5 Reasons to Protect Your VPN With MFA

Duo Security is now part of Cisco.

CISCO

BBH SOLUTIONS

www.bbhsolutions.com

Virtual private networks (VPNs) are a tried and true method for providing remote access to internal applications. Essentially, they create a private, encrypted tunnel for an off-site user to connect to applications in a corporate data center. But VPNs aren't a silver bullet – organizations that provide users with just a username and password to log into their VPN connections could be exposed to data breaches if those credentials are stolen.

Protecting your VPN access with multi-factor authentication (MFA) adds an additional layer of defense. Here are five reasons you should secure your VPN with MFA to ensure trusted access.

1 Protect Against Credential Theft

According to the Verizon 2018 Data Breach Investigations Report, 81 percent of hacking-related incidents leverage stolen or weak passwords. And a VPN is not immune. With stolen credentials, an attacker can access the corporate network over the VPN and from there, can try to gain higher privileges and move to other systems, applications and servers. An attacker could also potentially install malware on internal systems to gain persistent backdoor access to the network.

Layering strong MFA on top of a VPN defends against credential theft. MFA verifies the identity of all users with a second factor before granting access to corporate applications. This protects against phishing or other access threats.

2 Achieve Regulatory Compliance

Securing VPN access is also a data regulatory compliance requirement, and MFA helps achieve compliance.

For example, PCI DSS 3.2 requires organizations with cardholder data environments (CDE) to secure all remote access – even through a VPN – with MFA. Other compliance requirements, such as HIPAA and NIST 800-171, also have similar MFA requirements.

Adding MFA with your VPN deployment instantly reduces the risk of a data breach while helping you easily meet compliance requirements.

3 Enable Consistent Access Security for On-Premises and Cloud Apps

While VPNs deliver remote access to on-premises applications, many organizations are moving workloads to the cloud. That can often introduce inconsistency into how users access applications – creating different processes for on-premises and for cloud.

MFA ensures consistent access security across on-premises and cloud apps, meaning the process for logging into the VPN is the same as the process to log into email, file sharing, collaboration or any other applications that have moved to the cloud.

4

Gain Visibility Into All Devices

Some MFA solutions open up a world of rich device telemetry to give you insights into the devices accessing all applications – on-premises and in the cloud, including your VPN deployment.

You can see the security posture of all user devices, such as laptops, desktops and mobile devices, including all personal devices – aka bring your own devices (BYOD) – that access cloud applications.

5 Enforce Granular Access Security Policies

There are certain MFA solutions that offer the ability to enforce security policies based on user and device risk. For example, you can enforce a security policy for VPNs to allow access only from specific locations, such as the U.S., and from devices that have up-to-date software. This gives you a higher level of assurance before you grant a user or their device access to applications.

For many businesses, MFA is the first step along the path to a zero-trust security model – also called the “software-defined perimeter" – in which you base application access on user identity and the trustworthiness of devices.

Adding MFA to a VPN unlocks secure access to both on-premises and cloud applications – and ensures that access is trusted.

Duo for Cisco AnyConnect

Duo's multi-factor authentication (MFA) provides secure remote access to internal corporate applications using Cisco's AnyConnect VPN on Adaptive Security Appliance (ASA) or FirePower Threat Defense (FTD).

Duo's MFA gives Cisco AnyConnect VPN users three distinct benefits:

It's easy to use: Duo provides the easiest to use MFA solution for AnyConnect VPN logins. With **Duo's MFA**, users can validate their identities with one-tap authentication called **Duo Push.** MFA is an effective security control against stolen credentials because an attacker would not only need to compromise a user's credentials, but also get physical access to that user's device to execute an attack.

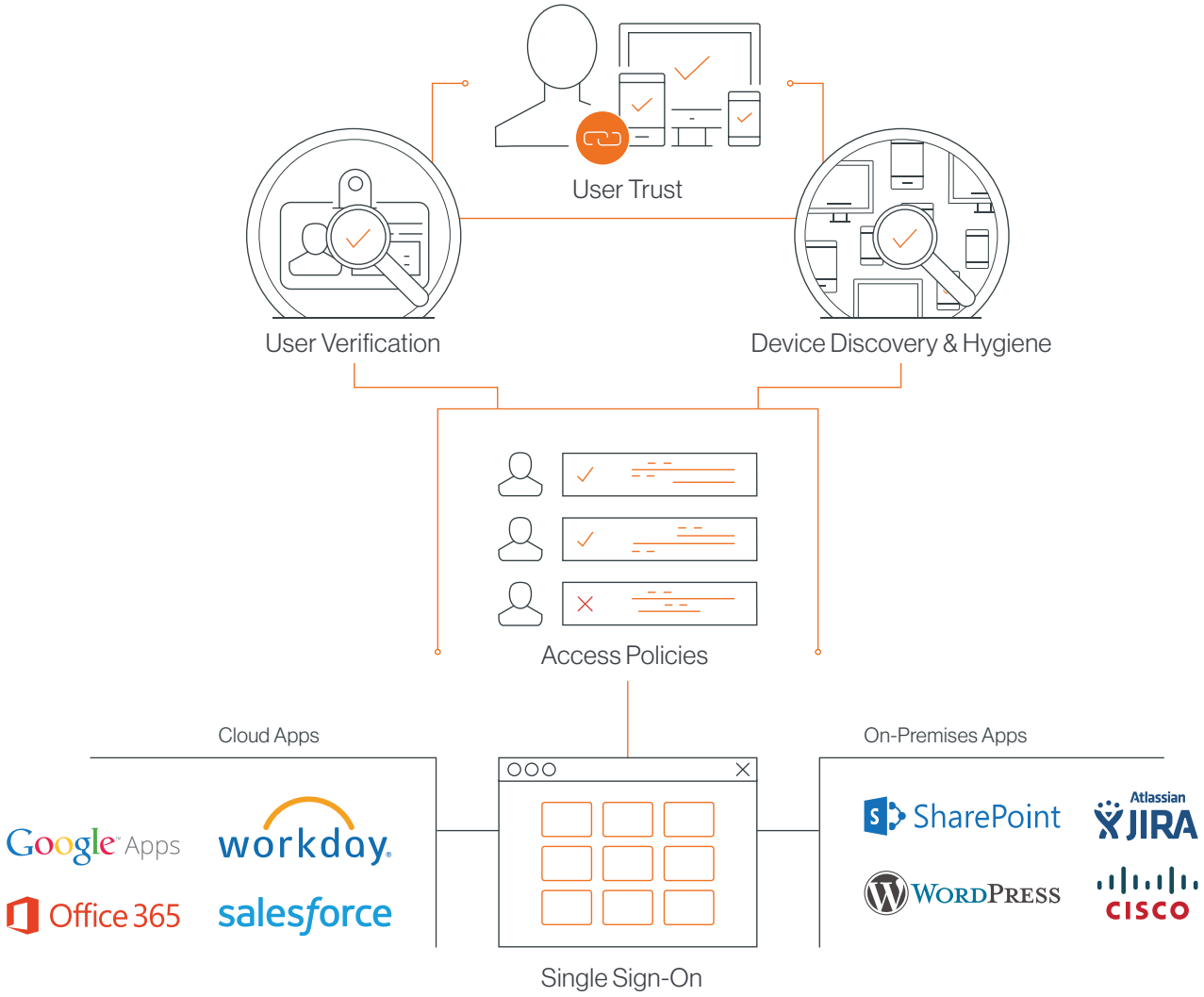
It offers flexible authentication options: Duo offers several **methods of authentication** to enable every user to easily access internal applications: Duo Push, one-time passcodes (OTP), phone calls, SMS or hardware tokens with AnyConnect VPN. IT admins can enable one or more of these authentication options based on their environment and user convenience.

It delivers stronger security with zero trust: Duo with AnyConnect v4.6 or later on Cisco ASA can provide admins with insights into devices and their security posture. Admins can **check for device health** and **enforce policies** to allow access to internal applications only from secure and healthy devices. For example, admins can enforce a policy to allow VPN access only from a corporate-managed and up-to-date device.

To learn more about using Duo MFA with Cisco AnyConnect VPN, contact us at **866.760.4247** or **duo.com**.

Beyond

Trusted Users. Trusted Devices. Every Application.



Duo Beyond secures access to all applications, for any user, from any device, and from anywhere. Cloud-first organizations and those looking for a secure, rapid transition to the cloud use Duo Beyond to protect their on-premises and hosted applications, while securing their mobile workforce and their chosen devices.

Duo Beyond delivers a zero-trust security platform that enables organizations to base application access decisions on the trust established in user identities and the trustworthiness of their devices, instead of the networks from where access originates. Duo delivers this capability from the cloud and without reliance on outdated, cumbersome, and costly technologies.

Contact **BBH Solutions** to learn more about Duo. **www.bbhsolutions.com**