Phishing-Resistant Authentication (PRA)

Datasheet

Challenges

Government Agencies, Enterprises, and supporting vendors are being held to a higher standard for user authentication. The latest standards specify Phishing-Resistant Authentication as defined by specific criteria and best practices guidance. Most organizations do not have a solution in place that meets these requirements.

Further, these standards are increasing in rigor over time. Keeping up with these standards is likely out of reach for even the largest organizations.

Finally, compliance tracking across all these standards is daunting. Security teams that are already stretched thin may not have the ability to track compliance.

Criteria for Government-grade PRA

350% Increase in phishing attacks on remote workers

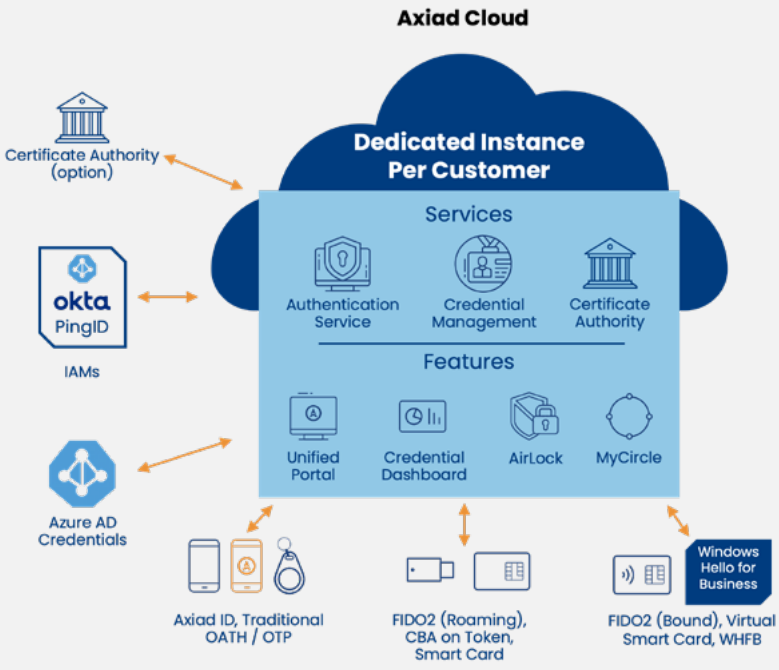
66% Have been impacted by a phishing attack

71% Say that phishing is the most-concerning threat

Product Overview

Leveraging the power of the Axiad Cloud, Axiad Phishing-Resistant Authentication (PRA) provides consolidated, consistent, and efficient passwordless and phishing-resistant PRA for end users. Axiad PRA delivers a broad range of enterprise-grade phishing-resistant methods such as FIDO2 and CBA to government-grade phishing-resistant strong hardware tokens and conformance to standards including user behavior validation, at scale and everywhere it's needed. Axiad PRA helps organizations address government mandates and provide the highest level of authentication to privileged users and knowledge workers.

Enterprise-grade Multi-Factor Authentication



How Axiad PRA is unique

- **Consolidated:** A single approach serves all end user needs, everywhere across the environment
- **End-to-end Security:** All entities are secured without passwords or shared secrets
- **Unified view of all credentials:** Unified portal provides a single pane of glass for managing all end user 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

Consolidated: Serves all authentication needs, 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 government-grade AAL3 Authenticators

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

- **Government-grade Authentication:** Combines strong tokens and user behavioral criteria per Government 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

Attain Phishing Resistance

Eliminate reliance on credentials that can be compromised in a variety of ways

Fortify Existing Investments

Help get the most out of existing investments across the entire organization

Authenticate Consistently

Authenticate a user whether he or she is online or offline - anywhere around the globe.

axiad

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.