Choosing the Right Identity Provider

A Checklist for CIOs & CISOs

Safeguard Your Organization Against Fraud & Insider Threats

Organizations face more challenges than ever protecting themselves from both internal and external threats, while also trying to meeting evolving customer, employee, and partner expectations. With rising cases of account takeovers (ATO), new account fraud (NAF), hiring fraud, and insider threats, the stakes are high.

By leveraging a comprehensive identity and access management (IAM) platform built for all user types (customer, workforce, partners, and AI agents), enterprises can equip themselves with the necessary tools to drive security, compliance, and user satisfaction.

This checklist is designed to help decision-makers assess their fraud readiness with a list of key IAM capabilities used for fraud and threat mitigation. Does your organization have these critical capabilities? If not, it's time to evaluate a unified IAM platform purpose-built for fraud and threat protection.

Customer Identity: Mitigate NAF Before and During Registration

- ☐ Automate registration workflows with no-code/low-code orchestration for **seamless, secure onboarding**.
- ☐ Use no-code/low-code orchestration to seamlessly integrate **real-time identity proofing** tools.
- ☐ Conduct robust **identity verification and liveness detection** across the user registration journey.
- ☐ Utilize **verifiable credentials** to ensure tamper-proof identity verification during customer registration.
- ☐ Implement **decentralized identity** to give users secure control over their identity attributes and credentials.

Customer Identity: Prevent ATO Fraud

- ☐ Implement **adaptive multi-factor authentication (MFA)** to dynamically adjust methods according to risk.
- ☐ Use **policy-based access control (PBAC)** for real-time, context-driven access decisioning.
- ☐ Continuously monitor **session behavior** to detect unusual patterns and neutralize threats before escalation.
- ☐ Employ **advanced threat detection tools** to identify deepfake attempts and other emerging fraud tactics.
- ☐ Secure data and sensitive APIs with **fine-grained access control** to protect customer and transaction data.
- ☐ Employ intelligent bot detection that can **differentiate between malicious bots and helpful AI agents**.

Choosing the Right Identity Provider

A Checklist for CIOs & CISOs

Customer Identity: Build Trust and Loyalty

- ☐ Enable **passwordless authentication** to create a frictionless and secure customer experience.
- ☐ Use **identity analytics** to deliver personalized experiences and identify access blindspots and vulnerabilities.
- ☐ Strengthen security across third-party loyalty programs by leveraging **secure API integrations**.
- ☐ Streamline and secure **account recovery** processes across all devices and channels of engagement.
- ☐ Get a **single view of the customer** by unlocking data silos and integrating your hybrid IT organization-wide.

Workforce Identity: Improve Efficiency and Achieve Compliance

- ☐ Streamline provisioning, de-provisioning, and access reviews with **automated identity lifecycle management**.
- ☐ Utilize **artificial intelligence (AI)-driven governance** to ensure compliance through automated workflows.
- ☐ Maintain comprehensive **audit trails** to support regulatory reporting and detect compliance violations.
- ☐ Use strong authentication standards like **passkeys** to reduce vulnerabilities associated with weak credentials.
- ☐ Enable **journey orchestration tools** to adapt to evolving compliance requirements.

Workforce Identity: Modernize Access Control and Governance

- ☐ Automate **identity lifecycle management** to ensure accurate and efficient provisioning and de-provisioning.
- ☐ Apply **Zero Trust principles** to continuously validate users and devices accessing sensitive systems.
- ☐ Enforce **least-privilege access policies** using role-based, attribute-based, and policy-based access control.
- ☐ Monitor workforce behavior for **anomalous activities** that may indicate compromised identities or credentials.
- ☐ Integrate **multi-layered security** for hybrid/remote workforce environments across geographies and boundaries.
- ☐ Onboard and manage lifecycle for **digital workers and AI agents**.

Choosing the Right Identity Provider

A Checklist for CIOs & CISOs

B2B Identity: Deliver Seamless and Secure Third-Party Access

- ☐ Enable **secure third-party access** with PBAC to ensure contractors/partners can access only what they need.
- ☐ Maintain **real-time visibility** into third-party activities and make quick adjustments to access permissions.
- ☐ Align third-party access with **compliance standards** to protect sensitive systems and data.
- ☐ Reduce risks by implementing **adaptive MFA and passwordless** for third-party users based on access context.
- ☐ Automate **onboarding and de-provisioning** for third-party accounts to minimize vulnerabilities.

Implementation: Accelerate Time-to-Value

- ☐ Choose a **single, unified IAM platform** and **low-code/no-code orchestration** for rapid deployment and reduced operational costs.
- ☐ Integrate seamlessly with legacy and cloud systems through **identity convergence**.
- ☐ Centralize the monitoring of policies, user activity, and regulatory compliance through a **single dashboard**.
- ☐ Leverage easy **extensibility** for future upgrades and ecosystem expansion.
- ☐ Partner with the industry's leading IAM provider to **streamline implementation** and ensure operational excellence.

Up Level Your Identity Game

Where to go from here? Get a list of identity definitions and RFP questions in our **CIAM** , **Workforce**, and **B2B Buyer's Guides**, or

Let's chat about your unique needs and challenges.