onelogin

PRODUCT DATASHEET

OneLogin Adaptive Authentication

COMBAT PHISHING & ACCOUNT COMPROMISE
BALANCE USABILITY AND SECURITY

Next-Generation Multi-Factor Authentication Powered by Machine Learning

There is no denying the increasing volume of cyberattacks - particularly attacks that attempt to compromise accounts. As shared in the 2017 Verizon Data Breach Investigations Report, 81% of hacking-related breaches leveraged either stolen and/or weak passwords.

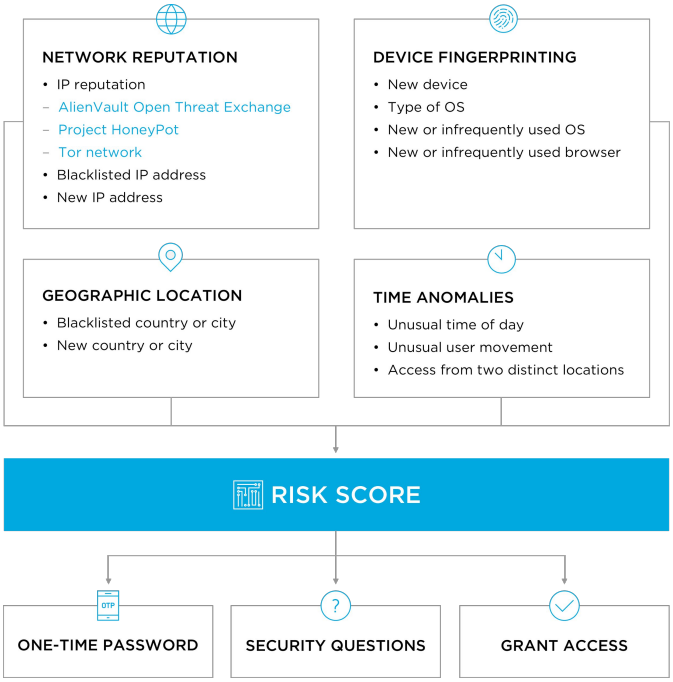
Multi-factor authentication has emerged as a common solution to protect credentials, and by extension, accounts. However, conventional multi-factor authentication solutions present their own set of challenges, as they are 1) difficult for IT staff to configure, operationalize and deploy across a broad portfolio of applications, 2) burdensome to end-users, often requiring users to carry an additional physical device or enroll a personal device in a corporate program, or 3) limited to static enforcement capabilities applied in a blanket fashion, whereby low-risk users are frequently challenged with unnecessary MFA requests despite exhibiting zero risk factors. These challenges often discourage IT teams from rolling out MFA solutions, create annoyances for end-users or even encourage circumvention.

OneLogin Adaptive Authentication

As an Identity-as-a-Service (IDaaS) solution, OneLogin has a unique vantage point, with insight into a wide range of relevant intelligence when an individual attempts to log in, including not only basic information such as geographic location, but more revealing factors, such as network reputation and device fingerprint.

With OneLogin Adaptive Authentication, we enable analysis weighing a wide range of elements to determine a user risk score. Should the risk score cross a specified threshold, OneLogin is able to enforce step-up authentication and demand an additional factor for security.

Conversely, if the user is exhibiting low risk behavior, such as login from a typical location, on a known device, at a similar time of day (and so on), then OneLogin will not require an additional factor for improved usability.



OneLogin Adaptive Authentication weighs a wide range of variables to determine a user risk score and modify authentication requirements accordingly.

Why OneLogin Adaptive Authentication?

- Combat phishing and account compromise with intelligent multi-factor authentication
- Improve the user experience for low risk users
- Extend the value of existing MFA factor / solutions such as Duo Security, RSA SecurID, Google Authenticator, and more

"I love OneLogin because it allows me to enforce two-factor authentication on pretty much any application."

Matt Thorne, HEAD OF IT at PINTEREST

Over 2,000 enterprise customers globally secure their applications with OneLogin

AAA AIRBUS pandora Steelcase STITCH FIX zendesk

Unlock the Power of Machine Learning

Conventional MFA solutions driven by static rules lack the adaptability and enforcement granularity to optimally balance usability and security. A user on the corporate network should not automatically be trusted. What if the access pattern is atypical, or the device or OS has not been seen before? Conversely, a remote worker at their home office should eventually be trusted if they consistently exhibit identical behavior. OneLogin Adaptive Authorization employs machine learning to profile user behavior over time to build an understanding of typical access patterns - and dynamically enforce additional or fewer authentication requirements based on real-time risk scoring.

Assessing Risk: All Things Considered

OneLogin Adaptive Authentication users machine learning which analyzes a broad range of inputs to calculate risk scores and subsequently determine the most appropriate security action. Elements analyzed include:

- **Network Reputation**, including IP reputation, whether an IP address is new or blacklisted, and references threat intelligence resources including the AlienVault Open Threat Exchange, Project HoneyPot, and known Tor network nodes
- **Geographic Location**, including blacklisted geographies or a new country or city
- **Device Fingerprinting**, including whether or not the device has been seen before, the OS type, if the OS is new or atypical, and if the browser is new or atypical
- **Time Anomalies**, including whether or not the time of day is unusual or if there is simultaneous / rapid access from geographically disparate locations

OneLogin Protect as an Additional Factor

Users often find one-time password solutions to be a nuisance due to usability considerations. OneLogin protect removes friction from multi-factor authentication by letting users simply respond to a push notification on their smartphone or even smartwatch during the login process. OneLogin protect is available on the Apple and Android app stores and works for BYOD as well as company-owned devices.

We play nicely with others, including your 2FA

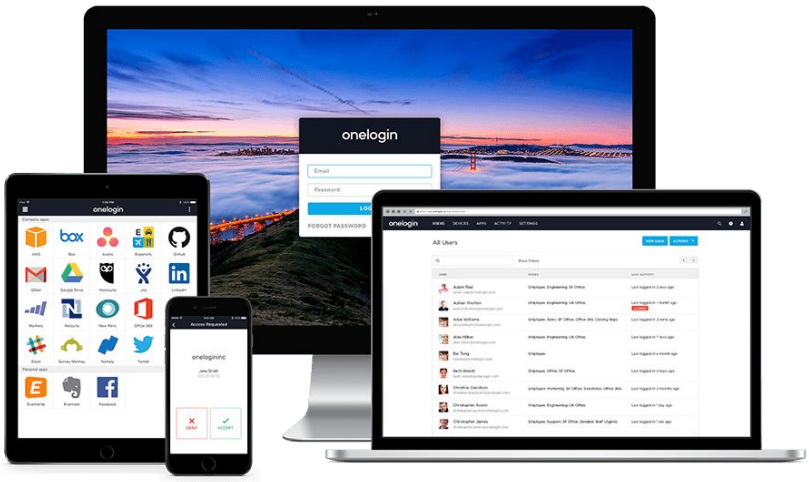
OneLogin Adaptive Authentication integrates with a number of third-party authentication providers, including Duo Security, RSA, Yubico, Symantec, Google Authenticator, SafeNet, Vasco, FireID, and Swivel Secure.

No existing MFA solution? No problem.

One-time passwords may also be sent over SMS. Alternately, security questions can be used as an additional authentication factor for sign-in and password reset. OneLogin comes with dozens of standard questions that are available in over 20 languages.

Cloud-Based Identity and Access Management with OneLogin

OneLogin is the Identity-as-a-Service (IDaaS) solution that enables quick and secure access to applications from anywhere, on any device, through Single Sign-On (SSO). Technology leaders at innovative organizations like Airbus, Uber, and Zendesk choose OneLogin to accelerate cloud application adoption and rollout, enhance user productivity, increase IT efficiency, reduce costs, and reduce security and compliance risk. Unlike other Identity and Access Management solutions, OneLogin enables you to:



- Accelerate cloud application rollout by integrating user directories and automating user onboarding and offboarding
- Remove obstacles to deploying Single Sign-On for employees, partners, and contractors with a catalog of over 5,000 pre-integrated apps
- Improve IT team efficiency and substantially reduce tactical workload through automated identity workflows that scale with the dynamic nature of your business
- Make it easy for all users, including employees, partners, and customers, to access all apps through one portal with one secure password, from any location or any device at any time
- Add adaptive multi-factor authentication powered by machine learning to your apps to dynamically respond to anomalous behavior and protect against security threats, including phishing, account compromise, and data theft