SyberKey CPE: Human-Verified Cryptographic Execution Control

Architecting the foundational execution layer for the AI and post-quantum enterprise.

CPE

CONTINUOUS PATHWAY ENFORCEMENT

POLICY ENDPOINT VERIFY

Syberkey

Patented Tech

We secured the perimeter, the identity, and the endpoint

Despite massive investments across these layers, a critical, systemic vulnerability remains unaddressed.

Pillar 1:
Perimeter Security

Firewalls and network controls.

Pillar 2:
Identity Security

IAM, MFA, PAM, Zero Trust.

Pillar 3:
Data Governance

DLP, classification, compliance.

Pillar 4:
Endpoint Security

EDR/XDR and behavioral analytics.

The Void:
The Execution Gap

(Unresolved)

ACCESS IS NOT EXECUTION

THE ASSUMPTION: SECURITY SYSTEMS DETERMINE WHETHER A USER SHOULD HAVE ACCESS.

THE REALITY: ONCE ACCESS IS GRANTED VIA SESSION TRUST, BEARER TOKENS, OR CACHED IDENTITY, EXECUTION HAPPENS FREELY.

THE FATAL FLAW: SENSITIVE ACTIONS EXECUTE WITHOUT FRESH PROOF OF INTENT, CONTEXT, OR VERIFIED HUMAN PRESENCE.

Syberkey
Patented Tech

Traditional access control structurally fails the AI era

Enterprise systems—driven by AI copilots, autonomous agents, and automated workflows—now act exponentially faster than humans can supervise.

Legacy Model

- Linear security reviews
- Manual approval gates
- Time-intensive supervision

Modern Reality

- AI copilot delegation
- API-driven execution chains
- Automated machine-to-machine workflows

Syberkey
Patented Tech

Converging threat vectors exploit static session trust

Without execution-time verification, the enterprise is vulnerable to high-velocity threat vectors.

Syberkey
Patented Tech

Existing platforms answer crucial questions, but leave one unanswered

Microsoft Entra ID:
Who is the user?

Microsoft Purview:
What is the data?

The Central Void:
Policy, monitoring, and entitlement managers are powerful, but who controls the execution?

CyberArk:
Is the user privileged?

Defender for Endpoint:
Is the device risky?

The cryptographic keystone completing the enterprise stack

CPE is the missing enforcement layer that unifies identity, data, endpoints, and privilege.

SyberKey answers the final question: Can this exact action execute right now with fresh human **cryptographic verification?**

Syberkey
Patented Tech

Verification strictly at execution time

Live Biometric Verification: Passwordless, QR-anchored cryptographic identity.

Payload Binding: Tied exclusively to the exact action requested.

Replay Protection: Cryptographically prevents duplicated or hijacked execution attempts.

Execution Examples: High-risk actions like file exports, privileged PowerShell execution, cloud infrastructure modification, and database extractions.

Syberkey
Patented Tech

Architected for the post-quantum and AI-driven enterprise

Hybrid Cryptographic Signing: Designed for the post-quantum transition.

Cryptographic Agility: Resilient execution control independent of legacy algorithms.

Threat Resilience: Neutralizes long-term cryptographic exposure and AI-assisted credential attacks.

Syberkey
Patented Tech

Defeating session hijacking and machine-speed fraud

Use Case: Financial Approvals

When a payment approval is requested, CPE validates endpoint risk, requires a live biometric, and issues a 10-second single-use token to cryptographically enforce the transaction.

Syberkey
Patented Tech

Live biometric privileged execution bound to the exact payload

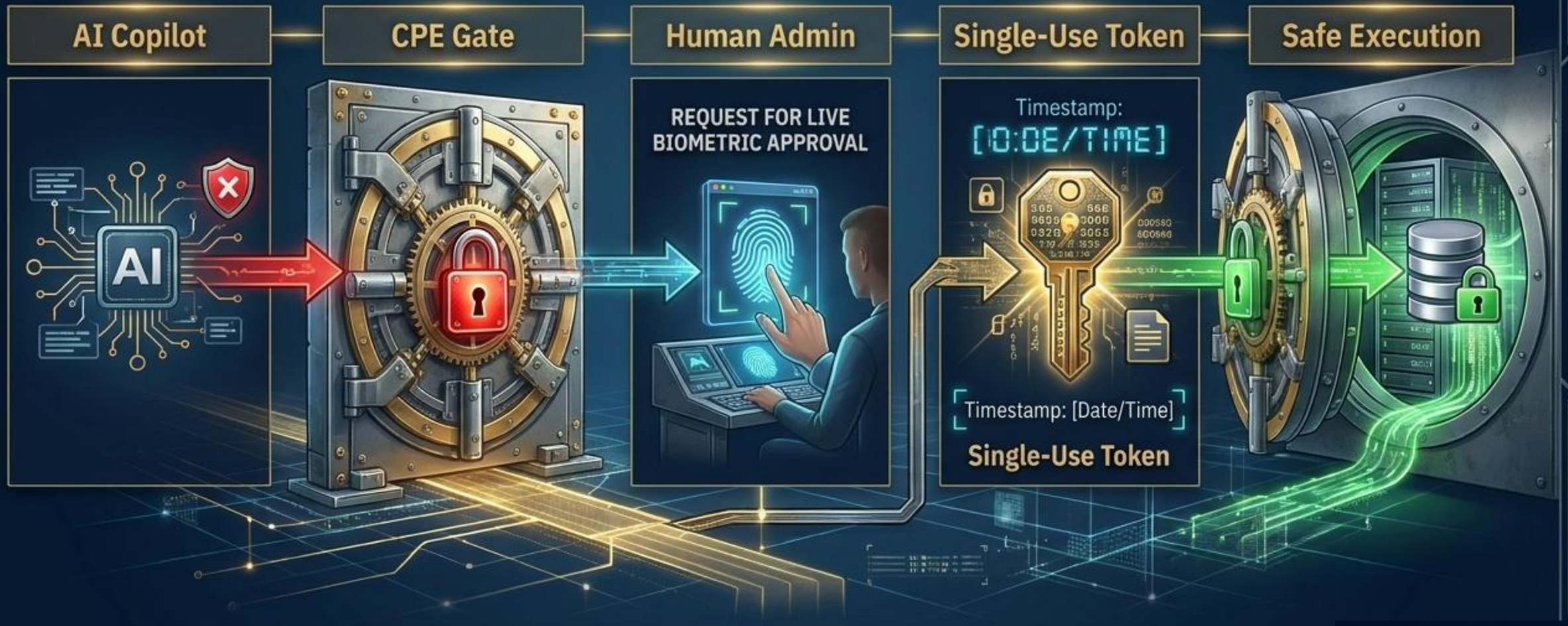
Use Case: Privileged Admin Execution

Even if an admin holds a privileged role, elevated endpoint risk triggers a biometric requirement, generating an action-bound token that allows only the exact PowerShell execution requested.

Syberkey
Patented Tech

Cryptographically gating autonomous AI execution chains

Enforcing human-in-the-loop cryptographic approval for AI-generated actions, preventing automated catastrophe.



Syberkey
Patented Tech

Enforcing human verification for highly sensitive data extraction

Use Case: Human-Verified File Download

Governance Signal:
Microsoft Purview

Risk Signal:
Microsoft Defender

Execution Enforcement:
SyberKey CPE Engine

Clamp it Gimmput:

CPE intercepts the download request, demands a live biometric scan, and issues a 10-second replay-protected token bound explicitly to that exact file export.

Syberkey
Patented Tech

A complementary enforcement layer for existing investments

Identity Platforms
(Entra ID, Okta, Ping Identity)

- Current Function: Identity & Conditional Access

→ **SyberKey Adds:** Execution-time enforcement and action-bound JIT tokens

PAM Platforms
(CyberArk, BeyondTrust, Delinea)

- Current Function: Privileged Sessions & Credentials

→ **SyberKey Adds:** Payload-bound privileged actions and live biometric execution

Data Governance
(Purview, Netskope, Zscaler)

- Current Function: Classification & DLP

→ **SyberKey Adds:** Biometric-verified download approval and cryptographic export control.

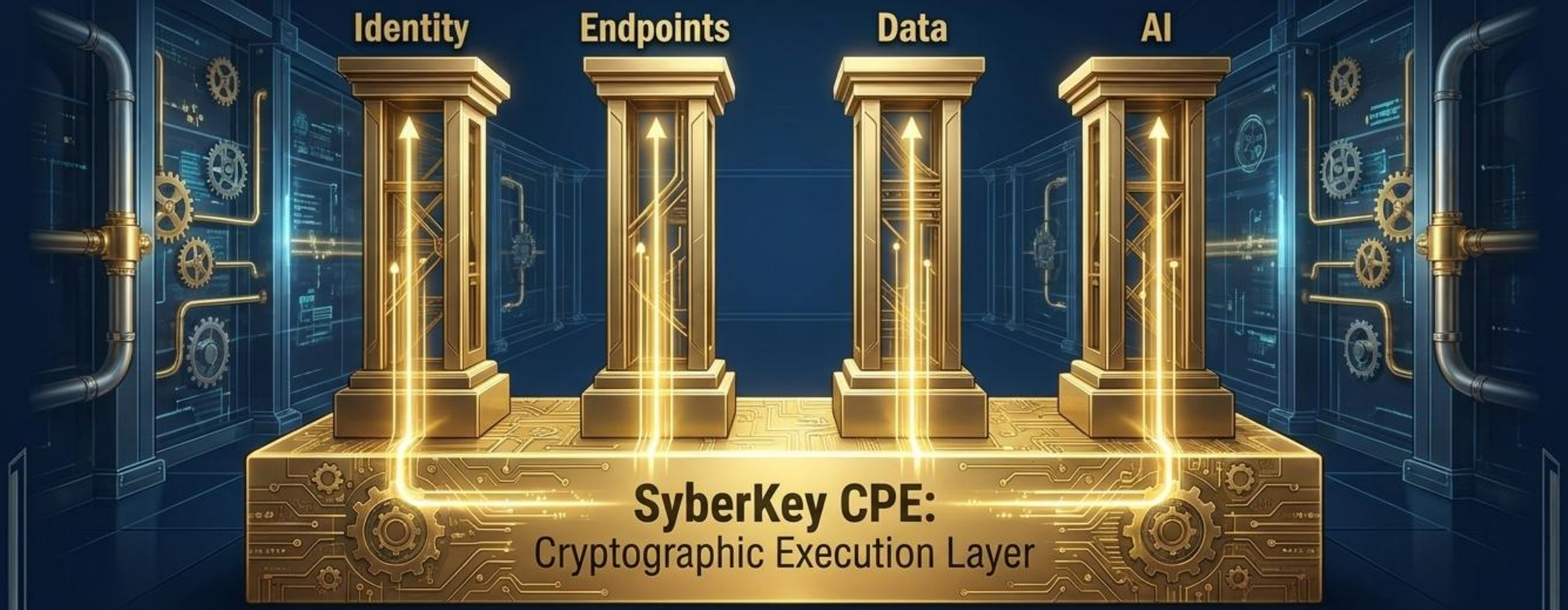
Endpoint Security
(Defender, CrowdStrike, SentinelOne)

- Current Function: EDR/XDR & AI Security

→ **SyberKey Adds:** Endpoint execution gating and device-risk-aware action enforcement.

Syberkey
Patented Tech

The foundational security control layer for the next-generation enterprise



Transitioning enterprise cybersecurity from static perimeter defense and session trust to continuous, human-centric cryptographic enforcement. The human-verified cryptographic execution-control layer designed for the AI-driven, post-quantum enterprise.

Syberkey
Patented Tech