

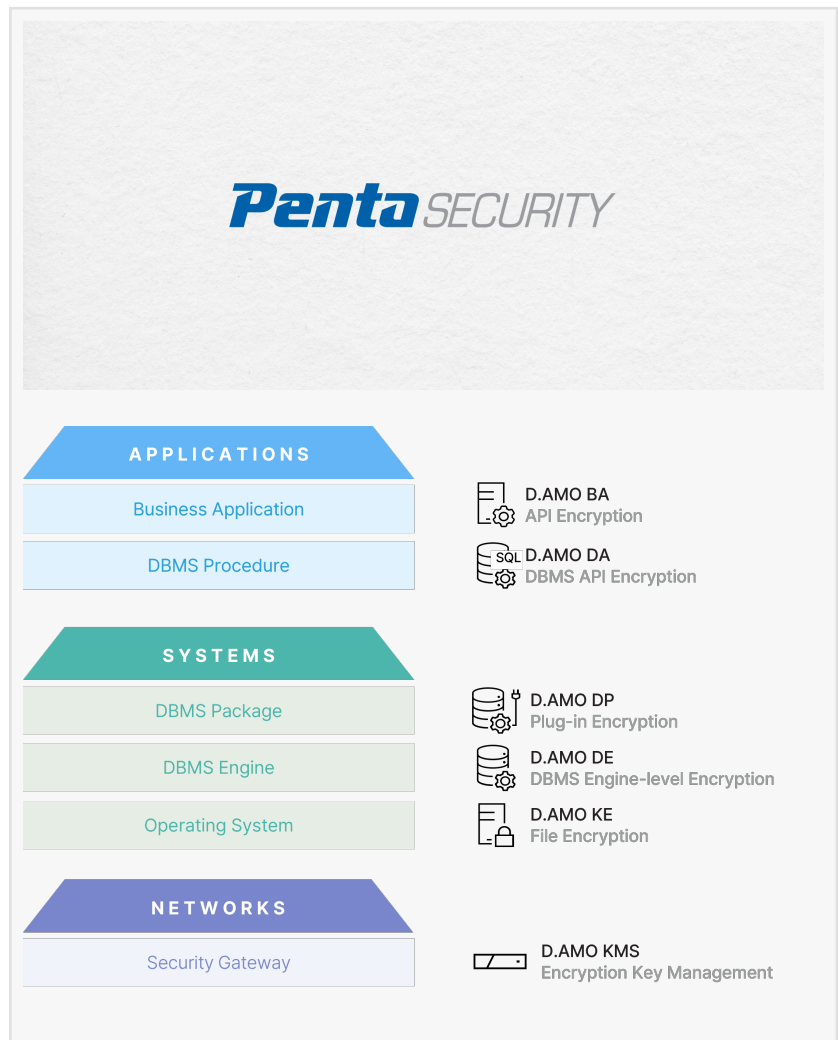
Data Breach Response: Management Adopts Encryption

SEOUL, SOUTH KOREA, November 28, 2025 /EINPresswire.com/ -- The year 2025 has seen a wave of high-profile security breaches, reinforcing the urgent need for robust cybersecurity strategies across industries.

In March, the personal data of 3 million applicants dating back to 1999 was stolen from the State University of New York. By August, sensitive business account information was leaked from Google, and in September, [FinWise Bank](#) suffered a breach compromising financial data of approximately 700,000 customers, resulting in significant reputational damage. IBM reported that the average cost of a data breach in the U.S. reached an all-time high of \$10.22 million in 2024. Cyber threats have clearly evolved into a critical business risk, affecting every sector without exception.

Most recent attacks bypass traditional defenses such as firewalls, antivirus programs, and EDR systems, directly targeting the data itself. Once an organization's core assets are exposed, the consequences can escalate rapidly and unpredictably. In this increasingly volatile environment, encryption has emerged as an essential technology. Even if a breach occurs, encryption neutralizes the value of the stolen data, acting as the last line of defense. According to security research institutions, companies that implement encryption can reduce their breach-related costs by an average of \$237,000.

There are many proven cases demonstrating the business value of encryption. A global electronic component manufacturer recently experienced an insider data breach at one of its overseas plants. However, due to full encryption of its production and design data, the incident



resulted in zero actual damage. The cost of investigation was reduced by approximately 70%, and there were no recalls or compensation claims from clients. Similarly, a major Japanese financial institution saw the number of improvement requests from regulators drop by more than half after making encryption a core component of its security framework. These examples show that encryption is more than a technical safeguard—it delivers direct business benefits in compliance, incident response, and brand trust.

Despite these advantages, many companies still perceive encryption as costly or performance-intensive. However, modern encryption engines now use hardware acceleration and intelligent key management to minimize performance impact to around 3%. Global cloud providers increasingly emphasize the "shared responsibility model" and list encryption as a core security requirement. International regulations such as GDPR, NIST, ISO 27001, and HIPAA all explicitly mandate encryption as a foundational control.

Encryption also plays a decisive role in global market entry. In the U.S., regulations like HIPAA and CCPA mandate encryption in finance and healthcare sectors, effectively making it a prerequisite for market access. Europe, under GDPR, is moving toward a privacy-first security model that requires encryption across all stages of data processing. Japan enforces strict data-centric security expectations in the financial and manufacturing sectors, making it nearly impossible to secure contracts without robust encryption and key management systems. In Southeast Asia, rapid digital transformation is outpacing local security capabilities, leading to growing demand for encryption solutions from overseas providers. [Penta Security](#)'s expansion in Japan and Southeast Asia is a direct response to these global regulatory trends and rising enterprise needs.

As encryption becomes a cornerstone of enterprise security, Penta Security's flagship encryption platform [D.AMO](#) stands at the forefront. Launched in 2004 as Korea's first commercial data encryption solution, D.AMO marks its 21st anniversary this year. It has maintained the highest cumulative procurement share in the domestic market for over 18 years and is now deployed in over 14,000 enterprise systems worldwide. D.AMO protects mission-critical data in sectors such as finance, healthcare, and public services, serving as the ultimate defense line across industries.

In today's threat landscape where data breaches are a constant, encryption is no longer just an IT measure—it is a business imperative that determines organizational sustainability. Since not all attacks can be prevented, companies must build systems that ensure core information remains secure even when breaches occur. In an age where cyber incidents are the norm, only companies that place encryption at the center of their strategy will earn global trust and maintain competitive advantage.

Seo yeon Jung
Penta Security Inc.
+82 2-2125-5629

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/870573401>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.