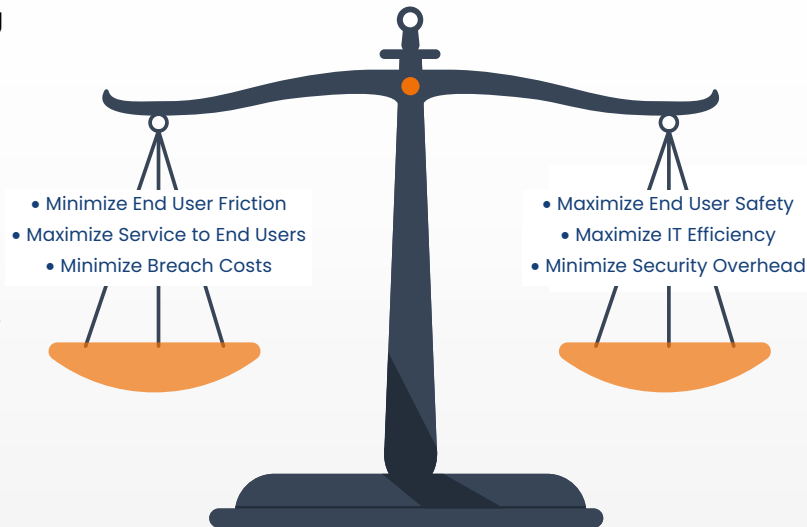# Pragmatic Phishing Resistant Authentication for Government

AXIAD

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

- Minimize End User Friction
- Maximize Service to End Users
- Minimize Breach Costs

- Maximize End User Safety
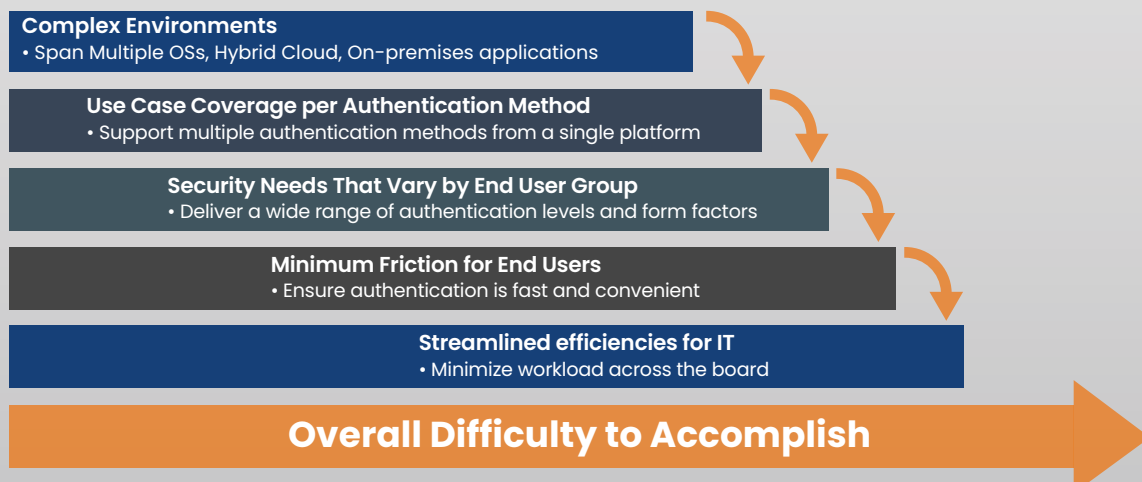- Maximize IT Efficiency
- Minimize Security Overhead

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

Complex Environments
• Span Multiple OSs, Hybrid Cloud, On-premises applications

Use Case Coverage per Authentication Method
• Support multiple authentication methods from a single platform

Security Needs That Vary by End User Group
• Deliver a wide range of authentication levels and form factors

Minimum Friction for End Users
• Ensure authentication is fast and convenient

Streamlined efficiencies for IT
• Minimize workload across the board

Overall Difficulty to Accomplish

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

INTRODUCING AXIAD CONDUCTOR

Axiad Conductor 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 Conductor 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.

Axiad Conductor

Authentication
SaaS Platform

COMPREHENSIVE

All Authentication Methods

All End Users & Locations

Entire Ecosystem

EFFICIENT

Operationalizes Authentication

Enables End User Self-Service

Automates IT Workload

SECURE-BY-DESIGN

Dedicated Instance per Customer

Hardware-based Key Storage

Encrypted Communications

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.
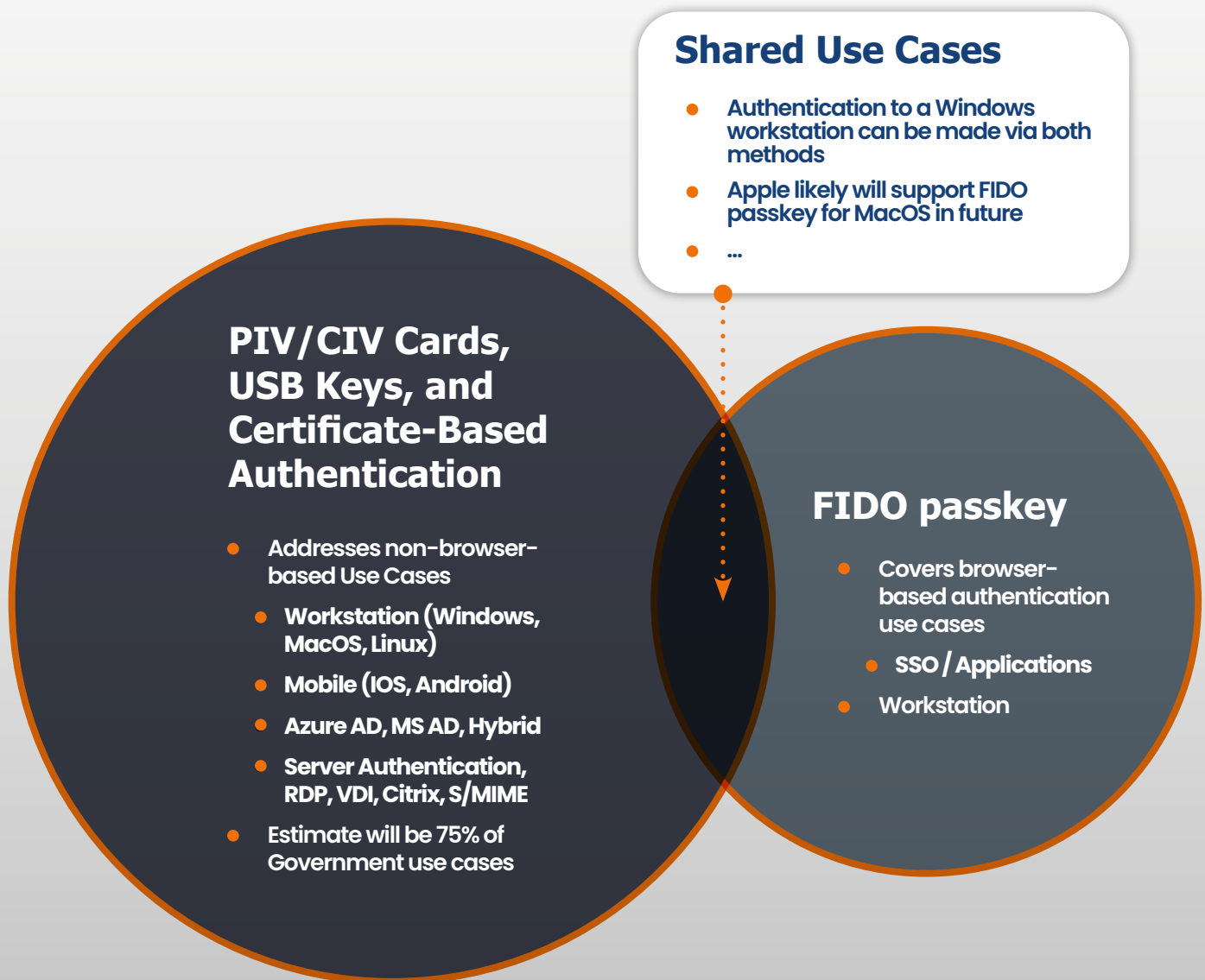
PRAGMATIC PHISHING RESISTANCE OVERVIEW

As shown in the previous section, a key advantage of the Axiad Conductor 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

Shared Use Cases

- Authentication to a Windows workstation can be made via both methods
- Apple likely will support FIDO passkey for MacOS in future
- …

PIV/CIV Cards, USB Keys, and Certificate-Based Authentication

- Addresses non-browser-based Use Cases
  - Workstation (Windows, MacOS, Linux)
  - Mobile (IOS, Android)
  - Azure AD, MS AD, Hybrid
  - Server Authentication, RDP, VDI, Citrix, S/MIME
- Estimate will be 75% of Government use cases

FIDO passkey

- Covers browser-based authentication use cases
  - SSO / Applications
- Workstation

"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.
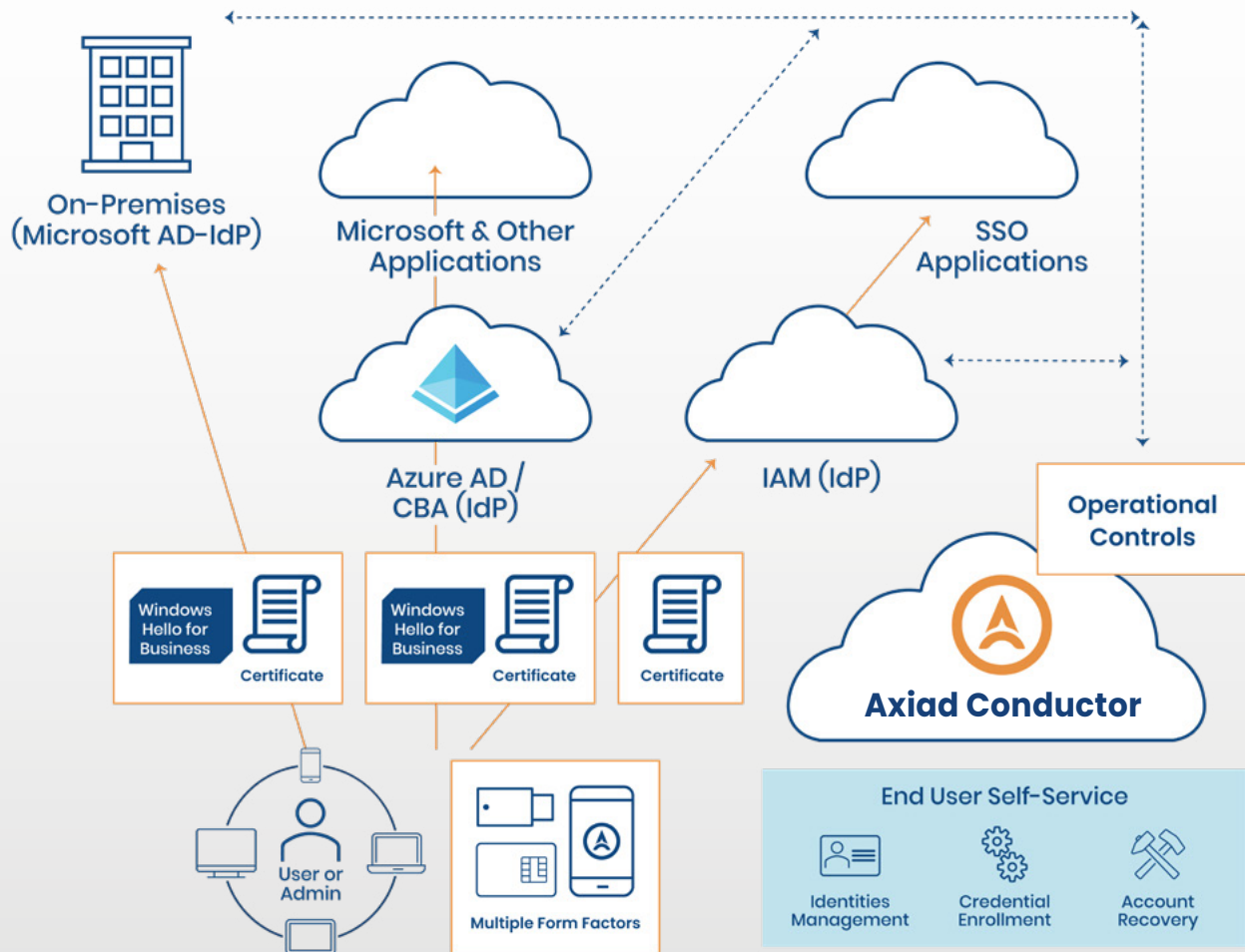
Option 1 – Enhance Security and Minimize Disruption

With this option, Axiad handles the authentication management lifecycle 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 Conductor's 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

On-Premises (Microsoft AD-IdP)

Microsoft & Other Applications

SSO Applications

Azure AD / CBA (IdP)

IAM (IdP)

Operational Controls

Windows Hello for Business — Certificate

Windows Hello for Business — Certificate

Certificate

Axiad Conductor

User or Admin

Multiple Form Factors

End User Self-Service

Identities Management

Credential Enrollment

Account Recovery

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 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.

  - Current: Operational controls keep Axiad Conductor 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
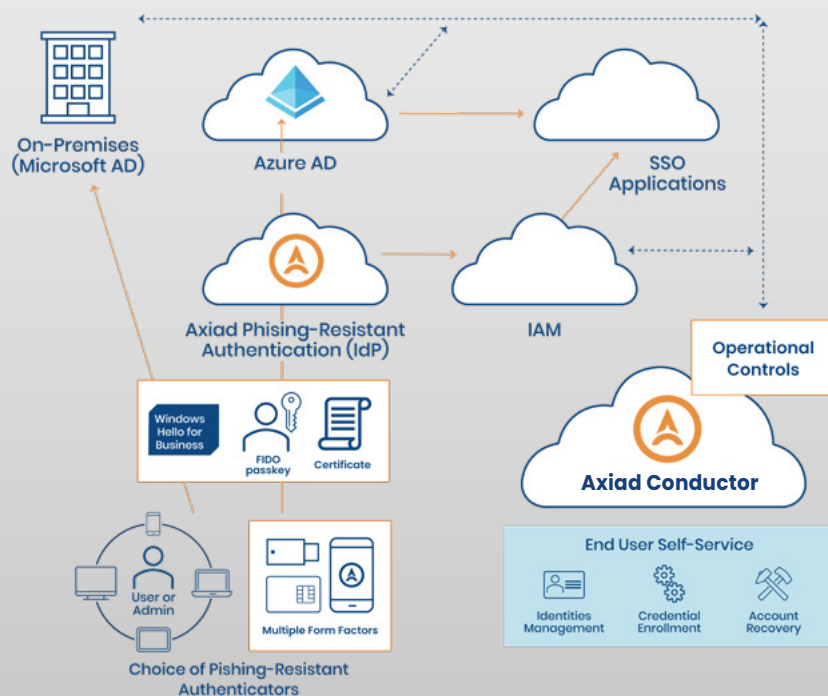
Centralized phishing-resistant authentication increases security and adds life to existing infrastructure and IAM investments

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: The Axiad Conductor 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 is an identity security company tackling the growing threat of compromised credentials, which drive over 70% of enterprise breaches. The sprawl of human and non-human identities across organization silos creates security blind spots that existing tools fail to secure. Axiad tackles this problem head-on, detecting identity risks and poor credential hygiene across systems, providing actionable insights, and enhancing security without needing a complete overhaul. Axiad makes identity simple, effective, and real. Discover more at _____ or follow us on _____.