# Securing VPN with Multi-Factor Authentication

## Virtual Private Networks Background and Challenges

Virtual private networks (VPN) allow users to securely access an organization's intranet while located outside the office. VPNs use encrypted connections to sensitive internal resources through the internet. However, while VPNs aim to promote better connectivity and security for organizations, IT and security teams face growing challenges to secure their VPN.

## Current Cybersecurity Challenges for IT

Enterprises have long connected their remote workers with a virtual private network to promote connectivity and security. But that's all changing today. While the cloud has offered the potential of greater collaboration and convenience, organizations face growing security challenges. When taking VPN to the cloud, organizations expose themselves to risks where hackers can gain unauthorized access to sensitive data.

### Criminals Target Credentials

One attack trend is credential phishing, which involves stealing username and password combinations by masquerading as a reputable individual or entity in email, IM or other communication channels. After the criminal obtains the victim's credentials, the criminal extracts the assets they are targeting, or may use that identity to target others within the organization. Corporate accounts are being targeted with sophisticated spear phishing aided by social engineering—an attack where criminals try to get victims to divulge sensitive information by playing to emotional aspects of human decision making.

## Use Multi-Factor Authentication (MFA) to Secure VPN

MFA augments your primary authentication (e.g. a password) with an additional layer of authentication (e.g. using a security token) to validate a user's identity. Typically, it involves at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

The goal of MFA is to provide higher degrees of identity assurance of a user attempting to access a resource via VPN. MFA prevents attackers from accessing your account even if they obtain your username and password. For example, if you create a multi-layered mechanism, an unauthorized user would have to defeat all layers to gain access.

However, not all MFA solutions and approaches are equal. Legacy on-premises MFA solutions are often cumbersome to deploy, solve only limited use cases and provide a poor user experience. The net result is limited end user adoption along with sunken IT and security costs.

Adaptive MFA (AMFA) is ideal for today's rapidly changing security landscape as it can integrate with an organization's applications and resources while adding an additional layer of identity assurance.

## Okta Adaptive MFA for VPNs

Okta Adaptive MFA empowers your organization to overcome current cyber security and VPN challenges by providing additional security to protect organizations from data breaches. Okta recommends the following three best practices pillars as essential components of an ideal Adaptive MFA solution.

1. **Secure**

   Okta Adaptive MFA delivers secure authentication for all environments, protecting identity and access to data wherever users go. This is extremely pertinent for organizations using VPN and expanding into the cloud. Today, data is no longer contained to on-premises; data is on mobile devices, in the cloud and in transit.

   Okta Adaptive MFA can help secure your VPN via factors such as one-time passwords and physical security tokens. Different authentication situations require different approaches. For example, an SMS second factor may not be ideal for users in areas with poor cell reception. Consider an MFA solution, such as Okta Adaptive MFA, that offers a wide range of factor and assurance level support.

### Okta Adaptive MFA supports all major VPN providers:

CISCO™

paloalto NETWORKS®

Pulse Secure®

FORTINET

Check Point®
SOFTWARE TECHNOLOGIES LTD.

JUNIPer NETWORKS®

f5®

SOPHOS

Okta Adaptive MFA helps organizations harden critical applications with step-up authentication based on user or device context and location. From an IT and security administrative perspective, Okta Adaptive MFA helps organizations apply a unified policy and provide a centralized view of on-premises, cloud and mobile data, therefore, augmenting levels of visibility and control.

2. **Simple**
   Okta Adaptive MFA delivers simplicity for both end users and administrators. Okta integrates with thousands of applications through standards-based protocols and can centrally enforce MFA across all of them. When selecting an MFA solution, be sure to consider one that can integrate to existing applications and services your organization is already using and will be flexible enough to support custom scenarios.

   Okta Adaptive MFA is easy to deploy and gives administrators more flexibility, visibility and control. When considering an MFA solution to help secure your VPN, it's imperative you select a solution that offers ease-of-use and simple, non-disruptive integration to your existing solutions.

   Okta's Adaptive MFA is simple for end users to verify their identity when accessing VPN and data. Ensuring that end users can enroll in a simple and flexible manner (such as in-line with existing login flows), while only prompting for factors in higher risk scenarios (such as when off the corporate network) all contribute to a better end user experience. If your users do not adopt an MFA solution due to complexity, the technology will not be embraced, and security goals will not be achieved.

3. **Extensible**
   An ideal MFA solution extends and adapts to other areas of your organization. Okta's Adaptive MFA plays a pivotal role providing visibility in all risk areas from on-premises networks, to mobile devices and to the cloud. When a security incident occurs, you'll have more visibility and be able to implement faster response.

   As previously noted, organizations face the challenge of fragmented approaches and disparate solutions. Okta Adaptive MFA seamlessly integrates with existing security tools and provides strong authentication for virtually all applications.

   Overall, Okta Adaptive MFA augments visibility, control and response extending to the entire organization. As emerging platforms and new business models develop, you need an MFA solution that will evolve and adapt with your changing security needs.

## Conclusion

Organizations realize they need to use MFA to authenticate remote users when accessing VPN. However, not all MFA solutions are equal. It's imperative to select an MFA solution that includes adaptive functionality with step-up authentication, non-intrusive and quick implementation, and ease-of-use for users and administrators. The ideal MFA solution should have extensible flexibility across the entire organization and security stack. Select an MFA solution provider that values innovation with solutions that will adapt to your evolving security needs.

Okta Adaptive MFA overcomes these challenges and provides the additional security required to adequately protect against data breaches while helping you meet new regulatory standards. Okta Adaptive MFA ensures security across virtually any application, whether in the cloud or on-premises, and for all user groups. With a full range of factors across the entire assurance spectrum, Okta Adaptive MFA reduces security risks by hardening access based on device and user context or location. With over 5,000 out-of-the-box connections on the Okta Integration Network, and API support for custom applications, Okta Adaptive MFA extends across the entire organization. Okta connects business applications and ensures seamless productivity and integration with a variety of security tools for end-to-end visibility and improved security.