



## Company Overview

---

**Founded** 1997년 7월  
**CEO/Founder** 이석우  
**Staff** 약 230 명 (연구 개발 및 기술 인력 130명)  
**Headquarters** 대한민국, 서울  
**Overseas Branch** Tokyo, Houston, Singapore  
**Overseas Network** Taiwan, Thailand, UAE, Malaysia, Indonesia, Italy, Ukraine

**Business Area** 암호화/웹보안/인증보안 등 기업정보보안, 사물인터넷, 블록체인  
**Clientele** 정부, 공공, 기업, 교육, 금융 등 분야 4,000여 고객사 보유  
**Products** 암호 플랫폼 **D'Amo**  
지능형 웹방화벽 **WAPPLES**  
인증 플랫폼 **ISign+**  
사물인터넷 및 블록체인 사업 **PALLET**

## 기업정보보안



### 현재 사업 기반

#### 데이터 암호화 + 웹 보안 + 인증 보안

- 국내 1위 + 아시아-태평양 1위
- 기업정보보안 시장 절대적 우위

#### Product Lineup

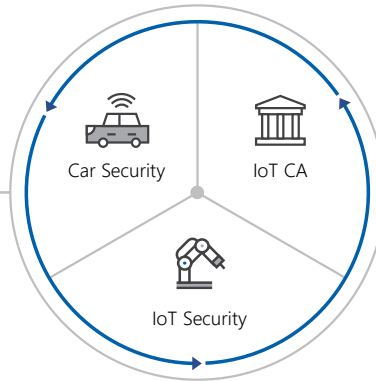


MyDiamo

WAPPLES

ISign+

## 사물인터넷 보안



### 미래 사업 기반

#### 교통 보안 + 사물인터넷 보안

- 자동차에서 인프라까지 교통보안 토탈 솔루션
- 스마트팩토리 등 산업분야별 IoT 보안 플랫폼

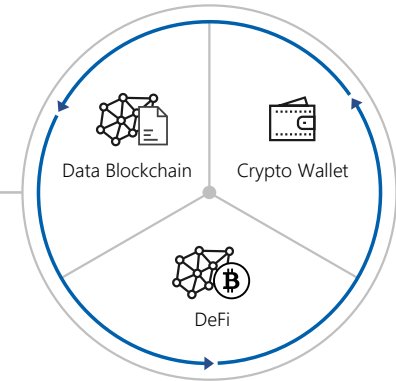
#### Product Lineup

AUTOCRYPT

AMO CA

Penta IoT Security

## 블록체인



### 미래 시장 개척

#### 데이터 블록체인 + 블록체인 금융

- 데이터 공유 블록체인 플랫폼
- 지갑에서 거래소까지 DeFi(Decentralized Finance)

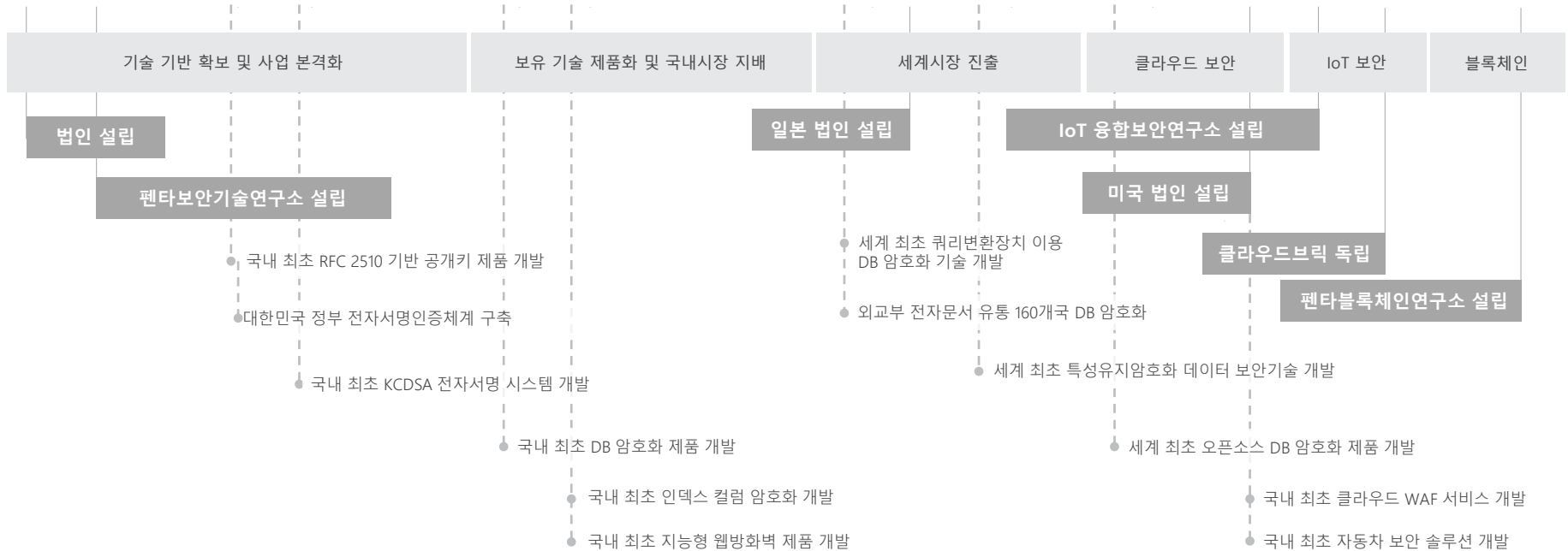
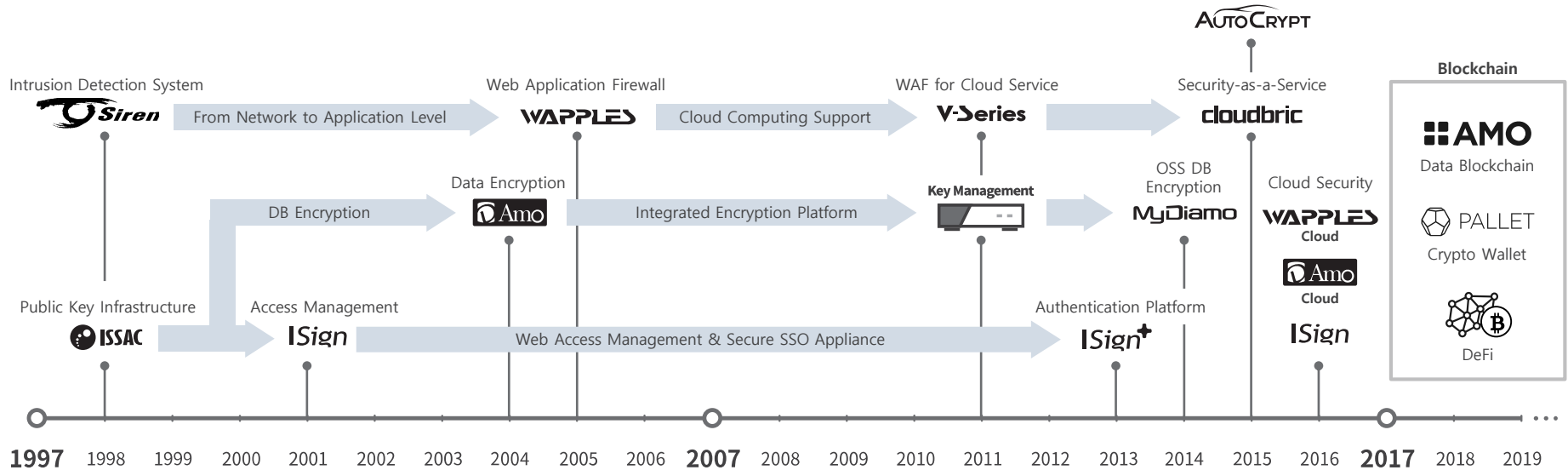
#### Product Lineup

AMO

PALLET

# 회사 연혁


1997년 설립 1세대 정보보안 전문기업




# 기술 현황

세계/국내 최초 개발 기록 및 보유 기술 사양


## 세계 최초


 쿼리변환장치 이용  
DB 암호화 기술 개발


 특성유지 암호화  
데이터 보안기술 개발


 오픈소스 데이터베이스용  
암호화 제품 개발

## 국내 최초


 RFC2510  
공개키 기반 제품 개발

 DB 암호화 솔루션  
D'Amo 출시

 스마트팩토리 보안 솔루션  
Penta Smart Factory Security 출시


 인텍스 컬럼 암호화 개발


 SaaS 웹사이트 보안 서비스  
Cloudbric 출시


 스마트에너지 보안 솔루션  
Penta Smart Energy Security 출시


 KCDSA  
전자서명 시스템 개발

 스마트카 보안 솔루션  
AUTOCRYPT 출시

 키관리 서버 출시 및  
국내최고등급 EAL3+ 인증 획득


 일본 마이넘버 보안 솔루션 출시

 POS 보안 솔루션 출시

 어플라이언스 타입 SSO  
ISign+ 출시

 국내외  
기술특허 **95개**

 국내외  
기술인증 **58개**

 기술인력  
비중 **60%**

 제품기술  
수상 **37개**



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



Asian Cyber  
Security Vendor  
of the Year

Gartner

Recognized on the  
Gartner WAF  
Magic Quadrant



No.1 WAF  
Vendor in the  
APAC Region



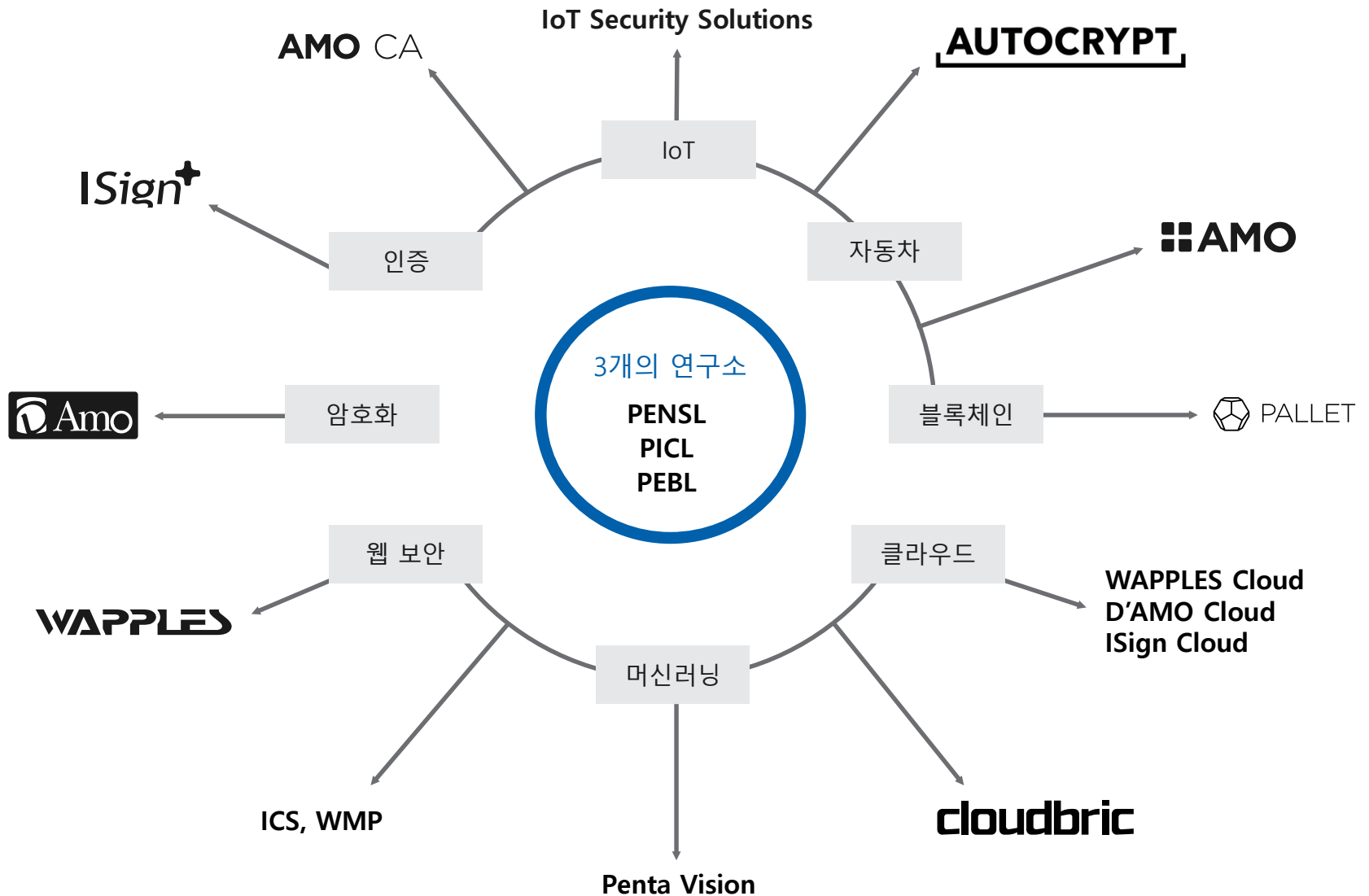
ICSA Labs  
Certified WAF



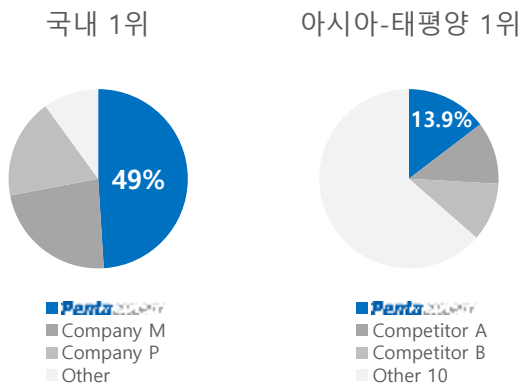
The First and Only  
CCEAL4 Certified  
WAF



PCI-DSS  
Compliance



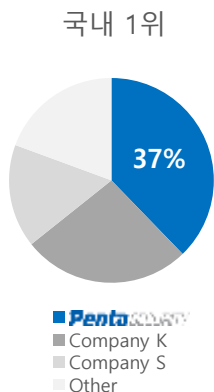
## 웹 보안



보호하고 있는 웹사이트 수 **658,000+**

- 국내 최초 지능형 논리 기반 탐지 엔진 WAF 개발
- 국내 최초 머신러닝 기반 자가 진단 엔진 개발
- 국내 최초 클라우드 WAF 서비스 출시
- 국내 최초 Gartner 웹방화벽 부문 등재

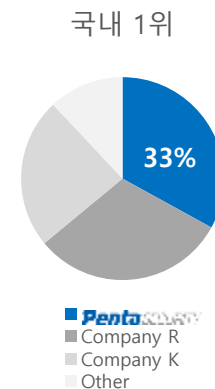
## 데이터 암호화



암호화가 적용된 서버 수 **5,800+**

- 세계 최초 쿼리변환장치 이용 DB 암호화 기술 개발
- 세계 최초 특성유지 암호화 데이터 보안기술 개발
- 세계 최초 오픈소스 데이터베이스용 암호화 제품 개발
- 국내 최초 인덱스 컬럼 암호화 개발
- 일본 마이넘버 보안 솔루션 출시
- 국내 최초 POS 보안 솔루션 출시
- 국내 최초 키관리 서버(KMS) 출시

## 인증 보안



보안인증이 적용된 서버 수 **3,200+**

- 국내 최초 어플라이언스 타입 제품 개발
- 국내 최초 RFC2510 공개키 기반 제품 개발
- 국내 최초 KCDSA 전자서명 시스템 개발

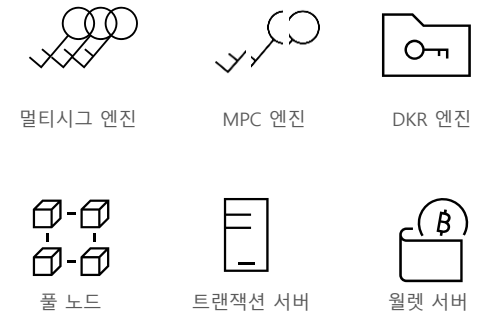
## PALLET Framework



## PALLET Product



## PALLET Service



### 암호 알고리즘, 지갑 표준 및 블록체인 프로토콜을 탑재한 자체 개발 프레임워크

- 해킹 위험이 존재하는 영역 E2E 보안 실현
- 오픈소스의 취약점을 해결하여 연산속도 및 개발 생산성 향상
- 전문적이며 지속적인 유지보수 제공

### 분산 금융(Decentralized Finance) 생태계에서 이용 가능한 디지털 자산 지갑

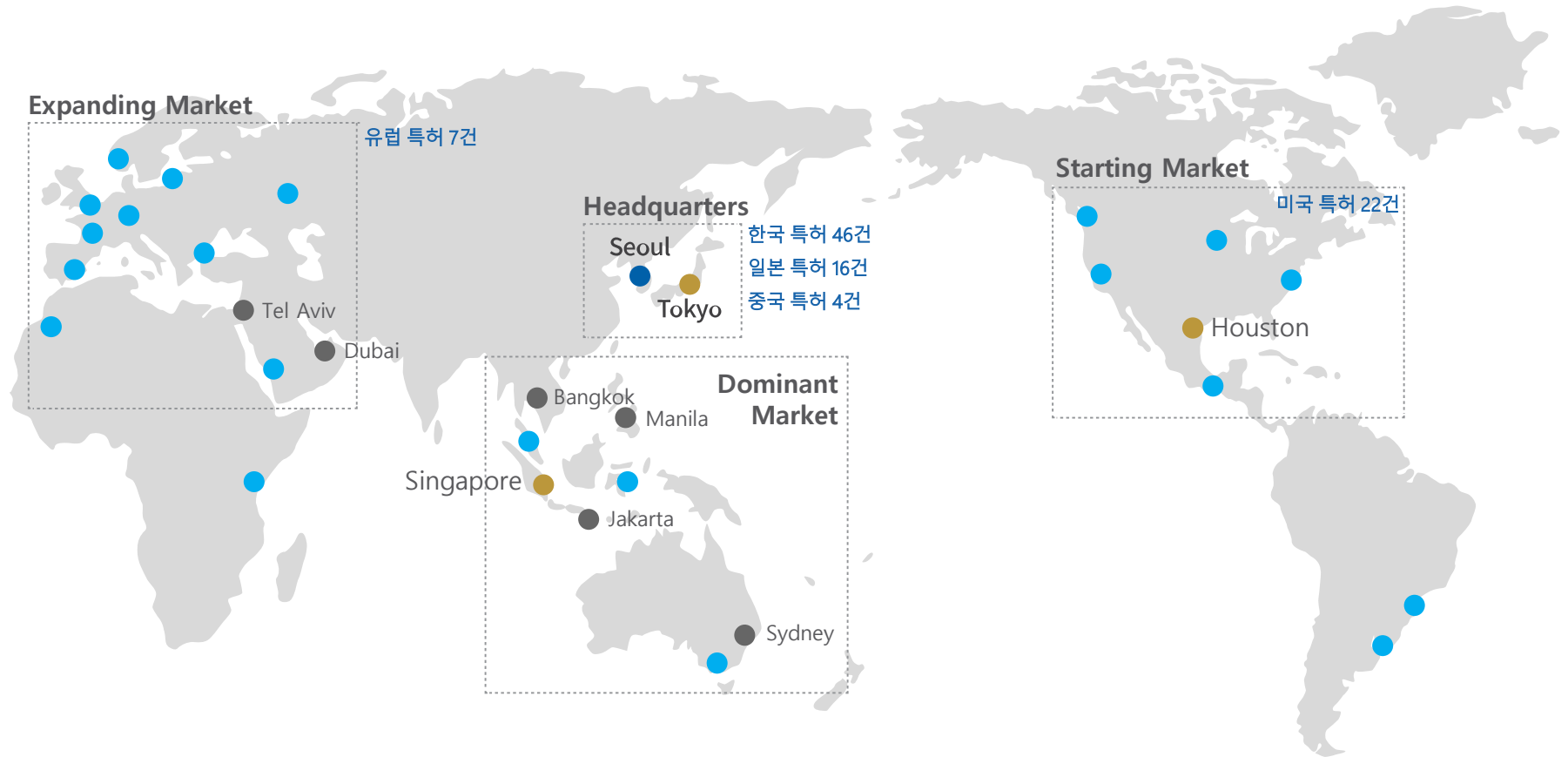
- 개인 사용자부터 기업 사용자까지 암호화폐 자산의 안전한 보관과 효율적인 관리
- 지갑 생성부터 트랜잭션 서명까지 모든 과정에 대한 권한 분리를 구현하여 기업 상황에 맞는 자산 관리 기능 지원

### 디지털 자산을 더욱 효과적으로 관리할 수 있도록 돕는 서비스

- 빠르고 안정적인 암호화폐 지갑 운영과 손쉬운 블록체인 데이터 접근
- 모든 종류의 암호화폐에 대해 다중 서명 기능 제공, 안전하고 중립적인 공간에서의 개인 키 보관과 복구 지원

# 세계 시장

아시아 · 태평양 기반 글로벌 파트너 네트워크



● Headquarters

● Branch Office

● Sales & Services

● Governments & Main Customers

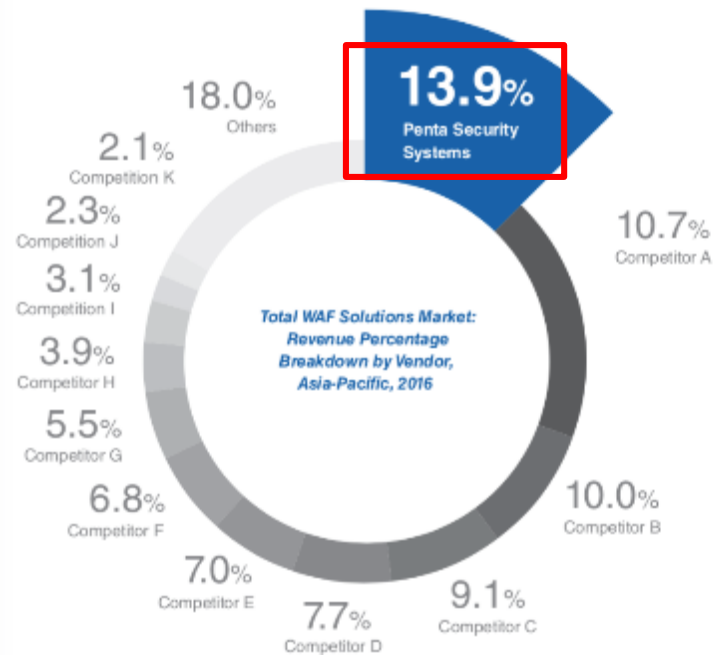


## WAF (Web Application Firewall) 분야 아시아-태평양 시장 1위

Figure 5: Frost IQ Matrix 2015 – Web Application Firewall Vendors



WAF Solutions Market Performance in Asia-Pacific



Source: Frost & Sullivan Asia-Pacific Web Application Firewall Solutions Market, Forecast to 2021

## 4년 연속 가트너 매직 쿼드런트(Magic Quadrant)& 하이프 사이클(Hype Cycle) 시장 분석 보고서 등재

Gartner.

### Magic Quadrant for Web Application Firewalls

Published: 7 August 2017 ID: G00314552

Analyst(s): Jeremy D'Hoinne, Adam Hills, Claudio Navea

The WAF market is growing, driven by the adoption of cloud-based WAF service. Enterprise security teams should use this research as part of their evaluation on how WAFs can provide improved security that is also easy to consume and manage, while respecting data privacy requirements.

Gartner.

### Penta Security Systems

Penta Security Systems is in the Niche Players quadrant. The vendor has a faithful base of customers, and its international expansion in Asian countries is promising.

Penta Security Systems is based in Seoul, Republic of Korea, and has 220 employees. Its product portfolio includes WAFs (Wapples appliances and Cloudbric cloud-based WAF service), a database encryption platform (D Amo) and authentication/SSO (ISign+). Penta Security emphasizes Wapples' "logic detection" technology, which does not require regular signature updates.

Recent corporate and WAF news from Penta Security includes Wapples version 5.0, with a change in operating system; support for TLS 1.2 and new centralized management solution.

Penta Security Systems is a good choice for organizations looking for an easy-to-operate WAF, and especially for organizations in East Asia.

Gartner.

### Hype Cycle for Data Security, 2017

Published: 28 July 2017 ID: G00314204

Analyst(s): Brian Lowans

Data is a pervasive critical asset that crosses traditional silo boundaries on-premises and in public clouds. This requires a data-centric security strategy that prioritizes datasets and mitigates evolving business risks such as regulatory compliance and threats from hacking, fraud and ransomware.

Gartner.

### Hype Cycle for Privacy, 2017

Published: 20 July 2017 ID: G00314626

Analyst(s): Bart Willemsen

As privacy laws follow a Hype Cycle of their own, security and risk management leaders with a focus on privacy have to take into account both regulatory and technological evolutions. Both are covered in this research, allowing the prioritization of relevant requirements and investments.

# 글로벌 시장 분석 보고서

## 가트너(Gartner), 프로스트 앤 설리반(Frost & Sullivan) 등 주요 시장 분석 기관으로부터 인정받는 기업

Gartner.

### Prioritize Enterprisewide Encryption for Critical Datasets

Published: 28 June 2017 ID: G00331161

Analyst(s): Brian Lowans

Security and risk management leaders face a rapidly increasing volume and variety of complex data security challenges, both on-premise and in the

Gartner.

### Defining Cloud Web Application and API Protection Services

Published: 24 October 2017 ID: G00337777

Analyst(s): Jeremy D'Hoinne

Cloud web application and API protection service is the evolution of cloud-delivered web application firewall services. Security and risk management

Gartner.

**User Advice:** Organizations should use FA to better understand their unstructured data, including where it resides and who has access to it. Data visualization maps created by FA can be presented to other parts of the organization and be used to better identify the value and risk of the data, enabling IT, line-of-business and compliance organizations to make better-informed decisions regarding classification, information governance, storage management and content migration. Once known, redundant, outdated and trivial data can be defensibly deleted, data can be migrated or quarantined, and retention policies can be applied to other data.

**Business Impact:** FA tools reduce risk by identifying which files reside where and who has access to them. They support remediation in areas such as the elimination or quarantining of sensitive data, identifying and protecting intellectual property, and finding and eliminating redundant and outdated data that may lead to unnecessary business risk. FA shrinks costs by reducing the amount of data stored. It also classifies valuable business data so that it can be more easily leveraged and analyzed, and it supports e-discovery efforts for legal and regulatory investigations. In addition, FA products feed data into corporate retention initiatives by using file attributes.

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Sample Vendors:** Active Navigation; Bloomberg; Capax Discovery; Hewlett Packard Enterprise; IBM (StorageIQ); Kazup; Komprise; STEALTHbits; Varonis; Veritas Technologies

**Recommended Reading:** "Market Guide for File Analysis Software"

"Organizations Will Need to Tackle Three Challenges to Curb Unstructured Data Glut and Neglect"

"How to Move From Data Negligence to Effective Storage Management"

"Information Governance Gets Real: Four Case Studies Show the Way Out of Information Chaos"

"Overcome Data Gravity and the 'Heavy' Bits That Keep Data From Moving"

"Market Guide for Data-Centric Audit and Protection"

**Format-Preserving Encryption**

**Analysis By:** Brian Lowans, Joerg Fritsch

**Definition:** Format-preserving encryption (FPE) is used to protect data at rest, in use and when accessed through applications while maintaining the original data length and structure. It is used to protect fields within an application's database, relational database management systems (RDBMSs)

Gartner.

Data Security Standard applications. FPE should be deployed as part of a broader data security governance approach that balances business needs against appropriate security controls.

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Sample Vendors:** Datasecure; Gemalto; HPE; Mantic; Penta Security Systems; PKWARE; Protegrity; Thales e-Security

**Recommended Reading:** "Develop Encryption Strategies for the Server, Data Center and Cloud"

"Develop an Encryption Key Management Strategy or Lose the Data"

"Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization"

"Market Guide for Data-Centric Audit and Protection"

"Market Trends: Database Security; Worldwide, 2017"

**Privacy by Design**

**Analysis By:** Bart Willemsen

**Definition:** Privacy by Design (PbD) is a set of universal privacy principles and mandatory in several jurisdictions, including Europe and Canada. PbD is about protecting privacy proactively by embedding it into technology (for example, application or customer interaction design), as well as into procedures and processes through (for example, privacy impact assessments). There is no commonly agreed-on definition of what PbD entails. One of the more widely used definitions is the one from the Information and Privacy Commissioner (IPC) of Ontario.

**Position and Adoption Speed Justification:** Since the EU passed the General Data Protection Regulation (GDPR), which explicitly demands PbD (which is called "data protection by design and by default"), privacy professionals and product vendors have intensified the debate as to what "privacy by design" actually means, justifying a position that is a little post-peak. While the new law comes into force on 25 May 2018, in the meantime recommendations and regulators' opinions are bringing further clarification, and vendors have started arguing that their products are designed with PbD in mind.

Yet it is not a new concept. The term "privacy by design" was introduced in the late 1990s, but did not gain widespread recognition beyond the circles of privacy professionals. The information and

Gartner.

**HDD Controllers**

HDD controllers manage the flow of data to the physical drive media typically included as part of storage product offerings. These offer bulk storage encryption and scale in proportion to the number of HDDs, with full bandwidth requirements. HDD controller encryption can reduce complexity by retrofitting environments and using existing HDD infrastructures. Most products are compliant with KMIP.

**Recommendation:** Use HDD controllers to retrofit existing or new installations, and typically offered as a license to existing storage solutions.

**Use Cases:** Provides bulk encryption at rest, but does not provide any access control and has limited compliance benefit, because it protects only against loss or theft of the media from the data center.

**Sample Vendors:** EMC, Fujitsu, HP, IBM, Oracle, Symantec

**TDE and File Encryption**

Vendors that offer the ability to target the protection of unstructured data typically offer both file encryption and TDE for database management systems (DBMSs) at rest. Vendors typically provide a centralized interface or the ability to encrypt multiple DBMS platforms and offer SOD through the management of access control lists (ACLs), typically linked through AD. Some vendors also provide APIs, which offer TDE to applications accessing DBMSs or unstructured files, such as SAP and Microsoft SharePoint. A few relational DBMS (RDBMS) vendors have native TDE encryption tools, such as MariaDB, Microsoft SQL Server, MongoDB, PostgreSQL, Oracle and Sybase, but the keys are accessible and managed by the DBA. However, most enterprises use multiple instances of RDBMSs from different vendors, making their selections unattractive.

**Recommendation:** Use this encryption when specific files, DBMSs or other common file types need to be encrypted. Protected files can be stored on-premises, in data centers or in the public cloud.

**Use Cases:** Provides targeted encryption to mitigate the need for breach notification requirements, even if the storage media is lost or stolen. When combined with access controls through applications and endpoints, this can prevent access by administrators or unauthorized users. TDE does not prevent access to DBAs.

**Sample Vendors:** eper, Gemalto, HPE, IBM, KSI, Penta Security, Protegrity, PKWARE, QuintessenceLabs, Security First, Townsend Security, Thales e-Security

**Column Encryption, FPE and Tokenization**

vendors are now offering products that mask data on presentation to application users, in combination with FPE or tokenization. This concept means that the sensitive fields are replaced with randomized data that has the same format as the original data. Competition is growing, and several vendors have introduced new products into this market during the past few years.

Traditional approaches to using column-level encryption are still available, but are less commonly used. These products do not maintain the field structure, which may interfere with the database operation requiring schema changes or software changes to applications. A few RDBMS vendors have native column-level encryption tools, such as Microsoft SQL Server, PostgreSQL, Oracle and Sybase, but the keys are accessible and managed by the DBA. However, most enterprises use multiple instances of RDBMSs from different vendors, making their selections unattractive.

Regardless of the technology, these tools can affect database and application performance through problems that include key management standards, indexing, schema changes or connection pooling.

**Recommendation:** Use third-party encryption products to enable EKM of multiple-vendor RDBMSs.

**Use Cases:** Provides targeted encryption to mitigate the need for breach notification requirements, if the storage media is lost or stolen. This can prevent access by database, system or IT administrators, and provides access restrictions to database and application users.

**Sample Vendors:** Datasecure, eper, DBSec, Global Systems, Gemalto, HPE, IBM, KSI, Liason Technologies, Netlib, Penta Security Systems, Protegrity, Thales e-Security

**SaaS**

Enterprises continue to expand their use of public-cloud-based SaaS. Protecting sensitive data to meet data residency and compliance requirements has led to the use of products that include searchable-encryption algorithms. FPE or tokenization offered by cloud data protection gateways (CDPGs) and CASBs. However, protecting the sensitive data may affect the processing ability of a cloud-based service. For example, FPE or tokenization can be used to enable indexing, searching and sorting, in combination with external tables.

Care is required when using searchable-encryption algorithms, because the vendor's particular implementation will result in weakened security with unquantified risk of cryptanalysis. However, all cryptographic implementations will result in lost functionality for numeric calculations performed in the cloud. Protection can be performed within an on-premises gateway appliance or a hosted appliance, which interfaces with SaaS applications as a reverse proxy. Alternatively, endpoint products can operate on the endpoints and use a forward proxy.



KOREA [www.pentasecurity.co.kr](http://www.pentasecurity.co.kr)

GLOBAL [www.pentasecurity.com](http://www.pentasecurity.com)

JAPAN [www.pentasecurity.co.jp](http://www.pentasecurity.co.jp)



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



Asian Cyber  
Security Vendor  
of the Year



Recognized on the  
Gartner WAF  
Magic Quadrant



No.1 WAF  
Vendor in the  
APAC Region



ICSA Labs  
Certified WAF



The First and Only  
CCEAL4 Certified  
WAF



PCI-DSS  
Compliance