daisy.

cisco Partner
Gold Certified
Solution Partner

LOCKED DOWN: CISCO DUO AND THE POWER OF MULTI-FACTOR AUTHENTICATION (MFA)

SECURING THE REMOTE WORKFORCE

Virtual private networks (VPNs), cloud computing and video conferencing tools ensure that employees can work effectively even when away from the office. Today, more and more organisations are embracing remote access to enable employees to work from anywhere – transforming their networks from the data centre to multi-cloud, either out of necessity or because they promote a flexible working culture.

This shift in the way we are working and connecting remotely requires a robust security solution for remote workers whether they are on or off the network, meaning that the more traditional perimeter-based network security is no longer adequate.

IT departments are responsible for making sure the remote workforce is protected on any device in or outside the office environment. This means an organisation's authentication strategy must make it as easy as possible to access business applications safely from anywhere, at any time. Attackers are increasing their focus on compromising user credentials to leverage corporate networks and system access, and the threat of compromised credentials can be magnified when you are outside of your office work environment.

Organisations must find new ways to effectively manage security by focusing not just on making quick decisions around remote working strategies, but on making the right long-term decisions.

ZERO-TRUST MUST BE THE NEW SECURITY MINDSET

Traditional security relies on location-based trust with the security walls or the perimeter living in and around the network. Mobility, bring-your-own-device (BYOD), and cloud applications have changed that. The office is no longer a fixed location and connecting to the network and applications has expanded the perimeter to anywhere access.

Today's security approach must shift from unconditional confidence in users to zero-trust fundamentals. This means that you should assume no trust when someone or something is requesting access to your work assets. A zero-trust approach uses a variety of factors for verification and authentication before granting access to work resources and business applications.

The whole concept of zero-trust becomes even more relevant as people start their journey to a secure access service edge (SASE) model, which consolidates networking and security capabilities and functions into a single, fully integrated cloud service. By embracing SASE as part of their long-term security strategy and implementing zero-trust, organisations can create a reliable and secure environment for employees to easily interact both on and off-premise, optimising operational efficiency while keeping sensitive data safe.

With a zero-trust security platform such as Cisco Duo, you can help to prevent unauthorised access and data breaches, as well as reduce the risk of attacks. Cisco Duo ensures only the right users and secure devices can access applications, regardless of location.

MAKING MFA YOUR DAY-TO-DAY

Zero-trust, along with multi-factor authentication (MFA), must become the new normal. With more people working remotely, internal systems and cloud systems alike are operating without the trusted barrier of being inside the network. MFA enables IT teams to rest a little easier, knowing that they have deployed a security strategy that protects both platforms and users, thus reducing complexity while ensuring access and boosting the flexibility of remote workers.

For many businesses, MFA is the first step along the path to a zero-trust security model, in which you base application access on user identity and the trustworthiness of devices. MFA strengthens access security by requiring two methods of verification and is now the expected standard. Without it, you run the ongoing risk of falling victim to credential-based cyberattacks, and anything less should be seen as a security weakness.

Integrating MFA with your applications means that attackers are unable to gain access without possessing the physical device needed to complete the second factor. MFA from Cisco Duo protects your applications by using a second source of validation, such as a phone notification or one-time password (OTP) hardware token, to verify user identity before granting access – all of which protects against phishing, compromised credentials or other identity-based attacks.

FIVE GOOD REASONS TO USE MFA TO PROTECT YOUR VPNS AND CLOUD-BASED APPLICATIONS

VPNs provide remote access to internal applications, but if you provide users with just a username and password to access a VPN connection, your organisation could be exposed to data breaches if those credentials are compromised. Similarly, cloud-based applications are available without the requirement of being on the network or VPN, and therefore require additional protection.

MFA adds an extra layer of defence. Here are five reasons you should use it to ensure trusted access:

1. Protect against credential theft

With stolen credentials, an attacker can access your corporate network using the VPN and from there, can try to gain privileges and move on to other systems, applications and servers. An attacker could also install malware on internal systems to gain persistent backdoor access to the network.

- Layering secure MFA on top of a VPN defends against credential theft
- MFA verifies the identity of all users with a second factor before granting access to corporate applications, which protects against phishing or other access threats

2. Reduce security and compliance risk

Securing application access, whether through VPN or the cloud, is also a data regulatory compliance requirement which MFA helps to achieve.

- By adding MFA, you instantly reduce the risk of potentially expensive data breaches, protecting your and your customers' sensitive data in the process and reducing the risk of heavy fines

3. Enable consistent access security for on-premise and cloud apps

While VPNs deliver remote access to on-premise applications, many organisations are moving workloads to the cloud. That can often introduce inconsistency into how users access applications, creating different processes and security postures for on-premise and cloud.

- MFA ensures consistent and secure access across on-premise and cloud apps, meaning the process for logging into the VPN is the same as the process to log into email, file sharing, collaboration or any other applications that have moved to the cloud

FIVE GOOD REASONS TO USE MFA TO PROTECT YOUR VPNS AND CLOUD-BASED APPLICATIONS (CONT...)

4. Gain visibility into all devices

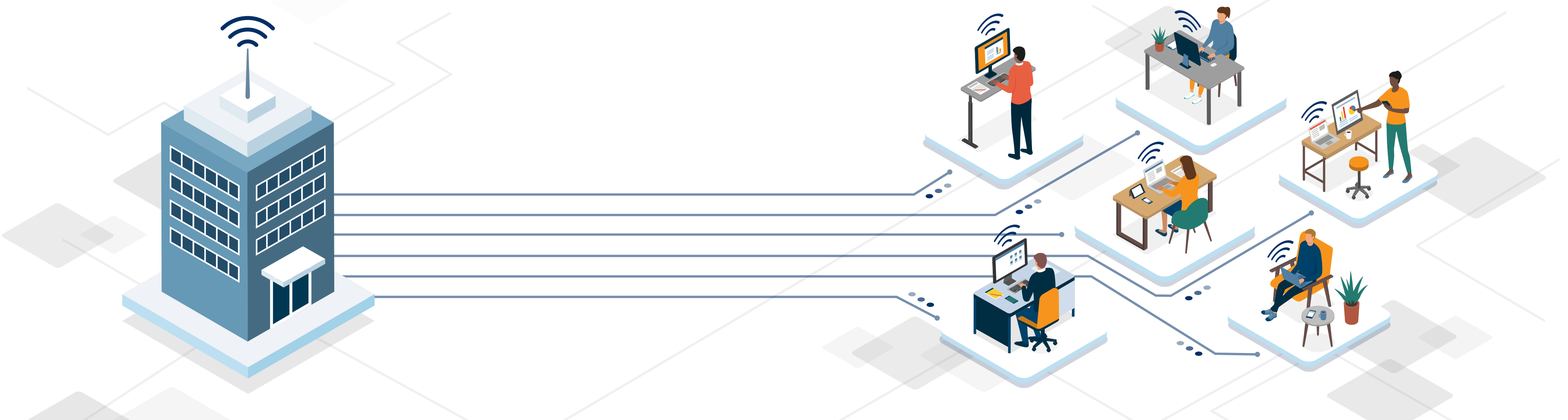
Some MFA solutions, like Cisco Duo, can give you insights into the devices accessing all applications – on-premise and in the cloud, including your VPN deployment.

- You can see the security posture of all user devices, such as laptops, desktops and mobile devices, including all personal devices that access cloud applications. This information is invaluable in understanding the compliance status of the devices in your estate

5. Enforce granular access security policies

Certain MFA solutions, such as Cisco Duo, can offer the ability to enforce security policies based on user and device risk.

- You can enforce a security policy for VPNs to allow access only from specific locations, and from devices that have up-to-date software such as anti-virus. This gives you a higher level of assurance before you grant a user or their device access to applications and the network



WHAT CAN CISCO DUO DO FOR YOU?

Cisco Duo provides a simple, streamlined login experience for every user and application, and as a cloud-based solution, it integrates easily with your existing technology.

✓ **Strengthen access security with multi-factor authentication (MFA)**

Verify the identity of all users with Cisco Duo's secure, one-tap-approval MFA. Cisco Duo is fast and easy for users to set up, and with several available authentication methods, they can choose the one that best fits their workflow.

✓ **Protect every application, whether it's in the cloud or on-premise**

With Cisco Duo's remote access and single sign-on (SSO), you give users secure access to all business applications, from any device and any location.

✓ **Safeguard against vulnerable or compromised endpoints**

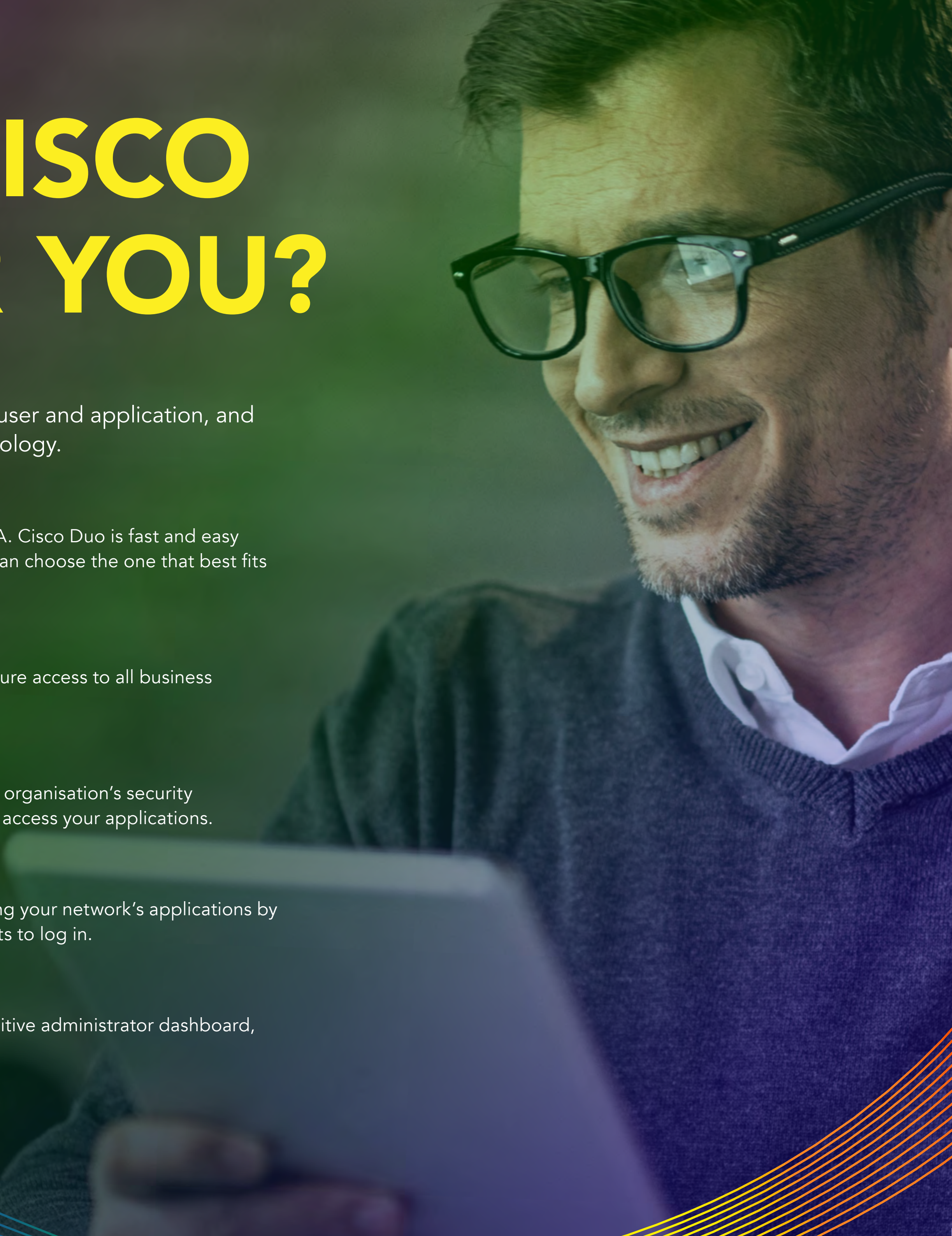
After verifying user identities, Cisco Duo checks that their devices meet your organisation's security standards. You gain visibility, insight and control over all devices before they access your applications.

✓ **Monitor the health of managed and unmanaged devices**

Cisco Duo allows you to ensure only healthy and trusted devices are accessing your network's applications by performing a complete health check for all devices every time a user attempts to log in.

✓ **Set adaptive security policies tailored for your business**

With Cisco Duo, you can set up detailed policies in minutes via a simple, intuitive administrator dashboard, and manage rules globally or for specific applications or user groups.



GET IN TOUCH

In today's fast-moving world, the ability to work anywhere can be the catalyst that drives your organisation's success. However, be wary of making rushed and poorly thought-through decisions with the potential to render your organisation vulnerable to cyberattacks. Now is an excellent time to re-evaluate how to discover, prevent and respond to the new threat landscape to support your business operations both now and into the future.

At Daisy we're able to ensure that our customers have the best levels of defence and mitigation against attacks of all kinds so that you can concentrate on driving your organisation forward. We can help put your organisation in the best position to ensure security postures are maintained.

As a Cisco Gold Partner, we can combine Cisco Duo with Cisco Umbrella's integrated network and security architecture, and SD-WAN powered by Cisco Meraki to deliver secure access to applications anywhere users work.

Get peace of mind today, why not schedule a no-obligation call with one of our security experts to discuss what might work for your business?

Call: **0344 863 3000**

or email: **enquiry@daisyuk.tech**

CISCO Partner
Gold Certified
Solution Partner

daisyuk.tech