

Managed multi-factor authentication—your first step to a zero trust network

The modern workforce is more mobile than ever before. Users and devices can connect from anywhere—so companies must protect them everywhere. A zero trust security model establishes trust in users and devices through authentication and continuous monitoring of each access attempt with custom security policies that protect every application. While one tool is not the answer to a zero trust network, providing the greatest marginal return on time and resource investment is.

Adoption of managed multi-factor authentication (MFA) can help address common security challenges in the workforce such as phishing, malware, credential theft, remote access, and device security (BYOD), without placing additional burden on your IT staff. By implementing managed MFA, you are one step closer to enabling your “never trust, always verify” approach to security.

This is done by securing the three primary factors that make up the workforce: **users, their devices, and the applications they access.**



CBTS deploys and manages Cisco Duo in your environment.



Verify identity in seconds.



Protect any application on any device.

User-friendly, secure authentication

Adding multi-factor authentication to your security stack doesn't have to be disruptive to your users. 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. No headaches, no interruptions.

Scalable technology

Managed MFA by CBTS natively integrates to secure any application or platform, so whether you're adding 2FA to meet compliance goals or building a full zero trust framework, CBTS managed MFA with Cisco Duo is the perfect addition to your security portfolio. And because it functions like a gateway for your existing and future IT infrastructure, it's the ideal solution for growing businesses of any size.

- Multi-cloud, hybrid, or on-premises environments.
- SaaS tools, critical infrastructure, custom applications, including SSH.
- Secure remote access and VPN clients, BYOD, with offline devices ability.

Speak to a **managed security expert** today.



Managed multi-factor authentication—your first step to a zero trust network
cbts.com 001220427 B



Security, covered.