MyCena® Technical Whitepaper

Eliminating Credential Risk: A New Cybersecurity Paradigm

Updated version: July 2025
Contact Information: julia@mycena.co

Table of Contents

1. Executive Summary
2. Problem & Market Context
3. MyCena® Solution Overview
4. Technical Architecture
5. Use Cases / Industry Examples
6. Competitive Comparison
7. Compliance & Trust
8. Implementation & Deployment
9. Conclusion & Call to Action
10. Appendices

1. Executive Summary

In today's threat landscape, over 90% of cyber breaches begin with stolen or misused credentials. Despite **$215 billion spent on cybersecurity in 2024**, credential-based attacks continue to dominate breach vectors, driven by the rise of AI-powered phishing and infostealer malware. Major incidents like those at M&S, Snowflake, UnitedHealth/Change Healthcare, Synnovis, Qantas, Allianz or M&S all stemmed from a single design flaw: allowing humans to create, manage, or reuse their own access credentials. These user-visible credentials are routinely phished, leaked, or stored insecurely, turning every employee and vendor into a potential breach point. As a result, organizations face compounding financial, operational, and reputational damage that existing tools fail to prevent.

The root cause lies in a flawed architecture where identity and access are conflated into a single layer. Unlike physical systems where identification and authentication are separate, digital systems rely on individuals to prove who they are *and* hold the key at the same time—often in the form of passwords, tokens, or biometrics. IAM, SSO, and password managers still merge identity and access, merely centralizing credentials into a single point. To stop humans from being the vulnerability, identification and authentication need to be separated so people no longer create, store, or manage their own credentials.

MyCena® was built to eliminate this vulnerability at its root. Rather than relying on people to create, manage, and secure credentials, MyCena® replaces user-managed credentials with an **unphishable, encrypted access architecture.** At the heart of the platform is the patented Multi-Layered Dynamic Access Encryption Security (ML-DAES) model, which **separates identification from authentication** and distributes segmented, encrypted, invisible credentials users never see, know, or handle. This design eliminates credential phishing, blocks lateral movement, and stops attackers from accessing critical systems even after an initial compromise.

It overlays existing infrastructure without disrupting workflows, enabling centralized credential management, automatic revocation, access segmentation, and real-time audit access logs. The result is a zero-trust, zero-knowledge access architecture that makes businesses unphishable, simplifies compliance with GDPR, ISO 27001, and SOC 2, and delivers long-term cyber resilience. MyCena® ML-DAES model is not only a better way to manage passwords—it is a mathematical way to close the breach pathway entirely.

Figure 1. MyCena® Multi-Layered Dynamic Access Encryption Security (ML-DAES) technology platform delivers invisible, encrypted, segmented access credentials to users

2. Problem & Market Context

2.1. The Paradox: Record Cyber Spending, Record Credential Breaches

Despite a record **$215 billion spent on cybersecurity in 2024**, credential-based attacks remain the leading cause of breaches worldwide. Sophisticated firewalls, identity and access tools, and endpoint protections continue to overlook the most exploited vulnerability: human-managed credentials. According to Verizon's 2024 Data Breach Investigations Report, 91% of breaches begin with phishing, and 80% involve weak or stolen credentials. Now, with the rise of AI-powered attacks, phishing campaigns have become faster, more targeted, and harder to detect—dramatically increasing risk exposure and overwhelming traditional defences. The attack surface isn't shrinking—it's evolving and accelerating.

The real-world consequences of credential-based vulnerabilities are both severe and widespread. In 2024, Snowflake, a major SaaS data platform, suffered a credential stuffing attack that compromised over 165 customer accounts. The attackers used credentials stolen by infostealer malware from unrelated systems to breach Snowflake's environment, exposing vast amounts of sensitive data across multiple sectors, including financial institutions and healthcare providers.

These risks extend far beyond isolated data loss. In the same year, a cyberattack on UnitedHealth Group's subsidiary, Change Healthcare, resulted in a financial hit of over $2.45 billion, including $1.5 billion in direct response costs and hundreds of millions in lost revenue and operational disruption. Similarly, Synnovis, a pathology services provider for the NHS in the UK, suffered a £32.7 million loss due to a ransomware attack, while KNP Logistics, a 158-year-old UK firm, was permanently shut down after attackers phished a weak employee password. These aren't isolated failures; they're cross-sector catastrophes, all rooted in the same weakness: human-managed credentials.

2.2. The Root Cause: A Broken Access Architecture

At the core of these failures lies a fundamental design flaw: modern access systems have merged identification and authentication into a single, user-managed process. In the physical world, these are separate use cases. Identification means proving who you are, like showing an ID at an airport or when sitting an exam—it cannot be your sibling or friend. Authentication means proving you have the right to access something, like unlocking a door with a key—the door doesn't care who you are as long as you have the key.

But in digital systems, these two layers were merged into a single layer. Users are asked to *prove who they are* by *creating, storing, and managing their own credentials*. In effect, it means employees are making the keys to companies' digital buildings and are responsible for the security of those keys. Here the risk of credential compromise multiplies exponentially at scale.

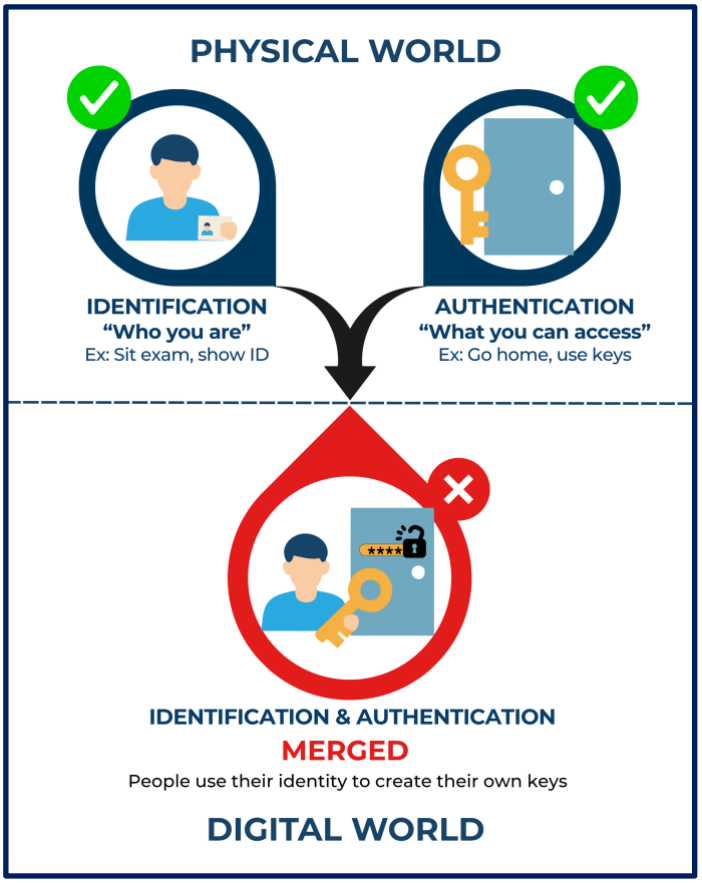

Figure 2. Separation of Identity and Access: Physical vs. Digital Paradigms

As organizations rely on complex ecosystems of third, fourth, and even fifth-party vendors, each with their own access points and passwords, this flawed architecture effectively turns every password in your supply chain into a breach risk—making humans the largest and most vulnerable attack surface in the entire system:

- Employees and third parties generate passwords that are visible, phishable, and shareable. There are millions of credentials across your supply chain—from internal teams to contractors, vendors, and outsourced partners. Every login is a potential breach point.
- These credentials are stored in browsers, spreadsheets, or reused across systems.
- From one stolen credential, attacker can inject malware, scan the environment, look for credentials to move laterally and find privileged access to take over the network (from CRMs to payroll systems to critical infrastructure), steal data and launch ransomware attacks.

Allowing employees to create and manage their own passwords not only invites human error but violates core compliance principles around data governance and access control. Regulators under GDPR, LGPD, HIPAA, and emerging frameworks like DORA now expect companies to demonstrate control over who can access what and how.

2.3. Why Existing Solutions Fall Short

Despite their widespread adoption, tools like IAM (Identity Access Management), SSO (Single Sign On), and password managers fail to address the core issue: they still rely on user-visible, human-managed credentials—whether it is a password, token or biometric. These solutions may improve convenience or centralize control, but they don't eliminate the underlying vulnerability of merging identity with access. Credentials can still be phished, copied, leaked, or reused—leaving organizations exposed to the very attacks these tools were meant to prevent. Rather than solving the problem, they simply shift it, maintaining a broken model that continues to depend on the weakest link: the user.

2.4. The Market Gap: Restoring Separation of Identification and Authentication

What the market needs isn't another identity layer. It's a return to proper separation of duties:

- Identification should verify users.
- Authentication should be controlled by the enterprise—secure, encrypted, and invisible.

By removing human involvement from credential creation, storage, and use, organizations can eliminate the weakest link—user-visible credentials. This shift not only closes the door to phishing and credential theft but also reclaims control over access from end users, establishing a secure-by-design zero-trust foundation for the digital enterprise.

3. MyCena® Solution Overview

MyCena® was created to eliminate the root cause of most cyber breaches: human-managed credentials. While traditional access management systems focus on verifying identities, they still require users to create, remember, or use passwords—leaving the organization vulnerable to phishing, credential stuffing, and insider threats. MyCena® replaces this broken model with a patented system that distributes invisible, encrypted, segmented access credentials that users never see, know, or manage.

At its core, MyCena® separates **identification** from **authentication**—a fundamental shift in how secure access is delivered. Instead of asking users to generate passwords and store them in a vault or rely on Single Sign-On (SSO) systems that centralize risk, and which still require a user-managed password or identity, MyCena® ensures that access credentials are created by the company, segmented by application, and encrypted at rest and in transit. This segmented, zero-knowledge zero-trust approach means there are no shared credentials, no single points of failure, and no opportunities for phishing to succeed.

Users interact with MyCena® through a secure mobile or desktop application, where they identify themselves using multi-factor authentication (MFA), security questions and personalized security layers (PIN, pattern, or passphrase). Once identified, users can retrieve their access credentials from predefined tiers (Bronze, Silver, Gold), based on the sensitivity of the system they are accessing.

Figure 3. Quick and easy credentials access for users

Users click on the system icon on the application that they want to access, and those specific credentials are then automatically injected by the MyCena® Desk Center (MDC) extension —without the user ever seeing or typing them.

Figure 4. Users click to log in

This approach has several benefits:

- No password creation, reuse, or sharing by employees.
- No phishing or social engineering risk since users don't know passwords.
- Segmentation of access, preventing any lateral movement in the event of a breach.
- Zero-trust access architecture doesn't rely on someone's identity.
- Rapid credential rotation in case of compromise or personnel change.

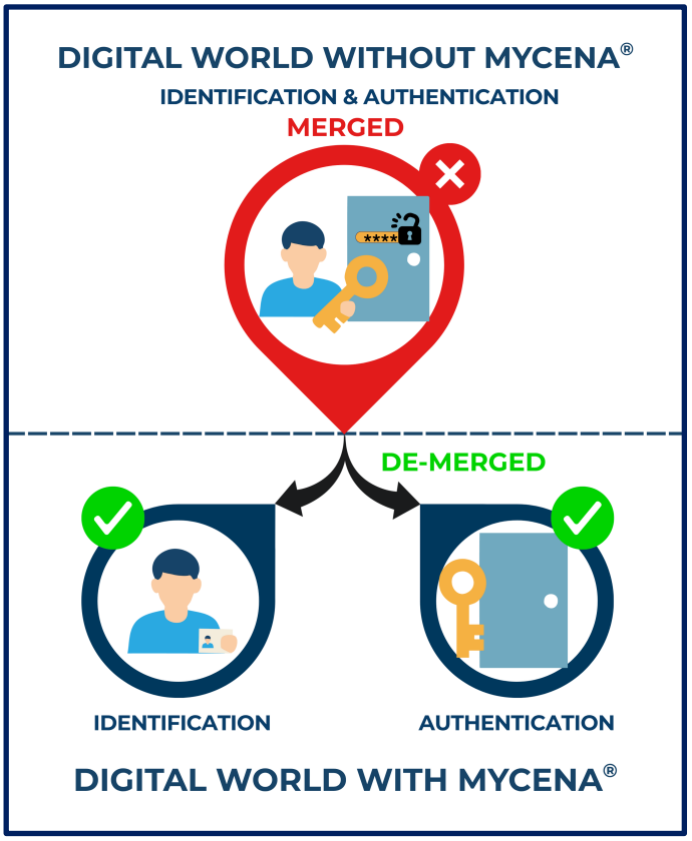

Figure 5. Restoration of Identity-Access Separation Through MyCena®

MyCena® acts as an overlay to your existing infrastructure. If the company already uses IAM, SSO, or PAM systems, it complements them by protecting their access credentials. MyCena® integrates with systems like Active Directory, RDP, SSH, HTTPS, legacy applications, and even supply-chain portals (see 4. Technical Architecture). This makes it fast to deploy, with no need to rip and replace existing systems, providing an immediate positive impact on security posture.

MyCena® also enhances audit and compliance. All credential access events are logged on the MyCena® console, creating immutable records that support GDPR, SOC 2, ISO 27001, and other regulatory frameworks. Role-based MyCena® console and application permissions, IP/device restrictions, and rapid onboarding/offboarding help enterprises regain control over who can access what, when, and from where.

In summary, MyCena® doesn't just manage credentials—it eliminates the attack surface they create. By removing humans from the credential loop and distributing encrypted, invisible access at scale, MyCena® delivers a future-proof model of secure authentication that enhances resilience, simplifies compliance, and frees IT teams from the burden of password-related incidents.

Figure 6. No Identity Theft. No Password Resets.

4. Technical Architecture

The MyCena® Multi-Layered Dynamic Access Encryption Security (ML-DAES) platform was designed as a modular, layered architecture that replaces human-managed credentials with encrypted, segmented, invisible access — preventing phishing, lateral movement, and privilege escalation by design.

It is deployed as a security overlay to existing infrastructure (IAM, SSO, PAM, https…) and is composed of four integrated product layers:

4.1. Core Solution: Unphishable Access

At the heart of the MyCena® platform lies the Unphishable Access solution, which eliminates credential vulnerabilities by removing user knowledge from the authentication process.

Key mechanisms include:

4.1.1. Credential Generation and Encryption from a Console

- All credentials are generated from the MyCena® Desk Center (MDC) console using secure randomization.
- Each password is unique per user and system, encrypted using combination of AES-256, and SHA-256 algorithms.
- Credentials are encrypted at rest and in transit, with distinct keys per user and company to prevent replay or interception attacks.

Figure 7. MyCena® encryption model

4.1.2. Credential Segmentation and Cascading Access Tiers

Credentials are grouped into access tiers to mitigate internal lateral movement:

- **Bronze** (low risk): Accessed via PIN (e.g. internal tools, HR)
- **Silver** (medium risk): Accessed via lock pattern (e.g. CRM)
- **Gold** (high risk): Accessed via passphrase (e.g. SSH, servers, banking)

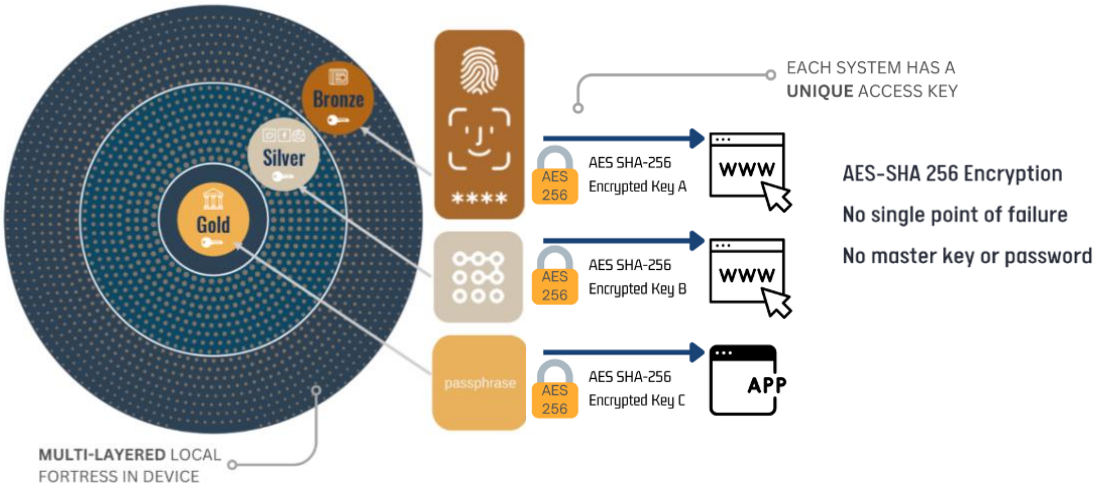

Figure 8. Cascading tiers ensures that compromising one tier does not expose the rest.

4.1.3. Zero-Knowledge Zero-Trust Authentication Model and Autofill

- MyCena® uses proofs to validate identity without credential exposure.
- Secure channel retrieval after multi-factor authentication (2FA, security questions)
- Users never see, type or handle credentials — preventing phishing.
- Credentials are auto filled via the MDC extension across web, desktop, or mobile.
- Credentials are not stored in browsers or memory— preventing clipboard leakage.
- No infrastructure replacement needed — MyCena® acts as a drop-in security wrapper over your current stack.
- One credential per system prevents lateral breaches from third-party access.

Figure 9. Multi-Layered Dynamic Access Encryption Security Model

4.1.4. User registration

Admins can register employees in multiple ways:

- Via LDAP/LDAPS, Entra ID.
- Via template upload.
- One by one on the console.

4.1.5. Role-Based MyCena® ML-DAES Access Permissions

Admins define granular permissions for user groups and roles, controlling what they can do within the MyCena® console and application.

4.1.6. Breach Response and Credential Rotation

From the MyCena® console, admins can instantly revoke, rotate, or reassign credentials globally — without requiring employee action — reducing time-to-containment during incidents.

4.1.7. Integration with Web-based Applications

- Businesses can immediately protect all web-facing applications against credential-based attacks such as phishing, social engineering and credential stuffing.
- First points to secure are usually IAM/SSO: e.g. Okta, Ping, Azure AD, etc.

4.2. Third-Party Resilience Layer

This layer builds business continuity and breach containment into the architecture:

- **IP and device restrictions**: Lock access to known endpoints.
- **Contingency plan**: Maintain access during outages.
- **Encrypt API connections**: Never share visible passwords with third parties, including bots.
- **Supply-chain risk mitigation**: Prevent lateral movement if a vendor is breached.

Together, these functions ensure that credential misuse is self-limiting, and access control persists through operational disruptions.

4.3. Admin Tools Layer

Built for IT and security teams to govern internal access and servers:

- Remote protocols: RDP, SSH.
- Legacy apps: SAP, internal tools.
- Custom integration with local applications.

4.4. Governance & Compliance Layer

- Provides real-time visibility and compliance automation.
- All login events, credential requests, MFA challenges, and system activities are logged.
- Logs are exportable to SIEM platforms for monitoring, threat detection, and forensic analysis.
- Encrypts external GRC API connection.

- Supports GDPR, SOC 2, ISO 27001, DORA, and HIPAA reporting: Managers can track access by user, tier, system, or endpoint — ensuring demonstrable control over digital access as required by regulators.

This layered architecture ensures progressive adoption: start with phishing elimination, then scale into enterprise-grade governance—without user friction or architectural disruption.

5. Use Cases - Industry Examples

MyCena® ML-DAES has been successfully deployed across multiple industries where credential misuse poses a critical threat. Three real-world examples demonstrate how MyCena® helps enterprises gain control over access, eliminate phishing and credential-related vulnerabilities at the root, stop lateral movement, and ensure regulatory compliance—with rapid deployment and no need for infrastructure replacement.

5.1. Financial Services – Stopping Password Fraud & Protecting PII

A 1,200+ employee credit collection firm, serving banks and financial institutions, faced rampant credential misuse. Employees were reusing, sharing, and even selling passwords, creating substantial risks of ransomware, data breaches, and non-compliance with data protection regulations. With a huge amount of PII handled daily, any breach could result in fines of up to 4% of global turnover and serious reputational damage.

By deploying MyCena® Unphishable Access with encrypted credential autofill, IP restrictions, and access governance, the company:

- Eliminated password fraud and resets.
- Improved compliance and auditability.
- Reduced SLA penalties and IT workload.
- Rolled out securely with no infrastructure changes.

The firm now operates with invisible, segmented credentials, immutable access logging, and dramatically enhanced cyber-resilience—all without disrupting user workflows.

5.2. Logistics – Securing Third-Party Access & Stopping Ransomware

A 10,000+ employee transportation company serving essential supply chains faced growing risks from unmanaged credential practices. With no centralized access control, passwords to critical systems—including ERP, fleet, warehouse, client portals, SSH, RDP —were shared informally via spreadsheets, messaging apps, and email threads with no traceability over unauthorized use, making the company vulnerable to ransomware and supply-chain compromise.

After using MyCena® to segment and encrypt access, the organization:

- Eliminated password visibility entirely.
- Achieved full credential traceability and governance.
- Secured critical infrastructure without disrupting operations.
- Blocked phishing, lateral movement, and credential stuffing.
- Integrated seamlessly with existing systems.

This transformation enabled the company to control all access, protect vital operational systems, and meet regulatory mandates.

5.3. Insurance – Ending Password Chaos and Enabling Secure Growth

A 1,200+ employee insurance brokerage firm managing access to over 60 partner portals—many without APIs—struggled with rampant password sharing, frequent credential resets, and login failures that disrupted financial pipelines and exposed the firm to serious compliance risks. Sales, finance, and development teams were emailing passwords like "Zurich: XYZadmin / 123456" across departments, causing daily failures in commission data pipelines, and a constant cycle of blocked accounts and IT tickets. Developers relied on manually embedded credentials for automation tasks, and ex-employee access remained an open risk.

By deploying MyCena® with segmented credential vaults, secure API integration, and zero password visibility for end users and developers, our customer:

- Eliminated over 40 weekly login failures and password resets.
- Restored uninterrupted access to critical data and commission flows.
- Cut developer ticket escalations by ~60%.
- Closed GDPR and ISO 27001 compliance gaps.
- Strengthened their cyber-insurance posture with their insurer.

MyCena® was embedded into DevOps automation pipelines and rolled out without infrastructure changes. End users no longer needed to "guess" or share credentials, while developers accessed systems securely without ever seeing a password.

"Before MyCena, it was chaos. Credentials were shared in chat groups, resets happened daily, and critical processes failed all the time. Now, there are no more bugs, no more login issues, and we're finally compliant—without adding friction to user workflows." — Head of Infrastructure, Cybersecurity, Data & CRM, Insurance brokerage firm.

6. Competitive Comparison

The access security market is saturated with tools like SSO (Single Sign On), IAM (Identity and Access Management), PAM (Privileged Access Management), password managers, and MFA (Multi-Factor Authentication) providers—but none solve the core issue of human-managed credentials.

Figure 10. Existing tools require user identity or password, which can be stolen

MyCena® ML-DAES takes a fundamentally different approach: it removes employees from the credential process entirely by distributing invisible, encrypted, segmented access credentials they never see or manage.

Figure 11. Employee clicks a phishing email but doesn't know password so can't give it away

How MyCena® ML-DAES Compares

Function	Traditional Tools	MyCena® ML-DAES
Credential visibility	Users manage passwords	Users never see or create credentials
Password security	Vault-based or shared	AES-256 encrypted, segmented per app/tier
Integration	Often requires infrastructure changes	Drop-in overlay with existing systems
Access tiers	One-size-fits-all	Bronze/Silver/Gold tiered access
Phishing defence	Reactive (MFA alerts, training)	Proactive – no password to phish
Credential rotation	Manual or privileged accounts only	Centralized, user-free

Figure 10. Traditional access tools vs. MyCena® ML-DAES

What MyCena® ML-DAES Is Not

- A password manager that stores credentials for user access or reuse - though it a password manager feature as an add-on.
- A vault – it doesn't let users see or manage stored passwords.
- An SSO or IAM platform – it doesn't federate identity or session tokens.
- A PAM system – it's not limited to privileged access.
- A standalone MFA app – though it offers built-in MFA as an add-on.

Instead, MyCena® ML-DAES platform is a credential encryption, segmentation and automation platform—designed to be an overlay on top of or beneath your existing IAM, SSO, and PAM stack to eliminate phishing, password reuse, and lateral movement. It comes with many optional add-on features, including:

- Password Manager for Non-Sensitive Use: While MyCena® eliminates passwords for sensitive systems, some use cases still require user-managed access—like trialling SaaS tools, working with clients, or temporary project logins. To support this, MyCena® includes an optional encrypted password vault, giving users a secure space to manage non-critical credentials—without compromising the platform's integrity or auditability.
- Integrated Multi-Factor Authentication (MFA): MyCena® also includes an MFA add-on for enterprises needing a fully self-contained access security environment inside one platform.

7. Compliance & Certifications

MyCena® is fully compliant with GDPR, ensuring all user data is handled with the highest privacy and security standards.

Data privacy regulations such as GDPR specifically require companies to have control over their data access. Non-compliance, especially following a breach, can be very costly, with errant companies subject to fines of up to 4% of their global turnover.

By using MyCena®, employees can no longer create and use their own passwords. This control is essential to meet regulatory expectations around data access governance, least-privilege enforcement, and access traceability.

MyCena® regularly undergoes third-party security audits and holds relevant certifications to validate its security measures and operational integrity.

Figure 12. Compliance and certifications

8. Implementation & Deployment

MyCena® is designed for fast, frictionless deployment—without requiring changes to existing infrastructure. As a security overlay, it integrates easily with your current IAM, PAM, SSO, and legacy systems, making it ideal for both modern cloud environments and traditional on-premises architecture.

Deployment can be completed in as little as a **few days**, depending on the organization's size and complexity. For most small and mid-sized enterprises, full rollout—including admin training, tier mapping, and credential provisioning—can be achieved within **2-4 weeks**.

Key Implementation Steps:

1. **Discovery & Scope Definition**: Define credential types, systems, user groups, and access tiers.

2. **Implementation**: Add external apps and cloud platforms via the MyCena® Desk Center (MDC) **console, then in a second phase add legacy systems, local apps, APIs.**
3. **User** Onboarding: Assign system credentials to users, and users configure personalized login layers (PIN, pattern, passphrase).
4. **Go Live**: Users receive access through the MyCena® app or extension, with no visible or stored credentials involved.

MyCena®'s modular approach allows organizations to start with access unphishability, then continue with internal resilience, admin tools, and governance & compliance. Throughout the rollout, IT teams retain full control via the centralized console, and end users experience no change to their workflows—only a smoother, more secure login experience.

With no rip-and-replace required, MyCena® delivers immediate security gains with minimal internal disruption.

9. Conclusion & Call to Action

Credentials-based attacks remain the leading cause of breaches—and traditional access models continue to expose organizations to unnecessary risk, complexity, and compliance burden. MyCena® ML-DAES offers a fundamentally different approach: by eliminating employee-managed credentials and automating invisible, encrypted, segmented access, it closes the gap that attackers exploit.

Whether you're looking to prevent phishing, secure critical infrastructure, reduce IT workload, or simplify audit preparation, MyCena® delivers immediate, measurable value—without changing your existing architecture or disrupting user workflows.

Organizations across regulated sectors are already experiencing stronger security, reduced operational risk, and enhanced compliance through MyCena®'s zero-knowledge, zero-trust model.

It's time to take back control of your access.

No passwords. No phishing. No breaches.

Book a free consultation or request a live demo today:
contact@mycena.co | www.mycena.co

10. Appendices

Appendix 1 - MyCena® ROI, Economic and Strategic Value

Cybersecurity decisions often hinge not only on technical strength but on quantifiable outcomes. MyCena® delivers measurable ROI by eliminating the initial infection vector (stolen credentials) and preventing breach propagation through access segmentation. This enables organizations to assess value not just in cost savings, but in avoided losses, operational continuity, and compliance readiness.

Quantitative Risk Model

Most cyberattacks follow a predictable pattern:

1. **Initial infection via stolen credentials.**
2. **Lateral movement across systems.**
3. **Data exfiltration, encryption, or disruption.**

MyCena® intervenes at key stages:

- **Source Elimination**: Credentials are invisible, encrypted, and never user-managed—removing the ability for attackers to phish, steal, or reuse them.
- **Propagation Control**: Segmented access prevents compromised systems from infecting others, halting lateral movement.

This dynamic mirrors epidemiological models of infection containment. To conceptualize the impact of MyCena®, we used an epidemic-inspired risk containment model or SIR (Susceptible-Infected-Recovered) epidemic model, applied to cyberattack propagation.

Let **S(t)** be the number of secure (susceptible) systems, **I(t)** the infected systems, and **γ** the rate of isolation. Credential-based attacks spread at rate **ε**, the likelihood of a stolen credential compromising another system:

$$\frac{dI}{dt} = \epsilon \cdot S(t) \cdot I(t) - \gamma \cdot I(t)$$

Because MyCena® drives **ε → 0** (i.e., credential theft becomes nearly impossible), and enables fast segmentation (**γ ↑**), the model simplifies to:

$$\frac{dI}{dt} \approx -\gamma \cdot I(t)$$

In simple terms, infections decay rapidly, unable to propagate. This dramatically reduces:

- Breach likelihood.
- Incident response time.
- Data loss and reputational damage.
- Regulatory fines and insurance premiums.

ROI

Organizations using MyCena® typically realize:

In real-world cases, companies have avoided:

Metric	Before MyCena®	After MyCena®
Login failures	Dozens per week	0
Credential resets	Weekly	Eliminated
Compliance gaps	Persistent	Resolved (GDPR, DORA, HIPAA)
Cyber insurance premiums	Rising	Reduced risk profile
User friction, training	High	None – no behaviour change

- Fines of up to 4% of global turnover for non-compliance (GDPR, LGPD).
- Business interruption costs in the millions of dollars per incident.
- Reputation loss and customer churn due to data breaches.

Economic & Strategic Value

MyCena® goes beyond traditional ROI—it shifts cybersecurity from a reactive cost center to proactive value enabler by:

- Reducing IT support workload.
- Enhancing auditability and trust.
- Freeing resources for innovation.
- Demonstrating control to regulators and insurers.

This makes MyCena® a cornerstone of digital resilience—not just a security tool, but a business continuity asset.

Appendix 2 - Credential Maturity Ladder

The **Credential Maturity Ladder** framework outlines nine stages of access security maturity, from fully phishable, user-managed passwords without MFA (Level 1) to fully encrypted, segmented, and governed infrastructures with IP/device restrictions (Level 9). It helps organizations benchmark their current state and chart a path towards unphishable, zero-trust credential architecture—essential for compliance, resilience, and cyber-insurance alignment.

Level 9	**Full Ecosystem Segmentation + IP/Device Restrictions + Governance + 2FA = Maximum Security** Adds **device and IP restrictions**. Access only allowed from approved devices or locations. Maximum lockdown.
Level 8	**Full Ecosystem Segmentation + Governance + 2FA for critical systems** All critical systems require 2FA on top of access segmentation and encryption. Even stronger defence if someone tries to log in.
Level 7	**Full Ecosystem Segmentation + Governance** Adds governance layer. All access is logged and auditable. See who accessed what, when, and from where.
Level 6	**Full Ecosystem Segmentation** All credentials are encrypted for employees, third parties, and machines. Internal systems like servers and APIs are isolated too. Breach containment is enforced across the full ecosystem.
Level 5	**Encrypted + Segmented + Third Party Protection** Employees and third parties use encrypted, unphishable credentials. Third parties access systems securely via MyCena® app or encrypted APIs. No one sees passwords.
Level 4	**Encrypted + Segmented for Employees** Credentials are encrypted, auto-filled and unphishable, and each app/system access is isolated for employees. A breach in one app doesn't affect the others.
Level 3	**Unphishable: Encrypted for Employees (No Segmentation)** Employees can't see the passwords anymore—they're encrypted, auto-filled and unphishable —but all apps are grouped together behind SSO, IAM, PAM, so a breach in one can spread.
Level 2	**Phishable, With MFA** Passwords visible to everyone, but MFA is enabled on important systems. Still phishable; only slightly better.
Level 1	**Phishable, No MFA** All passwords are visible to employees and suppliers. No multi-factor authentication (MFA). Easy for attackers to steal, sell, reuse.

Appendix 3 - Access Control Compliance Across Global Regulations: Legacy vs. MyCena®

This appendix compares how traditional user-managed credential systems versus **MyCena® ML-DAES** align with key access control requirements across **global cybersecurity regulations**. This table serves as a practical tool for CISOs, auditors, and compliance leaders seeking to assess or strengthen their organization's security posture and audit readiness.

Control Area	Regulatory Requirement	Relevant Regulations & Articles (incl. Taiwan FSC)	Legacy Systems Compliance	MyCena® ML-DAES Compliance
User Access Provisioning	Only authorized users should access systems	ISO 27001 A.9.2, DORA Art. 5, NIS2 Art. 21, GDPR Art. 25, MAS TRM 9.1.2, 11.1, LGPD Art. 46, Taiwan FSC §2.2.1.1–2.2.1.3, FCA/PRA, CBEST, GLBA §501(b), APRA CPS 230, HIPAA §164.308(a)(3)	Depends—manual user creation; inconsistent governance.	Automated provisioning via encrypted credential delivery.
Password Complexity	Strong, unique, complex credentials	ISO 27001 A.9.2.1, PCI DSS 8.2.3, NIST SP 800-63, MAS TRM 11.2.2, LGPD Art. 46, LGPD Art. 46, Taiwan FSC §2.2.3.1–2.2.3.2, HIPAA §164.308(a)(5)(ii)(D)	Weak or reused passwords.	Auto-generated, encrypted credentials strong by default.
Access Control Policy	Role-based, policy-driven enforcement	ISO A.9.1, DORA Art. 6, NIS2 Art. 21, CBEST, LGPD Art. 46, FCA/PRA, Taiwan FSC §2.2.1.5, HIPAA §164.312(a)(1)	Partially defined, inconsistently applied.	Policy-driven segmented vaults per role and per system.
Segmentation of Access	Prevent lateral movement, data minimization	ISO A.9.1.2, GDPR Art. 5(1)(c), DORA Art. 9, CBEST, LGPD Art. 46, Taiwan FSC §2.2.1.6, HIPAA §164.308(a)(4)	Flat access structure with lateral risk.	Segmented access zones (Bronze/Silver/Gold).
Least Privilege	Match access to job role	ISO A.9.2.3, GDPR Art. 5(1)(c), DORA Art. 9, LGPD Art. 46, Taiwan FSC §2.2.1.4, GLBA §501(b), HIPAA §164.308(a)(4)	Overprovisioning is common.	Role- and system-based credential assignment.
Joiner-Mover-Leaver	Access updates based on user role changes	ISO A.9.2.6, DORA Art. 8, NIS2 Art. 23, APRA CPS 230, MAS TRM 11.1.2, CBEST, FCA/PRA, GLBA §501(b), APRA CPS 230, LGPD Art. 46,	Manual and slow.	Real-time revocation and provisioning.

		Taiwan FSC §2.2.1.7, HIPAA §164.308(a)(3)		
Credential Storage & Encryption	Passwords must be encrypted and invisible to users	ISO A.10.1, GDPR Art. 32, DORA Art. 6, NIS2 Art. 21, PCI DSS 3.4, MAS TRM 11.2.3, APRA CPS 230, Taiwan FSC §2.2.3.2, LGPD Art. 46, HIPAA §164.312(a)(2)(iv)	Often visible/stored in insecure ways (browsers, docs).	Credentials encrypted and invisible to users.
Authentication Security	Secure login beyond passwords (e.g., MFA, zero-trust)	ISO A.9.4.2, DORA Art. 6, NIST SP 800-63B, PCI DSS 8.3, MAS TRM 11.2.4, GDPR Art. 25, Taiwan FSC §2.2.3.3, LGPD Art. 46, HIPAA §164.312(d)	MFA often limited or bypassable; credentials still user-managed.	Unphishable encrypted access with optional MFA add-on.
Audit Trails for Access	Log all access events for traceability	ISO A.12.4.1, DORA Art. 9, NIS2 Art. 22, FCA/PRA, MAS TRM 11.2.5, GLBA §501(b), Taiwan FSC §2.2.4.1, LGPD Art. 37, Art. 41, HIPAA §164.312(b)	Basic logs; not real-time or complete or audit-ready.	Real-time immutable logs and dashboards.
Third-Party Access Management	Control access by vendors and supply chain	ISO A.15, DORA Art. 6(9), NIS2 Art. 21(3), GLBA §501(b), CBEST, APRA CPS 230, MAS TRM 11.3, Taiwan FSC §2.2.5.1, LGPD Art. 42, HIPAA §164.308(b)(1)	Little third-party visibility or control. Vendor access unmanaged.	Sgemented and encrypted vendor accounts or API access, optional restricted by IP/device.
Access Revocation	Remove access instantly if no longer needed	ISO A.9.2.6, DORA Art. 8, NIS2 Art. 23, GDPR Art. 17, GLBA §501(b), CBEST, Taiwan FSC §2.2.1.7, MAS TRM 11.1.2, LGPD Art. 46, HIPAA §164.308(a)(3)(ii)(C)	Manual, error-prone, slow.	One-click revocation from the console.
Rotation Compliance	Periodic credential rotation	ISO A.9.2.4, NIST SP 800-53 IA-5, PCI DSS 8.2.4, MAS TRM 11.2.2, Taiwan FSC §2.2.3.4, HIPAA §164.308(a)(5)(ii)(C)	Relies on users/admins to remember to rotate.	Fully automated or admin-controlled rotation.
Credential Visibility Risk	Prevent password sharing, reuse, and theft	ISO A.9.4.3, NIS2 Art. 21, GDPR Art. 25, PCI DSS 8.2.5, CBEST, LGPD Art. 46, Taiwan FSC §2.2.3.2, HIPAA §164.312(a)(2)(iv)	Passwords visible to users; prone to reuse and leaks.	Users never see or manage credentials; unsharable and unphishable.

Appendix 4 – MyCena® Countermeasures Against AI-Enabled Threat Vectors

This table outlines how MyCena® defends against AI-driven threats like deepfakes, phishing automation, and credential stuffing. By eliminating visible credentials and enforcing encrypted, segmented access, MyCena® neutralizes emerging attack vectors and ensures future-proof protection.

AI Threat Vector	How It Works	How MyCena® Neutralizes It
Phishing emails, vishing, deepfake, social engineering	Large Language Models (LLMs) can generate personalized, grammatically correct phishing emails at scale, increasing open and click-through rates. AI can impersonate trusted voices via deepfake audio or video to trick employees and help desks into giving up access	Users never see or manage credentials. There's nothing to phish or socially engineer.
Credential theft	Credential Harvesting: AI-enhanced malware can scrape saved credentials from browsers or file systems within seconds of infection.	MyCena® credentials are encrypted, segmented, and stored securely.
Credential stuffing, brute force	Attackers use leaked username-password pairs from past breaches and automate login attempts across multiple platforms, exploiting widespread password reuse.	MyCena® credentials are never reused, guessed, or known. Each access is cryptographically unique.
Lateral movement, privilege escalation	AI bots can map out infrastructure and escalate privileges faster than human responders can react.	Segmentation prevents access propagation across systems, even with a compromised endpoint.

Appendix 5 – Regulatory Best Practices for Access Systems

This table summarizes best practices for secure-by-design compliance to core access control principles required by global regulations like GDPR, DORA, ISO 27001, and HIPAA.

Practice	Description	Benefit
Enforce separation of duties	Prevent users from managing their own credentials (creation, visibility, reset)	Eliminates phishing, credential reuse, and insider threats
Credential invisibility	Ensure credentials are encrypted, segmented, and invisible to end users	Stops infostealers, AI-powered social engineering, and supply chain compromise
Auditability by design	Require credential access logs, segmentation records, and automatic revocation policies	Simplifies enforcement under NIS2, DORA, GDPR, ISO 27001
No browser-stored credentials	Disallow storage of credentials in browsers, apps, spreadsheets, or plaintext	Mitigates malware and third-party endpoint risk

Appendix 6 - Credential Security Impact Pre- vs. Post- MyCena®

The following table illustrates the tangible security and operational improvements organizations can expect when transitioning from traditional, human-managed credentials to MyCena®'s encrypted, invisible access control model. By eliminating password visibility and introducing segmentation, real-time logging, and automated credential management, MyCena® drastically reduces breach exposure, operational burden, and compliance risk—transforming credential security from a liability into a strategic asset.

Control Dimension	Pre-MyCena®	Post-MyCena®	Change Impact
Credential Attack Surface	High (all users and third parties type/store credentials)	Minimal (credentials not typed/stored)	Critical substantial reduction in attack surface
Credential Visibility	Visible to users and attackers	Invisible to users and attackers	Eliminated exposure
Password Sharing	Credentials are visible and shared	Credentials are encrypted and bound to users/systems	Prevents sharing, selling, leaks and other misuse
Password Reset	Frequent resets (50–100/month per 1,000 users)	Near-zero resets (automated delivery)	Saves IT time and costs attached to resets. Improves labour uptime and productivity.
Access Segmentation	Flat access—no separation by role or function	Sensitivity-based zones (Bronze, Silver, Gold) and access air-gapped	Lateral movement blocked.
Multi-Factor Authentication	After password is phished, MFA is easy to find (online tutorials)	Added on top of MyCena® for even greater security	Stronger defence
Credential Revocation Speed	Manual via ticket (hours/days)	Instant (real-time deactivation)	Rapid response to threats
Audit & Monitoring Capability	Limited access logs and delayed insights	Real-time access logs + dashboards	Enables fast, accurate auditing, instant insight
Phishing Protection	Low—Users can be tricked	High—Users don't know credentials so can't be phished	Prevents credential-based attacks (over 90% of all breaches)
Risk of Credential Breach	High (4–6% chance annually) — #1 breach vector	Close to zero	Lowers overall breach probability substantially
Incident Response Time	3–5 days on average	Under 24 hours with visibility and control	Faster containment and recovery

Appendix 7 – PIMFA WealthTech Tech Sprint Findings

WHY CYBER SECURITY?

In the face of ever increasing sophistication of financial criminals and the cost it brings to customers and firms alike, this topic was chosen as the statistics surrounding it are genuinely alarming, with latest research showing that the number of cyber-attacks rising by over 200% since the pandemic and, on average, the cost of cybercrime to financial services is 40% higher than other industries. The average cost of a data breach stands at $5.9M against a global average of $4.45M *.

Apart from cost, the consequences of service disruption and reputational damage following an attack can be severe and the effect on clients can, in some cases, be devastating.

THE PROBLEM STATEMENT

Fintechs that participated in this tech sprint were asked to answer the following problem statement:

"How can a specialist cyber security Fintech provide unique and additional value to support wealth managers in preventing, detecting, responding and recovering from cyber security attacks?"

THE FINDINGS

Two Fintech firms were particularly successful and presented their solutions to a panel of members of PIMFA WealthTech and its Advisory Council. Below is a summary of some their key findings and proposed solutions:

MYCENA UNPHISHABLE ACCESS https://mycena.co/pimfa/

Offered a preventative solution that worked to eliminate password-related vulnerabilities as they reported '90% of breaches are caused by criminals stealing login credentials (passwords and two-factor authentication tokens)' and AI-powered phishing and deepfake attacks make it almost impossible for employees to distinguish legitimate requests from fraudulent ones.

Their solution tackles credential-based risks at the root by separating the identity layer (who you are) from the authentication layer (what you're allowed to access):

1. **No Stored or Known Credentials:** their technology generates and distributes encrypted credentials that employees never see or know, removing the risk of password reuse, phishing, and theft.
2. **Multi-Layered Security Model:** technology that applies multiple security layers, ensuring that even if an attacker breaches one level, they cannot access critical systems.
3. **Eliminates Single Point of Failure:** Unlike traditional password managers or SSO solutions, Mycena ensures that each system has unique credentials, preventing an attack on one system from compromising others.