Duo for...

cisco SECURE

Cyber Essentials

Duo helps organisations on their journey to Cyber Essentials certification

THE CHALLENGE:

The global pandemic has accelerated existing trends in the way we work. From digital transformation to the move to cloud services to working from anywhere and everywhere, events that typically take years materialised in a span of a few months.

However, huge strides in technology adoption have also had negative consequences. A transition to a new way of working happened before it was even possible to bridge any gaps in processes and technologies, an inevitable by-product of a large-scale change. The gaps were quickly exploited by cybercriminals, leading to a multi-fold increase in cyberattacks across the globe.

In response to these changes, the National Cyber Security Centre (NCSC) introduced the biggest overhaul of the *Cyber Essentials* technical controls since they were first launched in 2014.

Key changes in the new Cyber Essentials update focus heavily on the cloud and security challenges of remote work. They include:

- **New home working requirement.** This change, which includes instructions on how to include it in the scope of certifications, reflects widescale adoption of remote work and hybrid environments from 2020 forward.
- **Broader scope now includes the cloud.** All cloud services are now within certification scope: Infrastructure as a service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- **Cloud included in MFA requirements.** Both administrator and cloud-connected accounts now need MFA.
- **New device-unlocking requirements.** Added guidelines cover device-locking for physically present users, from PIN length to number of login attempts.
- **New updates on password-based authentication.** Beyond a new section on MFA, this content, relocated to 'user access' control, includes specific password parameters and types of additional factors.
- **Clarification on end-user devices (within scope).** Smartphones, tablets, and any other devices used to connect to organisational services fall into this category.
- **Clarification on BYOD devices (outside of scope).** Remote or mobile BYOD (bring your own device) items that are only used for texting, voice calls, or with MFA-authentication apps now fall outside of certification scope.

The NCSC has provided a series of **Cyber Essentials FAQs** on these changes, along with the updated IT infrastructure requirements.

CYBER ESSENTIALS SCHEME

- **Issuer:** The UK's National Cyber Security Centre, part of Government Communications Headquarters (GCHQ)
- **Scope:** Recommended for organisations of all sizes, mandatory for firms with some UK Government contracts
- **Objective:** To ensure systems are guarded against the most common cyber threats.
- **Requirement:** Certification that addresses five technical controls: Firewalls, secure configuration, user access control, malware production, and security update (patch) management.

THE SOLUTION:

Duo delivers the access control, malware protection, MFA, and critical security for Cyber Essentials certification.

01

Firewalls

GOALS

- Ensure that internet-connected devices are protected by a firewall to create a secure perimeter controlling traffic in and out of your organisation.
- Ensure that access to your gateways is secure when utilised as a VPN by users accessing internal applications.

HOW DUO HELPS

Duo helps protect company assets by using multiple factors to verify the identity of users before allowing them to access network resources. Duo's strong MFA secures access to web-based firewall administration. You can secure your SSH firewall access with the **Duo Network Gateway** (DNG), a part of Duo Beyond edition. DNG enables organizations to provide **zero trust remote access** to web applications, web pages and SSH servers without the requirement of a VPN or exposing those applications to the internet directly. Moving beyond traditional perimeter-based controls, **Duo Beyond** addresses threats that can bypass the firewall, including stolen passwords, policy gaps, vulnerable endpoints and more.

Duo Beyond focuses on the combination of an authenticated user and a secure, healthy device. With risk-based, adaptive two-factor authentication, you can both verify the identities of your users and apply stronger user access policies at log in.

Duo Beyond also checks the security posture of devices to ensure they meet your security requirements. This includes firewall status, drive encryption status, password status and if an antivirus/ anti-malware agent is running.

By adding Duo's MFA to your VPN deployment you instantly reduce the risk of a data breach while helping you easily meet Cyber Essentials compliance requirements. So, whether you want to add an extra layer of protection to an existing VPN or try a VPN-less alternative (Duo Network Gateway), Duo can help.

02

Secure Configuration

GOALS

- Ensure you have chosen the best security posture for your devices and software. Utilise a strong MFA to assure the security for device and application access.
- MFA is a great first step to securing configuration but is limited to only ensuring that a user is who they say they are.
- Secure configuration also extends to devices and the need to ensure that the devices accessing your data have an acceptable security posture.
- Many devices are left at a default posture with no mechanism to check or enforce that they meet an organisation's security standards before accessing applications and data.
- Change any default or guessable account passwords

HOW DUO HELPS

Duo verifies the identity of all its users – before granting access to corporate systems and applications. A foundation of a **zero trust security model**, MFA can assist with mitigating breaches that target user passwords and accounts, such as phishing, credential theft, keyloggers, and brute force attacks. You can enforce user **access policies** to block logins, based on IP addresses, countries, anonymous networks such as TOR or anonymous VPNs. Additionally, you can define and enforce rules via granular based per-application policies. Duo's **Policy & Control** allows you to control which operating systems and versions are allowed to access your applications.

03

User Access Control

GOALS

- Implement MFA, where available. Authentication to cloud services must always use MFA.
- Employees should only have access to the applications and services that are necessary for them to perform their role.
- Privileged access should only be provided to those that carry out administration roles.
- Ensure appropriate device locking controls
- Provide additional protection to administrative accounts, and accounts that are accessible from the internet.

HOW DUO HELPS

You can verify the identity of all users with Duo's strong MFA before granting access to corporate systems and applications.

Protect against credential theft by adding MFA to your virtual private network (VPN). Add an extra layer of defence to achieve compliance with the Cyber Essentials requirements.

04

Malware Protection

GOALS

Implement a malware protection mechanism on all devices that are in scope. Use at least one of the three mechanisms listed below:

- Anti-malware software
- Application allow listing
- Application sandboxing

HOW DUO HELPS

Duo verifies user identities and establishes **device trust** before granting access to applications.

Secure Endpoints prevent breaches and block malware at the point of entry, then rapidly detect, contain and remediate advanced threats at the endpoint.

Duo and Secure Endpoints work together to detect malware and automatically respond to threats by blocking risky endpoints with access policies.

05

Security Update Management

GOAL

- Ensure that your devices, software, and applications are kept up to date with the latest security patches.

HOW DUO HELPS

Detect when a device (a mobile device, laptop, or desktop) accessing an application is running an out-of-date operating system.

You may choose to warn your end users when their software is out of date, require software updates before allowing access, or even block access from devices that don't meet your organisation's requirements.

Duo's **Endpoint Remediation** with in-built self-remediation enables users to update their devices, both corporate and BYOD, immediately with direct links provided, alleviating the load on the help desk to provide assistance.

Enforce **security policies** where necessary to ensure compliance and block non-compliant devices at the time of authentication.

Duo for Cyber Essentials

CONCLUSION

With Duo, you can start your journey towards Cyber Essentials certification introduced by the NCSC. In addition, Duo can help you incrementally achieve a zero-trust transformation, a strategic approach to securing your environment. Establishing user and device trust before granting access to applications, ensuring secure access for any user and device connecting to any application, from anywhere – Duo provides the foundation for a zero-trust security model.

This trust-centric security approach for the extended perimeter makes it much more difficult for attackers or unauthorised users to gain access to applications without meeting certain identity, device and application-based criteria.

“

This is the brilliance of Duo — most people spend so little time interacting with it, as it’s so quick and simple, that they barely know they’re using it.”

Ben Hughes
Network Security Manager, Etsy