CISCO DUO

The Smarter Security Toolkit for MSPs

Best practices for daily security challenges

Table of Contents

Introduction

The Managed Service Provider (MSP) sector has seen incredible growth over the last decade, and predictions for the future are buoyant.

Canalys estimates a 12% growth in managed services revenue in the channel in 2024.

By 2028, the managed services market size is expected to **grow from USD 275.5 billion** in 2023 to USD 372.6 billion according to Markets and Markets.

What these numbers don't reveal is the increasing pressure on MSPs to serve their growing portfolio of customers and the new services they demand.

MSPs must serve general IT needs in an increasingly complex environment – varied hardware, new applications, hybrid office working, and more. The problem of security has become so acute, with new threats and new vulnerabilities seemingly uncovered every day, that many MSPs have become security as well as IT advisors. Some have specialized as Managed Security Service Providers (MSSPs), focusing on protecting clients with a strong security expertise.

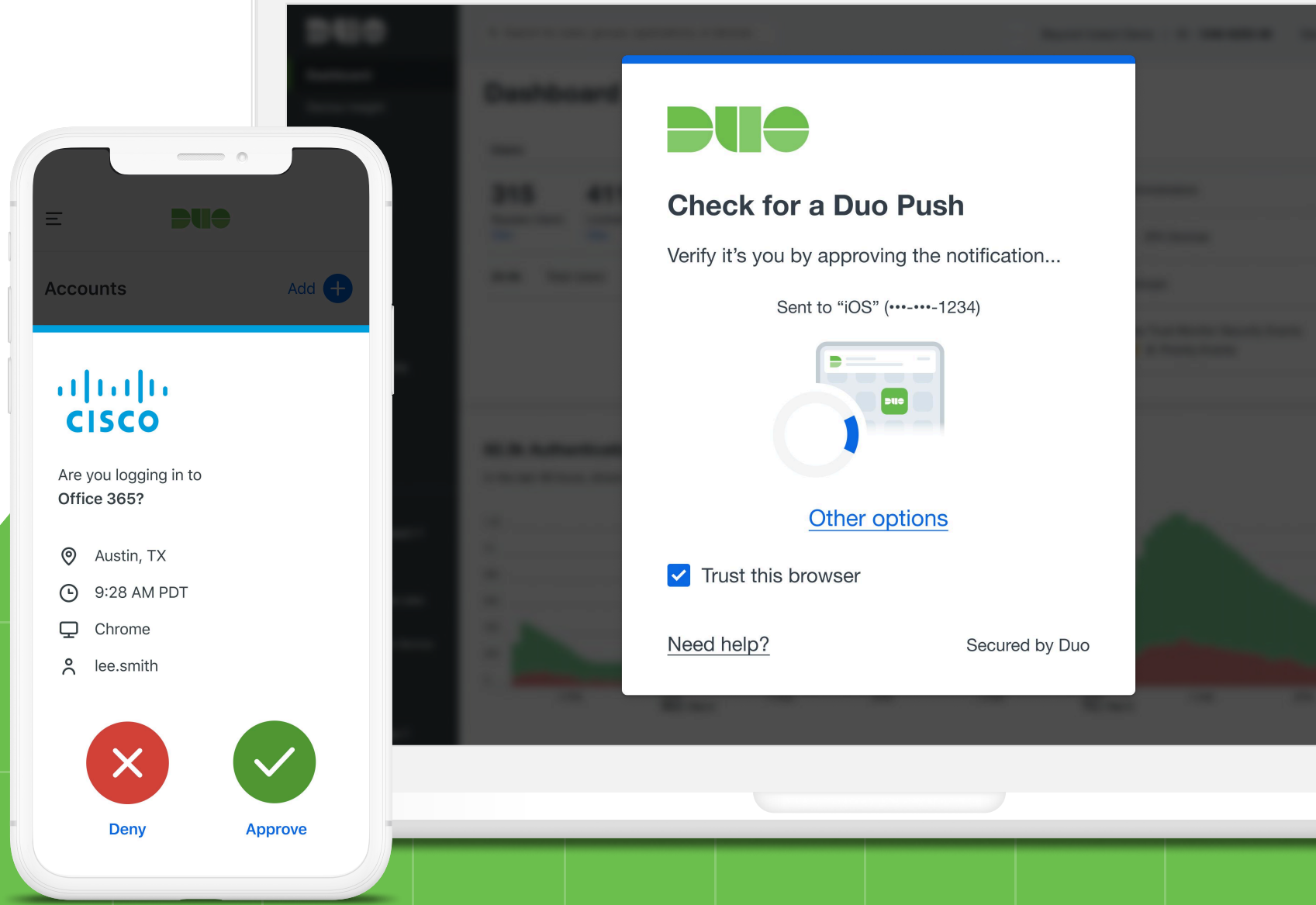
In this environment, it makes sense to be as strategic as possible: to scale, to be more efficient, and in the process provide customers with a better service. But this is tough when everyday tasks are all- consuming. Updating software, setting up product integrations, identifying and creating roles for the right access controls, compliance reporting, and of course responding to helpdesk tickets securely can eat up any time when a team could be working on strategic projects instead.

Think “Quality of Life”

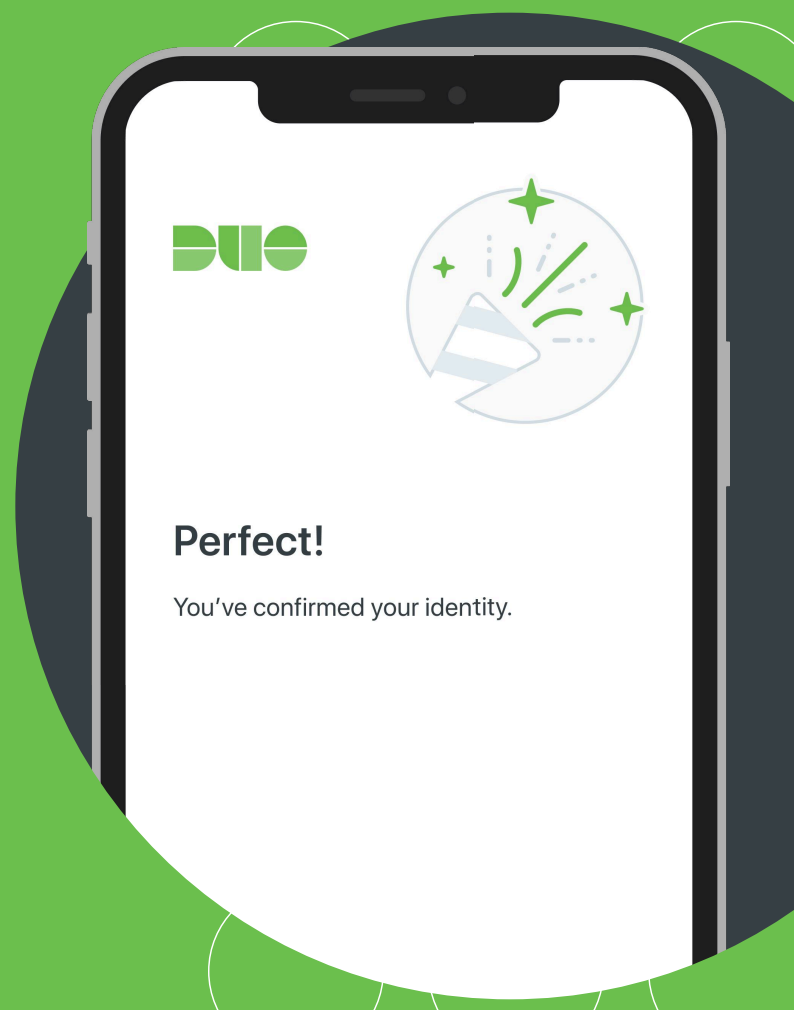
Just because something has always been done a certain way, it doesn’t always mean it’s the best way. We can look around our homes and find technologies that offered a huge quality of life advantage when they were adopted en-masse. A dishwasher, a washing machine, even a TV remote control can make us think: I can’t believe we used to do that another way. Assessing current challenges can help MSPs find novel solutions to common challenges whether that be securing help desk calls, keeping logs for compliance or finding documentation quickly.

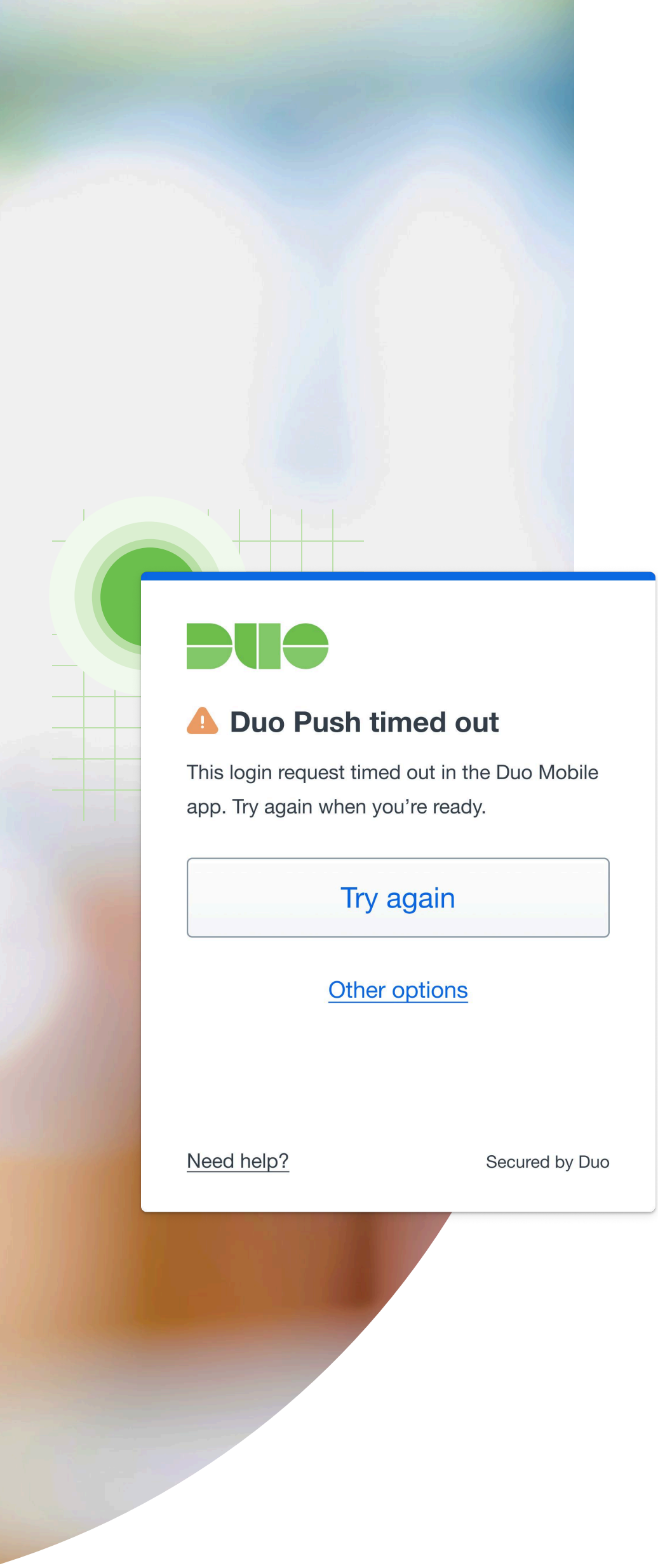
Modern quality-of-life features can help MSPs to offer faster, simpler, and easier solutions, not just for the benefit of clients, but also to free up internal resources and become more strategic. When considering new services and software, think beyond the client feature set.

A strong MSP vendor partnership will also answer: **how do we ensure these solutions minimize the impact on already stretched MSP teams and improve their quality of life?**



Security Challenges & Quality of Life Improvements





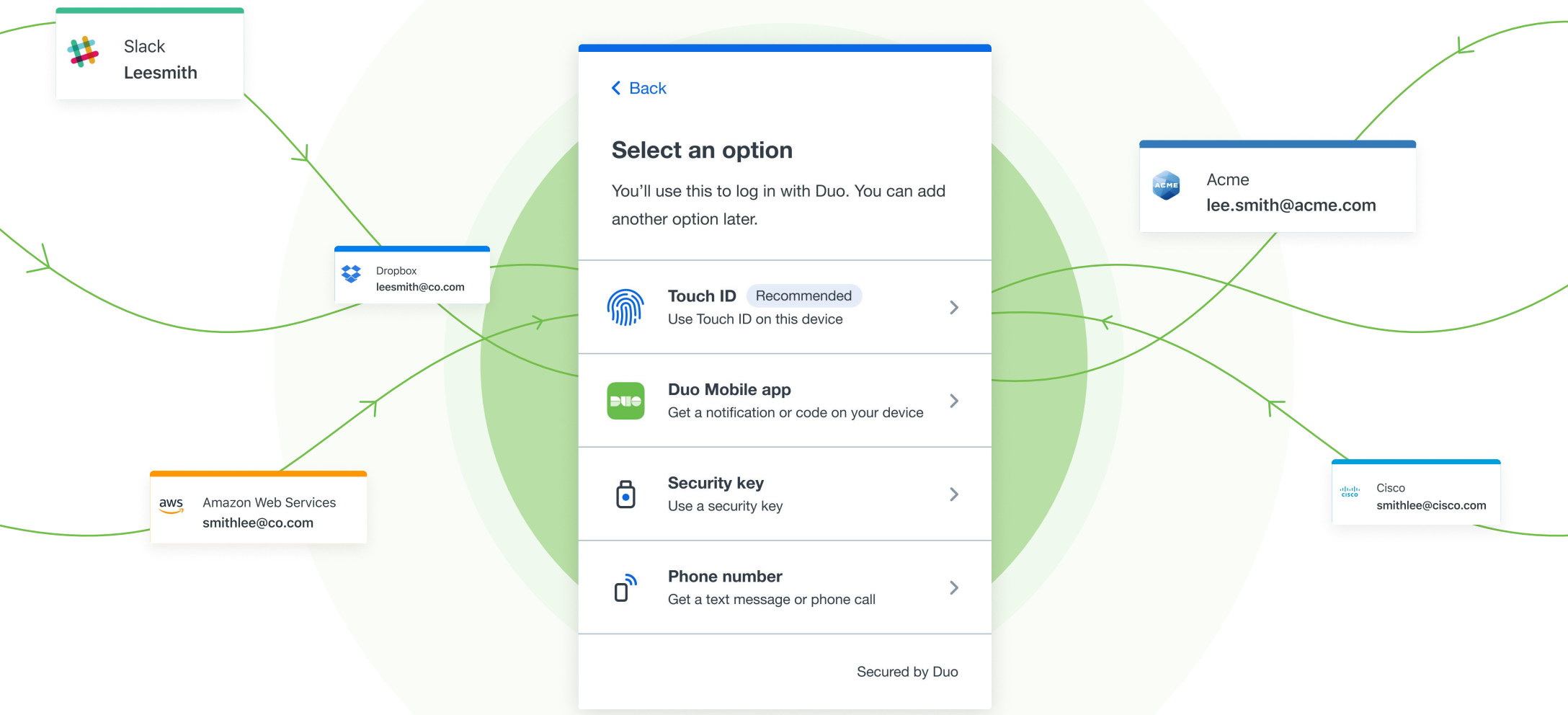
SOFTWARE UPDATES:

Ensuring Good Device Hygiene

In 2024, Duo research revealed that **the percentage of denied authentications due to out-of-date devices increased by 74.7%** – tracking for operating system updates, browsers patches, and installed plug-ins like Java and Flash. Not only do regular updates fix critical bugs, but they also increase functionality, improve monitoring, and lower security vulnerabilities. The more operating systems (OS) and devices an organization allows to authenticate, the more likely it is those authentications will occur with an out-of-date OS.

Keeping track of this can be time consuming for MSP administrators and deploying updates without risking business continuity can be challenging. But general device health and hygiene practices must be prioritized. Organizations – particularly those which are expanding their IT environments – are increasingly expecting stricter controls, aiming to reduce risks posed by out-of-date software. Mobile device managers (MDMs) require heavy resources to set up and can be seen as intrusive if installed on personal devices.

A tool that works quietly in the background but doesn't "take over" a device will be far more welcome. Duo Desktop and Duo Mobile, can assess the security posture of devices attempting to access corporate resources, reducing the risks of outdated software, and ensuring critical security patches are up to date.



These tools can also trigger a push for the customer to update their own systems according to IT requirements without having to go through the helpdesk. If a customer's users can perform this by themselves, it removes the burden from the MSP and can help the end user feel more in control by the guided self-remediation it offers. The process runs alongside regular preemptive actions like warnings about time-sensitive software updates that will lock a user out of a system if not actioned.

Duo can also provide actionable insights across an organization's entire device landscape, allowing a team to perform more targeted remediation if needed.

PRODUCT INTEGRATIONS:

Compatibility with Existing Tools

One widely recognized problem is ‘tool sprawl’, which occurs when businesses have a variety of different tools to address different use cases. This proliferation of tools is not surprising – with more than 4,500 security vendors in the market, many specializing in particular threats, it can be tricky for organizations to choose a centralized solution. With this array of security solutions, it’s important for an MSP to be able to integrate with multiple platforms to reduce overhead and operational costs.

Duo, for example, integrates with hundreds of leading industry vendors, providing deep integrations and pre-configured SSO (single sign-on) options that take the uncertainty around various customer tools out of the equation. It integrates with **Windows Logon and RDP** as well as Microsoft’s suite of productivity and security solutions, on-premise or cloud, with **product compatibility** that enables trust and provides secure access. Other integrations include **Google** across Google Cloud, Workspace, Chrome, and ChromeOS alongside AWS to ensure cloud-first security, and common industry-specific providers like Epic Systems.

On the day-to-day business side, **Duo’s Admin API** enables workflows with other MSP solution providers like Professional Services Automation (PSA) and Remote Monitoring and Management (RMM) tools that combine to scale business and reduce overhead.

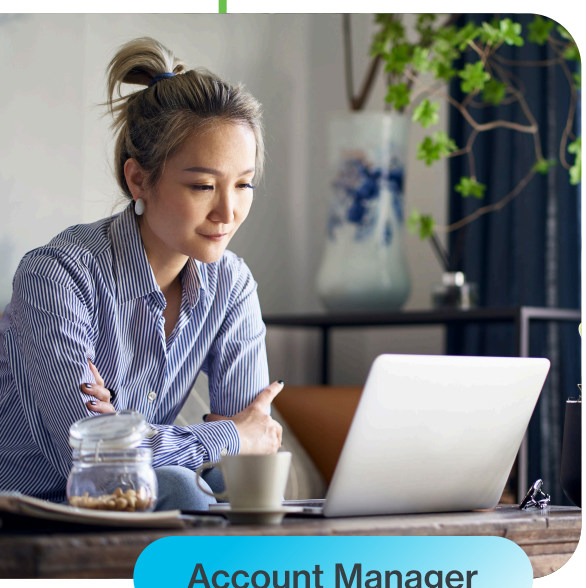
ACCESS CONTROLS:

Building for Secure MSP Administration

A more personalized view to access control is key to letting the right user in while keeping bad actors out. But managing these admin permissions within a multi-tenant structure can be complex and often that complexity is at the expense of administrator's ease of use. This can prove detrimental to both productivity and security.

Different employees require different levels of access. Over-permissioning or credential sharing can be insecure and challenging to maintain. Specific MSP-centric management controls like role-based access controls, especially at a sub-account level, can reduce the security risks of blanket permissions with the technology acting as a key for distinct admin roles.

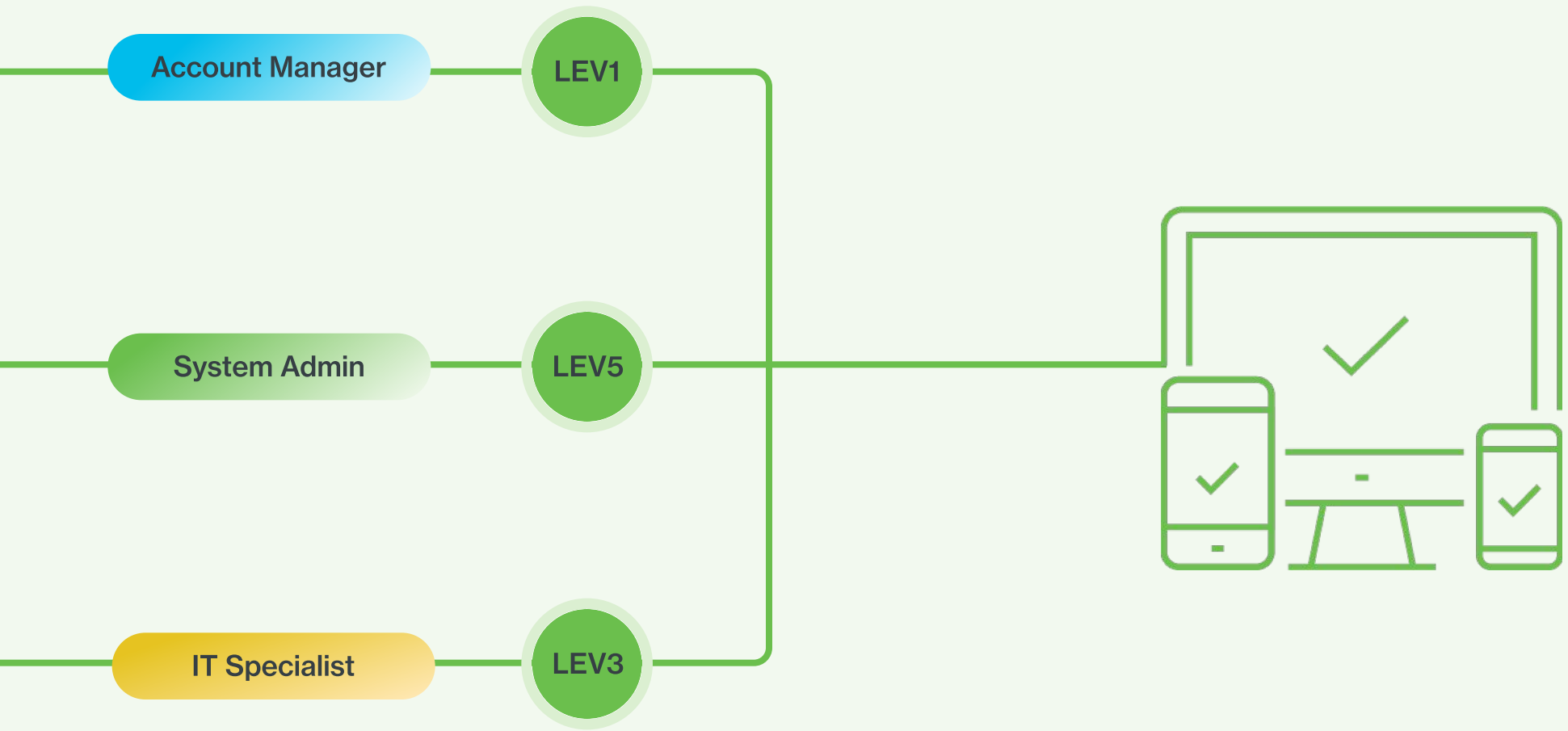
Taking a limited approach to access control is a key aspect of zero trust security, a strategy that keeps the most confidential files protected from social engineering attacks simply by ensuring they can only be accessed by employees who truly need access.



Account Manager

System Admin

IT Specialist

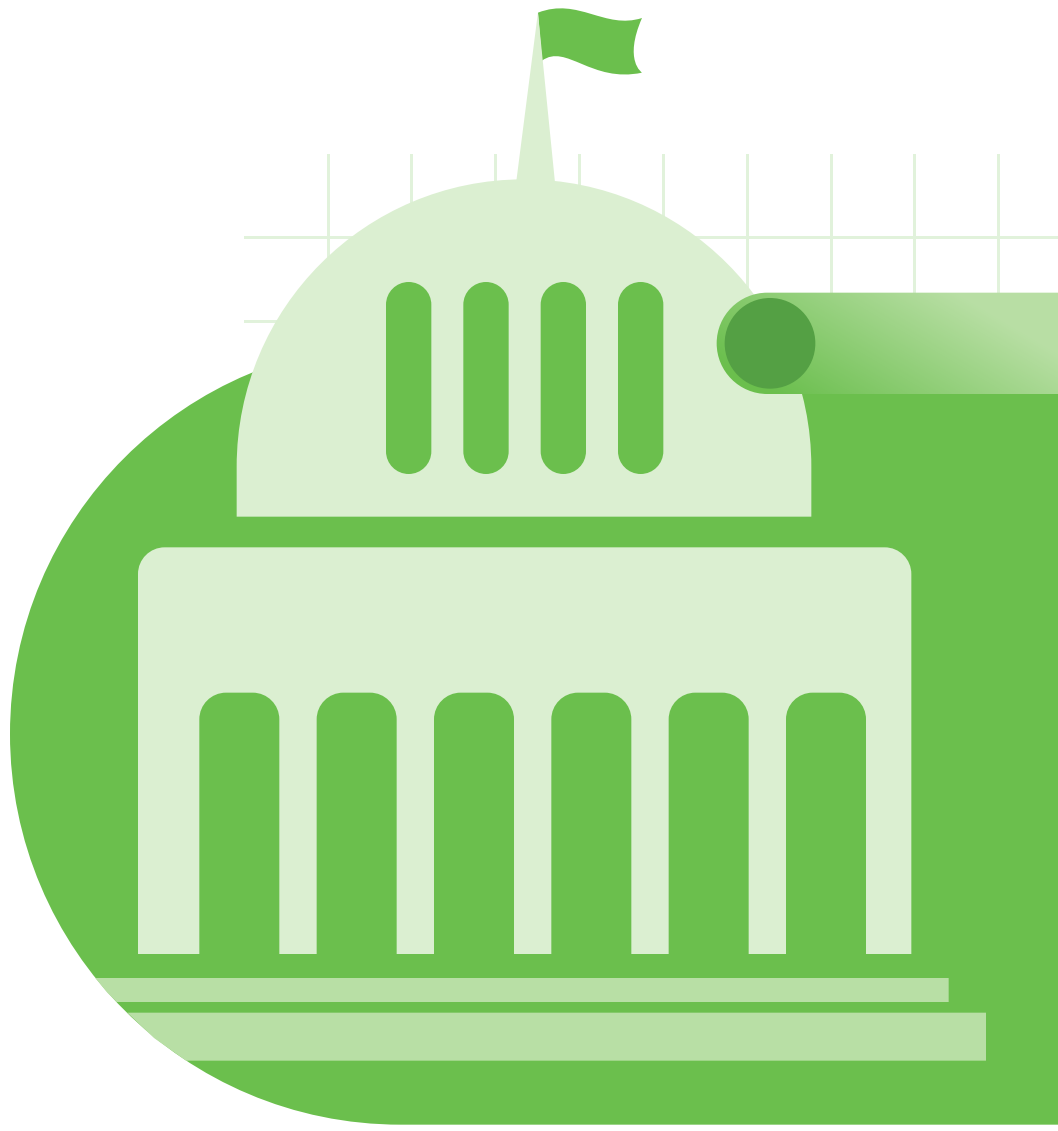


By implementing the principle of least privilege access, you are limiting the access strictly necessary for the role. For example, a helpdesk administrator should be able to view and edit security logs but not confidential HR files. Giving these permissions restricts lateral movement within the system following a security incident or other unauthorized access to sensitive information.

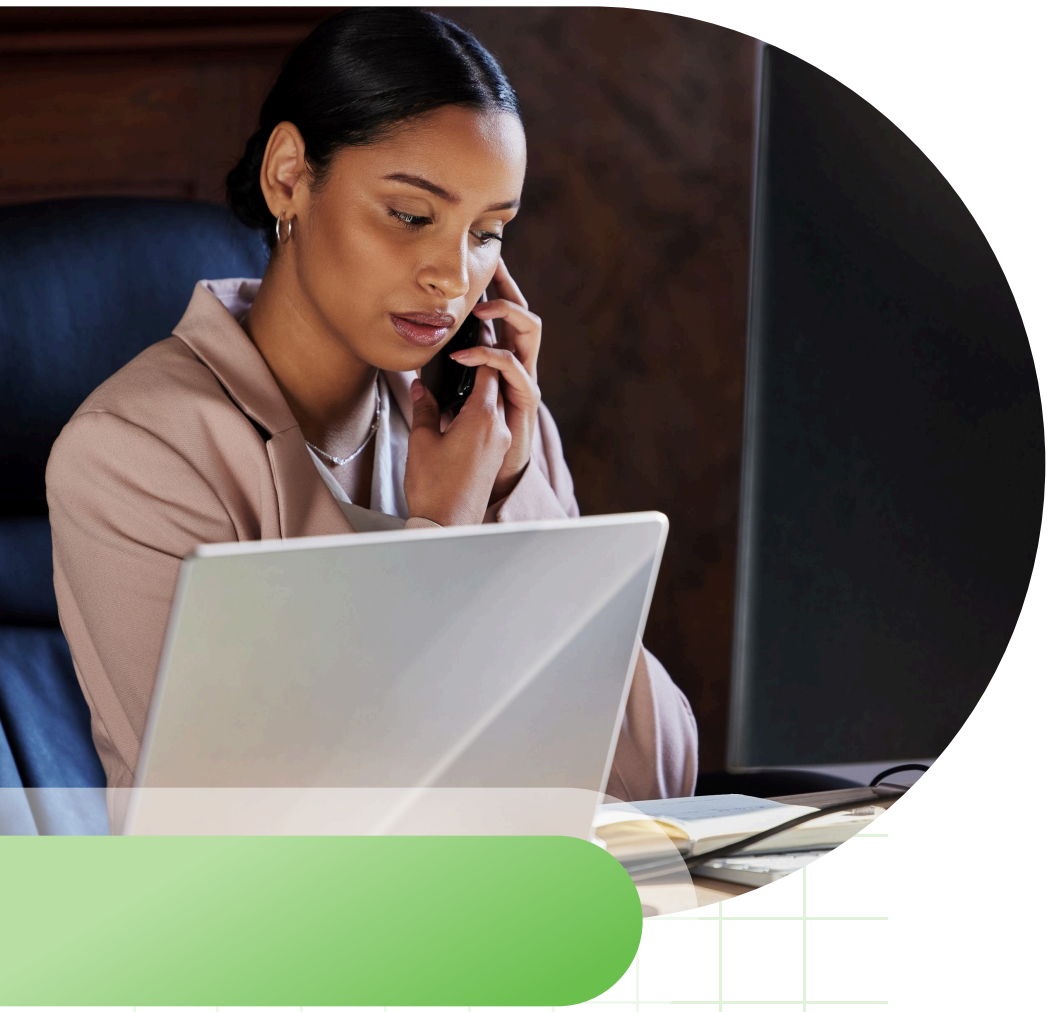
Within Duo, RBAC or **role-based access controls**, allows for granular admin permissions via the Duo Admin Panel. By defining subaccount roles and easily setting up access policies with sub-account tagging, it's easier to onboard new clients with appropriate admin privileges, simplifying security management.

COMPLIANCE REQUIREMENTS:

Easily Cover Your Bases



Compliance is important to clients – so proving compliance becomes important for MSPs. Failure can result in fines, lawsuits, and lost business. Many customers come to MSPs with specific requirements to meet regulatory compliance or cyber insurance needs. Tools like Duo can help by meeting all the requirements for a **compliance-effective security product** including industry standards from the National Institute of Standards & Technology (NIST) and regulations such as the General Data Protection Regulation (GDPR), PCI-DSS, and EPCS.



However, responsibilities also include recording and reporting that can eat into the time of employees as well as trying to keep up with the tasks that maintain compliance. Straightforward, comprehensive documentation and help articles packaged with Duo are also great resources to ensure compliance and help with any issues that arise.

In a similar vein, the evolving world of cyber insurance is simplified through proper documentation helping to prove the correct security controls such as MFA are in place. Duo is there to help organizations comply with insurance requirements through embedded security protocols like MFA, device trust, and establishing least privilege access policies.

A BETTER HELPDESK EXPERIENCE:

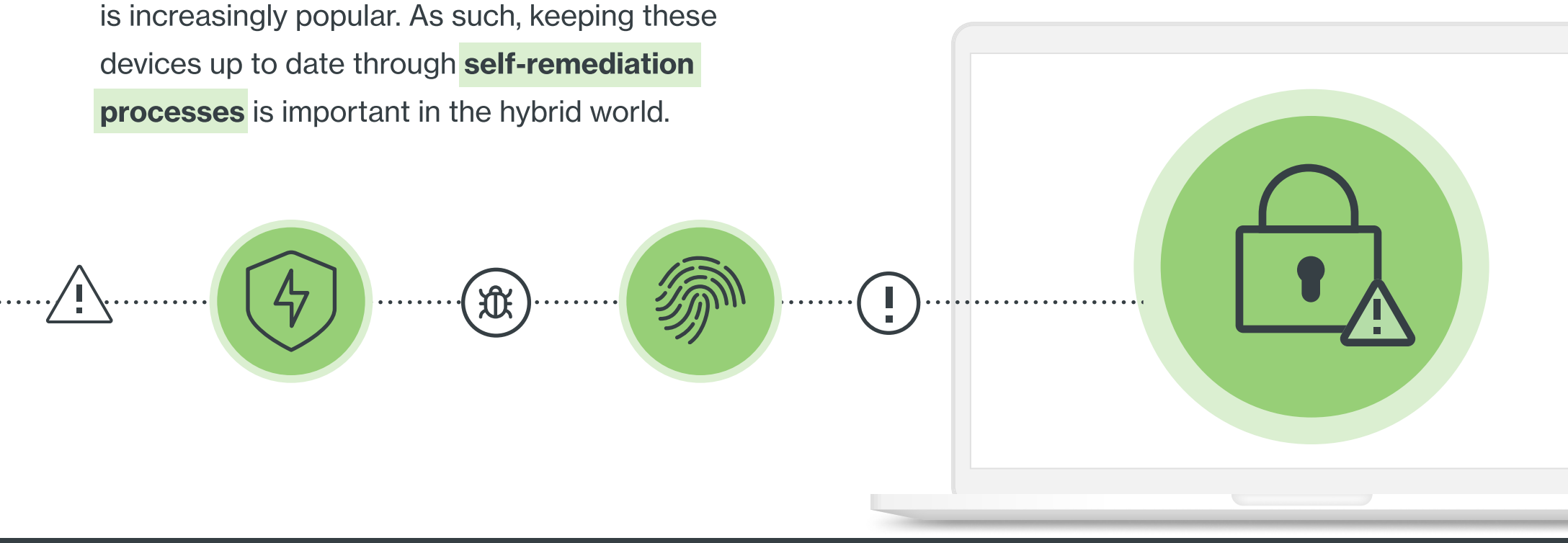
Identity Verification and Self-Service Password Resets

An MSP's helpdesk is a key interaction point with clients. But when a customer is calling for assistance, authentication procedures like calling back to verify the client's identity delays the process, and can be vulnerable to threats like SIM swapping, voice phishing (vishing), and newer sophisticated scams augmented by AI. Traditional security question, "secret passcode", or verbal confirmations may no longer be a secure option. Instead, check the source in real time. This can be in the form of a simple push notification to the user's phone where identity can be verified while still on the call. With Duo, free **helpdesk identity verifications** are sent and logged through the Duo Admin Panel, making it an easy reference point for compliance and other business functions.

This is especially important with a hybrid workforce where Bring Your Own Device (BYOD) is increasingly popular. As such, keeping these devices up to date through **self-remediation processes** is important in the hybrid world.

Duo's endpoint self-remediation process empowers the end user by guiding a user through updating a device, browser or app before they're able to access resources rather than going through an IT admin. For new devices, actions like Duo's self-enrollment processes make it easy for MSPs to roll out MFA to a new client with the process no longer taking days or weeks.

With password resets being one of the most common calls to a helpdesk, a self-service option is a great way to ensure good security hygiene without adding administrative burden. Expired password resets with **Duo SSO** allow users to reset their expired Active Directory passwords while authenticating through Duo SSO. Cut down on the administrative time required to answer the most common helpdesk tickets.



Finding the Right Partners

MSPs are distinct from internal IT departments. They may perform a lot of the same functions, but their solutions and operations need to be effective and scalable. Finding the right partner also relieves burdens in other areas so that an MSP can focus on true customer support.

Like the Greek myth of Sisyphus, MSPs can feel like they are constantly pushing a boulder uphill, and every day they need to start pushing from the bottom of the hill again. But there are ways to increase efficacy and efficiency in the face of these daily challenges.

Therefore, **finding the right partner program is imperative for MSPs**. It can mean direct access to strategic advisors, procedures, and program benefits that enable product adoption while keeping everyday overhead simple.

This includes dedicated partner managers, and the sales and marketing support needed to grow an MSP who may not have a specialized team. MSPs need technology partners that understand this need, provide services that help them scale and increase efficiency, and go beyond providing a simple multi-tenant license towards a better quality of life.

About Duo MSP

Now more than ever, **Duo's MSP program** helps you eliminate complexity and grow your business with industry-leading secure, scalable, and flexible access management.

Duo's MSP partnership includes premier-level Not For Resale (NFR) licenses that allow a partner to trial the product and protect MSP operations without locking into a lengthy contract.

The pay-as-you-go model offers a usage-based program making it easier to offer clients flexibility without assuming risk and means your team spends less time on billing processes.

For MSPs without a dedicated sales and marketing function, the Duo partner program offers sales and marketing support to ensure partners have the right tools to scale business.

The Duo MSP program makes is easy to:

- **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 Duo RBAC
- **Succeed with technical and marketing support** from our team and access to an extensive documentation library and 50 NFR licenses

CISCO DUO

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