Syberkey
Patented Tech

AIPQCAM
AI DRIVEN • POST QUANTUM READY • CONTINUOUS ACCESS MONITORING

PQ-Ready AI-Controlled Continuous Access Monitoring and Verified Action Enforcement

1. Executive Summary

SyberKey CPE — Continuous Pathway Enforcement — is a next-generation enterprise security control plane designed for the AI-driven, post-quantum, zero-trust enterprise.

It is enterprise execution-control platform supported by integrated adapters across identity, endpoint security, PAM, cloud, data, workflow, SaaS and security operations environments.

SyberKey CPE is not simply another MFA product, PAM tool, SIEM system, DLP product, EDR platform or identity provider. It is designed to operate as the missing enforcement layer between enterprise security systems and the sensitive actions that users, administrators, applications, AI agents and automated workflows attempt to perform.

The core principle is simple:

Identity systems know who the user is. Security tools know what the risk is. SyberKey CPE decides whether the exact action should be allowed to execute right now.

SyberKey CPE combines:

- Continuous Access Monitoring
- AI risk evaluation
- Live biometric verification
- Role and privilege context
- Adaptive policy enforcement
- Action-specific approval
- Verified human intent

- Post-quantum-ready cryptographic protection
- Adapter-based enterprise integration
- Signed execution approval and audit evidence

The platform has now moved from a standalone concept into an integrated enterprise model, with adapters across major security and business platforms. This allows SyberKey to work with existing enterprise investments rather than replace them.

The result is a new category:

Human-Verified Cryptographic Execution Control

This allows organisations to move beyond traditional access control and into verified action control.

2. The Enterprise Security Gap

Enterprises already invest heavily in cybersecurity. Most large organisations use identity, PAM, endpoint, data governance, SIEM, SOC and Zero Trust platforms.

These tools are powerful, but they often focus on one of the following:

- Authenticating the user
- Granting access
- Monitoring activity
- Detecting threats
- Managing privileges
- Classifying data
- Raising alerts
- Recording incidents
- Enforcing broad policy

However, a critical gap remains:

Once access has been granted, many sensitive actions can still execute based on session trust, cached credentials, bearer tokens, administrative permissions or policy assumptions.

This creates risk in areas such as:

- Privileged access

- Data export
- Cloud infrastructure changes
- Payment approval
- AI-agent execution
- Code deployment
- Sensitive document signing
- Database extraction
- Security policy changes
- Privilege elevation
- Automated remediation
- Remote access
- Insider misuse
- Compromised sessions

Traditional security asks:

“Is this user allowed to access the system?”

SyberKey CPE asks:

“Should this verified human, in this context, be allowed to perform this exact action right now?”

That is the difference.

3. What SyberKey CPE Is

SyberKey CPE is a PQ-ready, AI-controlled Continuous Access Monitoring and execution enforcement layer.

It continuously evaluates identity, privilege, risk, policy, system context and action intent before allowing sensitive actions to proceed.

CPE is designed to govern:

- Who is acting
- What action is being requested
- Whether the user is live and verified

- Whether the device or endpoint is safe
- Whether the user has the required role
- Whether the action is high risk
- Whether the data is sensitive
- Whether workflow approval exists
- Whether AI or automation is involved
- Whether a fresh human verification is required
- Whether a signed execution approval should be issued

The key is that CPE does not only monitor risk. It enforces decisions at the moment of action.

4. CPE as Continuous Access Monitoring

SyberKey CPE started as a standalone continuous access monitoring platform.

In this mode, CPE continuously observes and evaluates:

- User identity
- Session behaviour
- Device context
- Access pattern
- Privilege level
- Risk signals
- Role assignment
- System access
- Transaction context
- Endpoint posture
- Suspicious change in behaviour
- Sensitive action request

This is not one-time login verification.

It is continuous monitoring of whether the access pathway remains valid.

Traditional access model:

Authenticate user

→ Grant session

→ Permit actions

SyberKey CPE model:

Verify identity

→ Monitor context continuously

→ Evaluate risk dynamically

→ Require live verification where needed

→ Permit or block exact action

→ Create signed audit proof

This is why CPE should be positioned as:

Continuous Access Monitoring plus real-time action enforcement.

5. From Monitoring to Verified Action

The evolution of SyberKey CPE is important.

Phase 1 — Standalone CPE

The platform began as a standalone control layer for continuous monitoring and enforcement.

It focused on:

- Continuous identity validation
- Adaptive access monitoring
- Risk-based policy decisions
- Privileged action control
- Live verification at sensitive moments
- Post-quantum-ready control design

Phase 2 — Enterprise Adapter Integration

CPE has now evolved to integrate with enterprise systems through adapters.

The current adapter direction includes approximately sixteen key enterprise integration categories across:

- Microsoft Entra ID
- Microsoft Defender
- Microsoft Purview
- CyberArk PAM
- Zscaler
- CrowdStrike Falcon
- Snowflake
- Databricks
- ServiceNow
- Workday
- Jira
- SOC platforms
- SIEM platforms
- Cloud and data systems
- IAM / SSO systems
- Additional enterprise applications as required

The strategic shift is:

CPE no longer sits alone. It can now receive signals from the enterprise security stack and enforce verified actions across business systems.

Phase 3 — Verified Action Enforcement

With adapters, CPE becomes more than monitoring.

It becomes the verified action layer.

This means CPE can sit between enterprise systems and high-risk actions such as:

- Export data
- Approve payment
- Release privilege
- Execute admin command

- Apply AI-generated fix
- Rotate secret
- Sign document
- Deploy production code
- Release room access
- Approve procurement
- Authorise workflow
- Change security policy

The verified action layer allows enterprises to require live human verification before sensitive action execution.

6. The Role of Live Biometrics

One of the strongest SyberKey differentiators is real-time live biometric verification.

Most enterprise platforms rely on:

- Login session
- SSO token
- MFA challenge
- Device trust
- Role assignment
- Admin permission
- Policy rule

SyberKey adds a stronger question:

Is the real authorised human live and approving this exact action now?

Live biometric verification can be required when:

- Risk is high
- Action is sensitive
- Device posture is uncertain
- Data is classified

- Privilege is elevated
- User behaviour is abnormal
- AI agent is acting
- Payment is being approved
- Document is being signed
- Critical infrastructure is being changed
- Production code is being deployed

This enables SyberKey to provide:

- Human-verified privileged access
- Biometric action approval
- Biometric document signing
- Biometric payment approval
- Biometric AI-agent oversight
- Biometric access release
- Biometric risk step-up

The value is not simply authentication.

The value is verified human authority at the moment of action.

7. PQ-Ready Cryptographic Control

SyberKey CPE is designed for post-quantum readiness and cryptographic agility.

This matters because enterprise security is moving into an era where traditional cryptographic assumptions are under pressure from future quantum capability, AI-assisted attacks and long-term data exposure risks.

CPE's PQ-ready direction supports:

- Crypto-agile control signals
- Post-quantum transition readiness
- Stronger approval tokens
- Action-bound execution control
- Long-term audit resilience

- Reduced “harvest now, decrypt later” exposure
- Future-ready enterprise identity assurance
- Secure human-action proof

In marketing language:

CPE is built for the post-password, AI-driven and post-quantum enterprise.

This gives SyberKey a forward-looking security position that many conventional MFA, PAM and access-control systems do not yet clearly occupy.

8. AI-Controlled Risk Layer

CPE includes an AI-controlled risk layer that evaluates context dynamically.

The AI risk layer can assess signals such as:

- User behaviour
- Device posture
- Location anomaly
- Access frequency
- Privilege sensitivity
- Data classification
- Endpoint alerts
- Workflow state
- AI-agent involvement
- Transaction value
- Business context
- Threat intelligence
- Security system alerts

The purpose is not only to score risk.

The purpose is to decide what level of enforcement is required.

Examples:

Risk Context	CPE Response
Low-risk action	Allow normal access
Medium-risk action	Require push/QR confirmation
High-risk action	Require live biometric verification
Critical action	Require live biometric + policy approval
AI-agent action	Require verified human approval
Sensitive data export	Require biometric + action-bound token
Privileged command	Require biometric + CPE approval
Suspicious endpoint	Block or escalate
Unapproved workflow	Reject action

This is where CPE becomes adaptive and action-aware.

9. How the Adapter Model Works

The adapter model allows SyberKey to connect to enterprise systems without replacing them.

Each adapter contributes context, workflow state, identity signal, risk signal or enforcement trigger.

Identity adapters

Examples:

- Microsoft Entra ID
- Okta
- SSO / IAM systems

They provide:

- User identity
- Role
- Group membership
- Authentication state

- Conditional access context

CPE adds:

- Live biometric action verification
- Execution-time approval
- Action-bound token
- Human-approved audit proof

PAM adapters

Examples:

- CyberArk
- ARCON
- Other PAM systems

They provide:

- Privileged role
- Credential/session request
- JIT access workflow
- Admin session context

CPE adds:

- Live biometric privileged approval
- Verified human authority
- Action-specific privilege release
- Independent proof of human intent

Endpoint adapters

Examples:

- Microsoft Defender
- CrowdStrike Falcon
- SentinelOne

They provide:

- Device posture
- Endpoint risk
- Security alert state
- Compromise indicators

CPE adds:

- Endpoint-aware action gating
- Real-time execution block
- Biometric step-up when device risk changes

Data governance adapters

Examples:

- Microsoft Purview
- Snowflake
- Databricks
- DLP / data classification systems

They provide:

- Data classification
- Sensitivity label
- Export risk
- Access pattern
- Data movement context

CPE adds:

- Human-verified data access
- Biometric export approval
- Action-bound data release
- Cryptographic audit trail

Workflow adapters

Examples:

- ServiceNow
- Jira
- Workday

They provide:

- Ticket approval
- Business justification
- Change request
- HR role context
- Operational workflow state

CPE adds:

- Verified human approval
- Enforcement at action execution
- Prevention of action without approved workflow

SOC / SIEM adapters

Examples:

- Microsoft Sentinel
- Splunk
- QRadar
- SOC platforms

They provide:

- Threat signals
- Correlated events
- Security alerts
- Incident severity
- Investigation state

CPE adds:

- Real-time block/allow decision
- Biometric step-up during risk events
- Enforcement rather than only alerting

10. CPE as the Missing Layer Between Security Tools

The easiest way to explain SyberKey CPE is:

- Entra knows who the user is.
- Purview knows what the data is.
- Defender knows whether the device is risky.
- CyberArk knows whether the user has privileged access.
- ServiceNow knows whether there is an approved workflow.
- CrowdStrike knows whether the endpoint is under threat.
- SIEM knows whether the environment is abnormal.

But SyberKey CPE answers the missing question:

Can this exact action execute right now with verified human authority?

That is the missing enterprise security layer.

11. Verified Action Layer

The verified action layer is the commercial evolution of CPE.

Instead of only asking whether a user can access a system, Verified Action asks whether a sensitive action should execute.

Verified actions can include:

- Approve privileged access
- Approve data export
- Approve payment
- Approve production deployment
- Approve AI agent action

- Approve document signing
- Approve security policy change
- Approve secret rotation
- Approve customer refund
- Approve database extraction
- Approve high-risk login
- Approve administrative command
- Approve patient consent
- Approve hotel key release
- Approve code remediation

This is powerful because the same SyberKey engine can apply across enterprise security, AI governance, DevSecOps, payments, healthcare, hospitality, document signing and critical workflows.

12. Example Use Case: Sensitive Data Export

A user attempts to export a sensitive customer dataset.

Existing systems provide context:

- Entra confirms identity
- Purview labels the dataset as confidential
- Defender reports device risk
- ServiceNow provides approval ticket
- SIEM reports no active incident

CPE evaluates:

- Is the user authorised?
- Is the device trusted?
- Is the export justified?
- Is the data sensitive?
- Is live biometric approval required?
- Is the action allowed now?

CPE enforces:

- Requires live biometric verification
- Generates action-bound approval
- Allows export only if approval is valid
- Logs audit proof

Result:

The organisation does not merely know that a user accessed data. It knows that the verified live human approved this exact export.

13. Example Use Case: Privileged Admin Action

A privileged administrator attempts to execute a high-risk command.

Existing systems provide context:

- CyberArk confirms privileged role
- Defender checks endpoint risk
- SIEM checks threat environment
- ServiceNow checks change ticket

CPE evaluates:

- Is the admin role valid?
- Is the command approved?
- Is the endpoint safe?
- Is the action within scope?
- Is biometric step-up required?

CPE enforces:

- Requires live biometric approval
- Creates action-specific token
- Allows only the approved command
- Blocks replay or unauthorised variation
- Creates audit proof

Result:

Privileged access becomes human-verified and action-bound.

14. Example Use Case: AI Agent Governance

An AI security agent wants to remediate a vulnerability or rotate a secret.

Existing tools provide context:

- Code platform identifies repository
- DevSecOps tool identifies vulnerability
- CI/CD platform identifies deployment risk
- Ticketing system records approval request

CPE evaluates:

- Which AI agent is acting?
- Who owns the agent?
- What action is requested?
- Is the action high risk?
- Is human approval required?
- Is the approval live and verified?

CPE enforces:

- Requires human biometric approval
- Issues one-time action approval
- Allows only the authorised agent action
- Stores agent + human + action audit proof

Result:

AI can recommend or prepare the action, but sensitive execution requires verified human authority.

15. Example Use Case: Payment or Financial Approval

A user attempts to approve a high-value payment.

CPE evaluates:

- User identity
- Payment amount
- Beneficiary
- Device posture
- Business workflow
- Fraud risk
- Transaction context

CPE enforces:

- Requires live biometric approval
- Confirms action statement
- Issues action-bound approval
- Creates audit record

Result:

Payment approval is tied to a verified live human, not merely to a logged-in account.

16. Example Use Case: Document Signing

A person signs a sensitive legal, financial or compliance document.

CPE evaluates:

- Signer identity
- Document hash
- Signing authority
- Risk level
- Consent statement

CPE enforces:

- Requires live biometric verification
- Binds approval to document hash
- Generates signing proof

- Creates audit certificate

Result:

The document is not only electronically signed; it is live-human verified.

17. Example Use Case: Hospitality and Physical Access

A hotel guest or authorised person requests access.

CPE evaluates:

- Booking status
- Guest identity
- Payment/deposit status
- Registration status
- Access request
- Risk context

CPE enforces:

- Requires live biometric guest verification
- Approves key release only if policy is satisfied
- Blocks access without approval
- Creates audit proof

Result:

No approved SyberKey verification means no room key, no PIN, no mobile key and no access code.

18. CPE Competitive Positioning

SyberKey CPE does not need to be positioned as a direct replacement for existing enterprise tools.

It is better positioned as the missing layer that makes those tools stronger.

Compared with IAM

IAM answers:

Who is the user?

CPE answers:

Should this verified user be allowed to execute this action now?

Compared with MFA

MFA answers:

Can the user complete an authentication challenge?

CPE answers:

Has the live authorised human approved this exact action?

Compared with PAM

PAM answers:

Can this user access privileged credentials or sessions?

CPE answers:

Should this privileged action execute with verified human authority?

Compared with EDR/XDR

EDR/XDR answers:

Is the endpoint suspicious?

CPE answers:

Should action execution be allowed based on endpoint risk and live verification?

Compared with DLP

DLP answers:

Is the data sensitive or moving?

CPE answers:

Should this sensitive data action be cryptographically allowed?

Compared with SIEM/SOC

SIEM/SOC answers:

What is happening in the environment?

CPE answers:

Should the action be blocked or allowed now?

Compared with Thales / key management

Key management protects keys and cryptographic infrastructure.

CPE protects the execution pathway by binding identity, privilege, risk, action and human approval.

19. Why CPE Is Different

SyberKey CPE is different because it combines several layers into one control plane:

1. **Continuous Access Monitoring**
   CPE evaluates identity, session and risk continuously.
2. **AI-Controlled Risk Evaluation**
   CPE uses risk context to decide the level of enforcement required.
3. **Live Human Verification**
   CPE can require real-time live biometric approval when the action is sensitive.
4. **Action-Specific Enforcement**
   CPE controls the exact action, not merely system access.
5. **Adapter-Based Enterprise Integration**
   CPE receives context from existing IAM, PAM, EDR, DLP, workflow and SIEM systems.
6. **PQ-Ready Cryptographic Architecture**
   CPE is designed for crypto agility and future post-quantum security.
7. **Verified Action Audit**
   CPE creates proof of who approved what, when, and under what context.

This is the strategic differentiation.

20. Strengths

SyberKey CPE is a PQ-ready, AI-controlled Continuous Access Monitoring and Verified Action Enforcement platform.

SyberKey CPE continuously evaluates identity, privilege, risk and action context, then requires live human verification where necessary before sensitive actions are allowed to execute. It integrates through enterprise adapters across IAM, PAM, EDR, DLP, SIEM, workflow and cloud systems to create a human-verified, cryptographically protected execution-control layer for the AI and post-quantum era.

SyberKey does not just verify access. It verifies human authority before sensitive actions execute.

We do not replace security stack. We connect it and enforce the missing human-verified action decision.

SyberKey CPE is designed for the next era of enterprise trust — where identity, action approval and execution control must remain secure in a post-quantum world.

21. SyberKey Capability Stack

SyberKey's full capability stack in this area can be summarised as follows:

Layer	SyberKey Capability	Business Value
Identity	Bio-ID / OneBioID	Reusable biometric-rooted identity
Authentication	CAM / adaptive MFA	Continuous live human verification
Enforcement	CPE	Action execution control
Cryptography	PQ-ready key architecture	Future-ready approval security
Integration	16 enterprise adapters	Works with existing enterprise stack
AI	AI risk engine	Dynamic risk-based decisions
Biometrics	Real-time live biometric verification	Strong human authority proof
Approval	Verified Action	Exact action approval
Audit	Signed evidence record	Dispute, compliance and investigation support
AI Agent	Agent identity + human approval direction	Controls autonomous AI actions
Documents	FingerSign	Biometric document approval
Email	VerifiedBioMail direction	Human-verified communication intent
Payments	CVV/payment approval direction	Verified transaction authority

Layer	SyberKey Capability	Business Value
Hospitality	VerifiedStay direction	Verified guest and access release

This demonstrates that CPE is not an isolated product.

It is the enterprise enforcement expression of the broader SyberKey platform.

22. Suggested Product Packaging

Package 1 — CPE Standalone (CAM)

For organisations that need continuous access monitoring and verified action control without deep enterprise integration.

Includes:

- Continuous identity/session monitoring
- Live biometric step-up
- Role-based action approval
- Basic policy rules
- Approval dashboard
- Audit logging

Package 2 — CPE Adapter Edition

For organisations that want to connect CPE to existing enterprise systems.

Includes:

- IAM adapter
- PAM adapter
- Endpoint adapter
- Data governance adapter
- Workflow/ticketing adapter
- SIEM/SOC adapter
- Verified action APIs
- Webhooks and decision tokens

Package 3 — CPE Enterprise

For large enterprises with complex security environments.

Includes:

- Multi-adapter orchestration
- AI risk engine
- Dynamic policy enforcement
- Live biometric verification
- Post-quantum-ready control design
- Data-sensitive action control
- Privileged action control
- AI-agent action governance
- Audit evidence and reporting

Package 4 — CPE for AI and Automation

For AI-driven organisations and autonomous workflow environments.

Includes:

- AI-agent action approval
- Human-in-the-loop biometric control
- Verified execution token
- Repository / CI/CD / ticketing integration
- Sensitive automation approval
- Agent identity roadmap integration

23. Partner and Customer Message

SyberKey CPE should be presented as the missing verified action layer.

It does not compete directly with the customer's existing security tools. It strengthens them.

Customers already have IAM, PAM, EDR, DLP and SIEM. What they usually do not have is a unified way to verify the live human and enforce whether sensitive actions can execute in real time. That is where SyberKey CPE fits.

For implementation partners

The implementation focus should be:

1. Identify sensitive actions.
2. Identify existing systems that provide context.
3. Connect the required adapters.
4. Define CPE policy.
5. Trigger SyberKey verification before sensitive action.
6. Return approved/rejected decision.
7. Enforce allow/block in the target system.
8. Store audit proof.

For enterprise customers

SyberKey CPE gives you real-time human-verified control over sensitive actions across your enterprise security stack.

24. The Strategic Value

SyberKey CPE creates value because it moves security from access-based trust to action-based proof.

Traditional enterprise model:

User authenticated

→ Session trusted

→ Action permitted

SyberKey model:

User verified

→ Context evaluated

→ Action approved

→ Execution enforced

→ Audit proof created

This is a major shift.

It is highly relevant to:

- Zero Trust
- AI governance
- Privileged access
- Data protection
- Post-quantum security
- Insider risk
- Cloud security
- DevSecOps
- Regulatory compliance
- Identity assurance
- Automation control

25. Why the Timing Is Right

The timing for CPE is strong because enterprises are facing several converging pressures:

- AI agents are beginning to execute workflows.
- Cyberattacks are increasingly identity-based.
- Privileged access remains a major breach pathway.
- Data is distributed across cloud and SaaS systems.
- Session trust is no longer sufficient.
- Post-quantum preparation is moving onto enterprise roadmaps.
- Security teams need enforcement, not more alerts.
- Remote and distributed work increases identity risk.
- Sensitive actions happen across multiple disconnected systems.

SyberKey CPE directly addresses these pressures.

26. Final Positioning Statement

SyberKey CPE is a PQ-ready, AI-controlled Continuous Access Monitoring and Verified Action Enforcement platform.

It integrates with existing enterprise systems through adapters, continuously evaluates identity, privilege, risk, device and action context, and requires live human verification where necessary before sensitive actions can execute.

CPE does not replace IAM, PAM, EDR, DLP, SIEM or workflow platforms. It connects them and adds the missing enforcement layer:

Verified human authority before action execution.

This makes SyberKey CPE a foundational control plane for the AI-driven and post-quantum enterprise.

SyberKey CPE monitors access continuously, evaluates risk intelligently, verifies the live human when required, and enforces whether sensitive actions can execute across the enterprise stack.