idaptive

Idaptive Mobile Device and Endpoint Services

Secure Access Everywhere

Traditional measures of security are clearly not sufficient for today's new world. The sophistication and scale of cyber-attacks is unlike any previous era. With 81% of breaches originating from compromised credentials and 95% of phishing attacks followed by malicious software installation, it is time to ensure your endpoints are integrated with your identity and access management strategies. As devices are gateways to company data and resources, it is imperative that one only allow access to corporate resources from trusted endpoints.

Fragmented Identity Management Across Endpoints

Today's IT landscape demands a mixture of company-owned and user-owned devices, as well as desktop and mobile operating systems. The list of Windows, Mac, iOS and Android endpoints used to access corporate resources is anything but static and more devices are being used off the corporate network. Traditional on-premises management practices are no longer practical and IT needs to take a cloud-based approach when managing identity, authentication and policy enforcement for Windows, Mac, and mobile devices, enabling rapid identity consolidation while ensuring uniform security.

INCONSISTENT SECURITY POLICIES

With BYOD policies firmly entrenched within enterprise, users are bringing their own smartphones, tablets and laptops into the workplace. Enforcing security and configuration policy across all your endpoints to meet your security requirements is key. Deploy best practices for firewall settings, inactivity and screensaver lock settings, disk encryption and certificate management — providing consistent preventative security controls across all endpoint platforms.

DEVICE POSTURE AND CONTEXT

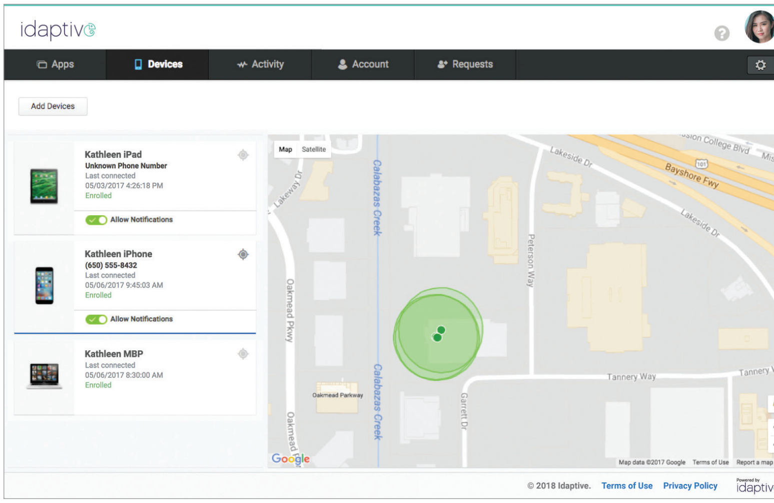
If an organization truly wants to enforce secure access, then it must have a means of determining whether an endpoint should be trusted. Limit access to company data through policy rules that define circumstances based on identity assurance and device posture. Allow access to applications from trusted corporate and BYOD devices while challenging MFA or blocking access from untrusted public devices.

A Zero Trust Security Approach

Idaptive Mobile and Endpoint Services leverages a zero trust approach to secure and manage users' access to applications from any device, based on user and device context and behavior analysis. It uses endpoint posture such as location of device, browser, or OS to provide secure access and prevents data from being accessed from devices that aren't trusted nor managed. With Idaptive, you can enable unified management across all endpoint management platforms, providing a single pane of glass for policy and management of all end user devices.

Adaptive MFA To and From Endpoints

Endpoint Services also ensures access is limited to authorized users with multi-factor authentication at the endpoint login screen through flexible options such as mobile authentication,



Kathleen iPad
Unknown Phone Number
Last connected
05/03/2017 4:26:18 PM
Enrolled
Allow Notifications

Kathleen iPhone
(650) 555-8432
Last connected
05/06/2017 9:45:03 AM
Enrolled
Allow Notifications

Kathleen MBP
Last connected
05/06/2017 8:30:00 AM
Enrolled

© 2018 Idaptive. Terms of Use Privacy Policy Powered by idaptive

Through a unified view, IT can manage endpoints and set policies for how apps are accessed.

©2019 Idaptive. All Rights Reserved.

smart cards and OTP tokens. With Idaptive Mobile and Endpoint Services, 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.

An Identity-Centric Approach to Securing Endpoints

Idaptive enables IT to allow access to apps only from trusted and secured endpoints while users get single sign-on across cloud and mobile apps from any device. Through a unified view, IT can manage endpoints and set policies for how apps are accessed.

SECURITY

- Leverage endpoint posture (location of device, browser, or OS) to provide secure access
- Ensure access to data is safe through full EMM features and integrated SSO including remote locate, lock and wipe capability across mobile devices and endpoints
- Implement a secure BYOD policy with Idaptive's integrated Mac and mobile device management. Secure the Idaptive app on mobile devices by unlocking with NFC, PIN, passcode or fingerprint
- Comply with regulations that mandate Smart Cards and enable new, secure mobile use cases with derived credentials for Smart Card access to mobile apps, sites and services

SIMPLICITY

- Unified Endpoint Management across all endpoint platforms including Windows, Mac, iOS and Android devices
- Common policy mechanism tied to application access thereby simplifying the decision-making process of who can access what from where
- Easy-to-use, cloud-based management
- Extend enterprise authentication services to the cloud without replicating identities

CONTROL

- Combine identity assurance and endpoint security posture to control access to apps and corporate resources when identity-centric conditions are met
- Enforce user policy from a single authoritative source, applied across devices, apps, and locations
- Cloud-based policy enforcement for remote BYOD, corporate laptops & mobile devices from non-compliant devices through role-based access controls

FEATURED HIGHLIGHTS

Mobility Management

Manage devices, secure rich mobile applications, and leverage device context for smarter access decisions.

Device Security Management

Control endpoint security posture with policy and configuration management ensuring consistent preventative security.

Strong Authentication

Enforce strong authentication via smart cards and derived credentials. Comply with security regulations without compromising device support.

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.

Multi-factor authentication at Endpoint functionalities will require Idaptive Multi-factor Authentication SKU.

Ready to learn more?

Please contact us at
hello@idaptive.com

©2019 Idaptive. All Rights Reserved.