onelogin
by ONE IDENTITY

OneLogin SmartFactor Authentication

Prevent cyber attacks with context-aware adaptive authentication

Overview

With cyber attacks on the rise, it's more important than ever to defend against phishing and account compromise. The Verizon 2022 Data Breach Investigations Report indicated that nearly 50% of breaches involve the use of stolen credentials[1]. Although Multi-Factor Authentication (MFA) has emerged as a common tool to protect user credentials and sensitive company data, traditional solutions create annoyances for end-users and negatively impact productivity.

OneLogin SmartFactor Authentication™

SmartFactor Authentication uses risk insights from One Identity's OneLogin Vigilance AI™ to automatically configure login flows and determine whether to prompt users for MFA, balancing security with usability. Login attempts with elevated risk scores are required to provide additional authentication factors or denied access entirely, while lower risk logins are prompted with fewer requirements or bypass MFA altogether.

> **Security is incredibly important for us here at Virgin Hyperloop One and OneLogin made us very comfortable with securing all of our intellectual property. We use it on all of our applications.**
>
> *Dawn Armstrong, Director of IT*
> *Virgin Hyperloop One*

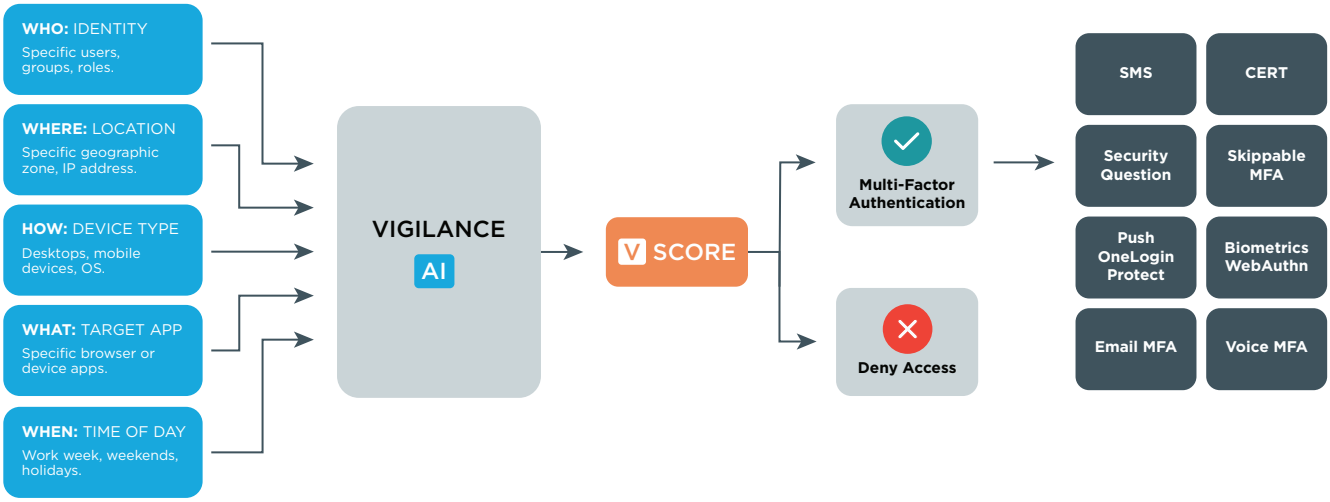
Key benefits

- **Combat phishing and account compromise** - Intelligent MFA requires users with high-risk login attempts to use other factors, such as the OneLogin OTP mobile app, SMS, or voice, as an additional layer of security.
- **Enable device-anywhere access** - Enforce authentication policies across corporate-owned or "bring your own" devices –all of which have different operating systems and, therefore, varying security vulnerabilities. Protect remote workers and "road warriors" whose user behavior may change on a daily basis.
- **Gain visibility into new login attempts** - Provide not only security and convenience, but also a compliance and reporting benefit by streamlining login events in real time to SIEM and other cloud communication tools to meet audit requirements.
- **Improve the user experience for low-risk users** - For users that exhibit minimal or zero risk factors, OneLogin can eliminate the requirement for an additional factor or bypass MFA to improve convenience when security confidence is high.
- **Extend the value of your existing MFA** - The OneLogin solution integrates with other multifactor authentication providers so you can layer SmartFactor Authentication **for even stronger MFA.**
- **Supported MFA providers include:**
  - Yubico
  - RSA
  - Duo Security
  - Symantec
  - Google Authenticator

1 Verizon Data Breach Investigations Report, May 2022, Verizon

How does SmartFactor Authentication work?

SmartFactor Authentication uses insights from the Vigilance AI risk engine to analyze a broad range of inputs, such as location, device, and user behavior, to calculate a risk score and determine the most appropriate security action to take for each login attempt.



OneLogin Functionality Includes:

Vigilance AI™ Threat Engine	OneLogin's proprietary risk engine uses machine learning to understand typical access patterns and dynamically enforce additional or fewer authentication requirements based on real-time risk scoring. Behavioral inputs include network & IP reputation, device fingerprinting, time anomalies, and known malicious activities used to hide identity (e.g. Tor browsers).
Smart Flows	Select the appropriate login flow for different sets of users based on standard, brute-force, or passwordless needs. Provide a secure, robust login experience that utilizes biometrics for mobile applications.
Smart MFA	Adjust MFA based on risk threshold to simplify login for low-risk attempts and step-up authentication for high-risk ones. Reduce support calls and the costs associated with transactional MFA (e.g. SMS, voice).
Smart Access	Restrict access based on location of user or if they have exhibited an unusual pattern of behavior for reduced threat exposure.
SMS Authentication	Instead of contacting the IT helpdesk, users can use a one-time password sent to their phone via SMS to authenticate and reset their own password via OneLogin's intuitive web interface.
Voice MFA	As an alternative to SMS or email, voice MFA allows users to receive a phone call to their mobile phone voice MFA or landline, verifying their identity to the OneLogin Portal.
Compromised Credential Check	Protect from password reuse attacks and automatically detect credentials that are compromised by a third-party data breach during password change and password reset.
Third-Party Integrations	OneLogin works with your existing third-party authentication provider to prompt users with high risk login attempts to submit additional factors. Stream events in real-time directly to SIEM or integrate with your existing CASB solution for User & Entity Behavior Analytics (UEBA) capabilities.

To learn more about OneLogin's SmartFactor Authentication, visit https://www.onelogin.com/product/smartfactor-authentication

onelogin by ONE IDENTITY