idenprotect

Identity Driven Zero-Trust Network Access for Mobile

Having the ability to collaborate remotely with employees, partners and other third parties whilst they are on mobile devices is an absolute necessity now for any agile business.

But in a world where mobile and hybrid networking is now fast becoming the norm, how do you ensure that your mobile device users are connecting with your organisation's on-premise data in the most secure way?

Identity Driven Mobile Access Supporting ZTNA

Give your mobile users quick and secure access to your on-premise services outside the cloud.

Idenprotect's identity driven secure mobile access provides secure connections without limitations or complexity, supporting Zero-Trust Network Access (ZTNA) architectures.

EASE OF ACCESS FROM ANYWHERE
Easy for users to connect from a wide variety of devices to any of your applications and services. From anywhere at any time.

MANAGED BY YOUR MDM/MAM SOLUTION
Using solutions such as Microsoft Intune and Blackberry UEM it is easy to manage the Idenprotect Secure Browser and Idenprotect Authentication apps.

ZERO TRUST NETWORK ACCESS - ZTNA
You also have the assurance of Zero Trust methodology to safely connect users to data.

The Hybrid Challenge

Security and Trust

Hybrid networking incorporates systems and data residing in the cloud with those that remain on-premise. Many organisations see the benefits of hybrid deployments but they can create a number of new unforeseen and very real problems for IT.

Despite the move towards cloud-based systems there are many instances where some data and systems are better kept on-premise.

Connecting mobile devices to on-premise data via the cloud normally presents several challenges. Cloud service providers may not support connections, to on-premise systems, that would comply with organisations' security policies. For example, it is not possible to employ corporate certificates for Mutual TLS when connections between on-premise systems and mobile devices are routed via the cloud.

VPN Risks

To enable hybrid working, it would seem logical to deploy a VPN to allow mobile users a secure passage to the corporate network but there are significant risks with this approach.

VPNs lack essential granular security controls, and so offer inappropriate levels of access, allowing users to have more network privileges than they need.

The Solution

Idenprotect's Identity-based authentication, secure browser and secure access gateway supports the Zero-Trust Network Access (ZTNA) architecture and establishes a direct path between mobile devices and on-premise systems.

Using a modern approach to connect users with data safely and securely, without using VPNs, it enables compliance with the most stingent requirements.

idenprotect

The ultimate in secure browsing

Idenprotect's identity driven secure mobile access solution is based on zero-trust. By strongly validating and authenticating a user before launching the secure browser and sharing digital identity attributes based on public key cryptography, it is more secure, does not require additional or complex infrastructure and is easier to manage.

Quick Deployment
Mobilise your applications and services to your staff quickly and without disruption.

Simple User Experience
With just a few clicks, users can gain access to applications without the complexity or frustrations of VPNs and passwords.

Robust Security
Reduce the risk of financial and reputational damage by eliminating the risk of a data breach.

The future is password-free

sales@idenprotect.com
+44 (0) 20 3900 2704
www.idenprotect.com

Going Beyond Mobile VPN with ZTNA

It's now possible to move beyond the mobile VPN. By leveraging the digital identity of a user, a secure connection can be established from the user's mobile device once the user's identity has been validated.

Protected by Idenprotect's world-class security mechanisms, our mobile hardware-backed authenticator app challenges the user for their biometric. Upon successful validation, a secure cryptographic key is shared with the Idenprotect Secure Browser. This secure key in combination with the Idenprotect Secure Browser and the Idenprotect Secure Access Gateway secures the connection to the on-premise network. It manages on-premise DNS lookups and handles the additional authentication steps that take place at the remote application, supporting ZTNA.

The result is secure, fast and passwordless access for the user and a system that IT can trust to prove that the user is who they say they are and that their connection is properly secured.

The Components

Idenprotect Secure Mobile Browser

The Idenprotect Secure Mobile Browser is a web browser built using modern standards-based browser technology. It is the first identity driven web browsing solution for mobile for use within corporate environments. The browser has the ability to support Proxy Auto Config (PAC) so that browser traffic can be directed as per an organisation's requirements to either on-premise or external locations. Users have to be properly authenticated via the Idenprotect MFA before they can open the browser and use its features. The secure browser has the ability to manage and use Kerberos tickets, x.509 digital certificates and keys from the Idenprotect MFA authenticator app to ensure that strong authentication to web applications and services can be achieved. Usual features such as bookmarks, navigation and favourites are also available.

Idenprotect Secure Access Gateway

The Idenprotect Secure Access Gateway is a high-performance proxy platform that can operate in whatever proxy mode is required to suit each specific use case. If you are using other Idenprotect solutions such as the Idenprotect Secure Browser for Mobile, the Gateway can allow an end-to-end connection between the mobile application and the target application. For example, if the application is enabled for certificate-based authentication (PKI) and requires the user's certificate you can authenticate the user directly.

About Idenprotect
Idenprotect is the first all-in-one password-free authentication, single sign-on and identity platform for organisations. Leading organisations use Idenprotect to improve security, meet regulatory mandates and reduce complexity and costs. It eliminates the hacker's #1 target—the password—to protect against fraud, phishing and credential theft, it makes employee access and customer payments and transactions more secure. It can be deployed quickly and promises a much better user experience