Trust. Every day.

gemalto
security to be free

Erol Dogan, Regional Sales Engineer, Enterprise & Cyber Security
March 2017

RECORDS BREACHED IN THE YEAR 2016

554,454,942

> *More and more organizations are accepting the fact that, despite their best efforts, security breaches are unavoidable.*

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY
3,046,456

EVERY HOUR
126,936

EVERY MINUTE
2,116

EVERY SECOND
35

NUMBER OF BREACH INCIDENTS

974

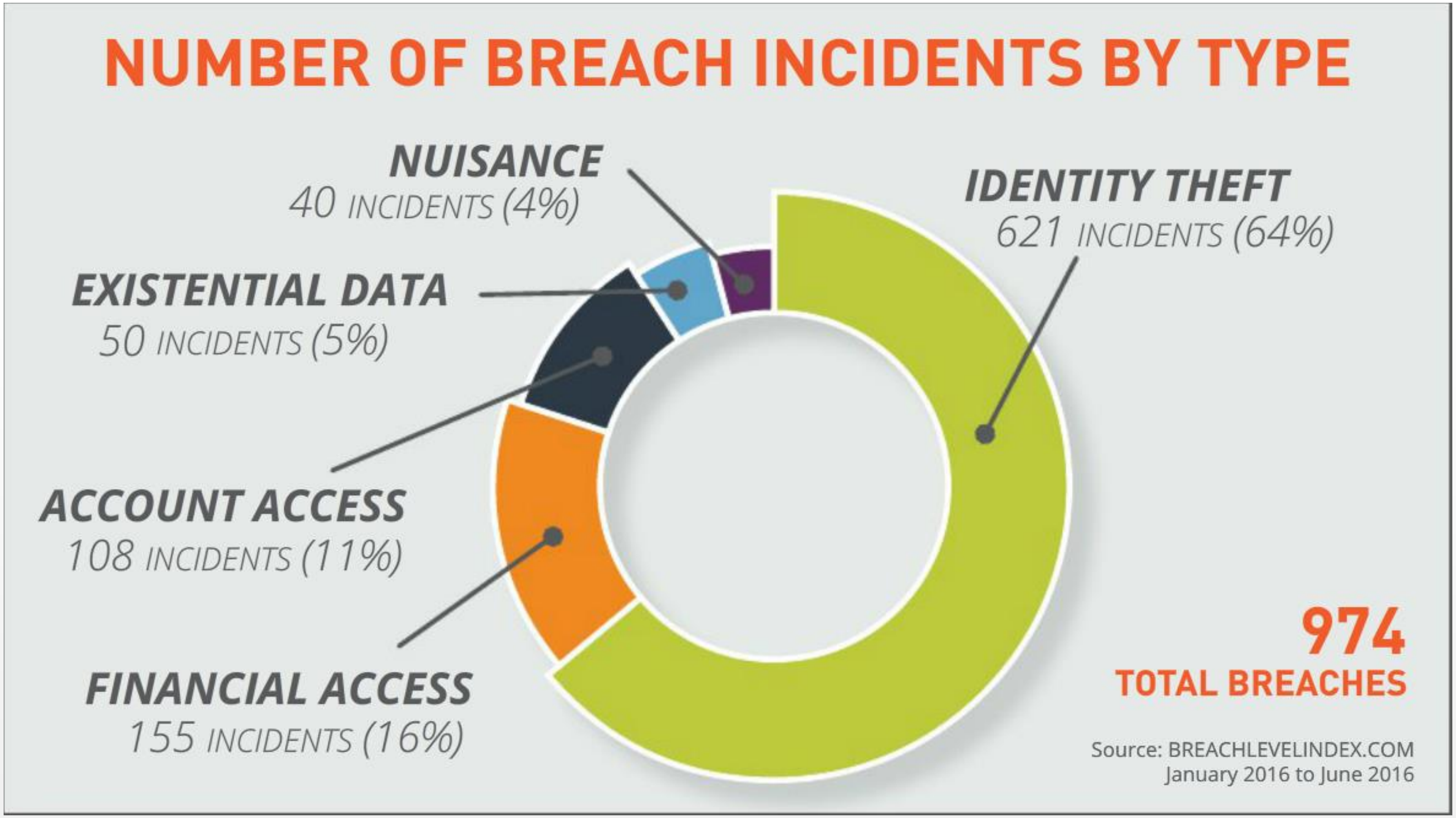
NUMBER OF BREACHES WITH OVER 1 MILLION RECORDS AFFECTED

29

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

52%

What data is targeted?

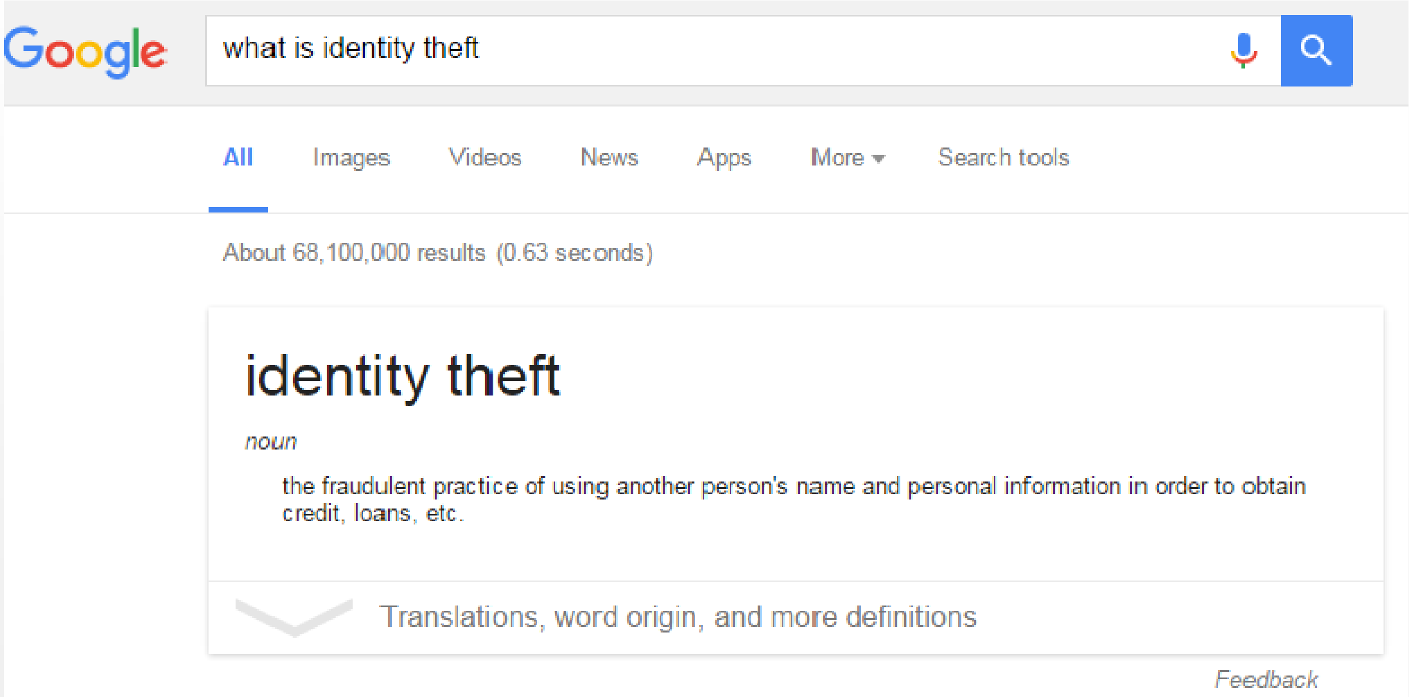


NUMBER OF BREACH INCIDENTS BY TYPE

Source: BREACHLEVELINDEX.COM
January 2016 to June 2016

Identity Theft is King

The increased targeting of **individuals' identities** and their **personal information** exposed just how valuable this information has become to cybercriminals.



About 68,100,000 results (0.63 seconds)

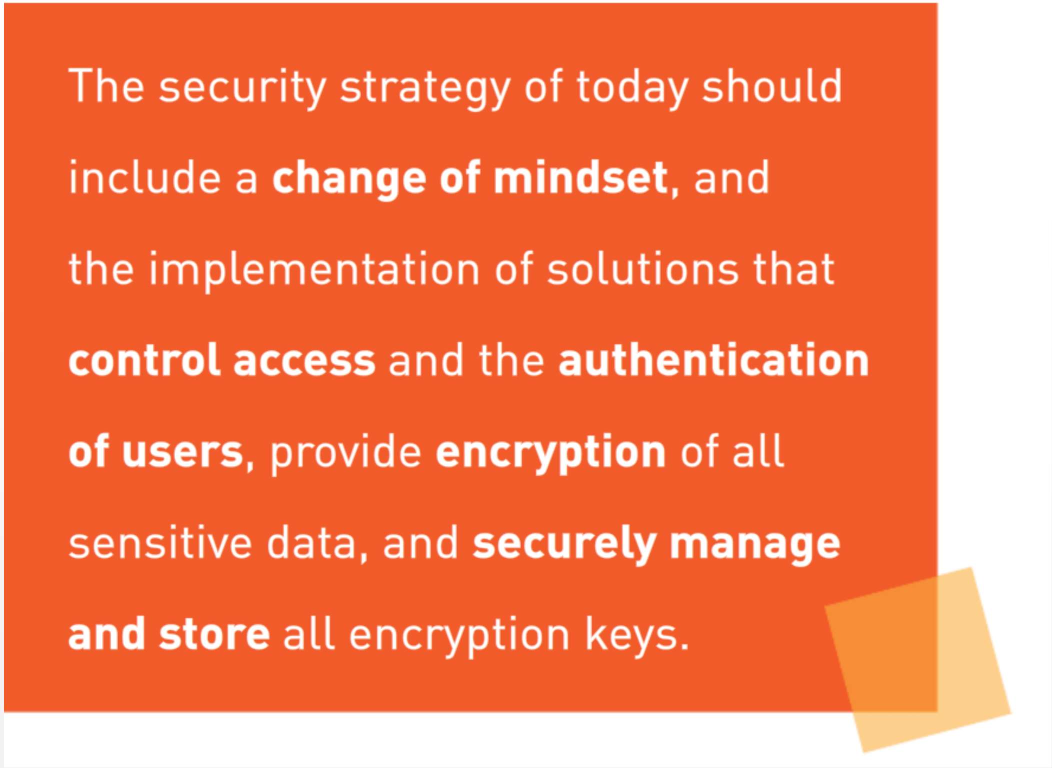
identity theft

noun

the fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.

SECURE THE BREACH

Breaches will happen – we must prepare!



The security strategy of today should include a **change of mindset**, and the implementation of solutions that **control access** and the **authentication of users**, provide **encryption** of all sensitive data, and **securely manage and store** all encryption keys.

A New Mindset is Needed…

1	**Accept the Breach**	**Perimeter security** alone **is no longer enough**.
2	**Protect What Matters, Where It Matters**	**Data** is the **new perimeter**.
3	**Secure the Breach**	**Attach security** to the **data** and **applications**. Insider threat is greater than ever.

Breaches will happen – we must prepare!

Why?

- 70% of breaches
  - => Due to weak/stolen passwords
- 80% of security investment
  - => Perimeter security
- 90% of companies
  - => No policies around keys

Disclaimer: numbers come from Gemalto and personal experience

RBA

Biometry

Privilege management

Encryption

We must protect what matters where it matters at the edge AND at the core

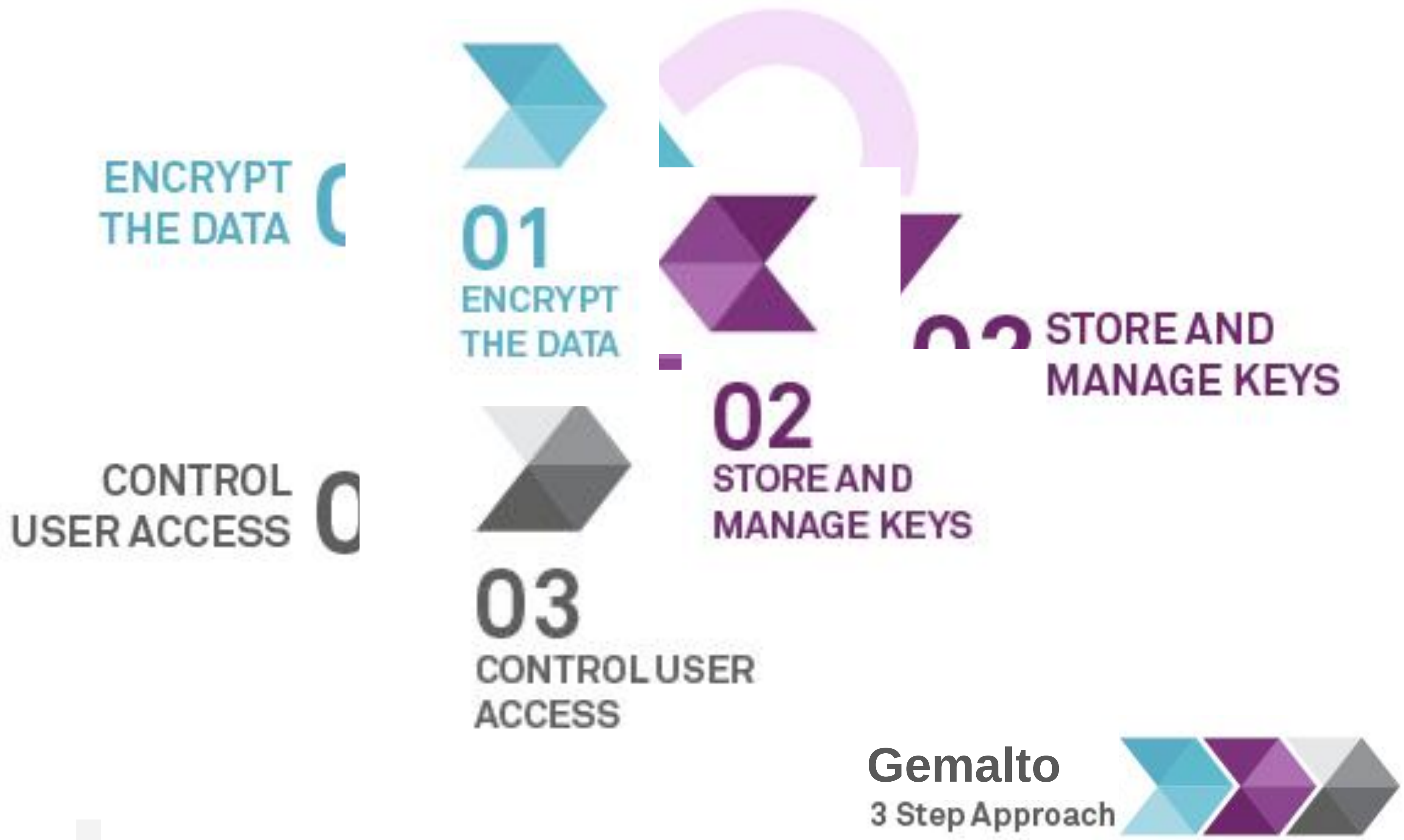
Convenience

Cloud-ready

Key Management

Contextual security

Gemalto’s Three Step Approach



ENCRYPT THE DATA

CONTROL USER ACCESS

01 ENCRYPT THE DATA

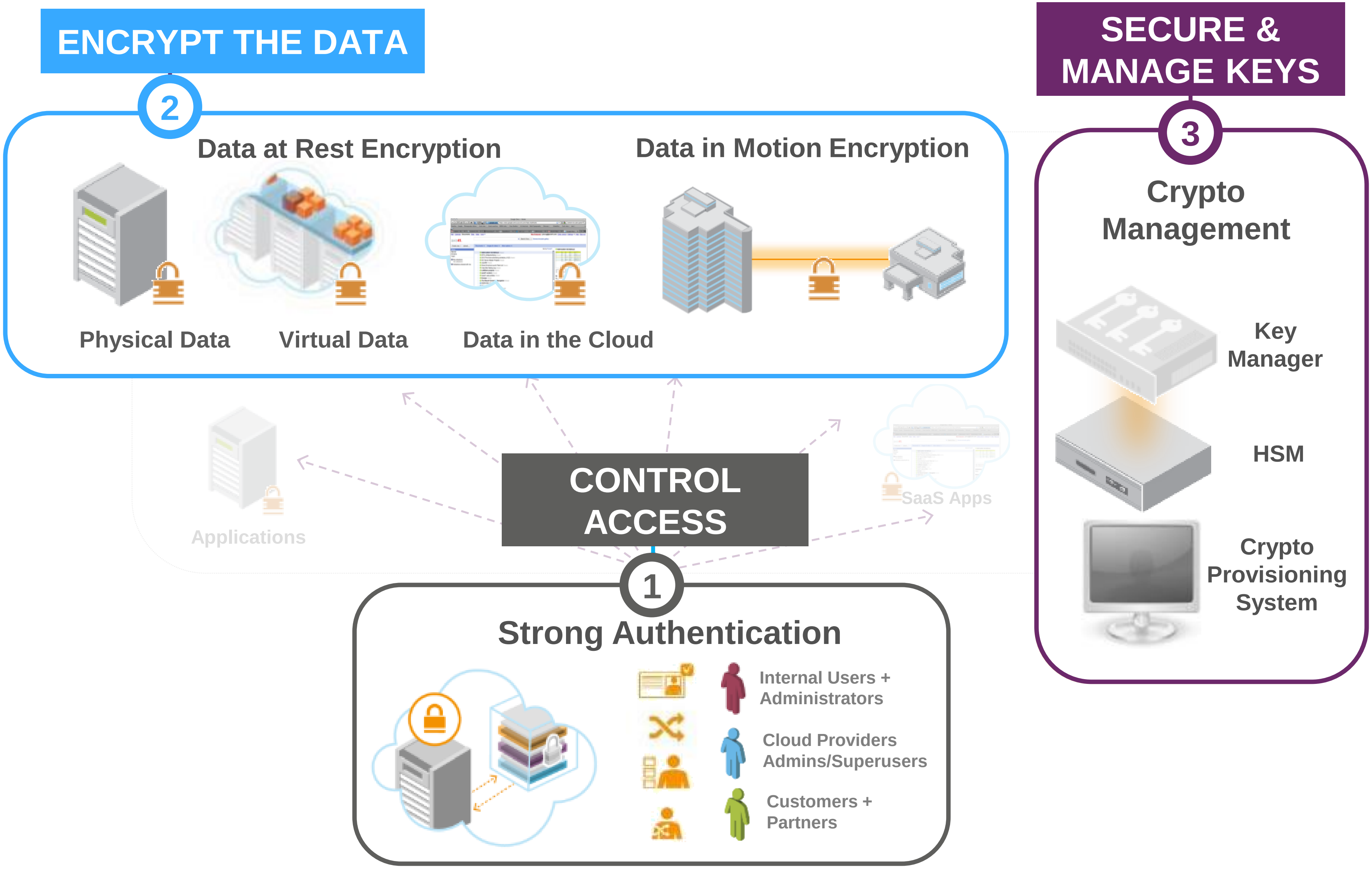
02 STORE AND MANAGE KEYS

STORE AND MANAGE KEYS

03 CONTROL USER ACCESS

Gemalto 3 Step Approach

Protecting the Data



ENCRYPT THE DATA

2

Data at Rest Encryption

Data in Motion Encryption

Physical Data

Virtual Data

Data in the Cloud

Applications

SaaS Apps

CONTROL ACCESS

1

Strong Authentication

Internal Users + Administrators

Cloud Providers Admins/Superusers

Customers + Partners

SECURE & MANAGE KEYS

3

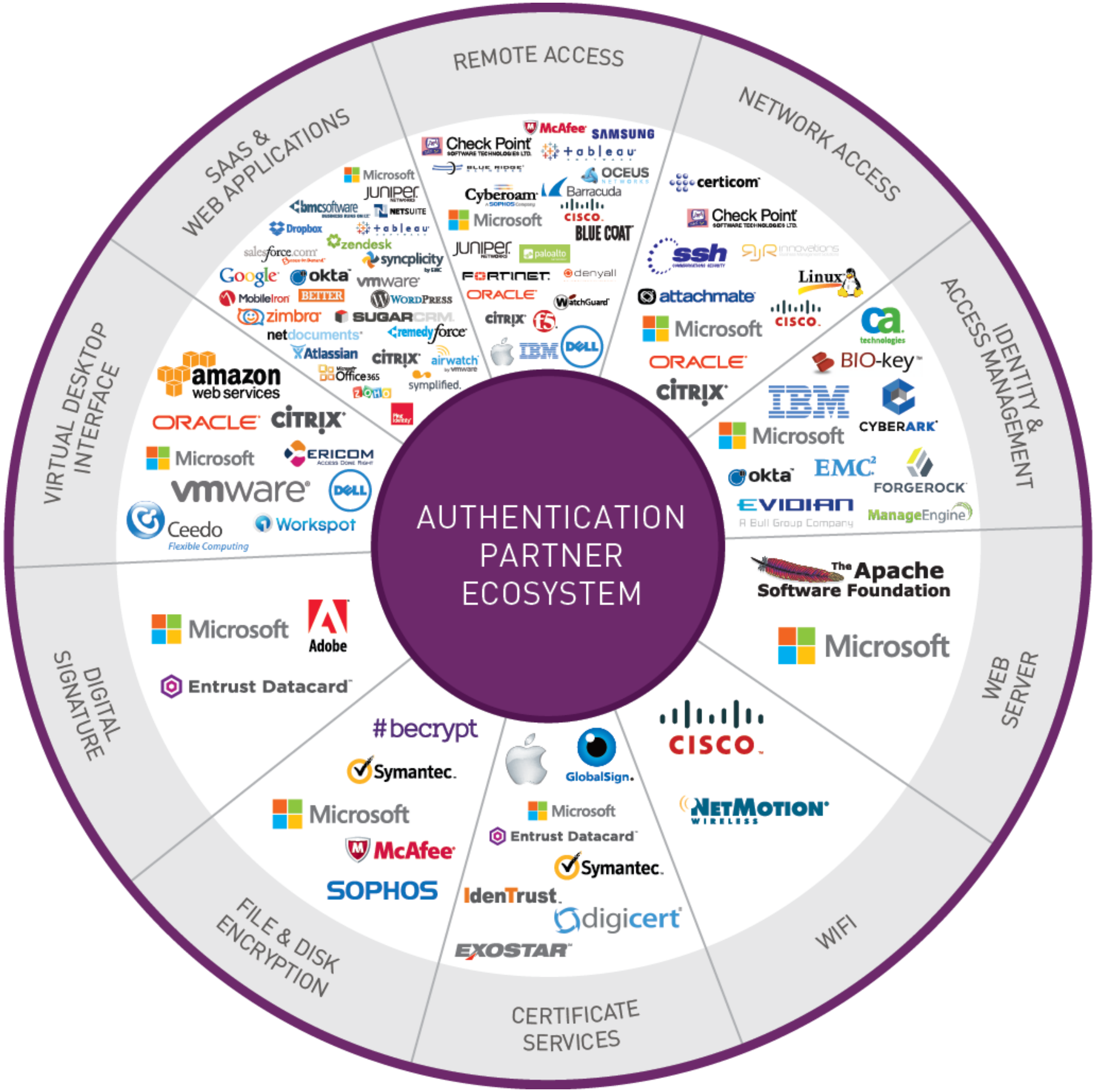
Crypto Management

Key Manager

HSM

Crypto Provisioning System

May 2016:
Authentication Partner Ecosystem



AUTHENTICATION PARTNER ECOSYSTEM

REMOTE ACCESS

McAfee, Samsung, Check Point, tableau, Blue Ridge, OCEUS, Cyberoam, Barracuda, Microsoft, Cisco, Blue Coat, Juniper, paloalto, Fortinet, denyall, Oracle, WatchGuard, Citrix, F5, Apple, IBM, Dell

NETWORK ACCESS

certicom, Check Point, ssh, RJR innovations, Linux, attachmate, Microsoft, Cisco, Oracle, Citrix

IDENTITY & ACCESS MANAGEMENT

ca technologies, BIO-key, IBM, CyberArk, Microsoft, okta, EMC², ForgeRock, Evidian A Bull Group Company, ManageEngine

WEB SERVER

The Apache Software Foundation, Microsoft

WIFI

Cisco, NetMotion Wireless

CERTIFICATE SERVICES

Apple, GlobalSign, Microsoft, Entrust Datacard, Symantec, IdenTrust, digicert, Exostar

FILE & DISK ENCRYPTION

#becrypt, Symantec, Microsoft, McAfee, Sophos

DIGITAL SIGNATURE

Microsoft, Adobe, Entrust Datacard

VIRTUAL DESKTOP INTERFACE

amazon web services, Oracle, Citrix, Microsoft, Ericom, vmware, Dell, Ceedo Flexible Computing, Workspot

SAAS & WEB APPLICATIONS

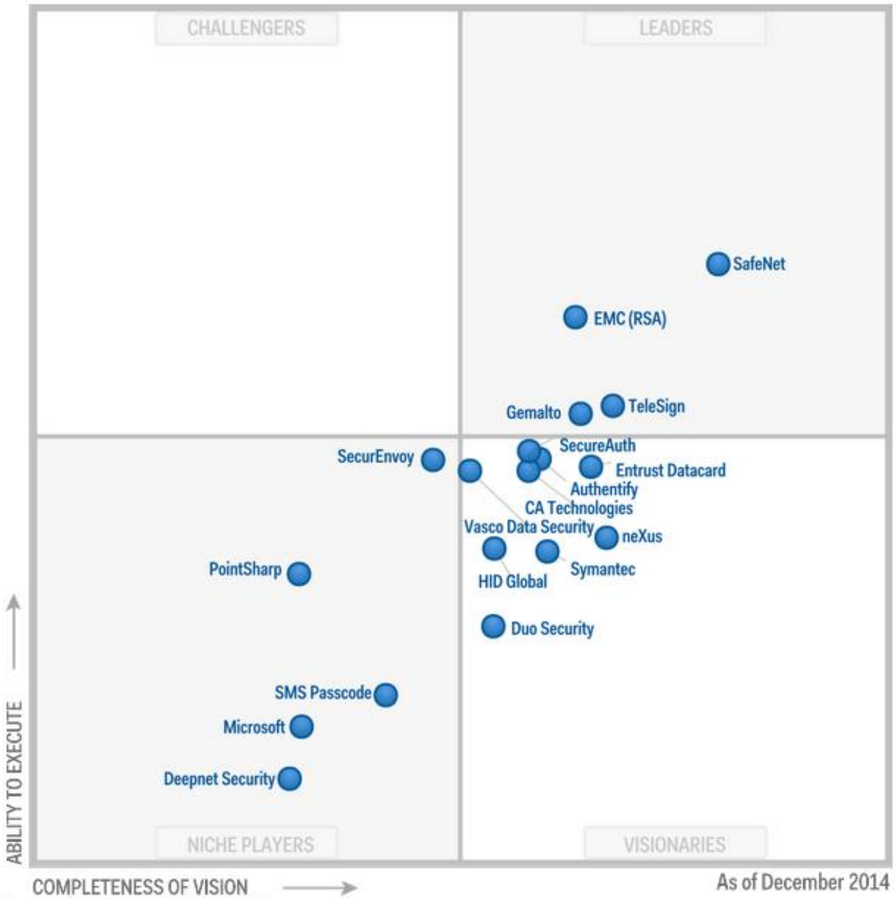
Microsoft, Juniper, bmcsoftware, NetSuite, Dropbox, tableau, zendesk, salesforce.com, syncplicity, Google, okta, vmware, MobileIron, Better, WordPress, zimbra, SugarCRM, netdocuments, remedyforce, Atlassian, Citrix, airwatch, Office365, symplified, zoho, Ping Identity

241

Authentication Integrations

We are leaders in the Authentication Market

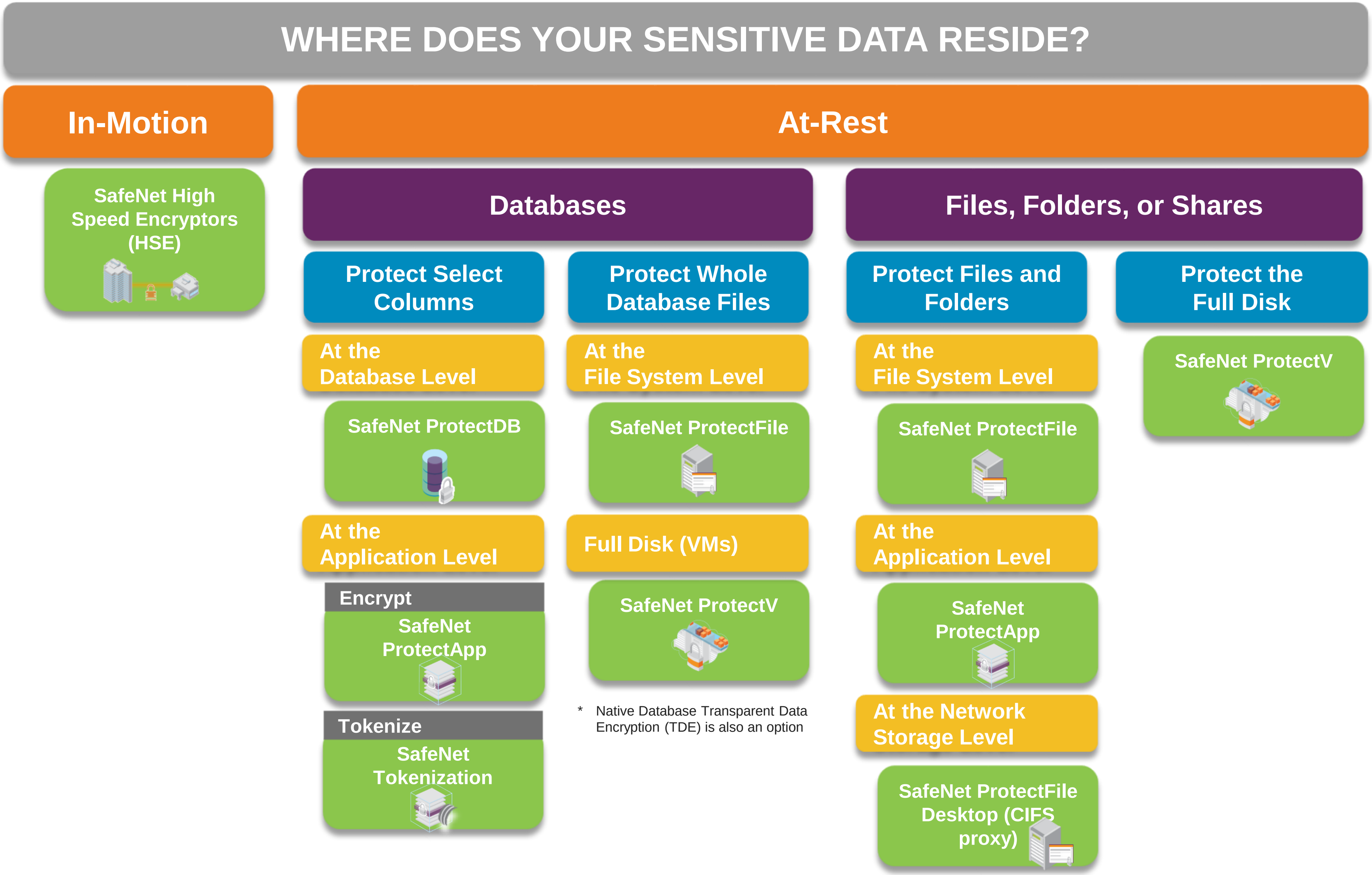
“[SafeNet] demonstrated a very sound market understanding and very strong product strategy and innovation.” - *Gartner*



Source: Gartner (December 2014)

Encrypt and Tokenize the Data

Encryption Product Selector Snapshot



WHERE DOES YOUR SENSITIVE DATA RESIDE?

- In-Motion
  - SafeNet High Speed Encryptors (HSE)
- At-Rest
  - Databases
    - Protect Select Columns
      - At the Database Level
        - SafeNet ProtectDB
      - At the Application Level
        - Encrypt
          - SafeNet ProtectApp
        - Tokenize
          - SafeNet Tokenization
    - Protect Whole Database Files
      - At the File System Level
        - SafeNet ProtectFile
      - Full Disk (VMs)
        - SafeNet ProtectV
  - Files, Folders, or Shares
    - Protect Files and Folders
      - At the File System Level
        - SafeNet ProtectFile
      - At the Application Level
        - SafeNet ProtectApp
      - At the Network Storage Level
        - SafeNet ProtectFile Desktop (CIFS proxy)
    - Protect the Full Disk
      - SafeNet ProtectV

* Native Database Transparent Data Encryption (TDE) is also an option

Database and File Protection Options

Physical/Virtual/Cloud

SQL Database Encryption

ProtectApp
Application level encryption

Tokenization
Application level tokenization

ProtectDB
Transparent column level encryption

ProtectFile
Transparent database file encryption

TDE
Transparent data encryption

NoSQL Database

ProtectApp
Application level encryption

Tokenization
Application level tokenization

ProtectFile
Transparent database file encryption

File/Folder/Share Encryption (DAS/NAS/SAN)

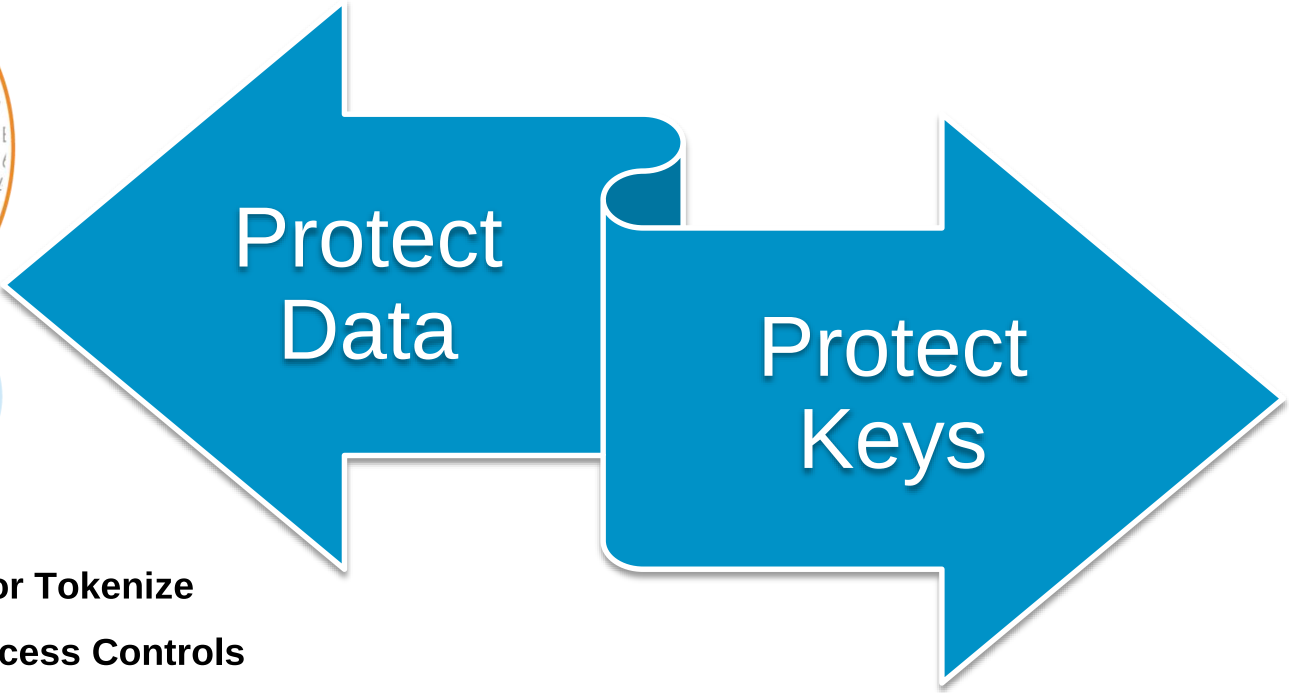
ProtectFile
Transparent file encryption at the file-system level

ProtectApp
Multi-purpose APIs to perform data encryption, including file encryption at the application level

Customer-Owned Key Management

SafeNet KeySecure | Physical
SafeNet Virtual KeySecure | Cloud/Virtual

Data Protection Best Practices



- Encrypt or Tokenize
- Apply Access Controls

- Manage Key Lifecycle
- Apply Access Controls

Decouple KEYS from DATA

GDPR Text

- SECTION 2: DATA SECURITY
- ARTICLE 30: Security of processing

1. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall **implement appropriate technical and organisational measures**, to ensure a level of security appropriate to the risk, including inter alia, as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

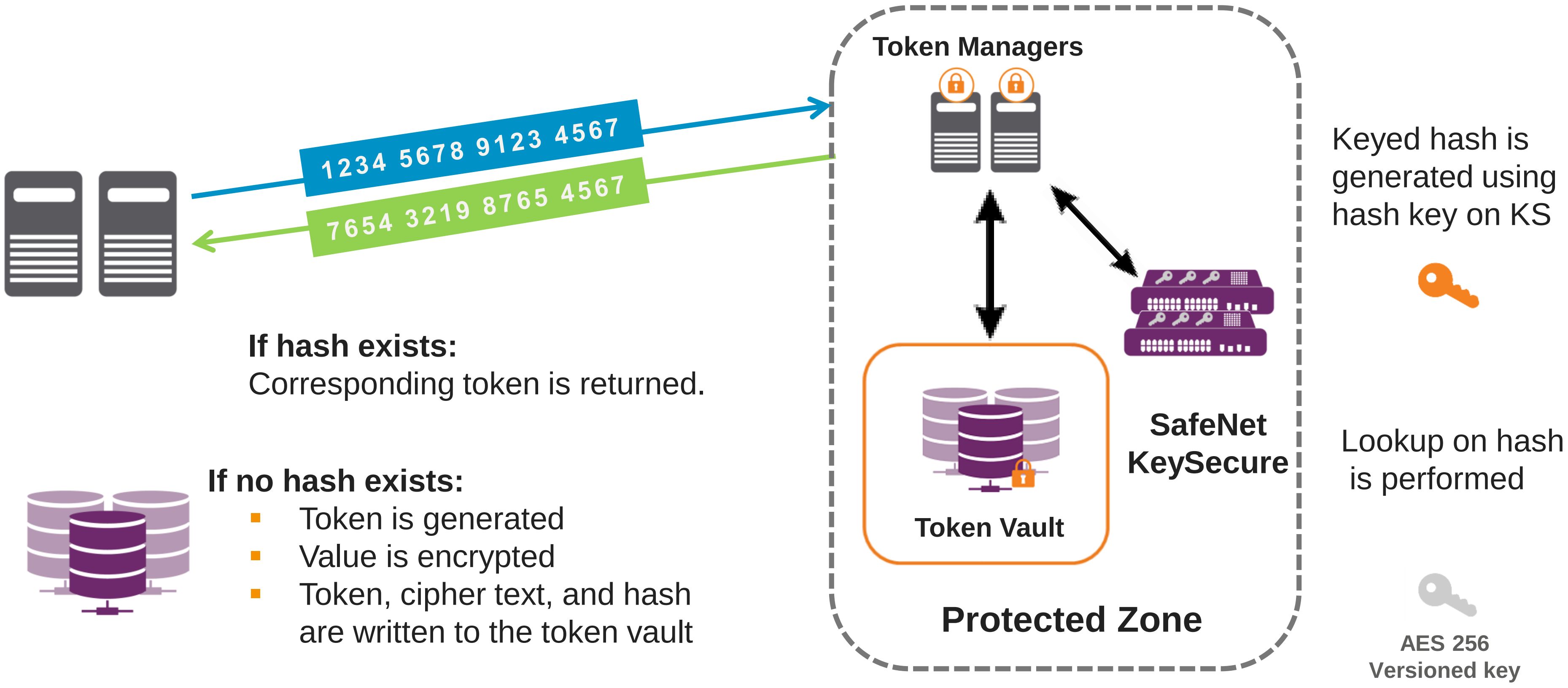
Privacy By Design

1a. In **assessing** the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Privacy Impact Assessment

Tokenization

Token generation: Plaintext (sensitive information) is sent by application with request for tokenization



If hash exists:
Corresponding token is returned.

If no hash exists:

- Token is generated
- Value is encrypted
- Token, cipher text, and hash are written to the token vault

De-tokenization: Token is sent by application with request for plaintext value (Get Token)

- Token is looked up
- Corresponding ciphertext is decrypted and sent back to the application

Reducing Audit Scope:

Requirements

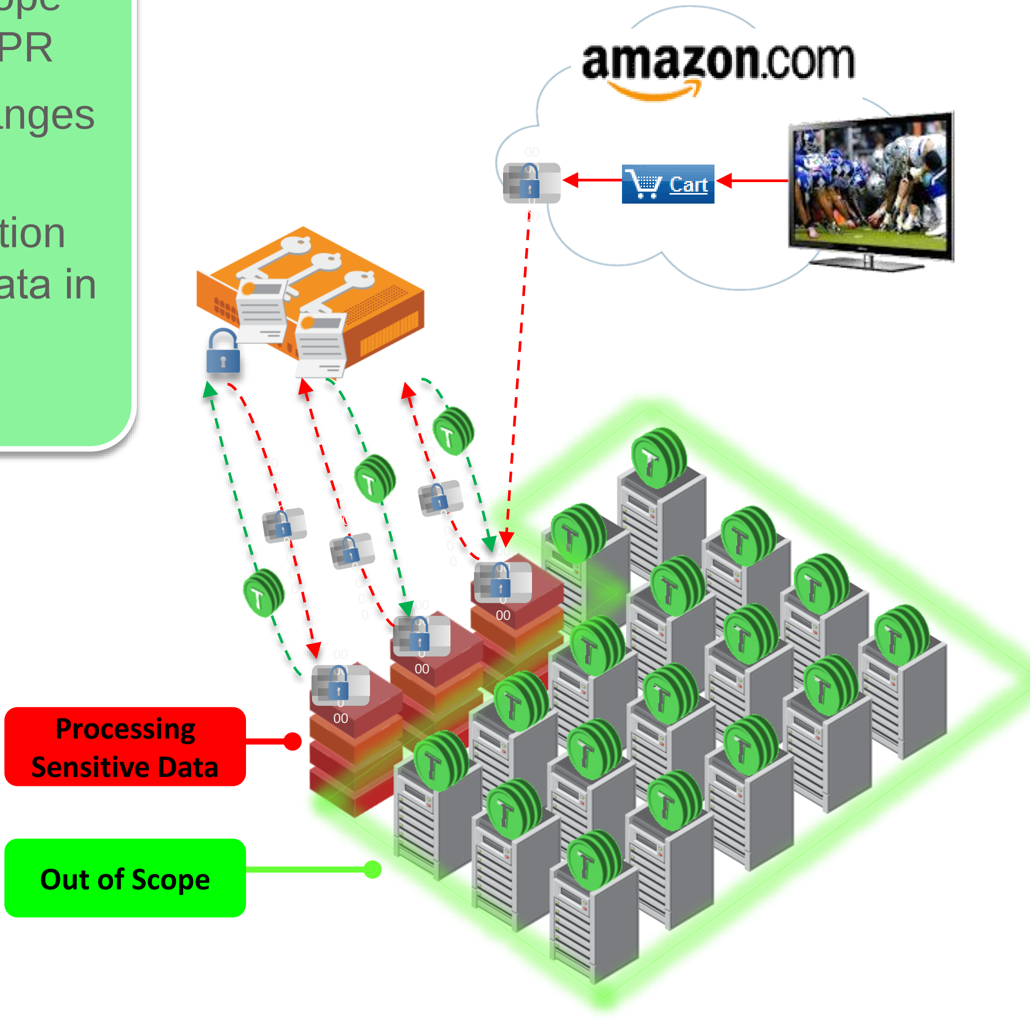
- Systems with tokens are taken out of scope of compliance audits such as PCI or GDPR
- Data protection is "transparent" – no changes to database tables or file layouts
- Format preserving—meaning no application changes for systems that don't handle data in the clear
- Wide support of various data types

Features

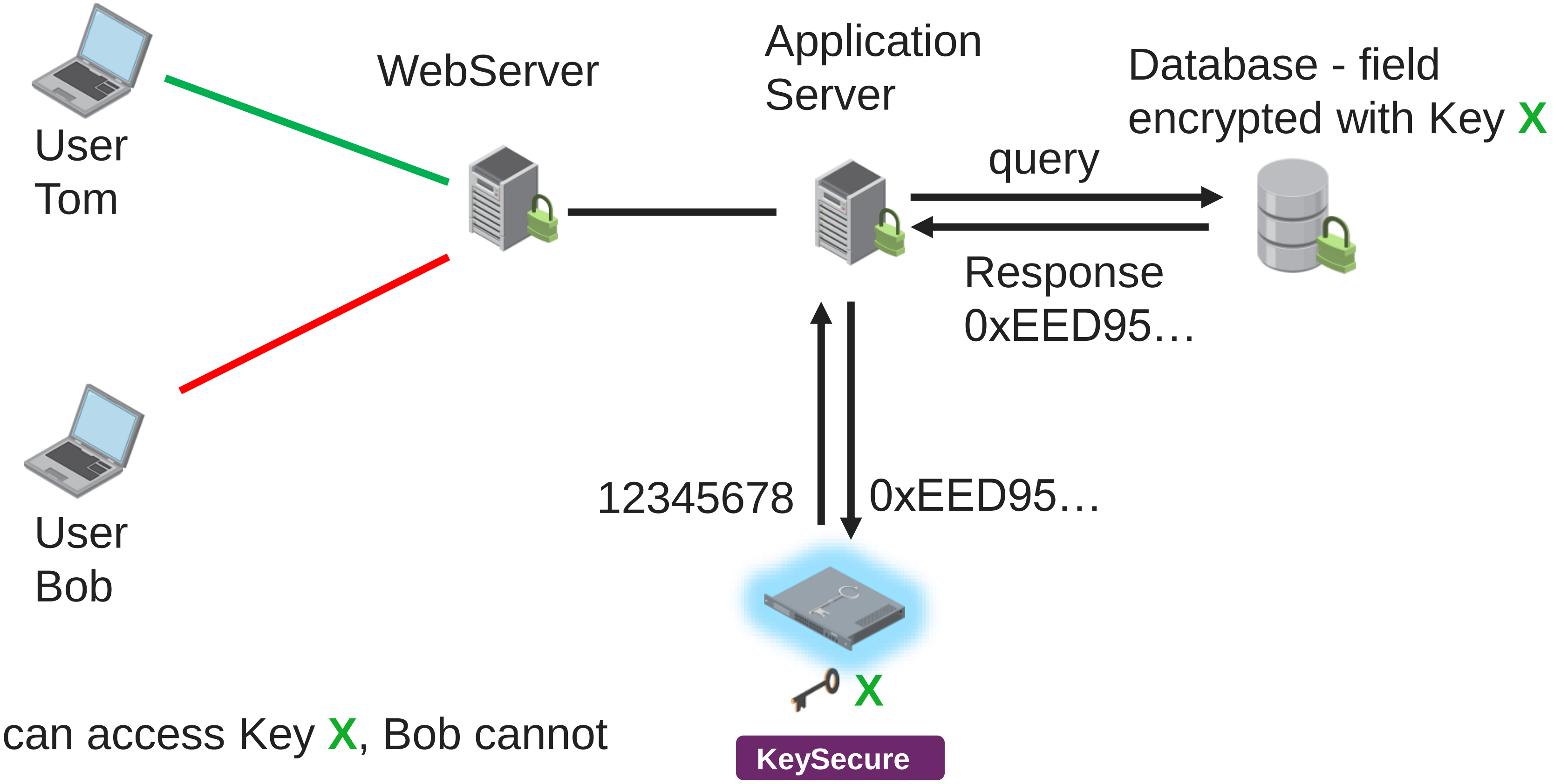
- Replacement of sensitive data with data of a similar size that is not sensitive (a "token")

1234 5678 9123 4567

- 1-to-1 mapping of tokens to sensitive data
- Customization of token formats

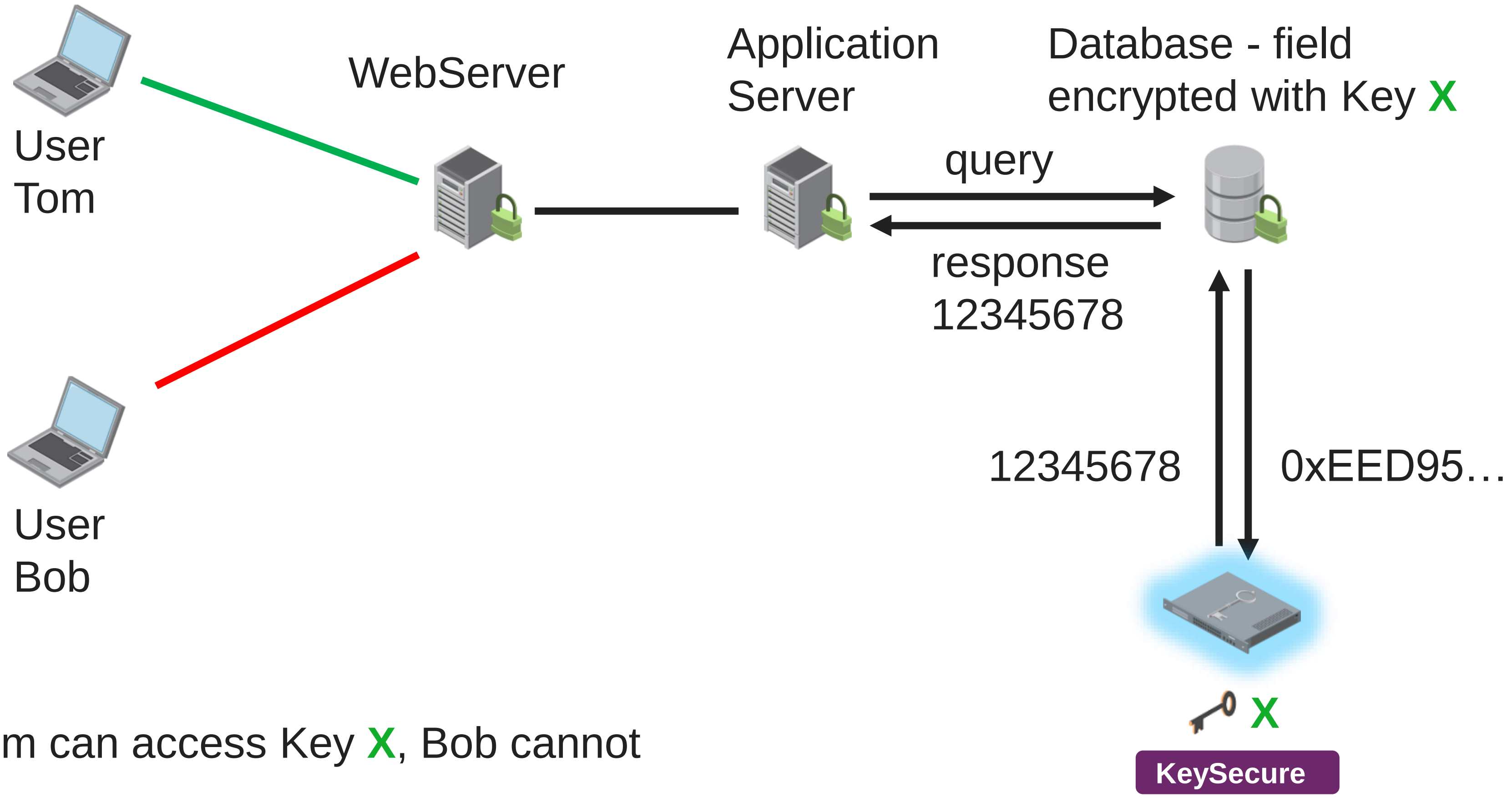


ProtectApp in Action



Tom can access Key X, Bob cannot

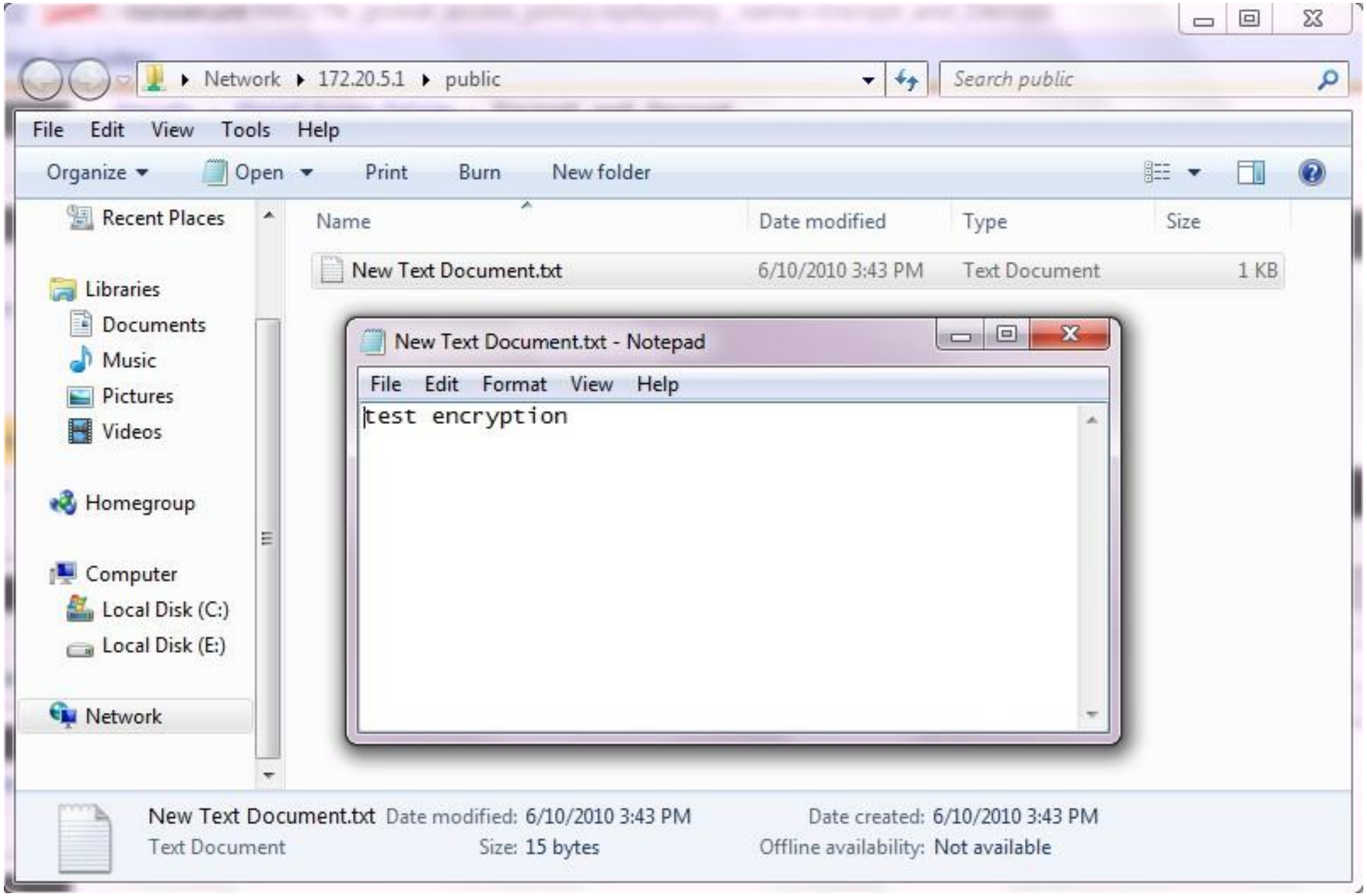
ProtectDB in Action



Tom can access Key X, Bob cannot

File Encryption Access Level – sample I

- User with Encrypt & Decrypt permissions


Network ▸ 172.20.5.1 ▸ public
Search public
File Edit View Tools Help
Organize ▾ Open ▾ Print Burn New folder
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Local Disk (E:)
Network
New Text Document.txt - Notepad
File Edit Format View Help

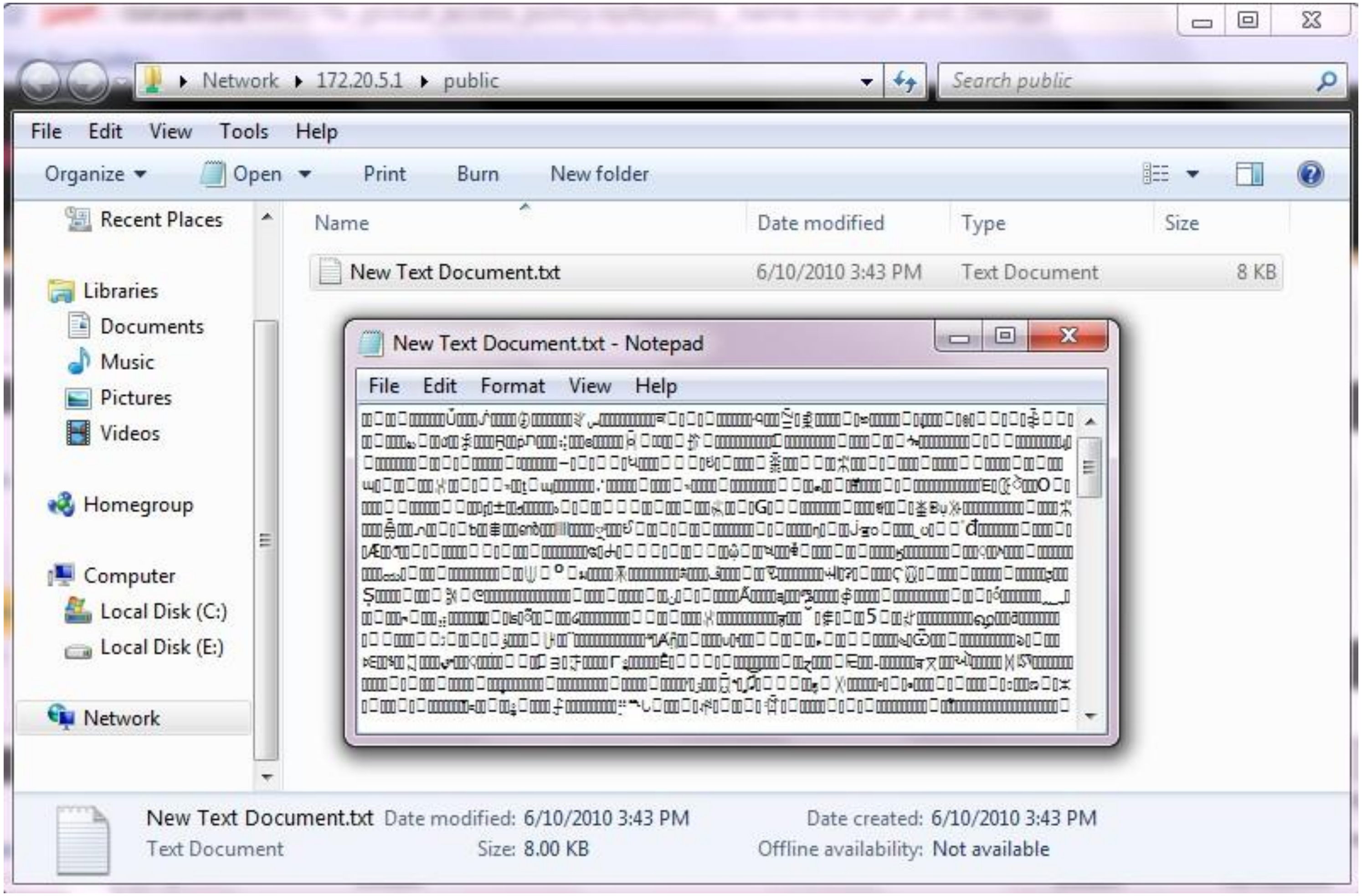
Name	Date modified	Type	Size
New Text Document.txt	6/10/2010 3:43 PM	Text Document	1 KB

```
test encryption
```

New Text Document.txt Date modified: 6/10/2010 3:43 PM Date created: 6/10/2010 3:43 PM
Text Document Size: 15 bytes Offline availability: Not available

File Encryption Access Level – sample II

- User with Backup & Restore Ciphertext permissions

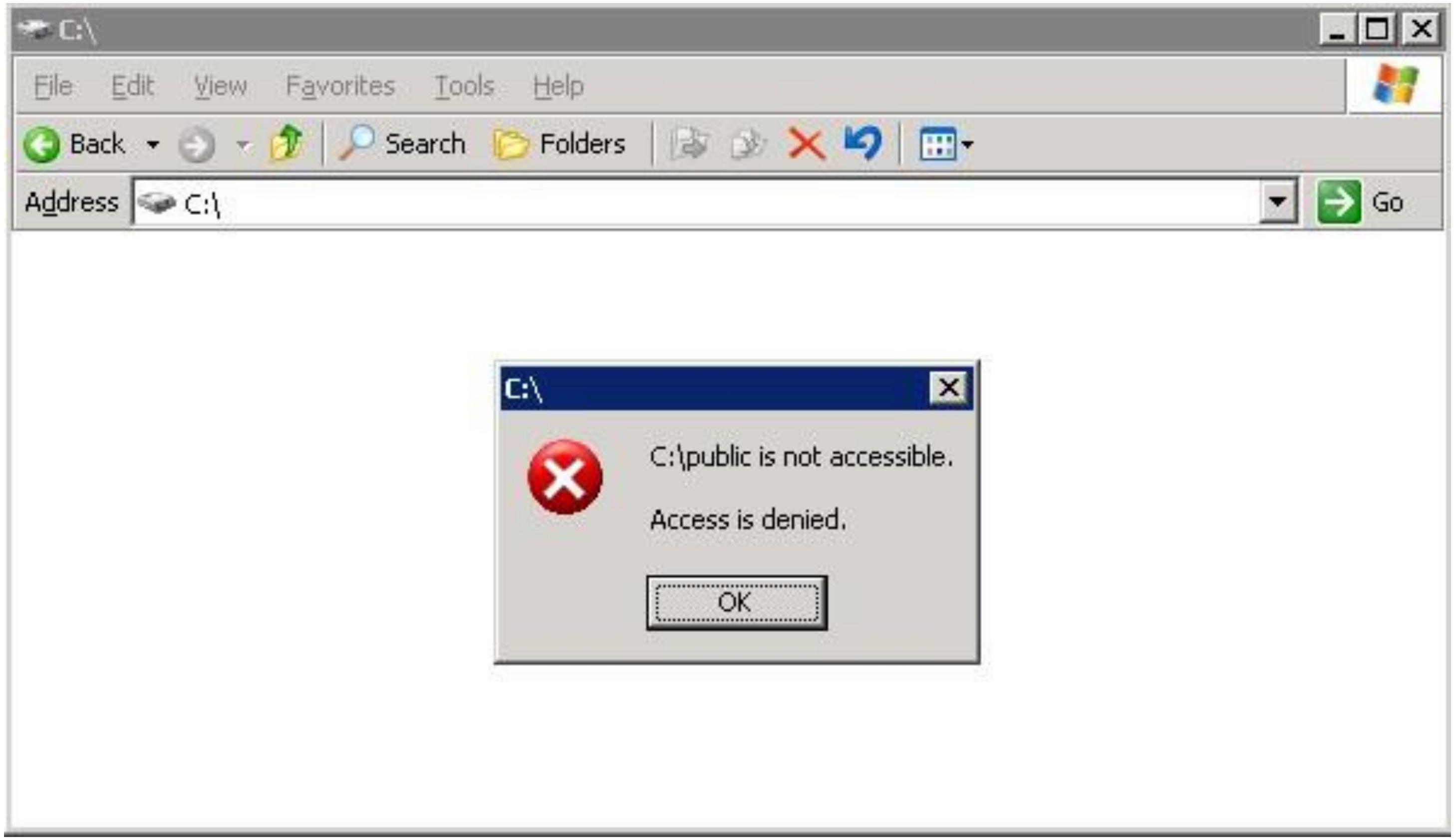

Network ▸ 172.20.5.1 ▸ public
Search public
File Edit View Tools Help
Organize Open Print Burn New folder
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Local Disk (E:)
Network
New Text Document.txt - Notepad
File Edit Format View Help

Name	Date modified	Type	Size
New Text Document.txt	6/10/2010 3:43 PM	Text Document	8 KB

New Text Document.txt Date modified: 6/10/2010 3:43 PM Date created: 6/10/2010 3:43 PM
Text Document Size: 8.00 KB Offline availability: Not available

File Encryption Access Level – sample III

- User with No Access permissions



C:\

C:\public is not accessible.

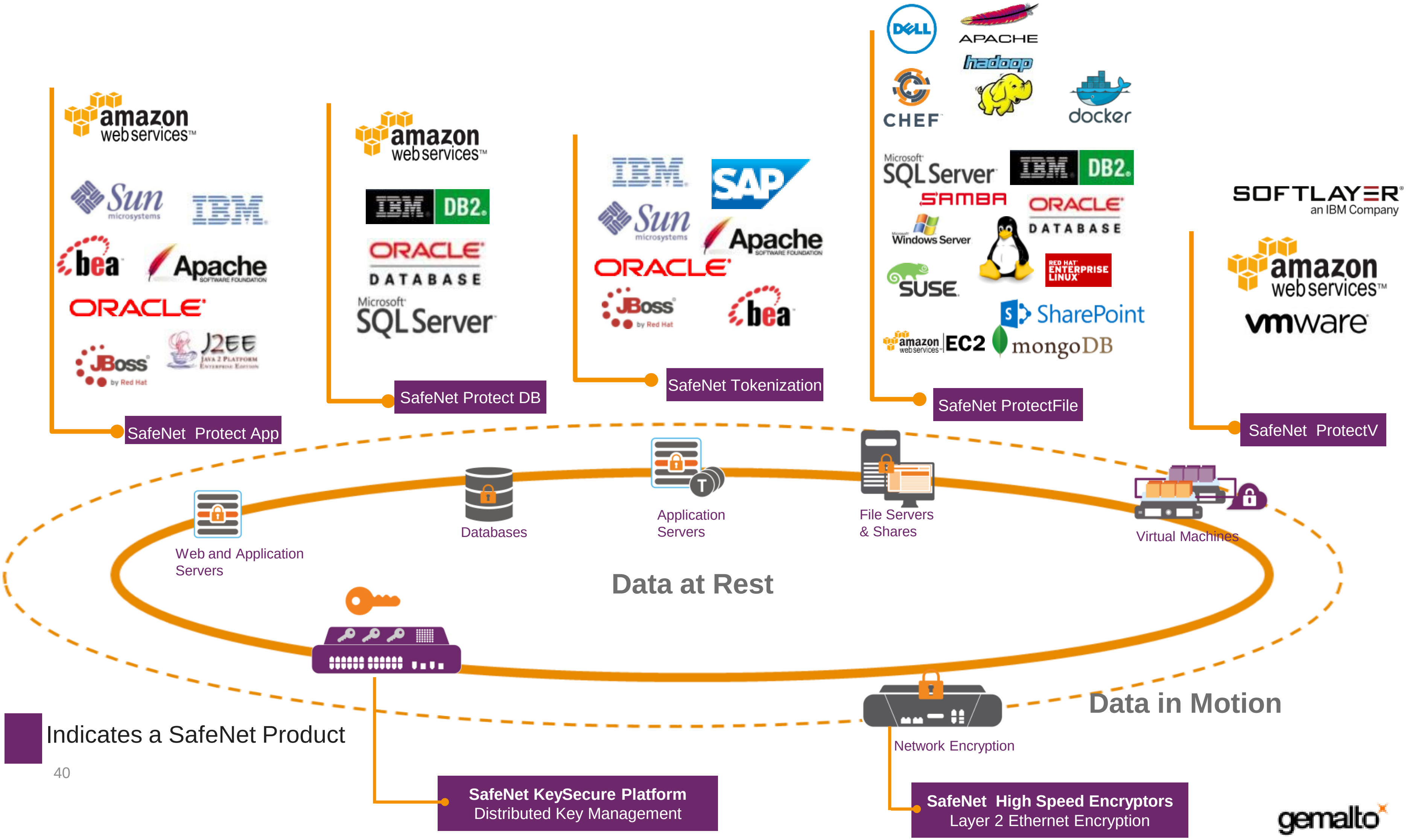
Access is denied.

OK

gemalto

Gemalto Encryption Ecosystem

Offers the industry's most expansive ecosystem of integrations for encrypting data within third party environments



SafeNet Protect App

SafeNet Protect DB

SafeNet Tokenization

SafeNet ProtectFile

SafeNet ProtectV

Web and Application Servers

Databases

Application Servers

File Servers & Shares

Virtual Machines

Data at Rest

Data in Motion

Network Encryption

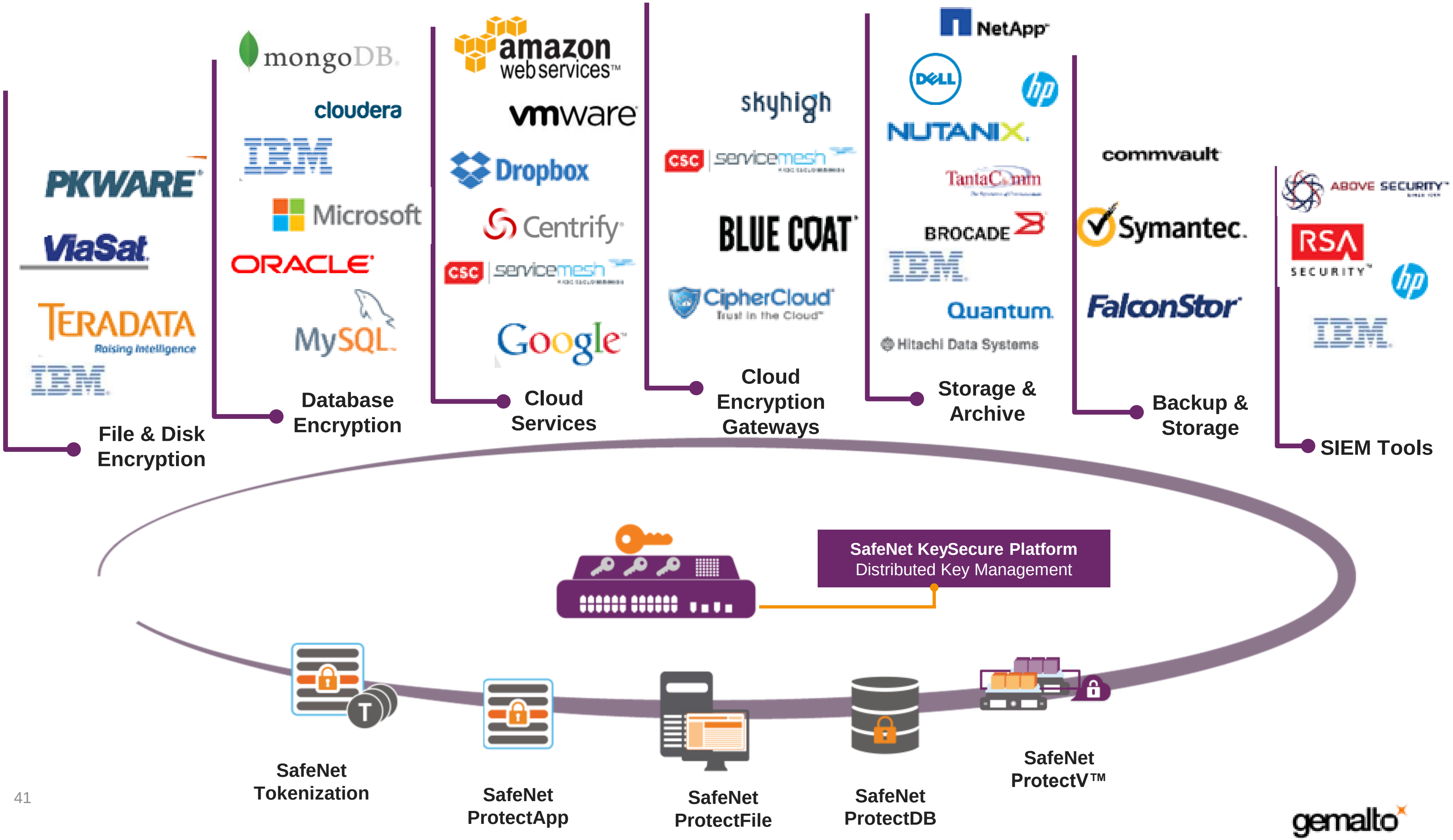
SafeNet KeySecure Platform
Distributed Key Management

SafeNet High Speed Encryptors
Layer 2 Ethernet Encryption

Indicates a SafeNet Product

Gemalto Key Management Ecosystem

The industry's most expansive and diverse ecosystem of integrations including the largest # of KMIP integration products



gemalto

732

Integrations

246

Different Vendors

Gemalto IDP:
The largest ecosystem of any security company

Why Customers Choose Gemalto Identity & Data Protection?

1

Breadth of Portfolio

The only security vendor to offer and end-to-end offering for protecting the entire data lifecycle. More ways to protect data than any other vendor- in Databases, Applications, File Servers, Mainframes, Desktops, and more.

2

Expansive Ecosystem

The industry's largest ecosystem of technology integrations for enabling encryption, key management, and strong authentication for 3rd party applications and technologies.

3

Certifications and Recognized Leadership

Gemalto has more FIPS 140-2 and Common Criteria certifications than any vendor, giving peace of mind to our customers.

4

Proven Execution

Proven track record of protecting critical data and transactions –trillions of dollars in bank transfers, stored streaming videos, and from M1 tanks to Air Force One. For the largest enterprise deployments - dedicated hardware and optimized software scales to millions of protected records and trillions of transactions.

ευχαριστώ

gemalto
security to be free