



Data Security Overview

GTUG – May 2018

Darren Burkey, Senior PreSales Consultant Atalla

darren.burkey@microfocus.com

The New Combined Company: built on stability, acquisition and innovation



MICRO FOCUS

COBOL

Borland **SERENA** **Novell**

SUSE **Attachmate** **NetIQ**

40
Years



Hewlett Packard Enterprise

Network Management/
Data Protector

FORTIFY SOFTWARE

OPSWARE **MERCURY** **ArcSight** **VERTICA**

Peregrine **SHUNRA** **ATALLA** **Voltage** security

30
Years

“Better Together” Portfolio Has Breadth and Depth



DevOps



Cobol Development,
Software Delivery
and Testing



IT Operations

Service Management,
Operations Bridge,
Data Center
Automation,
Network Management

Mainframe Solutions,
IT Operations
Management,
Host Connectivity,
Collaboration



Cloud

Cloud Service
Automation,
Hybrid Cloud
Management



Workload Migration



Security



Identity-based
Access Governance
and Security



Information Governance

Digital Safe, Data Protector,
Control Point,
Structured Data Manager,
Storage Optimizer



Linux & Open Source



Enterprise Linux,
OpenStack Private Cloud,
Software-defined
Storage

Big Data Analytics

VERTICA | IDOL

Data security portfolio: Voltage & Atalla

Data privacy & security compliance
& risk reduction

Secure analytics, privacy and
pseudonymization

Hybrid cloud data protection &
collaboration



Voltage SecureData

Enterprise, Big Data, Cloud, Mobile and Payments Data Security
Tokenization, Encryption, Masking



Voltage SecureMail

Easy, scalable email encryption

Voltage SecureMail Cloud

Enterprise email encryption SaaS



Atalla HSM

Payments crypto appliances & key storage



Enterprise Secure Key Manager

KMIP Key Management for Storage, 3rd party apps



Atalla Product Overview

History of Atalla

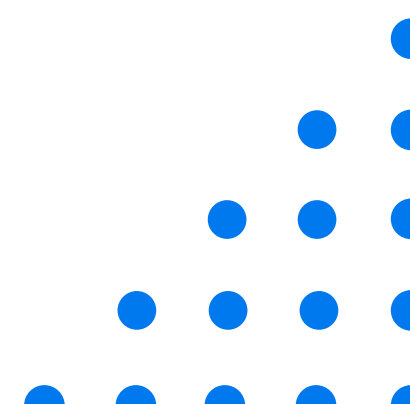
- Established in 1972
- Mission: Protect financial transactions
- Atalla introduced first Network Security Processor (NSP) in 1979
- Acquired by Tandem Computers in 1989
- Tandem acquired by Compaq in 1997
- Compaq acquired by HP in 2002
- HP splits with HPE in 2014
- HPE Software Spin Merges with Micro Focus in 2017



Martin 'John' Atalla (1924-2009)



ESKM: Enterprise Secure Key Manager



Why is enterprise key management a problem?



- **Storage encryption is a necessary cost of business to defend storage media breaches...**

- A well-proven **defense** against breaches—highly effective, often mandated for storage and servers
- **Easy** to implement: AES keys, standardized, now embedded—but...



- **Key management is a difficult social engineering problem...**

- Maintain central controls: Lose access to keys locally → lose access to the data
- Enforce consistent policy: Who manages keys? What authorization?
- Audit and prove compliance: Regulatory mandates require evidence of protection



The challenge is to coordinate and automate controls that protect access to keys across storage encrypted data, while remaining transparent to operations

Protecting data-at-rest with encryption

- **Scope:** Data-at-rest

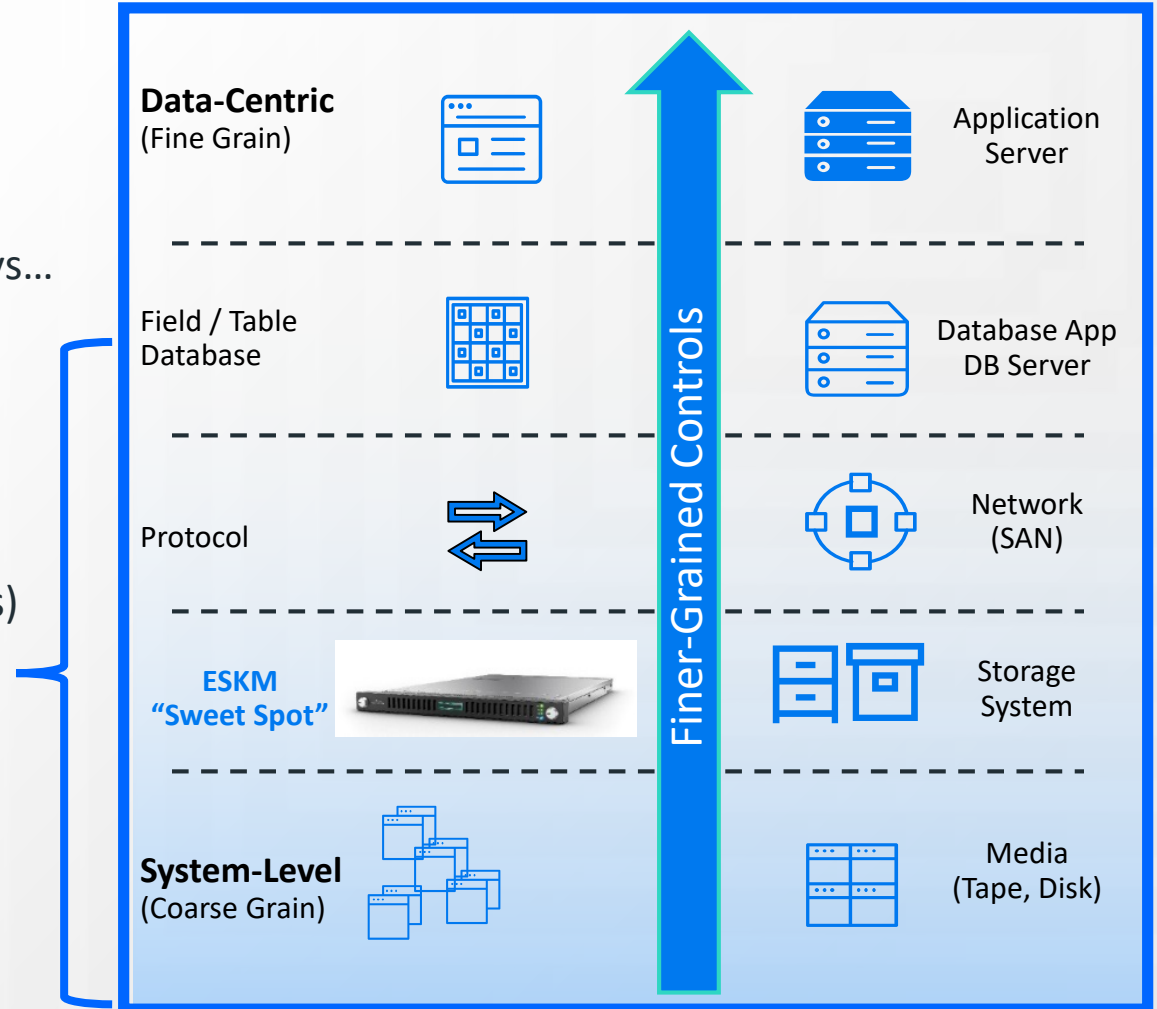
- Products: Storage, servers, networking...
- Applications: IT infrastructure, cloud, SAN...
- Solutions: Archiving, backup; block data; unlock keys...

- **Unlike:** Data-in-use, data-in-motion

- “Data-centric” application-level (see: SecureData)
- Tokenization, format-preserving (fine-grain controls)

- **Why do customers care?**

- Quick to implement with compliance deadlines!
- Global policy over large IT server/storage estates
- Easy, coarse-grain controls, undifferentiated data



ESKM – Enterprise Secure Key Manager

High-assurance key protection for a wide range of storage encryption applications

■ Primary Value Proposition

- Centrally manage global enterprise keys
- Reliably separate keys from the data
- Automate to simplify operations

■ Integrates large storage and server ecosystems

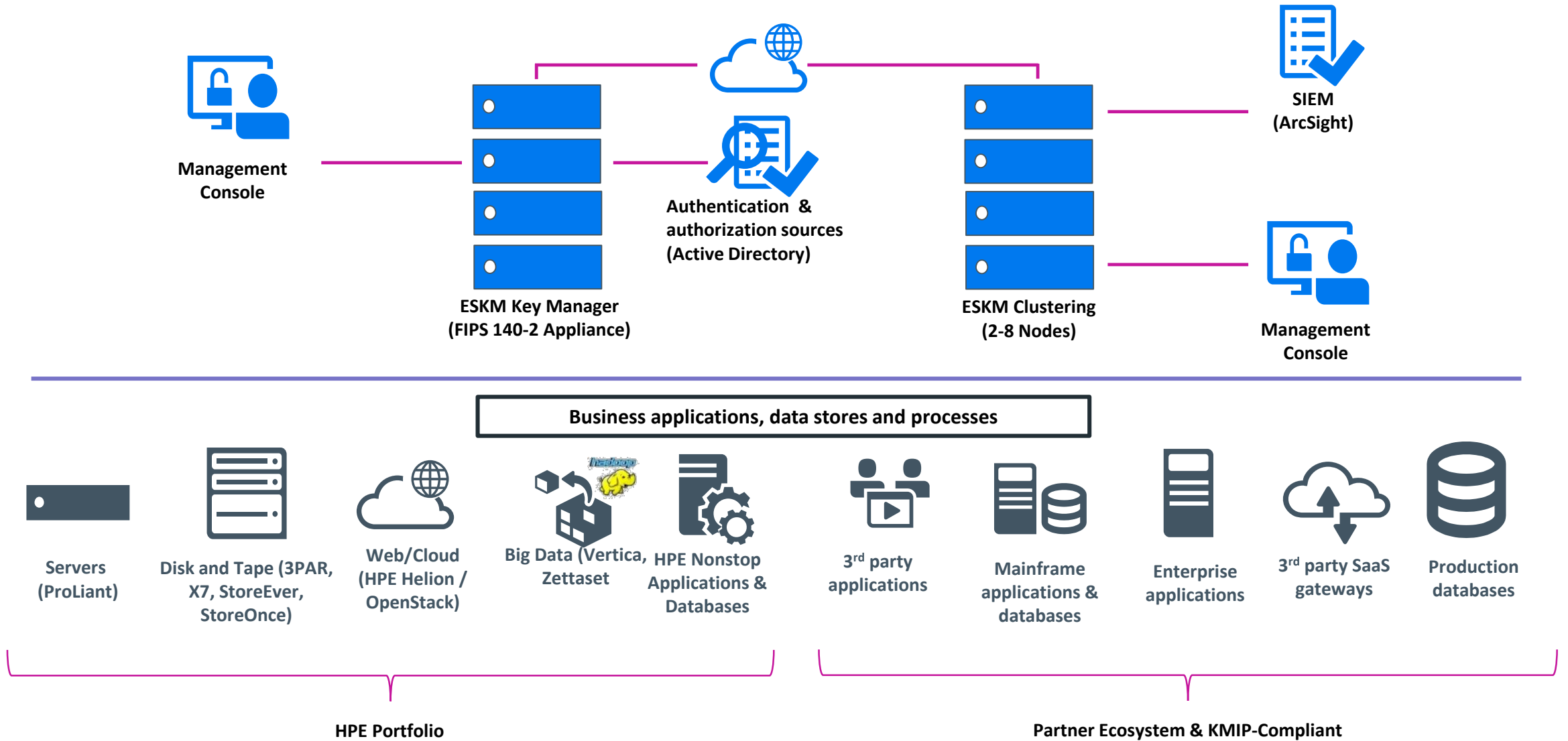
- Storage, server, cloud, backup...
- KMIP standard pre-qualified applications

■ Features at a Glance

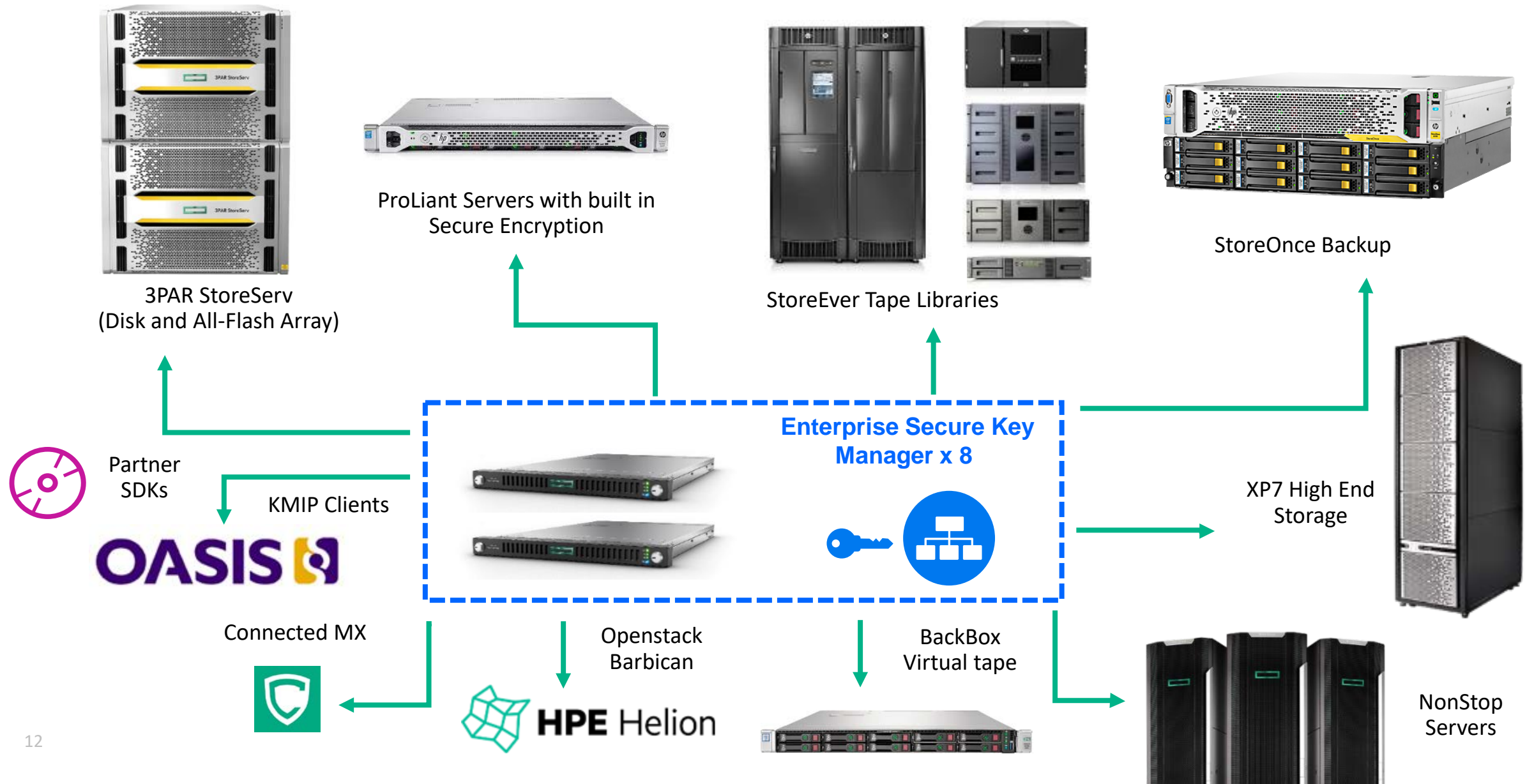
- **Trusted:** FIPS 140-2 Level 2
- **Reliable:** 1U redundant, proven hardware
- **Available:** 8-node appliance clustering
- **Scalable:** 25K clients, 2M keys, app groups
- **Interoperable:** industry-standard KMIP 1.4



ESKM: Integrates data-at-rest encryption management

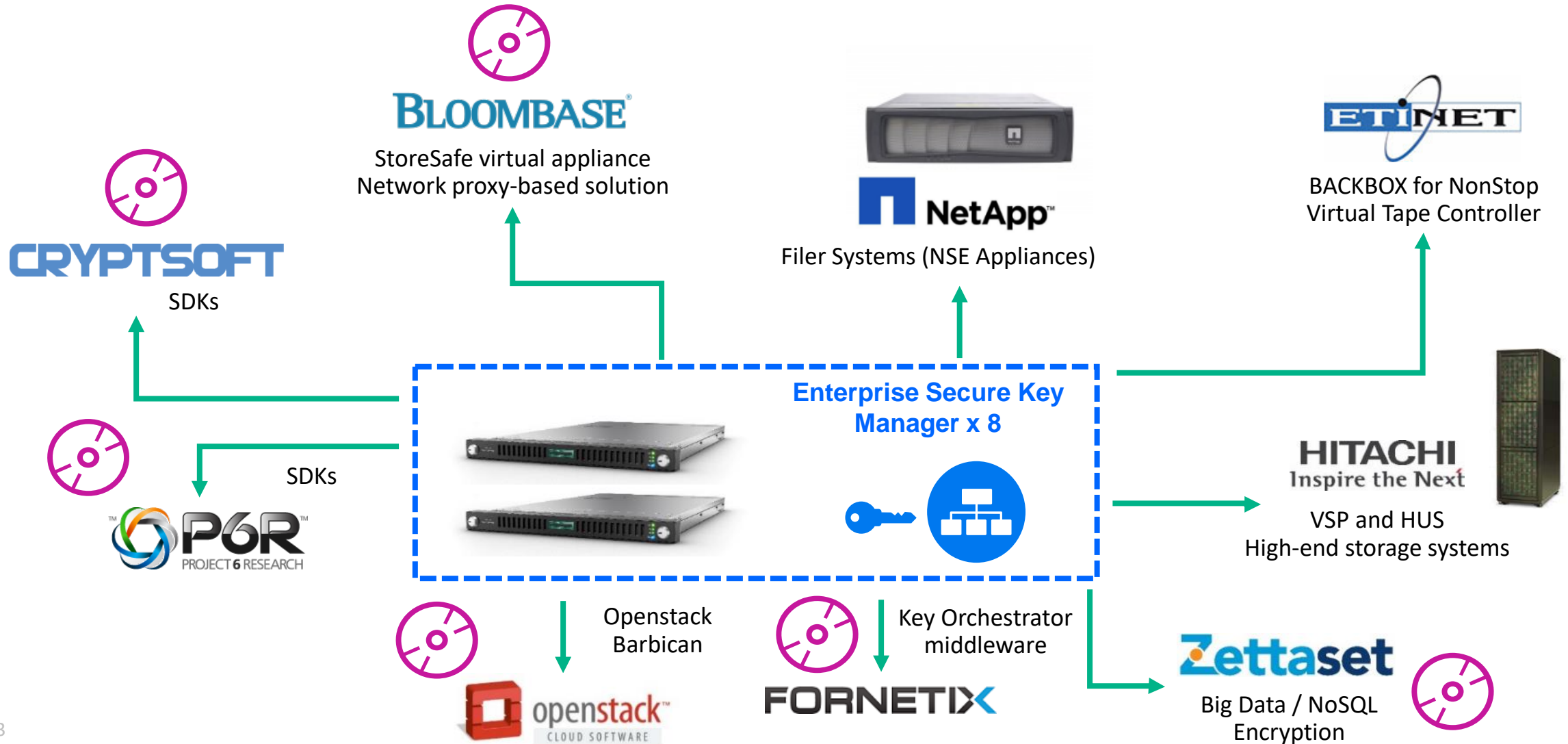


Security & business continuity with market-leading interoperability



OASIS KMIP standard: Open interoperability for easy expansion

ESKM leads the market in KMIP operational compliance for application interoperability



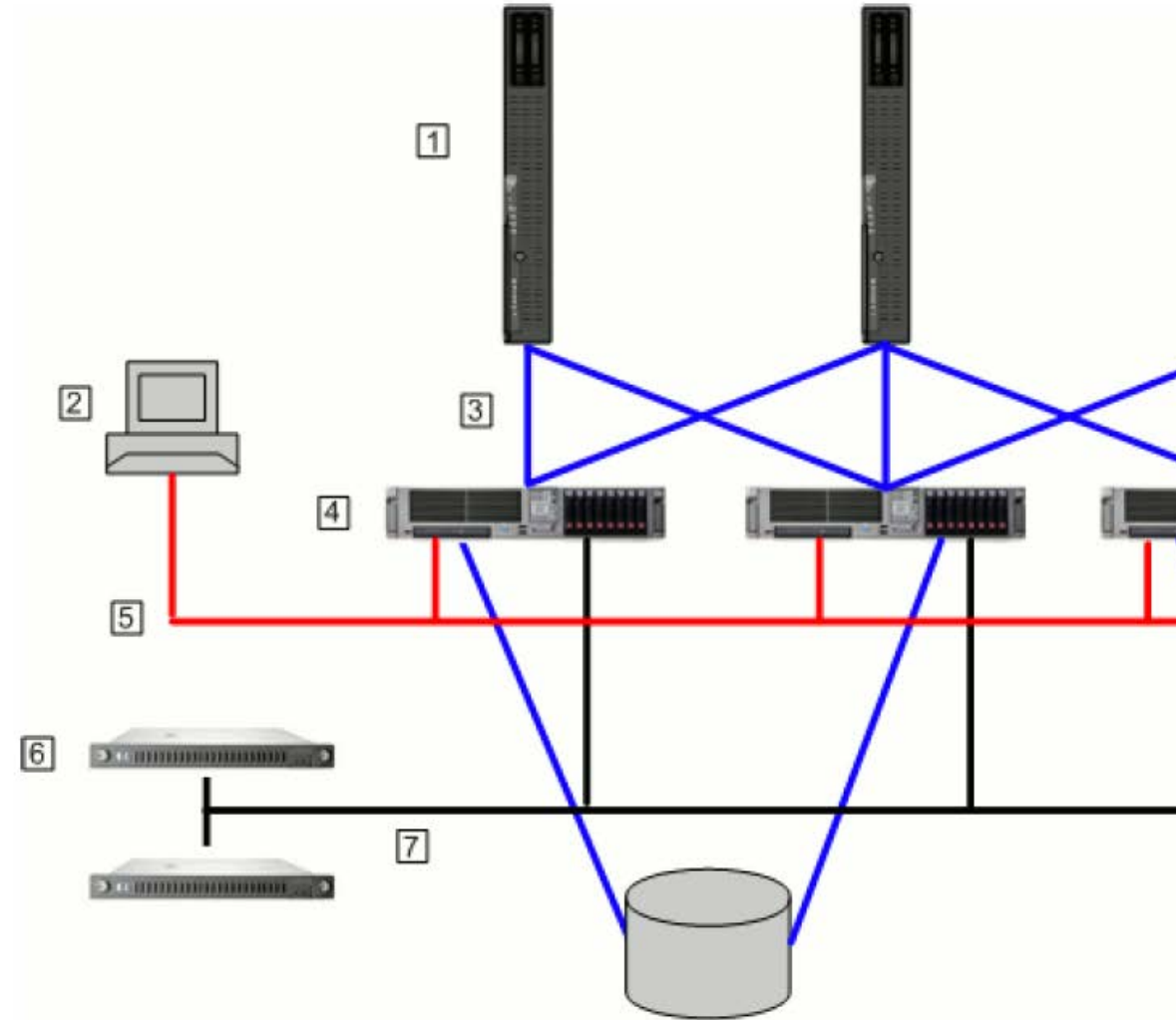
ESKM with NonStop VLE

Volume level encryption is supported on these systems:

- NonStop X (L-series)
- NonStop Integrity BladeSystems (J-series)
- NonStop Integrity NS16000 series servers (H-series)
- NonStop Integrity NS2000 series servers (H-series)

Encryption is supported on these devices:

- SAS disk drives
- Enterprise Storage Servers
- LTO-4, LTO-5 and LTO-6 tape drives
 - encryption may be applied per-drive or per-media



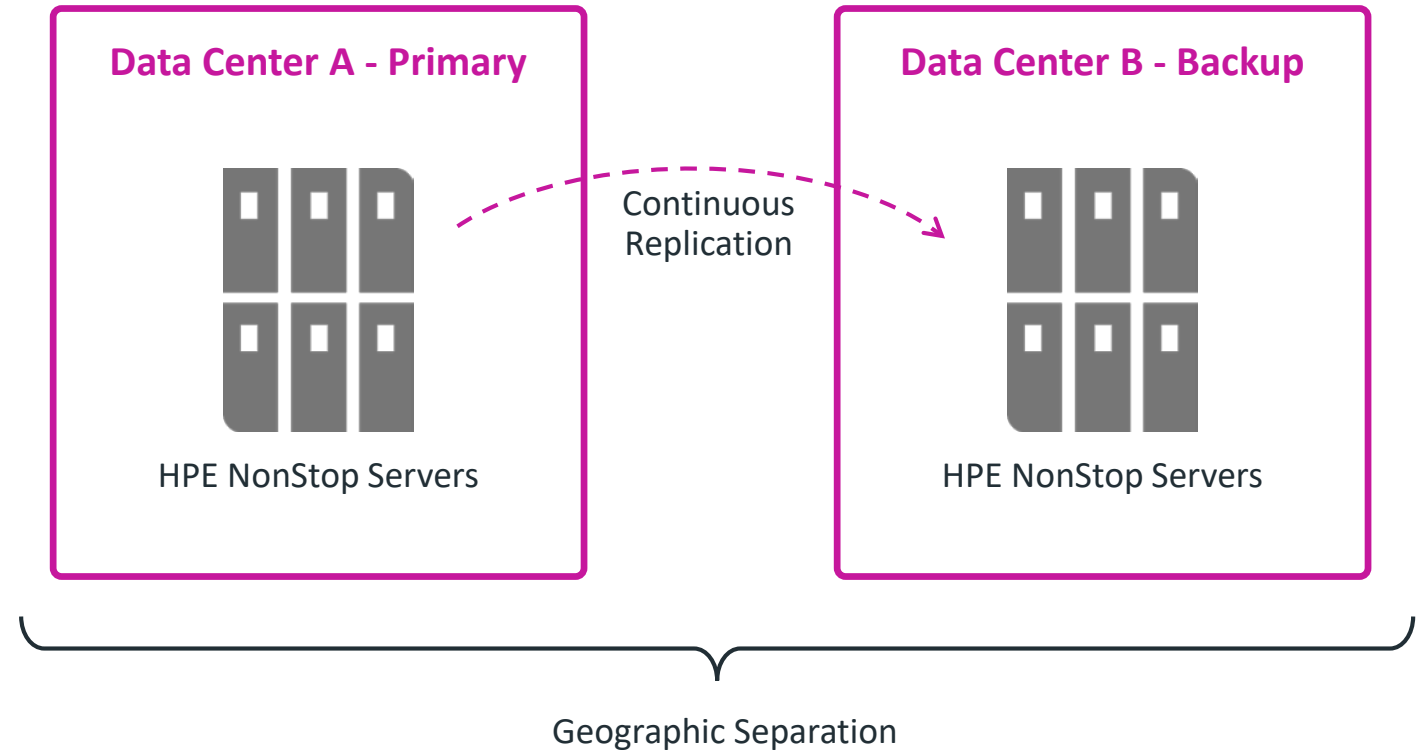
Global Payments Network Protects Core Transactional Data with ESKM on HPE NonStop

Business user

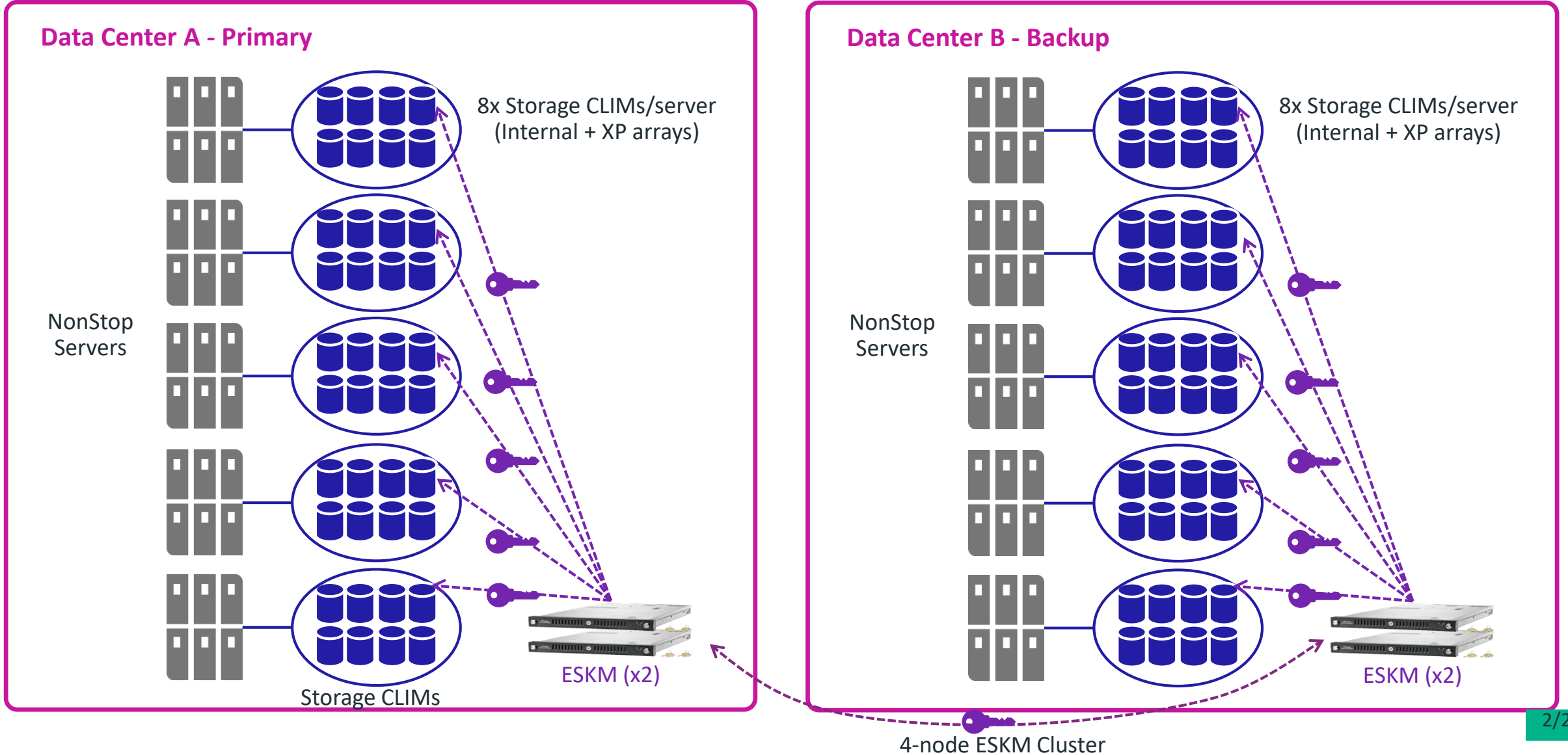
- Application IT
- Sensitive data
- PCI/PII data
- Business Challenge
- Continuously protect customer data at massive scale in extreme transactional environment

Data Infrastructure

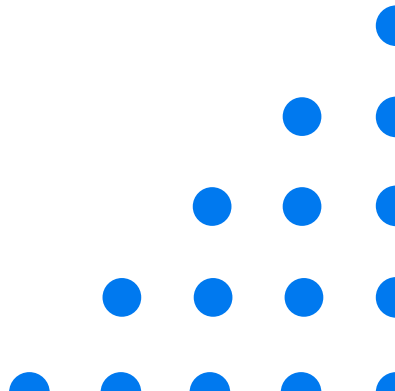
- HPE Integrity NonStop blade systems (NB56000, NB54000), Internal storage + XP storage arrays
- Fully replicated across two sites



Global Payments Network – Atalla Solution



Atalla HSM



What is the Atalla HSM?

Atalla Hardware Security Module (HSM) Is a **Payments Security Module** for **protecting sensitive data** and associated **keys** for **non-cash** Retail Payment Transactions, Cardholder Authentication and Cryptographic Keys

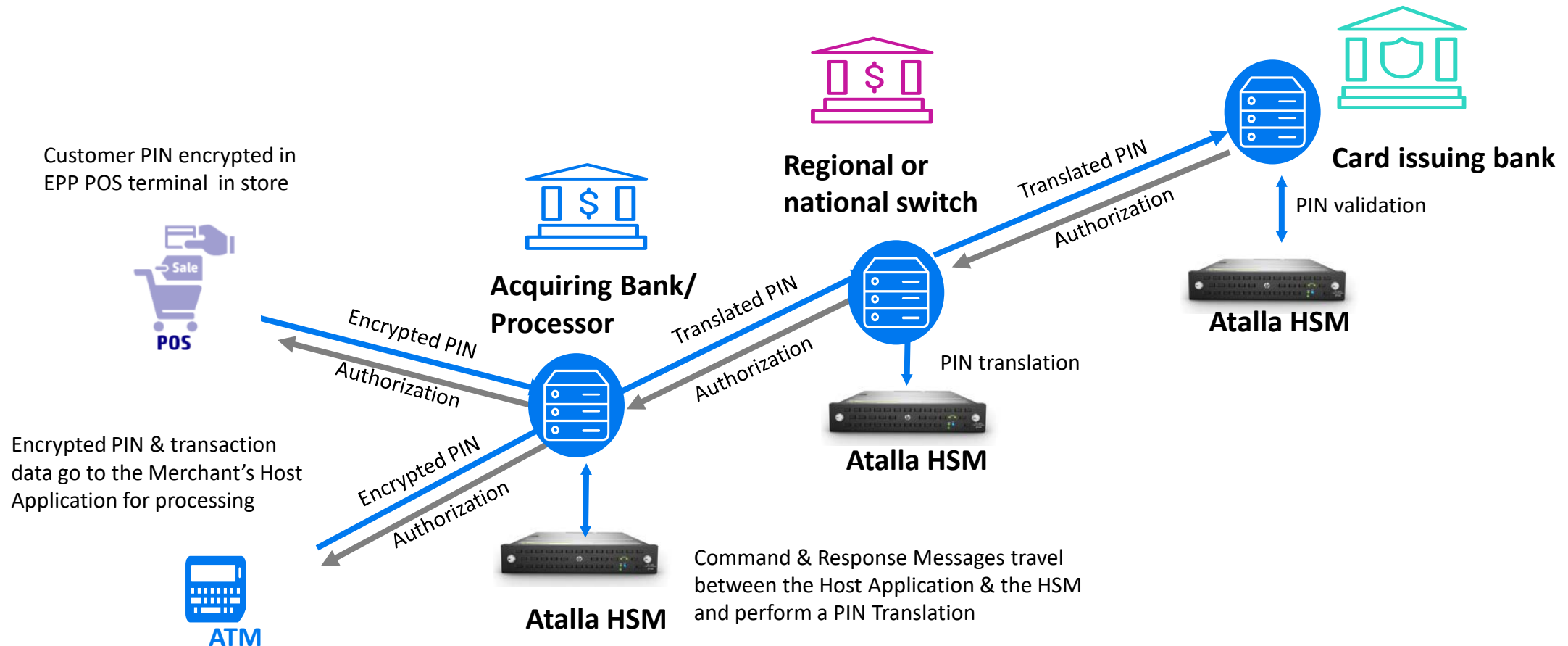
Atalla HSM enables **data** and **ecommerce protection** and **key management** operations for:

- PIN Translations
- Payment Card Verification
- Production And Personalization
- Electronic Funds Interchange (EFTPOS, ATM)
- Cash-card Reloading
- EMV Transaction Processing
- Key Generation And Injection



Atalla HSM – payments processing

The PIN, as it travels the payments network, is always encrypted and decrypted within the boundary of a Secure Cryptographic Device

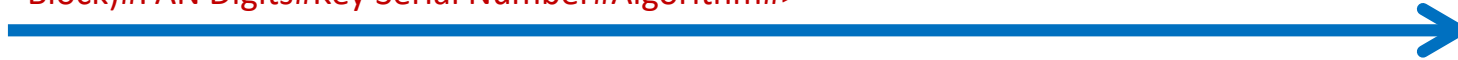


The Atalla HSM Command Message



Host System with a Payments Application

<31#7#Header,EMFK.E(Derivation Key),MAC#Header,EMFK.E(KPEO), MAC#EKPEn(PIN Block)#PAN Digits#Key Serial Number#Algorithm#>



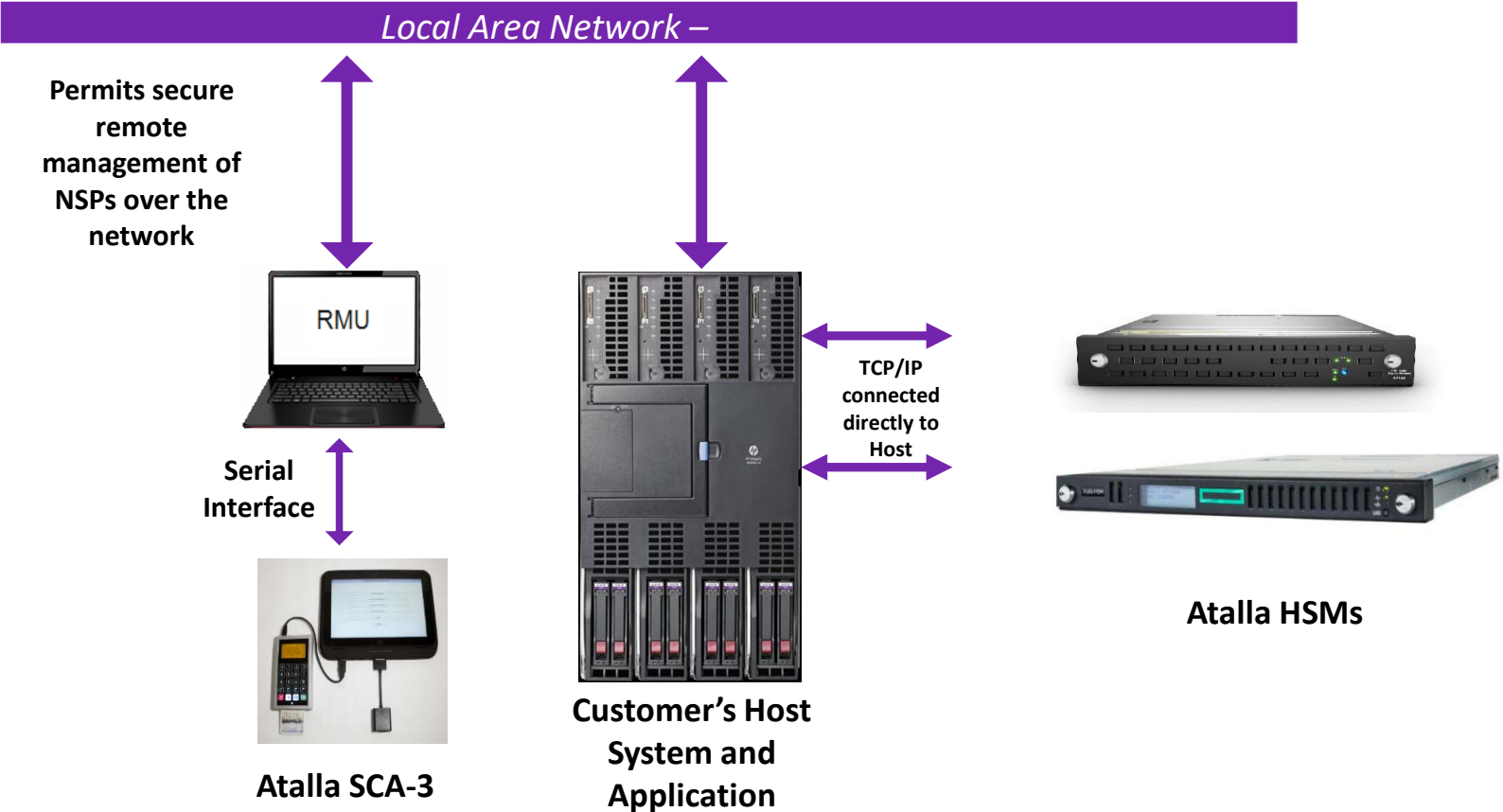
Atalla HSM

<41#EKPEO(ANSI PIN Block)#Sanity Check Indicator#[CRLF]



Atalla HSM & HPE NonStop

- Optimized Native Integration
- Improved Performance Efficiency Solution
- Allows Atalla HSM to sit “behind” the Customer Application running on the NonStop Server
- Still Access Atalla HSM Remotely



Boxcar

Atalla HSM Support on HPE NonStop platforms

- AAP – HPE Itanium
 - Currently available
 - Additional keep-alive features
- AAQ – HPE Integrity NonStop X
 - Currently available
 - Functionally the same as AAP
- Boxcar on Linux
 - Currently in Beta
 - Includes Load Balancing



What's New In Atalla HSM AT1000

| New Functionality | Description | |
|----------------------------------|---|---|
| Enhanced Monitoring Capabilities | SNMP (Polling & Traps) | ✓ |
| | Syslog | ✓ |
| Algorithm / Key Types | AES Keys | ✓ |
| | 4096-bit RSA keys | ✓ |
| Simplified Pricing | To ease the sales cycle | ✓ |
| Performance | Up to 10,000 TPS (Visa PIN Verifications) | ✓ |
| Form Factor | 1U chassis | ✓ |
| FIPS | FIPS 140-2 L3 Certified | ✓ |

Atalla HSM

Unique Capabilities to Payments Market

- **Unique PCI Certified Dual Control**
 - Dual Control is required by PCI
 - 'Workflow based model' – administrators do not have to be present to perform activities
- **Extremely Advance Backup / Restore Capability**
 - A policy can be set to allow N of M cards must be required for a restore" and/or approve changes
 - Protects against past lost or destroyed smart cards
- **Creator / Innovator of the ANSI Key Block**
 - Atalla Key Block is the proposed ANSI Key Block standard for the industry



Atalla HSM: AT1000

Hardened, secure environment for payment-specific cryptographic operations

Value Proposition

- FIPS 140-2 Level 3 approved HSM
- Payments Built-in Functionality, 80, 280, 1080 PIN Translate

Certified / Integration with 3rd Party Payments Ecosystem

- Promoted by Enterprise Security Partner Programs (Technology Alliances, System Integration Partners)
- Integrated solutions with all top payment ecosystem partners

Features at a Glance

- **High Performance:** 1U form-factor, high-performance economics
- **Full Payment Solution:** Visa, MasterCard, EMV, AMEX, Global Platform
- **Highest Availability:** Supports Native & Customer HA
- **Scalable:** Designed & supports Infield license upgrade(s)
- **Assurance Certified:** NIST FIPS 140-2 Level 3 validated & PCI-HSM V3.0 pending





Thank you

www.microfocus.com