idaptive

Idaptive Multi-factor Authentication Services

Adaptive Strong Authentication Across All Your Identities and Resources

Passwords alone are not enough to verify a user's identity and protect businesses from data loss, fraud and malicious attacks. Login credentials are more valuable than ever, as companies adopt more cloud applications, services and infrastructure. Multi-factor Authentication (MFA) makes it harder for attackers to get in. Idaptive's MFA capabilities provide additional layers of security, and helps protect organizations against the leading cause of data breaches — compromised credentials — with minimal impact to users.

Relying on simple username and passwords for authentication is not enough to protect critical applications and endpoints that house sensitive business data. In fact, passwords are now considered security's weakest link — especially in today's cloud and mobile-enabled world.

Multi-factor authentication (also referred to as MFA) strengthens security by requiring users to provide extra information or factors unique to what the user knows, is or has.

Many organizations think that standalone MFA products can better secure their organization's resources and mitigate the risk of data breaches. They may implement MFA for a specific set of applications or for a particular group of users like employees that have VPN access. But applying MFA for only certain apps or users still leaves your organization exposed.

Attackers are relentless. They hunt, phish, spear phish, scam, and social engineer end users to infiltrate your organization. Once inside they look for opportunities to elevate privilege and appropriate resources.

Implementing adaptive MFA across every enterprise user (internal, or external) and resource (applications and endpoints) can thwart attackers at multiple points in the attack chain. By limiting the usefulness of any compromised credentials that attackers may have acquired or created, MFA restricts their ability to move laterally within the organization.

Idaptive helps enterprises bolster security against attacks based on compromised credentials with adaptive MFA across enterprise identities and resources. Idaptive's adaptive MFA capabilities enable organizations with the ability to enforce strong authentication with a broad choice of authentication factors.

Adaptive Authentication

Stronger security is good, but not if it gets in your users' way. Traditional MFA is either "on" or "off", which results in constant prompting for an additional factor and annoyed users. Organizations need stronger, smarter and risk aware security controls to identify and take action on risky authentication activity.

With Idaptive's analytics and machine learning engine, access control policies to applications and endpoints and can be configured to allow SSO access to a resource, challenge the user with MFA or block access entirely. Define when to challenge users with MFA based on pre-defined conditions such as location, device, day of week, time of day and even risky user behavior.

Flexible Authentication Methods

Organizations require a choice of authentication methods to make MFA as painless and easy as possible to use.

The Idaptive Next-Gen Access Platform provides flexibility to choose from a comprehensive range of authentication methods. Choose from push notification to a mobile device; a soft OTP token generated by the Idaptive mobile app, SMS/text message or email; interactive phone call, security questions, existing OATH-based software or hardware tokens, FIDO U2F security keys, and Smart Cards, including derived credentials. Enterprise get the protection they need without sacrificing the convenience their users demand.

MFA Use Cases

SECURE APPLICATION ACCESS

Employees demand anytime, anywhere access to applications in the cloud, on mobile devices, and on-premises. As the number of applications grow, so do the number of passwords. These passwords are often weak, re-used across apps, and shared among employees. This password sprawl increases risk, and makes strong authentication critical to protecting against data breaches and unauthorized access.

Idaptive Application Service™ helps mitigate password risk. It simplifies and secures access to applications with adaptive MFA and conditional access controls integrated with SSO using federation standards like SAML.

SECURE VPN ACCESS

Today's mobile and remote workforce needs secure access into their organization's systems, applications and networks. VPNs are one way companies provide that access, by establishing an encrypted connection, or "tunnel" between a remote endpoint and the internal network. But any external connection that is permitted to access resources behind the firewall poses a significant security risk. A number of high profile data breaches started with attackers compromising VPN credentials, allowing them access to an organization's internal systems.

Idaptive reduces VPN risk with MFA enforcement on any VPN client that supports RADIUS, which include Cisco, Juniper Networks and Palo Alto Networks. Enforcing MFA for VPN access allows organizations to give employees and partners secure remote access to their corporate network, on-premises applications and resources.

To further reduce remote access risk, Idaptive provides secure, per-app, encrypted connections via an on-premises App Gateway. When combined with MFA, users get simple, secure access to specific on-premises apps, without full network access.

SECURE TO & FROM ENDPOINTS

Idaptive also ensures access is limited to authorized users with multi-factor authentication at the endpoint login screen through flexible options such as mobile authentication, smart cards and OTP tokens. With Idaptive, you can not only secure access to endpoints, but also enable unified management across all endpoint management platforms, providing a single pane of glass for policy and management of all end user devices.

FEATURED HIGHLIGHTS

Adaptive MFA Everywhere

Bolster security all users and protect a broad range of enterprise resources — cloud and on-premises apps, workstations, VPNs, network devices, servers and more.

Broad Authentication Methods

Provide the broadest choice of authentication methods to make MFA as painless and easy to use.

Risk Aware Methods

Through a combination of analytics, machine learning, user profiles, and policy enforcement, enforce access decisions based on user behavior in real time.

Idaptive delivers Next-Gen Access, protecting organizations from data breaches through a Zero Trust approach. Idaptive secures access to applications and endpoints by verifying every user, validating their devices, and intelligently limiting their access. Idaptive Next-Gen Access is the only industry-recognized solution that uniquely converges single single-on (SSO), adaptive multi-factor authentication (MFA), enterprise mobility management (EMM) and user behavior analytics (UBA). With Idaptive, organizations experience secure access everywhere, reduced complexity and have newfound confidence to drive new business models and deliver kick-ass customer experiences. Over 2,000 organizations worldwide trust Idaptive to proactively secure their businesses. To learn more visit www.idaptive.com.

Ready to learn more?

Please contact us at hello@idaptive.com