Penta SECURITY

D.AMO White Paper

Comprehensive Data Encryption Solution

Version 3.7

Planning Group
Plan.plod2@pentasecurity.com
Penta Security Systems, Inc.
Oct 2025

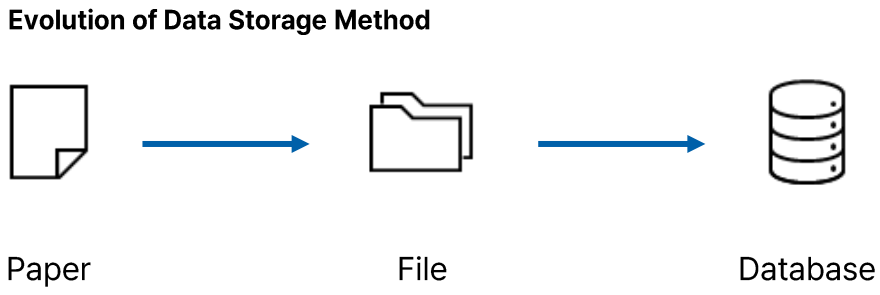
CONTENTS

Introduction

Advancement of Data and Arrival of Database

Historically, information such as personal information, medical records, education, tax, policy were stored in physical paper form. However, with the advance in technology as well as industrial spurt, information storage has changed. With the generalization of computers, the various industrial information stored in physical paper form became available in electronic file formats and systems allowed for safer and faster storage and modification of information.

As the general electronic file storage method developed, the amount of data stored increased drastically. And with the surge, came along inconveniences and inefficiencies including complex structures, search, update, lack of simultaneous control, etc., and to tackle such filing system issues, led to the development of database.



Pic 1. Evolution of Data Storage Method

With the arrival of database, a ‘base of data’, systemic and integrated management of data and storage of data en masse became possible. Insofar enabling analyzing and processing of massive information and organic integration of data to formulate meaningful information with ease.

The diversity of data stored in database also started to increase, from structured data like texts and numbers with predefined rules to unstructured data such as images, videos, audio, documents, biological data. With the wider array of data types being stored in a database, companies are now capable of providing quality service by adequately utilizing the stored data befitting the purpose.

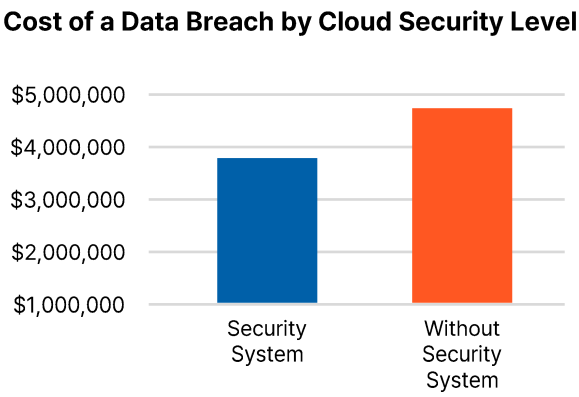
Although the advance in database led to the increase of commercial value of corporate information, it has attracted hackers to utilize various methods to threaten to exfiltrate key information from corporate databases. In fact, the information breaches and damages caused by hacking are constantly increasing. As such, many countries have introduced regulations to prevent corporate information breaches, and yet, many are still not fully aware of the need for data security.

Perceptions on Data Security

Enterprises consider databases secure against a hacker's threat as the databases are typically run in a closed environment, with no direct connection to the internet. Yet, contrary to this complacent perception, enterprise data security can easily be breached through various hacking methods. For instance, there are attack methods such as underhandedly installing a 'malware' in the PC of an administrator with database access, or 'SQL injection' that transmits queries to trigger database malfunction thus accessing the data.

Data security perception on cloud environments also have a long way to go. Despite the generalization of cloud transition in business environment for most enterprises, the regulations and security surrounding the cloud environment is yet to be systemized, indicating a higher likelihood of data being breached compared to on-premise environments.

IBM Security's Cost of a Data Breach Report 2022 conducted against approximately 500 global enterprises and organizations show that 45% of the enterprises currently employing cloud environment has suffered data breaches, and the difference in cost of a data breach between the organizations with cloud security system and organizations without was almost 700 thousand dollars.



Pic 2. Cost of a Data Breach by Cloud Security Level

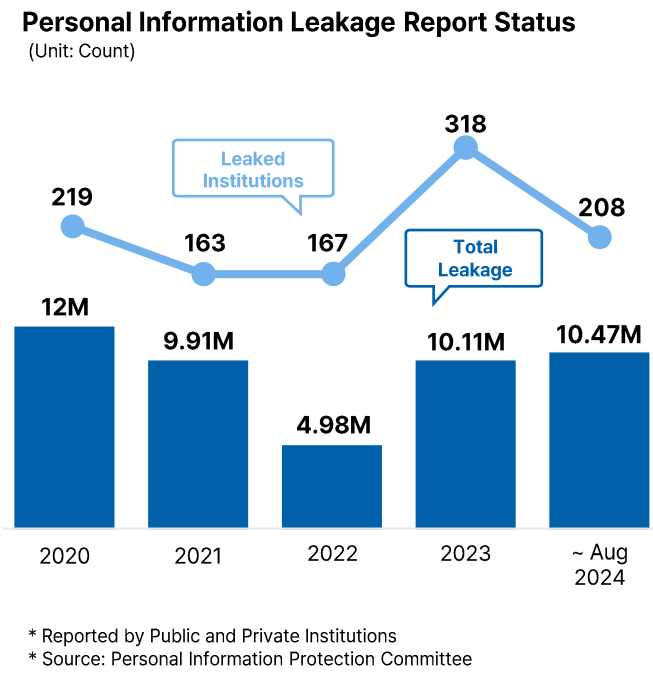
Along with the drastic corporate business environment changes, damage caused by data breaches is higher than ever. Such outcome is an indication of the unpreparedness in terms of security perception and systems amid the fast-changing business environment in many companies.

The recent Covid-19 pandemic forcing various companies to work remotely has led to companies experiencing the weakened corporate security and the dangers of increased cyber attacks.

According to the 2021 Global Information Security Survey (GISS), carried out against a thousand cyber security leaders, including Chief Information Security Officers (CISO) around the world, 56% responded that the new working environments, such as work-from-home and flexible working conditions, have led to weaker cyber security. Additionally, almost 77% responded that threatening cyber attacks increased compared to the previous year while 43% were highly concerned of cyber attack countermeasures since the increase in remote working. Despite the changing environment leading to the increase in an individual's perception of data security threats and the need for data security, many companies are yet to establish practical security systems. Therefore, companies need to take proactive measures, including strengthening security policies and implementing adequate security solutions for the new working environment.

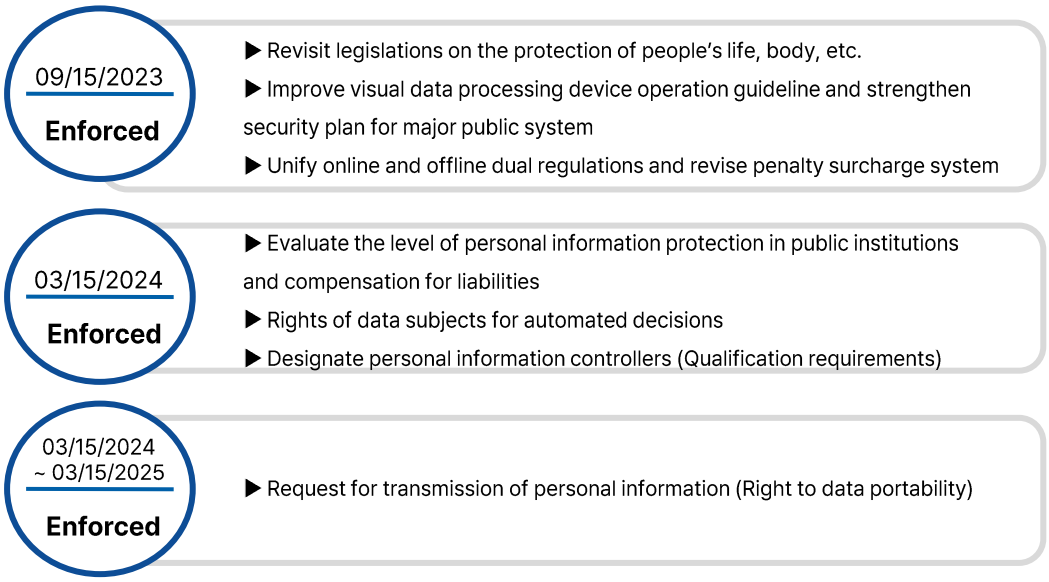
Regulatory Compliance on Data Protection (S. Korea)

As of August 2024, 10.47 million cases of personal information leakage were reported. A total of 208 institutions has experienced leakage as of August 2024 indicating a massive surge despite being just over half a year in comparison to the previous year's 318 institutions reporting a leak for the whole year.



Pic 3. Personal Information Leakage Report Status

Following the massive increase in personal information leakages, South Korea's Personal Information Protection Committee (PIPC) has revised the Personal Information Protection Act (PIPA) to reinforce a company's personal information protection accountability.



Pic 4. Revised Personal Information Protection Act, March 2024

The previously imposed penalty surcharge 'not exceeding 3/100 of the total revenues relating to the concerned violation' was revised to 'not exceeding 3/100 of the total sales,' and the exclusion of the total revenue unrelated to the violation. However, with the burden of proof placed on the companies, the revision implicates heavier penalty surcharges imposed for PIPA violations.

Additionally, the ‘Standards for Measures to Ensure Safety of Personal Information’ has been enforced on September 22, 2023.
The regulation aims to set the minimum for the technical, managerial, and physical safety standards necessary to ensure the safety of personal information. The fact that such regulations are consistently revised or put into effect is to be perceived as emphases on the need for secure data encryption and the importance of access management.

Article 4(1). Establishment and Implementation of Internal Management Plan

Establish an internal management plan for the safekeeping of personal information through internal decision process.

(Exempted for micro enterprises or individuals and organizations that process less than 10,000 data subjects)

Article 7. Encryption of Personal Information

Safe encryption algorithm must be used to encrypt authentication information such as passwords, or biometric information when storing or transmitting or receiving through information and communications networks.

(One-way encryption for passwords to prevent decryption)

Article 5. Management of Access Authority

Grant differentiated access authority to the personal information depending on the minimum requirement to do the work. Securely apply and manage authentication means of data subjects.

Article 8. Preservation and Inspection of Access Records

Access records are to be stored and managed for the minimum period of a year. Inspection on personal information access records is to be carried out at least once a month.

Measures are to be taken to safely store the access records.

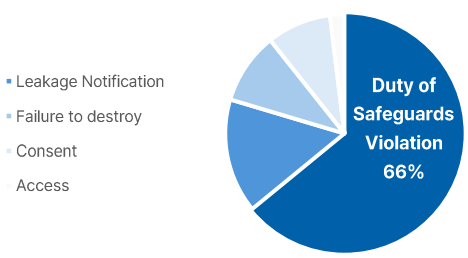
Pic 5. Standards for Measures to Ensure Safety of Personal Information, Sep. 2023

Legislations on personal information leakage are strengthened and yet, why is the number of personal information leakages increasing each year?

According to a Korea Internet & Security Agency (KISA) research, 66% of PIPA violations were failing to observe the ‘Duty of Safeguards.’ Violations were observed in the order of ‘encryption when transmitting·storing (25%)’, ‘retaining·inspecting access records (22%)’, ‘prevention measures against disclosure and leakage (19%)’, and ‘access authority management (15%).’

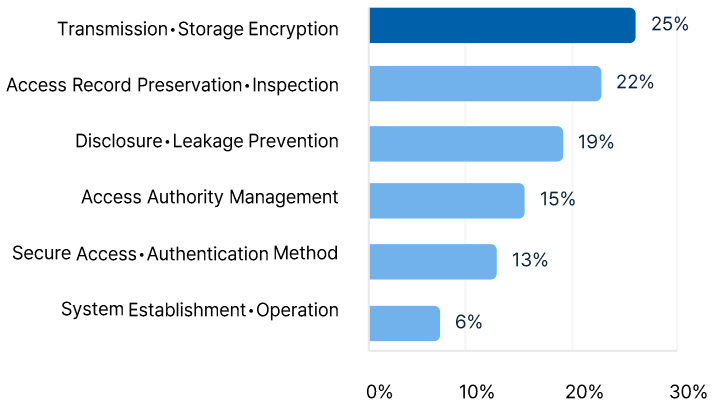
The common denominator for these violations is the lack of essential protection measures required for personal information protection, which is an indication of lack of encryption system and unresolved access management.

PIPA Violation Criteria



* Source: KISA

Types of Duty of Safeguards Violations

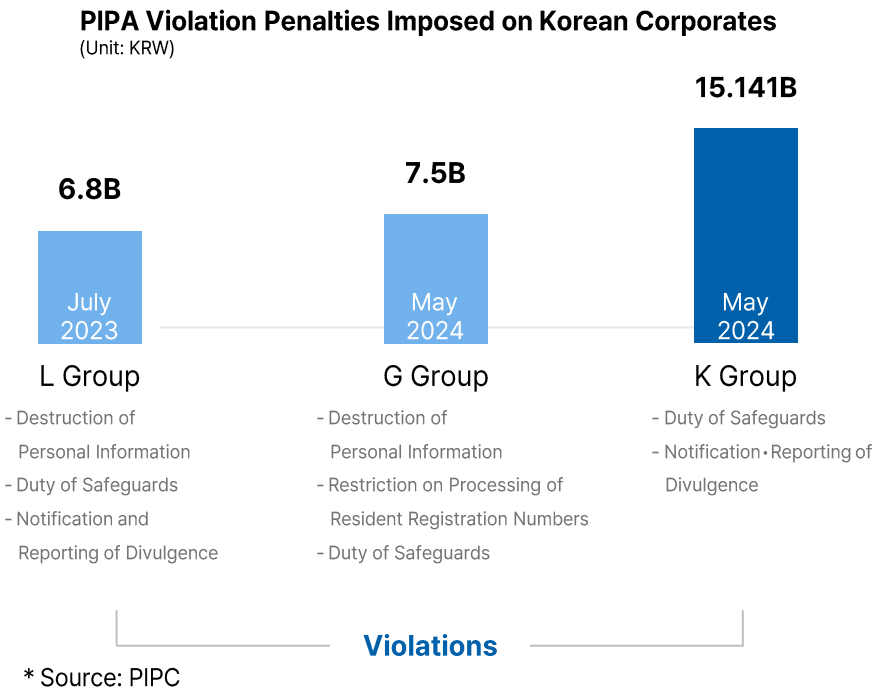


* Source: KISA

Pic 6. PIPA and Duty of Safeguard Violations by Type

The penalty surcharge or administrative fine is imposed on all PIPA violations, and they are not limited to a handful of companies.

In 2023, Korea's largest global mobile instant messenger service provider K Group was imposed a KRW 15.141 billion (approx. USD 10.59 million) in penalty surcharge and KRW 7.8 million (approx. USD 5,400) in administrative fine for the suspected violation of PIPA. Not only was it the heaviest sanction to have been imposed on a Korean corporation for the violation of PIPA, having caused significant damages to the users as a minimum of 65,000 items of personal information were leaked.



Pic 7. K Group PIPA Violations and Penalty Surcharge

As evidenced, the penalties for failing to uphold personal information protection have increased, regardless of a company's size, urging Korean corporations to establish personal information protection measures.

Regulatory Compliance on Data Protection (International)

Across the globe, governments and other regulatory agencies have been implementing laws and regulations as countermeasures against data leakage caused by hacking.

> **General Data Protection Regulation** (EU, 2018) GDPR is the EU Personal Information Protection Act, applied universally to all EU nations, which focuses on strengthening the rights of data subjects and corporate accountability. General violations of GDPR result in fines of 2% of global sales or 10M euros ($115M), whichever is higher, and serious violations result in fines of 4% of global sales or 20M euros ($230M), whichever is higher.

> **Sarbanes-Oxley Act** (USA, 2002) increased company responsibilities regarding accounting, auditing, and financial disclosures, as well as maintenance of information pertaining thereto. Similar laws include the European Union's **8th Company Law Directive** and Japan's **Financial Instruments and Exchange Law**. Fines for violations can go as high as $5M, depending on the country and the nature of the violations

Health Insurance Portability and Accountability Act (HIPAA, USA, 1996) HIPAA's Privacy Rule tightly regulates the use and disclosure of medical records, amended in 2009 to include **the Health Information Technology for Economic and Clinical Heath Act** (HITECH Act) which implemented strict new breach control and reporting requirements. Similar laws include the Australian Health Records Act and the European Union's Recommendation on the Protection of Medical Data. Fines for violations of such regulations have reached as high as $4.3M.

Payment Card Industry Data Security Standard (PCI DSS, 2004) is an international information security standard for companies dealing with electronic payment transactions, which requires secure management of cardholder data. Fines for violations can reach as high as $100K per month.

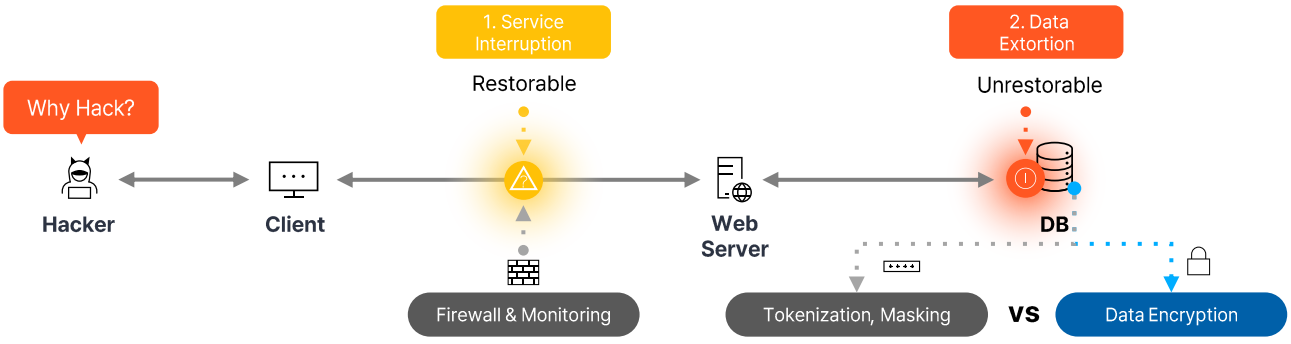
Federal Information Processing Standard (FIPS) is a set of standards required by the United States Federal Government for use in computer systems used by government agencies and contractors. Well known encryption standards include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES).

Other well-known privacy laws in place around the globe are the European Union's **Directive on Data Privacy**, the Japanese **Personal Information Protection Law**, the South Korean **Act on Protection of Personal Data**, and the Australian **Privacy Act**.

Despite these powerful regulations placed by various nations, massive data breaches continue to occur, increasingly underscoring the importance of data security.

Securing Database, Data Encryption

Hacker's Goals and Data Breach Countermeasures



Pic 8. Goals of Hacking

What are the goals of a hack? There are 2 main reasons for hacking.

First is **Service Interruption**. Hackers aim to make financial gains by interrupting a targeted agency or company's normal service operation. A security solution to prevent this from happening would be the use of firewalls. Most service interruption attacks can be restored in a few days, so it is less likely to cause major damage.

The other is **Data Breach**. This is aimed at exfiltrating critical data, such as confidential information, from agencies and companies for financial gain. Unlike the service interruption attack, which can be restored within days, for data to be exfiltrated is that a key asset is physically taken or exposed to the outside, meaning that it is unrecoverable. In other words, the exfiltrated data cannot be physically deleted or destroyed nor can it be retrieved, thereby causing permanent damage. Data exfiltration attacks may lead to secondary damages as the exfiltrated data can be distributed for various means, rather than just hackers keeping the data for themselves.

Not only is the intentional data exfiltration a threat, but inadvertent data breach just as dangerous. Just like data exfiltration attacks, unintentional data breaches share the trait that the data cannot be recovered, and the breached data is more likely to be misused compared to the exfiltrated data. Therefore, not only is it important to prevent data from being breached in the first place, is it crucial to have a data security mechanism in place to prevent hackers from abusing the data even if the data does get breached. And that requires the last line of defense for data, the data encryption.

Data Encryption

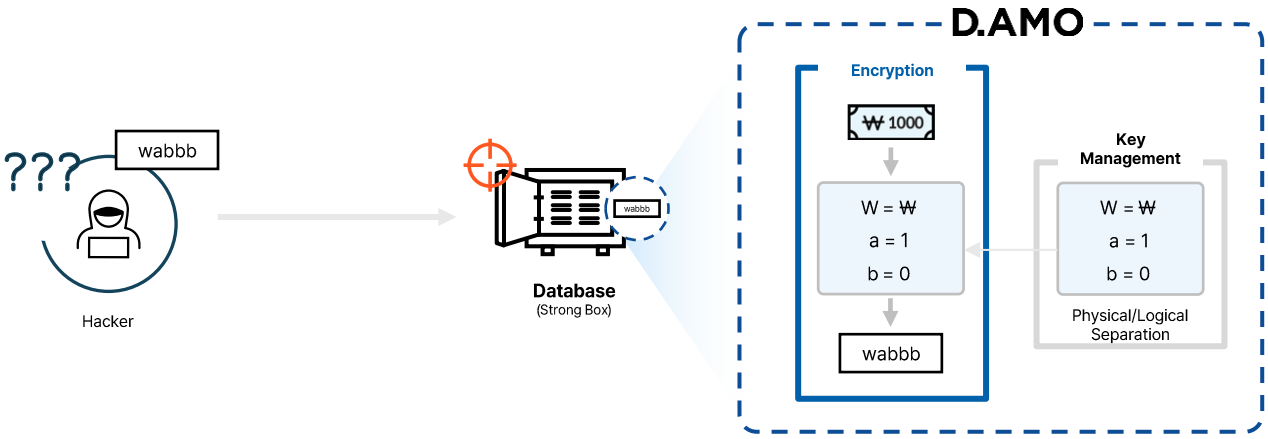
Despite the regulations placed by various nations and organizations, hackers utilize various means to exfiltrate information each year, causing literally billions of dollars in damage per year. Which is why agencies and companies that recognize the importance of data security try to minimize damages by integrating various security solutions such as DRM, DLP, and VDI.

While it would be the ideal to integrate the entire arsenal of security solutions for the sake of data protection, realistically, the cost of building up all the data security solutions would cost too much and even if one chose to do so, the risk of breach will persist.

In addition to the massive sum of money already spent to integrate all the solutions, too many resources would have to be placed to operate the solutions. In the end, it is about minimizing cost whilst retaining the maximum level of security. And to achieve that is with the most basic yet crucial form of security, encryption.

Let's imagine a strong box with cash inside and to protect the money, one has set up CCTVs, security guards, barricades, etc. Despite all these security measures, once a thief somehow gets through them and steals the money, there is nothing to stop the thief from keeping the money.

This time, let's imagine the money in the strong box is encrypted. The encrypted money is worthless unless it is decrypted. Regardless of how much the thief stole, unless the money is decrypted, it is but worthless pieces of paper. As in this scenario, the basic but crucial aspect in data security is data encryption that secures your information even if hackers somehow exfiltrate information.



Pic 9. The Importance of Data Encryption

What then, is encryption? Data encryption refers to randomizing data in critical information using mathematical procedures that render the critical information incomprehensible to a third party. The source data to protect is referred to as Plain Text, and once the encryption algorithm is applied to the plain text, it is then called Cipher Text. Encryption is the process of applying encryption algorithms to plain texts and turning them into cipher texts.

Pic 10. Algorithm-Based Initial Encryption Methods

Depending on where it is integrated and how it functions, data encryption can be divided into API Encryption, Plug-In Encryption, and Kernel Encryption.

The two main methods of encrypting structured data are API encryption and plug-in encryption.

The upside of **API encryption** is that it does not place a load on a DB server as it encrypts and decrypts in the external application area. However, as it requires source modification to perform encryption and is incapable of encrypting data computed inside the DB, it is commonly used in environments that prioritize performance.

For **plug-in encryption**, it requires less modification, encrypts and decrypts from the inside of a DB server, placing a direct load. It is used in environments less sensitive to performance.

Kernel encryption is preferred for the encryption of unstructured data. It encrypts and decrypts files and folders in an OS's kernel level and is used to encrypt logs, images, audio recordings, documents, OCR, etc.

Encryption Method	Build Location	Description
API Encryption	Application Server	Installs encryption modules on the web server as API thereby transmitting queries to a DB server. Requires source modification.
Plug-In Encryption	DB Server	Installs encryption modules in a DB server for encryption. Requires less modifications but places loads on the server.
Kernel Encryption	OS Kernel	Installs encryption modules at an operation system's kernel level to encrypt and decrypt unstructured data.

Table 1. Encryption Methods

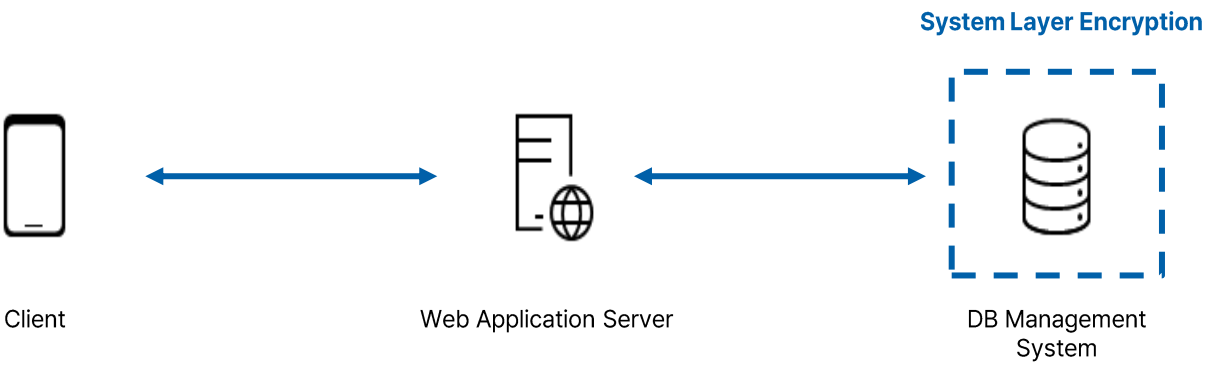
Since the application of the encryption methods, advanced encryption methods have been introduced. Hybrid encryption aims to resolve the downsides of API and plug-in encryption methods by concatenating encryption methods depending on the business type while engine encryption performs encryption from within a database engine. These constantly advancing encryption methods have made it possible to build up optimized encryption solutions that fit a corporate operation environment.

Encryption Method	Build Location	Description
Hybrid Encryption	Application Server, DB Server	Hybrid build that integrates API encryption for environments with heavier emphasis on performance, or plug-in encryption for environments with less emphasis on performance
Engine Encryption	DBMS	Encryption engine implemented inside a DBMS for encryption, not requiring previous APP or DB environments and provides fast encryption

Table 2. Advanced Encryption Methods

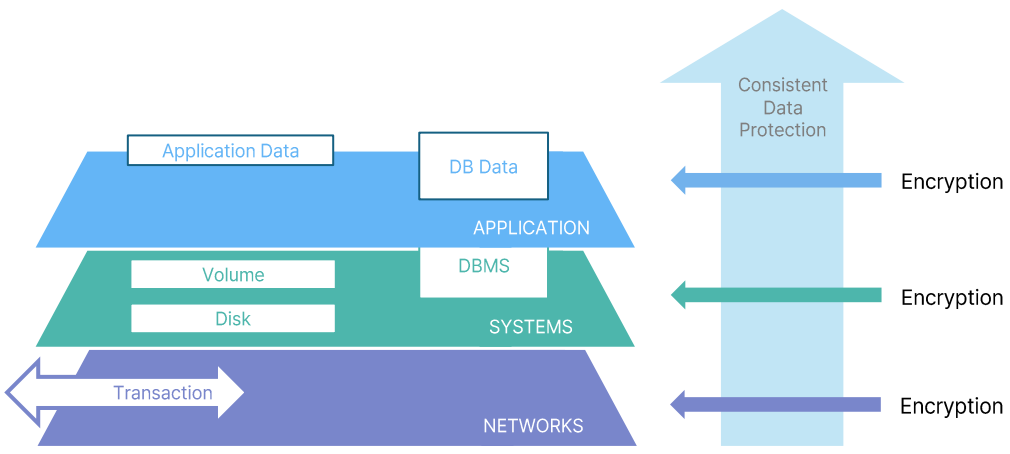
From the traditional encryptions applied at DBMS and application server, the advancement in technology has enabled the use of data encryption solutions designed for specific industries or environments such as POS security, SAP security, unstructured data security, medical information security, and corporate-wide key management.

As the advanced solutions are designed with data characteristics and encryption areas required for the industries in mind, they help greatly with providing strong encryption on all layers and areas of a system.

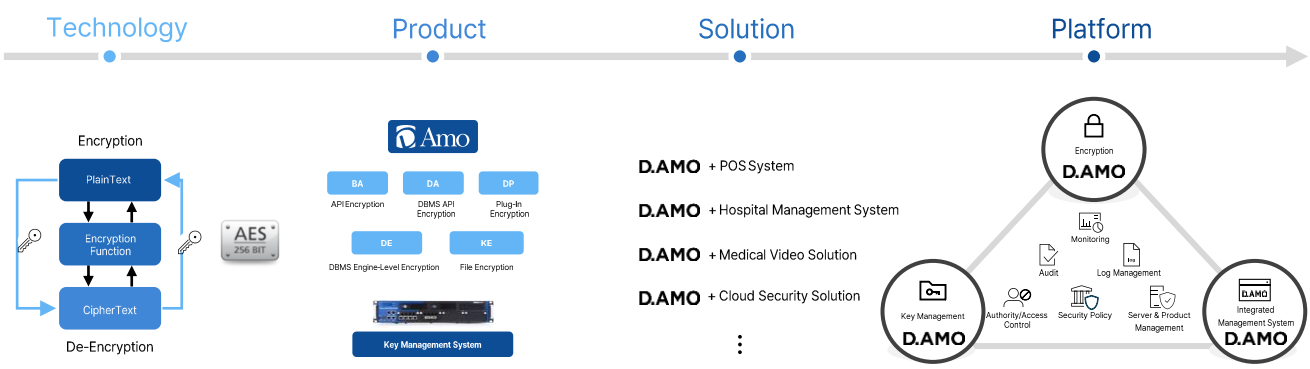


Pic 11. Traditional DB-Centered Encryption Before Platform Encryption

Recently, encryption solutions have evolved from being limited to specific environments or industries into an encryption platform that can be applied regardless of IT systems or environments. By integrating a key management system essential to encryption, and a central management system that oversees numerous data encryption products across the infrastructure, encryption operations can now be conducted in a more secure and efficient environment. To this date, encryption platforms are constantly evolving to keep up with the ever-changing environments and industries.



Pic 12. Structure of Encryption Platform Design Considering System Layer and Area



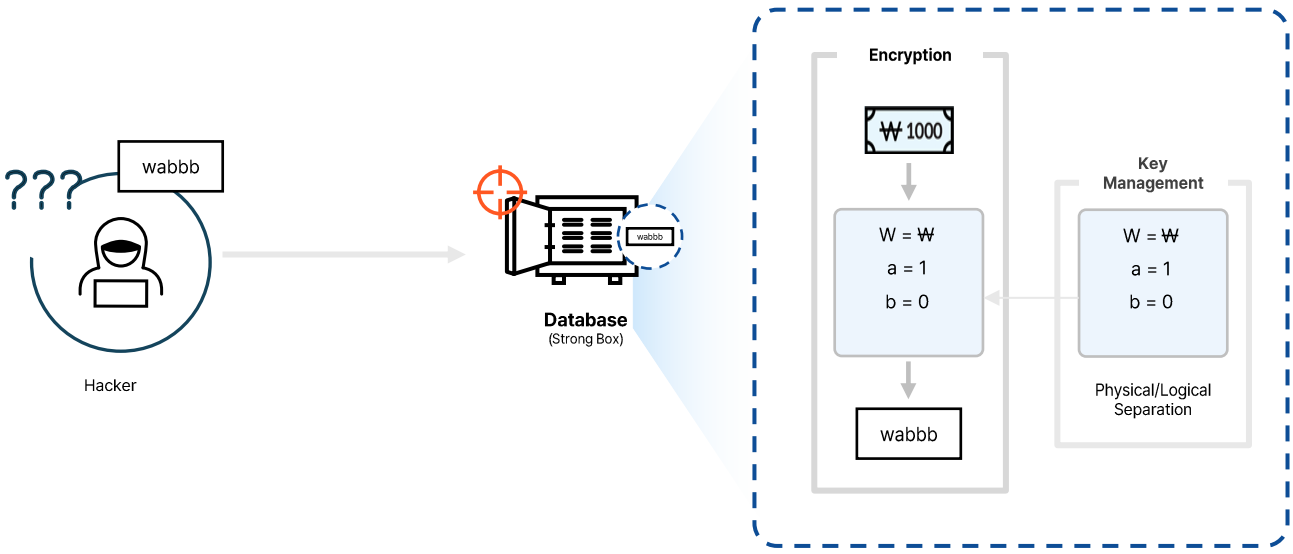
- 1999, Korea's First Encryption Technology
- 2004, DB Encryption Product, D'Amo Launched
- 7 Encryption Range with 38 Products Commercialized
- Customer Environment-Optimized Encryption
- Beyond a Solution, Applicable to Various Customer Environments and Technical Fields
- Encryption Platform, D.Amo Control Center (DCC) Provided for Effective Central Management of All D.AMO Products
- Increased Management Convenience Through Key and Log Management

Pic 13. Advancement of Data Encryption

Encryption Key, the Key to Encryption

Typically, a lock requires a key to secure it. The principle remains the same for encrypting data and a key used to lock data is the encryption key. Encryption key is the core of data encryption. Just like with a lock, each time data is encrypted, encryption key is used and the same goes for decryption. Only by using the encryption key, can the contents of the encrypted data be checked.

Let's assume that a thief has stolen the encrypted money. It's easy to think that the money would be of no use to the thief since it has been encrypted, but if the encryption key is also stolen, the money can be decrypted and used. In other words, if both the money and encryption key are taken, decryption becomes possible at any time. As seen above, encryption key plays a key role in data encryption and should be kept in a separate place so that even if encrypted data does get exfiltrated, it remains secure.



Pic 14. The Importance of Key Management

What types of encryption keys are there? Encryption keys can be divided into 2 types: symmetric and asymmetric keys. **Symmetric key** uses the identical key for both encryption and decryption, making it faster and smaller in size compared to asymmetric key. Also, its simple algorithm structure enables efficient data encryption. However, since the identical key is used for both en- and decryption, it is easy to decode, difficult to verify with certainty, and hard to manage.

Asymmetric Key uses different keys for encryption and decryption, and the encryption key is a public key that can be distributed to anywhere. It is also harder to decode and can be verified with certainty. However, the decryption key for asymmetric key is long and complex, making it slower compared to symmetric keys.

Item	Symmetric Key	Asymmetric Key
Key Relationship	Encryption Key = Decryption Key	Encryption Key ≠ Decryption Key
Encryption Key/ Decryption Key	Secret Key/Secret Key	Public Key/Private Key
Purpose	Large Data Encryption	Authentication, Non-Repudiation, Digital Signature
Advantages	Fast Computational Speed	Convenient Key Distribution & Management
Disadvantages	Difficult Key Distribution/ Management	Slow Computational Speed
Algorithm	DES, AES, SEED	RSA, DSA, ECC

Table 3. Comparison of Symmetric Key and Asymmetric Key

Both symmetric key and asymmetric key are crucial encryption keys, simply differentiated by their characteristics. If they are breached, the data, even if it is encrypted, cannot be protected.

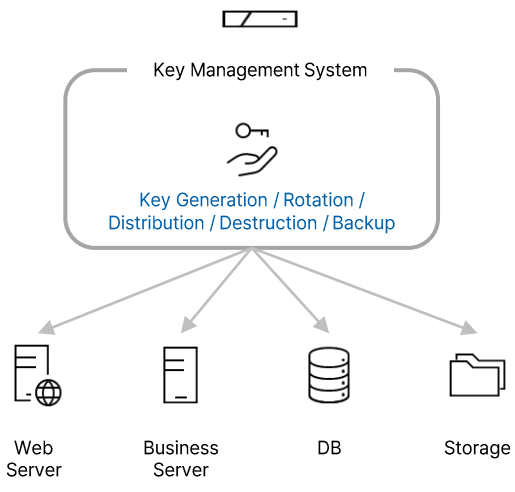
Governments and institutions have already recognized the importance of encryption keys, establishing detailed regulations and compliances.

Korea	
National Intelligence Service (NIS) Security Requirement	▪ Satisfaction of NIS Information Protection System and Network Equipment Security Requirement for Government required ▪ Utilization of CC-certified products for external storage of encryption keys recommended ▪ Protection of stored encryption keys through encryption, access control, and others
PIPC, 'Standards for Measures to Ensure Safety of Personal Information'	▪ Formulate and implement procedures on the generation, usage, storage, distribution, and destruction of encryption keys for the secure storage of encrypted personal information
Electronic Financial Supervision Regulation	▪ A financial company or an electronic financial business entity is to securely manage the keys applied to passwords and certifications by establishing procedures and methods on injection, operation, renewal, and destruction
Financial Security Institute (FSI), Guide to Utilizing Cryptography in Financial Sector	▪ Store encryption keys with extended usage separately from the cipher text, in a secure place such as a financial entity's Hardware Security Module (HSM), or ensure it is encrypted when stored ▪ Deny unauthorized user access to the encryption key ▪ Carry out regular backup of the encryption key in compliance with backup policy ▪ Establish procedure and method for the destruction of the key
Worldwide	
Personal Information Security Management System (ISMS-P)	▪ Formulate and perform procedure for encryption key generation, storage, distribution, recovery, destruction, etc. ▪ Store encryption keys in a separate secure location for recovery when required and minimize encryption key access authority
PCI-DSS 4.0	▪ Protect account data encryption keys by encrypting them with a key-encrypting key ▪ Define processes that protect encryption keys against disclosure and misuse ▪ Implement key management policies and procedures that includes the replacement or destruction of keys used to protect stored account data

Table 4. Major Legal Requirements and Compliances on Key Management

To satisfy such regulations and compliances, institutions and companies began to seek a way to manage encryption keys efficiently and security vendors developed Key Management System (KMS) along with data encryption.

A key management system provides central management of encryption keys used throughout the entire infrastructure by managing encryption key lifecycle (generation, rotation, distribution, destruction, backup) with one integrated system. Also, by storing and managing keys in a separate location other than the DB server and by rotating keys periodically, data security is maintained even if a hacker manages to exfiltrate the encryption key. It is also provided as an appliance and not only as a software, complying with physical secureness.



Pic 15. Key Management System Diagram

Encryption Across Environments (Cloud, IoT, Blockchain)

1. Cloud Encryption

Since the 2010s, numerous institutions and companies have been actively transitioning away from the legacy on-premise environment into the cloud environment. Companies actively try to utilize the cloud environment as compared to the preexisting hardware-based IT resources that require manual management, as the virtualized cloud environment allows more flexible countermeasures in case of sudden system overloads. Along with nationwide movements to implement public cloud environments, the trend of transitioning into the cloud environment is ongoing.

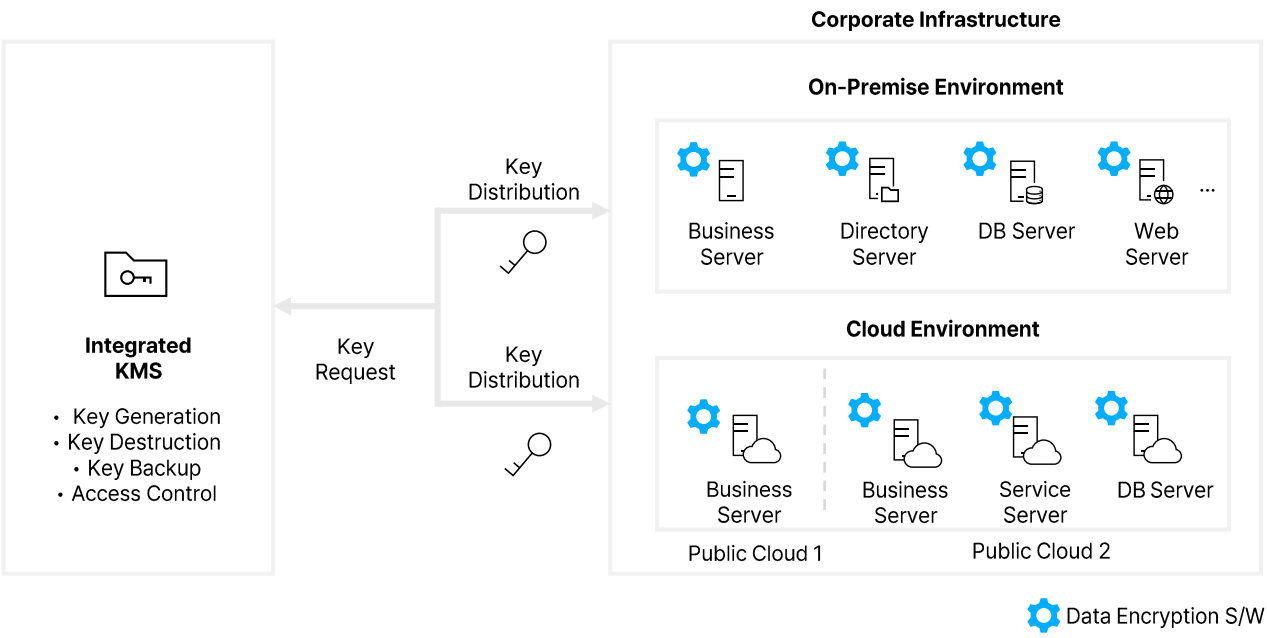
However, in contrast to the active transition, companies are yet to incorporate data encryption systems. According to the 2021 Thales Cloud Security Study report, only 17% responded to have encrypted over half of the sensitive information stored in the cloud and 40% of the companies responding to have suffered cloud-based data breaches within the past 12 months.

When incorporating public cloud environments, it is easy to think that as the environment is established through various Cloud Service Providers (CSP), such as AWS, MS Azure, Google Cloud, that the protection responsibility lies with the CSP. However, data protection responsibility lies solely with the service users and therefore requires the users' discretion.

Service Provider	Cloud Service Security Incidents Worldwide (* Source : Samjong KPMG ERI, Issue Analysis of Domestic Cloud Implementation)
Company G	Over 500,000 users' messages and contacts lost
Company M	Corporate information on cloud exposed to third parties due to service environment settings issue
Company A	Fake identity used to rent virtual server from company A to hack company S network
Company A	Account highjacked and all personal information deleted through iCloud, Gmail and Twitter account analysis
Company V	Malicious code injected into company V's product
Company D	User e-mail list leaked and spammed
Company E	Backdoor activity, company E's product used as a location to upload data stolen from C&C server
Company V	Zero-day attack deleting 100,000 customer websites
Company Z	Personal information leaked due to system hacking
Company D	Personal information leaked due to database hacking
Company K	Service interruption due to uCloud server switch and storage malfunction
Company A	Over 2.9 million users' personal information leaked
Company Y	Over 450,000 users' personal information leaked
Company C	All resources deleted due to DDoS attack

Table 5. Cloud Environment Security Incidents

In cloud environments, a single server can be logically partitioned into multiple isolated instances, enabling the concurrent operation of various services. These instances can scale up automatically by increasing their size or number in response to traffic demands. As a result, the complexity of managing data security can become significantly higher. Additionally, in multi-cloud environments utilizing multiple public clouds or hybrid environments using both on-premise and cloud environments simultaneously, the management complexity further increases. To manage encryption keys in such environments, an integrated management system for encryption keys across all infrastructures is needed.



Pic 16. Integrated KMS in Hybrid Cloud Environment

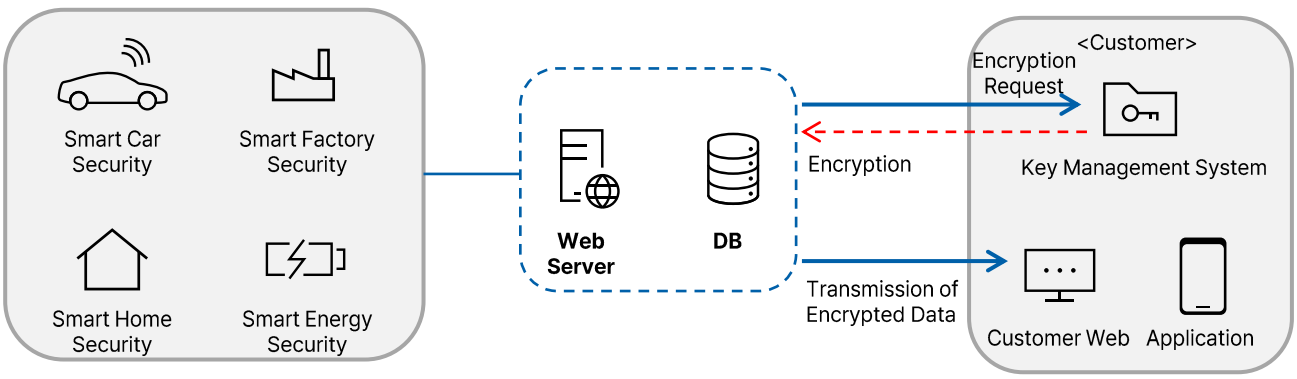
An integrated key management system in hybrid cloud environment controls encryption keys to effectively support a company's complex cloud environment. It is designed to be able to respond to the encryption S/W built in the servers, establishing an encryption infrastructure that can adapt to various corporate cloud environment settings.

2. IoT Encryption

Encryption in the IoT environment is also an issue. IoT stands for the Internet of Things, allowing convenient control of various objects, such as TV, home security camera, smart speaker by connecting them to the internet through integrating cameras, sensors, or communication technologies. Most IoT services consist of data closely related to a person's real life that is in direct contact with people. Also, as various devices are interconnected, security incidents due to IoT hacking may cause consequences far worse than personal information leakages, which is why data security is highly important.

According to a research published by Statista, a market research company, the global IoT market that was worth 1.177 trillion dollars in 2023 is estimated to reach 1.837 trillion dollars in 2024, a 17% growth compared to the previous year. The research also estimated the market to grow up to 2.82 trillion dollars by the year 2030, with a 12.5% growth per year on average. In Korea, the IoT industry generated about 25.116 trillion won (approx. USD 17.6 billion) in 2023, and the market has been growing almost 2 trillion won (approx. USD 1.4 billion) each year. Ironically, as the IoT industry continues to expand both domestically and internationally, the number of data leakages in IoT environment will likely continue to increase.

Devices used in IoT environments have relatively low performance, making it impossible to apply data encryption modules that require high specifications. Therefore, it is important to encrypt data using a lightweight encryption algorithm with low power usage and actively utilizing a key management system for proper encryption and decryption of encrypted data transmitted by IoT devices.

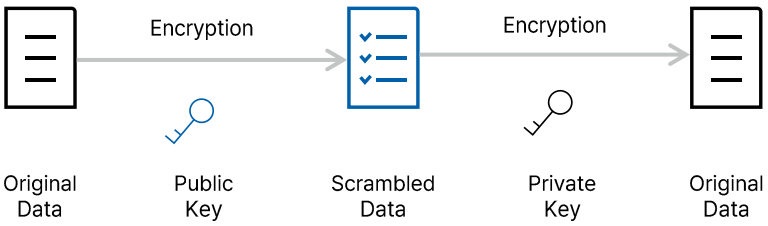


Pic 17. IoT Application Layer Encryption

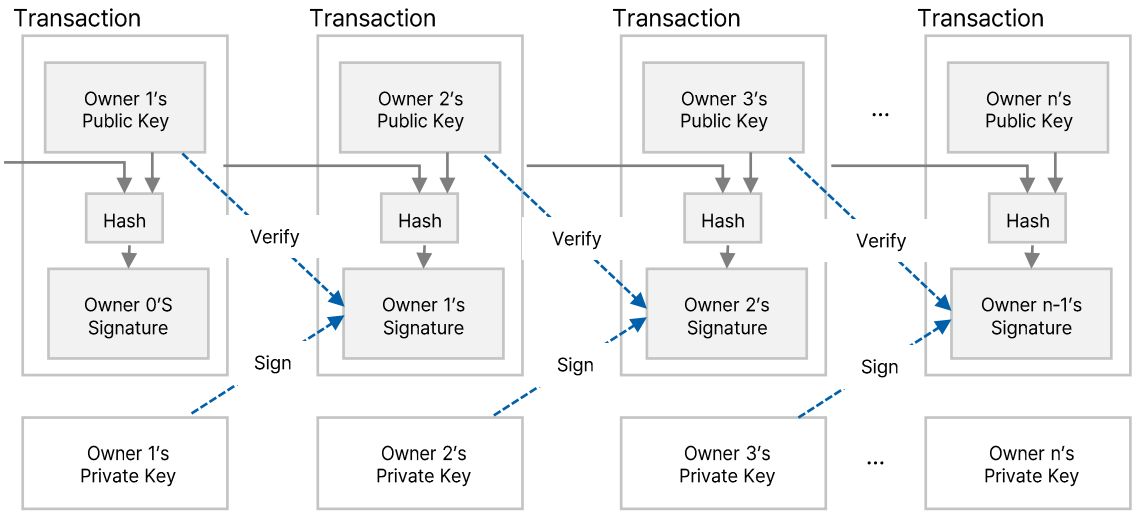
3. Blockchain Encryption

Encryption plays a crucial role in blockchain technology, one of the most significant innovations of the 2020s. Blockchain refers to the distributed data processing and storage technology that utilizes the properties of encryption to enable all participants within a network to access distributed data and record transaction details securely. In traditional centralized systems, transaction records are stored on a central server, leaving the entire system vulnerable to failure in the event of a server breach. In contrast, blockchain distributes the transaction records and relies on collective verification by the network participants, thereby reducing the risk of failure.

Blockchain systems primarily rely on public-key encryption, typically employing a compact elliptic curve-based schemes such as ECC and ECDSA. A public key is used for encryption while a private key is used for decryption so that a cryptocurrency can be sent to a specific person who is the only one with access to the specific cryptocurrency. Blockchain is primarily used in the financial field, especially regarding cryptocurrency, but it can be utilized in various other fields including supply chain management, real estate registration, authentication, and security, where there is high priority on the reliability of transaction details.



Pic 18. Digital Signature: Public-Key Encryption



Pic 19. Cryptocurrency Transaction: Private Key and Public Key

Despite the secureness of cryptocurrency, actual damages from hacking have been accumulating. According to The 2022 Crypto Crime Report published by Chainalysis, cryptocurrency theft amounted to 3.2 billion dollars in 2021, almost 6 times the amount compared to the previous year.

The biggest vulnerability in blockchain is the risk of private keys (secret keys) being breached by hackers. As a public key is primarily used for encryption, hackers can acquire the public key with ease, and if the private key is breached in the process and signatures forged, hackers can steal all the data with ease. Additionally, while periodic rotation of keys help prevent breaches, it is difficult to rotate the public keys or maintain records of it. Which is why encryption key management is fundamental to blockchain technology, including cryptocurrency.

Encryption Implementation Considerations

Institutions and companies that have realized the importance of data security and are looking to adopt encryption products and key management systems may encounter difficulties in selecting the appropriate encryption solution. This is likely because encryption, as a fundamental and essential component of information security, is often perceived as complex and complicated.

1. 100% Certified and Compliant

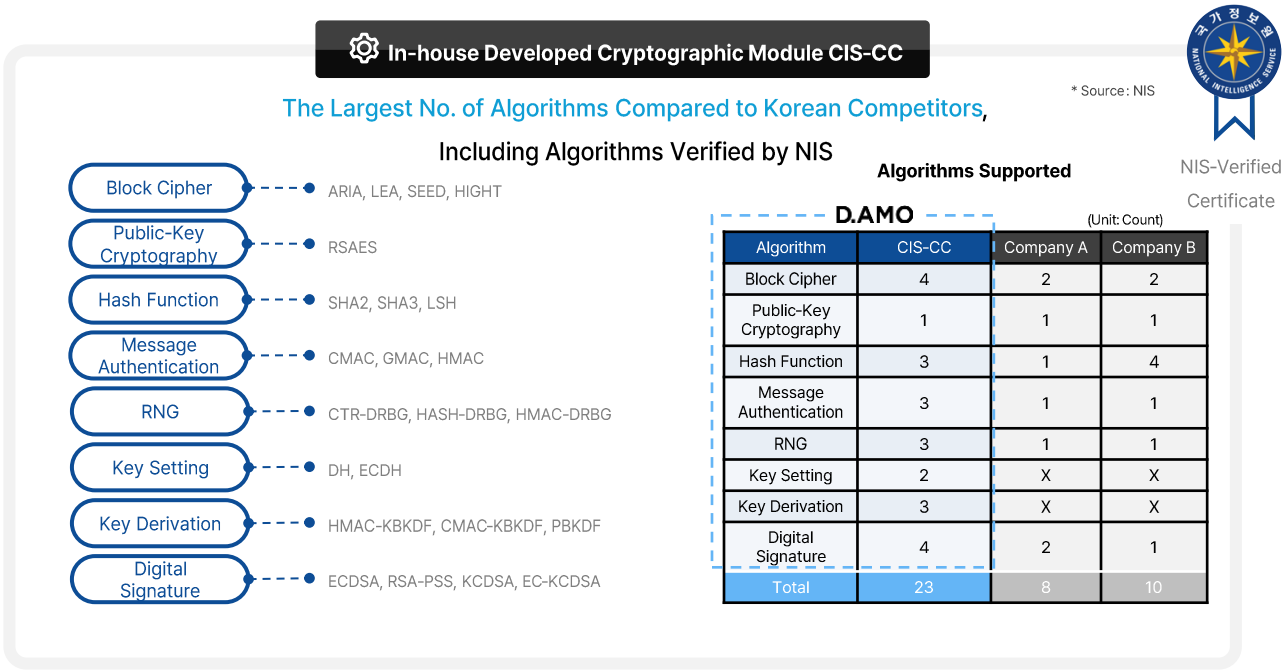
Korea heavily regulates data encryption and key management through various legislations such as PIPA, Medical Service Act, etc. and security solutions with CC certification and Korea's NIS certification ensure secure usage. Data encryption and key management solution must be 100% compliant with certifications and compliances.

2. Flexibility

The IT infrastructure of most institutions and companies has become increasingly complicated. Multi-cloud and hybrid environments, along with smart factories, blockchain technology, and IoT have diversified the infrastructure. A data encryption solution needs to be flexible to be implemented regardless of the environment and able to provide centralized monitoring and management.

3. Diverse Algorithm Support

The encryption solution is to support standard algorithms recognized by the NIS. NIS recognized algorithms include commercialized international encryption algorithms, Korean algorithms such as SEED and ARIA, and lightweight encryption algorithms including LEA and HEIGHT.



Pic 20. List of Supported Encryption Algorithms

4. Dedicated Key Management System

While the importance of encryption key is widely recognized, the significance of seamless integration and management between encryption solution and key management system should not be overlooked. A dedicated key management hardware appliance can be used to establish a secure communication channel for encryption key storage and seamless integration without requiring OS installation or software settings.

5. Central Management System

According to IBM Cost of a Data Breach Report 2021, companies with high system complexity experienced data breaches that cost an average of 52.4% more than those with lower system complexity – amounting to a difference of nearly 2.15 million dollars. This highlights the significant impact that system complexity can have on the financial consequences of a data breach.
Given the elevated risk, companies with complex systems should establish a data encryption framework and implement a centralized management system. The system should be capable of monitoring the status of encryption solution and key management, managing encryption, operation and integration settings, and checking various logs, including audit, access, and system logs.

6. Low Operating and Implementation Cost

Owing to their high level of technical sophistication, data encryption and key management systems are positioned at the higher end of the cost spectrum. As such, consideration should be given to reducing operation and implementation costs. Given that replacing security solutions is difficult and that financial resources must be allocated for ongoing maintenance, companies should approach initial implementation with long-term sustainability perspective. It is also crucial to evaluate the encryption method based on the potential performance degradation it may cause.

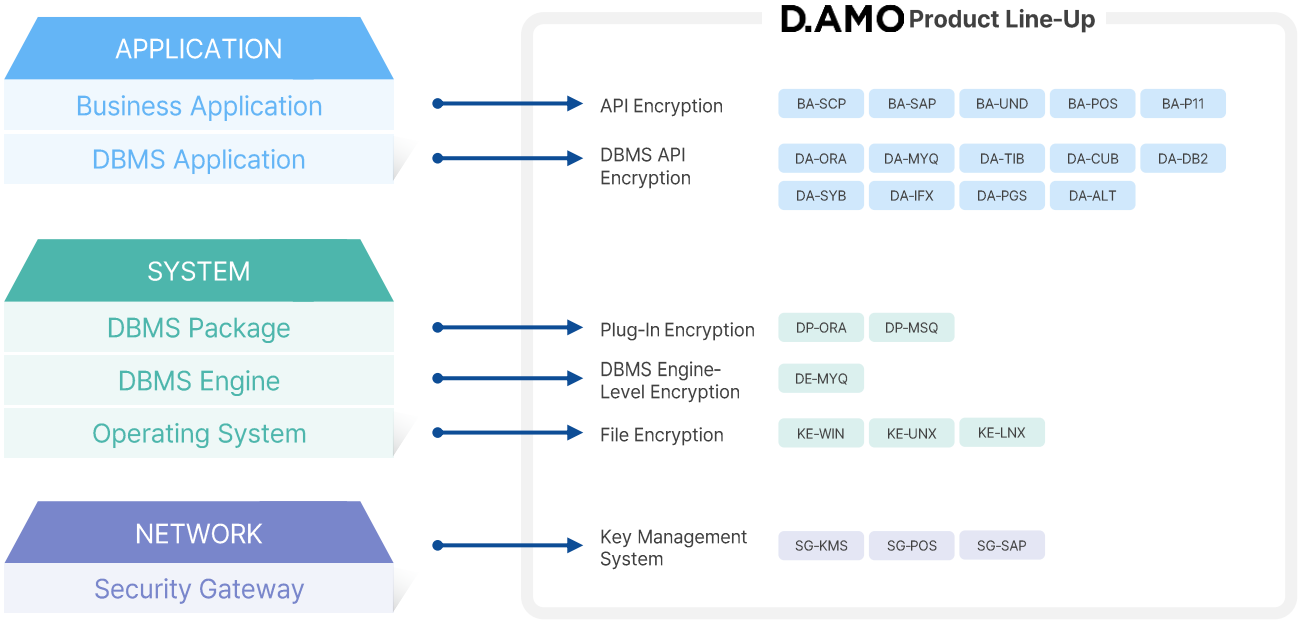
D.AMO is Korea’s first encryption platform that satisfies all 6 considerations for encryption solution implementation.

All That Encryption, D.AMO

D.AMO, Korea's First Encryption Platform

D.AMO is a leading encryption platform in the Korean database encryption market and the first Korean encryption platform equipped with NIS-verified encryption module and CC certification. The platform supports encryption across all layers of IT systems and offers a diverse portfolio of over 30 product lines. Through integration with dedicated hardware key management system, D.AMO enables management of keys, policies, and other settings, providing encryption optimized for business environments.

Instead of focusing only on a specific encryption method, D.AMO provides full array of encryption methods currently available in the market. D.AMO also satisfies various technical requirements for data protection, in compliance with PIPA, GDPR and other applicable regulations. Supported encryption environments include on-premise and cloud environments, both multi-cloud and hybrid environments, as well as environments that are difficult to apply security solutions such as IoT and blockchain.



Pic 21. System Layers Supported by D.AMO

BA (Business Application Encryption) is an encryption solution that injects API at the application server for encryption and decryption. BA is ideal for initial implementation and does not cause performance degradation after encryption as it is not dependent on DBMS. With various backward compatible products to choose from such as BA-UND for unstructured data encryption and BA-P11 for external key integration, D.AMO BA is one of the preferred solutions.

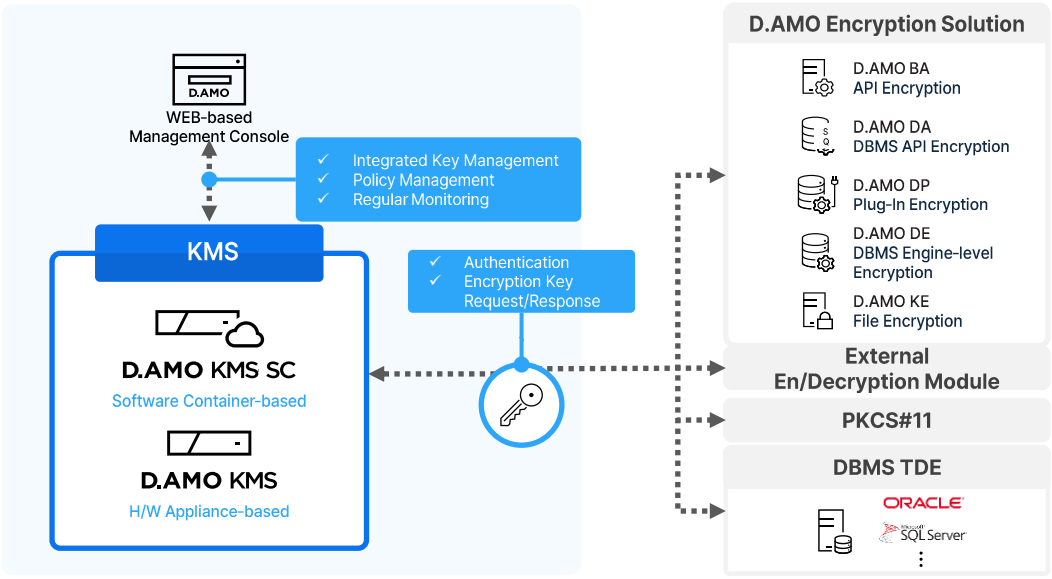
DA (DBMS Application Encryption) inserts API at the DB server to provide encryption without modifying the application server. Through user-defined functions that can be directly used against DB server, user-based encryption and decryption authority control is provided. DA requires minimum source modification, offering optimal performance and minimized DB server load. D.AMO DA provides encryption service optimized for customer environment by supporting 9 different DBMS platforms (Oracle, MySQL, MariaDB, Tibero, etc.).

DP (DBMS Package Encryption) is an encryption solution that provides security by installing packaged encryption modules in the DB server. DP is a powerful package consisting of strong encryption, access control, audit, integrated security, and additional features. Application source modification is not required for plug-in type of encryptions, as a separate package is installed at the DB server. D.AMO DP does not affect DB service during its encryption process as it generates a copy of the table for encryption.

DE (DBMS Engine Encryption) is an encryption solution optimized for opensource DBMS supporting MySQL and MariaDB. As the encryption engine is inserted inside the DBMS, providing data encryption, access control, and audit, application and DBMS modification is not required. D.AMO DE also supports Transparent Data Encryption(TDE) to ensure the database can be encrypted when accessed by external users. Finally, the product minimizes performance degradation and offers security through indexed column encryption.

As mentioned earlier, D.AMO provides encryption on all layers, including the operating system's kernel level. **D.Amo KE (Kernel Encryption)** can encrypt and decrypt applications, files and folders on database servers across various environments by operating at the OS kernel level. One of KE's most defining features is its convenient installation and ability to encrypt unstructured data. D.AMO KE is extensively used in medical sectors and other industries that require the encryption of unstructured data, including images and videos.

D.AMO KMS, Korea's First Key Management System Hardware



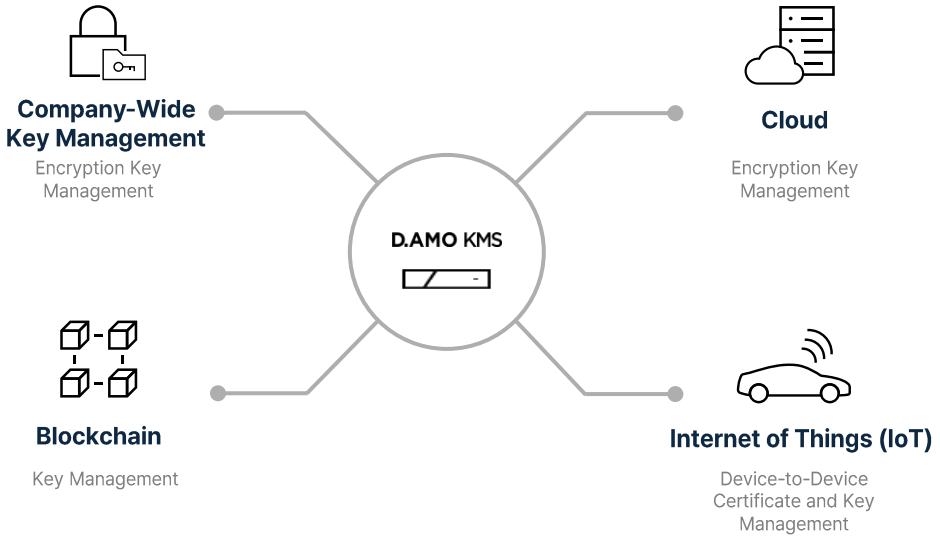
Pic 22. D.AMO KMS (Key Management System)

D.AMO KMS (Key Management System) can be divided into the H/W Appliance type and the SC (Software Container).

The D.AMO H/W appliance is Korea's first dedicated hardware key management appliance, implemented on on-premise environments, offering superior protection and operational convenience compared to the standard software-based key management solutions. It is equipped with NIS-verified encryption module and CC certified, complying with regulations related to encryption key management, such as ISMS-P and PCI DSS. With high availability (HA) configuration and scheduled self-monitoring features, D.AMO H/W appliance KMS provides stable and high level of security.

The container-based D.AMO KMS SC is designed to support various cloud environments, including multi-cloud and hybrid environments.

For cloud environments, the vertical or horizontal scaling capabilities and diverse commercial operating systems increase the complexity of security solution application. However, D.AMO KMS SC minimizes such restrictions and dependencies, and well-suited for all cloud environments.

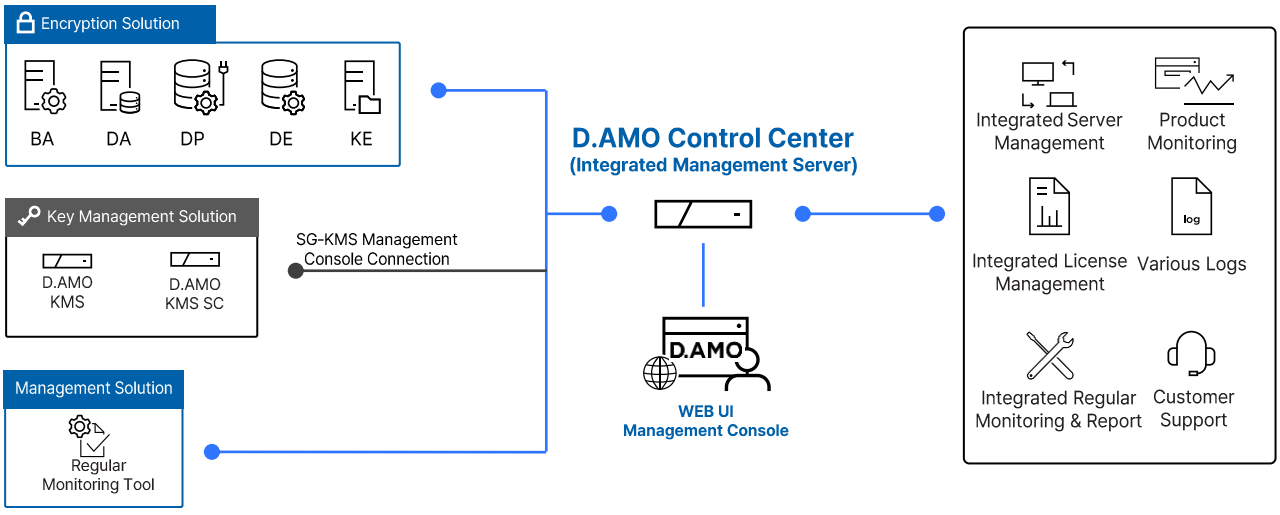


Pic 23. Versatile Application of D.AMO KMS

D.AMO Control Center, Integrated Central Encryption Management System

IT infrastructure environments are becoming increasingly diverse and complex, making it more challenging to operate or monitor the status of encryption solutions effectively. To address these challenges, an integrated management console, D.AMO Control Center (DCC) is provided.

D.AMO Control Center streamlines the management of security solutions and provides visibility into the applied D.AMO products across the system. Furthermore, by integrating key management system (D.AMO KMS), DCC offers an overview of individual solutions, enabling more efficient administration and reducing operational costs.



Pic 24. DCC Integrated Encryption System Diagram

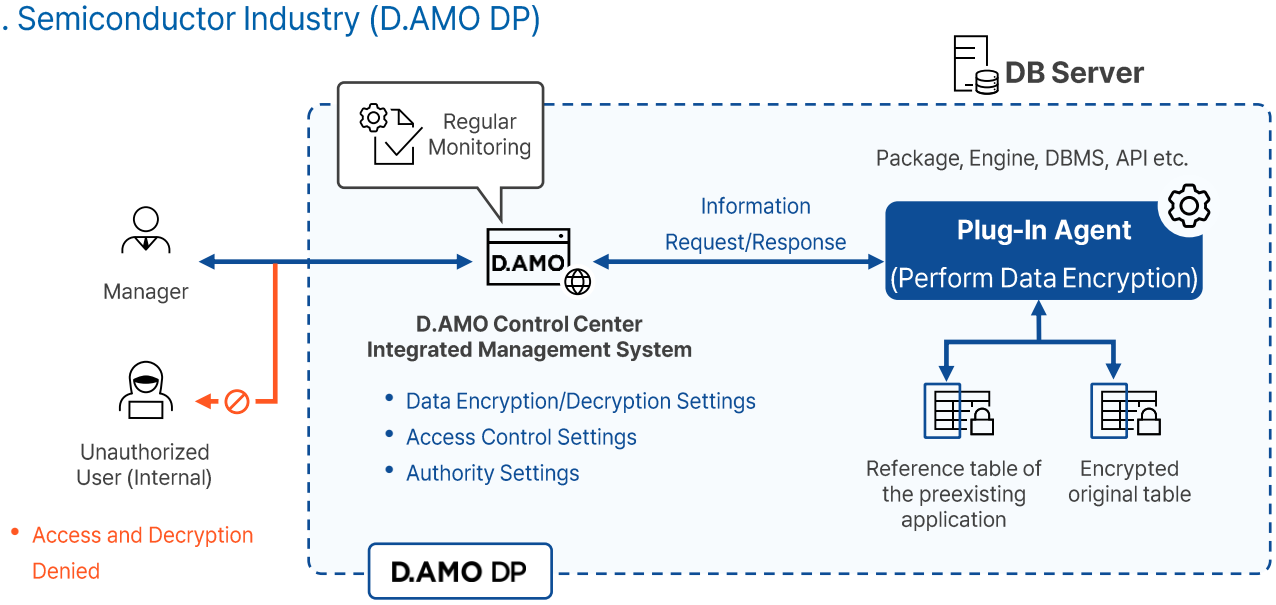
The encryption policies configured through D.AMO Control Center are encrypted before being transmitted to each encryption solution. These policies are then used to perform encryption, decryption, access control, logging, and security-related operations.

DCC features GUI-based interface with a visualized dashboard, enabling centralized monitoring of license usage, communication status, and other operational data for all integrated D.AMO solutions.

Through the integrated encryption solution management system, Penta Security Inc. remains committed to reducing security managers' operational burden and the management of complex encryption environments.

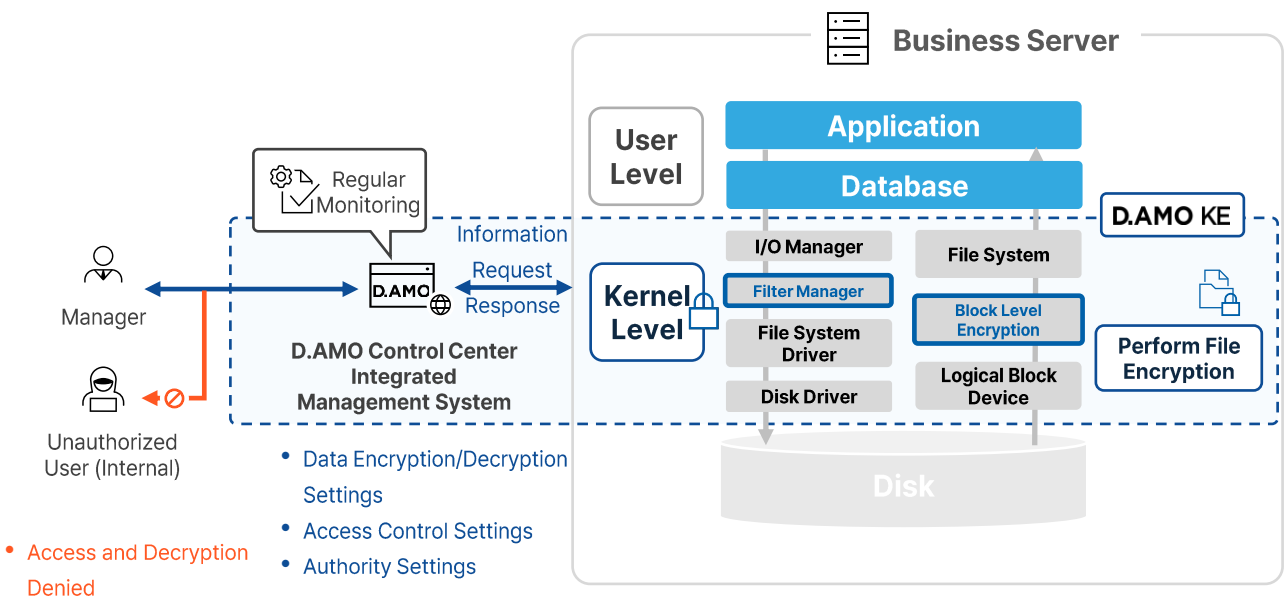
D.AMO Success Story

1. Semiconductor Industry (D.AMO DP)



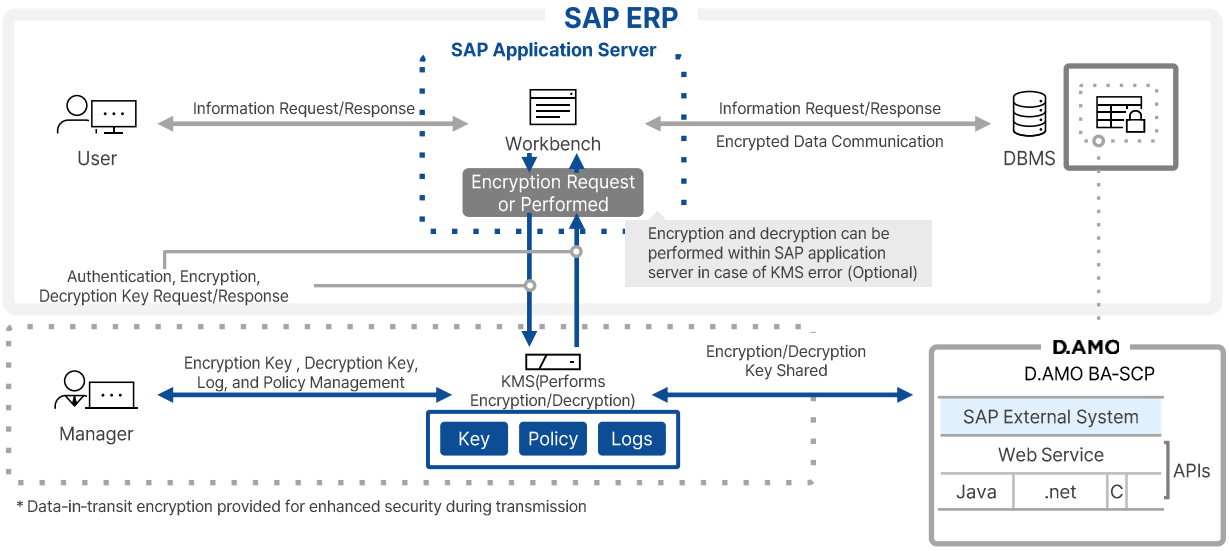
Customer	Company S (Semiconductor)
No. of Employees	32,000
Annual Revenue (2021)	KRW 44.648 trillion (approx. USD 31 billion)
Encryption Method	Oracle column-level encryption (DP-ORA)
Purpose	Implement new encryption system for semiconductor factory in China
Result	1. Reduce financial losses resulting from potential data breaches 2. Enhance performance through proactive optimization of specific queries 3. Enable high-performance real-time encryption field searches via index column encryption

2. Healthcare Industry (D.AMO KE)



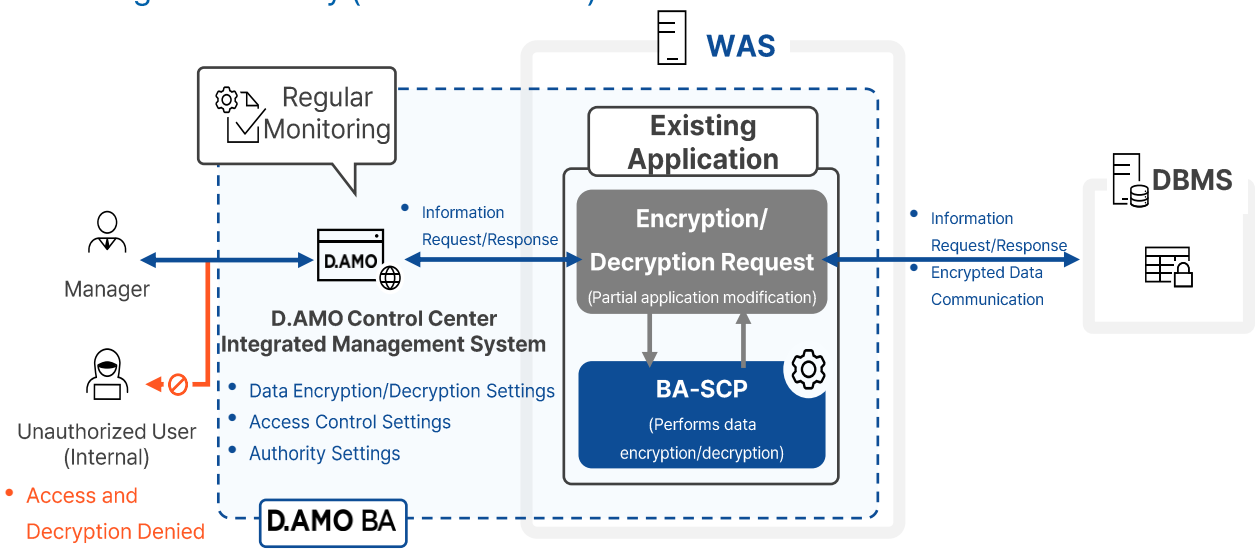
Customer	C General Hospital
No. of Employees	4,615
Annual Revenue (2021)	KRW 570 billion (approx. 401 million)
Encryption Method	Window kernel-level encryption (KE-WIN)
Purpose	Implement bio-information encryption system and PIPA compliance
Result	1. Comply with PIPA by preventing data breach and theft 2. Establish high level of security system through formulating and applying consistent data protection policy 3. Manage encryption directory history through user and system audit logs

3. Bio Industry (D.AMO for SAP)



Customer	S Corporation
No. of Employees	4,500
Annual Revenue (2021)	KRW 3 trillion (approx. USD 2.2 billion)
Encryption Method	Encryption and decryption within the SAP application server
Purpose	Integrate in-house developed SAP ERP system encryption
Result	1. Perform encryption without changes to the scale or configuration of the SAP ERP environment 2. Perform encryption, decryption and key management without any performance degradation 3. Satisfy European compliances on data encryption and key management

4. Rechargeable Battery (D.AMO BA-SCP)



Customer	L Corporation
No. of Employees	11,000
Annual Revenue (2021)	KRW 25.598 trillion (approx. USD 18 billion)
Encryption Method	API method encryption within the application server
Purpose	Establish National Core Technology (NCT) encryption
Result	1. Maximize developer convenience with multi-language library support 2. Comply with personal information regulations 3. Distribute processing at the DB server for performance load below 4% 4. Manage the operation of hundreds of BA-SCPs with DCC

Conclusion

Data is one of a company's most priceless asset, composed of personal, proprietary, and confidential data. Even the most physically secure systems can still be breached by threats such as SQL injection or e-mail phishing. Sometimes the leaks spring from within an organization itself, either intentionally or due to employee error. Once a system has sprung a leak, the only way to keep data safe is via encryption. The level of security can be further enhanced by integrating a combination of key management system, access control, and separation of authority.

D.AMO, the database encryption solution platform from Penta Security Inc., offers all of these. Additionally, various encryption solution features integrated can be managed through a single centralized management system, D.AMO Control Center. Implementing D.AMO enables companies and organizations to protect their valuable data while achieving compliance with a wide range of personal information regulations across the globe and to operate businesses with trust and confidence of their customers.

With the amount of commercially valuable data constantly increasing, the exponential growth in attempts to access data illegally is inevitable. To protect a company's valuable information, encryption is no longer an option, it's a necessity. Protect your data, your most priceless asset, with D.AMO.

Penta SECURITY
TRUST FOR OPEN SOCIETY

KOREA www.pentasecurity.co.kr
GLOBAL www.pentasecurity.com
JAPAN www.pentasecurity.co.jp

Cyber Security Awards Application Security 2020

IoT-based Smart Security Innovation Award 2020

Mwmber of the International Transport Forum CPB (~ 2020)

TU-Automotive Awards Best Auto Cybersecurity Product/Service 2019

Cybersecurity Excellence Awards Winner 2018

Hot Company in Web Application Security for 2016

SC Magazine Europe Best SME Solution

ICSA Labs Certified WAF

The First and Only CCEAL4 Certified WAF

PCI-DSS Compliance

Listed in Gartner®, 2023 Market Guide for Cloud Web Application and API Protection