Why Gemalto with F5

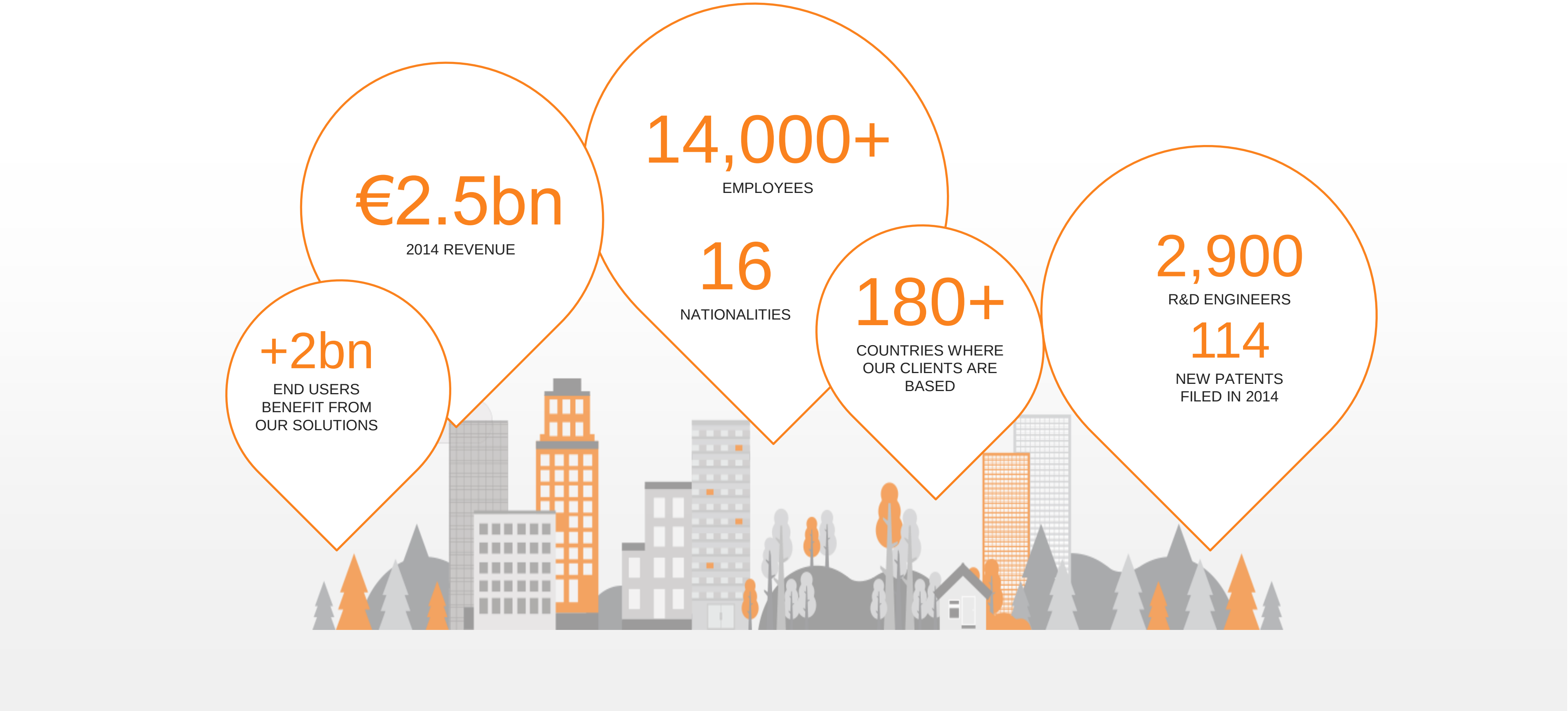
Trust. Every day.

gemalto
security to be free

Matija Mandarić, Presales Engineer, Veracomp

February 2017

We are the world leader in digital security



€2.5bn
2014 REVENUE

+2bn
END USERS BENEFIT FROM OUR SOLUTIONS

14,000+
EMPLOYEES

16
NATIONALITIES

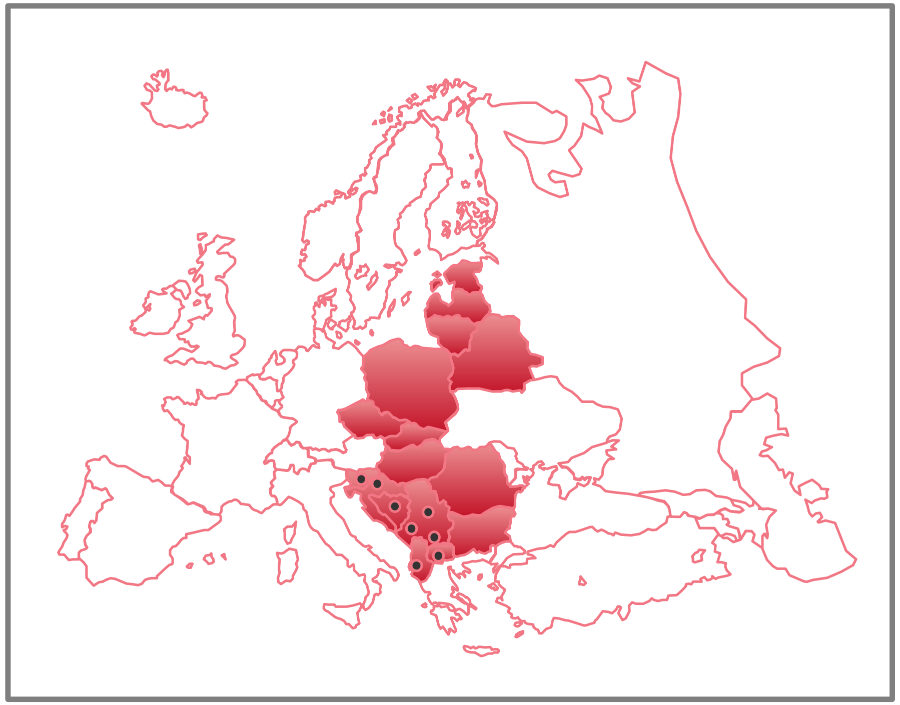
180+
COUNTRIES WHERE OUR CLIENTS ARE BASED

2,900
R&D ENGINEERS

114
NEW PATENTS FILED IN 2014

WE’RE UNIQUE. WE’RE GLOBAL. WE’RE INNOVATIVE

Veracomp Adriatics – brief overview



- 32 full-time employees
- Covering 8 countries: Albania, Bosnia and Herzegovina, Croatia, Kosovo, Macedonia, Montenegro, Serbia, Slovenia
- 5 regional offices (Beograd, Ljubljana, Rijeka, Sarajevo, Zagreb)
- 15+ distributions
- Value Added Distributor since 2001
- Trend Micro Authorized training center (ATC)
- Blue Coat, Polycom, Gigamon support provider

TREND MICRO
BLUE COAT
gemalto
proofpoint

Q4/2013
Mack IT becomes part of Veracomp group

extreme networks
lifesize

2014

Polycom

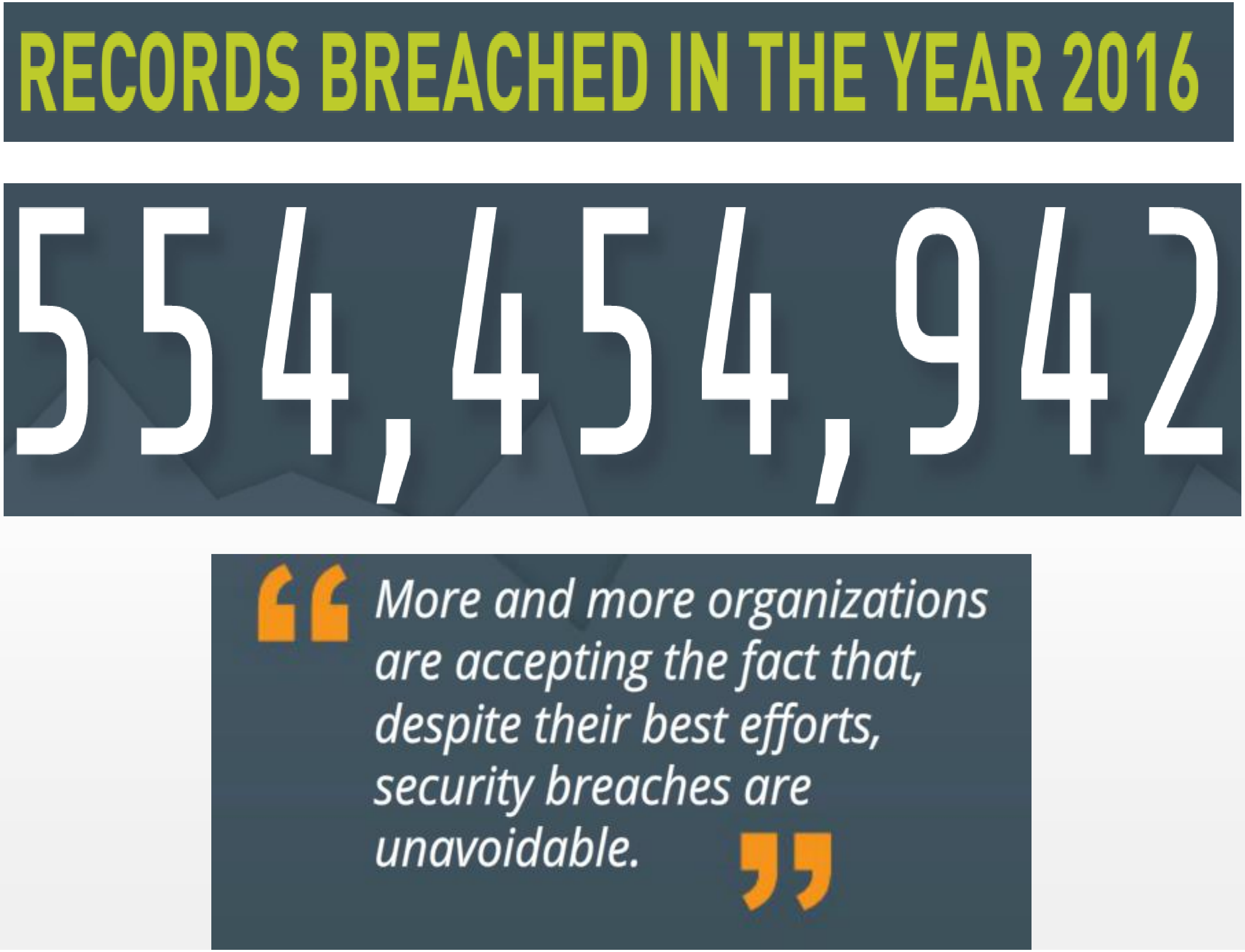
2015
New Zagreb office

HUAWEI
f5
Entrust Datacard
Gigamon

2016
Serbian office
Slovenian office

Hewlett Packard Enterprise
redhat
tenable network security

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

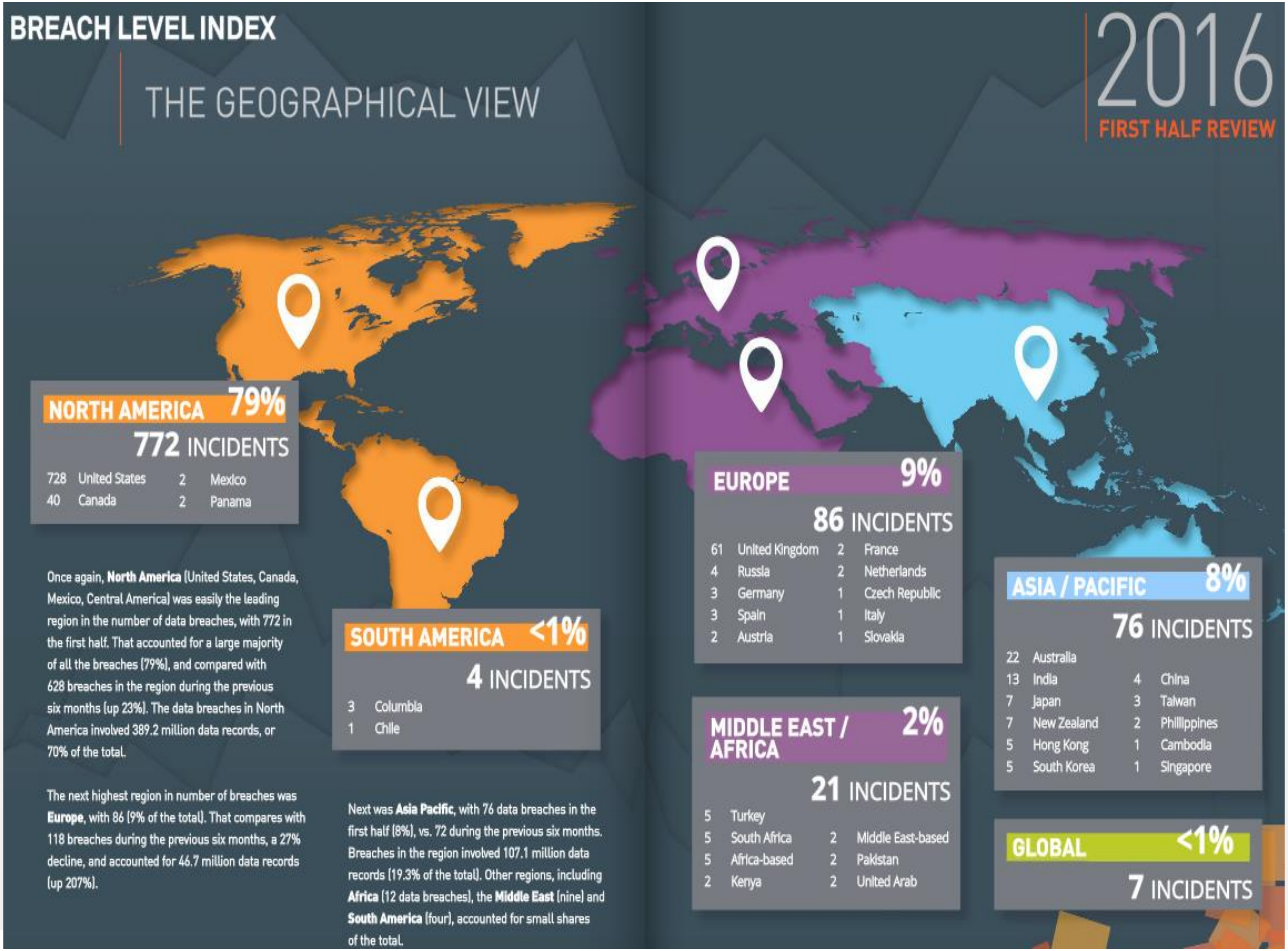
974

NUMBER OF BREACHES WITH OVER 1 MILLION RECORDS AFFECTED

29

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

52%



BREACH LEVEL INDEX

THE GEOGRAPHICAL VIEW

2016 FIRST HALF REVIEW

NORTH AMERICA 79%

772 INCIDENTS

728	United States	2	Mexico
40	Canada	2	Panama

SOUTH AMERICA <1%

4 INCIDENTS

3	Columbia
1	Chile

EUROPE 9%

86 INCIDENTS

61	United Kingdom	2	France
4	Russia	2	Netherlands
3	Germany	1	Czech Republic
3	Spain	1	Italy
2	Austria	1	Slovakia

MIDDLE EAST / AFRICA 2%

21 INCIDENTS

5	Turkey		
5	South Africa	2	Middle East-based
5	Africa-based	2	Pakistan
2	Kenya	2	United Arab

ASIA / PACIFIC 8%

76 INCIDENTS

22	Australia		
13	India	4	China
7	Japan	3	Taiwan
7	New Zealand	2	Phillippines
5	Hong Kong	1	Cambodia
5	South Korea	1	Singapore

GLOBAL <1%

7 INCIDENTS

Once again, **North America** (United States, Canada, Mexico, Central America) was easily the leading region in the number of data breaches, with 772 in the first half. That accounted for a large majority of all the breaches (79%), and compared with 628 breaches in the region during the previous six months (up 23%). The data breaches in North America involved 389.2 million data records, or 70% of the total.

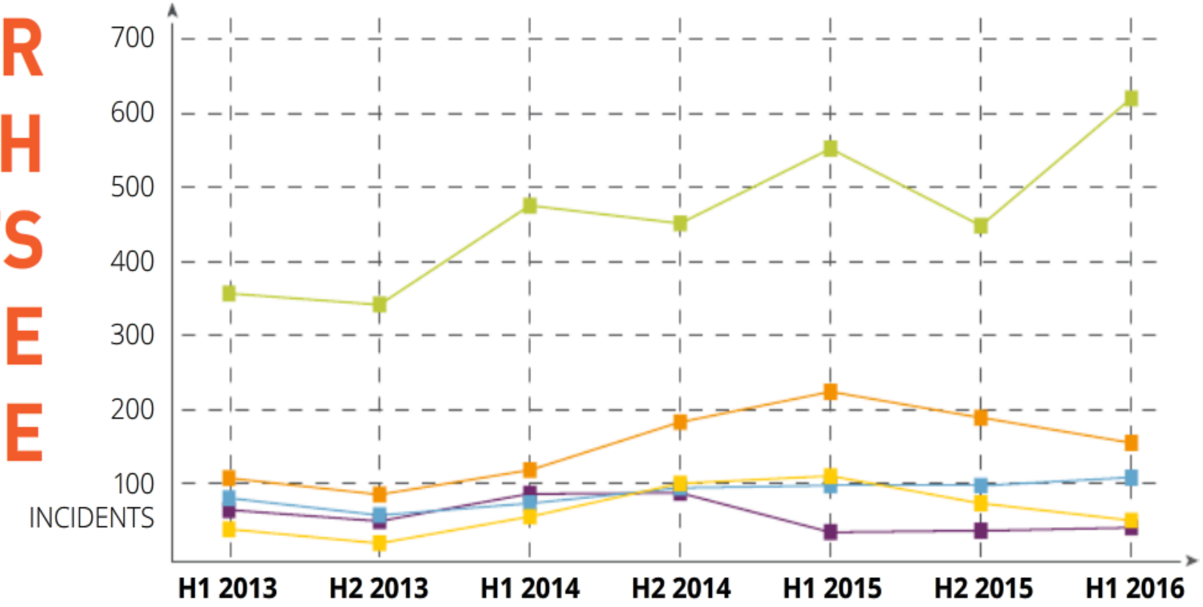
The next highest region in number of breaches was **Europe**, with 86 (9% of the total). That compares with 118 breaches during the previous six months, a 27% decline, and accounted for 46.7 million data records (up 207%).

Next was **Asia Pacific**, with 76 data breaches in the first half (8%), vs. 72 during the previous six months. Breaches in the region involved 107.1 million data records (19.3% of the total). Other regions, including **Africa** (12 data breaches), the **Middle East** (nine) and **South America** (four), accounted for small shares of the total.

No Industry is Safe –Top Breaches

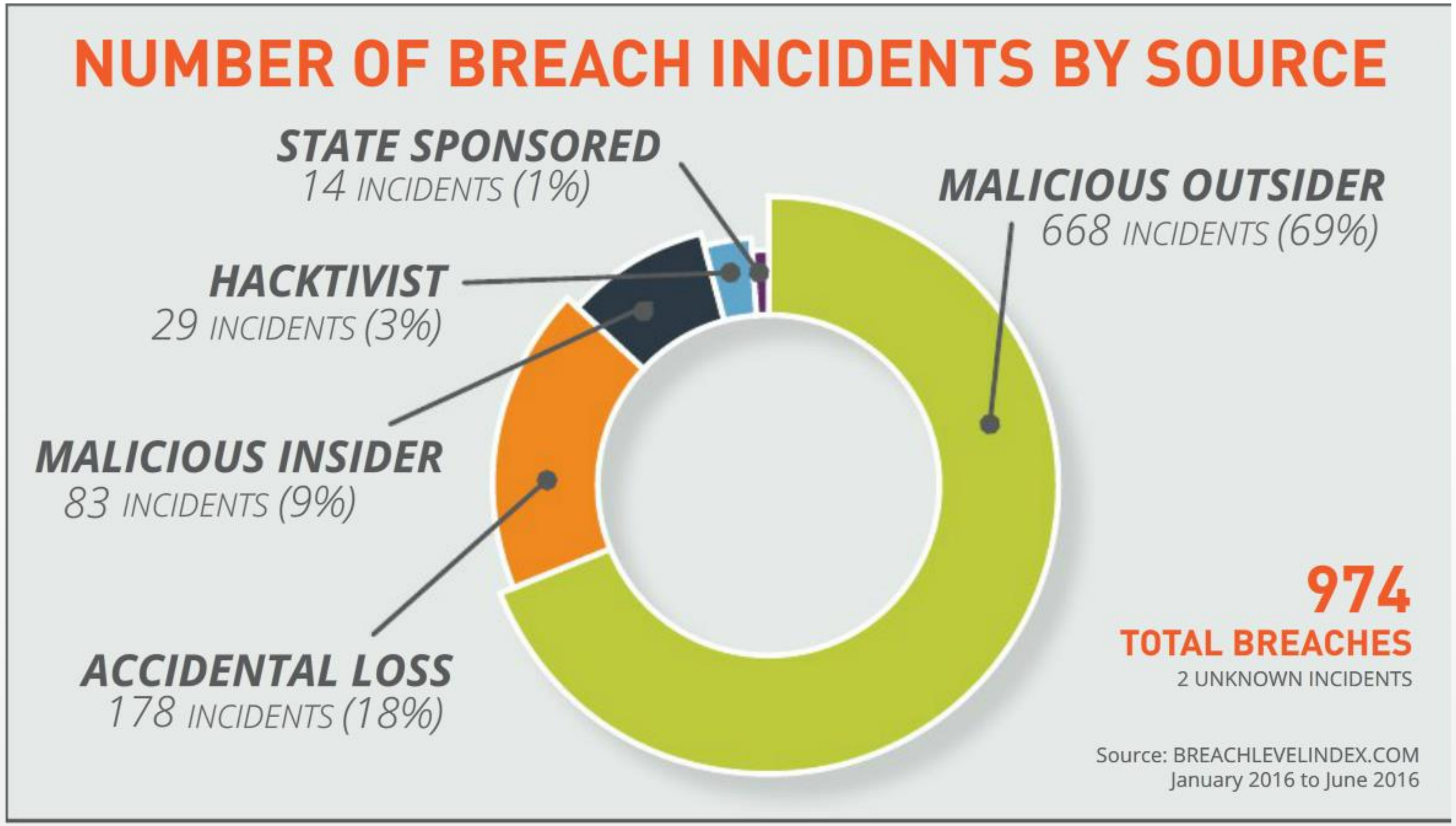
Target	Hacked	70,000,000
Home Depot	Hacked	109,000,000
JP Morgan	Hacked	83,000,000
Korea Credit	Inside	10400,000
Community Health	Hacked	4,500,000
Advocate Medical	Stolen Media	4,000,000
Adobe	Hacked	152,000,000
Yahoo Japan	Hacked	22,000,000
eBay	Hacked	145,000,000
Evernote	Hacked	50,000,000
Japan Airlines	Hacked	750,000
NYC Taxis	Inside	52,000
Sony	Hacked	100 Terrabytes
Living Social	Hacked	50,000,000
Florida Courts	Stolen Media	100,000
South Africa-Police	Unknown	16,000
Vodafone	Inside	2,000,000
TerraCom	Accidental	170,000
Public Works	Hacked	Unknown

NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016
Identity Theft	357	342	476	452	553	449	621
Financial Access	107	85	118	183	224	189	155
Existential Data	38	19	55	100	110	73	50
Account Access	80	57	73	94	97	97	108
Nuisance	64	49	86	87	34	36	40

Who's responsible for attacks?



NUMBER OF BREACH INCIDENTS BY SOURCE

Source: BREACHLEVELINDEX.COM
January 2016 to June 2016

SECURE THE BREACH

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.

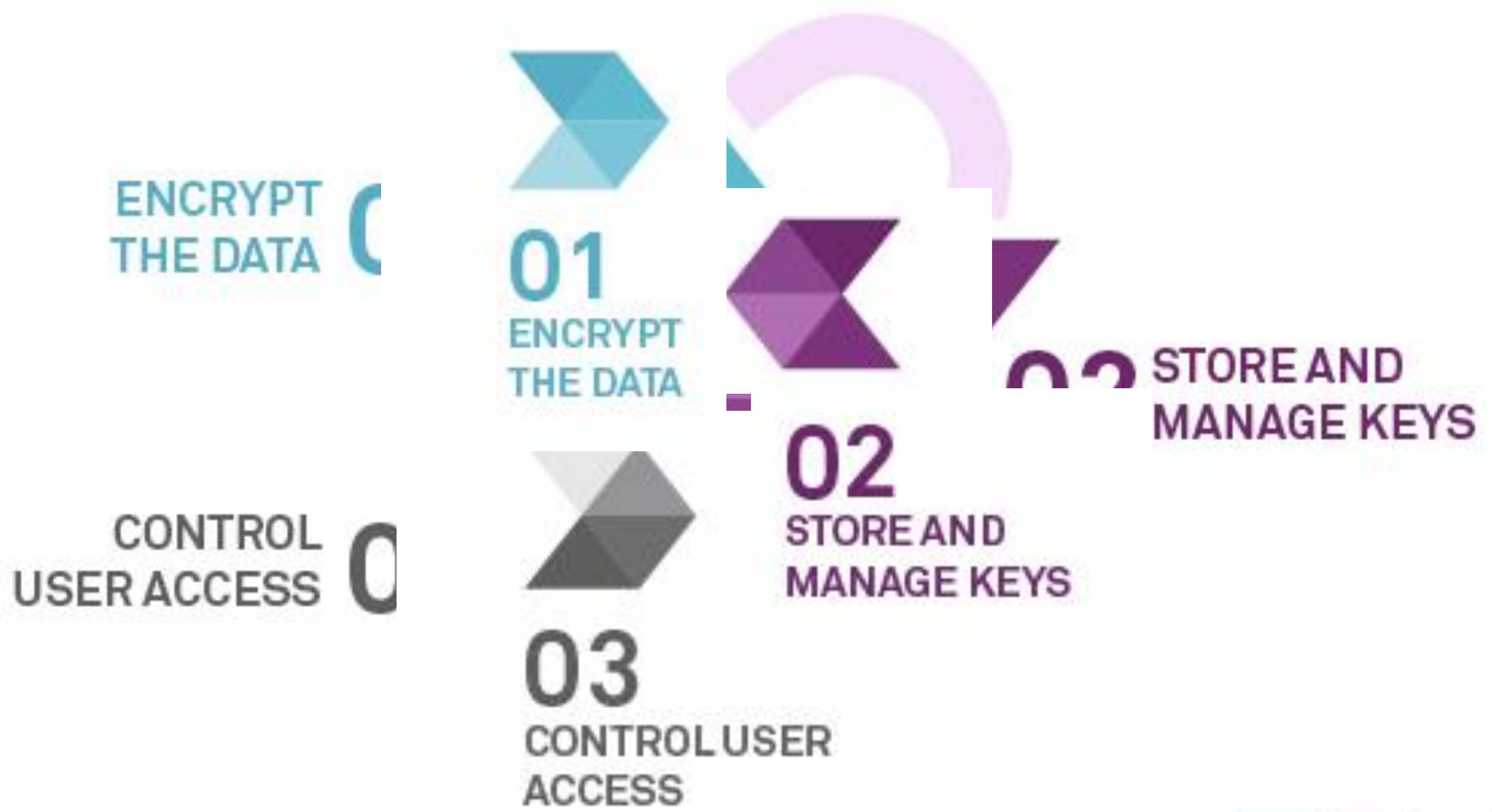
Breaches will happen – we must prepare!

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

Gemalto’s Three Step Approach



F5 APM for O365 with push OTP and ADAL - English

Matthieu Dierick

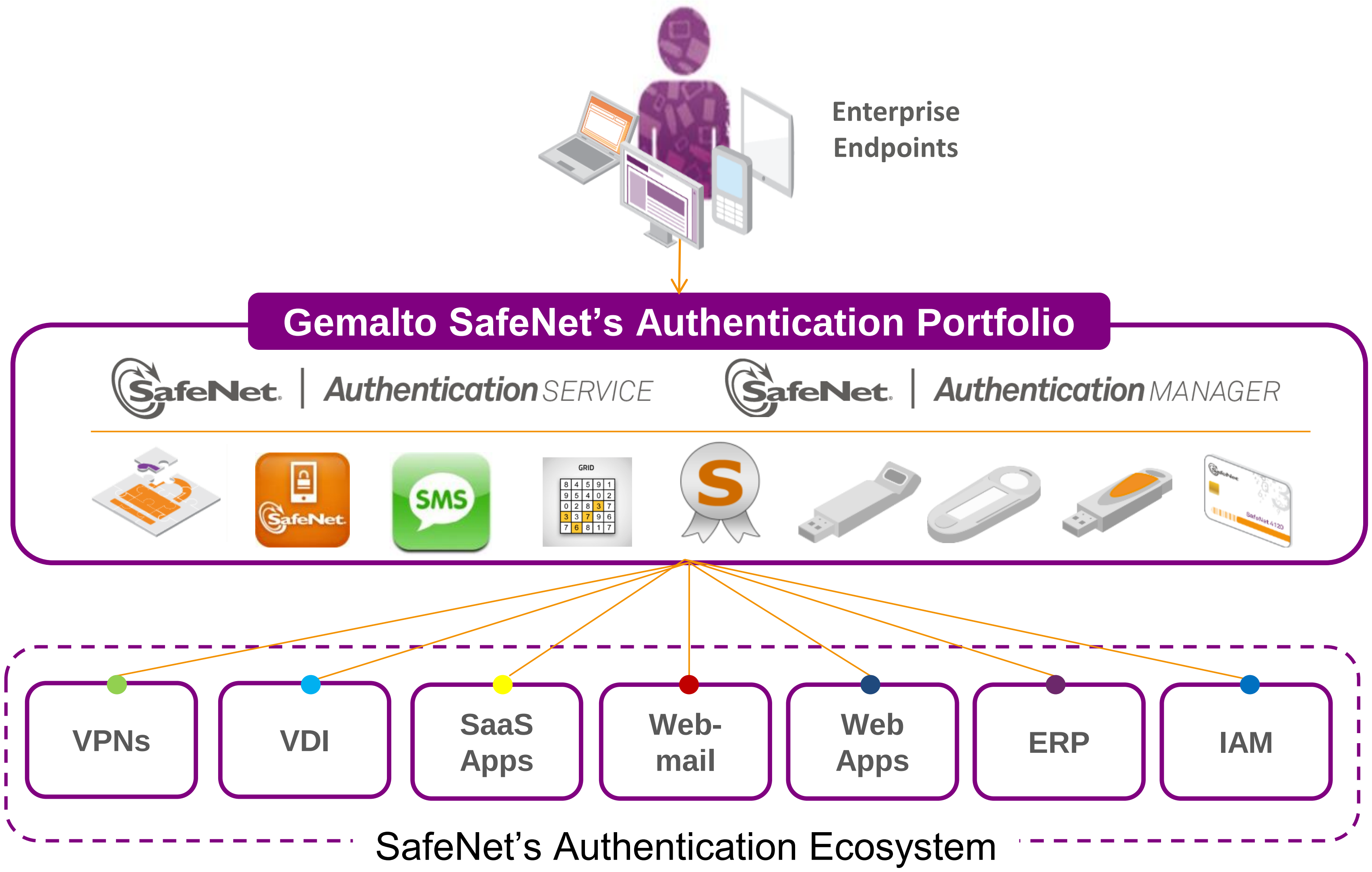
561 views

Published on Mar 8, 2016

How to enable Multi Factor Authentication on Office 365 with F5 APM as IDP.

Office 365 with Push OTP

Gemalto SafeNet Next Generation Authentication



Enterprise Endpoints

Gemalto SafeNet's Authentication Portfolio

SafeNet | Authentication SERVICE

SafeNet | Authentication MANAGER

VPNs

VDI

SaaS Apps

Web-mail

Web Apps

ERP

IAM

SafeNet's Authentication Ecosystem

Identity Protection Use Case:

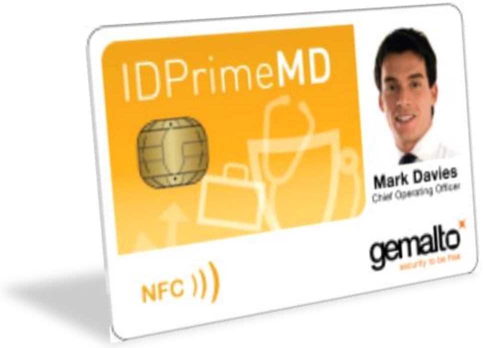
Badging. Physical and Logical Access

Customer Problem:

- Require photo ID badging
- Require central lifecycle administration of badges – provisioning, revocation, etc.
- Need to secure physical access to buildings and sites – parking, offices, etc.
- Need to offer employees electronic purse – cafeteria, coffee machines, etc.
- Need to secure access to corporate resources

Solution:

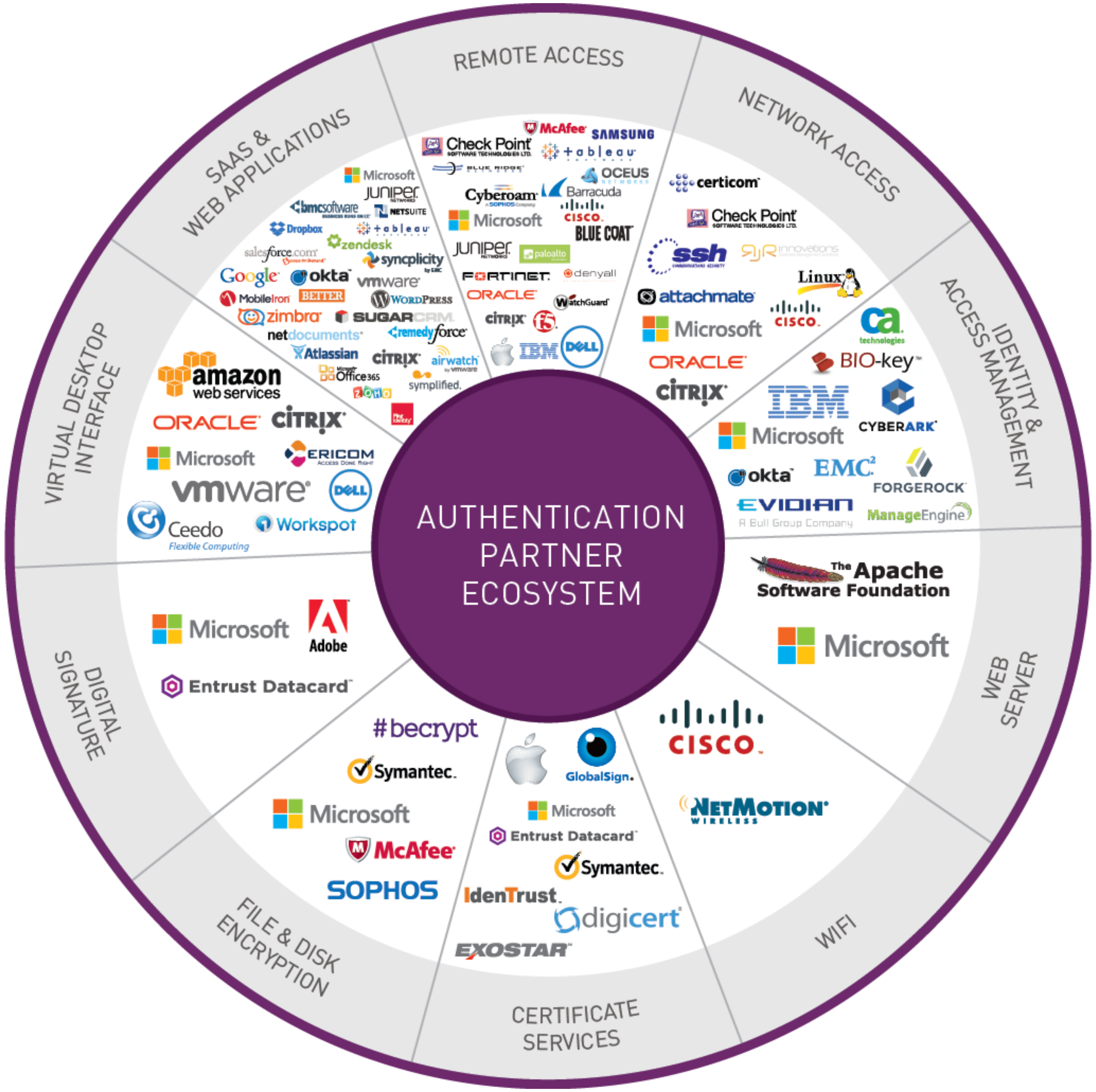
- IDPrime MD



Gemalto Advantages:

- Certificate based smart card that supports all the above:
  - Badging – photo printing
  - Physical access control
  - Lifecycle administration e-purse certificated-based authentication to resources
  - Certificate-based authentication to corporate resources
- Mobile friendly thru NFC
- Plug & play on Windows - No middleware required for deployment

May 2016:
Authentication Partner Ecosystem

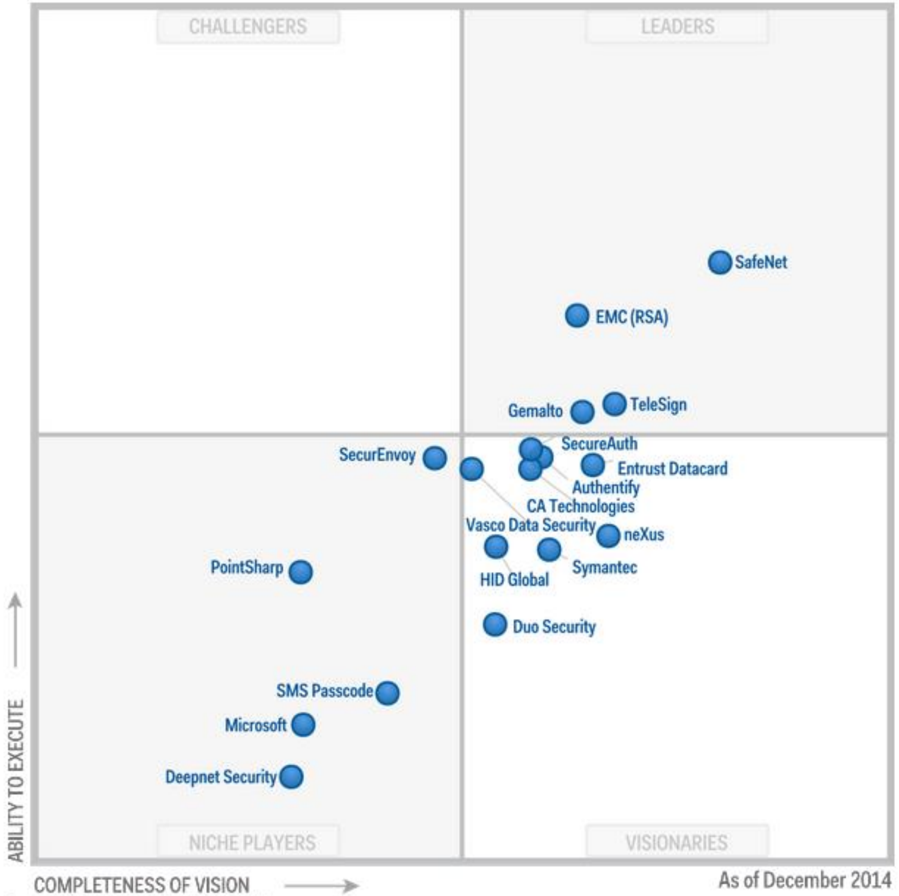


241

Authentication Integrations

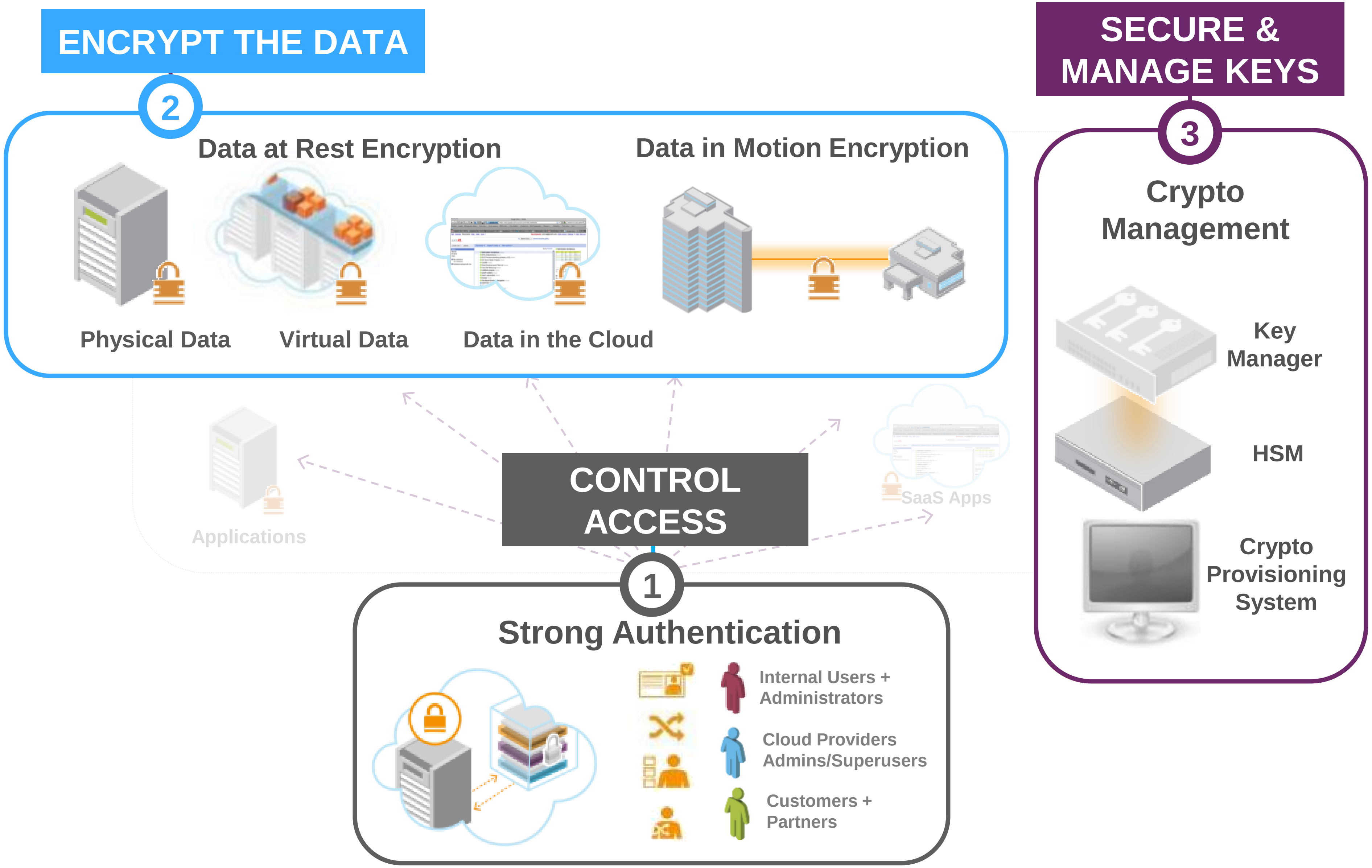
We are leaders in the Authentication Market

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



Source: Gartner (December 2014)

Protecting the Data



ENCRYPT THE DATA

2

Data at Rest Encryption

Data in Motion Encryption

Physical Data

Virtual Data

Data in the Cloud

SECURE & MANAGE KEYS

3

Crypto Management

Key Manager

HSM

Crypto Provisioning System

CONTROL ACCESS

Applications

SaaS Apps

1

Strong Authentication

Internal Users + Administrators

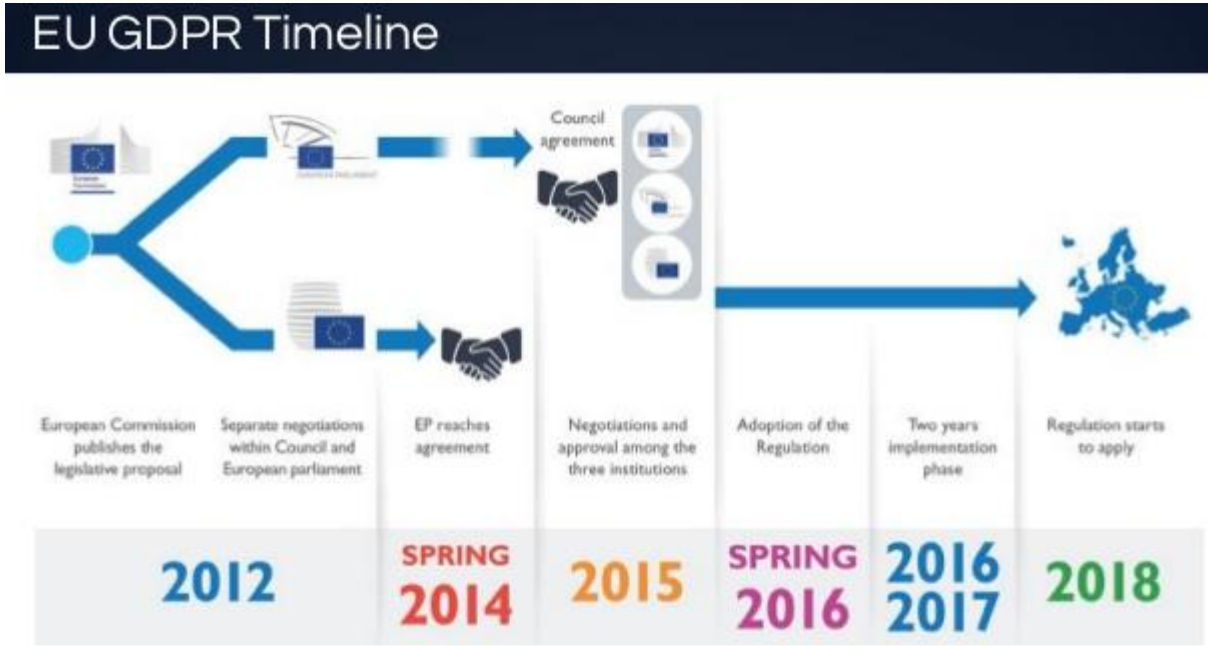
Cloud Providers Admins/Superusers

Customers + Partners

Encrypt and/or Tokenize the Data

If a business fails to comply with its data security obligations under the GDPR, it may get a fine of up to **10,000,000 EUR or 2 % of its total worldwide annual turnover** whichever is higher.

If prior to the breach taking place, the **data were rendered unintelligible**, for example by means of encryption, businesses will **not have to notify the data subjects** of the breach.


EU GDPR Timeline
Council agreement
European Commission publishes the legislative proposal
Separate negotiations within Council and European parliament
EP reaches agreement
Negotiations and approval among the three institutions
Adoption of the Regulation
Two years implementation phase
Regulation starts to apply
2012
SPRING 2014
2015
SPRING 2016
2016 2017
2018

Gemalto
3 Step Approach

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

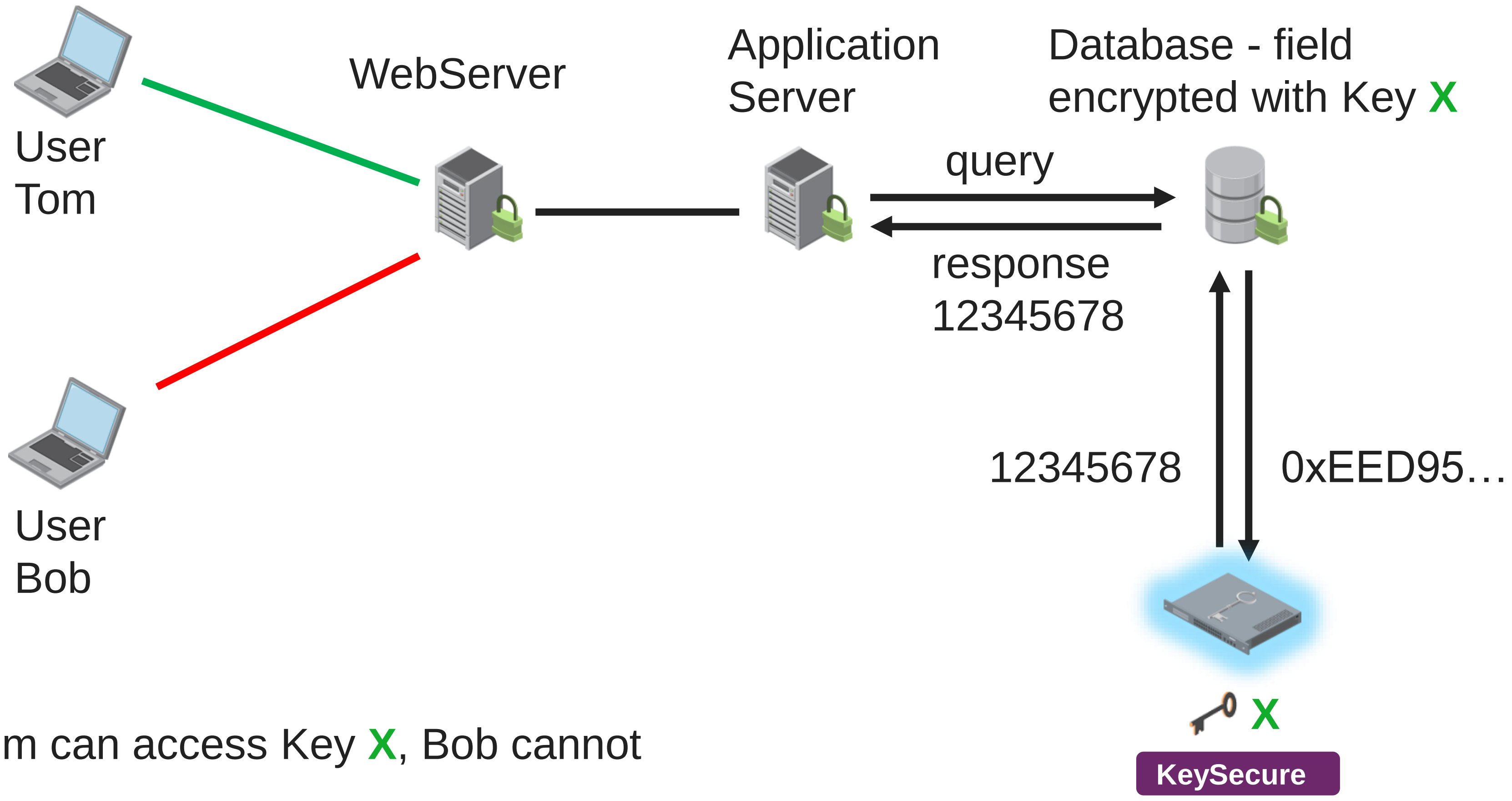
ProtectApp
Multi-purpose APIs to perform data encryption, including file encryption at the application level

+ Customer-Owned Key Management

SafeNet KeySecure | Physical
SafeNet Virtual KeySecure | Cloud/Virtual

gemalto

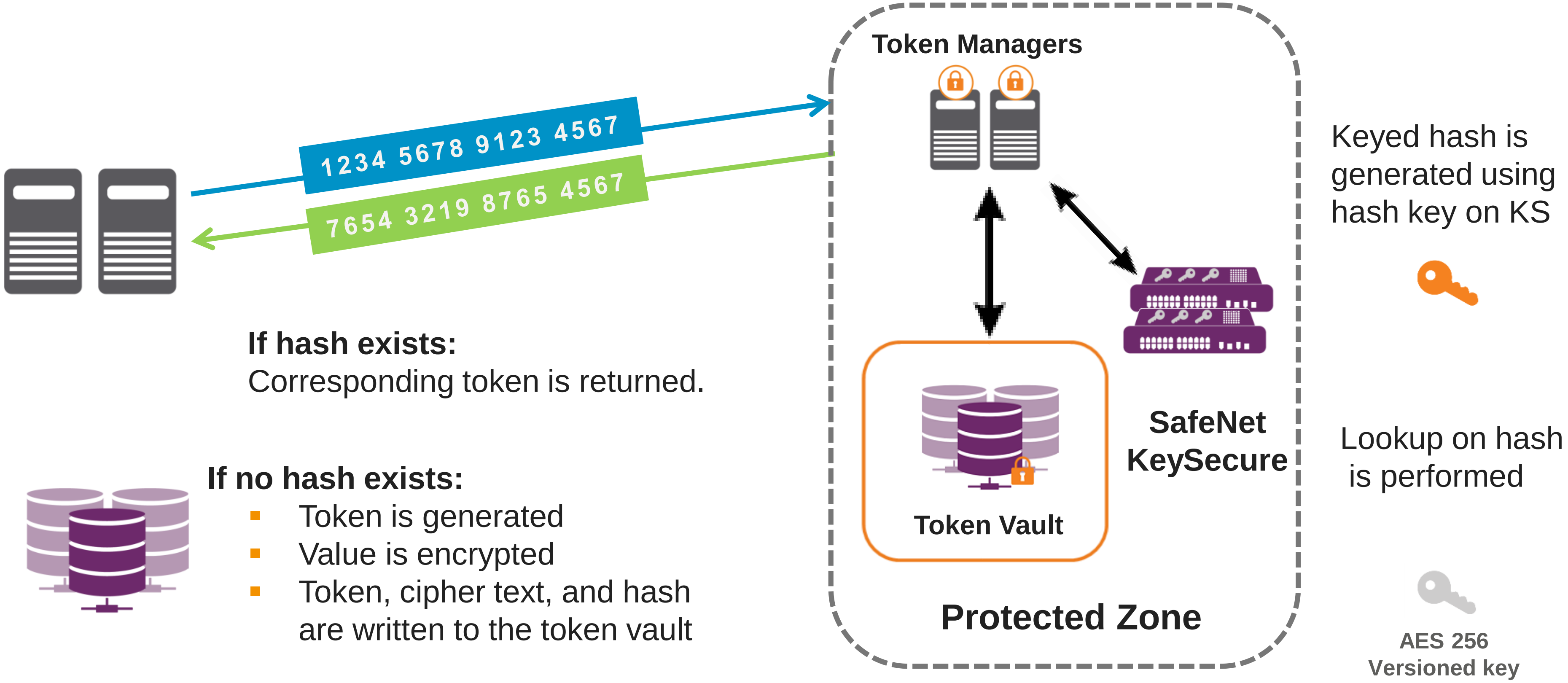
ProtectDB in Action



Tom can access Key X, Bob cannot

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

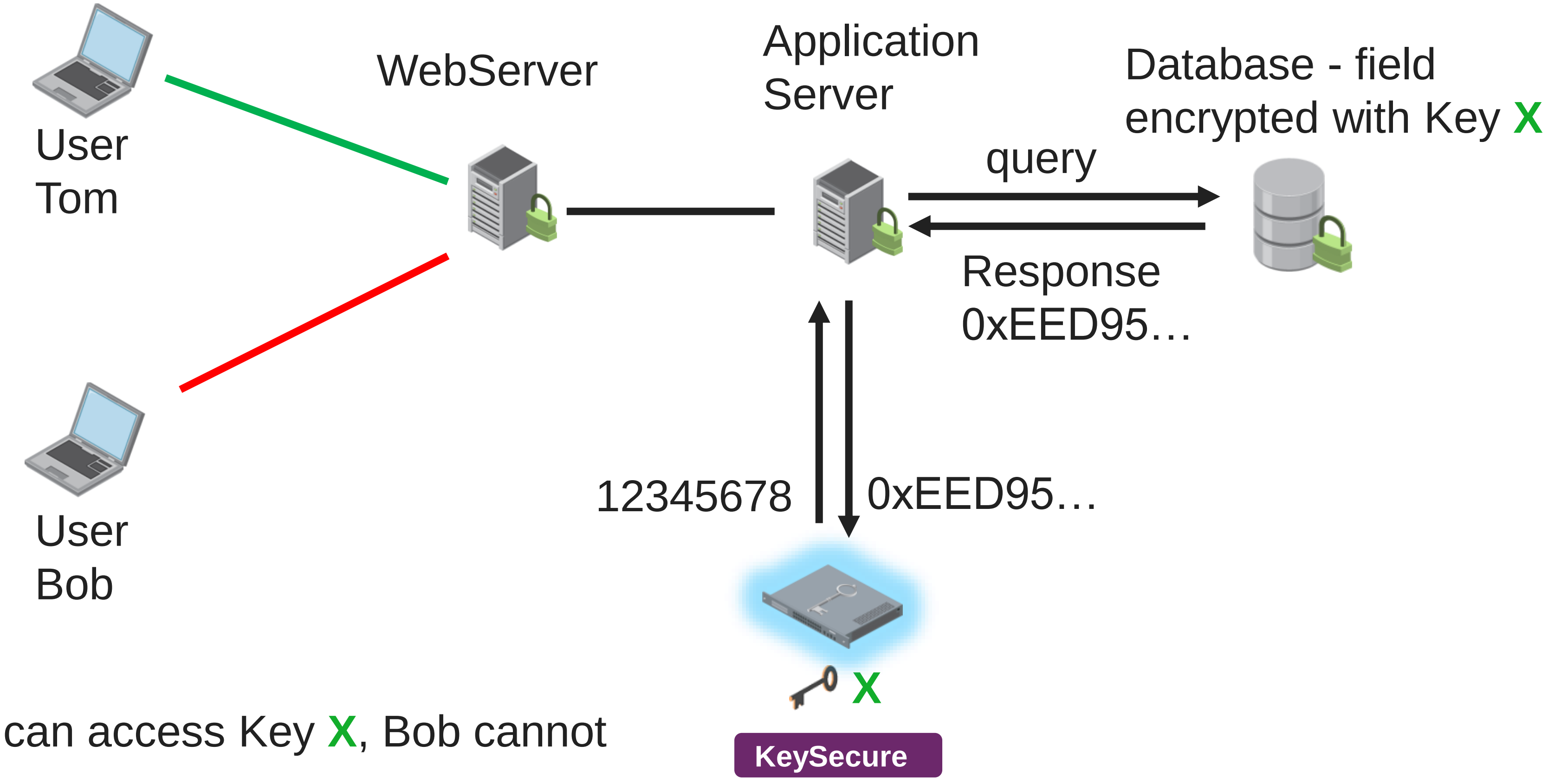
Keyed hash is generated using hash key on KS

Lookup on hash is performed

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

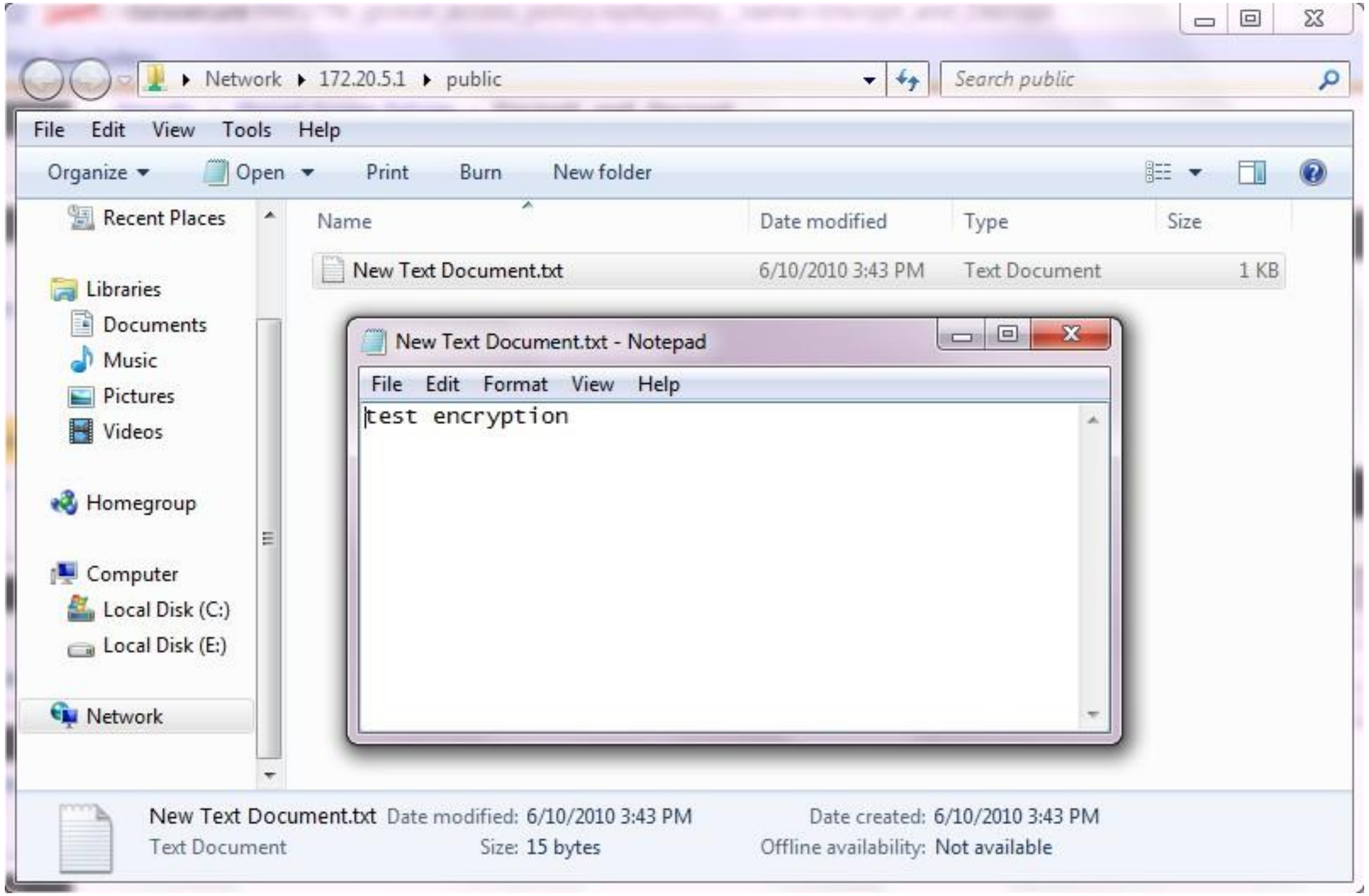
ProtectApp in Action



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

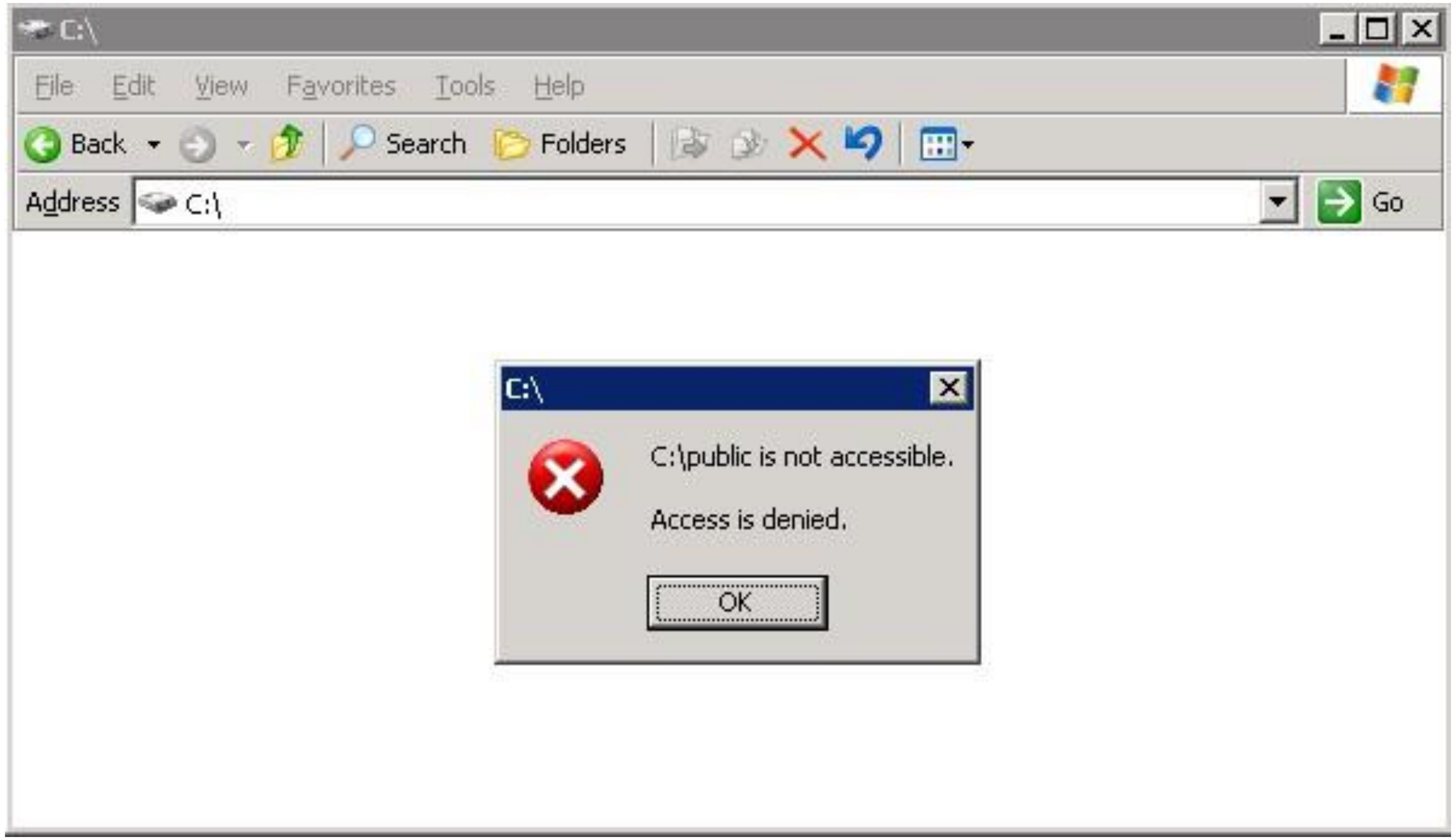
Name	Date modified	Type	Size
New Text Document.txt	6/10/2010 3:43 PM	Text Document	1 KB

```
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 III

- User with No Access permissions

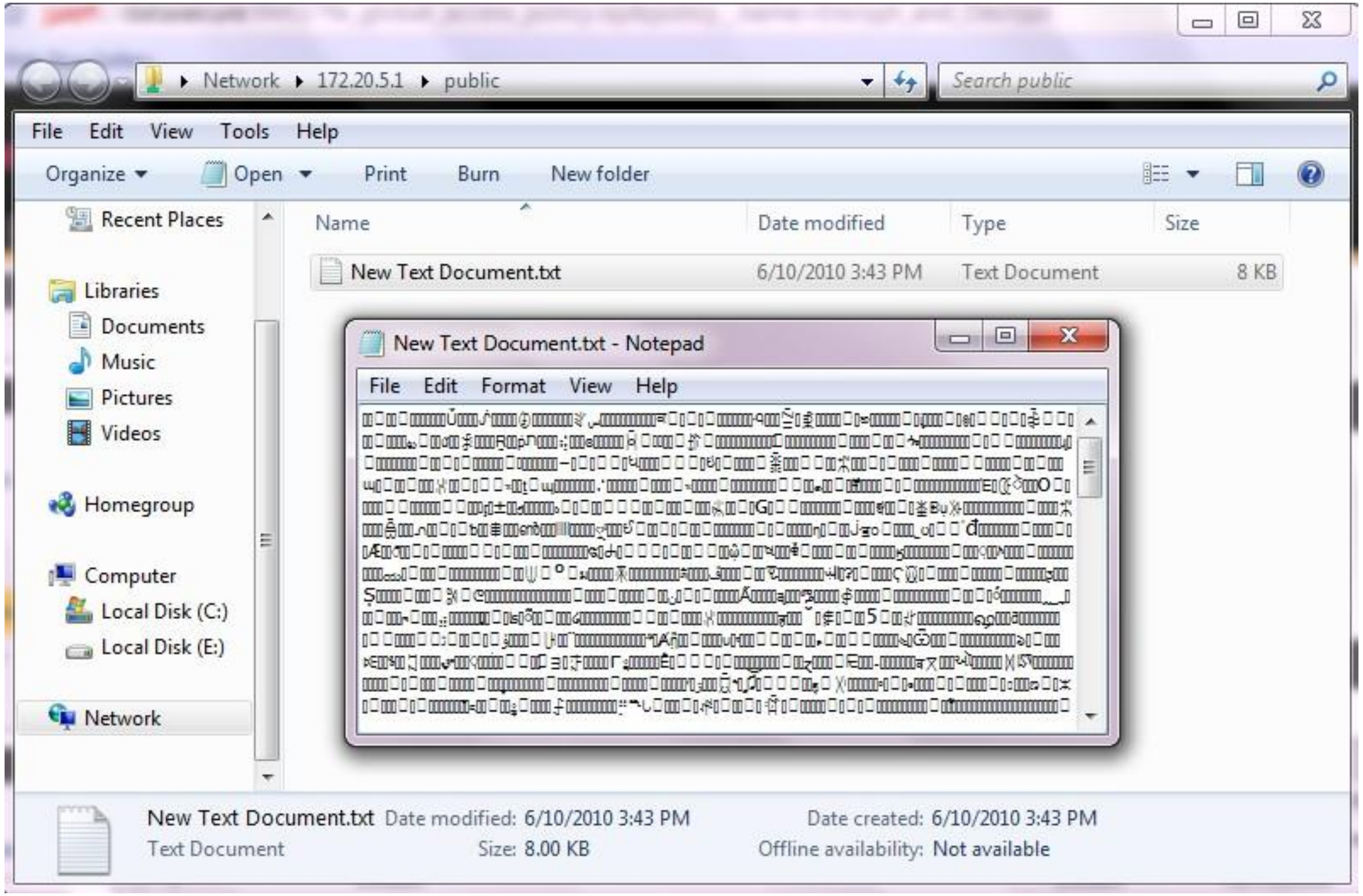


C:\public is not accessible.

Access is denied.

File Encryption Access Level – sample II

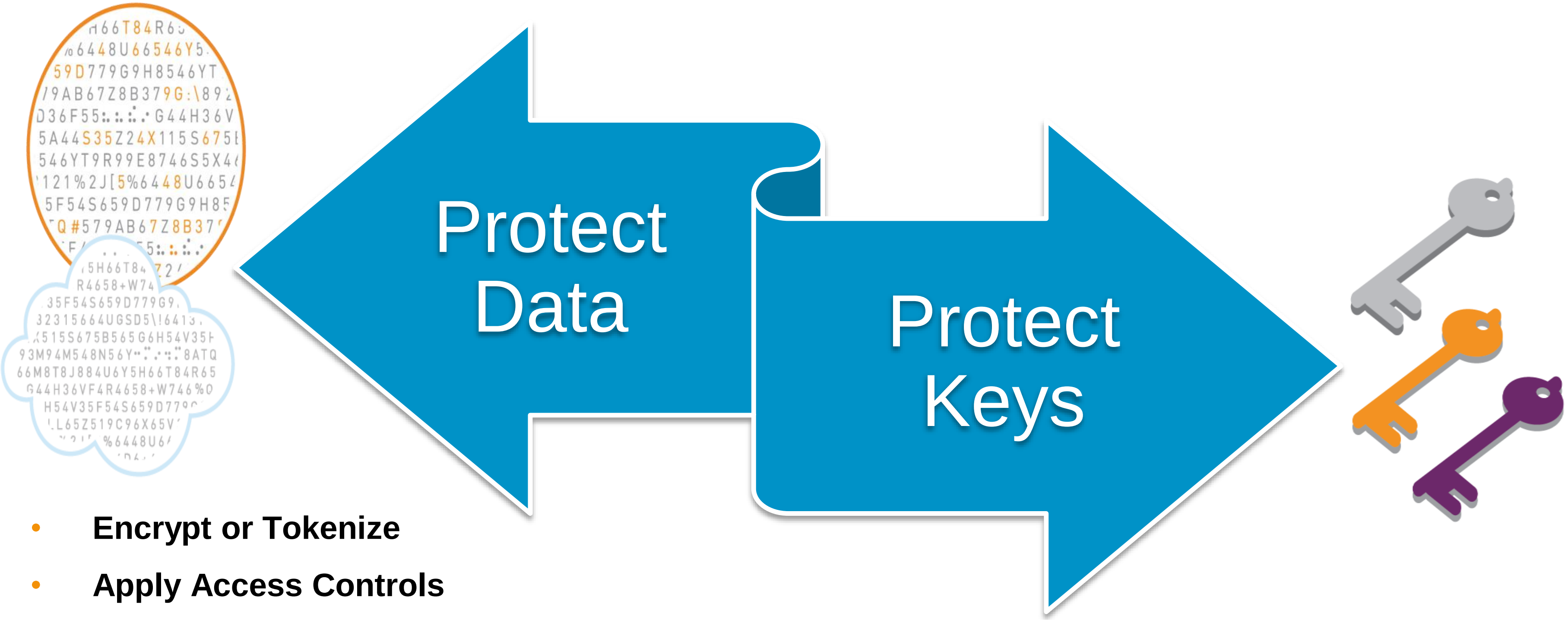
- User with Backup & Restore Ciphertext permissions


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

Data Protection Best Practices



Protect Data

Protect Keys

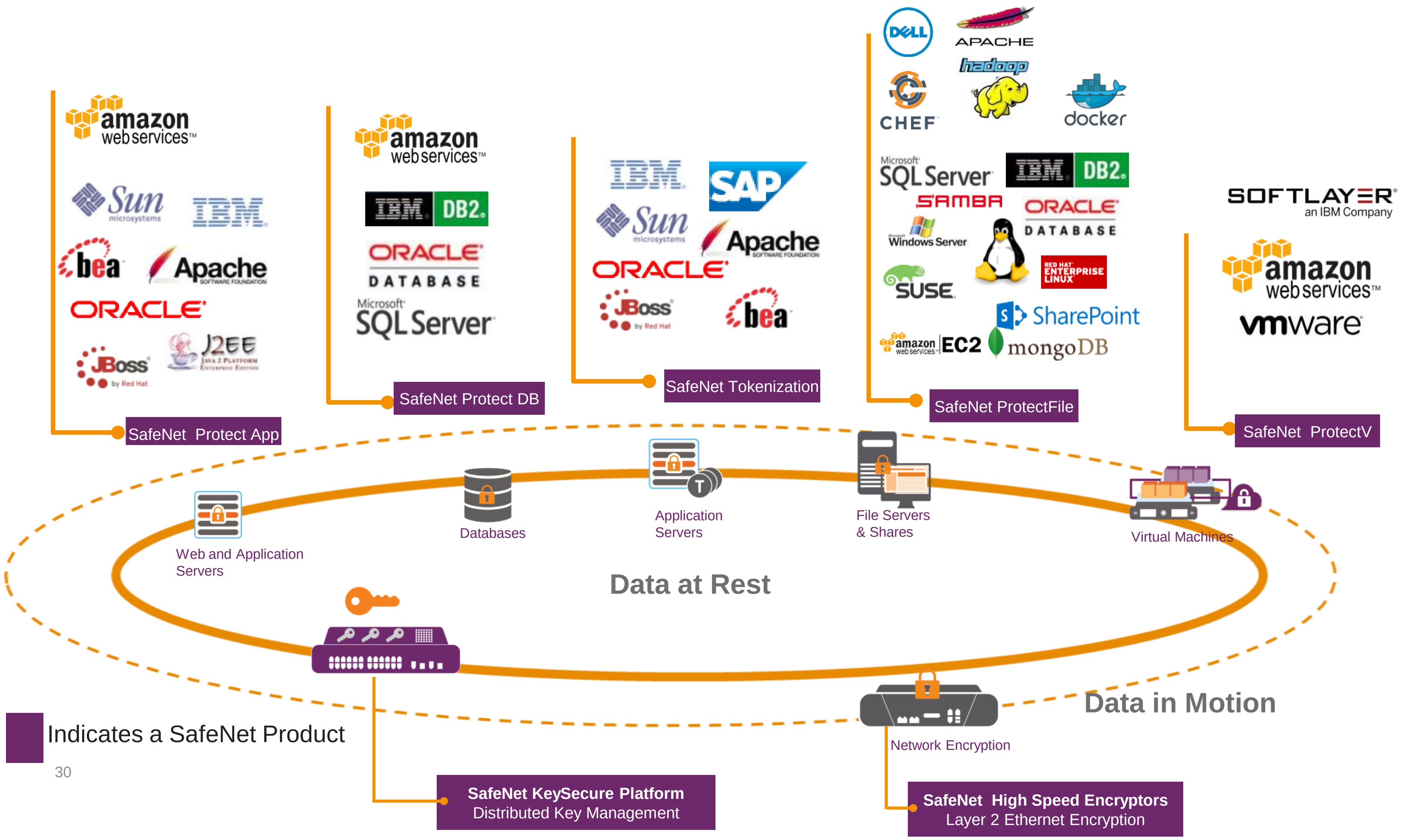
- Encrypt or Tokenize
- Apply Access Controls

- Manage Key Lifecycle
- Apply Access Controls

Decouple KEYS from DATA

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

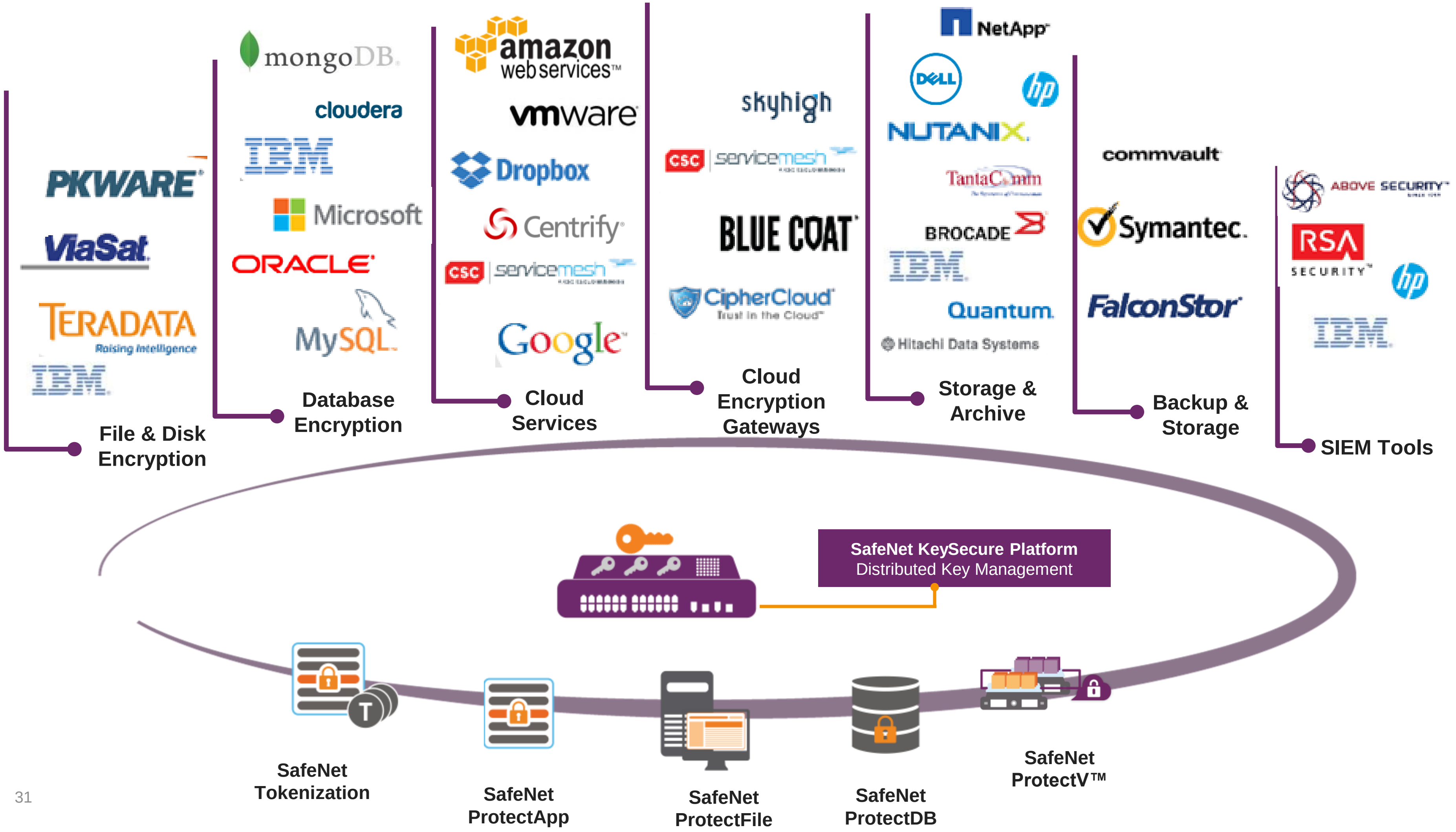
SafeNet KeySecure Platform
Distributed Key Management

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



File & Disk Encryption

Database Encryption

Cloud Services

Cloud Encryption Gateways

Storage & Archive

Backup & Storage

SIEM Tools

SafeNet KeySecure Platform
Distributed Key Management

SafeNet Tokenization

SafeNet ProtectApp

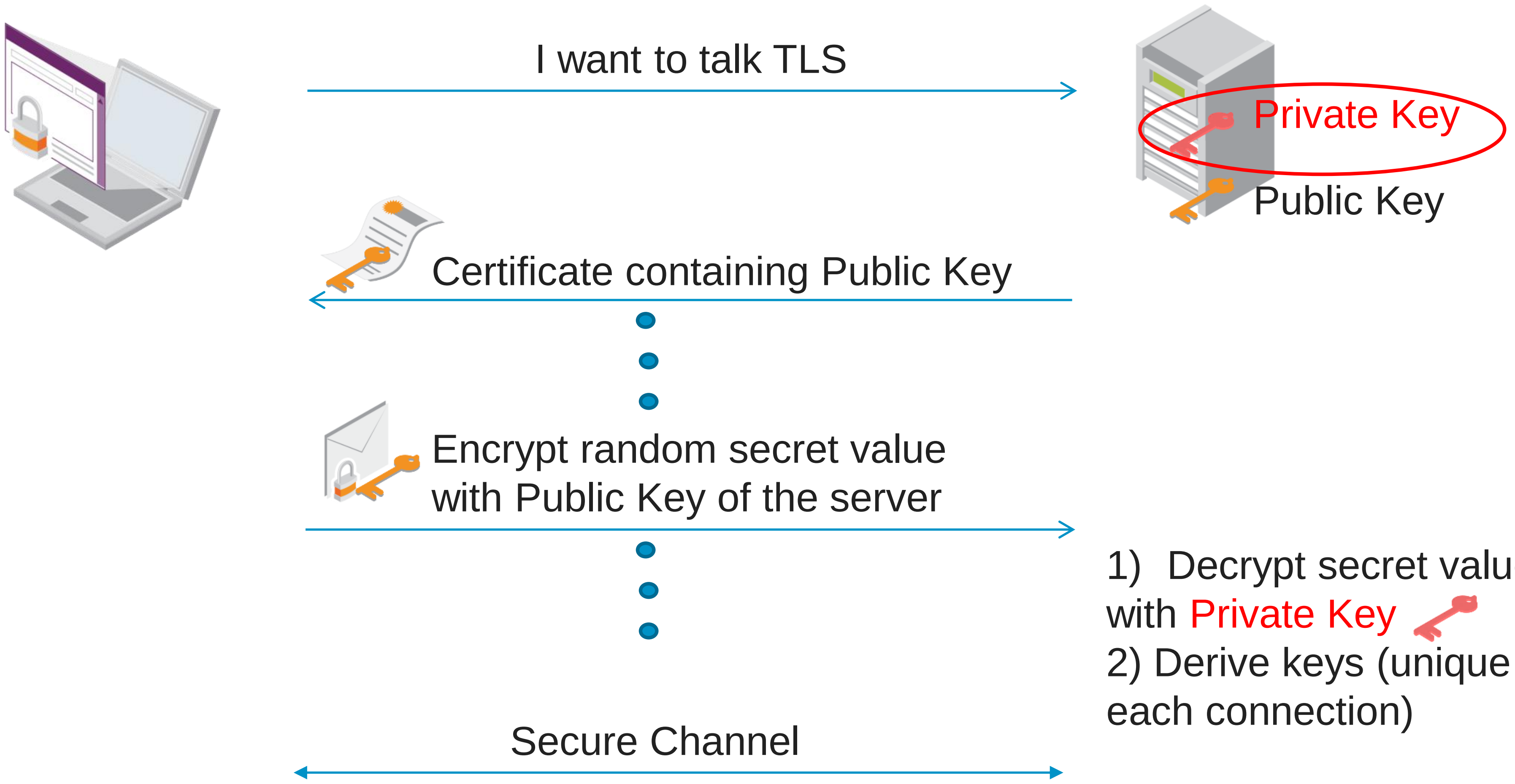
SafeNet ProtectFile

SafeNet ProtectDB

SafeNet ProtectV™

HSE L2 data in motion video

Without SafeNet Network HSM



I want to talk TLS

Private Key

Public Key

Certificate containing Public Key

Encrypt random secret value with Public Key of the server

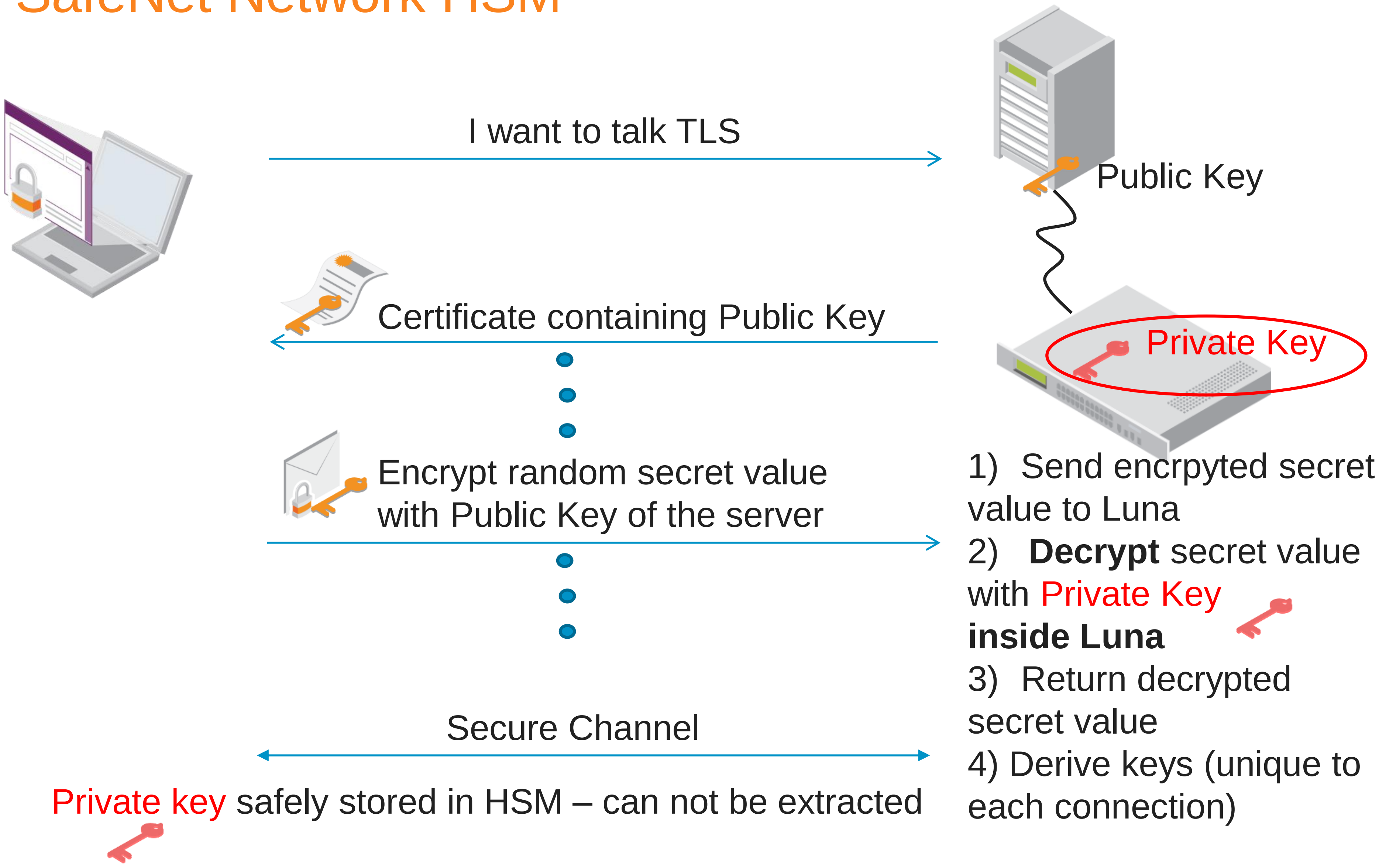
1) Decrypt secret value with Private Key

2) Derive keys (unique to each connection)

Secure Channel

If the Private key gets stolen **EVERY** TLS connection (past and future) is at risk!

With SafeNet Network HSM



I want to talk TLS

Public Key

Certificate containing Public Key

Private Key

Encrypt random secret value with Public Key of the server

Secure Channel

Private key safely stored in HSM – can not be extracted

1) Send encrpyted secret value to Luna

2) **Decrypt** secret value with Private Key **inside Luna**

3) Return decrypted secret value

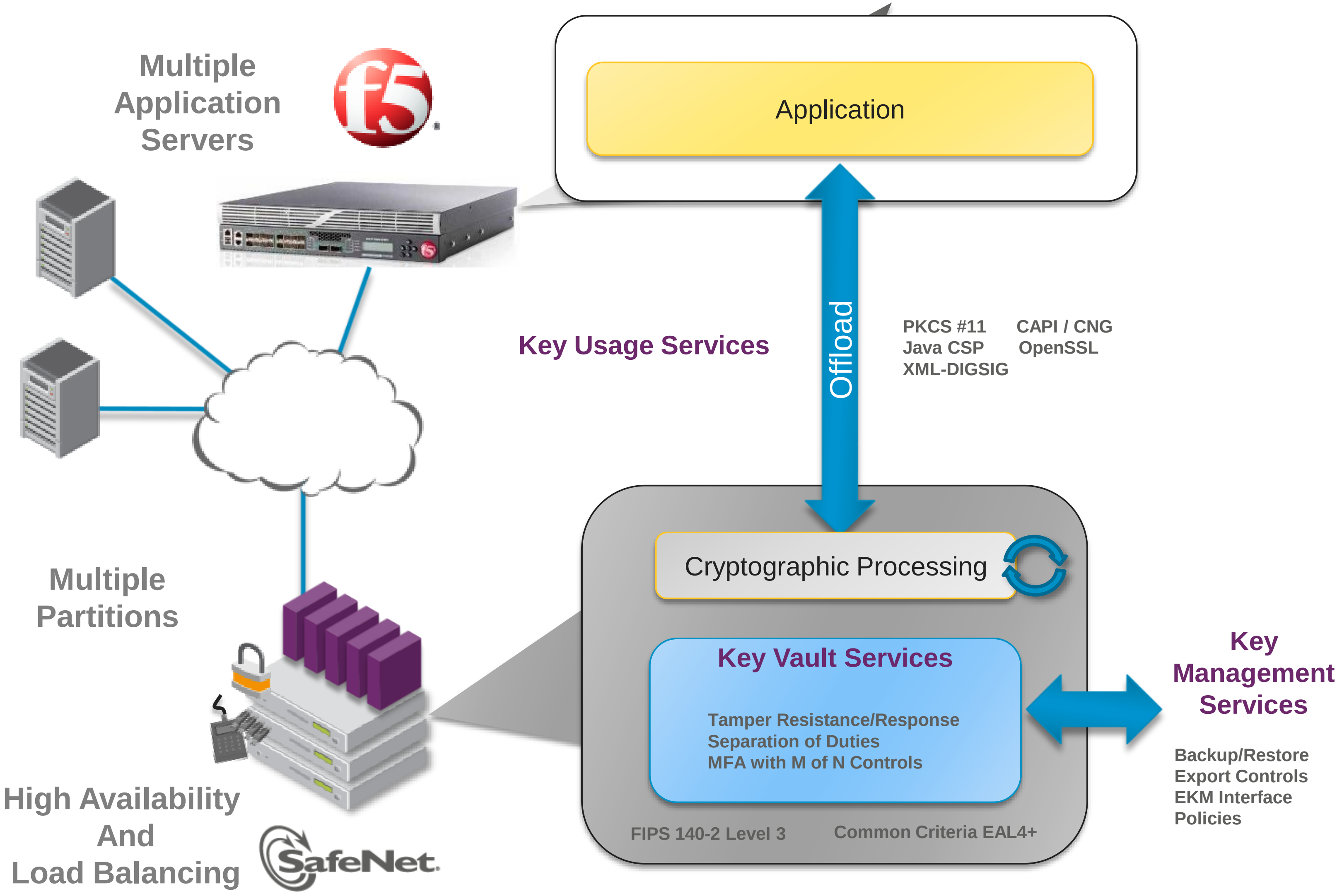
4) Derive keys (unique to each connection)

The Solution: SafeNet Luna SA Hardware Security Module

SafeNet Luna SA Network Attached HSM

- Stores SSL keys in a secure **FIPS 140-2 Level 3** tamper-proof hardware appliance.
- Private SSL key never leaves the **hardware appliance**.
- Offloads SSL transactions from BIG-IP to **accelerate operations**.
- Provides administrators with **full key control** in accordance with regulatory regimes (PCI DSS, SOX, HIPAA, etc.)

Luna SA HSM for SSL with BIG-IP



Multiple Application Servers

Key Usage Services

Offload

PKCS #11 CAPI / CNG
Java CSP OpenSSL
XML-DIGSIG

Application

Cryptographic Processing

Key Vault Services

Tamper Resistance/Response
Separation of Duties
MFA with M of N Controls

FIPS 140-2 Level 3 Common Criteria EAL4+

Key Management Services

Backup/Restore
Export Controls
EKM Interface
Policies

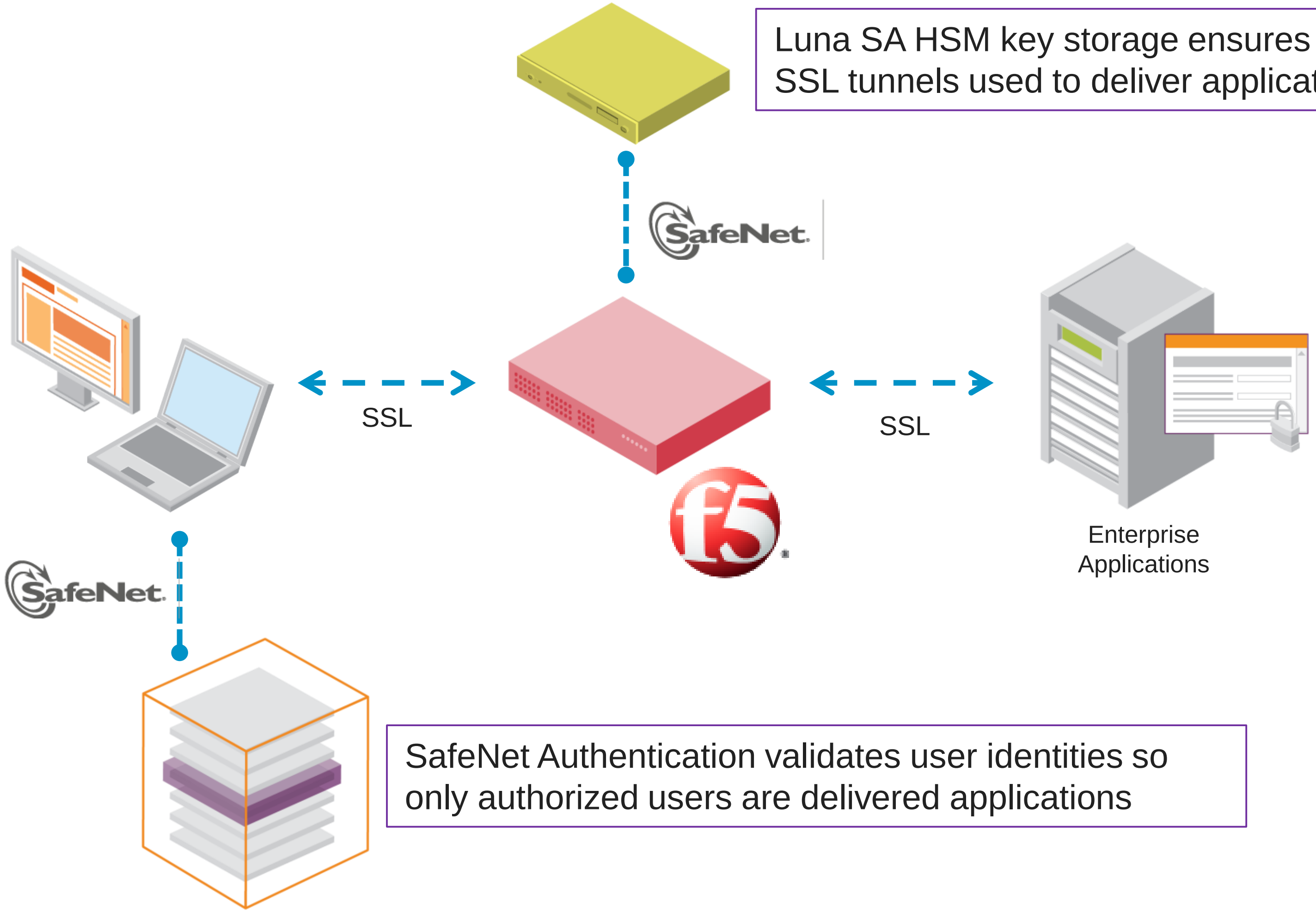
Multiple Partitions

High Availability
And
Load Balancing

Benefits of Using Luna SA for SSL with BIG-IP

- **High-Performance SSL Acceleration**
  - Up to 7000 transactions per second (1024-bit RSA decryptions)
- **Integrated FIPS-validated Hardware Key Management**
  - Defense in depth security
  - SSL keys remain in hardware throughout their lifecycle
  - Keyes always in full control of the security admin
- **Cloud-based hardware key storage available on AWS**
  - BIG-IP Virtual Edition
  - Luna SA-powered AWS CloudHSM
- **Scalability**
  - Multiple Luna SAs can be pooled together to scale capacity
- **Network Trust Links (NTL)**
  - Secure, authenticated network connections between Luna SA and clients
  - Use two-way digital certificate authentication and SSL data encryption to protect sensitive data

A complete solution from front to back…



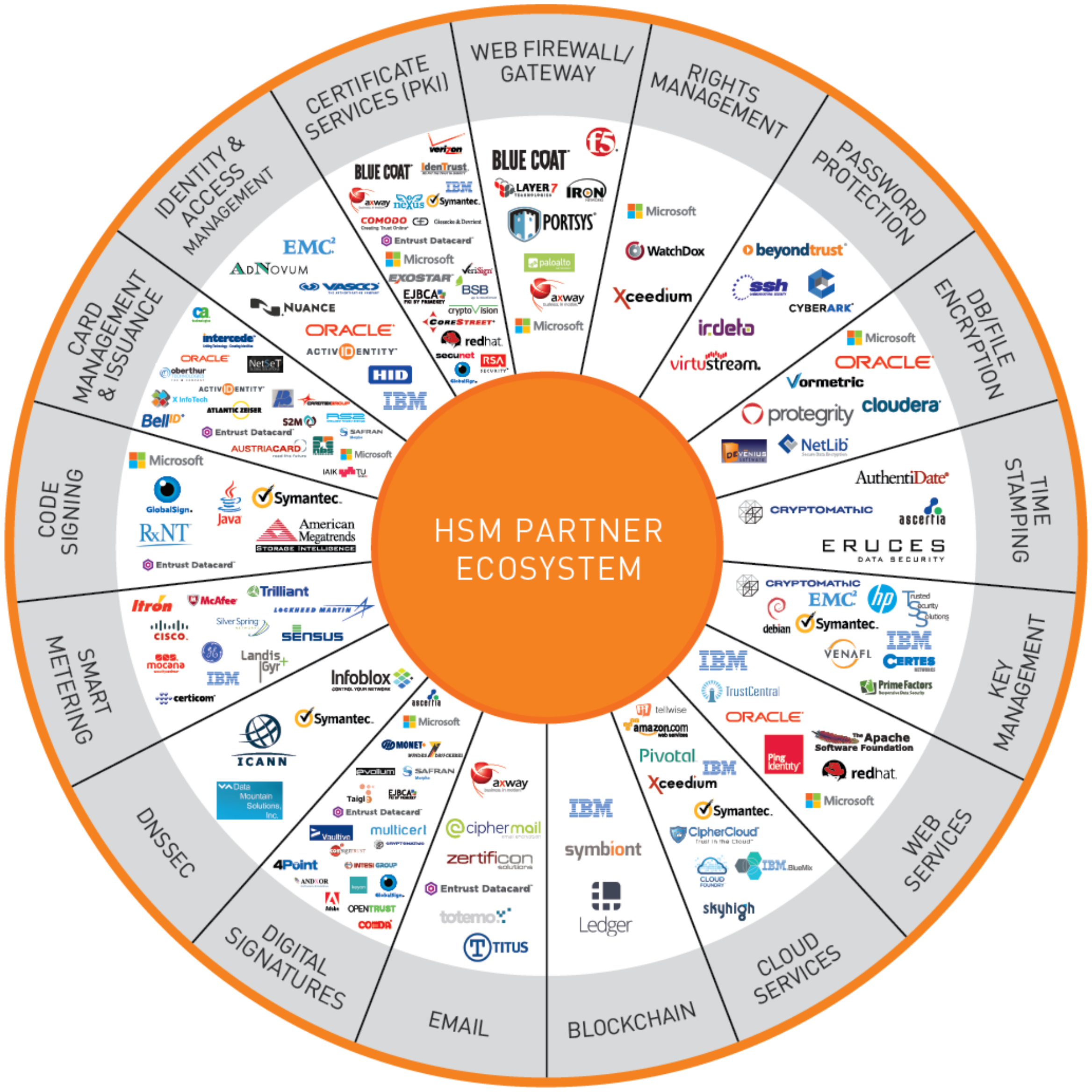
Luna SA HSM key storage ensures integrity of the SSL tunnels used to deliver applications

SafeNet Authentication validates user identities so only authorized users are delivered applications

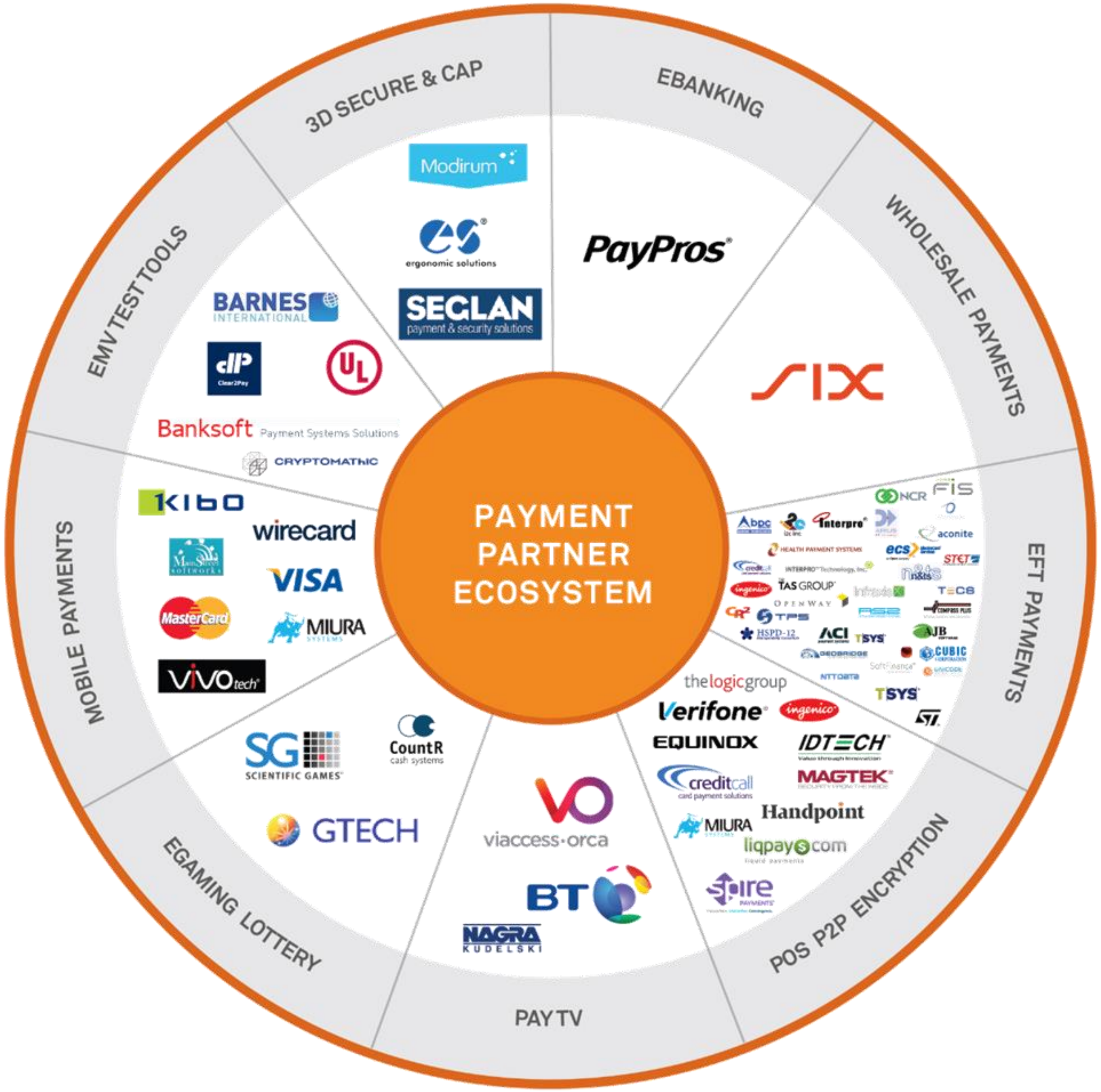
May 2016:
HSM Partner Ecosystem

338

HSM Integrations



May 2016:
Payment Partner Integrations



58

Payment Integrations

VERACOMP
WE INSPIRE IT

matija.mandaric@veracompadria.com