DUO for...

Office 365

Duo Security provides solutions that support security initiatives by enabling organizations to establish access policies and enforce easy to use multi-factor authentication to protect Office 365 applications quickly and efficiently.

THE CHALLENGE:

Protecting Productivity

The compatibility to a wide spectrum of operating systems and the variety of programs available on Office 365 make it a popular productivity suite for businesses of any size. Since the data and email in Office 365 are often sensitive to organizations, many organizations are looking for solutions that go beyond simply protecting the users, credentials. Many are implementing application access control policies that will block attempts from unknown origin points and devices that don't meet security policies.

To ensure adoption by the user base when implementing security controls for Office 365, it is key to find the right balance between security and usability.

"

[Duo is] one of the best products we have worked with so far. The speed and ease of deployment was particularly impressive."

Jim Jorstad
Director IT-Client Services, University of Wisconsin–La Crosse

Duo for Office 365

THE SOLUTION:

Balancing Security and Productivity

Duo provides an invisible layer of security that won't disrupt user productivity. Duo offers the ability to add an additional security layer to protect Office 365 and many other Microsoft applications. Duo's easy to use and manage solution results in high user adoption, reducing the burden on help desk for management and deployment.

01

Complete Visibility Into All Devices

Users can access Office 365 from a variety of sources, most commonly using web browsers or thick clients on corporate workstations. There is an increasing frequency of access attempts from personal devices such as smartphones, tablets, laptops and more.

With Duo, IT admins get complete visibility into all devices accessing Office 365 and gather deep insights into the security posture of devices running out-of-date operating systems (OS), browsers, Java and Flash without using any agents. With these security insights, administrators can assess if devices logging in are potentially vulnerable to exploits and attacks.

02

Enforce BYOD Policies For Office 365

Admins can create access policies to manage the risk of compromised devices or users accessing Office 365. Policies can be applied regardless of which client app a user chooses and can be based on group membership, network range, device type, device health, OS and more.

Administrators should be able to govern acceptable security risks for each access attempt. For example: If users are logging into Office 365 from a device that has an out-of-date browser, the access attempt should be blocked. An out-of-date browser can have several security vulnerabilities that haven't been patched.

03

Deployment Flexibility

Duo provides IT admins with several easy-to-deploy options to secure Office 365, reducing the risk surface without decreasing user productivity. IT admins can secure access to Office 365 with Duo's secure SSO solution. Alternatively, customers who have invested in Active Directory Federation Services (ADFS) can use Duo's secure SSO to get device insight and enforce security policies that complement ADFS without needing to rip and replace their existing setup. Duo's native integration with Azure AD helps organizations move to the Microsoft cloud faster and safer than ever before, making it easy for IT admins to add Duo as an additional layer of security for protected applications.

Duo protects all Microsoft applications with seamless integrations, offering protection for:

Windows 10 · Office 365 · Windows Server · Active Directory Federation Services · Azure Active Directory · Exchange