Syberkey
— Patented Tech —

AIPQCAM
AI DRIVEN • POST QUANTUM READY • CONTINUOUS ACCESS MONITORING

# Continuous Zero Trust Access Monitoring with Live Human Verification

## Passwordless. OTP-Free. Decentralised. Post-Quantum Ready.

### Executive Overview

Enterprise security is moving beyond perimeter protection, passwords, one-time MFA and static session trust.

For many years, organisations have relied on a familiar model:

A user logs in.
The user completes MFA.
A session is created.
Access continues until logout, timeout or policy interruption.

That model is no longer enough.

Modern cyber risk is identity-driven, session-based, cloud-enabled, AI-accelerated and increasingly difficult to contain once access has been granted. A user may pass authentication at login, but risk can change minutes later. Devices can become compromised. Sessions can be hijacked. Credentials can be shared. AI agents and automated workflows can initiate sensitive actions at machine speed. Remote and external access has become normal. Sensitive data now sits across portals, SaaS platforms, cloud systems, data lakes and business applications.

SyberKey CAM — Continuous Access Monitoring — is designed for this new environment.

SyberKey CAM provides a practical, low-friction, Zero Trust-style access monitoring layer that continuously evaluates session trust and triggers live human verification when risk, sensitivity or policy requires it.

It is not another password system.
It is not another OTP tool.
It does not require special biometric hardware.

It does not require the customer to replace its identity stack.
It does not need to ingest large amounts of personal or business data.
It does not need to become the customer's master identity directory.

Instead, SyberKey CAM operates as a decentralised, API-connected trust layer that can sit alongside existing portals, identity systems, applications and enterprise environments.

The core value is simple:

**Passwords and MFA prove a login. SyberKey CAM continuously verifies trust after login.**

## The Problem with Traditional Security

Traditional identity security still relies heavily on:

- Passwords
- OTPs
- One-time MFA
- Static session trust
- Device assumptions
- Directory-based access
- Perimeter security
- Long-lived tokens
- Cached credentials
- Broad application access

These tools are useful, but they often validate access at the beginning of a session rather than continuously throughout the session.

This creates a major security gap.

A user may be trusted at login, but after login:

- The device may become risky.
- The session may be hijacked.
- The user may move to an unusual location.
- A sensitive file may be accessed.

- A privileged application may be opened.
- A bulk download may be attempted.
- A payment may be approved.
- A high-risk transaction may be initiated.
- An AI agent may request execution authority.
- A contractor or remote worker may perform unexpected actions.
- A compromised account may appear legitimate.

The key problem is not only authentication.

The problem is ongoing trust.

Modern organisations need to know:

**Is the correct authorised human still behind this session, and should this access continue now?**

SyberKey CAM is built to answer that question.

## What SyberKey CAM Is

SyberKey CAM is a PQ-ready, AI-assisted Continuous Access Monitoring platform that provides ongoing session trust evaluation and live human verification when required.

It continuously monitors access context and applies adaptive security decisions based on:

- User identity
- Session behaviour
- Device context
- Access pattern
- Role or permission level
- Risk signals
- Location change
- Time of access
- Application sensitivity
- Data sensitivity

- Privileged access attempt
- Transaction value
- External-user behaviour
- Remote-worker context
- Policy requirement

When risk is low, access can remain smooth.

When risk increases, SyberKey CAM can require live verification.

When access becomes sensitive, SyberKey CAM can step up assurance.

When trust cannot be re-established, access can be blocked, limited or escalated.

This allows organisations to move from static login security to dynamic trust monitoring.

## The SyberKey CAM Principle

The SyberKey CAM principle is:

**Do not trust a session simply because the user passed login MFA. Keep verifying trust throughout the access pathway.**

Traditional model:

Password or MFA at login

→ session trusted

→ user continues access

SyberKey CAM model:

User logs in

→ session monitored continuously

→ AI risk layer evaluates context

→ live verification triggered when required

→ access continues, steps up, limits or blocks

This creates a much stronger security posture without forcing users through unnecessary friction every time.

## Why SyberKey CAM Is Closer to Zero Trust

Zero Trust is based on the principle that no access should be automatically trusted. Identity, device, context and behaviour should be evaluated continuously.

SyberKey CAM supports this principle by providing:

- Continuous access monitoring
- Risk-based session evaluation
- Live human re-verification
- Adaptive MFA evolution
- Policy-based step-up
- API-connected trust decisions
- Minimal data exchange
- Low-friction deployment
- Hardwareless biometric verification
- Pathway to verified action enforcement

This makes SyberKey CAM significantly more advanced than traditional perimeter security and one-time MFA.

**SyberKey CAM brings practical Zero Trust to active sessions — without forcing organisations into a full identity migration.**

## No Password. No OTP. No Special Hardware.

SyberKey CAM is designed to reduce dependency on outdated and vulnerable authentication methods.

### No password dependency

Passwords remain one of the weakest points in security. They can be stolen, reused, phished, shared or exposed through breaches.

SyberKey CAM reduces reliance on password trust by continuously monitoring session risk and requiring stronger verification when needed.

### No OTP dependency

OTP-based MFA is increasingly vulnerable to phishing, social engineering, SIM-swap attacks, fatigue attacks and man-in-the-middle compromise.

SyberKey CAM moves beyond OTP by enabling live human verification rather than relying on temporary codes.

### No special biometric hardware

SyberKey CAM is hardwareless.

It can work through normal user devices, allowing organisations to deploy live verification without purchasing scanners, issuing special tokens or installing dedicated biometric hardware.

This is critical for:

- Remote employees
- External users
- Doctors and clinical users
- Contractors
- Customers
- Partners
- Field staff
- Distributed workforces
- Portal users
- High-volume user bases

The result is stronger security without heavy infrastructure.

### Decentralised Trust Overlay

One of SyberKey CAM's most important advantages is its decentralised deployment model.

SyberKey CAM does not need to become the organisation's master identity system.

The customer can keep:

- Existing identity provider
- Existing portal
- Existing user database
- Existing employee directory

- Existing IAM or SSO
- Existing application permissions
- Existing business records
- Existing HR or customer systems
- Existing clinical, financial or operational systems

SyberKey CAM simply adds a trust layer.

It can connect by API and backend handshake to monitor access risk and trigger live verification when required.

This means:

**The customer keeps its identity stack. SyberKey adds continuous live human trust.**

## Minimal Personal Information Requirement

SyberKey CAM is designed to operate with minimal data exchange.

For many CAM deployments, SyberKey does not need to ingest:

- Full employee records
- Full customer profiles
- Patient records
- Financial records
- Business documents
- Full Active Directory data
- Sensitive application data
- Passwords
- Customer databases
- Clinical records
- Full personal identity files

SyberKey CAM can work with a mapped reference such as:

- Customer user reference
- Employee user reference

- Portal user reference
- Session ID
- Event type
- Risk context
- Verification status
- Policy level
- Timestamp

This reduces privacy exposure, integration complexity and customer resistance.

**SyberKey does not need to copy the customer's identity directory or sensitive business data. It only needs enough information to verify trust and return a decision.**

### Lightweight API Integration

SyberKey CAM is designed to be easy to integrate.

Instead of requiring a full identity replacement, directory migration or complex enterprise transformation, SyberKey CAM can integrate through:

- API
- SDK
- Webhook
- Login-level handshake
- Step-up verification redirect
- Backend risk event
- Signed decision token
- Application-level policy call

This makes it suitable for both:

- Large enterprises with existing identity systems
- High-volume portals with external users
- Mid-market organisations needing better security quickly

- SMBs seeking low-cost Zero Trust uplift
- SaaS platforms that need embedded trust monitoring
- Healthcare, finance, legal, property, hospitality and data-sensitive environments

The core implementation model is simple:

Application or portal detects login/session/action event

→ SyberKey CAM receives API handshake

→ CAM evaluates risk and policy

→ CAM allows, steps up, blocks or escalates

→ User completes live verification if required

→ SyberKey returns decision

→ Application enforces the decision

→ Audit event is recorded

This is far lighter than replacing the customer's full identity architecture.

### Adaptive MFA Evolved into CAM

SyberKey CAM can be introduced through adaptive MFA and then expanded into continuous monitoring.

The evolution is:

Adaptive MFA

→ Continuous Access Monitoring

→ Verified Action

→ CPE Adapter Enforcement

→ Enterprise Execution Control

This creates a practical adoption path.

Organisations can start with low-friction adaptive MFA and then progressively enable deeper monitoring and action-level verification.

This reduces adoption risk and allows customers to deploy in phases.

## How SyberKey CAM Works

SyberKey CAM evaluates each access pathway dynamically.

**Low-risk access**

A known user on a known device accessing a low-risk system may proceed without interruption.

**Medium-risk access**

A user accessing from a new network or unusual context may receive a push, QR or verification prompt.

**High-risk access**

A user accessing sensitive systems, high-value data, admin functions or unusual sessions may be required to complete live biometric verification.

**Critical-risk access**

A user attempting privileged actions, sensitive exports, payment approvals or AI-enabled execution may require live verification and additional policy controls.

**Suspicious access**

If trust cannot be re-established, SyberKey CAM can support blocking, limiting, suspending or escalating the session.

## Risk-Based Verification Model

| Risk Context | CAM Response |
|---|---|
| Known user, known device, normal behaviour | Allow session to continue |
| New device or unusual location | Step-up verification |
| After-hours or abnormal access pattern | Risk-based challenge |
| Sensitive application access | Live biometric step-up |
| Privileged system access | Strong verification required |
| Bulk download or data export | Live verification and audit |
| Payment or refund approval | Verified human approval |
| Contractor or remote worker risk | Re-verification |

| Risk Context | CAM Response |
| --- | --- |
| Suspicious session behaviour | Limit, suspend or block |
| AI-agent action | Human verification required |

This keeps security high while reducing unnecessary friction.

## Enterprise Employee Use Case

SyberKey CAM can be deployed across large employee populations.

For enterprises with tens of thousands or hundreds of thousands of employees, SyberKey CAM does not need to replace existing identity systems.

Employees are already known to the organisation through existing HR, directory and SSO systems.

SyberKey CAM simply maps the employee reference to a SyberKey trust reference and monitors the session through API handshakes.

This allows enterprises to protect:

- Remote employees
- Hybrid workers
- Executives
- Finance teams
- HR teams
- Developers
- Administrators
- Contractors
- Offshore teams
- Privileged users
- High-risk departments

The enterprise value is substantial:

- Stronger workforce identity security
- Reduced session-hijack risk

- Better protection for sensitive applications
- Live verification of the actual human
- Reduced dependence on OTPs
- Lower integration burden than full identity replacement
- Practical Zero Trust uplift
- Clear upgrade path into Verified Action and full CPE

Enterprise positioning:

**Keep your existing IAM, SSO and directory. Add continuous live human trust.**

## External Portal Use Case

SyberKey CAM is also highly suitable for high-volume external-user portals.

These may include:

- Healthcare portals
- Diagnostic and clinical portals
- Insurance portals
- Legal client portals
- Financial service portals
- Government citizen portals
- Education portals
- Contractor portals
- Supplier portals
- Franchisee portals
- Property platforms
- Hospitality platforms
- Customer service platforms

External portal users are often not employees and should not always be managed as workforce identities.

SyberKey CAM allows organisations to protect these users without forcing them into a full internal directory model.

The portal remains the source of truth.

SyberKey provides the trust decision.

**Protect high-volume external users without turning them into employees in your identity directory.**

## High-Value Use Cases for Fast Adoption

### 1. High-risk login

Trigger live verification when login risk increases.

Examples:

- New device
- New location
- VPN anomaly
- High-risk IP
- Failed login pattern
- Impossible travel
- Suspicious session

### 2. Sensitive application access

Require step-up before access to high-risk systems.

Examples:

- Finance
- Payroll
- HR
- Admin console
- Clinical systems
- Legal documents
- Customer records
- Data warehouses

### 3. Remote workforce monitoring

Re-establish trust for remote, hybrid, outsourced and offshore users.

Examples:

- Remote employees
- Contractors
- Call centre users
- IT support teams
- Virtual assistants
- External consultants
- Managed service providers

### 4. Admin and privileged access

Protect high-risk administrative environments.

Examples:

- Cloud console
- Database console
- SaaS admin portal
- Security dashboard
- Production environment
- User management panel

### 5. Sensitive data access

Require live verification before sensitive data is accessed or exported.

Examples:

- Customer records
- Patient records
- Financial data
- HR files
- Legal files
- Source code

- Intellectual property
- Reports and analytics

### 6. Payment and refund approval

Add live human verification to financial actions.

Examples:

- Refund approval
- Supplier payment
- Bank detail change
- Payroll change
- Invoice approval
- High-value transaction

### 7. Developer and DevOps access

Protect production systems and code workflows.

Examples:

- Production deployment
- Database export
- API key rotation
- Secret access
- Repository admin change
- Security patch approval

### 8. AI-agent supervision

Require verified human authority before AI or automation performs sensitive actions.

Examples:

- AI-generated patch
- Automated remediation
- Secret rotation
- Policy change
- Data extraction

- Customer communication
- Workflow approval

### 9. Document and consent workflows

Extend CAM into live verified document actions.

Examples:

- Document signing
- Contract approval
- Consent forms
- Legal approvals
- Compliance certificates
- High-risk acknowledgements

### 10. Physical-world access

Use CAM as a gateway to real-world access decisions.

Examples:

- Guest access
- Contractor site access
- Facility access
- Key release
- Secure pickup
- Identity-bound approval

## Why SyberKey CAM Is Cost-Effective

SyberKey CAM is designed for low-cost, high-scale deployment.

It can be cost-effective because:

- It does not require full identity replacement.
- It does not require hardware tokens or biometric scanners.
- It does not require large-scale directory migration.
- It does not need unnecessary personal data ingestion.

- It can operate through API handshakes.
- It can be priced by active use, risk events or portal scale.
- It can reduce support costs associated with OTPs and password resets.
- It can reduce breach exposure and audit risk.
- It can be rolled out in phases.

The value proposition is:

**Maximum security uplift with minimal disruption and low integration cost.**

**Enterprise-grade trust without enterprise-grade complexity.**

## Where SyberKey CAM Fits in the Market

SyberKey CAM sits between traditional MFA, adaptive access, identity threat detection and full enterprise Zero Trust.

It is more advanced than ordinary MFA because it monitors trust after login.

It is lighter than full identity replacement because it does not need to become the master directory.

It is more human-assured than ordinary risk scoring because it can require live biometric verification.

It is more commercially flexible because it can support employee, external-user and portal-based pricing models.

## Market position

| Category | What it does | SyberKey CAM difference |
|---|---|---|
| Passwords | Basic login credential | SyberKey reduces reliance on passwords |
| OTP MFA | One-time code challenge | SyberKey avoids OTP dependency |
| Traditional MFA | Verifies login | SyberKey monitors after login |
| Adaptive MFA | Changes challenge based on risk | SyberKey evolves adaptive MFA into continuous monitoring |

| Category | What it does | SyberKey CAM difference |
|---|---|---|
| IAM / SSO | Manages identity and access | SyberKey overlays live trust without replacing IAM |
| ITDR | Detects identity threats | SyberKey can re-establish live human trust |
| ZTNA | Controls network/application access | SyberKey focuses on live human session trust |
| CPE | Full execution control | CAM is the entry layer before Verified Action and full CPE |

## SyberKey CAM vs Traditional Identity Platforms

Traditional identity platforms are powerful but often directory-centric.

They may require:

- User import
- Directory sync
- Active Directory integration
- Identity governance
- App provisioning
- Policy migration
- User lifecycle management
- Full enterprise configuration

SyberKey CAM can be much lighter.

It can integrate through a mapped user reference and backend handshake.

The customer keeps its systems.

SyberKey provides live verification and trust decisions.

| Requirement | Traditional identity route | SyberKey CAM route |
|---|---|---|
| Existing employee directory | Central dependency | Customer keeps it |
| External portal users | May require identity migration or MAU model | Portal reference can be mapped |
| Personal information | Often more attributes required | Minimal data required |
| Integration | Directory and application project | API handshake and step-up trigger |
| Authentication | Login-focused | Login plus continuous monitoring |
| Verification | MFA/device/risk signals | Live biometric human verification |
| Deployment | Broader identity project | Lightweight trust overlay |
| Cost | Often per-user suite pricing | Flexible active-use/step-up pricing |
| Upgrade path | Identity governance | Verified Action and CPE |

## Competitive Edge

SyberKey CAM's competitive edge comes from the combination of capabilities.

**1. Continuous monitoring**

CAM does not stop at login. It monitors session trust continuously.

**2. Live biometric verification**

CAM can verify the real human, not just the account, device or token.

**3. No OTP dependency**

CAM reduces exposure to OTP phishing, SIM swap and MFA fatigue.

**4. No special hardware**

CAM can work without scanners, tokens or dedicated biometric hardware.

**5. Decentralised deployment**

CAM does not need to become the customer's identity directory.

**6. API-connected integration**

CAM can connect at login, session and step-up levels through lightweight APIs.

**7. Minimal personal data**

CAM can operate with mapped references rather than copying full personal records.

**8. Low-cost adoption**

CAM can be sold as a practical Zero Trust uplift rather than a full platform replacement.

**9. Large-scale suitability**

CAM can support high-volume employees, external users, contractors, customers and portal users.

**10. Pathway to Verified Action and CPE**

CAM is the entry layer into SyberKey's broader action-control architecture.

## From CAM to Verified Action

CAM monitors trust.

Verified Action confirms sensitive human approval.

CPE enforces execution.

The SyberKey product ladder is:

SyberKey CAM

Continuous access monitoring

→ SyberKey Verified Action

Live human approval for sensitive actions

→ SyberKey CPE Adapter Edition

Enterprise integration with IAM, PAM, EDR, DLP, SIEM, workflow and cloud systems

→ SyberKey Enterprise CPE

Full AI-controlled, PQ-ready execution enforcement

This creates a clear expansion pathway for customers.

Start with continuous access monitoring.

Expand to sensitive action approval.

Then connect to enterprise systems.

Then enforce execution across the organisation.

## Example: CAM to Verified Action

A user logs in to a portal.

CAM monitors the session.

The user attempts to access sensitive data.

CAM detects increased risk.

SyberKey requests live verification.

The user is verified.

Access continues.

Later, the user attempts to export data.

That is no longer just access monitoring. It becomes a Verified Action.

SyberKey verifies the human, binds the approval to the action and returns a signed decision.

This is how CAM naturally expands into stronger enterprise security.

## Post-Quantum Ready Security Direction

SyberKey CAM is designed as part of a broader post-quantum-ready with its own Post Quantum Key.

This means the platform is aligned with:

- Cryptographic agility
- Future-ready trust models
- Stronger approval records
- Secure control signals
- Long-term identity assurance

For many organisations, post-quantum readiness is becoming a board-level and long-term security concern.

**A practical Zero Trust product today, with a post-quantum-ready for tomorrow.**

## AI-Controlled Risk Direction

SyberKey CAM uses an AI-assisted risk model to decide when trust must be re-established.

The purpose is not to create more alerts.

The purpose is to decide:

- Allow
- Step up
- Limit
- Block
- Escalate
- Require live verification

This makes CAM practical.

Instead of overwhelming the security team with warnings, CAM can trigger real-time trust actions.

**AI evaluates risk. SyberKey verifies the human. The application enforces the decision.**

## Marketing Positioning

**SyberKey CAM continuously verifies trust after login — without passwords, OTP dependency or special hardware.**

**SyberKey CAM gives enterprises a low-friction Zero Trust access layer without replacing existing IAM, SSO or directory systems.**

**SyberKey CAM protects high-volume external users through API-connected continuous access monitoring and live biometric step-up.**

## Security positioning

**SyberKey CAM moves organisations from perimeter security to continuous human trust.**

## Cost positioning

**Maximum security uplift with minimal integration cost.**

## AI-era positioning

**In an AI-driven world, SyberKey ensures sensitive access and actions remain tied to verified human authority.**

## Post-quantum positioning

**SyberKey CAM is Ready  for the post-password, AI-driven and post-quantum security era.**

## Continuous Zero Trust Access Monitoring

**Without Passwords, OTP Dependency or Special Hardware**

SyberKey CAM continuously monitors user sessions, evaluates access risk and triggers live biometric verification when trust must be re-established.

Protect employees, external users, contractors, customers and portal users without replacing your existing identity stack.

**Keep your systems. Add continuous live human trust.**

## Move Beyond Login MFA

Traditional MFA verifies the user once. SyberKey CAM keeps evaluating trust throughout the session.

### Verify the Human, Not Just the Account

When risk increases, SyberKey CAM can require live biometric verification to confirm the authorised human is still present.

### Deploy Without Identity Replacement

SyberKey CAM connects through APIs and backend handshakes, allowing customers to keep existing IAM, SSO, portals and directories.

### Reduce Personal Data Exposure

SyberKey CAM can operate using mapped user references and minimal data, reducing privacy risk and integration burden.

### Built for Scale

CAM can support large employee populations, external portals, contractors, customers and distributed users.

### Start with CAM. Expand to CPE.

Begin with continuous access monitoring, then expand into verified action approval and full enterprise execution control.

## Pitch

Your organisation may already have IAM, SSO and MFA. But those systems often verify users at login and then trust the session.

SyberKey CAM adds a continuous trust layer.

It monitors access risk after login and triggers live biometric verification only when needed — such as new device, unusual location, sensitive application access, privileged access, bulk download, high-value transaction or suspicious session behaviour.

It does not require you to replace your identity stack. It does not require special biometric hardware. It does not depend on OTPs. It can integrate through lightweight APIs and backend handshakes.

SyberKey CAM gives you a practical path to Zero Trust access monitoring at low cost and low disruption.

## Partner Pitch

SyberKey CAM is an ideal product for implementation partners, systems integrators, MSPs and security consultants because it provides a simple, high-value security uplift without forcing a full identity transformation.

Partners can deploy CAM around:

- Employee login and session monitoring
- External-user portal protection
- Admin panel protection
- Sensitive application step-up

- Remote workforce verification
- Contractor access assurance
- High-risk transaction verification
- Data export monitoring
- Initial Zero Trust uplift

This creates fast implementation opportunities and a natural expansion path into Verified Action and Enterprise CPE.

## Buyer Message

**For CIOs**

Improve access security without replacing the identity stack.

**For CISOs**

Add continuous live human trust to sessions and sensitive access pathways.

**For compliance leaders**

Strengthen auditability and reduce unauthorised access risk.

**For operations leaders**

Protect users without unnecessary friction or hardware deployment.

**For digital portal owners**

Secure high-volume users through lightweight API integration.

**For boards**

Move beyond perimeter security into continuous human-verified trust.

## Product Packaging

**SyberKey CAM Starter**

For SMBs, SaaS platforms and smaller teams.

Includes:

- Continuous access monitoring
- Basic risk rules

- Live verification step-up
- Session logs
- API integration
- Admin dashboard

**SyberKey CAM Business**

For mid-market and high-volume portals.

Includes:

- Risk-based monitoring
- Live biometric step-up
- External-user support
- Role-based policy
- Portal integration
- Audit reporting
- API/webhook support

**SyberKey CAM Enterprise**

For large organisations.

Includes:

- Workforce session monitoring
- High-risk application policies
- Contractor and external-user monitoring
- Advanced risk rules
- Enterprise reporting
- Integration with IAM/SSO
- Verified Action upgrade path
- CPE adapter readiness

## Why Now

The timing for SyberKey CAM is strong because the security environment has changed.

Organisations are facing:

- Identity-based attacks
- MFA fatigue
- OTP phishing
- Session hijacking
- Remote workforce risk
- Contractor access risk
- Cloud application sprawl
- Sensitive data exposure
- AI-driven automation
- Insider risk
- High-volume external portal access
- Rising cyber insurance expectations
- Board-level security accountability
- Post-quantum transition planning

The market needs a lighter, more practical way to achieve continuous trust.

SyberKey CAM is designed for exactly that.

## Conclusion

SyberKey CAM is a decentralised, API-connected Continuous Access Monitoring platform that brings practical Zero Trust security to employees, external users, contractors, customers and high-volume portal environments.

It continuously evaluates session trust, applies AI-assisted risk decisions and triggers live biometric verification when risk or sensitivity requires it.

It does not require passwords, OTP dependency, special biometric hardware, full identity replacement or unnecessary personal data ingestion.

It allows organisations to keep their existing IAM, SSO, portals and directories while adding a powerful live human trust layer.

SyberKey CAM delivers:

- Stronger security
- Lower friction
- Faster integration
- Reduced privacy exposure
- Lower cost adoption
- Scalable protection
- Zero Trust-style continuous monitoring
- Upgrade path to Verified Action and CPE

The core message is:

**Keep your identity stack. Add continuous live human trust.**

**SyberKey CAM turns adaptive MFA into continuous Zero Trust access monitoring — passwordless, OTP-free, hardwareless, API-connected and built for the AI and post-quantum era.**