FEATURE BRIEF

AuthPoint Passkeys

Phishing Has Evolved. So Has the Answer

Traditional multi-factor authentication (MFA) still stops the vast majority of credential attacks. Push notifications, one-time codes, and authenticator apps remain effective for most users and should stay in place. But some attacks have become more advanced. Adversary-in-the-middle phishing toolkits intercept passwords and authentication codes in real time, targeting the users whose accounts matter most: executives, finance teams, and IT admins.

The industry answer is phishing-resistant authentication based on passkeys. AuthPoint brings that option to every cloud application your customers rely on, through OpenID Connect (OIDC) and Security Assertion Markup Language (SAML), under a single enrollment. Passkeys and traditional MFA coexist in the same Zero Trust policy. You deploy each method where it fits best.

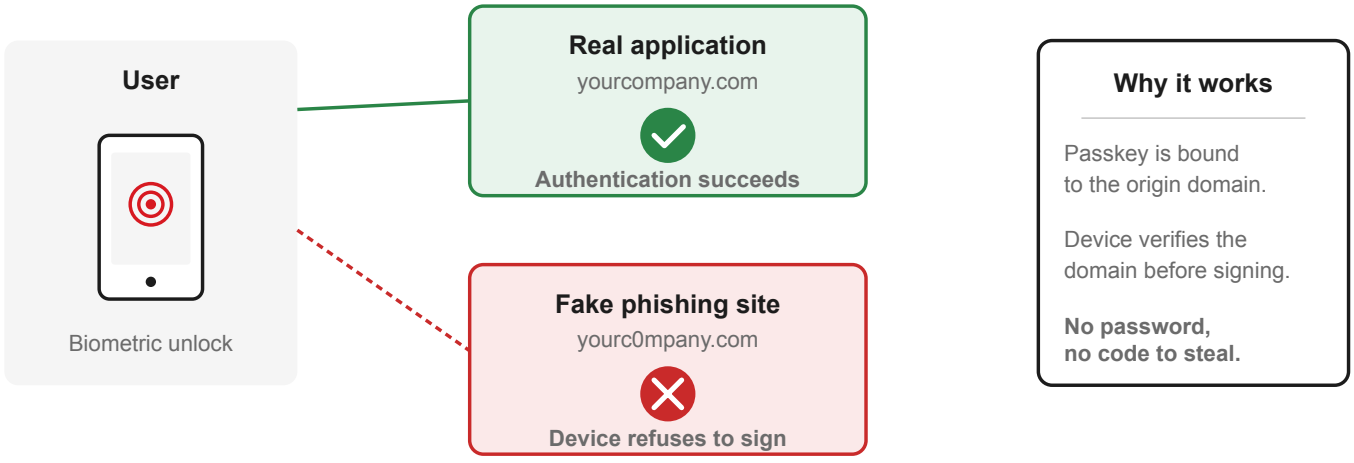
How AuthPoint Passkey Authentication Works

Enrollment. Users register once through a self-service flow with email verification. A single enrollment covers every supported cloud application, both OIDC and SAML. The passkey is generated on the user's device or hardware security key and bound to the AuthPoint identity provider. No admin intervention required.

Authentication. When the user signs in, AuthPoint asks the device to prove possession of the passkey. The user confirms with a fingerprint, face scan, or PIN. The device signs a cryptographic challenge and returns it. AuthPoint verifies the signature and grants access. No password is sent. No code is shared. Nothing travels through the network that an attacker could intercept.

Protection against phishing. Each passkey is cryptographically bound to the real application domain. When a user clicks a phishing link, the fake site cannot request the correct passkey because the device refuses to sign for the wrong origin. The attack fails before the user can be tricked.

How Passkeys Stop Phishing Attacks



FIDO2 passkeys are cryptographically bound to the real application domain. Fake sites cannot impersonate it.

Two Types of Passkeys, One Policy

Passkeys come in two forms. Synced passkeys live in the user's cloud account (Apple, Google, or Microsoft) and sync across the user's devices. They are convenient and cover most business scenarios. Device-bound passkeys live inside a hardware security key, such as a YubiKey, and never leave it. They offer the strongest protection and are the right fit for executives, administrators, and privileged roles. AuthPoint supports both types under the same policy. You choose which applies to which users.

	Synced passkeys	Device-bound passkeys
Stored in	Platform wallet: Apple, Google, or Microsoft	FIDO2 hardware key, such as YubiKey
Cross-device	Yes, synced via the user's cloud account	No, tied to the physical key
Best for	General workforce and standard business users	Executives, administrators, and privileged roles
Recovery	Via the platform account (Apple ID, Google, Microsoft)	Physical key replacement
Assurance level	High. Meets NIST AAL2 for most applications	Highest. Meets NIST AAL3 for regulated scenarios

What Passkeys Cover in AuthPoint

WatchGuard FireCloud
Passkey access to FireCloud Internet Access and FireCloud Total Access.

Microsoft Entra ID via External MFA
AuthPoint as MFA provider for Microsoft 365 and Entra ID apps.

OIDC-Connected Applications
SaaS apps like Microsoft 365, Salesforce, and Google Workspace.

SAML-Configured Resources
Passkey sign-in to SAML apps with AuthPoint acting as SAML Identity Provider.

Why Phishing-Resistant Authentication Matters Now

Three forces are moving organizations toward phishing-resistant authentication. AuthPoint passkeys align with all three.

The industry has aligned on a single standard. Passkeys are built on FIDO2 and WebAuthn. Apple, Google, Microsoft, and every major identity platform support them. NIST, a globally referenced authority on authentication standards, formally recognizes passkeys as a strong authentication method.

Regulators are raising the bar. Government cybersecurity agencies worldwide are moving from recommending MFA to requiring phishing-resistant authentication for critical systems and privileged accounts, with passkeys cited as a recommended method.

Cyber insurance is tightening. Carriers increasingly require phishing-resistant MFA for coverage, with stricter scrutiny on high-value accounts and administrative access. Organizations without phishing-resistant MFA face higher premiums or denied renewals.

To learn more about WatchGuard AuthPoint and passkey authentication, please contact your WatchGuard representative.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com WatchGuard Technologies, Inc.