Enterprise Passwordless Authentication Vendors Compared: HYPR vs Ping Identity vs Descope vs Beyond Identity vs ScrambleID

Buyer's Guide / Last updated 2026-06-11 / https://www.scrambleid.com/learn/enterprise-passwordless-vendors-compared

> **Last verified: April 29, 2026.** This comparison covers five enterprise passwordless platforms (HYPR, Ping Identity, Descope, Beyond Identity, ScrambleID). Other vendors exist (1Password, Duo, RSA, Microsoft Entra Verified ID, and others) and are not included here; the five were chosen because they are most directly comparable on the dimensions buyers ask about. The voice-channel claim further down (only ScrambleID offers native caller authentication with device-bound cryptographic proof on the voice channel) was confirmed against vendor product pages on the verification date above. **Vendor capabilities change quickly.** Treat the matrix below as a structured starting point for an evaluation, not a current-day source of truth. Validate every capability claim with the vendor's product team before making a procurement decision.

In one sentence: Enterprise passwordless platforms differ most on channel coverage, default phishing resistance, federation depth, and deployment model, choosing the right one depends on whether you need workforce-only web login, developer-centric CIAM, broad IAM coverage, device-trust-anchored workforce SSO, or true omnichannel identity across every surface a user or machine touches.

TL;DR (canonical)

- **HYPR:** Workforce-first, FIDO-first. Strongest when the requirement is phishing-resistant passwordless layered into an existing IAM stack.
- **Ping Identity:** Broad IAM platform. Strongest for large enterprises needing federation, legacy coexistence, and combined workforce/CIAM coverage.
- **Descope:** Developer-first CIAM. Strongest for fast no-code/low-code orchestration of passkeys and passwordless journeys in customer-facing apps.
- **Beyond Identity:** Workforce SSO with device trust integrated into the authentication ceremony. Strongest when continuous device-posture-on-every-auth is the primary control objective. Beyond Identity has positioned non-human identity as a strategic direction; validate specific NHI capabilities directly with the vendor.

- **ScrambleID:** Omnichannel identity. Strongest when authentication must span web, voice/call-center, desktop, in-person, and machine-to-machine, not just the browser login page.
- No single vendor is best for every scenario. The right choice depends on your channel requirements, existing IAM stack, deployment constraints, and whether your risk lives primarily at the web login or across multiple interaction channels.

How should you evaluate passwordless vendors?

Before comparing specific vendors, establish your evaluation criteria. These are the six dimensions that matter most for enterprise passwordless:

1. **Channel coverage**, Does the vendor authenticate users only on web/mobile, or also across voice, desktop, in-person, and M2M? If your risk includes the call center or shared workstations, web-only passwordless leaves gaps.
2. **Phishing resistance by default**, Does the vendor's primary ceremony use FIDO2/WebAuthn or equivalent cryptographic binding? Or does it default to magic links and OTP with passkeys as an optional upgrade? The CISA definition of phishing-resistant MFA is the benchmark.
3. **Federation breadth**, Can the vendor integrate with your existing IdP (Okta, Entra ID, Ping, etc.) via SAML/OIDC? Does it work as an upstream authenticator, a standalone IdP, or both?
4. **Deployment model**, Cloud-only, hybrid, or on-prem capable? Air-gapped or sovereign-cloud requirements narrow the field.
5. **Recovery and break-glass**, What happens when a user loses their device or can't complete the primary ceremony? A weak recovery path becomes the new attack surface.
6. **Total cost of ownership**, Licensing model (per-user, per-authentication, platform fee), integration effort, operational overhead, and ongoing enrollment/support costs.

Vendor comparison matrix

Criterion	HYPR	Ping Identity	Descope	Beyond Identity	ScrambleID
Primary use case	Workforce passwordless MFA	Enterprise IAM platform (workforce + CIAM)	Developer CIAM	Workforce passwordless with device trust	Omnichannel passwordless identity
Channel coverage	Web, mobile, desktop	Web, mobile	Web, mobile	Web, mobile, desktop	Web, mobile, voice/call-center, desktop, in-person, M2M

Criterion	HYPR	Ping Identity	Descope	Beyond Identity	ScrambleID
FIDO2/WebAuthn support	Yes, core capability	Yes, within PingOne/PingFederate	Yes, passkeys and WebAuthn	Yes, plus proprietary device-bound credential	Yes, plus QR-based cross-device pattern
Phishing-resistant by default?	Yes, FIDO-first architecture	Configurable, depends on policy setup	Configurable, supports passkeys, also offers magic links/OTP	Yes, device-bound cryptographic credential as default	Yes, cryptographic proof across all channels
Voice/call-center authentication	Not supported	Not supported	Not supported	Not supported	Native, device-bound cryptographic caller verification
In-person / People authentication	Not supported	Not supported	Not supported	Not supported	Native, branch/retail/clinical workflows
Federation	Integrates as upstream authenticator via OIDC/SAML	Full IdP with broad SAML/OIDC/SCIM support	OIDC/SAML; designed to plug into existing IdPs	OIDC/SAML; typically deployed upstream of Okta, Entra, Ping	SAML/OIDC federation; can act as IdP or upstream authenticator
Deployment model	Cloud, hybrid	Cloud (PingOne), hybrid, on-prem (PingFederate)	Cloud-only	Cloud SaaS	Cloud, hybrid
Developer experience	SDK-centric; requires IAM integration	Extensive APIs; complex configuration	No-code/low-code flow builder; fast time-to-value	SDKs and admin console; integration patterns documented for major IdPs	SDK + admin console; IVR/telephony integration APIs
Device trust / posture	Basic device binding	Configurable risk signals	Limited posture surface	Continuous device-posture evaluated at every authentication, native to the authenticator	Device-bound keys; EDR/MDM composability planned via the Overwatch risk fabric (in development)
Machine identity	Not a focus	OAuth-based; not PoP-specialized	Token-based; not PoP-specialized	NHI is a stated strategic direction; validate current	JWT client assertions (RFC 7523), mTLS, DPoP; cloud

Criterion	HYPR	Ping Identity	Descope	Beyond Identity	ScrambleID
				capabilities directly with the vendor	workload identity native
Recovery model	Multi-device enrollment, supervisor override	Depends on configuration; broad toolkit	Self-service recovery flows	Admin-driven device add; self-service flows	Identity proofing for new device; dual control for high-risk planned (Lockstep, in development)
Best fit	Enterprises adding phishing-resistant MFA to existing IAM	Large enterprises needing unified IAM with passwordless as one capability	Startups and mid-market building customer-facing apps fast	Workforce SSO programs centered on continuous device trust	Enterprises where authentication risk spans web AND voice AND desktop AND in-person AND machines

Where each vendor is strongest

HYPR, workforce-first FIDO

HYPR's architecture is built around FIDO2/WebAuthn as the primary authentication ceremony. It layers into existing IAM environments (Okta, Entra ID, Ping) rather than replacing them. The value proposition is clear: add phishing-resistant passwordless MFA to the workforce without rearchitecting your identity stack.

Strongest when: You need to eliminate passwords for employees across web and desktop login, and you already have an IdP handling federation and policy.

Gap: No native voice/call-center or M2M authentication. If your risk includes the phone channel or service-to-service identity, HYPR covers web but not the rest.

Ping Identity, broad IAM platform

Ping Identity is a full IAM platform that includes passwordless as one of many capabilities alongside SSO, federation, directory, access management, and API security. PingOne is cloud-native; PingFederate is the hybrid/on-prem option.

Strongest when: You need a single IAM platform that handles workforce and customer identity, with passwordless as part of a broader authentication policy engine.

Gap: Passwordless is one feature among many; it is not the architectural center. Voice/call-center authentication is not native. Complexity and configuration surface area can be high for organizations that primarily need passwordless.

Descope, developer-first CIAM

Descope's no-code/low-code flow builder lets developers compose authentication journeys (passkeys, social login, OTP, magic links) visually and deploy them to customer-facing apps quickly. The developer experience and time-to-value are the primary differentiators.

Strongest when: You are building a customer-facing app, want to ship passkey support fast, and need flexible orchestration without deep IAM engineering.

Gap: Primarily web/mobile focused. No native voice, desktop, or M2M channels. Not designed for enterprise workforce use cases or regulated environments that require on-prem deployment or cryptographic proof beyond the browser.

Beyond Identity, workforce SSO with integrated device trust

Beyond Identity delivers a device-bound asymmetric credential held in a hardware-protected key store (Secure Enclave, TPM, Android Keystore) and bundles continuous device-posture checks into the authentication ceremony. The platform integrates with Okta, Entra, and Ping as an upstream authenticator using OIDC/SAML. Beyond Identity has positioned non-human identity as a strategic direction in their public messaging; specific NHI product capabilities should be validated directly with the vendor.

Strongest when: Workforce SSO and desktop login are the dominant authentication risk surfaces, and continuous device-posture-on-every-auth is a primary control objective. Particularly strong fit for organizations that do not already run a mature EDR/MDM/posture stack and want posture native to the authenticator.

Gap: No native voice/call-center or in-person authentication. Organizations whose machine-identity scope spans cloud workloads, agentic systems, and standards-based service-to-service patterns may find ScrambleID's standards-native approach (JWT client assertions, mTLS, DPoP, cloud workload identity) composes more cleanly with their platform stack than Beyond Identity's currently-published surface; validate latest Beyond Identity NHI capabilities directly with the vendor. For a deeper head-to-head, see ScrambleID vs Beyond Identity.

ScrambleID, omnichannel passwordless identity

ScrambleID's differentiation is channel breadth. The same cryptographic identity that authenticates a user on the web also verifies them when they call the contact center, sign in to a desktop workstation, confirm an in-person transaction, or authorize a machine-to-machine action. The architecture uses device-bound credentials, QR(DID) for cross-device scenarios, and sender-constrained tokens (mTLS, DPoP) for machine identity.

Strongest when: Your authentication risk is not just at the web login page, it spans the call center, shared workstations, in-person interactions, and API/service boundaries. The value is eliminating per-channel authentication silos.

Gap: Younger vendor and smaller market footprint than HYPR, Ping, Descope, or Beyond Identity. Organizations looking for a broad IAM platform (SSO, directory, access management, governance) may need ScrambleID alongside a full-stack IdP.

How to choose

Start with your channel map: where do you authenticate users today, and where are the gaps?

- **Web/mobile only, workforce** → HYPR, Ping Identity, or Beyond Identity
- **Web/mobile only, customer-facing** → Descope
- **Workforce SSO with continuous device trust integrated into the authenticator** → Beyond Identity
- **Web + voice + desktop + in-person + M2M** → ScrambleID
- **Broad IAM platform with passwordless as one capability** → Ping Identity

Then layer in the secondary criteria: phishing resistance requirements (NIST SP 800-63-4, CISA), deployment constraints (cloud-only vs. hybrid), existing IdP integration, and budget.

No vendor covers every scenario perfectly. The right choice is the one that closes your highest-risk channel gaps without creating new ones.

Key Takeaway

Enterprise passwordless vendors differ most on channel coverage and architectural focus. HYPR is workforce-first FIDO with strong phishing resistance. Ping Identity is a broad IAM platform with passwordless as one capability. Descope is developer-first CIAM with fast no-code orchestration. Beyond Identity is workforce SSO with continuous device-posture integrated into the authentication ceremony, with non-human identity as a stated strategic direction (validate current capabilities directly). ScrambleID is omnichannel passwordless identity spanning web, voice, desktop, in-person, and M2M. The right choice depends on where your authentication risk lives, if it's only at the browser login, several vendors work; if it spans the call center, shared workstations, in-person interactions, and machine channels, the field narrows.

FAQ

What are the best passwordless authentication vendors for enterprises?

The answer depends on your use case. HYPR is strongest for workforce-centric, FIDO-first deployments layered into existing IAM. Ping Identity is strongest for large enterprises needing broad federation and legacy coexistence. Descope is strongest for developer-led CIAM with fast no-code/low-code orchestration. Beyond Identity is strongest for workforce SSO and desktop login with continuous device-posture integrated into the authentication ceremony. Beyond Identity has

positioned non-human identity as a strategic direction; validate specific NHI capabilities directly with the vendor. ScrambleID is strongest for omnichannel deployments spanning web, voice/call-center, desktop, in-person, and machine-to-machine channels.

Which passwordless vendor supports contact center and voice authentication?

Among the five vendors in this comparison, only ScrambleID offers native caller authentication with device-bound cryptographic proof on the voice channel as of this article's last verification date. HYPR, Ping, Descope, and Beyond Identity have historically focused on web, mobile, and desktop login rather than the voice channel. Vendor capabilities change; if voice authentication is in your requirements, validate with each vendor directly before a procurement decision.

Do all passwordless vendors support phishing-resistant authentication?

All five vendors support FIDO2/WebAuthn, which is phishing-resistant for web login. The difference is in coverage: some also offer non-phishing-resistant methods (magic links, OTP) as defaults or fallbacks. Evaluate whether the vendor's primary authentication ceremony is phishing-resistant by default, not just whether they support it as an option, and verify that recovery and step-up paths are also phishing-resistant.

How should enterprises evaluate passwordless vendors?

Evaluate across six dimensions: channel coverage (web, mobile, voice, desktop, M2M), phishing resistance (is it default or optional?), federation breadth (SAML, OIDC, existing IdP integration), deployment model (cloud, hybrid, on-prem), recovery and break-glass (what happens when the user loses their device?), and total cost of ownership (licensing, integration effort, operational overhead).

Can you use multiple passwordless vendors together?

Yes, many enterprises use a primary IdP (Okta, Entra ID, Ping) for federation and add a specialized passwordless layer (HYPR, ScrambleID) as an upstream authenticator. The key is that the passwordless layer integrates via SAML/OIDC so the IdP still manages policy and session lifecycle.

References (public)

- W3C WebAuthn Level 2: https://www.w3.org/TR/webauthn-2/
- FIDO Alliance, Passkeys: https://fidoalliance.org/passkeys/
- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- NIST SP 800-63-4 (Digital Identity Guidelines): https://csrc.nist.gov/pubs/sp/800/63/4/final
- RFC 8705 (OAuth 2.0 Mutual-TLS): https://datatracker.ietf.org/doc/html/rfc8705

- RFC 9449 (OAuth 2.0 DPoP): https://www.rfc-editor.org/rfc/rfc9449.html

Related reading

- ScrambleID vs Beyond Identity: A Technical Comparison
- What Is Passwordless Authentication?
- Phishing-Resistant Web Authentication
- Omnichannel Authentication
- ScrambleID + Okta Deployment Pattern
- ScrambleID + Microsoft Entra ID Deployment Pattern
- ScrambleID Evaluation Checklist