Semperis: Enforcing Phishing-Resistant Authentication at Scale with Passkeys

The Challenge

As a cybersecurity company serving government agencies and Fortune 2000 enterprises, Semperis understands what a credential-based attack looks like. Like many, the company has seen phishing attempts against its own employees, and realized that its authentication environment left a path open for exactly that kind of attack.

Before committing to passkeys, Semperis employees could choose from several authentication methods depending on their device, and nothing in policy forced them toward the strongest one. Windows devices used Windows Hello for Business. Mac users authenticated through platform SSO connected to Entra. Mobile users authenticated via Microsoft's passwordless push notifications, the number-matching variant that is convenient but not phishing-resistant. When any of those methods were inconvenient, employees could fall back to username, password and OTP.

Conditional access in Entra nudged users toward stronger methods, but nothing prevented someone from clicking "sign in another way" and choosing something weaker.

Semperis always required some form of MFA, but the weakest permitted path was still vulnerable to adversary-in-the-middle attacks. For a company whose business is identity security, that gap was increasingly hard to justify.

Why Passkeys

As the company was looking to reduce its own potential attack surface, it looked to a better form of phishing resistant strong authentication: passkeys.

Semperis was already building incident response products that required passkeys as the authentication method, on the basis that secure operations demand phishing-resistant credentials. As this progressed, on the operations side Semperis reflected on its own desires to enforce passkeys for the workforce, and shifted priority to realize this goal.

Passkey technology has matured significantly, making it a viable option for Semperis. Device-bound passkeys had become a reliable option within the Microsoft ecosystem, which is where Semperis runs its identity infrastructure. The company did not evaluate third-party identity providers; staying within Entra was a deliberate decision. When the technology reached a workable state, the timing aligned with leadership's appetite to act.

semperis

Semperis is an identity security company founded in 2013 and headquartered in Hoboken, New Jersey, with approximately 600 employees across North America, Europe, APAC and Israel. The company's platform protects Active Directory, Okta and Entra ID environments for government agencies and Fortune 2000 enterprises, covering threat detection, incident response and directory recovery.

> ***"We're a prime target for attacks,"***
>
> said Eric Woodruff, Chief Identity Architect at Semperis.

Implementation

Semperis built its passkey deployment entirely within Microsoft Entra, with no third-party identity providers in scope. The resulting architecture is tiered by user type:

General workforce.

Device-bound passkeys were enforced through conditional access policies in Entra for all users, with guest accounts excluded because Entra does not currently support passkey enrollment for guests. Windows users continued using Windows Hello for Business, which delivers equivalent native phishing-resistant authentication on Windows. Mac users remained on Mac Platform SSO, which similarly provides native phishing-resistant authentication on macOS. In addition, Semperis made FIDO-certified hardware security keys available to any employee who requested one, and a small number of employees chose to use them.

Privileged users.

Device-bound passkeys enforced through conditional access, mirroring the general workforce policy with one key difference: Temporary Access Pass (TAP) is not permitted for privileged accounts. This includes account recovery scenarios, where TAP is otherwise allowed for general workforce users.

Super-privileged and break-glass accounts.

Passkeys bound specifically to FIDO-certified hardware security keys. Privileged users may also authenticate with Windows Hello for Business from a Privileged Access Workstation, with a FIDO2 security key as a backup method.

Understanding synced vs bound passkeys

- **Synced passkey:** stored securely in a credential manager and accessed across devices (mobile phones, tablets, and computers)
- **Device-bound passkey:** bound to and used only on a single device (such as a security key or mobile app)

Learn more at passkeycentral.org

Deployment

IT and cloud platform teams adopted passkeys first, giving the teams time to build documentation, surface edge cases and develop a process before expanding to less technical groups.

Enrollment happened live.

The implementation team joined existing team meetings, asked for five to ten minutes, walked attendees through setup and had them enroll on the spot. The team also used a targeted adoption strategy to focus on departments and teams with slower uptake. Once a group reached strong adoption, remaining team members were more likely to follow, so the implementation team created a simple near-real-time BI report to monitor adoption and identify where additional outreach would have the greatest impact.

Groups initially received two weeks' notice before enforcement.

That window shortened to one week as confidence grew, and by the end some groups enrolled and were enforced the same day. Email communication was less effective than desired; a campaign on Teams with built-in deadlines would have driven enrollment more effectively, but the idea surfaced too late to be worth building.

Edge cases.

Although most use cases were straightforward, two categories required exceptions.

- **Older Android devices.** A subset of employees was running Android 13, which does not support device-bound passkeys. Those users were removed from enforcement temporarily while management worked out a path forward. Initial plans were to keep an enforcement exclusion, but the release of synced passkeys in Entra ID enabled Semperis to enforce passkey use for these users by leveraging their ability to use a synced passkey with Google Password Manager.
- **Unsupported mobile applications.** Four applications used authentication flows that bypassed the native browser libraries Microsoft requires for passkey support. Those applications received conditional access exceptions for passwordless push notifications instead. Users of those apps occasionally got caught in what the team called "the doom loop": Entra prompted for a method that failed conditional access, redirected the user to a registration page, confirmed completion, then sent them back to authenticate again. The cycle repeated indefinitely until the team added an application-level exclusion. Semperis continues to monitor vendor passkey support and removes exceptions as applications add support. One widely used mobile app made that shift in the months following the rollout.

The Human Factor

The complexity of Semperis's rollout was almost entirely behavioral, not technical.

Two questions came up repeatedly: whether enrolling a passkey meant giving Semperis access to employee biometric data, and whether adding a passkey to the Microsoft Authenticator app on a personal device would give the company visibility into the phone. The second concern was notable given that employees already had the Authenticator app installed on those same phones.

What also emerged was the fact that the convenience benefits moved more people towards accepting the change than security benefits did. Some employees would still use a username + password, despite having options for passwordless push, and subsequently would go through SSPR flows at times when they couldn't remember their password. Letting them know that the new approach eliminated the need to use or know their password landed differently than explaining phishing resistance.

> ***"One of the biggest things with employee buy-in was explaining that, for the most part, they were not going to have to remember passwords anymore," Michal Sinak, Cybersecurity Engineer, Semperis said. "That, honestly, was a big thing."***

The team built a documentation library on the company's internal intranet: scenario-specific, screenshot-heavy and built around actual Semperis flows, with internal branding and mascots throughout. This resource was heavily leveraged throughout the rollout and onboarding process. New employees start with a Temporary Access Pass and are directed to the intranet resources to complete passkey enrollment, and that process has worked well in practice.

Passkey Impact

Semperis reached 100% adoption among full-time employees, and has extended enrollment to contractors and vendors with accounts in the Entra tenant.

The volume of phishing attempts directed at Semperis has not declined since the rollout, which the security team expected. The vast majority of what arrives is still credential phishing: attempts to capture usernames and passwords.

Passkeys changed the team's response posture toward those attempts.

> ***"We kind of glance at it and go, you're doing basic credential phishing, which is less concerning now," Sinak said. "We're thinking more about things like session theft these days than we are worried about credential theft."***

There is still room to go, as certain types of attacks, like authentication downgrade attacks, will attempt to trick users into entering their password, even if they ultimately cannot authenticate with it. Semperis's long-term goal is an environment in which employees don't know or remember their password, which will effectively be a random set of data within the password attribute in Entra. The ultimate goal is that employees will find it really odd if they are asked for their password.

Key Recommendations

The Semperis deployment offers a set of lessons for organizations working through a similar rollout.

Enroll live, not by email.

Joining existing team meetings and walking employees through setup on the spot drove adoption far more effectively than email campaigns. Most employees enrolled without issue once shown how.

Set a deadline and enforce it.

Voluntary adoption stalls without a hard cutoff. Shortening enforcement windows as confidence grew accelerated the final phases significantly.

Lead with convenience, not security.

For the general workforce, the most effective message was that they would not need to remember or reset passwords anymore. Security benefits were secondary to most employees.

Budget for culture change.

The technical implementation was straightforward. Sustained reassurance, in-person sessions and internal champions took more time and effort than expected.

Build documentation for your environment, not the platform.

Generic vendor resources read as consumer tools to workforce users. Scenario-specific, internally branded documentation performed better and required ongoing maintenance as vendor UIs changed.

Enforce passkeys as the only option.

The availability of weaker fallback authentication gives attackers a path to exploit. Conditional access policies that permit no weaker alternative make phishing resistance real.

Test across platforms.

Passkey enrollment is phone-heavy and platform-specific. A small investment in test devices gives architects and engineers direct exposure to what users will encounter, and makes it easier to document and support those flows accurately.

Enable passkeys everywhere.

As passkeys become a familiar part of the user experience, make sure every new product introduced into your environment supports them to preserve a seamless, phishing-resistant authentication journey.

Closing the Gap Between Product and Practice

With the adoption of passkeys, Semperis now ships incident response products that require the same phishing-resistant authentication its own workforce uses daily. The gap between what the company sells and how it operates internally has closed.

The deployment succeeded on the strength of a clear mandate from leadership, sustained enrollment sessions across dozens of team meetings, documentation specific to the Semperis environment, and a conditional access policy that removed weaker fallback options entirely.

Semperis is evaluating synced passkeys for general workforce use to reduce the re-enrollment burden when employees upgrade devices, and plans to scramble remaining Entra passwords and disable self-service password reset for enrolled users, closing the residual exposure from credentials that may exist in shadow IT systems outside of SSO.

> ***"Without actually enforcing a passkey, or something phishing-resistant as your only option, you really aren't any better off."***
>
> Eric Woodruff, Chief Identity Architect, Semperis

