300 Cyber Security

WHY DO I NEED A MFA TOOL?

Multifactor authentication is one of the best measures to protect your network and personal assets. Stolen credentials are the easiest and most common way to access protected resources and commit cyber crimes. Adding an additional step beyond entering passwords to prove identity is a simple yet highly effective means of preventing unauthorized access. Most mid-sized organizations have adopted some form of MFA, but the breadth of adoption across sensitive resources is much less universal than it should be. MFA has one of the best ROIs to increase organizational security. It needs to be used by every employee to access almost any corporate resource.

It's also one of the easiest for non-technical stakeholders to understand. Insurance providers especially have focused on MFA as the minimum standard for insurability. As the cyber-insurance market tightens and thresholds for insurability increase, organization-wide MFA adoption is becoming the de facto minimum standard. Those who fail to implement MFA at scale face increased premiums, declined insurance applications, or will find themselves in a legal battle should they require an insurance payout. (see **https://300cybersecurity.com/resources/** - The Travelers Case) Governments, industry regulators, and trade organizations have adopted a similar attitude to MFA and are increasingly demanding its adoption as part of their audit process.

The challenge is how to add the second step to the authentication process. Text-to-mobile MFA is easy, but it's susceptible to SIM stealing/number porting attacks and lacks a management interface for IT teams to monitor. Free random number-generating authentication apps often don't have cloud management consoles that IT teams can use to manage organizations and assist users with authentication issues.

User resistance is one of the most significant barriers to the widespread adoption of MFA. A critical factor in winning user buy-in for MFA is the ability to quickly and easily remediate user issues. A cloud-based support console that allows IT teams to solve authentication problems and decrease user friction is essential. Reducing user inputs required during the authentication process is also an important factor in increasing employees' support for this critical security enhancement.

SUMMARY

- MFA represents an excellent ROI in enhancing organizational security
- It will soon be a minimum requirement for purchasing cyber insurance
- Governments, industry regulators, trade associations etc. are adopting it as a minimum standard
- Gaining user buy-in is made easier by reducing inputs required
- IT teams need a powerful management console to easily remediate user authentication issues

---

Why We Chose Cisco Duo?

Cisco is one of the largest technology companies in the world and is very friendly to the SMB market. They produce best-in-class enterprise solutions and have created a distribution network that makes them accessible to smaller organizations. Because Duo is a cloud-managed platform, fees can be kept low, even on small volumes, since no capital or infrastructure expenditure is required. SMB customers can use the exact same solution as global giants.

Duo represents the best opportunity to enhance security while minimizing user friction and maintaining IT management control. Users like Duo's Push function which allows them to authenticate the second factor with only a single touch on a smart device. Duo also offers authentication using a time-based one-time password generated through the Duo app when connectivity isn't available. IT teams like the ability to manage user authentication from a powerful and friendly cloud-based management console that makes troubleshooting support issues easy. Duo makes implementing a MFA policy across a user base easy and is an extremely cost-effective return on effort.

SUMMARY

- Cost-effective, no capital investment required
- Trusted by some of the world's biggest companies
- Users like the speed of 2nd-factor authentication
- Flexibility of authenticating when devices are off-line
- IT teams like the powerful and easy-to-use cloud-based management console