Passwordless Orchestration (PO)

Datasheet

axiad

Challenges

Many enterprises and public agencies are building proprietary, highly customized environments to protect “crown jewel” Intellectual Property vital infrastructure, and critical operations. As these environments are very often the target of nation-state as well as criminal threat actors, authentication of end users, machines, assets, and interactions is needed.

What’s needed is a single authentication approach that will work across the entire environment and maximize flexibility. To eliminate multiple attack vectors including phishing, the approach must also extend to validate interactions such as emails with file attachments.

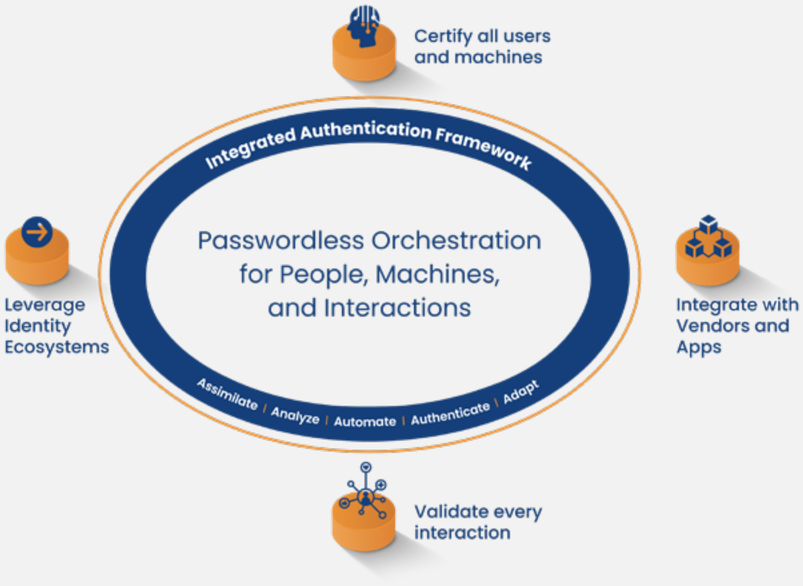
Passwordless Orchestration Challenges

61%	Plan to implement passwordless in 24 months
2/3	Of “passwordless” solutions use a shared secret
96%	Say passwordless shouldn’t have shared secrets

Product Overview

Leveraging the power of the Axiad Cloud, Axiad Passwordless Orchestration (PO) provides holistic, consistent, and efficient authentication for everything (users, machines, assets, and interactions), everywhere in even the most complex environment. This product aggregates the other cloud offerings’ functionality, adds Secure Interaction verification (Email and Doc certificates), and provides APIs for customization and integration into the organization’s environment. Axiad PO helps large organizations with multiple IAMs and many applications tailor authentication to their unique environment.

Authentication Tailored to Unique Environments


Certify all users and machines
Integrated Authentication Framework
Passwordless Orchestration for People, Machines, and Interactions
Leverage Identity Ecosystems
Integrate with Vendors and Apps
Assimilate | Analyze | Automate | Authenticate | Adapt
Validate every interaction

How Axiad PO is unique

- **Holistic:** A single approach serves all authentication, everywhere across the environment
- **Fully Customizable:** APIs enable full integration with custom software
- **Interaction Certification:** Authenticates email senders and attachments
- **Unified view of all credentials:** Unified portal provides a single pane of glass for managing all credentials
- **Broad token support:** A wide range of phishing-resistant tokens are supported as well as physical / virtual token consolidation
- **Secure Design:** Architected for best-practices security including isolation by customer, encrypted communications, and key storage in specialized hardware

Key Features

Holistic: Authenticates end users, machines, assets, and interactions, everywhere across the environment

- **End-to-end Security:** All entities are secured without using passwords or shared secrets so the authentication process is secure from end-to-end
- **Passwordless Multi-Factor Authentication (MFA):** Utilizes multiple types of authentication methods without a password or push notification that can be intercepted or phished
- **Phishing-Resistant Authentication:** Delivers a broad range of phishing resistant authentication based on FIDO2 and WebAuthn with Authenticators ranging from enterprise-grade mobile-based to government-grade AAL3
- **Fully Customizable:** APIs enable full integration with custom software
- **Interaction Certification:** Certifies email senders and attachments

Consistent: Ensures authentication is consistent across OSs, applications, services, and more

- **Government-grade Authentication:** Combines strong tokens and user behavioral criteria per Governement guidelines
- **Broad OS support:** Secures Microsoft Windows, Apple OSs, Linux, and more
- **Windows-friendly:** Provides authentication across Windows ecosystem including Azure, Windows Hello for Business, Windows OS, and more
- **Flexible Token Side-by-Side support:** Leverages any combination of phishing-resistant tokens, FIDO2 / CBA, and SmartCards side-by-side
- **Integrated:** Supports wide range of protocols, connectors, and standards for interoperation across the Identity ecosystem out of the box

Efficient: Increases IT and end user efficiencies at scale with automated, streamlined workflows

- **Unified view of all MFA credentials:** Manages all MFA credentials, including Azure AD's issued credentials such as WHFB and Microsoft Authenticator
- **Unified Portal:** Streamlines work and automates tasks for both IT and End Users across the organization
  - **Single Pane of Glass:** Delivers all functionality including custom workflows for both IT and End Users
  - **Airlock:** Provides help desk automation by eliminating temporary passwords, automating administration, and enabling self-service credential management
  - **MyCircle:** Empowers self-service by enabling the workforce to issue department-level credential resets, thereby avoiding temporary passwords and increasing efficiency for IT and end users
  - **Certificate Workflows:** Supports a range of certificate request and delivery workflows

Platform Capabilities: Leverages Axiad Cloud Platform capabilities including secure design, convenient implementation, and more.

Benefits

Deliver Optimal Protection

Ensure your passwordless solution is fully passwordless and phishing-resistant end-to-end to stop even the most sophisticated hackers in their tracks

Maximize Flexibility

Leverage an industry-best range of credentials and customize an approach with APIs, integrations, and more to build what's right for you

Certify Public Trust

Authenticate and securely exchange documents within regulated environments such as U.S. Federal Bridge, SAFE-BioPharma, and WebTrust

About Axiad

Axiad delivers organization-wide passwordless orchestration to secure users, machines, assets, and interactions for enterprise and public sector organizations that must optimize their cybersecurity posture while navigating underlying IT complexity. The company's flagship offering, Axiad Cloud, is a comprehensive, secure, and integrated authentication platform that allows customers to move to a passwordless future without the friction and risk of fragmented solutions. Axiad supports the widest range of credentials in the industry including FIDO, mobile MFA, Windows Hello for Business, YubiKeys, smart cards, TPM and biometrics.