

# Financial Services

Many financial services organizations use multi-factor authentication (MFA) to protect their company and their users. Duo offers MFA as an important layer of security, as well as additional features to ensure secure remote access.

## THE CHALLENGE:

### Secure Access With Ease

With the rise of remote work and hybrid workforces, security teams have to insert controls to confirm user identity and prevent potential security risks. This is especially important with the increase in the number of user types, devices, and access locations. Organizations must secure against unknown threats, put barriers into place to stop bad actors, and maintain trusted user access - all while finding a solution that works across complex IT infrastructure and a dispersed workforce.

Specifically within the financial services industry, companies rely on a mixture of on-premise legacy systems, as well as new cloud solutions. This has led to diverse systems that can be difficult to manage. These systems, containing some of the most sensitive and sought-after financial data, are prime targets for cyber-attacks. For these companies, it is essential to not only have strong access controls, but to also have a solution that can work for them, regardless of current infrastructure.



## THE SOLUTION:

# Broad Coverage with Duo

Duo helps financial institutions protect all users, devices, and applications to enable security:

## 01

### Efficient & Seamless MFA

Usable security is effective security. Different types of applications often require users to follow different authentication processes – burdening users and help desks. Duo's strong focus on authentication ease of use minimizes user resistance and reduces total cost of ownership.

Duo offers several methods of authentication to enable every user to easily access internal applications, including Duo Push, one-time passcodes (OTP), phone calls, SMS or hardware tokens. This consistent experience for all users, including third parties and contractors, allows secure access across the enterprise to protect sensitive information.

## 02

### Enforce BYOD Policies

Mobile workers and the bring your own device (BYOD) trend has sparked a digital transformation. Organizations have to deal with a diverse set of users such as employees, contractors and partners who work from anywhere at any time and on any device, which can increase security risks for the organizations. It's no longer safe to assume that users are who they say they are and their devices are secure.

Organizations can use Duo to limit remote access to specific internal applications. This helps avoid the risk of lateral movement and privilege abuse as part of a zero-trust security model. Duo provides complete visibility into all computers and mobile devices and empowers administrators to limit or block access from unknown or risky devices.

## 03

### Enterprise Ready Solution

Offering more than 200 out-of-the-box integrations, Duo protects access to both on-premises and cloud-based applications like Office 365, Dropbox, and Cisco VPN.

Duo also scales to meet companies' security needs, providing offline MFA, compliance-friendly reporting and logs, and the ability to add users and devices at any time.

MFA can pair with single sign-on to create a consistent login workflow across all applications and sync with directories to ensure policies stay current even as the user base changes. No headaches, no interruptions – it just works.

“We loved Duo's speed to security, the experience working with their subject matter experts, the time and money we save with the ease of integration, and the overall end-user experience.”

**John Bryant**

Chief Technology Officer

Options Technology (managed services provider for financial institutions)

---

Start your free 30-day trial at [duo.com/trial](https://duo.com/trial).