ScrambleID vs Beyond Identity: How They Compare on Channels, Device Trust, and Non-Human Identity

Buyer's Guide / Last updated 2026-06-11 / https://www.scrambleid.com/learn/scrambleid-vs-beyond-identity

> **Last verified: April 29, 2026.** Both Beyond Identity and ScrambleID iterate quickly, and Beyond Identity rebranded its product portfolio in August 2025. The capability claims in this article reflect publicly available product information as of the verification date above. Treat this as a structured starting point for an evaluation, not a current-day source of truth. Validate every capability claim with each vendor's product team before a procurement decision.

In one sentence: Beyond Identity and ScrambleID both deliver phishing-resistant, device-bound passwordless authentication. The meaningful difference is that Beyond Identity is strongest as a workforce-and-device-trust platform anchored at web and desktop login, while ScrambleID extends the same cryptographic identity across voice, in-person, and machine channels in addition to web.

TL;DR (canonical)

- Both vendors meet the CISA definition of phishing-resistant MFA on the web channel using device-bound cryptographic credentials.
- Beyond Identity's core differentiator is **device trust integrated into the authenticator** (continuous posture checks at every authentication), strongest for workforce SSO and device-centric Zero Trust programs.
- ScrambleID's core differentiator is **channel coverage**: the same cryptographic identity authenticates the user on web, voice/call-center, desktop, in-person, and machine-to-machine.
- Both integrate with Okta and Microsoft Entra ID as upstream authenticators via OIDC/SAML.
- Pick Beyond Identity when device-posture-on-every-auth is the primary outcome and authentication risk is concentrated at workforce SSO. Pick ScrambleID when authentication risk also spans the contact center, frontline/in-person, or service-to-service identity.
- The two are not mutually exclusive in every scenario; some enterprises run Beyond Identity for workforce SSO and ScrambleID for the voice or M2M channels their primary authenticator does not cover.

Why this comparison matters

Buyers running an enterprise passwordless evaluation almost always shortlist Beyond Identity. The architecture is genuinely strong: a device-bound asymmetric credential held in a hardware-protected key store, continuous device-posture checks, and tight integration with Okta, Entra, and Ping as an upstream authenticator. For a workforce-SSO-centric program, it is a credible answer.

The reason ScrambleID shows up in the same evaluations is that workforce SSO is rarely the only place authentication risk lives. Calls into the contact center, branch and store associates verifying customers in person, machine-to-machine API calls between services, all of these are authentication events. They typically use different credentials, different vendors, and different operational models, which is how attackers find seams. The question this comparison helps answer is: where does my authentication risk actually live, and which architecture closes more of it?

Architecture: how the credential lives

Both vendors use asymmetric, device-bound cryptographic credentials as the primary authentication ceremony. The differences are in how the credential is provisioned, where it lives, and what binds it to context.

Architectural element	Beyond Identity	ScrambleID
Credential type	Asymmetric key pair, proprietary credential plus FIDO2/passkeys	Asymmetric key pair, FIDO2/WebAuthn for web; same family of cryptographic proof on voice, desktop, in-person, M2M
Key storage	Hardware-protected key store: Secure Enclave (Apple), TPM (Windows), Android Keystore	Hardware-protected key store on the bound device, plus cross-device QR-based binding for shared/borrowed device scenarios
Origin/context binding	Web ceremony binds to relying-party origin (WebAuthn semantics); device-posture binds to device state	Web ceremony binds to relying-party origin (WebAuthn semantics); voice ceremony binds to caller identity and call session; M2M ceremony binds via sender-constrained tokens (RFC 8705 mTLS, RFC 9449 DPoP)
Authenticator surface	Beyond Identity Authenticator app (desktop and mobile); browser extension where applicable	ScrambleID Authenticator app (mobile); browser-side WebAuthn for cross-device binding; channel-specific ceremonies for voice/in-person
Replay and lateral-movement protection	Device-bound key plus continuous device-posture evaluation	Device-bound key plus session binding (per-session ephemeral key tied to issuance); continuous risk signals planned via Overwatch (in development)
Cross-device binding	Multi-device enrollment with admin policy controls	QR-based cross-device pattern for one-shot binding (web shows QR, mobile authenticator signs)

Key takeaway: On the web channel, both architectures meet the same security bar. The architectural divergence shows up off the web channel and at the boundary between authentication and device posture.

Channel coverage

This is the dimension where Beyond Identity and ScrambleID diverge most.

Channel	Beyond Identity	ScrambleID
Web (workforce SSO)	Yes, primary use case	Yes, primary use case
Web (CIAM, customer-facing)	Yes, Secure Customer	Yes, customer-facing flows supported
Mobile	Yes, native authenticator app	Yes, native authenticator app
Desktop login (Windows, macOS)	Yes, strong native integration with continuous posture	Yes, desktop sign-in flows
Voice / call-center	Not native	Native, device-bound cryptographic caller verification with IVR and contact-center integration
In-person / People	Not native	Native, branch/retail/clinical flows for verifying a counterparty in person
Machine-to-machine (M2M)	Stated strategic direction; specific NHI capabilities should be validated with the vendor	Native, JWT client assertions (RFC 7523), mTLS (RFC 8705), DPoP (RFC 9449), cloud workload identity
AI agent / MCP server identity	Not a published focus area as of the verification date; validate roadmap with the vendor	Native, agent identity, tool-access governance, MCP server identity

The practical implication: if an attacker who fails on web SSO can still reach you through the contact center or as a service principal, web-only passwordless is incomplete. Both vendors recognize this; they have answered it differently. Beyond Identity expanded vertically (deeper into device trust and continuous authorization). ScrambleID expanded horizontally (the same cryptographic identity across more interaction channels).

For a deeper architectural view of how a single identity spans channels, see The ScrambleID Identity Fabric.

Phishing resistance and authentication ceremony

Both vendors clear the CISA phishing-resistant MFA bar on the web channel. The relevant questions for an enterprise are subtler:

1. **Is the primary ceremony phishing-resistant by default, or is it one option among several?** Both vendors default to a phishing-resistant primary. Magic links and OTP are not part of either default workforce flow.
2. **Are recovery and step-up paths also phishing-resistant?** This is the more important question. A phishing-resistant primary with an OTP-based recovery flow leaves the same attack surface a workforce had with passwords plus push MFA, just shifted to the recovery path.
3. **Does the architecture meet NIST SP 800-63-4 AAL3 properties?** Both architectures are designed to meet AAL3 properties (verifier-impersonation resistance, verifier-compromise resistance, hardware-bound keys), subject to specific deployment configuration. Validate your specific configuration against the finalized 800-63B-4 with each vendor.

ScrambleID's Recovery and Fallback Playbook is explicit about the recovery threat model and outlines the warm/cold/assisted recovery pattern; ask Beyond Identity to walk you through the equivalent path so you can compare like-for-like.

Device trust: integrated vs composable

Beyond Identity's most distinctive design choice is making device-posture checks part of the authentication ceremony itself. Disk encryption disabled, screen lock missing, OS out of date, EDR not running, the authentication can be denied or step-up triggered, evaluated on every authentication.

ScrambleID's design choice is to keep authentication and device posture as composable layers. The cryptographic ceremony proves the user holds a hardware-bound key on a known device; the broader risk fabric is designed to correlate signals from your existing EDR, MDM, ZTNA, and posture stacks to drive policy decisions and step-up (Overwatch, in development, is that layer). Both approaches deliver the outcome of "do not let an unhealthy device authenticate." The trade-off:

Property	Beyond Identity (integrated)	ScrambleID (composable)
Authenticator covers posture out-of-the-box	Yes	Partially; richer posture comes from EDR/MDM integration
Tight coupling to device-posture roadmap	Vendor controls posture surface	Customer controls via existing tools
Best fit for organizations with no EDR/posture stack	Strong	Workable, but you are leaving a layer of value off the table
Best fit for organizations with mature EDR/MDM	Some posture functions duplicate	Avoids duplication, integrates with what you already run
Posture coverage off the web channel	Limited (no native voice/in-person)	Risk signals apply across channels

There is no universally right answer. Buyers with a mature CrowdStrike, SentinelOne, or Microsoft Defender for Endpoint deployment, paired with strong MDM, often prefer the composable model because they have already paid for those signals and want their authenticator to consume rather than replace them. Buyers without that maturity often value Beyond Identity's batteries-included posture model.

Federation and IdP integration

Both vendors are designed to integrate with leading IdPs as an upstream authenticator. The federation surface is comparable.

Federation surface	Beyond Identity	ScrambleID
Okta integration pattern	OIDC IdP / inbound federation; supports Identity Engine policy interplay	OIDC IdP / inbound federation; supports Identity Engine policy interplay (see ScrambleID + Okta deployment pattern)
Microsoft Entra ID integration pattern	External Authentication Methods (EAM) / federation	External Authentication Methods (EAM) / federation (see ScrambleID + Entra ID deployment pattern)
SAML / OIDC	Both protocols supported	Both protocols supported
SCIM provisioning	Yes	Yes
Acts as standalone IdP	Yes (limited; usually deployed upstream of an IdP)	Yes
Acts as upstream authenticator	Yes (most common pattern)	Yes (most common pattern)

Federation is rarely the deciding factor between these two vendors; the integration patterns mirror each other.

Recovery and break-glass

The strongest passwordless architecture can be undone by a weak recovery flow. Both vendors have answers; the questions to ask are the same in both directions.

Ask Beyond Identity: What does the new-device enrollment flow look like for an employee whose laptop was stolen? Who can authorize a device add, and what is the proof requirement? Is the recovery channel phishing-resistant, or does it fall back to an email link or a help-desk call without identity proofing?

Ask ScrambleID: Same questions. ScrambleID's pattern is documented in the Recovery and Fallback Playbook: warm path (multi-device, automatic), cold path (identity-proofing-based new-device enrollment), assisted path (help-desk with strong proofing and dual control; Lockstep, in development, is designed to enforce that dual control).

The right framing for both vendors: treat the recovery path as part of the authentication architecture, and require the same phishing-resistance and verifier-impersonation-resistance properties from it.

Machine identity and non-human identity

Beyond Identity has positioned non-human identity as a strategic direction in their public messaging. As of the verification date above, specific NHI product capabilities (privileged access, service-account replacement, scope of supported workload types) should be validated directly with the vendor.

ScrambleID's M2M architecture is built natively into the platform from the start. The pattern is standards-based: JWT client assertions (RFC 7523), mutual TLS (RFC 8705), DPoP (RFC 9449) for sender-constrained tokens, plus cloud-native workload identity (AWS IRSA, GCP Workload Identity, Azure Managed Identity). For AI workloads specifically, ScrambleID treats the agent and the MCP server as first-class identities (see AI Agent Authentication and AI Agent Tool Access Playbook).

The two approaches converge on the same outcome (eliminate long-lived secrets, attest to workload identity, scope access tightly) but reach it through different surfaces. Buyers should evaluate based on:

- **What identities are in scope?** Just human-adjacent service accounts and SSH? Or also cloud workloads, agents, and MCP servers?
- **What standards do your platform teams already use?** If your SREs and platform engineers are already comfortable with OIDC token exchange, mTLS, and DPoP, the standards-based pattern composes cleanly with what they run.
- **What is the operational model?** Vault-style secret rotation versus issuer-style short-lived credentials versus broker-style protocol replacement.

Total cost and operational footprint

Both vendors are commercial SaaS with workforce-priced licensing. Neither publishes list pricing; both will quote based on user counts, channels in scope, and integration depth. The buyer-side variables that drive total cost of ownership are similar:

1. **License model:** per-user/month is standard; M2M and CIAM volumes can shift the model.
2. **Integration effort:** day 1 IdP integration is straightforward for both; the cost shows up in the channels beyond the IdP (custom apps, voice/IVR, in-person flows, M2M).
3. **Authenticator distribution:** MDM-driven app deployment for Beyond Identity vs. authenticator app distribution for ScrambleID, both are tractable but require IT effort.
4. **Help-desk and recovery operational load:** the strongest predictor of operational cost. Plan for the cold-recovery path before you launch.

The cleanest TCO comparison is to scope by channel rather than by authenticator. Pricing per workforce SSO seat looks similar; pricing per voice authentication or per machine identity is where the value calculation diverges.

When Beyond Identity is the better fit

- Workforce SSO is the dominant authentication risk surface; the contact center, frontline workers, and machine identity are out of scope or already addressed.
- Device-posture-on-every-authentication is a stated security control objective and you do not have a mature EDR/MDM stack to compose with.
- The customer-facing application portfolio is web/mobile and the existing CIAM gap maps cleanly to Beyond Identity Secure Customer.
- Privileged access and service-account replacement are the immediate non-human identity priorities, and Beyond Identity's current published NHI capabilities (validated directly with the vendor) map to your roadmap.

When ScrambleID is the better fit

- Authentication risk extends meaningfully into the voice channel, in-person interactions, or machine-to-machine (including AI agent and MCP server identity).
- You already run a mature EDR/MDM/posture stack and want device posture as a composable signal feeding the authenticator, not a parallel implementation inside it.
- The non-human identity scope spans cloud workloads, agentic systems, and standards-based service-to-service patterns (JWT client assertions, mTLS, DPoP) rather than primarily service-account password replacement.
- A single identity model across channels reduces operational and audit overhead more than per-channel point solutions.

When both might be right

It is not unusual to see Beyond Identity covering workforce SSO and desktop login while ScrambleID covers the voice channel, in-person workflows, or M2M. Both vendors compose cleanly on top of Okta or Entra ID, and the IdP enforces a single policy and session model regardless of which authenticator the user used to sign in. The cost of running two authenticators is real but bounded; the cost of leaving the contact center or the M2M channel on legacy authentication is unbounded.

Evaluation questions to ask both vendors

When you take this comparison into a vendor call, ask each side the same questions and compare answers:

1. Walk me through the cryptographic ceremony on web, end to end, from challenge to assertion to session establishment. Where is the private key held, what binds it to origin, and what binds it to the user's device state?
2. Walk me through the same ceremony for a non-web channel that is in your roadmap (Beyond Identity: pick one; ScrambleID: voice, in-person, or M2M).
3. What is the strongest recovery path you support today, and what are the proof requirements? What is the weakest recovery path that is still enabled by default in a typical deployment?
4. How do you meet NIST SP 800-63-4 AAL3 properties, and what specific deployment options would change the AAL determination?
5. How does device posture flow into the authentication decision? If I already run EDR/MDM, what is the integration story, and what duplicates rather than composes?
6. Show me the audit trail for a sensitive action: what is captured, what is signed, what is queryable, and how does it map to my SIEM (Splunk, Sentinel, Chronicle)?
7. What is the M2M / NHI roadmap and how does it integrate with my cloud workload identity (IRSA, Workload Identity, Managed Identity) today?

The answers should be specific. Vague answers on these questions are a signal in either direction.

Key Takeaway

Beyond Identity and ScrambleID both deliver phishing-resistant, device-bound passwordless authentication that meets the CISA phishing-resistant MFA bar on the web. Beyond Identity is strongest as a workforce-SSO-and-device-trust platform with continuous device posture integrated into the authentication ceremony. ScrambleID is strongest as an omnichannel platform that extends the same cryptographic identity across voice/call-center, desktop, in-person, and machine-to-machine channels in addition to web. The right choice depends on where authentication risk lives in the enterprise: concentrated at workforce SSO favors Beyond Identity; spread across channels favors ScrambleID. The two are not mutually exclusive; some enterprises run both with the IdP enforcing unified policy.

FAQ

How does ScrambleID compare to Beyond Identity for enterprise passwordless?

Both vendors deliver phishing-resistant, device-bound passwordless authentication that integrates with leading IdPs as an upstream authenticator. The key difference is channel coverage. Beyond Identity is strongest at the web and desktop login with deep device-posture integration. ScrambleID extends the same cryptographic identity into the voice/call-center, in-person, and machine-to-machine channels using a single proof model. If your authentication risk is concentrated at workforce SSO, both fit. If it spans the contact center, frontline workers, or service-to-service identity, the field narrows.

Is Beyond Identity phishing-resistant?

Yes. Beyond Identity uses an asymmetric, device-bound cryptographic credential as its primary ceremony, with the private key held in a hardware-protected key store (Secure Enclave on Apple silicon, TPM on Windows, equivalent on Android). This meets the CISA definition of phishing-resistant MFA. The same is true of ScrambleID, which uses device-bound keys with origin binding on the web channel and a comparable cryptographic proof on voice, desktop, in-person, and M2M channels.

Does Beyond Identity authenticate calls into a contact center?

As of this article's last verification date, Beyond Identity does not offer native caller authentication on the voice channel. Beyond Identity's product surface is focused on workforce SSO, device trust, customer (CIAM) authentication on web/mobile, and a stated strategic direction in non-human identity (validate specific NHI capabilities directly with the vendor). ScrambleID provides device-bound cryptographic caller verification that integrates with IVR and contact-center platforms. Vendor capabilities change; if voice authentication is a requirement, validate with both vendors directly.

Both vendors talk about device trust. How are the approaches different?

Beyond Identity bundles device-posture checks into the authentication ceremony itself, evaluating signals like OS version, disk encryption, screen lock, and EDR presence at every authentication. ScrambleID uses device-bound keys, with continuous risk signals planned via Overwatch (in development), and treats device posture as a complementary control surface that can be integrated with EDR, MDM, or your existing posture engine rather than as the primary differentiator. Both approaches are defensible; the choice often comes down to whether you already run a posture/EDR stack you want to integrate with versus whether you want posture native to the authenticator.

What about machine-to-machine and non-human identity?

Beyond Identity has positioned non-human identity as a strategic direction; specific NHI product capabilities should be validated directly with the vendor. ScrambleID uses standards-based, sender-constrained tokens (RFC 7523 JWT client assertions, RFC 8705 mTLS, RFC 9449 DPoP) plus cloud workload identity (IRSA, Workload Identity, Managed Identity) and short-lived credentials with keys held in hardware/cloud KMS.

Which is easier to deploy?

Both vendors are SaaS by default and integrate with Okta and Microsoft Entra ID as upstream authenticators using OIDC/SAML, so the day-1 federation pattern is similar. Beyond Identity's typical workforce rollout deploys an authenticator app and an admin console; ScrambleID's typical workforce rollout deploys an authenticator and an admin console plus the channels you want to enable (voice, in-person, M2M) over time. The right comparison is not which is faster on day 1 but which closes more of your authentication surface over the first year.

Can a recovery flow be a phishing-resistant MFA bypass?

Yes, and this is one of the most underrated evaluation criteria. A passwordless system is only as strong as its weakest recovery path. Beyond Identity supports admin-driven device add and self-service flows; ScrambleID supports identity-proofing-based new-device enrollment, with dual control for high-risk actions planned (Lockstep, in development). For both vendors, ask the same question: what does an attacker need to control to enroll a new device under my account, and is that path phishing-resistant?

How recent are these capability claims?

Capability claims in this article reflect public product information as of the `last_updated` date in the article frontmatter. Vendor product surfaces change frequently. Treat this comparison as a structured starting point for evaluation, not a current-day source of truth, and validate every capability with the vendor's product team before procurement.

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: https://csrc.nist.gov/pubs/sp/800/63/4/final

- RFC 7523 (JWT Profile for OAuth 2.0 Client Authentication): https://datatracker.ietf.org/doc/html/rfc7523
- RFC 8705 (OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens): https://datatracker.ietf.org/doc/html/rfc8705
- RFC 9449 (OAuth 2.0 Demonstrating Proof of Possession, DPoP): https://www.rfc-editor.org/rfc/rfc9449.html

---

Related reading

- Enterprise Passwordless Authentication Vendors Compared
- The ScrambleID Identity Fabric
- ScrambleID + Okta Deployment Pattern
- ScrambleID + Microsoft Entra ID Deployment Pattern
- Recovery and Fallback Playbook
- ScrambleID Evaluation Checklist (RFP)