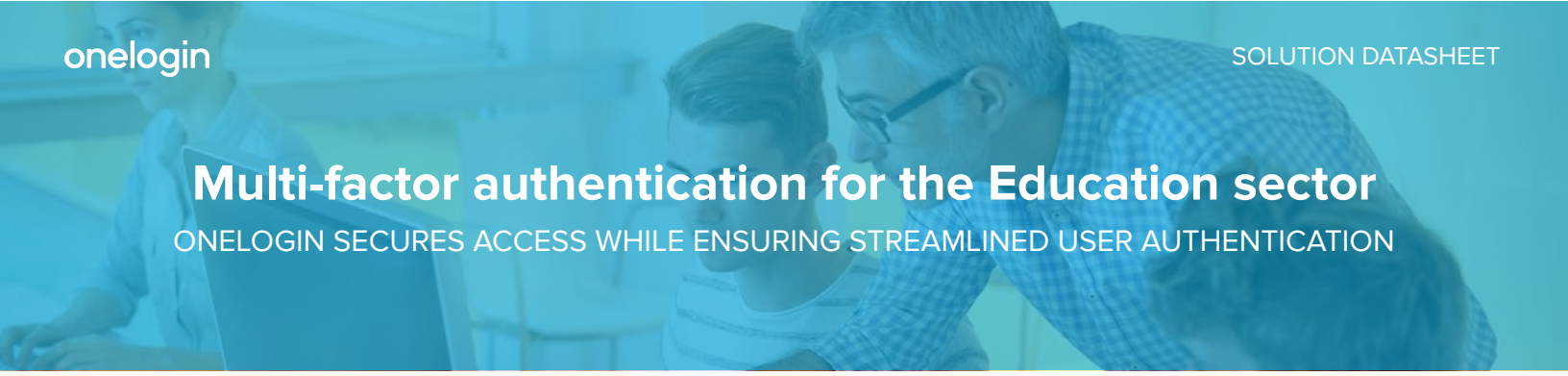
onelogin

SOLUTION DATASHEET



Multi-factor authentication for the Education sector

ONELOGIN SECURES ACCESS WHILE ENSURING STREAMLINED USER AUTHENTICATION

Multi-factor authentication and adaptive authentication in the Education sector

Reducing the number of passwords is a great first step to improving security. But it's not enough. It only takes one stolen password to crack your school open to cyber attack. And the cost of a breach can be high, with an average cost of $148 per record and ransomware demands in the millions.

You can't rely just on passwords. Multi-factor authentication (MFA) adds an extra level of security by requiring users to respond to a challenge in order to authenticate. Modern MFA is easy and fast for users—which is why schools are moving quickly to match other industries by implementing MFA.

Challenge: Prevent account compromise

- 25 percent of employees use the same password for all accounts. And 59 percent reuse passwords on work and personal accounts.
- 81 percent of hacking-related breaches use stolen and/or weak passwords.
- 38 percent of successful phishing attacks result in compromised accounts.

Challenge: Meet cybersecurity requirements

- Cyber insurers are beginning to expect and even require MFA. Soon, most will require MFA for the best rates.
- Many schools now seek to comply with the GLB Act, which requires NIST 800-171 compliance. MFA is key to meeting the NIST 800-171 guidelines.

Challenge: Do it all without adding friction

- You need security, but can't sacrifice streamlined processes for student applications, registrations, or other services
- In a competitive environment, impressions matter. How you deliver services can make the difference in whether students and parents select your school.
- Barriers to registration, payment, and other services can literally cost you.

Solution: Multi-factor authentication with OneLogin

When users try to login by entering a username and password, OneLogin's multi-factor authentication challenges them with a push notification. Users can respond by simply clicking a button on their device. No need to hunt down a PIN.

OneLogin MFA:

- Let's users respond via the app they want and that you approve, such as OneLogin Protect, Duo Security, Google Authenticator, or the built in biometric authentication on their laptop.
- One-click authentication with OneLogin Protect. And enforce restrictions such as requiring a lock screen or prohibiting jail-broken devices.
- Provides one-click registration via a QR code.

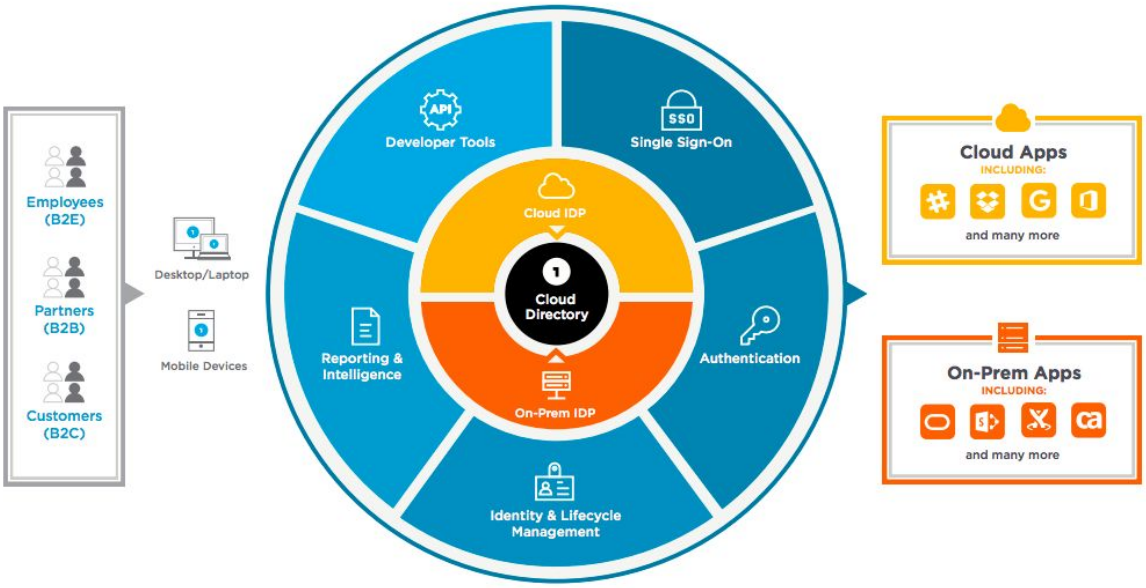
Solution: Adaptive authentication with OneLogin

For an even more secure and streamlined experience, add adaptive authentication. Using machine learning, OneLogin builds a profile of each user based on information such as where the user logs in from, common times of day, common devices, and more.

Each login attempt is then checked against the user's risk profile. High-risk login attempts are prompted for additional factors while low-risk logins can proceed with no challenge.

"The product was very easy to install and integrate into our environment while proving a sophisticated secure solution with an easy to use interface. Our staff and students have adopted with little difficulty."
- Tony Casciotta, CIO and VP of IT, Broward College

The OneLogin Unified Access Management Platform



Multi-factor authentication: How it works

OneLogin Protect provides a streamlined multi-factor authentication solution that increases security without slowing down users. OneLogin MFA includes:

- Simple registration via a QR code
- Push notifications for fast authentication
- Backup and restore in the event of a lost device
- Ability to verify device hygiene

Registration is easy. Students, alumni, and others just install OneLogin Protect and scan the QR code.

OneLogin uses push notifications to ensure fast authentication. When a student, alumni, or employee tries to log in to an application, OneLogin challenges the user.

On a biometric-enabled laptop, the user verifies on the laptop with his or her biometrics. On a mobile device, the user simply presses a button. If required, the user verifies on the device with biometrics, as well. OneLogin MFA supports many providers, including: OneLogin's own mobile app, OneLogin Protect for iOS and Android, Webauthn, Duo Security, Google Authenticator, and more.

With OneLogin Protect, you can set restrictions on the user's device for added protection, including blocking devices that have been jail-broken and requiring users to have a lock screen. And, in the event a user's device is lost or stolen, they can restore their MFA settings on a new device via OneLogin's backup and restore feature.