Axiad Cloud

Challenges

As IT architectures became more complex and multitiered and began to leverage smart and IoT devices, Authentication became critical. Authentication silos arose among applications, OSs, workplace location (especially for hybrid workforces), and more. This led to four major challenges:

- Breaches: The combination of easily-compromised passwords and silos has led to the majority of breaches seen to date.
- Architecture: Many approaches lock down one aspect of authentication yet leave other aspects unsecured
- Inefficiencies: IT teams are swamped by managing authentication, especially account recovery workload.
- End User friction: End users frequently find authentication to be onerous and bypass it where possible.

Authentication Platform Challenges

84% Experienced an identity-related breach in 12 months

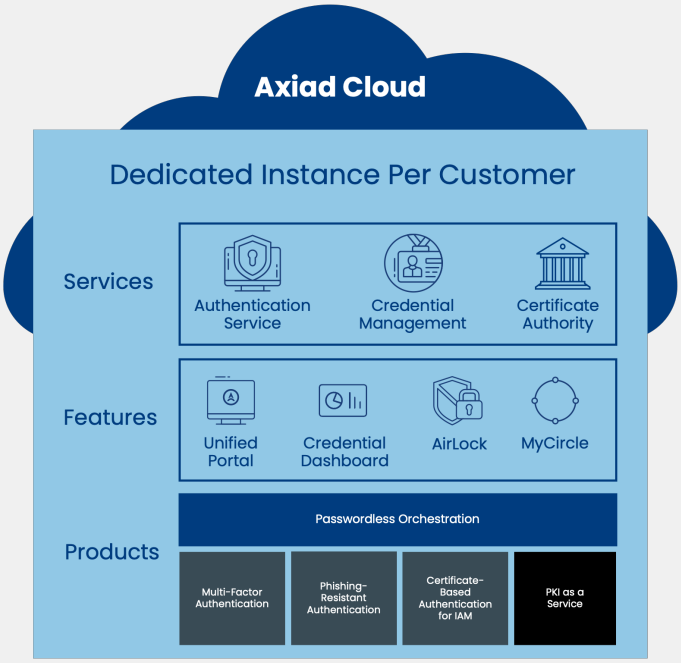
89% Of "passwordless" solutions really use a password or shared secret

>40% Password-related issues take over 40% of IT's time

Product Overview

Axiad Cloud is a comprehensive, secure, and efficient authentication SaaS platform that eliminates silos across the environment. Architected for best-practices security, it enables "mix-and-match" use of any or all of the Axiad Cloud product line. It can be applied in heterogeneous IT environments – e.g., organizations operating Windows, Mac and Linux operating systems or with multiple existing IAM systems in place – allowing organizations to remove gaps and inconsistencies in how they authenticate across complex ecosystems, and ultimately to become more programmatic in their overall cybersecurity practices.

Authentication SaaS Cloud Platform



How Axiad Cloud is unique

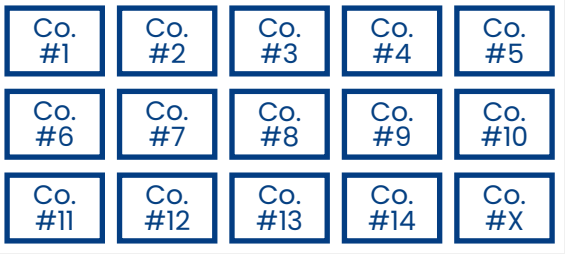
- **Comprehensive:** Supports all Authentication methods across users, machines, and more while interoperating with the entire Identity ecosystem
- **Secure Design:** Architected for best-practices security including a private instance for each customer, encrypted communications, and key storage in specialized hardware
- **Efficient:** Streamlines and automates help desk workload, enables end user self-service, and minimizes overall IT overhead
- **Mix-and-Match:** Supports any combination of the cloud product line for each organization

Secure by Design

The Axiad Cloud Platform is architected to isolate and protect each customer's credentials.

Typical Cloud-Based Authentication Solutions

Credentials are comingled in a Cloud environment

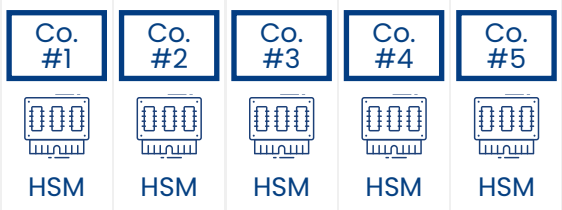


Bad actors gain access to all keys by breaching a single company

Your credential are only as protected as your most-vulnerable neighbor

Axiad Cloud's Customer-Segmented Authentication

Credentials are protected from others with airtight segmentation, including hardware-based storage



Bad actors cannot access your credentials by breaching another

Your keys to the kingdom are segmented, under your control, and optimally secure

Key Features

Comprehensive: Supports all Authentication methods and works with entire Identity ecosystem across the entire environment

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 Authenticators ranging from enterprise-grade mobile-based to government-grade AAL3
- Certificate-Based Authentication: Leverages an international standard X.509 certificate to interoperate across a broad range of vendor products
- Custom Certificates: Creates custom certificates and workflows
- Fully Customizable: APIs enable full integration with vendor products or custom software
- Interaction Certification: Certifies email senders and attachments

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

- Broad OS support: Secures Microsoft Windows, Apple OSs, Linux, and more
- Windows-friendly: Provides authentication across Windows ecosystem including Azure, Windows OS, and more
- Token Side-by-Side support: Leverages a wide array of physical and virtual tokens side-by-side
- Integrated: Supports wide range of protocols, connectors, and standards for interoperation across the Identity ecosystem out of the box

Secure Design: Architected for best-practices security including isolation by customer, encrypted communications, and key storage in specialized hardware

- Hardened Approach: Leverages the Axiad cloud platforms' private instance for each customer, private certificate store, and secure, encrypted network communications
- End-to-end Security: All entities are secured on the front-end with MFA or greater and on the back-end without using shared secrets so the authentication process is secure from end-to-end
- Asymmetric Cryptographic Authentication (ACA): Eliminates shared secrets with ACA so credentials cannot be intercepted in transit
- Hardware Root of Trust: Each customer's cryptographic information is stored in a dedicated Hardware Security Module (HSM) partition
- Customer Control: All customer data is under customer control & edited via Unified Portal
- Current Compliance: There is an annual SOC2 Type II audit of the security framework based on NIST controls

Efficient: Streamlines and automates workload for both IT and end users and minimizes implementation and management overhead

Operational Efficiencies: 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

Convenient Implementation: Minimizes overhead to implement

- Non-code Implementation: Makes implementation convenient with non-code integrations for major Identity vendors
- Proven Scalability: Is hosted by a name-brand CSP with very high scalability
- High Availability and Reliability: Is engineered for high reliability and availability
- Mix-and-Match: Supports any combination of the cloud product line for each organization

Benefits

Empower Users Across the Enterprise

Ensure employees can access what they need, when they need it, and without business disruption for optimized workforces.

Optimize Administrative Processes

Streamline processes for administrators and the help desk, lowering total identity security costs across the organization.

Enhance Your Cybersecurity Posture

Prevent phishing-based attacks with systematic policy application and enforcement, and take a step toward Zero Trust, with consistent authentication.

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.