Pragmatic Phishing Resistant Authentication for Government

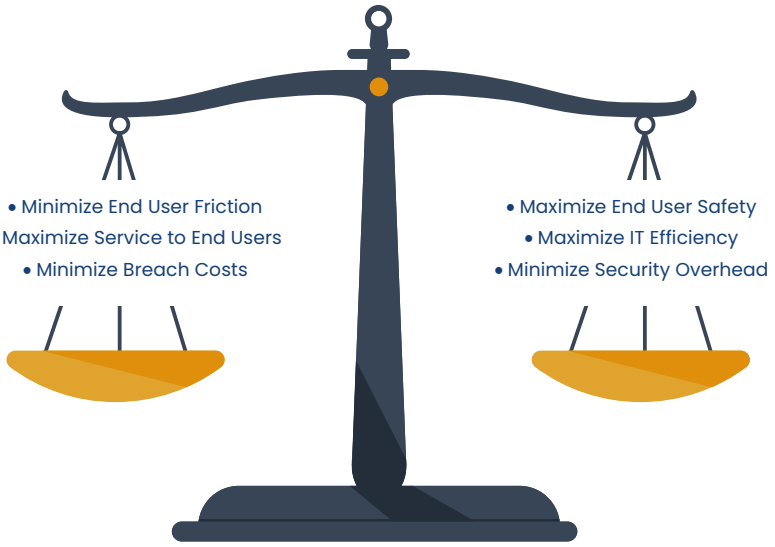
USE CASE

Overview of Use Case

In many important ways, authentication is a balancing act with key tradeoffs:

- End User: Minimum End User Friction is a tradeoff versus End User Safety since increasing security can increase the authentication burden on end users up to the limit where pushback occurs.
- IT Resources: Maximize Service to End Users trades off against IT efficiency since these services can drain scarce IT resources, particularly those that rely on Help Desk support.
- Overheard: Breach and other security downside costs are balanced against overall security budget since "bank vault-level" security may not be justifiable for all size of agencies.

Authentication Tradeoffs

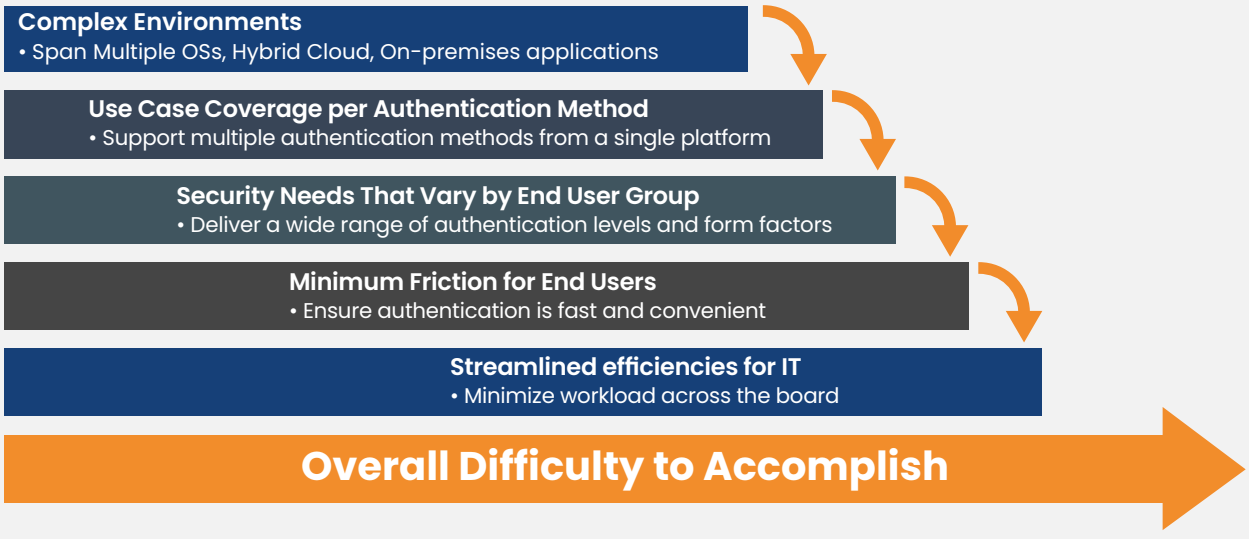


Challenges at Scale

As illustrated by the tradeoffs discussed above, phishing resistance challenges are interrelated. So, the challenges are not discrete but instead compound as each challenge is factored into the full picture:

- **Complex environments: Each major component (such as OS and cloud variant) adds complexity.**
- **Use Case Coverage: No authentication method covers all use cases.**
- **Group Needs: Different groups often require different levels of authentication.**
- **End User Friction: If friction is too high, end users push back.**
- **IT Efficiencies: Already-constrained IT resources need streamlined utilities to handle additional demands.**

Phishing Resistance Challenges Compound

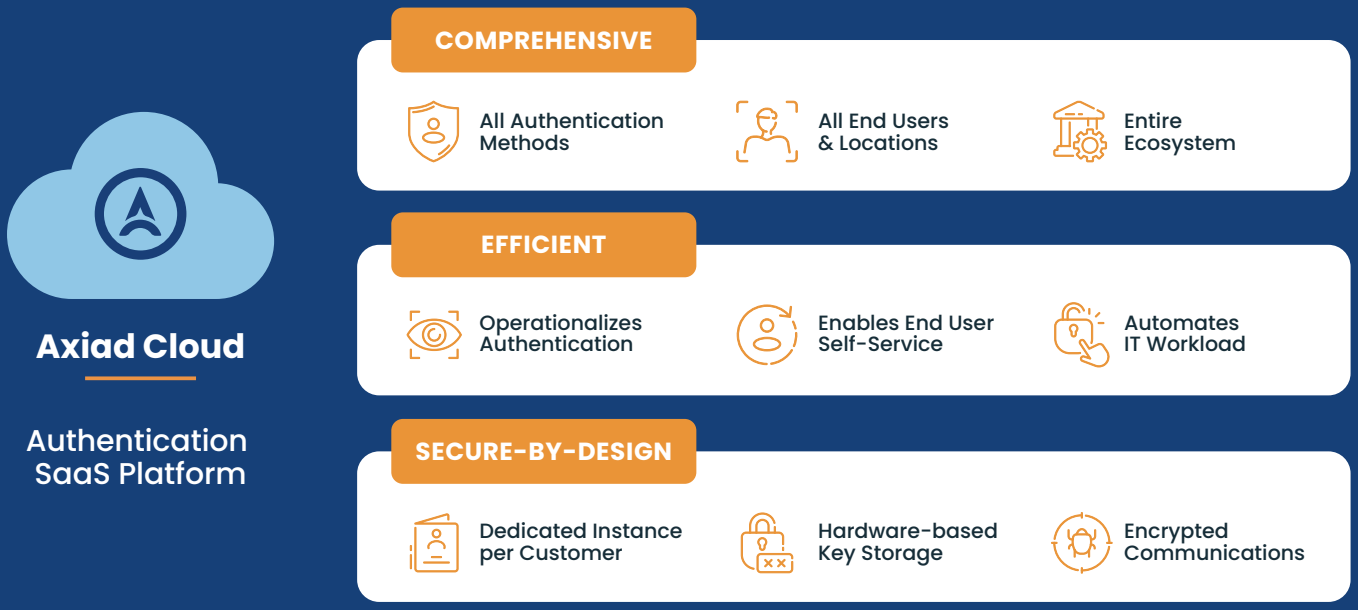


Phishing resistant authentication challenges build on each other, compounding implementation difficulties for agencies

Introducing Axiad Cloud

Overview

Axiad Cloud is a comprehensive, efficient, and secure authentication SaaS platform that eliminates silos across the environment. Architected for best-practices security, it enables "mix-and-match" use 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.



Capabilities

- **Comprehensive:** Supports all authentication methods across users, machines, and more while interoperating with the entire Identity ecosystem
- **Efficient:** Streamlines and automates help desk workload, enables end user self- service, and minimizes overall IT overhead
- **Secure-by-Design:** Architecture designed with best-practices security including a private instance for each customer, key storage in specialized hardware, and encrypted communications.

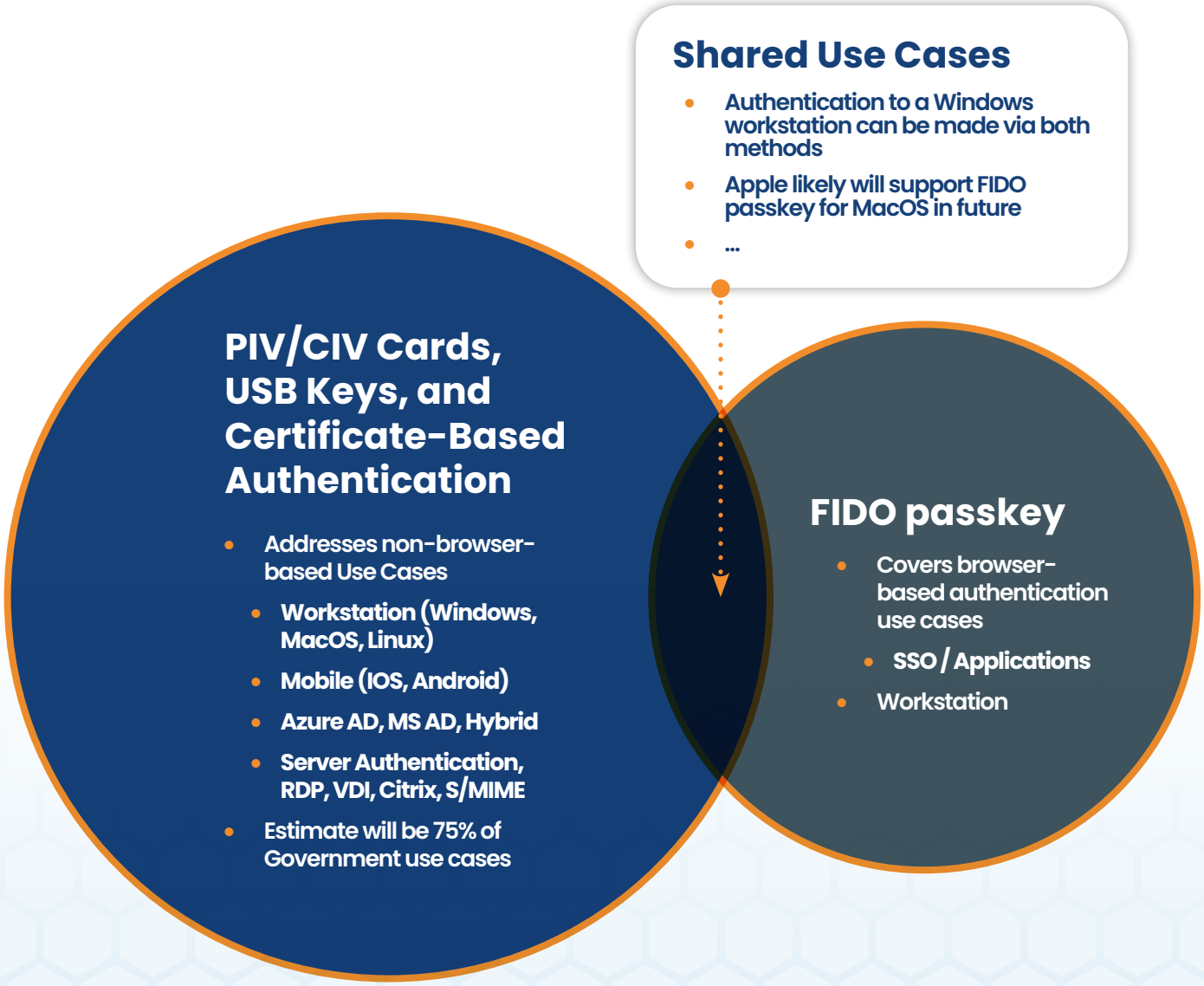
Pragmatic Phishing Resistance Overview

As shown in the previous section, a key advantage of the Axiad Cloud platform is support for multiple authentication methods including Certificate-Based Authentication (CBA) and FIDO passkey. This capability is of high value since Axiad estimates that PIV/CIV cards, USB Keys, and Certificate-Based Authentication (CBA) will in future handle 75% of use cases. FIDO passkey support provides future-proofing as Axiad estimates it will grow to 25% of use cases. (There are also use cases that are supported by both authentication methods today such as Windows workstation authentication and likely soon such as MacOS workstation authentication.)

Axiad believes that "Pragmatic Phishing Resistance" – supporting best-of-breed authentication methods today such as CBA while futureproofing with FIDO passkey – is the best strategy for government agencies. This strategy handles today's threats while increasing security levels over time to master tomorrow's threats.

Provide Broad Phishing Resistant Authentication

Solve Today's Problems with PIV / CBA and Future-proof with FIDO passkey



"Pragmatic Phishing Resistance" is the optimum strategy today for agencies of all sizes

Pragmatic Phishing Resistance – Two Options

To best illustrate pragmatic phishing resistance, two options have been selected:

- The first – **Enhance Security and Minimize Disruption** – describes how phishing-resistant authentication can be added to an existing environment without changing how authentication operates among 1 to many Identity Access Management (IAM) vendors.
- The second – **Maximize Security and Get More from Investments** – outlines a scenario where authentication is centralized by Axiad, thereby extending existing investments in IAM vendors' products as well as infrastructure components provided by Microsoft.

Option 1 – Enhance Security and Minimize Disruption

With this option, Axiad handles the authentication management lifecycle (discussed in a dedicated use case) for the organization's choice of phishing-resistant authenticators. Key attributes:

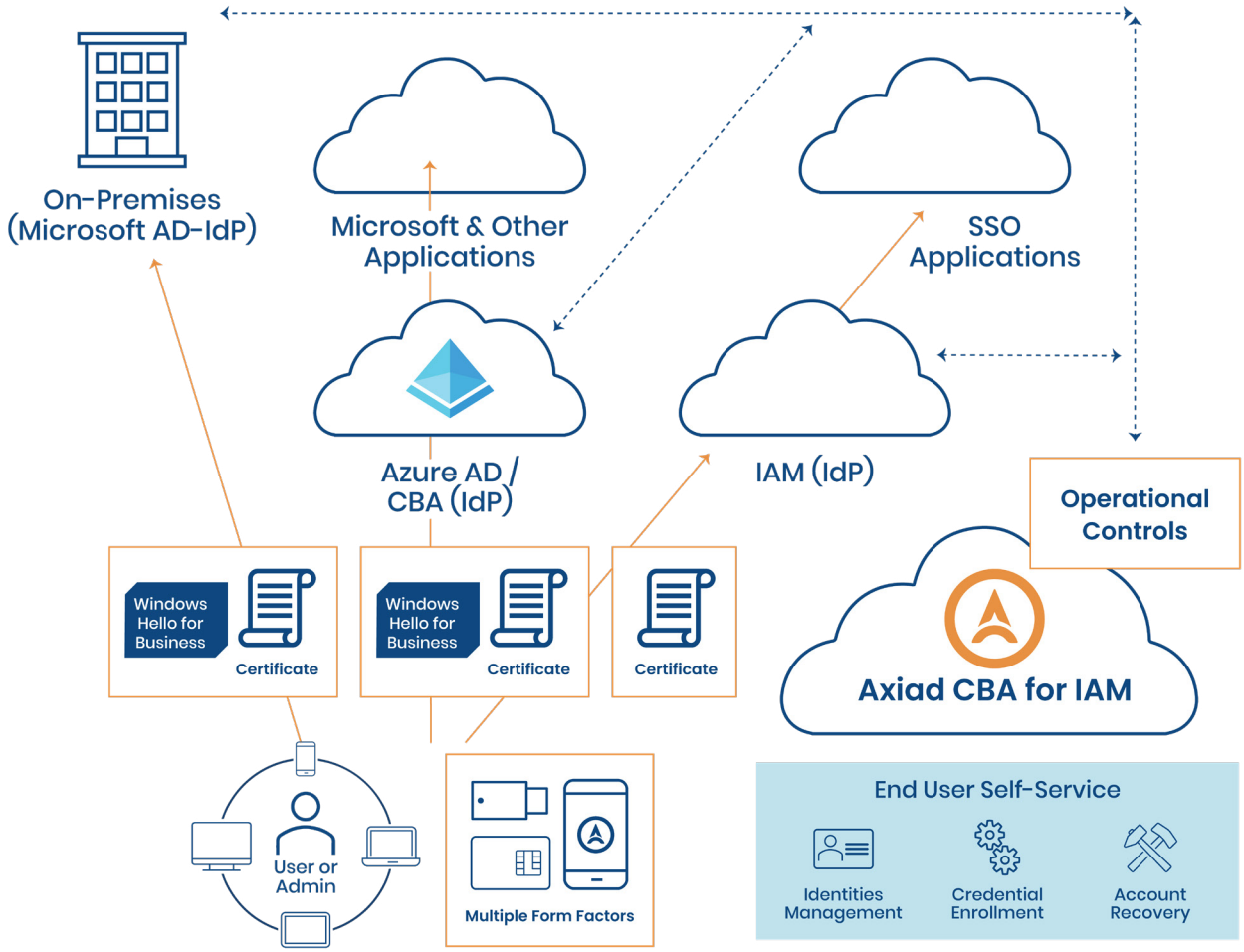
- Challenges: Challenges experienced by government agencies include:
  - Siloed Infrastructure: Siloed authentication typically results in poor end user experience as well as increases the security exposure surface.
  - Enrollment and Renewal: Phishing-resistant authenticators are challenging for IT to roll out and periodically renew due to high manual effort and support needs.
  - Skills Shortage: Key authentication infrastructure skills, such as Certificate-Based Authentication and Public Key Infrastructure (PKI), are in short supply.

- Pragmatic Phishing Resistance: For this scenario, Axiad Certificate-Based Authentication (CBA) for IAM "bolts on" to the existing infrastructure including IAM systems. Credentials that can be leveraged are Certificates and Windows Hello for Business. Key attributes:
  - End user self-services CEAR: Credential Enrollment and Account Recovery (CEAR) is performed by end users in self-service mode, thereby offloading IT.
  - Phishing resistance is fully enabled: By using strong authenticators consistently across the environment, phishing resistance becomes the baseline security across the agency.
  - Current: Operational controls keep Axiad CBA for IAM in sync with each IdP.

- Business Outcomes
  - Non-disruptive: Since authentication is performed by the installed system (IAM, Azure AD, and Microsoft AD), existing systems are not disrupted.
  - Maximizes Acceptance: With helpful self-service utilities replacing onerous and lengthy calls to Help Desk, end user acceptance is maximized.
  - IT Productivity: By being offloaded by self-service for end users and made more efficient with specialized utilities, IT productivity is significantly enhanced.
  - Increases Investment Return: By improving security without requiring upgrades, this option increases the return on investment for both infrastructure (e.g., Microsoft AD) and IAM products.

Pragmatic Phishing Resistance

Option 1 Enhance Security and Minimize Disruption



Phishing-resistant authentication can be "bolted on" to upgrade authentication for on-premises and IAM systems

Option 2 – Maximize Security and Get More from Investments

With this option, Axiad adds a unified Identity Provider (IdP) capability and an additional authenticator option (FIDO passkey) to the authentication management lifecycle (discussed in a dedicated use case) from option 1. Key attributes:

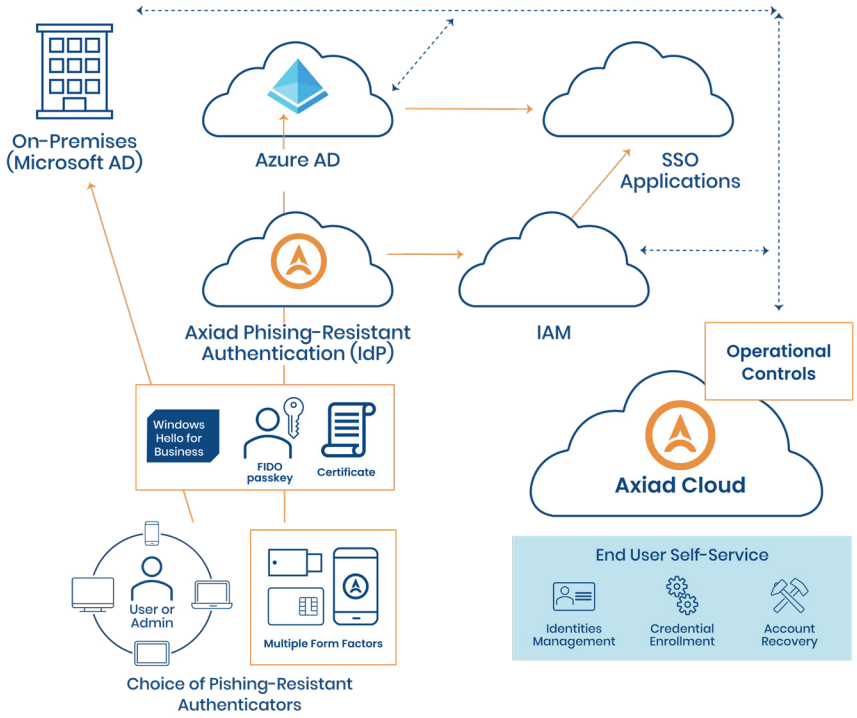
- Challenges: Challenges experienced by government agencies include:
  - Siloed Infrastructure: Siloed authentication typically results in poor end user experience as well as increases the security exposure surface.
  - Enrollment and Renewal: Phishing-resistant authenticators – including FIDO passkey – are challenging for IT to roll out and periodically renew due to high manual effort and support needs.
  - Skills Shortage: Key authentication infrastructure skills, such as Certificate-Based Authentication and Public Key Infrastructure (PKI), are in short supply.

- Pragmatic Phishing Resistance: For this scenario a combination of FIDO passkey and Certificate-Based Authentication (CBA) are the optimal authentication methods. Credentials that can be leveraged are Certificates, FIDO log-on, and Windows Hello for Business. Key attributes:
  - End user self-services CEAR: Credential Enrollment and Account Recovery is performed by end users in self-service mode, thereby offloading IT.
  - Phishing resistance is fully enabled: By using strong authenticators consistently across the environment, phishing resistance becomes the baseline security across the agency.
  - Identity Provider: A strategic Axiad package, Axiad Phishing-Resistant Authentication, consolidates authentication for the entire environment.
  - Current: Operational controls keep Axiad Cloud in sync with each IdP.

- Business Outcomes
  - Maximizes Flexibility: With an authentication platform that supports a broad range of phishing-resistant authenticators and credentials, the organization can ensure secure authentication for every need.
  - Increases Investment Return: By improving security without requiring upgrades, this option increases the return on investment for both infrastructure (e.g., Microsoft AD) and IAM products.
  - Maximizes Acceptance: With helpful self-service utilities replacing onerous and lengthy calls to Help Desk, end user acceptance is maximized.
  - IT Productivity: By being offloaded by self-service for end users and made more efficient with specialized utilities, IT productivity is significantly enhanced.

Pragmatic Phishing Resistance

Option 2 Maximize Security and Get More from Investments



Centralized phishing-resistant authentication increases security and adds life to existing infrastructure and IAM investments

Unique Authentication Management Capabilities

As of this writing, Axiad's approach provides capabilities that cannot be matched elsewhere:

- Complex Environment Support: Axiad supports complex environments across OSs (Windows, MacOS, and Linux), hybrid environments (Microsoft AD, Azure AD), and multiple IAMs (such as Okta, Ping Identity, and Azure AD).

- Full Use Case Coverage: Axiad's Cloud Platform supports multiple authentication methods seamlessly including Certificate-Based Authentication (CBA), FIDO passkey, Phishing-Resistant MFA, and PKI.

- Authentication Matched to Department Need: Axiad supports varying authentication levels by department such as PIV cards for the Finance team and USB Keys for everyone else.

- High End User Satisfaction: Axiad enables end users to self-service the authentication management lifecycle from initial enrollment through account recovery, thereby minimizing end user friction and increasing satisfaction.

- Maximized IT Efficiencies: IT efficiencies are maximized via leveraging Axiad's utilities for authentication lifecycle management and via enabling end users to self-serve most of their authentication needs.

Benefits for this Use Case

Continuing the balancing analogy from the introduction, these pragmatic phishing resistance use cases provide a win-win perspective from the perspective of the End User, IT, and the budget.

Maximize End User Security

Passwordless, phishing-resistant authentication maximizes end user security while minimizing friction

Maximize IT Efficiency

By operationalizing authentication into playbooks, IT efficiency is maximized

Minimize Security Overhead

By minimizing breach costs and by streamlining effort for end users and IT, overall security overhead is minimized

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.