Syberkey

OneBiold

Welcome to Post-Credential Security

Human Authenticity Infrastructure

From Credential Security → To Human Authenticity

Syberkey

OneBiold

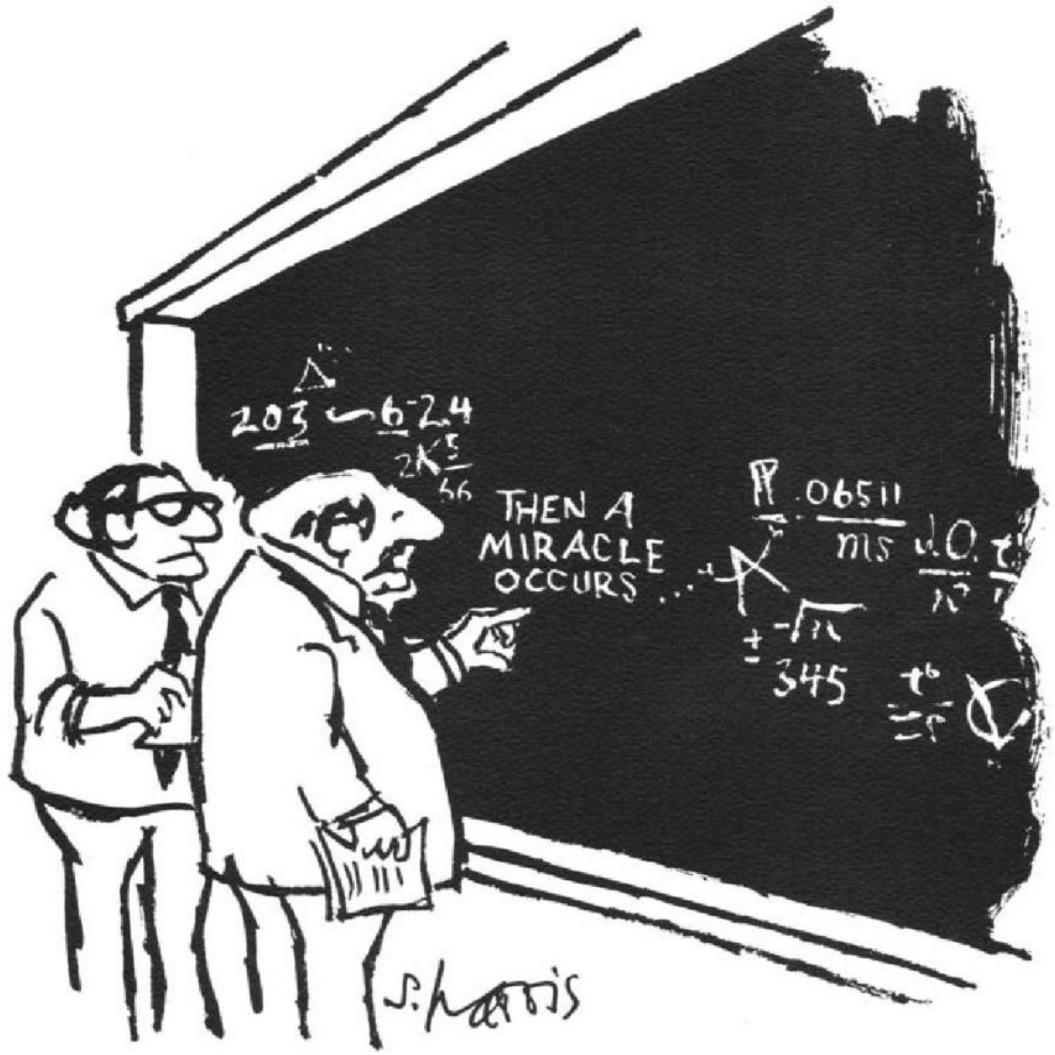
Welcome to Post-Credential Security

No OTP No Passwords

Live Biometrics Option from any Device

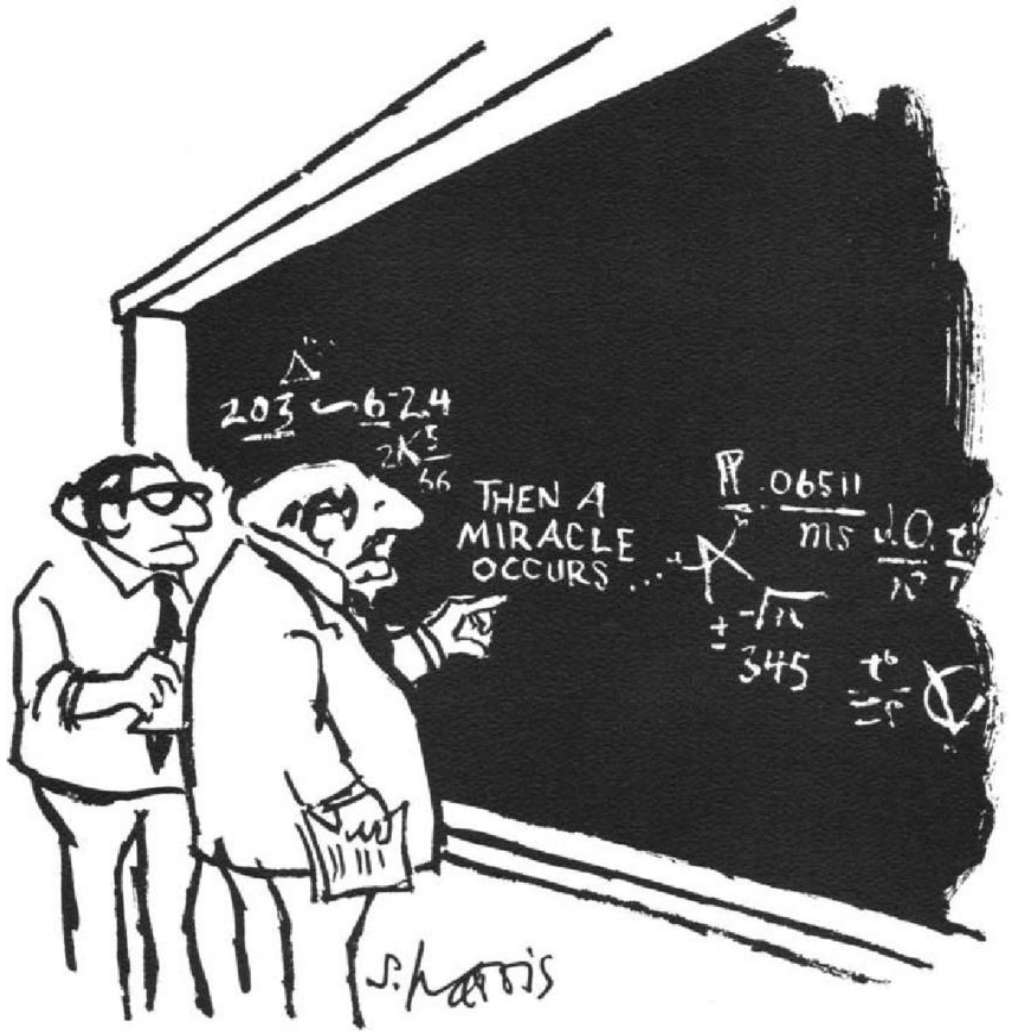
Patented Technologies

Current Situation



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Current Situation

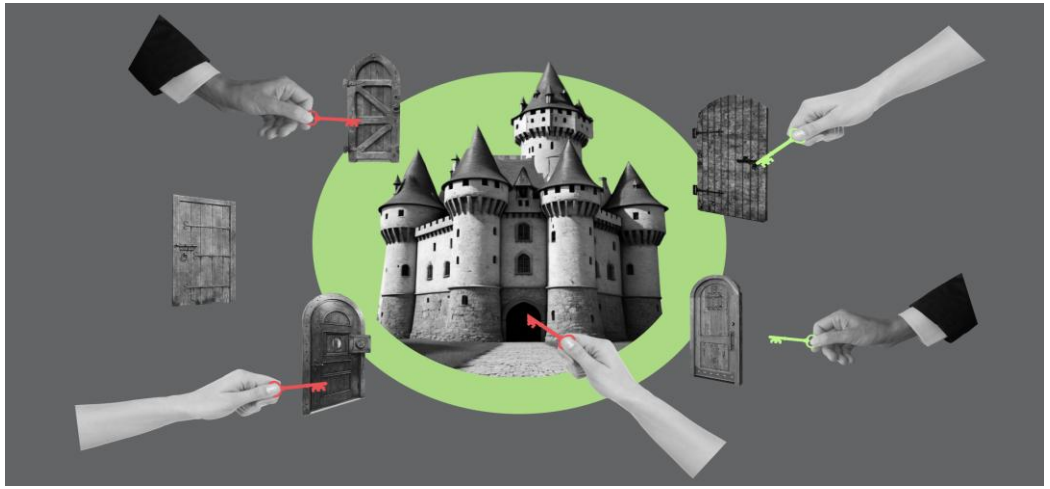


"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Our Mission: To Address These Market Realities

- **The Trend:** Stolen credentials have surpassed software exploits to become a leading initial access vector
- **The Scale:** * **Verizon (2025 DBIR):** Found that **68% of breaches** involved a human element, including stolen credentials, phishing, or social engineering.
- **IBM (2025):** Reports that the global average cost of a data breach has reached **$4.44 million**, with phishing as the most common entry point
- **Microsoft:** Detected **147,000 token replay attacks** in a single year, a **111% increase** year-over-year
- **The Trend:** "Identity Farming" and deepfake-as-a-service are being used to bypass biometric systems that lack advanced liveness detection
- **The Scale:** * **Projected Losses:** AI-driven fraud is projected to reach **$40 billion by 2027**, impacting sectors like banking and healthcare
- **Expert Quote:** > *"Millions on firewalls and encryption mean nothing if humans are the weakest link."* — **Kevin Mitnick**, late cybersecurity expert and author.

The Problem



Identity is the new perimeter

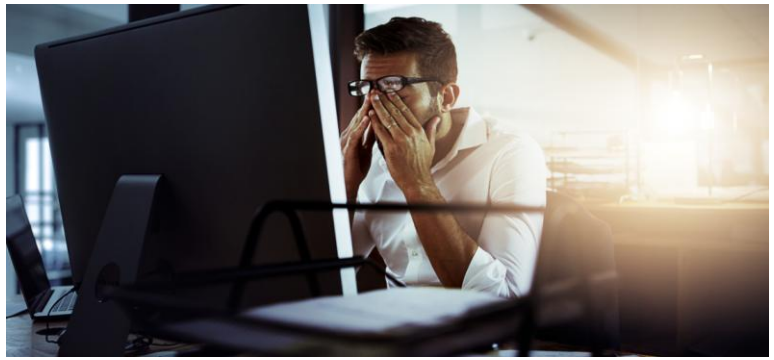
- 80%+ of breaches originate from credential misuse
- MFA fatigue attacks are increasing
- Session hijacking bypasses traditional IAM
- Vendor backend flaws create systemic exposure
- Quantum computing will break current crypto assumptions

The market still protects credentials.
No one has removed them.

Legacy Model	SyberKey Model
Identity = Credentials	Identity = Human
Secure login	Secure every action
Session trust	Continuous enforcement
Vault secrets	No secrets exist
Backend trust	Independent assurance layer

AI-generated identities and deepfake impersonations are increasing the risk of credential-based security models
These threats expose a fundamental limitation: digital systems verify credentials, but not human presence
Human Authenticity Infrastructure solves this gap

Rewriting the Architecture of Trust



Multi-factor authentication (MFA) challenges include user resistance due to increased friction, high implementation costs, and technical complexities with legacy systems. Vulnerabilities like MFA fatigue (prompt bombing), phishing attacks, and SIM swapping can bypass security, while lost devices cause account lockouts

- **User Friction and Adoption:** Users may resist MFA due to the inconvenience of extra steps, leading to low adoption rates or complaints about increased workload.
- **MFA Fatigue and Prompt Bombing:** Attackers spam users with authentication requests, hoping they will approve one out of frustration or confusion.
- **Security Vulnerabilities:** Attackers can bypass MFA through sophisticated phishing, session hijacking (stealing cookies), or SIM swapping to intercept SMS codes.
- **Implementation and Cost:** Integrating MFA into legacy systems or non-federated SaaS apps is technically complex and resource-intensive.
- **Device Dependency and Lockout:** If a user loses their phone, changes numbers, or has no connectivity, they may be locked out of their accounts, increasing IT support costs.
- **Privacy Concerns:** Users may hesitate to provide personal data like biometrics or private phone numbers for authentication purposes.
- **The fatal flaw of modern IAM** (Okta, Entra ID) is **'Session Trust.'** A single MFA event creates a static, hijackable session token, leaving the most critical internal actions vulnerable
- **80% of breaches involve compromised credentials** or session hijacking.

MFA still verifies credentials — not the human performing the action
The next step in identity security is verifying human presence and intention, not simply adding more authentication layers
SyberKey addresses this through Human Presence Verification

Rewriting the Architecture of Trust

Passwordless authentication replaces vulnerable, user-created passwords with inherently secure methods like biometrics (fingerprint/face), hardware keys, or magic links
. It is adopted to eliminate credential theft, phishing, and password fatigue while boosting user convenience and significantly reducing IT support costs for password resets

Key Reasons for Adopting Passwordless Authentication:

- **Enhanced Security:** By removing passwords, you eliminate the target for 18 billion+ annual attacks, including phishing, brute-force, and credential stuffing. It provides a stronger, single-action identity assurance.
- **Superior User Experience:** Users no longer need to remember, manage, or frequently update complex passwords, resulting in faster logins.
- **Reduced IT Costs and Burden:** Eliminating password reset requests and password lifecycle management significantly lowers help desk volume and operational costs.
- **Improved Productivity:** Eliminating password-related hurdles, such as lockouts and forgotten credentials, reduces time wasted, improving overall workflow

Passwordless authentication removes passwords, but identity is still tied to credentials or devices and therefore **doesn't not confirm human presence.**

SyberKey extends passwordless security by **verifying human presence during sensitive actions.**

Redefining the Root of Trust

Strategic Positioning Statement
SyberKey is a non static biometric digital credential security platform that replaces OTPs, passwords, tokens, and stored secrets with a continuously enforced, biometric-rooted trust fabric — securing identity, privilege, and data in a quantum-resilient architecture.

In traditional systems, trust is derived from credentials.
In SyberKey, trust is derived from **verified human identity and presence.**

From:
"IAM platform"

To:
Remote Digital Biometric Credential IAM Platform
+ AI layered
++ Post Quantum Resilient
+++ Cryptological Access Plane

Digital systems must now verify:
- the identity of the user
- the **presence of the human**
- the **intent behind the action**

SyberKey addresses this through **Human Authenticity Infrastructure**

Human Presence Verification ensures that the identity holder is physically present when sensitive actions occur.

From Identity Access to Human Authenticity Infrastructure (HAI)

SyberKey/OneBioID: The Missing Trust Layer for a Human Zero Trust World.

Integration Band

INTEGRATION LAYER: Works with Okta, Microsoft Entra ID, Google Workspace, SAP, and Core Financial Platforms.

Security Modules

SYBERKEY
(ACCESS)

Human Zero Trust Access.

Continuous identity verification beyond the login.

Eliminates session hijacking.

CPE
(CONTINUOUS ENFORCEMENT)

Continuous Pathway Enforcement.

AI-driven, action-based gating. PQC-ready for post-quantum resilience.

FINGERSIGN

Verifiable Digital Agreements.

Links every signature to a live human presence. Prevents contract repudiation.

VERIFIEDBIOMAIL

Human-Verified Email.

Authenticates the sender, not just the domain.

Eradicates Executive Impersonation & BEC.

Infrastructure Plane
(The Platform)

HUMAN AUTHENTICITY INFRASTRUCTURE (HAI)

The missing trust layer for the digital world.

Real-Time Human Presence Verification | Verifiable Action Certificates

Core Hub
(The Root)

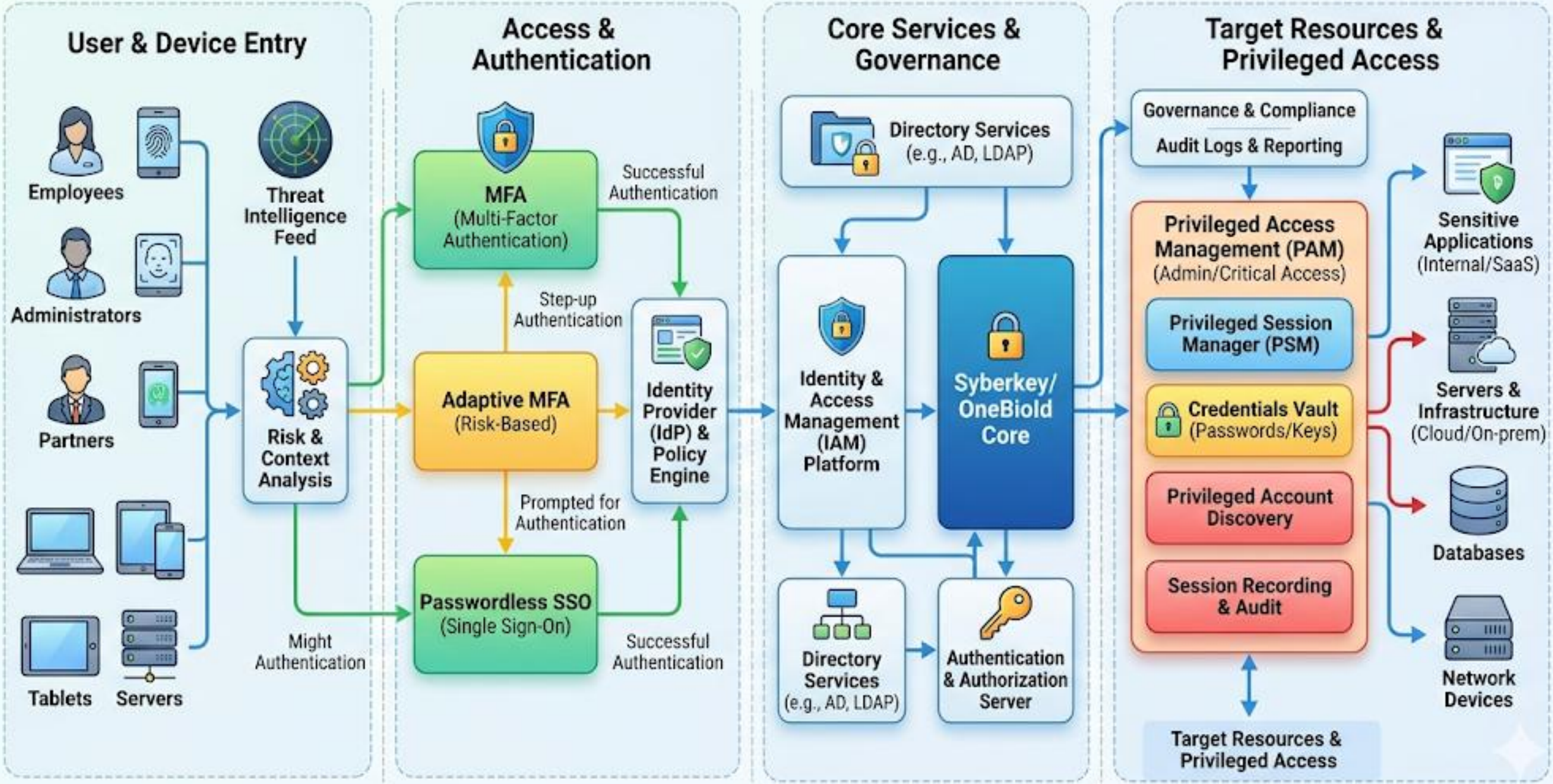
ONEBIOID™

The Single, Portable Human Identity Root.

Hardware-Free | Privacy-Preserving | Self-Sovereign

Never Trust the Session. Verify the Human. At the Moment of Action.

Syberkey/OneBiold: Unified IAM & PAM Architecture



Market Size

Positioned across combined markets:

- **IAM – Identity Access Management** (USD 18–22 billion in 2025 - exceed USD 40–70 billion by 2030–2034)
- **MFA – Multi Factor Authentication** (USD 21–22 billion in 2025 – exceed USD 50–70 billion by 2030-2034)
- **PAM – Privileged Access Management** (USD 3 billion in 2025 – exceed USD 7-10 billion by 2030-2034)
- **Zero Trust** (USD 37 billion in 2025 – exceed USD 90-190 billion by 2030-2034)
- **Identity Governance** (USD 9 billion in 2025 – exceed USD 27-33 billion by 2030-2034)
- **Post-Quantum Security** (USD 1 billion in 2025 – exceed USD 8 billion by 2030-2034)

We are creating a **multi-billion TAM intersection**, not a niche.

Rewriting the Architecture of Trust

Why Now

1. Entra Actor token class vulnerabilities expose backend fragility
2. Deepfake + synthetic identities are surging
3. PQC mandates are emerging in government
4. MFA fatigue attacks have become normalised
5. CISO's are shifting from detection → prevention

Our Moat

- Credential elimination architecture
- Action-bound biometric approval
- PQC-native identity binding
- Patent-pending Continuous Pathway Enforcement
- Independent cryptographic audit chain

Start with Pain

"Your IAM stack protects logins. Attackers don't attack logins anymore."

"Your biggest exposure isn't authentication failure — it's trusted sessions being abused."

"What if credentials simply didn't exist?"

"We have spent 25 years protecting credentials. Attackers have spent 25 years stealing them."

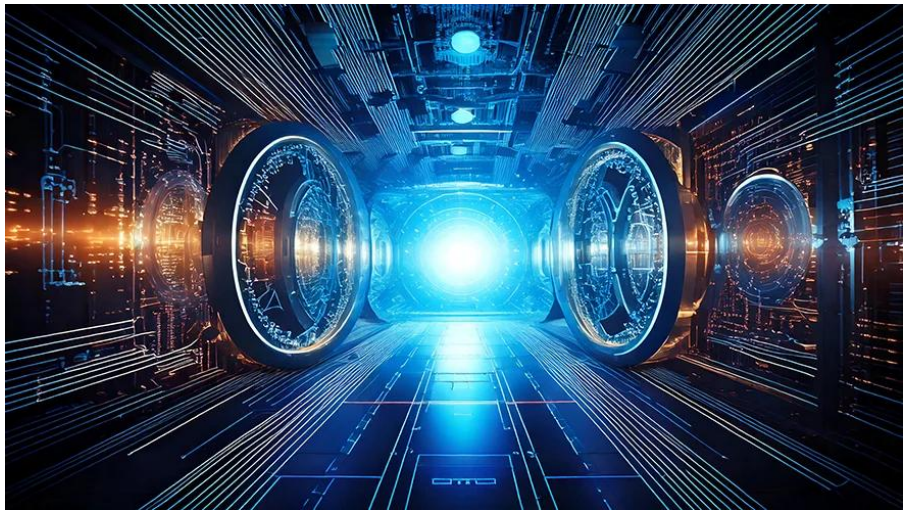
"Maybe the problem isn't how we protect credentials.

Maybe the problem is that credentials exist at all."

AI-generated voices, faces, and identities are making credential-based authentication increasingly unreliable.
This creates a need for systems that **verify real human presence**

Human Authenticity Infrastructure: from Credential Security → to Human Authenticity

Quantum-Ready Identity

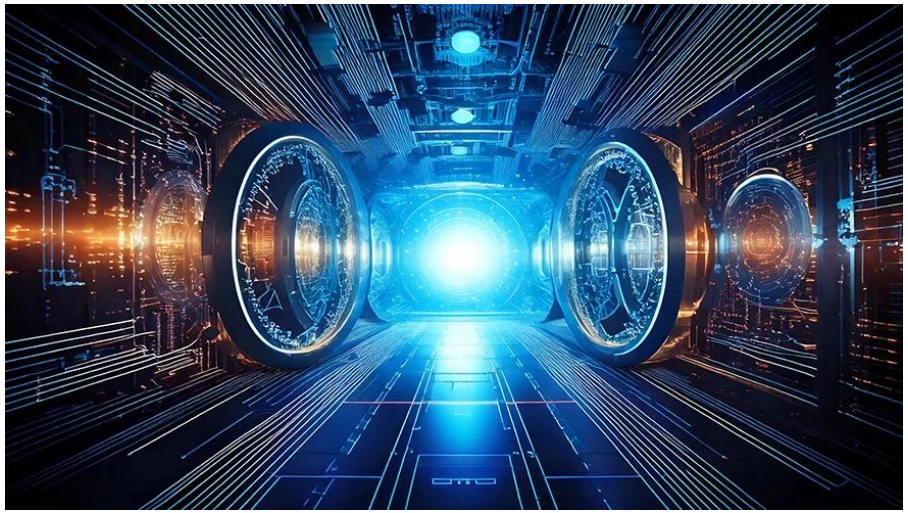


The "Harvest Now, Decrypt Later" Quantum Threat

Adversaries are currently stealing encrypted data with the intent to decrypt it once quantum computers reach sufficient power.

- **The Trend:** Organizations are moving toward "Quantum-Resilient" or Post-Quantum Cryptography (PQC) standards to protect long-term data.
- **The Scale:** * **Gartner:** Forecasts that current asymmetric cryptography (like RSA) must be retired by **2029** to remain secure.
- **DigiCert/NIST:** The first three post-quantum algorithms (FIPS 203, 204, and 205) have been standardized for encryption and authentication.
- **Expert Quote:** > *"Post-quantum cryptography is a critical component of future-proofing organizations... Gartner anticipates this being a critical component of the 2025 Hype Cycle for Digital Identity."* — **Gartner (2025 Hype Cycle)**.

Quantum-Ready Identity



From Identity "Layers" to "Identity Fabric"

The market is shifting away from siloed security tools toward a "connected system" that governs every action, not just the login.

- **The Trend:** The shift toward **Zero Trust Network Access (ZTNA)** where "continuous verification" is the standard.
- **The Scale:** * **Gartner:** Estimates that by 2025, over **60% of enterprises** will phase out traditional VPNs in favor of ZTNA and identity fabrics.
- **Expert Quote:** > *"Identity is the core—the Control Plane—not a layer... The way to fix fragmentation is by approaching identity as a connected system."* — **Gartner IAM Summit 2025 Analysis**.

Syberkey/OneBioID Integrated Identity & Access Governance Architecture

Unified, Patented Bio-Auth Powered IAM & PAM Solution

Identity Onboarding & Discovery

Unified Identity Store → Identity Discovery & Assessment → Directory Services → No Scanners/Tokens → One-Time Enrollment

Patented Bio-Auth Engine

- **Hardware-Free Biometric Verification**
  Biometric nullswaok verification, dropenaiist, and flaces with the biometric verifications
- **Human-Stored Credentials**
  Human-stored human-stored credentials toiupron the customer-erized featurees
- **Bio-Auth Core**
- **Cryptographic Binding (CPE)**
- **FIDO2 & WebAuthn Native Support**
  FIDO2 & WebAuthn, crertification, wnltconten, rative cryptographic and WebAuthn native support

Core Services

- **IAM Unified Platform**
  - Policy Engine
  - Adaptive MFA
  - Passwordless SSO
- **Syberkey/OneBioID Core**
- **PAM Integrated Platform**
  - Privileged Session Manager (PSM)
  - Credentials Vault
  - JIT Access & Elevation

Enforcement & Audit

- **Compliance & Governance**
  - **Audit Logs & Reporting**
    Audit logs, logmons;annd and densnisvnrotimont reporting
  - **Verifiable Audit Trail**
    Verifiable molters pux and aoesnativis of audit trail
- **Verifiable Cryptographic Log of Biometric Approvals**
- PAM Recording & Audit
- User Access Logging

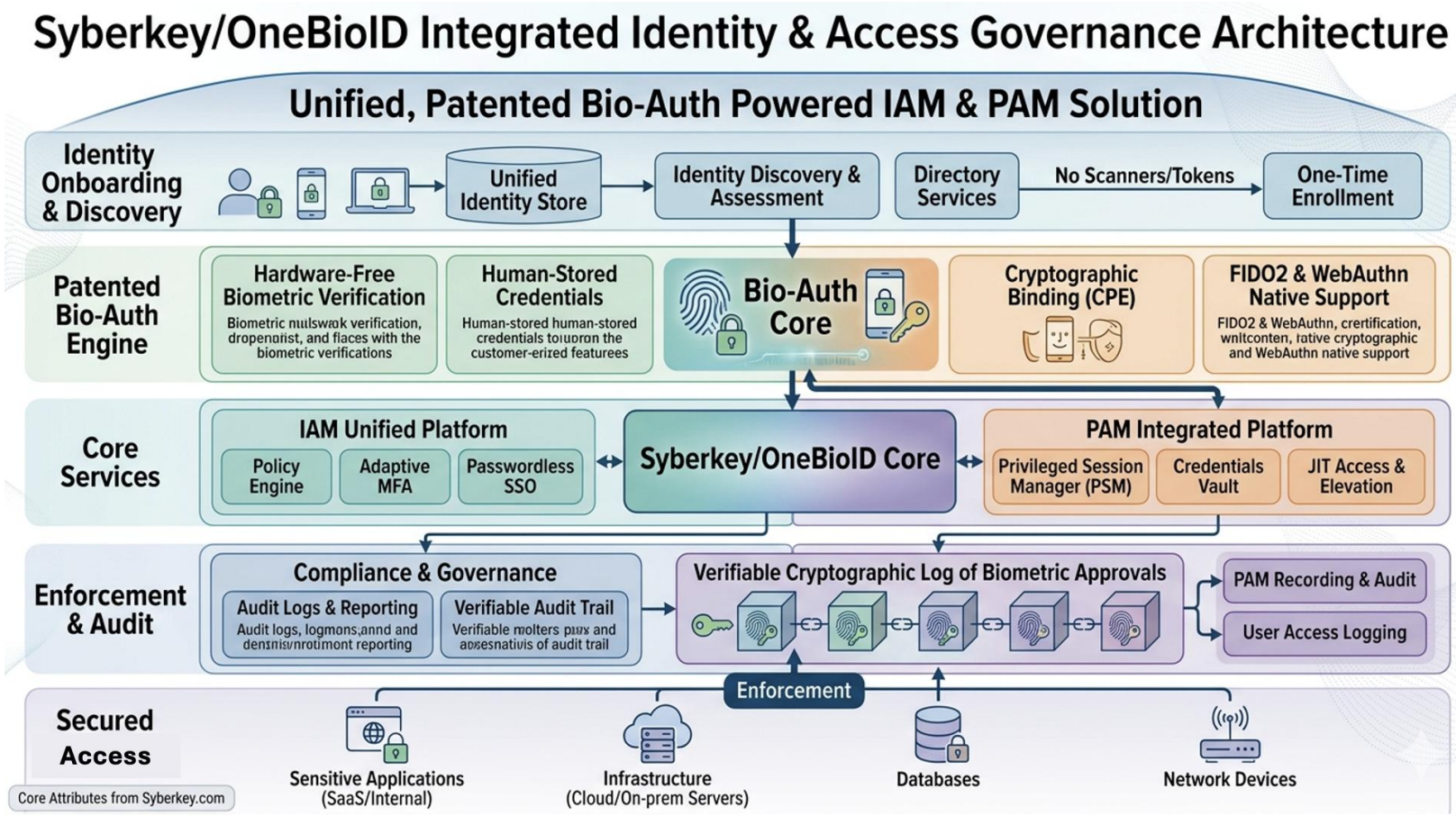
Secured Access

Enforcement

- Sensitive Applications (SaaS/Internal)
- Infrastructure (Cloud/On-prem Servers)
- Databases
- Network Devices

Core Attributes from Syberkey.com

We Don’t Strengthen Credentials…We Remove Them



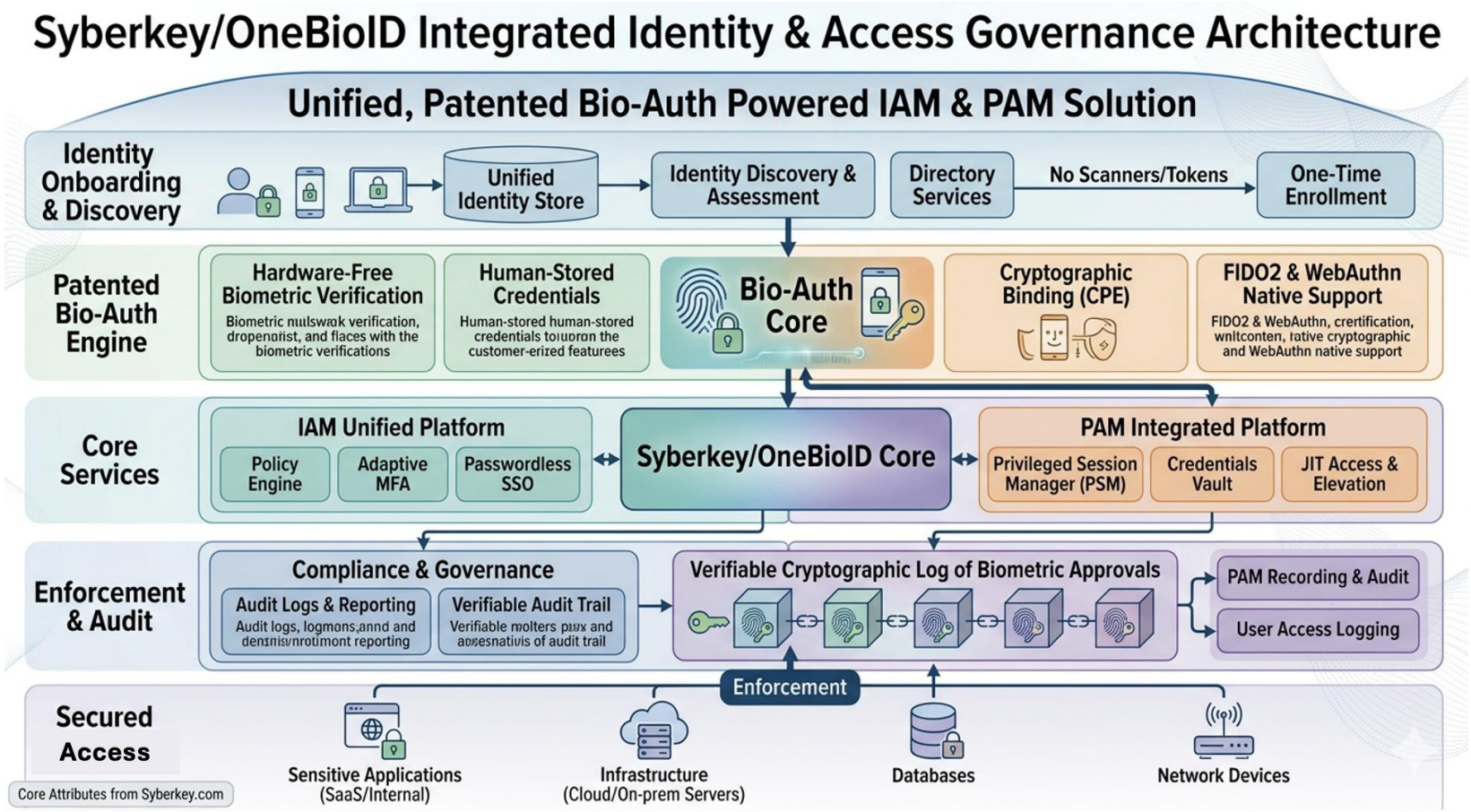
ARCHITECTURE:

OneBioID – biometric-rooted digital identity

- **Human Presence Verification** – live verification of the user
- **Continuous Pathway Enforcement** – policy control of actions

- Trust the Human. Not the Password
- Beyond Login. Beyond MFA
- Eliminate Credentials. Elevate Trust.
- The End of Reusable Identity
- Human-Rooted Security
- Control beyond Authentication
- Continuous Trust. Zero Secrets
- The Future of Identity Assurance

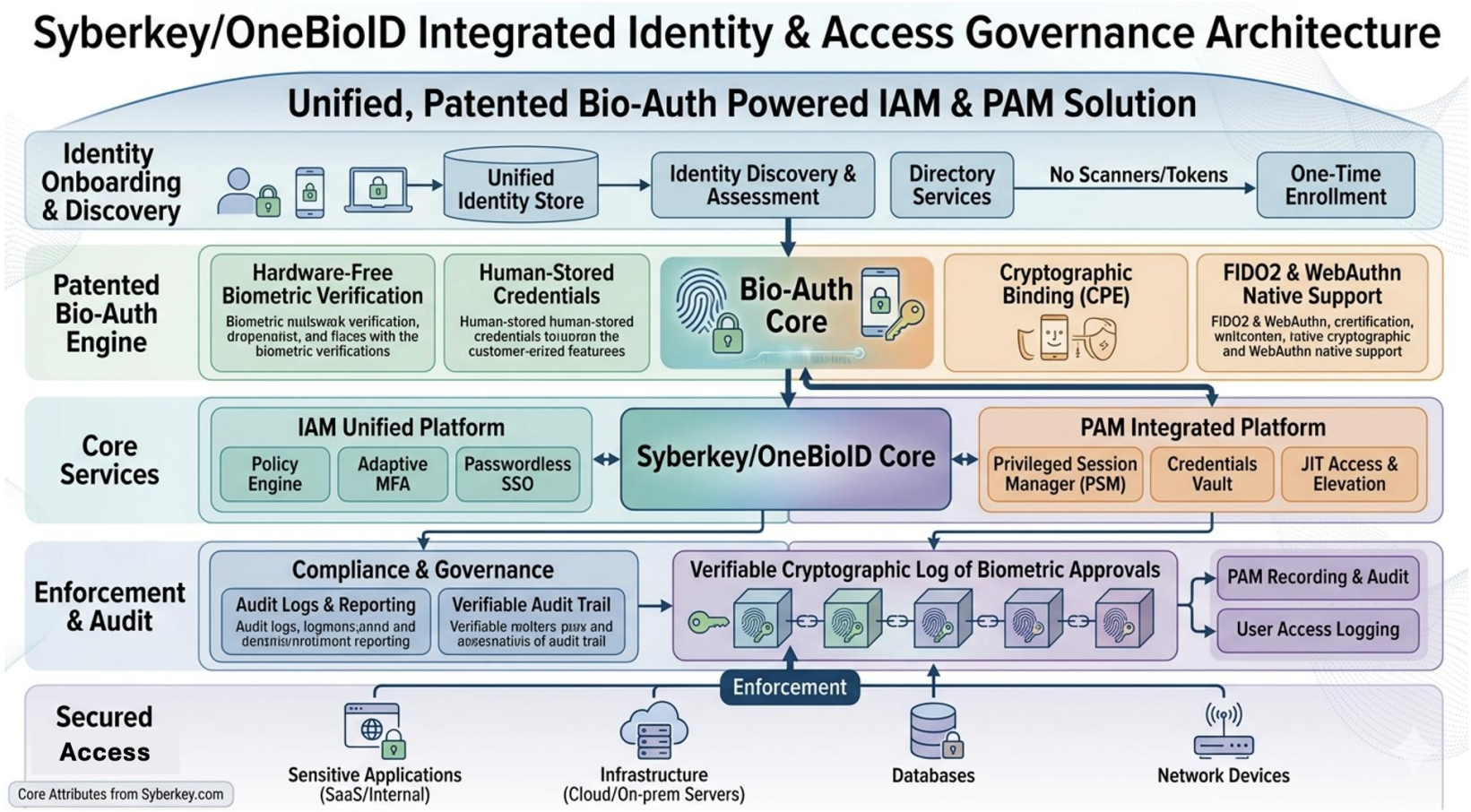
We Don’t Strengthen Credentials…We Remove Them



KEY DIFFERENTIATORS:

- **Hardware-Free OneBioID™**: Uses existing smartphones for unhackable biometric hashes.
- **Continuous Pathway Enforcement (CPE™)**: AI-driven, runtime control that gates actions, not just users.
- **Human Action Certificates**: The output of your system. It proves who authorized what and when.
- **Quantum-Safe (PQC-Ready): Cryptography** built for the next decade.

We Don’t Strengthen Credentials…We Remove Them



THE TECHNOLOGY:

1. **Identity Root:** User registers once with their portable, hardware-free OneBioID™.
2. **Action Trigger:** A sensitive system request (e.g., wire transfer, new admin user) automatically pauses execution and demands verification.
3. **Presence Assertion:** The user performs a local biometric check on their device, generating a non-repudiable Human Action Certificate that unlocks the task.

Red-Team Simulation Narrative

Scenario: Global Financial Services Enterprise

Environment:
Microsoft Entra ID, Okta for Partner Access, PAM Vault, MFA Push Approvals, Conditional Access Policies

Phase 1 – Initial Compromise

Attacker:
- Phishes a regional finance manager.
- Captures session token post-MFA.
- Performs token replay inside trusted session.

Traditional Stack Result:

- Login legitimate.
- Conditional Access satisfied.
- Session trusted for 8 hours.
- Privileged elevation requested.
- MFA fatigue push attack succeeds.

Blast radius:

Admin-level access obtained.

Phase 2 – Privilege Escalation

Attacker:
- Adds new Global Admin.
- Injects credential into service principal.
- Creates persistence mechanism.
- Exfiltrates financial data.

Traditional Detection:

- Logged.
- Flagged hours later.
- SOC response begins.

Damage already done.

Same Attack under Syberkey

Step 1 – Phishing

Password stolen?
Irrelevant. No password exists.

Step 2 – Token Replay Attempt

No reusable session token grants blanket privilege.

Step 3 – Privilege Escalation Attempt

Action requires:
- Live biometric approval
- Context validation
- Policy validation
- Cryptographic action binding

Attacker cannot generate human approval.
Escalation blocked.

Step 4 – Persistence Attempt

Service principal modification requires:
- Human-in-the-loop biometric sign-off
- Policy-bound approval

Blocked.

Same Attack Under SyberKey

Scenario: Global Financial Services Enterprise

Environment:

Microsoft Entra ID
Okta for partner access
PAM vault
MFA push approvals
Conditional Access policies

Step 1 – Phishing
Password stolen?
Irrelevant. No password exists.

Step 2 – Token Replay Attempt
No reusable session token grants blanket privilege.

Step 3 – Privilege Escalation Attempt
Action requires:
- Live biometric approval
- Context validation
- Policy validation
- Cryptographic action binding

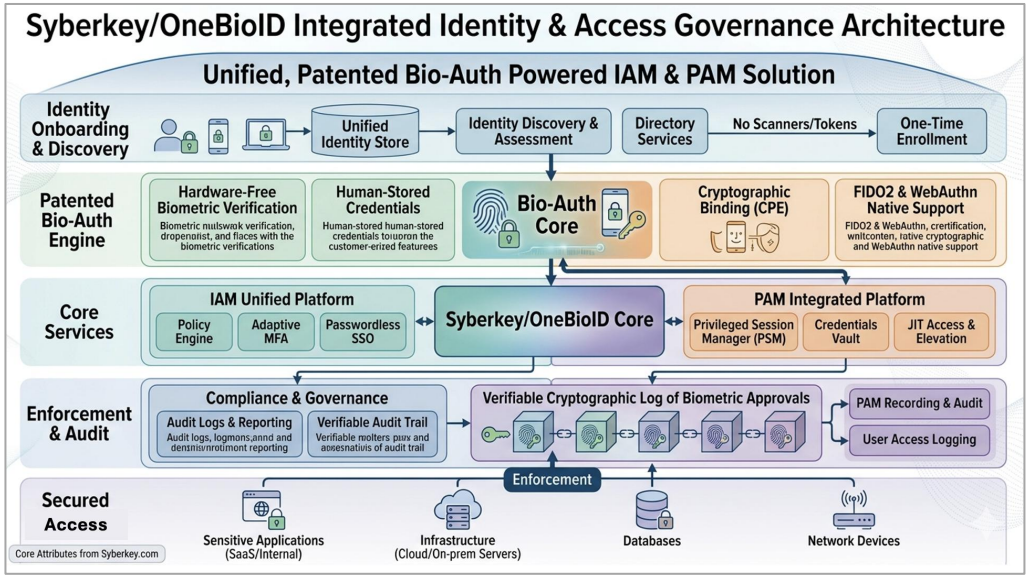
Attacker cannot generate human approval.
Escalation blocked.

Step 4 – Persistence Attempt
Service principal modification requires:
- Human-in-the-loop biometric sign-off
- Policy-bound approval

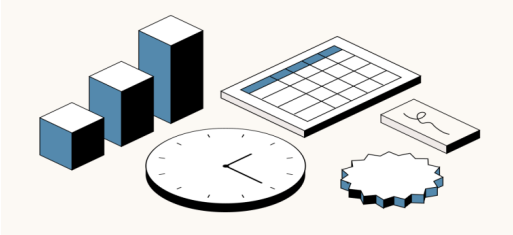
Blocked.

Red-Team Conclusion

Attack Stage	Traditional IAM	SyberKey
Phishing	High success	Neutralized
MFA fatigue	Exploitable	Not applicable
Session replay	Possible	No blanket trust
Privilege escalation	High risk	Biometric-gated
Persistence	Achievable	Human approval required
Blast radius	Tenant-wide	Action-contained



Ideal Customer Profiles (ICP)



We are not providing generic IAM.
We are providing:
- **Credential elimination**
- **Privileged action control**
- **Blast radius containment**
- **Quantum readiness**
- **Independent assurance layer**

Our ICP understands & reflects that.

ICP Tier 1 — High-Privilege, High-Regulation Enterprises
- 2,000–10,000 employees
- Complex IAM stack (often hybrid cloud)
- Mature SOC
- Board-level cyber oversight
- Significant privileged workflows
- Highly regulated industry

Target Industries
- Financial services
- Critical infrastructure
- Defense contractors
- Energy & utilities
- Healthcare systems
- Federal government contractors

Tech Environment
- Microsoft Entra ID
- Okta
- PAM (CyberArk, BeyondTrust, Delinea)
- SIEM (Splunk, Sentinel)
- Cloud (AWS / Azure / GCP)

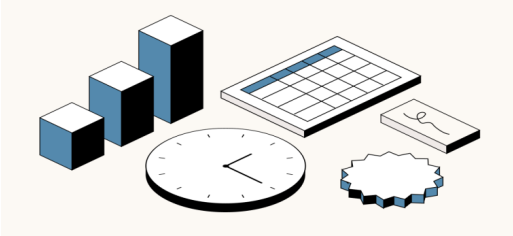
Buying Trigger Signals
- Recent audit findings around privileged access
- MFA fatigue incidents
- Insider threat concerns
- Service account sprawl
- Zero Trust transformation initiative
- Quantum-readiness policy discussion
- Board pressure after high-profile breach
- Change in regulations

Economic Buyer
- CIO / CTO / CDO
- CISO
- Deputy CISO
- Head of Identity
- VP Infrastructure Security

Why They Buy

Not for convenience.
They buy to:
- Adhere to regulations
- Become more secure
- Reduce blast radius
- Eliminate credential-based risk
- Strengthen privileged governance
- Provide board-level assurance

Ideal Customer Profiles (ICP)



We are not providing generic IAM.
We are providing:
- **Credential elimination**
- **Privileged action control**
- **Blast radius containment**
- **Quantum readiness**
- **Independent assurance layer**

Our ICP understands & reflects that.

ICP Tier 2 — Privilege-Heavy Organizations
These are not necessarily regulated — but privilege dense.

Examples:
- Fintechs
- SaaS platforms with admin tooling
- Crypto exchanges
- Payment processors
- Enterprise SaaS vendors

Why attractive:
- High-value admin accounts
- High reputational risk
- High attack probability
- API/service principal complexity

They understand session abuse risk.

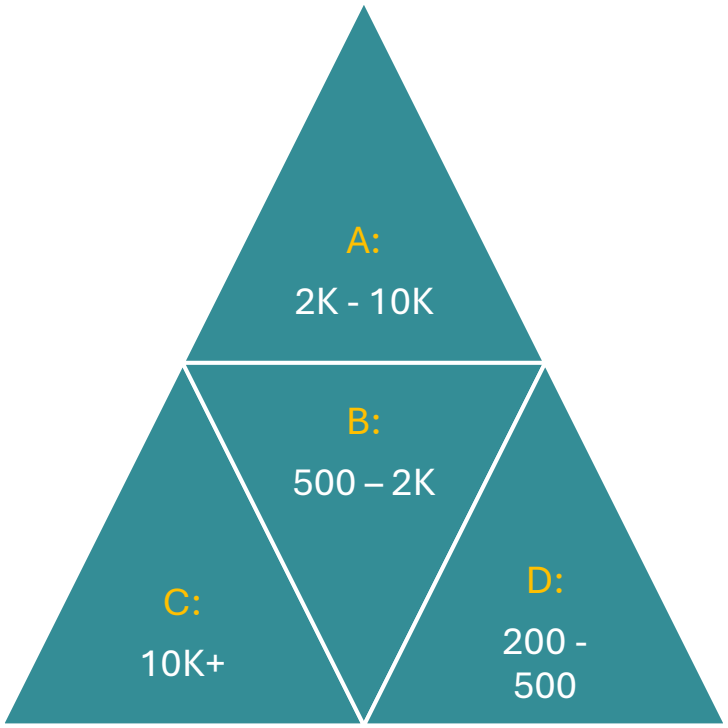
ICP Tier 3 — Government & Defense
Particularly attractive due to:
- Post-quantum mandates emerging
- Supply chain security requirements
- Insider threat concerns
- Auditability needs

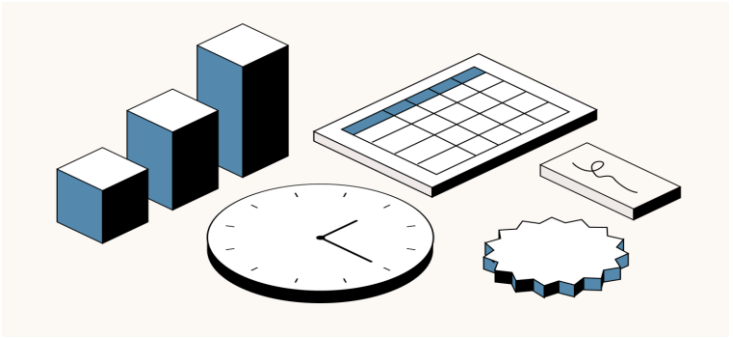
They are slower — but once landed, very sticky.

Who Is NOT Our ICP
Avoid:
- SMB under 500 employees
- Low-regulation industries
- Cost-driven IT buyers
- Organizations that view MFA as “solved”
- Pure consumer security markets

Your solution is architectural, not commodity.

Ideal Customer Profiles (ICP)





Criteria	Ideal	Not Ideal
Employee Count	2k+	<200
Privileged Density	High	Low
IAM Maturity	Advanced	Basic
Board Involvement	Active	Minimal
Regulatory Pressure	Medium–High	Low
Security Budget	Strategic	Tactical

Ideal Customer Profiles (ICP): Departments

CISO

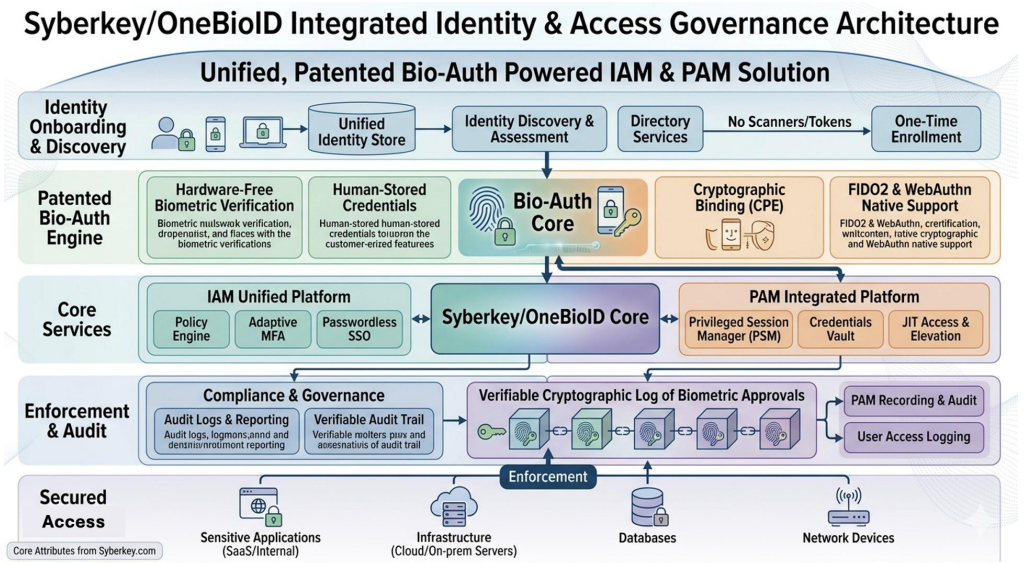
Identity Risk Reduction

CIO

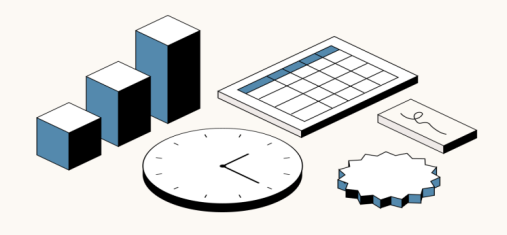
Infrastructure Assurance

CRO / Risk

Regulatory Exposure



Customer Scenarios – Use Case 1



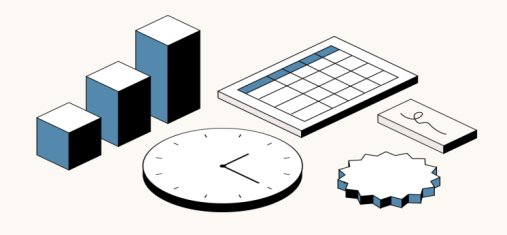
We are not providing generic IAM.
We are providing:
- **Credential elimination**
- **Privileged action control**
- **Blast radius containment**
- **Quantum readiness**
- **Independent assurance layer**.

Use Case 1: Administrative Pathway Protection

Strategic Distinction: Securing the consequences of an admin-level breach.

- "**Locking the Administrative Perimeter** – Moving from 'Admin Access' to 'Admin Authenticity.'"
- "**The SyberKey Fix:** A compromised administrative session (hijacked token) is useless. Critical internal actions, such as creating new privileged users, disabling logs, or exporting sensitive data, automatically trigger an out-of-band **Human Presence Assertion**. The system demands and receives a unique **Human Action Certificate** before the execution can complete."

Customer Scenarios – Use Case 2



We are not providing generic IAM.
We are providing:
- **Credential elimination**
- **Privileged action control**
- **Blast radius containment**
- **Quantum readiness**
- **Independent assurance layer**

Our ICP understands & reflects that.

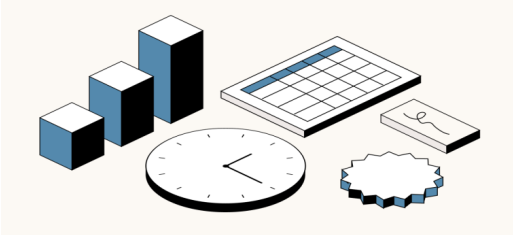
Use Case 2: Multi-Factor Authentication (MFA) Evolution

Strategic Distinction (Solving MFA's Fatal Flaw):

Solving the core vulnerabilities of traditional MFA: **Phishing and Push Bombing**.

- "**Evolving from MFA to Human Zero Trust.** Traditional MFA verifies *nothing* beyond the possession of a device or a secret."
- **The SyberKey Fix:** Our hardware-free, biometric-approval approach means **phishing is technically impossible** as there is no password or shared secret for the user to type. We eliminate 'MFA Fatigue' by making the approval process seamless and **action-aware**.

Customer Scenarios – Use Case 3



We are not providing generic IAM.
We are providing:
- **Credential elimination**
- **Privileged action control**
- **Blast radius containment**
- **Quantum readiness**
- **Independent assurance layer**

Our ICP understands & reflects that.

Use Case 3: Securing Financial Transactions

Strategic Distinction (The Non-Repudiable Transaction):

Providing unique, non-repudiable protection for high-value financial actions compared to standard MFA.

- **Current State:** A compromised session (hijacked token) allows an attacker to authorize a wire transfer invisibly.
- **The SyberKey Fix:** The transfer request itself triggers an out-of-band **Human Presence Assertion**. The bank receives a cryptographic **Human Action Certificate** that proves—at the *moment* of the transfer—the actual, authorized human was present and approved. This makes fraud and transfer repudiation technically impossible.