Crypto Management: Encryption management & optimal security of your data

Enterprise Key Manager & HSM

Ugo Piazzalunga

Pre-sales Manager, Southern Region, EMEA

ugo.piazzalunga@safenet-inc.com

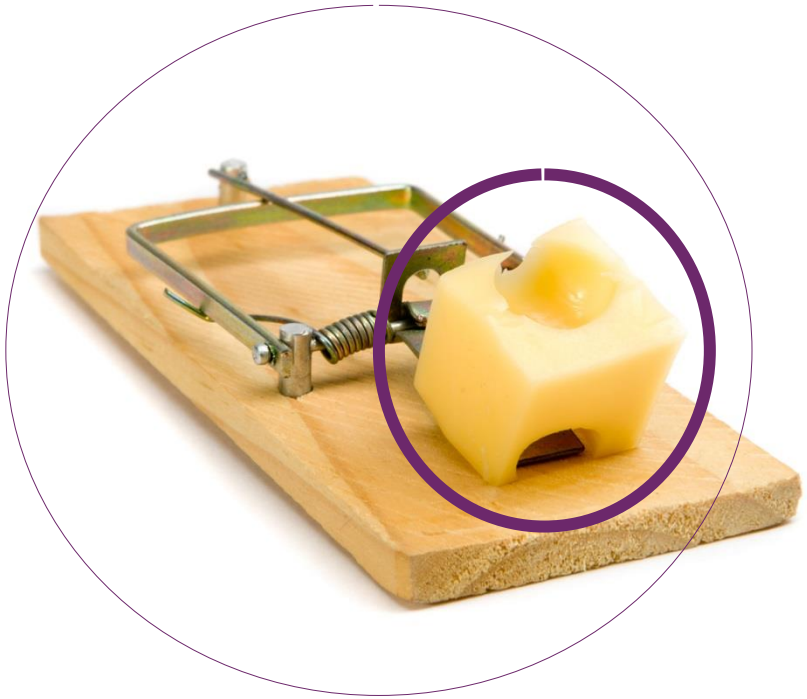
Agenda

- Data breaches – a Given!
- The need for a different approach to data protection
- Use Cases
- The Technology: Cryptography
- Key Management – centralized key policies, auditing ...
- HSM – Trusted Key Vault
- HSM vs Key manager
- SafeNet HSM Overview

Protect the target, not the perimeter

or

Protect the CHEESE, not (just) the mousetrap



SafeNet. THE DATA PROTECTION COMPANY

The best technology to protect data (the cheese)

Cryptography

provides

- Confidentiality
- Authenticity
- Integrity
- Non-Repudiation

... but done the right way

Weak

Strong

vs.

Keys in Software

Keys in Hardware

SafeNet. THE DATA PROTECTION COMPANY

What **CAN happen** if you go *weak* ...

www.theregister.co.uk/2013/02/11/bit9_hack/

bit9 hacked

Whitepapers | The Channel

The Register®

Biting the hand that feeds IT

Data Centre | Software | Networks | **Security** | Policy | Business | Hardware | Science | Bootnotes | Columnists | Video | Forum | Search »

SECURITY

Bit9 hacked after it forgot to install ITS OWN security product

Malware signed by stolen crypto certs then flung at big-cheese clients

By John Leyden, 11 Feb 2013

11

IT security biz Bit9's private digital certificates were copied by hackers and used to cryptographically sign malware to infect the company's customers.

The software-whitelisting firm's certificates were swiped when its core systems were hacked last week. The intruders then signed malicious code and distributed it to the company's corporate clients.

A number of Bit9's customers were subsequently infected by the malware because the software was - thanks to the purloined certificates - regarded as safe by networks guarded by Bit9's technology.

RELATED STORIES

Securo-boffins link HIRED GUN hackers to Aurora, Bit9 megahacks

Infosec 2013

MOST READ

Report: Climate change has already hit USA - and time is RUNNING OUT

Epson takes on Google Glass with wired 'augmented reality' glasses

Google buddies up with Intel for this year's big Chromebook push

How Google's Android Silver could become 'Wintel for phones'

Virtual universe in a supercomputer's pocket, spanning post-Big Bang to present day

SPOTLIGHT

Titsup UK Border IT causes CHAOS at air and seaports in

Web cesspit 4chan touts '$20 bug bounty' after

What **CAN happen** if you go *weak* ...

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Reports | White Papers | Events | Black Hat

ATTACKS/BREACHES | APP SEC | CLOUD | ENDPOINT | MOBILE | PERIMETER | RISK | OPERATIONS

ATTACKS/BREACHES

11/1/2012
07:16 PM

Researchers Develop Cross-VM Side-Channel Attack

A new attack vector shows that isolation in public clouds is not a perfect answer for security, researcher says

Dark Reading
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login

50% 50%

Like 18

A group of researchers has developed a side-channel attack targeting virtual machines that could pose a threat to cloud computing environments.

The attack is described in a paper entitled "Cross-VM Side Channels and Their Use to Extract Private Keys," authored by Yinqian Zhang, a PhD. student at the University of North Carolina at Chapel Hill; UNC professor Michael K. Reiter; Thomas Ristenpart, an assistant professor at University of Wisconsin-Madison; and Ari Juels, chief scientist at EMC's RSA security division.

According to the paper (PDF), the group was able to demonstrate an attack in a lab environment that allowed a malicious virtual machine (VM) to extract a private ElGamal decryption key from a co-resident virtual machine running Gnu Privacy Guard, which implements the OpenPGP email encryption standard.

NEWS SUBSCRI

LIVE EVENTS

UBM Tech

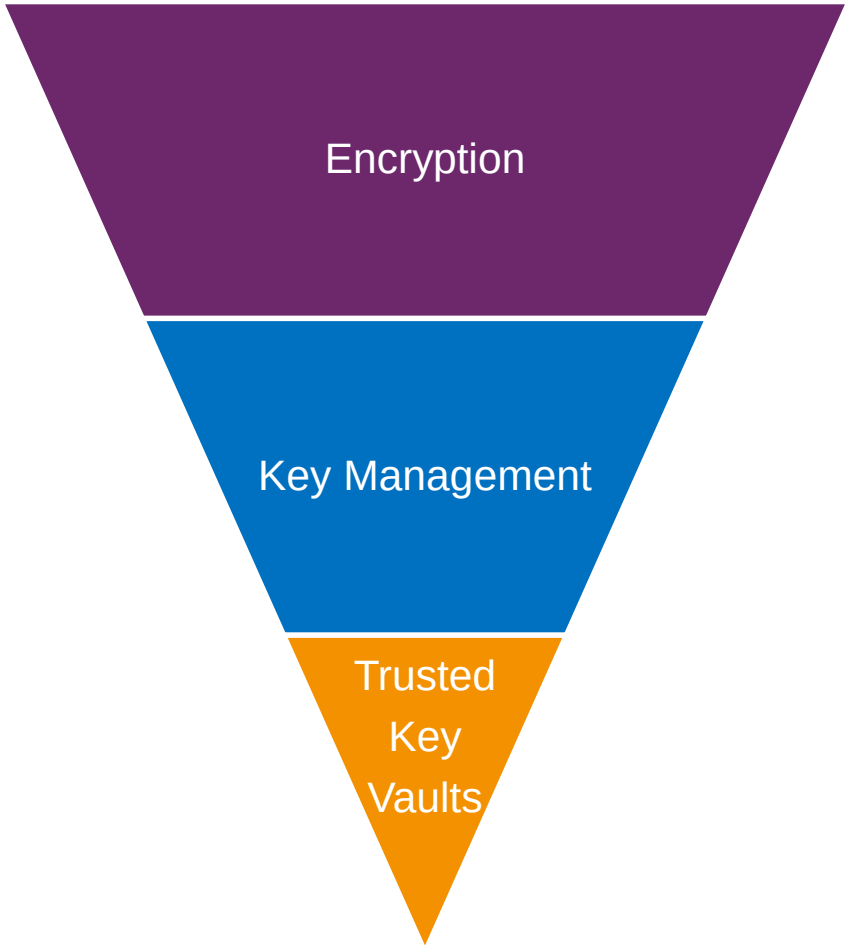
MORE UBM TECH LIVE EVENTS

WHITE PAPERS

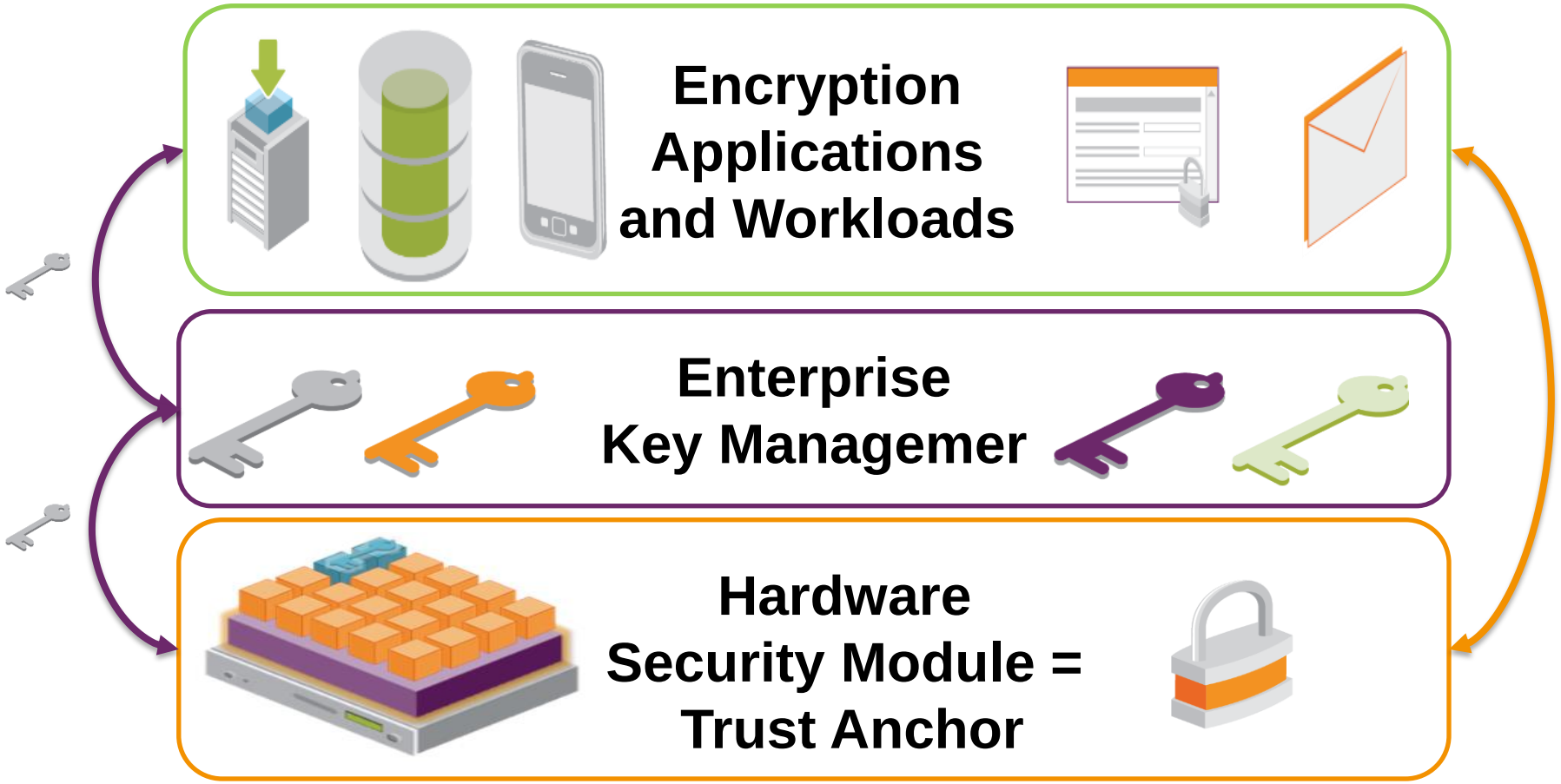
- IT Start-Up Cuts Operat... Geographical Reach
- The Business Value of ...

Net. THE DATA PROTECTION COMPANY

The Foundation of High Assurance Encryption

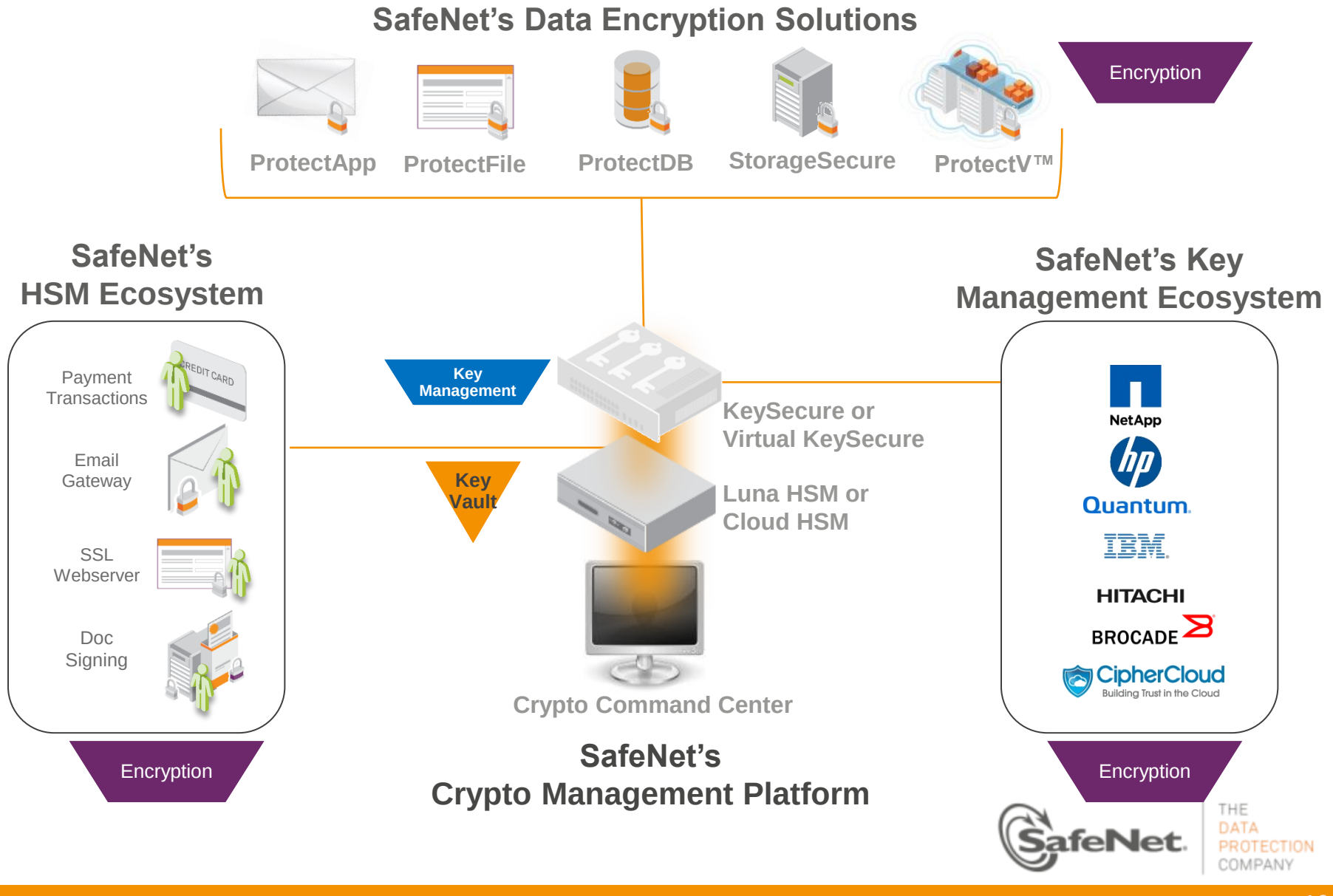


The Foundation of High Assurance Encryption



SafeNet. THE DATA PROTECTION COMPANY

SafeNet Data Encryption & Crypto Management



Key Manager

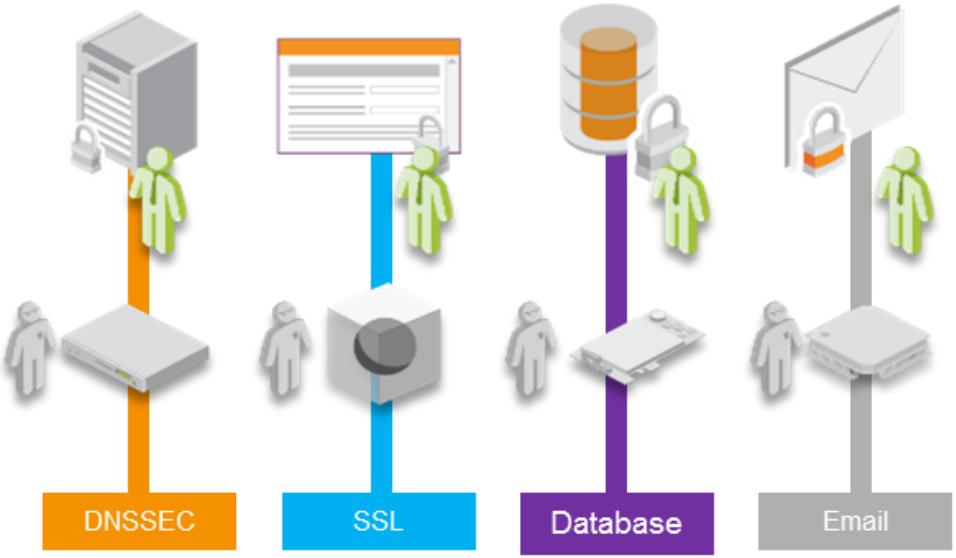
Key Management

SafeNet. THE DATA PROTECTION COMPANY

Challenge: Encryption Creep

Encryption-dependent systems like secure web services, encrypted backups, certificate authorities, etc. are deployed in isolation

Disparate, isolated islands of encryption scattered across workgroups, infrastructure elements, and other locations



Challenge: Organizations Manage Thousands of Keys!

Keys reside in inconsistent states/levels of security

Key location/usage can be difficult to audit

Lost, stolen, guessable/weak, and copied keys have lead to significant breaches

Goals of Key Management

Key Management

- **Decreased exposure** of keys
- Consistent **policy enforcement**
- **Streamlined administration**
- **Encryption efficiency**
- **Unified auditing** and **remediation**

SafeNet. THE DATA PROTECTION COMPANY

Key Secure - “What Is It”

Key Management

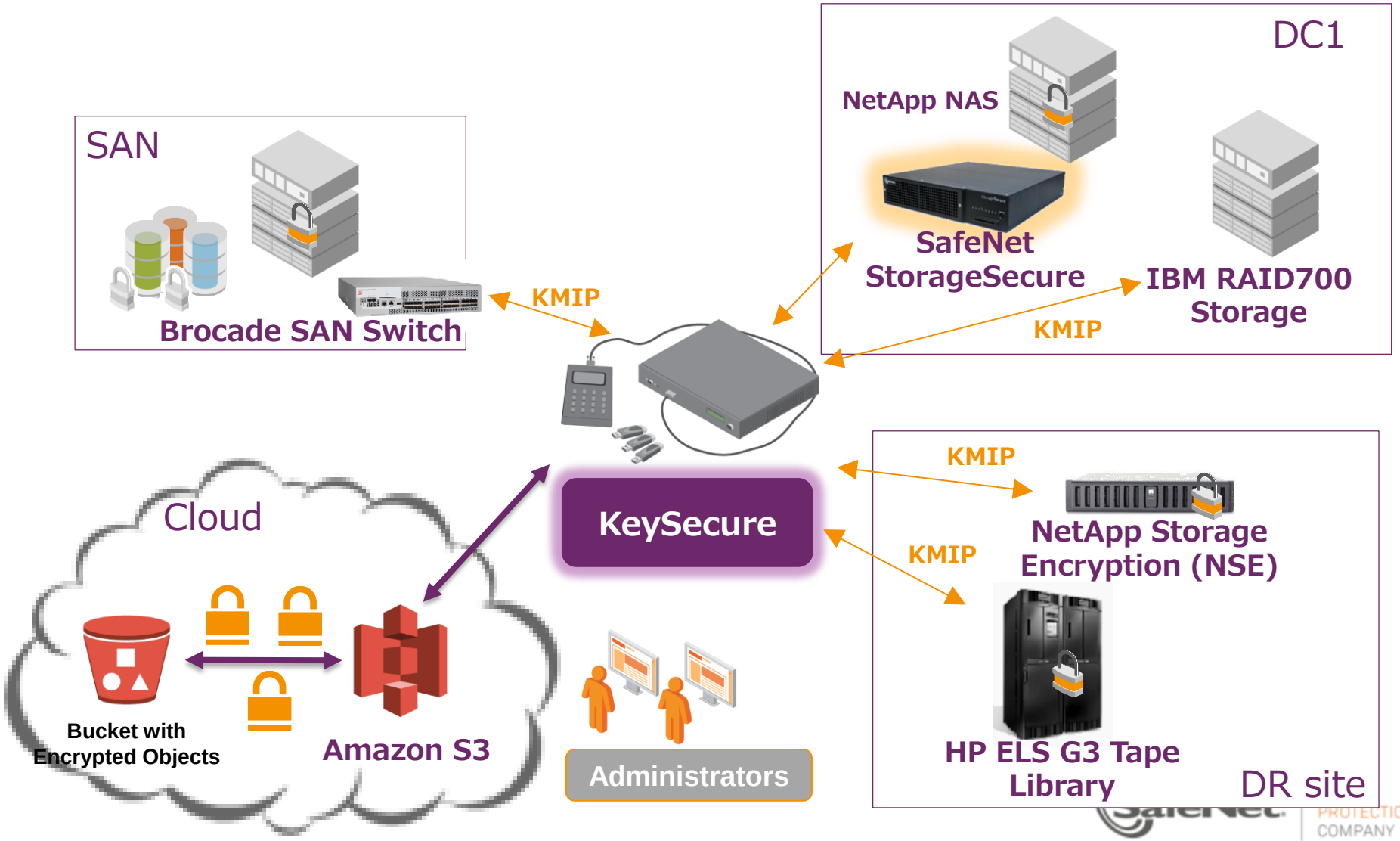
- High performance, centralized crypto & key management solution
  - Centralized policy, key management, logging, and auditing
  - Covering broad range of data formats and environments
- Integrated connectors to handle specific data protection scenarios
  - Protect File, Protect DB, Tokenization Manager, Protect App, ProtectV
- Use KMIP to integrate with multiple partners for storage, backup and encryption
- Physical and Virtual offering

SafeNet. THE DATA PROTECTION COMPANY

KeySecure

Key Management

Enterprise Key Manager with 18+ Integrated Partners, Cloud Ready



Enterprise Key Manager Solution Partners

SIEM Tools	IBM Radar, HP ArcSight
Storage & Archive	Brocade, Quantum, NetApp, HP, Sepaton, Hitachi Data Systems
Cloud Encryption Gateways	CipherCloud (Building Trust in the Cloud), servicemesh, PerspecSys (protecting cloud data)
Cloud Storage	Dropbox, Google, amazon web services
Backup & Restore	Symantec, FalconStor
Custom KMIP Client (Beta)	python
File & Disk Encryption	ViaSat, IBM, PKWARE

SafeNet. THE DATA PROTECTION COMPANY

Hardware Security Module (HSM)

SafeNet. THE DATA PROTECTION COMPANY

A Hardware Security Module is…

Trusted Key Vault

…a dedicated crypto processor…

…designed for the protection of the crypto key lifecycle…

…validated as secure by third parties…

…a Trust Anchor…

SafeNet. THE DATA PROTECTION COMPANY

Why use HSM: AWS “voice”

Why CloudHSM ?

- Lower the barrier for developers to encrypt sensitive data
  - ✓ API and SDKs to abstract complexity
- Encrypted data opaque to Cloud Service Provider’s operations staff and cyber criminals
- Horizontally Scalable – CloudHSM as a Service!
- Pay-as-you-go
- Meet compliance goals when data is resident in cloud e.g. PCI-DSS, HIPAA

Luna HSM Strengths

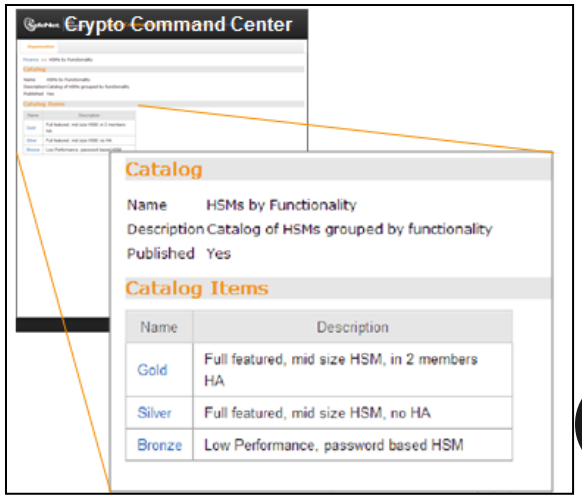
Trusted Key Vault

- High Assurance
- 2FA Trusted Path Authentication
- Sophisticated Role Concept (incl. MofN) & Separation of Duties
- Keys in Hardware
- Partitioning
- Secure Client – HSM connection (NTLS)
- Performance
- HA & LB
- Backup to HW
- Remote Administration and Backup
- Integrations
- Secure Audit Logging
- EKM, KMIP Support
- Support for virtualized environments (HTL Support)
- Crypto Hypervisor - Luna Crypto Command Center (CCC)

SafeNet. THE DATA PROTECTION COMPANY

Crypto Hypervisor: Designed for the Cloud Operational Model

1. On-demand crypto delivery
2. Self-service portal for users
3. New crypto services spin up easily
4. Encryption now a cloud enabler
5. Part of “New VM Rollout Process”
6. Apps can now migrate to cloud



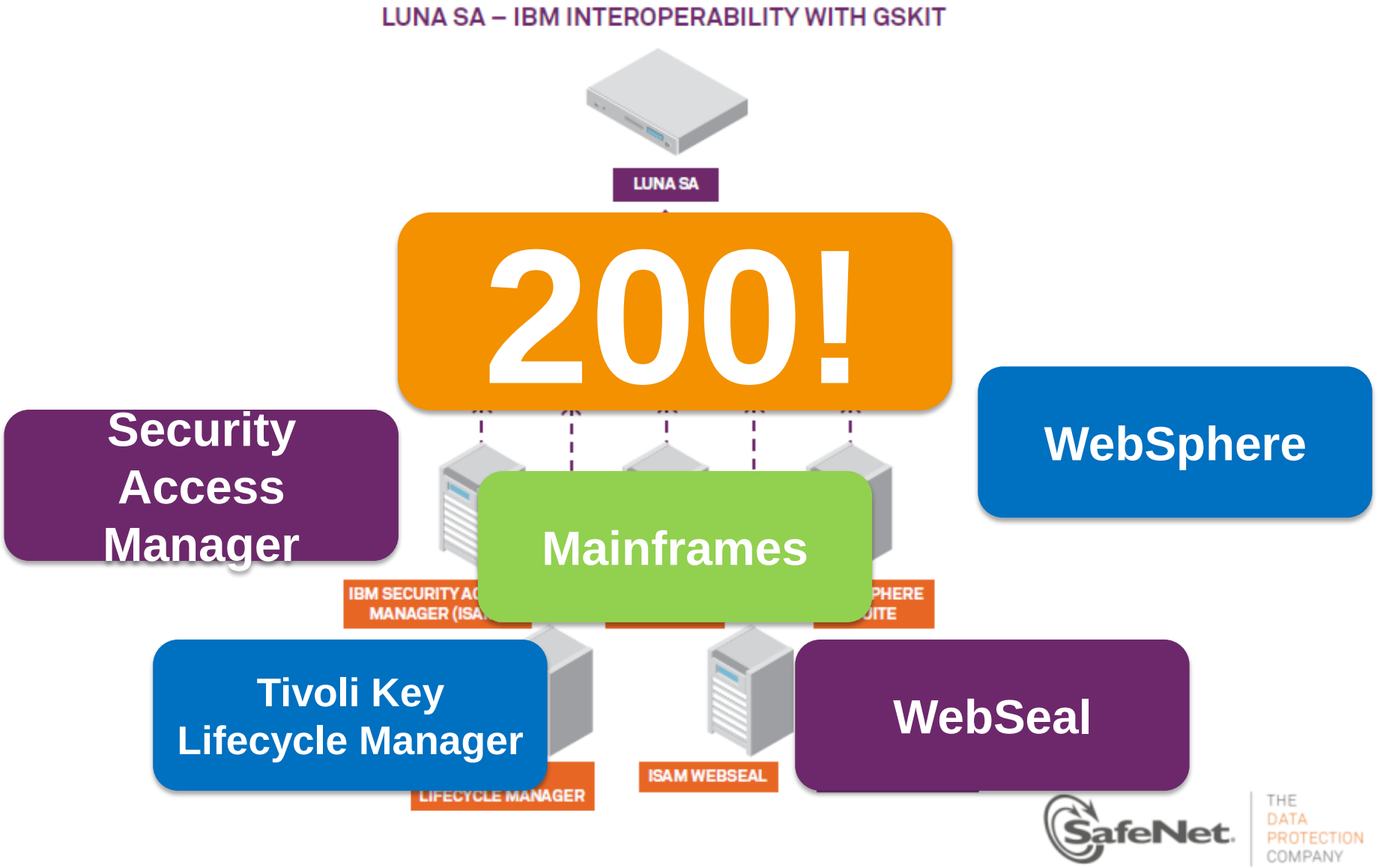
SafeNet. THE DATA PROTECTION COMPANY

SafeNet HSM Solution Partners

Certificate Services (PKI)	Document Signing	AMI	Password Protection	Timestamping
Microsoft Symantec/Verisign Entrust Verizon/Unicert Globalsign Axway/Tumbleweed AI/Corestreet Identrust Red Hat EMC/RSA Comodo Exostar PrimeKey (EJBCA) …	Microsoft Adobe 4Points Globalsign Ascertia Evolium Andxor Cryptomathic Intesi Group Comda/ComSignTrust Keyon Taigle Valtive	Landis & Gyr Trilliant Sensus Itron IBM Lockheed McAfee GE Energy Mocana Green Hills Software Cisco Certicom	Cloakware Symark Xceedium Cyber-Ark Virtustream Lighton Tech SSH	Authentidate nSync Ascertia Cryptomathic
DB/File Encryption	**Key Management**	**Web Services**	**Mobile Payments**	**Web Firewall/Gateway**
Microsoft Oracle Vormetric NetLib Devenius Gazzang	HP RSA Venafi TSS Cryptomathic Symantec/PGP Certes IBM TKLM	IBM Tivoli IBM Websphere Oracle Weblogic Sun Fed Mgr PingID Apache HTTP Server Microsoft IIS	Vivotech Monetra Erricson KTFC (Korea)	Layer 7 Vordel nAppliance Portcullis Imperva F5 Palo Alto Networks Citrix
DNS Sec	**Cloud Services**	**Email**	**Code Signing**	**Secure Manufacturing**
Infoblox DataMountain ICANN Verisign DNS Sec	AWS Symantec Symantec .Cloud Xceedium CipherCloud	Totimo Axway Open Source: DJIGZO Entrust EMS Zertificon	Microsoft Java Globalsign Symantec	Certicom
eID / ePassport	**IAM**	**Card Management**	**EMV Test Tools**	**Rights Management**
Entrust Cryptomathic Monet+ Morpho (Identification) Kinectis OpenTrust PrimeKey (EJBCA) SafeID Bundesdruckerei	Vasco HID / ActivIdentity DS3 AdNovum	Microsoft FIM Intercede ActivIdentity CA/Arcot Entrust ID Guard DS3 Bell ID	UL (Collis) Barnes International Clear2Pay (Integri)	Microsoft RMS Watchdox

SafeNet. DATA PROTECTION COMPANY

SafeNet HSM Solution Partners
IBM Example



SafeNet HSM Solution Partners
Microsoft Example

Active Directory Certificate Services

SQL Server

Windows Rights Management System

Windows OCSP responder
(Online Certificate Status Protocol)

Authenticode

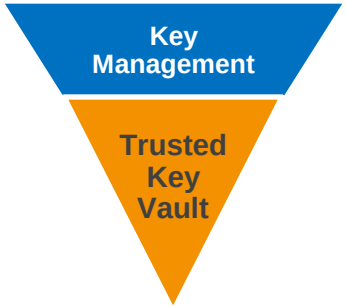
Forefront Threat Management Gateway

IIS
(Internet Information Services)

Forefront Identity Manager

SafeNet. THE DATA PROTECTION COMPANY

Key Manager vs HSM

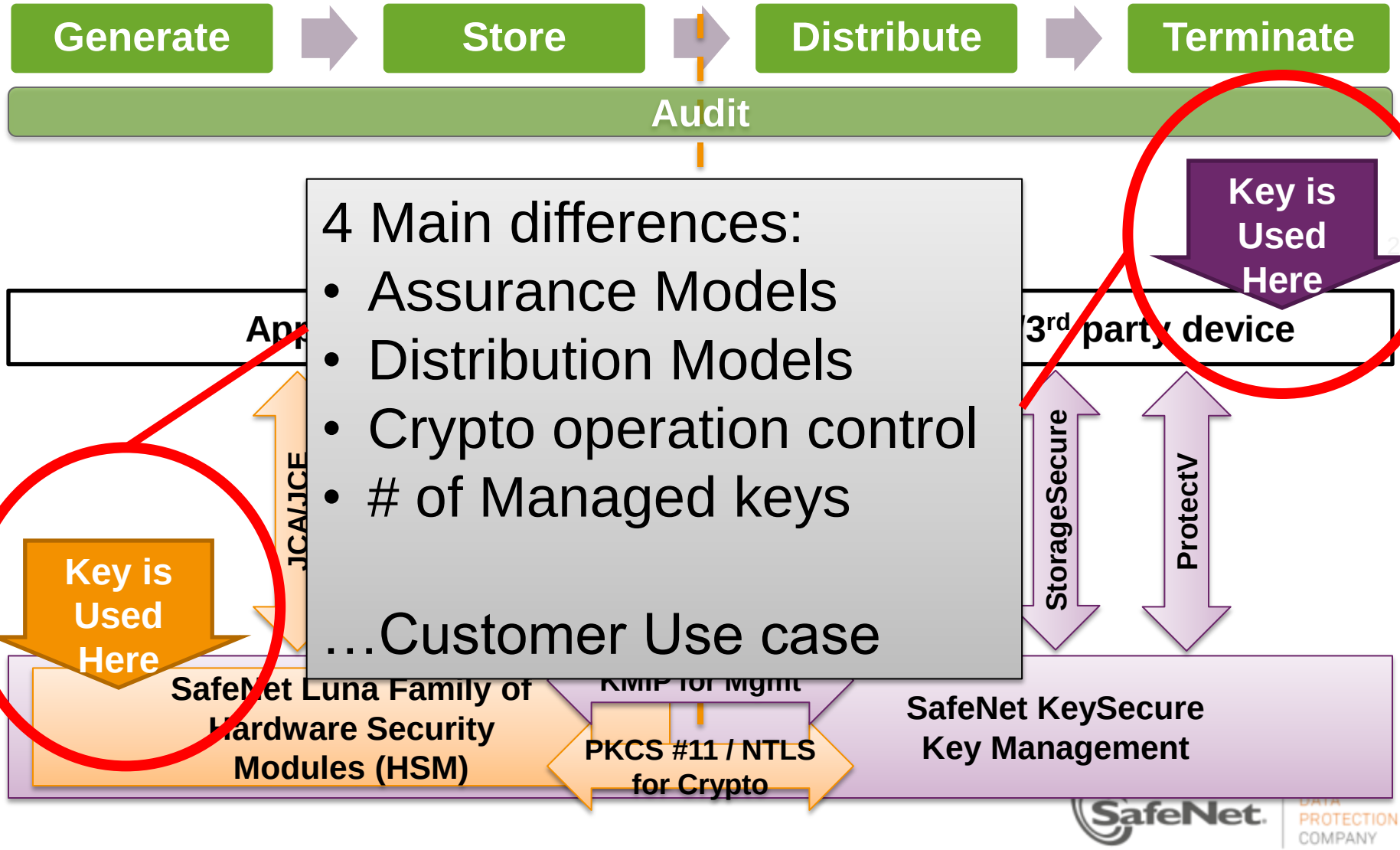


SafeNet. THE DATA PROTECTION COMPANY

Key Management

Trusted Key Vault

HSM and Key Management

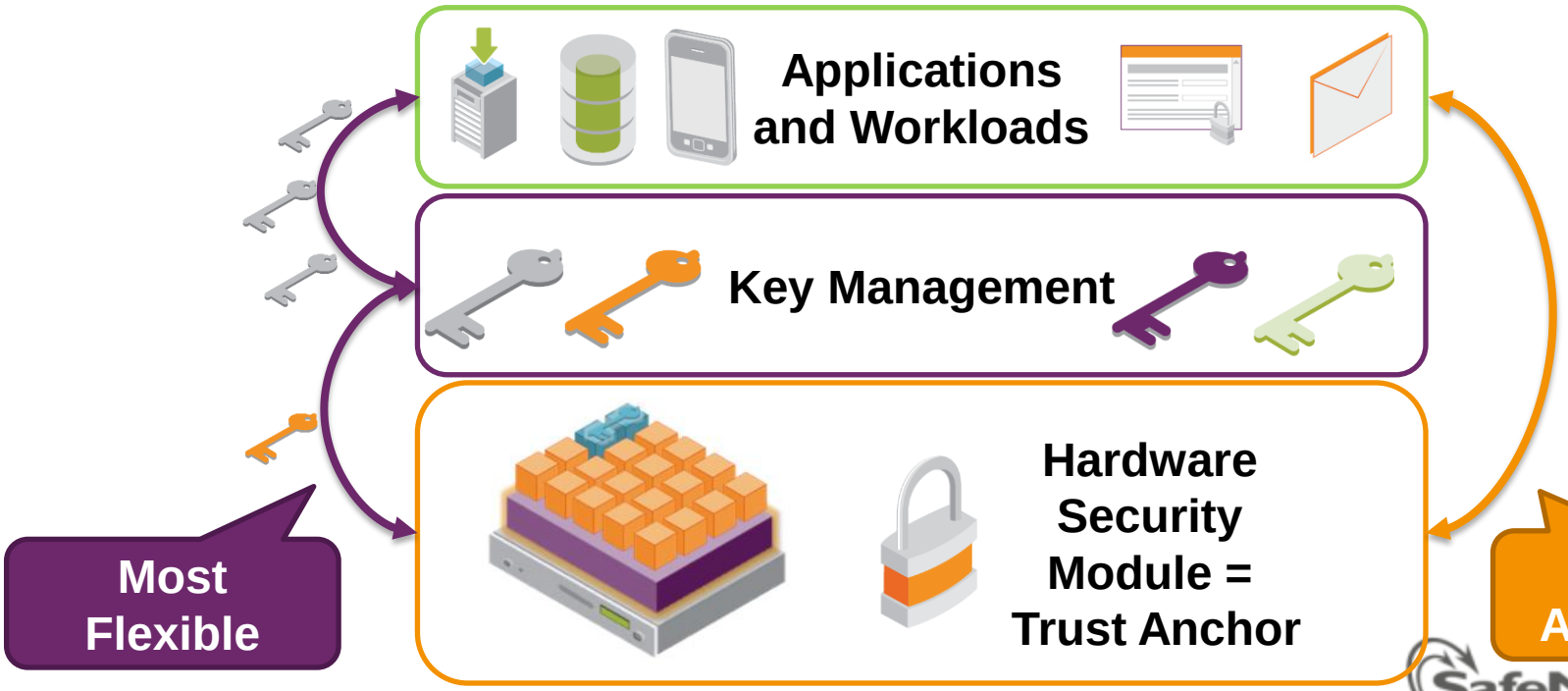


SafeNet DATA PROTECTION COMPANY

SafeNet's Crypto Management Ecosystem

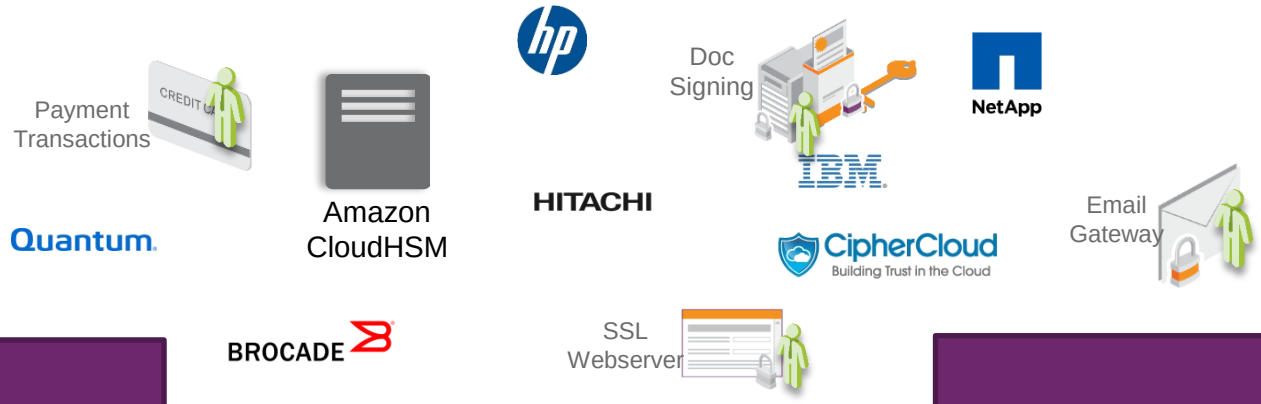
SafeNet Encryption Products
(ProtectApp, ProtectDB, ProtectFile, ProtectV, StorageSecure)

SafeNet Partners
(CAPI, CNG , ICAPI , JCA/JCE,.NET, KMIP, PKCS #11, OpenSSL, and more!)



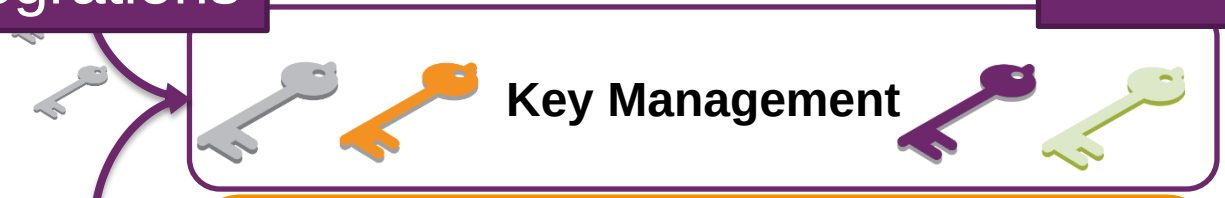
SafeNet. DATA PROTECTION COMPANY

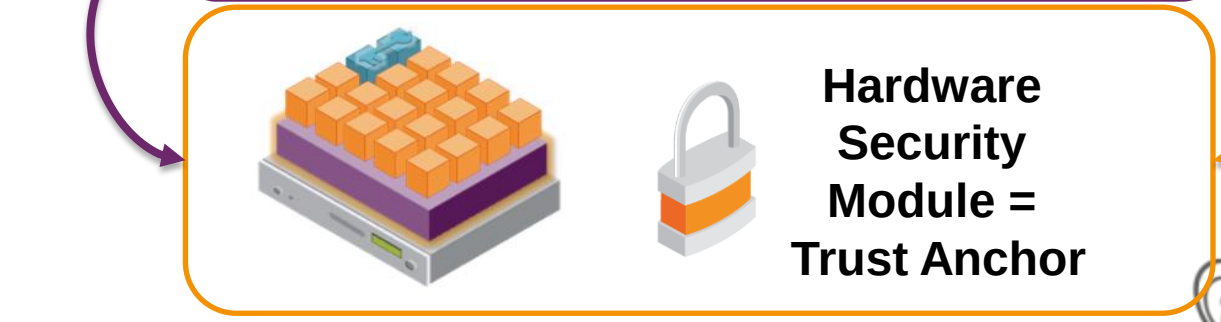
SafeNet's Crypto Management Ecosystem



Key Management
18+ Partners
33+ Integrations

HSM
179+ Partners
229+ Integrations
30+ Solution Areas!





SafeNet. THE DATA PROTECTION COMPANY

SafeNet HSM Portfolio

Trusted Key Vault

Luna SA

Luna SP

Luna PCI

Luna G5

PS Internal Express

ProtectServer External

Luna EFT

EKM

SafeNet. THE DATA PROTECTION COMPANY

▶ Network Attached General-Purpose HSM

▶ Certifications	Validated to FIPS 140-2 (level 2 and level 3), Common Criteria EAL 4+, security boundary is the HSM itself – keys always in hardware
▶ Future-Proof	Offers HSM partitioning, 100+ clients, high-performance cryptography, features and capabilities updated in-field, feature-rich
▶ Cloud-Ready	Provision via Crypto Command Centre, supports virtual environments, high security client binding, available in physical and CloudHSM models
▶ Enterprise-Ready	Robust High Availability, complete remote manageability, secure shipping, comprehensive signed audit logs, wide-ranging SNMP support, crypto utilisation metrics and controls

▶ Luna SA

SafeNet. THE DATA PROTECTION COMPANY

Authentication, Signing & Key Issuance PCI-e HSM

- **Certifications** — Validated to FIPS 140-2 (level 2 and level 3), security boundary is the HSM itself – keys always in hardware, hardware backup
- **Flexibility** — A choice of Signing or Key Export, 3000 or 7000 RSA s/s, Password or PED-Authentication, features and capabilities updated in-field
- **High Performance** — Highest performance for Signing and Encryption, ideal for use as an embedded HSM in servers or appliances
- **Enterprise-Ready** — High Availability support, complete remote manageability, secure shipping, comprehensive signed audit logs, crypto utilisation metrics and controls

Luna PCI-e

SafeNet. THE DATA PROTECTION COMPANY

Root-Key Protection USB-attached HSM

- **Certifications** — Validated to FIPS 140-2 (level 2 and level 3), security boundary is the HSM itself – keys always in hardware, hardware backup
- **Flexible** — A choice of Signing or Key Export, Password or PED-Authentication, features and capabilities updated in-field
- **Form Factor** — USB attached, ideal for storing offline cryptographic material such as in a Root CA, can be connected to a server or to a Luna SA
- **Enterprise-Ready** — High Availability support, complete remote manageability, secure shipping, comprehensive signed audit logs, crypto utilisation metrics and controls

PCI-e & Network-Attached Programmable HSMs

- **Certifications** — Validated to FIPS 140-2 level 3, security boundary is the HSM itself – keys always in hardware, hardware backup
- **Customisation** — Programmable HSM enabling custom commands, algorithms, mechanisms and functions to be added in-field
- **Rich API Support** — Full and flexible support for PKCS #11, Java, Microsoft Crypto APIs – developer friendly tools
- **Flexibility** — A range of cost/performance/form-factor models to meet a wide variety of use-cases and deployment models

ProtectServer

SafeNet. THE DATA PROTECTION COMPANY

Network Attached Payments HSM

Certifications	Validated to FIPS 140-2 level 3, PCI-HSM certification, PCI P2PE Compliance
Standards	Support for Visa, Mastercard, EMV, American Express, Global Platform, CEPS, German ZKA Debit Card, Italian Banking and Debit Card
Rich API Support	Offers comprehensive and rich payments API, as well as support for alternative common Payment HSM command sets
Remote Management	Luna EFT Remote Management removes the need to visit data centres in order to manage payment HSM infrastructure.

Luna EFT

SafeNet. THE DATA PROTECTION COMPANY

Why SafeNet HSMs ...

- Crypto Hypervisor

- AWS CloudHSM

- SWIFT

- Enterprise Key Management Support
  - KMIP

SafeNet. DATA PROTECTION COMPANY

Conclusions

1. Infrastructure to **Consolidates**, **Provisions** and **Manages** the MOST cryptographic assets on the market
2. Flexible solution for **Physical**, **Virtual** and **Cloud** environments, which enables **customer /partner /solution provider** evolution and choice
3. Provide **Compliance**, **Governance** and **Control** for distributed cryptographic assets

SafeNet. THE DATA PROTECTION COMPANY

Thank You!