsource this processing. From as early as February 2018, PCI DSS rules demand two-factor authentication for all remote access into the cardholder environment.

- **HIPAA and EPCS**
  To protect sensitive health information, account security through the likes of MFA is recommended to maintain compliance. The Electronic Prescription for Controlled Substances rules (EPCS), the system used to transmit prescription of controlled substances directly to pharmacies, includes 2FA requirements that must be met.

- **New CJIS MFA requirements**
  Recent Criminal Justice Information Systems (CJIS) MFA requirements state that agencies that store and access CJIS must implement MFA to ensure their data is protected from bad actors. The deadline for this requirement was October 1st, 2024.

- **GDPR, IRAP, C5, ISMAP**
  Holding and transmitting data across borders requires meeting the data protection standards of every country involved. Meeting these requirements often means complying with the strictest rules to ensure compliance everywhere. GDPR, for example, does not mandate MFA but it is recommended for consideration by the UK's Information Commissioner.

- **Industry vendor MFA mandates**.
  The **2024 Microsoft Azure MFA mandate** and Google MFA mandate are a growing factor in adopting strong identity security. After a long time of strongly recommending MFA, both Microsoft and Google are making it mandatory for all users of their cloud products. Organizations without MFA will need to find a solution that can be rolled out quickly with minimal disruption and cover a wide range of applications.

Meeting all these compliance requirements can be a headache. A big part of reducing this pain is looking for efficiency – where can you find solutions that make it simple to meet the widest range of requirements possible? The key is working with a partner that puts security first, one that will maintain and evolve its product so that you know compliance today means compliance tomorrow. The best partners will not only adapt their products to address evolving attack vectors and modern security research, but they will also keep you in the loop as to the latest requirements and changing regulations – and how they are helping you meet them for your clients.

Duo stays at the leading edge of industry standards to ensure we meet all your – and your clients – requirements for a compliant, effective security product. We focus on compliance so you can skip right to the work that matters to you, worry-free. For more details, visit our **Industry and International Compliance** page.

Long-term partnerships with solution providers are another strategy for operational efficiency. When it comes to MFA, that means choosing a provider that keeps customers safe in the face of new threats and compliant even with changing regulations. However, it also needs to be a flexible solution to meet uniquely different customer needs.

SECTION THREE

Protecting All Customer Environments

No two customers are the same. Businesses use different applications, different endpoints, and all have different requirements. From unique OS combinations and BYOD considerations to legacy applications and messy identity storages, finding one-size-fits-all solutions can be tricky.

The ideal situation is to be proactive, either by having solutions “ready-to-go” in response to customer requests, or even better, preempting those requests with solutions that solve customer problems before they even arise and position your MSP as a security advisor.

There are two key considerations for efficiently protecting diverse customer environments:

1. Finding vendor-agnostic security options
2. Predicting and deploying common integrations

SECTION THREE

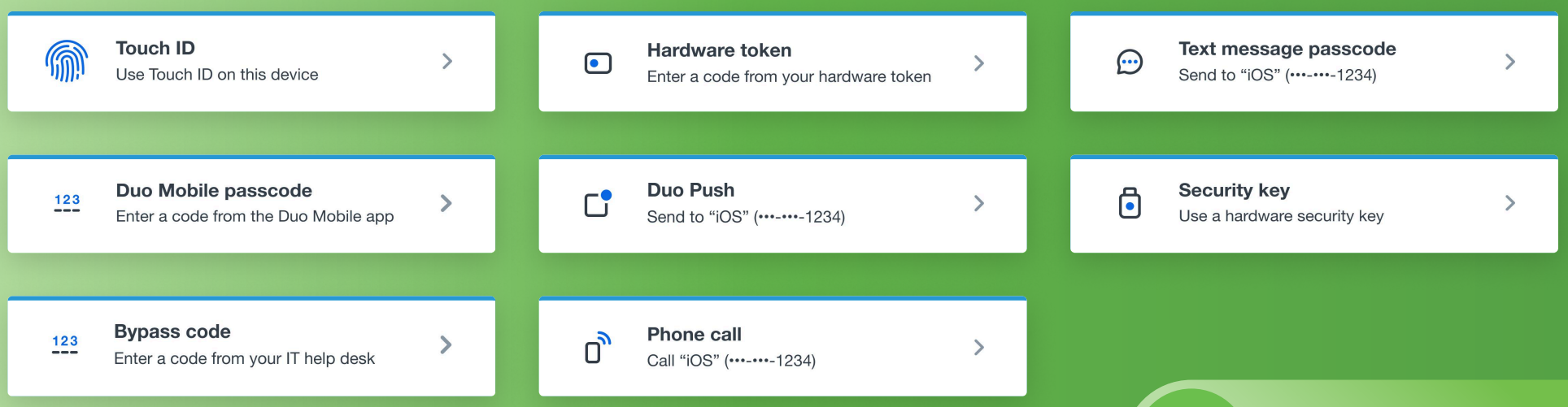
Providing Vendor-Agnostic Options

Tech-debt is a reality. So is the fact that client businesses are often at varying stages in their security journey. They may be reluctant to rip-and-replace what has worked to date with something unfamiliar. MSPs must be able to offer security options that are both flexible for their customers without adding too much additional overhead to their own management costs.

Security solutions provided by an MSP need to work with everything, no matter the vendor, the operating system, or whether they are managed by the MSP or not. Security needs to be a layer of protection on top of what already exists, rather than demanding a customer change their preferred setup to meet new requirements.

Duo's diverse set of authenticators means users can choose a solution that works for them, whether that's an authenticator app, biometrics, physical security tokens, or even passwordless when your clients are ready. See all the options.

Poor authentication methods lead to help desk tickets ("I can't log in!"), a universal solution means less time spent supporting multiple applications, while a simplified, consolidated environment allows MSPs to invest their time and effort elsewhere – moving closer to the ultra-efficient ideal.



SECTION THREE

Providing Common Integrations

Technologies need to work well together to be effective. Without this, customers can be frustrated, or MSPs required to create a makeshift solution. While every business will have its own software needs, there are some applications that are nearly ubiquitous. This is an opportunity for MSPs. They can make onboarding for their customers easy rather than a hassle, provide the best MFA solution that integrates with Microsoft Azure and many other applications, and use a solution that will streamline their operations.

Duo + Microsoft Better Together

One of the first questions a client will likely ask of any new piece of software is: will it work with Microsoft? And if it does, will it integrate easily?

Duo, through its partnership with Microsoft, is now a secure third-party **External Authentication Method (EAM)** integration for Entra ID – an improvement on previous Microsoft Custom Controls. Duo is a fully integrated MFA and advanced identity security provider within Entra ID, meaning frictionless integration of its full security feature set, making simple to set up SSO, deploy passwordless, or create and manage granular access policies and ensure that only trusted users and devices are given access to Microsoft applications.

It also integrates with many other Microsoft solutions, including Windows Logon and RDP, Microsoft 365, and Azure Directory Federation Services. It protects many popular services including email (on-premises and cloud-based), Windows servers, remote desktops, and more.

Pre-built integrations and clear documentation make it simple for MSPs to deploy – vital for easy onboarding. Integration with Microsoft Entra ID and Active Directory Federation Services (ADFS) automatically secure logins to any web-based application that is connected to ADFS, securing multiple applications at the same time.

Bonus: for MSPs, this means a more seamless Partner Center authentication experience as well. For more information on Duo's partnership with Microsoft, visit **duo.com** or get the **Duo Microsoft Partnership Solution Brief.**

SECTION FOUR

Make Maintenance & Reporting Simple

Good administrative experience is key. Ease of use is often – rightly – touted as a must for end-users of security solutions. Not enough is said about the user experience of those administering these solutions. Ensuring a solution is simple and intuitive not only makes the life of the MSP easier, but it can also have a tangible impact: a lower administrative burden can mean lower cost. An MSP's biggest outgoing is likely to be its employees' time, after all, so reducing the time spent on admin tasks and solving problems means that time can go elsewhere.

It can also make it easier for MSPs to show how valuable their work and provided solutions are. If it's simple to produce a report showing threats kept at bay, failed login attempts from attackers, or how many users needed help with their credentials, it's far easier to prove the value of a provided solution.

Ways to improve efficiency from a maintenance perspective:

Simplify onboarding

Self-enrollment and automatic provisioning can help make the deployment process smooth and efficient.

Enrolling Users in Duo

Reduce help desk phone calls for end-user device issues

Allowing users to securely manage new devices on their own cuts down on help desk requests.

Duo Self-Service Portal

Secure incoming client calls easily

A simple way for a help desk to make sure they are speaking to the right person can minimize security risk and ease the frustration of callbacks.

Duo Helpdesk Verification

Empower users to keep their devices up to date

Users are accustomed to applying updates on their personal devices, so why not make it easy to ensure work devices are updated too?

Duo Device Remediation

The problem with efficiency is that MSPs need to be able to justify the investment made in their services: making it look easy means you have to prove to the customer that the money has been well spent. This can be done by reporting on the effectiveness of a security solution, through proof points such as the number of "push-spray" attacks mitigated, the reduced number of out-of-date devices, and suspicious locations where MFA attempts have been blocked. These are important not just for auditing purposes, they can also give customers a tangible sense of where their investment is going.

Prove Value with Duo

Duo reports in a number of ways – deployment progress, admin actions, and policy impact – as well as providing detailed logs and real-time alerts. These not only help ensure a customer is secure, they also help the customer understand just what you, and Duo, are doing to keep them safe. See all the ways you can prove the value of Duo in the Duo Admin Panel.

SECTION FIVE

Why Duo MSP

MSPs service a wide range of customers, with different needs. Their customers may differ by size, vertical, location, culture, age, IT maturity... and that makes flexibility important. While MSPs may strive to unify their solutions and be as efficient as possible, each customer may need a slightly different approach to ensure success. Their vendor partners need to understand these needs that sometimes work in opposition: flexibility and efficiency.

Duo is an advanced identity security solution with a program built for MSPs to move fast.

Duo helps meet your customer compliance needs with comprehensive support, and not only provides a simple user experience, but also a simple and powerful admin experience too.

Now more than ever, Duo's security-first MSP program helps you eliminate complexity and grow your business with industry-leading secure, scalable, and flexible access management including risk-based MFA, SSO, device trust, and easy-to-set policy engine. Focus on what matters to clients and experience how Duo makes identity security easy and efficient.

Partnering with Duo means MSPs can:

- **Scale your business** with pay-as-you-go pricing with no complex pricing tiers or minimums
- **Manage all customers in one console** with delegated access, now improved with dedicated role-based access controls for MSPs
- **Succeed with technical and marketing support** from our team and access to an extensive documentation library and 50 NFR license

CISCO DUO

Visit **Duo's MSP Program** page or reach out to **msp@cisco.com** to start your Duo MSP partnership today.