onelogin

PRODUCT DATASHEET

OneLogin SmartFactor Authentication™

Prevent Threats with Context-Aware Adaptive Authentication

With cyber-attacks on the rise, it's more important than ever to defend against phishing and account compromise attacks. The Verizon 2019 Data Breach Investigations Report indicated that 29% 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 may even encourage circumvention.

OneLogin SmartFactor Authentication™

SmartFactor Authentication uses risk insights from Vigilance AI™ to dynamically adjust authentication requirements in real-time. Login attempts with elevated risk scores are prompted for multi-factor authentication, denied access to particularly sensitive applications, or denied access to the portal entirely.

Key benefits of SmartFactor Authentication

Combat phishing & account compromise

Intelligent MFA requires users with high-risk login attempts to use other factors, such as OneLogin's OTP mobile app, SMS, or security questions, 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 altogether to improve convenience when security confidence is high.

Extend the value of your existing MFA

OneLogin integrates with other multifactor authentication providers to empower you to layer SmartFactor Authentication for even stronger MFA. Supported MFA providers include:

- Yubico
- RSA
- Duo Security
- Symantec
- Google Authenticator

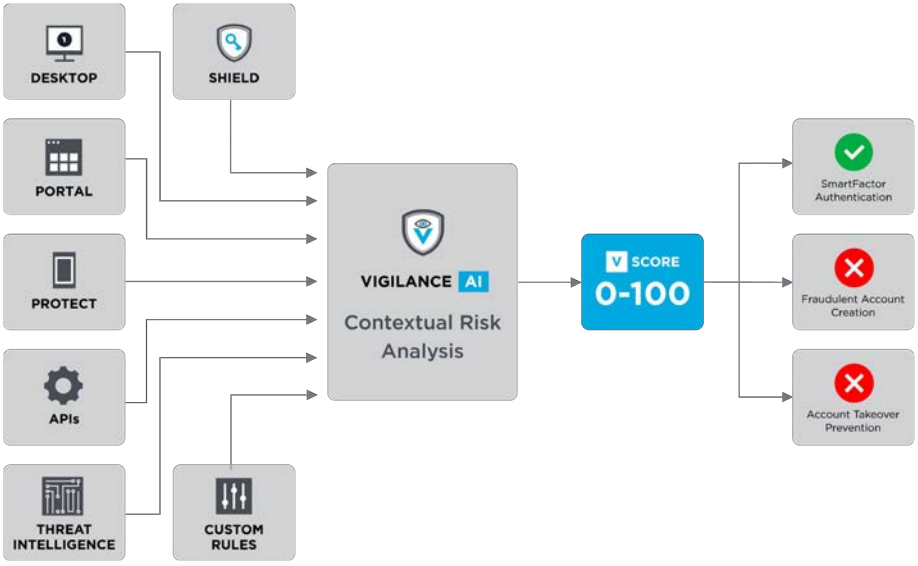
"After thorough research, OneLogin stood out amongst its competitors. Not only did its local presence appeal to us, but it could deliver an effective replacement for the two-factor authentication (2FA) solution we had in place."

NEIL DAVISON | IT Director, Farrer & Co

1. Verizon Data Breach Investigations Report, May 2019, Verizon

How does SmartFactor Authentication work?

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



OneLogin Functionality Includes:

Single Sign-On (SSO)	OneLogin uses SSO protocols SAML, WS-Fed and OpenID Connect to allow customers to sign into applications without using a password. If your online portal consists of multiple, discrete applications, end-users have a streamlined, seamless user experience.
Machine Learning	OneLogin's machine learning engine profiles 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.
Behavioral Inputs	OneLogin comes up with a risk score to determine the most appropriate security action by analyzing several elements including network & IP reputation, device fingerprinting, geographic location, time anomalies as well as known malicious addresses and techniques used to hide identity (e.g. Tor browsers).
SMS Authentication	Instead of contacting the IT helpdesk, users can use a one-time password sent to their phone via SMS to authenticate and to reset their own password via OneLogin's web interface.
Security Questions	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 20+ languages.
Compromised Credential Check	OneLogin can automatically detect credentials that are compromised by a third-party data breach. This occurs during password change and password reset (forgot password).
App/User Policies (Deny)	Leverage user behavior knowledge to deny access to users with risky logins, reducing threat exposure. Ensure valid access to sensitive applications and financial information for best business practices.
Third-Party Integrations	OneLogin integrates with a number of third-party authentication providers and can prompt users with high risk login attempts to submit a second factor. Stream events in real-time directly to SIEM and cloud communications tools. OneLogin also features a tight knit integration with your existing CASB solution for User & Entity Behavior Analytics (UEBA).

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