



PQ Mythos Key
— Human Zero Trust —

Syberkey
— Patented Tech —

Human-Bound Post-Quantum Authority for Critical Actions.

Verifies the live authorised human and enables quantum-resilient authority only for the exact permitted action.

Protect the authority to use critical keys, approve sensitive transactions and execute high-consequence actions.

Live biometric verification. No OTP or password. No special hardware. Post-quantum action authority

IAM / PAM

HSM / KMS

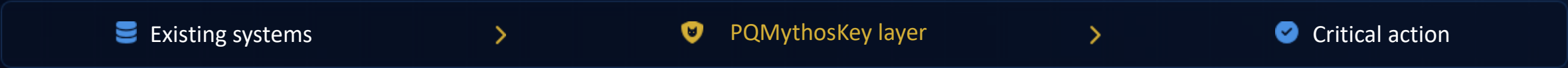
PKI / Cloud

Business systems



Protect Critical Human Authority Now. Continue Enterprise PQ Migration at Your Pace.

Protect selected high-consequence authority pathways while broader PQ migration continues



The Market Gap: Organisations know quantum risk is coming, but many cannot fund or execute full migration immediately.

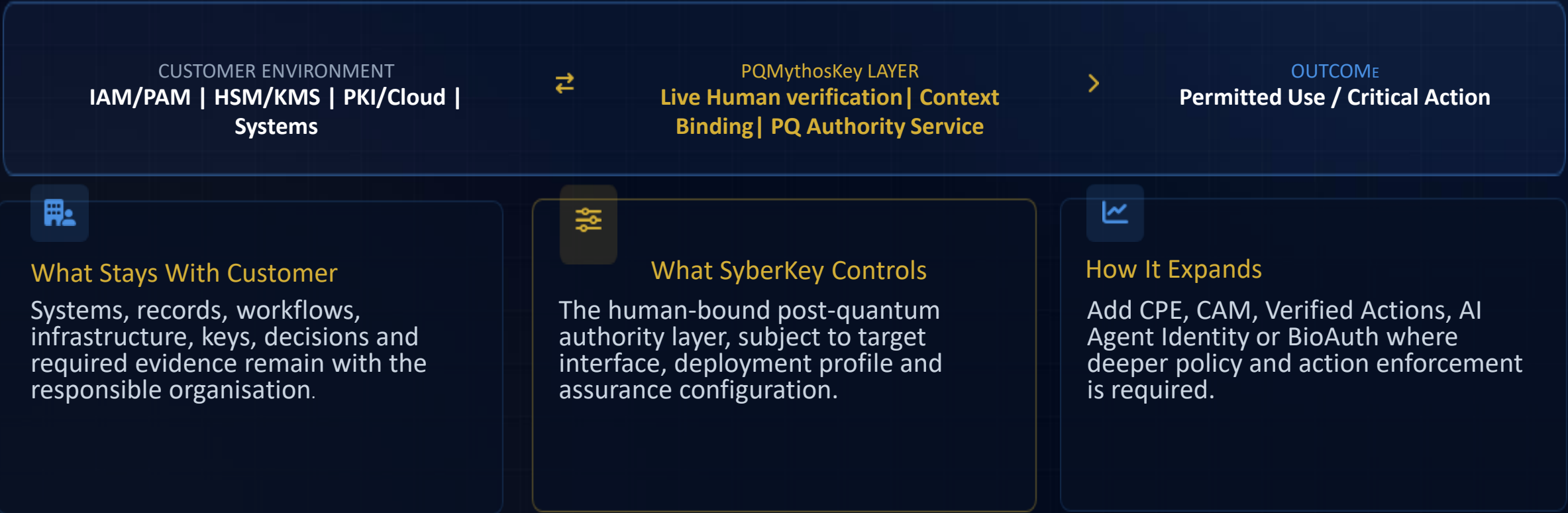
Strategy	Description & Impact
Do nothing	Avoids capex today but leaves critical authority pathways dependent on legacy credentials and cryptographic controls while migration is delayed.
Full PQ migration	Necessary over time, but expensive, multi-year and dependent on legacy systems, vendors, PKI, HSMs, KMS and applications.
PQMythosKey entry layer	Protect high-value human authority, key use and critical actions now while the broader estate migrates at its own pace. PQMythosKey does not replace enterprise-wide cryptographic migration.

Do not wait for the entire enterprise to become quantum-safe before protecting the authority that matters most.



The Architecture: A low-disruption layer around selected critical keys, transactions and actions

Verifies the live authorised person, validates the requested purpose and returns short-lived quantum-resilient authority for the approved operation..





Some Use Cases

Start with the use cases where quantum risk and human authority meet highest business consequence.



Banking
Payments



HSM / KMS
Authority



AI Agents
Human
Control



Government
Critical Infra



Cloud
Privileged Admin

Protect selected high-consequence authority now, then expand into the broader SyberKey portfolio as customer needs mature.



1. Banking and Payments

Protect high-value transactions before full PQ migration

⚠ The Risk

Banks cannot transform payment, PKI and cryptographic infrastructure overnight, but high-value transactions concentrate immediate financial and operational risk.

🛡 PQMythosKey Approach

Introduce PQMythosKey around selected payment workflows so verified human authority is required before a protected critical release operation proceeds.

📈 Business Value

Protect high-consequence transaction authority now while broader migration progresses over time.



Payment
request



Verified
human



PQMythosKey
authority



Release
operation

Treasury operations | SWIFT transactions | high-value transfers | settlement instructions | executive payment approvals

Existing MFA may validate credentials at login. PQMythosKey verifies the live authorised human for the exact high-value action.



2. HSM and KMS Authority

Protect the authority to use the key, not just the key itself

⚠ The Risk

HSMs and KMS platforms protect keys, but they do not by themselves prove that the correct human should invoke a key for a sensitive operation right now.

🛡 PQMythosKey Approach

Place PQMythosKey between selected users/workflows and the existing HSM or KMS, while the organisation retains infrastructure and key custody.

📈 Business Value

Strengthen existing key-management investments without replacement or rip-and-replace migration.



Operator /
workflow



PQMythosKey
check



Existing HSM /
KMS



Permitted key
use

Root and signing keys | certificate authority operations | encryption-key release | privileged HSM administration



3. AI Agents

AI may request the action but verified human authority controls execution.

 The Risk

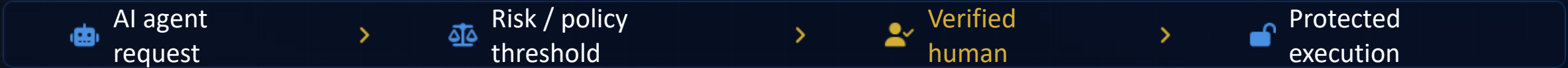
AI agents increasingly hold credentials and can initiate infrastructure, financial or data actions. A valid agent credential does not prove human approval for a high-risk action.

 PQMythosKey Approach

Allow routine agent activity to continue, while high-consequence actions require verified-human authority before protected execution proceeds.

 Business Value

Retain human control over sensitive autonomous actions without removing the productivity benefits of AI.



Treasury agents | infrastructure agents | security agents | DevOps agents | procurement agents | regulated AI workflows



4. Government and Critical Infrastructure

Protect critical authority while legacy systems catch up

 The Risk

Government, energy, transport and OT environments often contain long-life systems that cannot be replaced quickly, even when PQ migration is required.

 PQMythosKey Approach

Introduce PQMythosKey around selected high-consequence human operations while existing infrastructure remains in service.

 Business Value

Begin protecting critical authority now while the underlying environment progresses through a longer migration lifecycle.



Privileged administration | configuration changes | protected information release | operational commands | remote engineering access



5. Cloud and Privileged Administration

Stop stolen credentials becoming unlimited authority

⚠ The Risk

Cloud and privileged credentials can enable destructive or high-impact actions if compromised. Strong algorithms do not solve misuse of legitimate authority.

🛡 PQMythosKey Approach

Add verified-human post-quantum authority to selected critical cloud or privileged operations while preserving existing IAM, PAM and KMS controls.

📈 Business Value

Move beyond protecting privileged access to protecting privileged authority.

👤 Admin
request



📄 Credential /
session



🛡 PQMythosKey step-
up



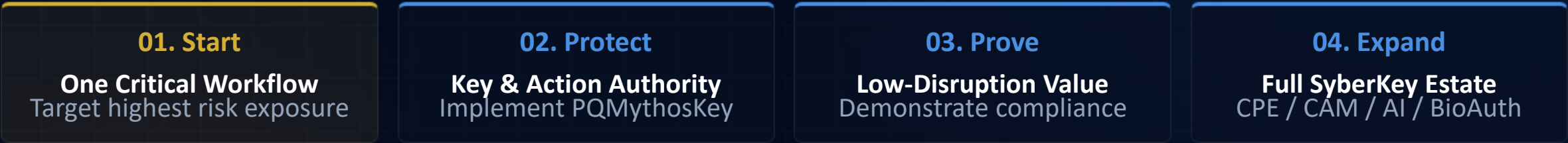
⚡ Sensitive
action

Root operations | production infrastructure changes | KMS administration | key deletion | security-policy changes | data exports



Land with PQMythosKey. Expand with SyberKey.

A focused entry Solution that grows into the wider trust architecture.



Phase	Strategic Focus
Entry	PQMythosKey protects the first high-value authority pathway.
Expansion	CPE adds exact-action, policy, risk and pathway enforcement.
Continuity	CAM and BioAuth strengthen ongoing human trust and verification across customers wider applications.
Future	AI Agent Identity extends the same authority model to delegated machine actions.