Infographics

Data Security in the Age of AI: Is It Truly Safe? Countering Insider Threats with Zero Trust and Integrated Security Solutions

Approx. USD 3.3 Million

Average Cost of a Data Breach in Korea

80%

of Leaks
Caused by Current or Former Employees

About UNION biometrics

UNION biometrics is a global leader in biometric security, delivering comprehensive, high-performance access control solutions and premium multi-modal recognition devices built on proprietary technologies and patented anti-spoofing methods, protecting critical infrastructure, corporate, and government facilities worldwide through a trusted global partner network.

1. Introduction

A Realized Threat, Data Security Collapse by AI and Insiders

As data breach incidents utilizing AI become a reality, AI has emerged as a tangible security threat, no longer a mere possibility. The 2024 deepfake video conference scam in Hong Kong (approx. $25.6 million in damages) is a prime example proving this risk. Sophisticatedly manipulated AI voices and deepfake video calls have surfaced as a new key attack vector, deceiving the weakest link in existing security systems: **the 'Trusted Insider', to access core corporate data.**

Many companies have implemented 'Network Segmentation' to protect data, but this is optimized under the premise of blocking 'external threats infiltrating the network.' According to the National Industrial Security Center (NCISE), **approx. 80% of domestic technology/secret leaks are caused by current or former employees.** Furthermore, the Ponemon Institute reports that 56% of these insider threats stem from 'negligence' or 'mistakes' rather than malicious intent. This implies that network segmentation environments inherently contain a fundamental vulnerability to AI-based social engineering attacks, lacking a strong identity authentication mechanism to verify the actions of 'trusted insiders' (whether malicious or unintentional).

According to IBM's 2023 report, the average **cost of a data breach for a Korean company reaches 3.3 Million USD.** This should be interpreted not as a simple technical error, but as a policy warning signifying the severe 'Structural Security Debt' that can be caused by strategies relying solely on existing information security solutions, including network segmentation.

2. Background

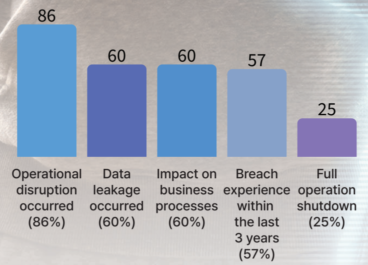
The Illusion of a 'Robust System' and the Scope of Threats

As data-centric infrastructure becomes commonplace, the traditional 'perimeter-based security' model is revealing its limitations. Threats do not distinguish between outside and inside. According to Trend Micro, **57% of healthcare organizations have experienced a ransomware attack within the last three years,** with 25% suffering damage severe enough to halt operations. As external attacks targeting social infrastructure like governments and hospitals increase, the outdated belief that "the internal network is safe" is crumbling in the face of actual insider incidents.
In particular, **the 525% surge in personal information breaches at public institutions over the last five years** (from 8 cases in 2019 to 41 in 2023) highlights the need to analyze the pathways by which network segmentation is neutralized by insider threats.

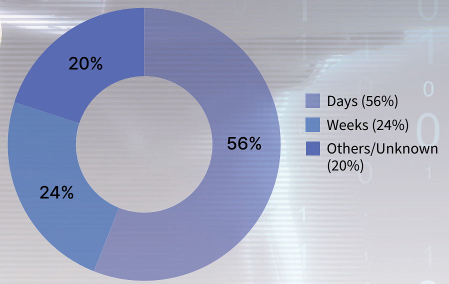
- **[Type 1]** Malicious Insiders and Abuse of Privilege (2013 Snowden NSA Incident / 2023 Tesla Incident)
Cases where high-privilege insiders, such as system administrators, intentionally leak data. Snowden used his colleagues' IDs and passwords, and in the 2023 Tesla incident, former employees violated internal policies to exfiltrate 100GB of confidential data.
- **[Type 2]** Negligence and Contractor Risk (2014 Korean Card Company Data Breach)
Insider 'negligence' or 'mistakes' (the 56% mentioned in the introduction) are as fatal as malicious intent. The 2014 card company breach is a representative case where, despite a network-segmented environment, a dispatched contractor's employee leaked over 100 million customer records via a physical medium (USB). This demonstrated that failures in physical access control and media control can neutralize network segmentation.
- **[Type 3]** Collapse of Physical/Logical Junctions (2016 Ministry of Defense DIDC Hack / 2024 'GoldenJackal' APT) Even in a network-segmented environment, 'junctions' between the two networks, such as vaccine or patch servers, exist. The 2016 Ministry of Defense hack exploited this junction to infiltrate the internal operations network. In 2024, the 'GoldenJackal' APT group attacked air-gapped environments via malicious USBs.

Traditional information security strategies, including the implementation of network segmentation, cannot simultaneously respond to such sophisticated external attacks and complex insider threats. This creates a severe security vacuum across finance, manufacturing, public, and defense sectors.

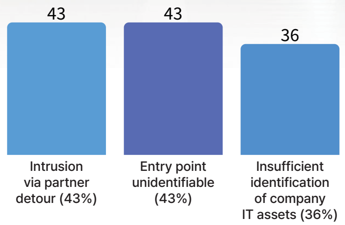
- **Specific Impact of Ransomware Attacks**



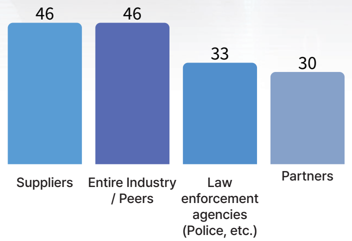
- **Time to Restore Operations**



- **Risk of Detour Attacks via Partners and Unidentified Assets**



- **Targets Not Sharing Threat Information**



출처 : Trend Micro ResearchgQuarter of Healthcare Ransomware Victims Forced to Halt Operations **(Unit: %)**

Technical Response:

The Paradigm Shift to 'Zero Trust'

- **1st Generation: Physical Security**
  Reliance on traditional physical controls like locks and security guards.
- **2nd Generation: Perimeter-Based Security**
  Building 'digital barriers' like firewalls and network segmentation to block external intrusion.
  Limitation: Vulnerable to insider threats as trust is assumed once inside the perimeter.
- **3rd Generation: Zero Trust Architecture**
  The latest security model based on the principle of "Never Trust, Always Verify."
  Continuously verifies all access regardless of internal or external origin.

3. Technical Response

The Paradigm Shift to 'Zero Trust'

In response to the evolution of threats, the data access security paradigm is also shifting from the 'Castle-and-Moat' model to the **'Zero Trust' model**.

• 1st Gen (Physical Security): Traditional physical controls like locks and guards.
• 2nd Gen (Perimeter-Based Security): Building a 'digital moat' to separate outside and inside, using firewalls, IPS, etc. Network segmentation falls into this category. The fundamental limitation of this model is that once inside the perimeter (login successful), the user is 'trusted'. The global physical security market is projected to reach $196.7 billion by 2032, but this 2nd-gen approach alone cannot stop insider threats.
• 3rd Gen (Zero Trust Architecture): The principle is "Never Trust, Always Verify." This is a paradigm that does not distinguish between internal and external, but rather repeatedly and continuously verifies the user's identity, device safety, access location, and the appropriateness of the request at every moment of data access.

At a time when AI can steal insider IDs or deceive users with sophisticated deepfakes, the core of security must shift from 'network separation' to 'trusted user authentication'.

4. Technology Reliability Verification

UNION biometric's Integrated Access Control (UBio-Connect ezPass)

The 'Zero Trust' architecture is based on the principle of "Never Trust, Always Verify." UNION biometric provides the server-based integrated biometric authentication solution, UBio-Connect ezPass, which strongly supports the most fundamental elements of 'Identity' and 'Authentication' required when building such a Zero Trust environment, thereby complementing the structural vulnerabilities of network segmentation.
UBio-Connect ezPass is not just a simple one-time login; it effectively supports the Zero Trust principle of 'Continuous Verification' throughout the entire process of system access, fundamentally managing insider threats.

Core Function 1: Facial Recognition-Based Login and History Management (Supporting the 'Always Verify' Principle)
Traditional ID/Password methods are extremely vulnerable to theft (e.g., the Snowden case). UBio-Connect ezPass reinforces the core Zero Trust principle of 'Always Verify' not with static passwords, but with dynamic biometric information (face) verified with Anti-spoofing (PAD - Presentation Attack Detection). This verifies that The Right Person is accessing the system and ensures a strong Audit Trail by storing all login histories with biometric information.

Core Function 2: Blocking Multiple User Logins and Preventing Account Sharing (Supporting the 'Least Privilege' Principle)
The 'Principle of Least Privilege' is another pillar of Zero Trust. UBio-Connect ezPass blocks simultaneous access from multiple terminals with one account (account sharing) or access by unauthorized users at the system level. This is a core function that realizes the Zero Trust principle of least privilege, controlling unauthorized actions by internal staff or contractors.

Core Function 3: Physical-Logical Security Convergence (Enhancing 'Context-Aware Access')
UBio-Connect ezPass can be integrated with **physical access control (UNION biometric's UBio-X Series)** for data centers or server rooms. Zero Trust emphasizes 'Context-Awareness.' Cross-verifying whether the "person who physically entered the space" and the "person who logically logged into the server" are the same identity implements a powerful context-aware security policy, providing a dual layer of protection against physical media threats, such as those seen in the 2014 card company breach.
The integration of these technologies provides a strong security foundation that simultaneously maximizes the two key security indicators required in **high-risk environments: Access Assurance and Data Integrity.**

- **UBio-Connect ezPass**
  UBio-Connect ezPass is a server-based biometric solution that fundamentally blocks unauthorized access and data loss through single face authentication PC login and integration with existing access controls, establishing a powerful and reliable security system.

Attendance Dashboard
Provides a dashboard for intuitive and easy tracking of attendance status, divided into total users, working hours, and location

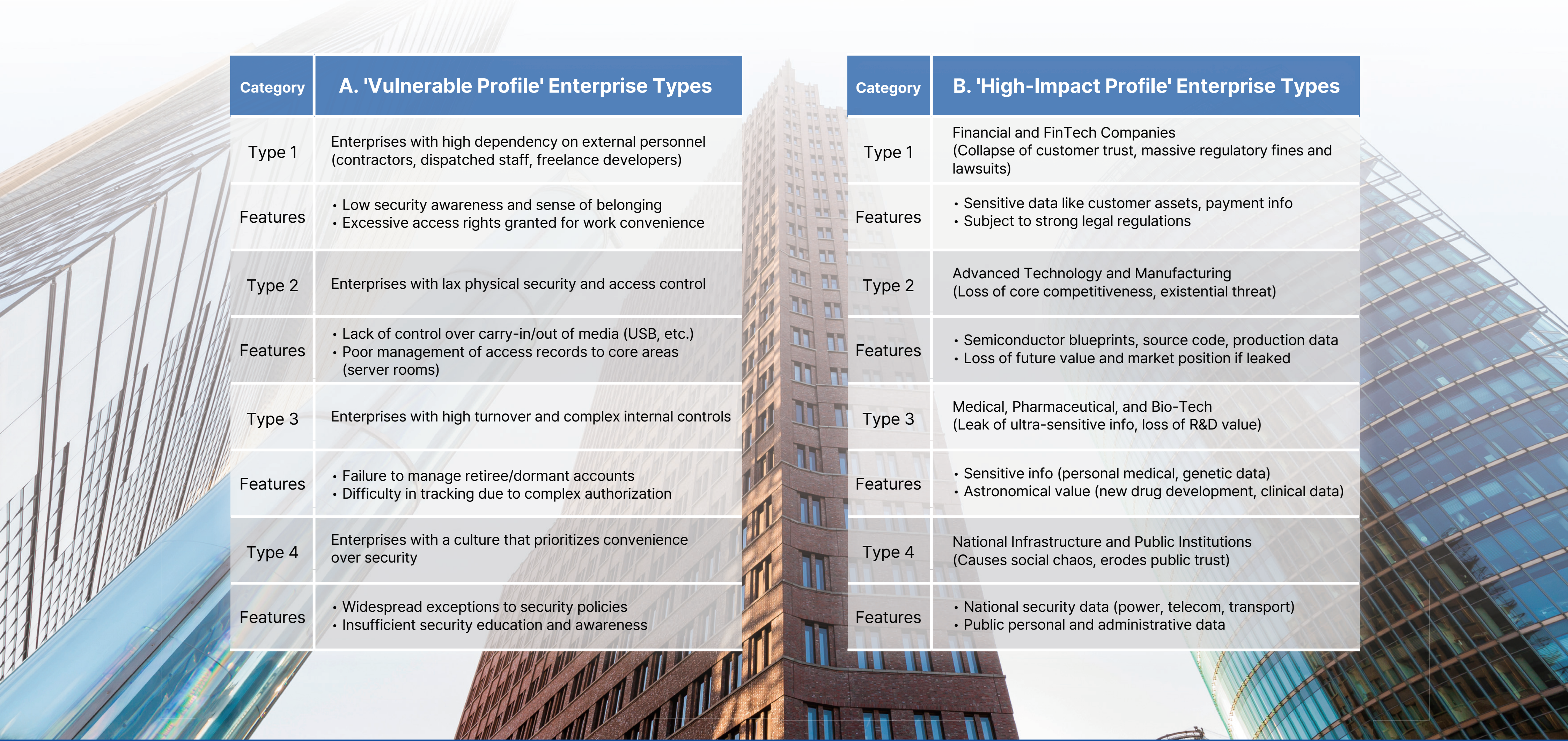
Face Recognition Biometric Solution
Prevents data and personal information leaks by eliminating the need for passwords through face authentication

Decentralized Biometric Data Storage
Stores user biometric data with automatic encryption algorithm updates for enhancing data security

Unauthorized Access Prevention
Real-time face analysis and automatic PC lock on unauthorized detection to prevent data exposure

5. Enterprise Security Self-Diagnosis

If your company falls into both Type A and Type B below (e.g., a financial institution with high reliance on external developers, or an advanced technology company with poor retiree account management), a data breach is not just an accident, but a 'predictable disaster'.



Category	A. 'Vulnerable Profile' Enterprise Types
Type 1	Enterprises with high dependency on external personnel (contractors, dispatched staff, freelance developers)
Features	• Low security awareness and sense of belonging • Excessive access rights granted for work convenience
Type 2	Enterprises with lax physical security and access control
Features	• Lack of control over carry-in/out of media (USB, etc.) • Poor management of access records to core areas (server rooms)
Type 3	Enterprises with high turnover and complex internal controls
Features	• Failure to manage retiree/dormant accounts • Difficulty in tracking due to complex authorization
Type 4	Enterprises with a culture that prioritizes convenience over security
Features	• Widespread exceptions to security policies • Insufficient security education and awareness

Category	B. 'High-Impact Profile' Enterprise Types
Type 1	Financial and FinTech Companies (Collapse of customer trust, massive regulatory fines and lawsuits)
Features	• Sensitive data like customer assets, payment info • Subject to strong legal regulations
Type 2	Advanced Technology and Manufacturing (Loss of core competitiveness, existential threat)
Features	• Semiconductor blueprints, source code, production data • Loss of future value and market position if leaked
Type 3	Medical, Pharmaceutical, and Bio-Tech (Leak of ultra-sensitive info, loss of R&D value)
Features	• Sensitive info (personal medical, genetic data) • Astronomical value (new drug development, clinical data)
Type 4	National Infrastructure and Public Institutions (Causes social chaos, erodes public trust)
Features	• National security data (power, telecom, transport) • Public personal and administrative data

6. Conclusion and Policy Recommendations: The End of 'Network Trust' and the Shift to 'Identity Verification'

As explained in the background, the complex combined threats from AI and insiders demonstrate just how significant a 'Structural Security Debt' the reliance on 'network segmentation alone' has been.

The common thread shown by the major security incidents reviewed earlier is clear. Every incident occurred when the weakest link—named the 'trusted perimeter' or 'authorized insider'—collapsed. In a reality where AI mimics users' faces and voices (the threat) and insiders make mistakes or act maliciously (the vector), a static defense wall like 'network separation' can no longer serve as the core solution.

The security paradigm must shift to a Zero Trust model, assuming an 'Untrusted Network' and continuously verifying the 'Identity' that accesses data.

Union Biometric's UBio-Connect ezPass is the most practical technology to meet these timely demands, implementing the core principles of Zero Trust (Always Verify, Context-Aware) through anti-spoofing biometric authentication and physical-logical security convergence. It compensates for the fundamental vulnerabilities of network segmentation by not relying on the nominal trust of an 'authorized user,' but by verifying 'The Right Person' in real-time.

References

- CNN, SCMP, etc. (2024). "Hong Kong 'deepfake' scam sees finance worker pay out $25.6 million after video call." (Source for 2024 Hong Kong deepfake scam)
- IBM. (2023). Cost of a Data Breach Report 2023. (Source for 4.53B KRW avg. breach cost / 108-day reduction with security AI)
- Ponemon Institute. (2023). 2023 Cost of Insider Threats Global Report. (Source for 56% of insider threats being non-malicious)
- NCISE (National Industrial Security Center) & Police Industrial Technology Leak Investigation Unit Statistics. (Source for 80% of domestic leaks by insiders)
- Trend Micro. (2022). "Quarter of Healthcare Ransomware Victims Forced to Halt Operations." (Source for 57% ransomware experience, 25% operation halt)
- CatchSecu. (2024). "How many personal information breaches occurred in public institutions in H1 2024?" (Source for 525% increase in public institution breaches)
- Fortune Business Insights. (2024). "Physical Security Market Size, Share | Industry Trends [2023]." (Source for $196.7B physical security market projection)
- The Guardian. (2023). "Report: 'massive' Tesla leak reveals data breaches, thousands of safety complaints." (Source for 2023 Tesla 100GB data leak)
- ESET. (2024). "Mind the (air) gap: GoldenJackal gooses government guardrails." (Source for GoldenJackal APT attacking air-gapped networks via USB)
- BoanNews, Yonhap News, etc. (2014-2016). (Sources for 2014 card company breach / 2016 Ministry of Defense DIDC hack)

Policy Recommendations: Mandating Standards in High-Risk Environments

1. **Adopt Zero Trust-Based Integrated Identity Authentication (UBio ezPass)**

   To counter AI and insider threats, mandate user identity verification (Always Verify) based on anti-spoofing biometrics (face), not simple ID/PW, when accessing the 'internal network' of a segmented environment.

2. **Implement Physical-Logical Security Linkage (Context-Aware)**

   Strengthen 'Context-Aware' security by building a cross-verification system (e.g., UBio-Connect ezPass + UBio-X Face) between physical entrants to core areas (data centers, server rooms) and logical system users.

3. **Transition to a Zero Trust Architecture**

   Discard the 2nd-gen perimeter security assumption that "the internal network is safe." Apply the 'Principle of Least Privilege' to all access and establish a continuous monitoring and audit system.