IDEMIA PUBLIC SECURITY

The Strategic Imperative for Security Convergence

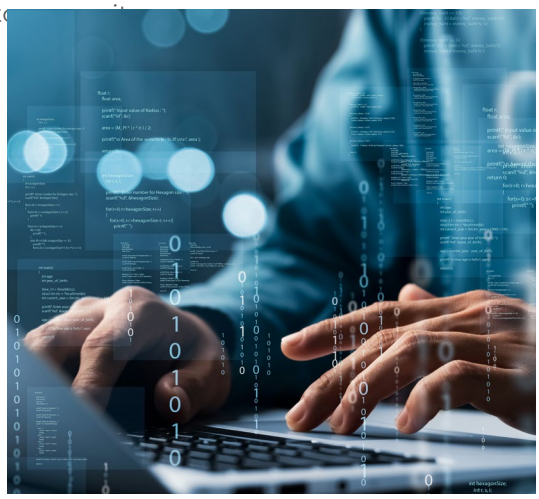
Teresa Wu
VP, Smart Credentials & Access

Invest in the Future with Employee Identity and Access Credentials

In an era of escalating cyber threats, dispersed workforces, and transformative technologies like generative AI (Gen AI), post-quantum computing, and agentic AI, enterprises face unprecedented security challenges. Traditional siloed security approaches are no longer enough. Security convergence—integrating identity, access, and security operations—is critical to building a resilient, adaptive security posture. This white paper argues that the convergence of employee identity and access credentials, including both digital and physical access controls and secure account recovery processes, is foundational to addressing Zero Trust complexities, mitigating threats, and preparing for a post-quantum future.

Imagine a global enterprise where employees access critical systems and secure facilities from home offices, airports, coffee shops, or corporate campuses worldwide. In this context, a single stolen credential can cause chaos: sensitive data is siphoned off in a deepfake phishing attack, an attacker exploits a weak recovery question to hijack an account, or an unauthorized entry compromises a data center, costing millions and eroding trust. This scenario is not fiction; it's a reality for many organizations. Gen AI enables sophisticated phishing, deepfakes, and automated attacks. Darktrace observed a 135% increase in AI-driven social engineering attacks in the first two months of 2023, corresponding with the availability of ChatGPT, and account takeover attacks saw an increase of 28% in 2024 according to Security Boulevard, often exploiting weak recovery mechanisms.[1] **Security convergence, which unifies cybersecurity, physical security, and identity management, offers a path to resilience.**

Enterprises can significantly enhance their security posture by focusing on employee identity and access credentials, fortified by high-assurance identity proofing leveraging advanced technologies like biometrics, liveness detection, and document authentication, or government-issued digitally verifiable credentials like mobile driver licenses (mDLs), along with FIDO2 security keys for phishing-resistant authentication and secure account recovery. Additionally, integrating physical access control systems—such as smart card readers, biometric access control readers, and geofenced entry points—ensures that only authorized personnel access sensitive facilities. Secure recovery processes prevent unauthorized account resets, aligning physical and digital security under a single identity framework. Technology providers who deliver these converged platforms based on industry interoperability standards will lead the $500 billion global cybersecurity market by 2030, as forecasted by Grand View Research. According to Gartner, worldwide end-user spending on information security is projected to total $212 billion in 2025. The adoption of AI and Gen AI continues to drive investments in security markets like application security, data security, privacy, and infrastructure protection. Gen AI will trigger a spike in the cybersecurity resources required t



Source

The Rising Stakes in a Connected World

Every employee's login, physical access attempt, or account recovery request is a potential gateway to identity data compromise and chaos. As cyber and physical access systems intertwine, the workforce becomes part of the attack surface, and malpractice creates vulnerabilities that hybrid attacks exploit with devastating precision. CISA's Cybersecurity and Physical Security Convergence Action Guide warns of "hybrid attacks targeting both physical and cyber assets," a reality underscored by sobering statistics. The 2024 Verizon Data Breach Investigations Report notes that **38% of breaches involved stolen credentials in 2023,** a trend driven by the increase of remote and hybrid work. Enterprise vulnerabilities are exacerbated by weak account recovery processes, such as easily guessed security questions or SMS-based verification, which contributed to account takeover incidents. For example, Scattered Spider is a well-known hacker group that has been active since at least 2022. This collective systematically exploits vulnerabilities and carries out increasingly advanced social engineering attacks targeting the theft of usernames, login credentials, and multifactor authentication (MFA) tokens. The impact of their activities—including lost revenue, disrupted operations, diminished market capitalization, reputational harm, legal expenses, and recovery costs—has reached several billion dollars.

Physical security breaches such as misuse of access cards or stolen badges, accounted for 38% of facility-related incidents in 2023, according to ASIS International, highlighting the need for integrated physical access controls. Security convergence starts with employee identity and access credentials, enhanced by PKI- and FIDO2-based cryptographic technologies and advanced biometric algorithms. It offers a roadmap for security empowerment. By weaving these solutions into a cohesive approach, enterprises and technology providers can shape a secure, resilient future.

Why Start with Employee Identity and Access Credentials? A Human-Centered Story

By starting with employee identity and access credentials, enterprises can enhance their security posture without degrading the employee experience. While friction may be seen as a security measure, excessive friction can incentivize employees to bypass security controls. Identity serves as the anchor for Zero Trust, as emphasized by CISA's Zero Trust Maturity Model (ZTMM), enabling phishing-resistant authentication, least-privilege access, and secure account recovery to protect critical systems and facilities. It supports a global workforce by ensuring seamless, secure access across diverse locations, from bustling offices to remote home setups. Converged identity systems streamline physical access, allowing employees to use a single credential—such as a biometric smart card or digital credentials—for both building entry and system logins, improving efficiency and reducing the risk of lost or stolen badges.

Similarly, secure account recovery processes, using the same high-assurance mechanisms such as biometrics or digital verifiable credentials, prevent unauthorized resets while maintaining user convenience. This can be achieved through self-service recovery portals with multifactor authentication (MFA). Proactively incorporating high-assurance identity proofing during like that offered by IDEMIA at onboarding along with secure recovery mechanisms strengthens this. Converging employee physical and digital access management, along with account recovery, creates a single source of truth, empowering enterprises to protect their people, data, and facilities.

Strengthening the Identity Lifecycle: Technologies That Future-Proof—A Secure Story

Picture an employee joining a global firm, their identity verified not with a digital ID document sent by email but with cutting-edge technologies that ensure trust from day one. Starting with high-assurance identity proofing during onboarding, then leveraging the identity credential in a converged IAM framework, fortifies the identity lifecycle. Robust verification methods, such as biometrics and government-issued IDs, reduce fraud risks tied to 51% of PII compromises from scams like job fraud, as reported by the ITRC in 2025. Biometric technologies, including facial recognition, fingerprints, and iris scans, offer secure verification.[2] For physical access, biometric-enabled smart cards or mobile credentials can be used at entry points equipped with facial recognition or fingerprint scanners, ensuring only verified employees access secure areas like server rooms or executive offices.

Digital document authentication leverages AI and optical character recognition (OCR) to verify government-issued IDs like passports and driver's licenses by analyzing holograms and electronic chips, ensuring authenticity. Cryptographically signed digital IDs, such as mobile driver's licenses (mDLs), secured by cryptographic signatures and biometrics, enhance privacy and reduce fraud. Physical access credentials can be derived from these government-issued digital verifiable credentials, allowing employees to unlock doors or gates via NFC-enabled readers, while seamlessly integrating with digital IAM systems.

For account recovery, mDLs, biometric credentials, or FIDO security keys can authenticate requests, replacing less secure methods like security questions or email links. FIDO passkeys ensure phishing-resistant authentication, while liveness detection prevents deepfake spoofing, and MFA and cryptographic signatures verify identity to reduce account takeovers. These technologies create a unified security strategy by integrating identity proofing, biometrics, liveness detection, and digital credentials. This supports CISA's emphasis on cyber hygiene and addresses the 53% of identity crimes tied to compromised credentials. It also simplifies access and secure recovery for remote teams through SSO, entitlement verification, and strong authentication, enhancing productivity.

[2] https://www.identity.com/the-growing-importance-of-biometrics-in-digital-identity/

Implementation Roadmap: Writing the Next Chapter

CISA's convergence framework calls for communication, coordination, and collaboration to build a robust security convergence strategy. Enterprises can start by assessing their current state, using CISA's Security Road Map Assessment to identify gaps in identity access management, onboarding processes, physical access control, and account recovery processes. They should strengthen onboarding by implementing deepfake-resistant identity proofing, incorporating biometrics, document authentication, and digital credentials to fortify the identity lifecycle. For account recovery, enterprises should deploy phishing-resistant mechanisms, such as biometric-based MFA or verifiable digital credentials recovery portals, to prevent unauthorized account takeovers. For physical access, enterprises should deploy integrated systems like biometric access control readers and video analytics technologies to secure facilities, linking these to the IAM platform used for digital access and account recovery.[3] [4]

The stakes are higher than ever, and security convergence offers a path forward to resilience. By integrating identity management systems for physical access controls with those governing access permissions for systems and data to use a common credential, enterprises can protect both their digital and physical assets under a unified framework. **Convergence of security systems is no longer optional—it's a strategic imperative.** A unified identity framework, powered by industry-leading technologies, lays the foundation for a resilient, agile, and future-ready security posture. In a world where AI-driven threats, fast-looming post-quantum risks, and hybrid attacks are evolving by the day, enterprises cannot afford to delay. By embracing converged security solutions based on interoperable security standards, organizations can transform vulnerabilities into strengths, ensuring trust and resilience across all enterprise operations.

Further reading:

- Cybersecurity and Physical Security Convergence Action Guide | CISA
- SIA-Security-Convergence-2024.pdf
- ASIS-Access-Control-Research-Report.pdf
- Cyber Security Market Size to Garner $500.70 Billion by 2030 at CAGR 12.9% - Grand View Research, Inc.
- Gartner Forecasts Global Information Security Spending to Grow 15% in 2025
- 2024 Cloud Security Report: Unveiling the Latest Trends in Cloud Security - Cybersecurity Insiders
- 2024 Verizon DBIR: Credential Compromise Dominates
- An identity security crisis looms in the age of agentic AI | SC Media
- Preparing Security Defenses For the AI Cyber Attack Era
- Novel social engineering attacks soar 135% amid uptake of generative AI | IT Pro

[3] https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
[4] https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

About IDEMIA

IDEMIA Public Security, a division of IDEMIA Group, is a global leader in trusted biometric-based solutions to both public and private sectors. Drawing on decades of expertise in biometrics and cryptography, and built using a privacy-first approach, our solutions revolutionize public security, identity, travel and transport, and access control. Our iris, fingerprint, and facial recognition solutions top independent benchmarking for accuracy, fairness, and scalability, allowing our clients to build safer, fairer societies.

IDEMIA PUBLIC SECURITY

NA.IDEMIA.COM