

Secure Storage

Encryption Implications

Data Storage Security Summit
September 24, 2015

PROBLEM

ATTACKS OUTPACING DEFENSES



Office of Personnel
Management

Sony Picture
Digital Break-in

E-Bay
Compromised

Staples
Data Breach

Kmart
Victim of
Hacker Attack

Home
Depot
Credit
Card Theft

Target
POS
Breeched

Anthem Health
Malicious Attack

- No longer IF, but
WHEN and HOW BAD
- Heartbleed Hack
2/3 Internet Servers
- Cyber-Warfare, Industrial
Espionage
- FBI Cyber Division
500M Finance records
(12 months)
- Cost of a Data Breach
average \$5.5 million

Attackers don't just want to get in, they want the stored data

STORAGE ON THE FRONT LINES

Canary in the Coal Mine



- Where does storage reside?
Everywhere!
- What types of storage targeted?
All Types!
- Is there a 'Silver Bullet'?
No!
- Can we do something?
Yes, Encrypt!

Storage systems can't rely on perimeter security to keep data safe

SOLUTION

Visionary, Scalable, Disruptive

Protect
Data-at-Rest
&
In-Transit



Encryption Is Needed
Everywhere
~ Millions & Billions ~

Bypass
“Complexity Culture”

Key Orchestration™

Encryption key management at scale is a data messaging problem - not an encryption problem

Integrating Identity & Policy with Encryption Management Workflow = Automation & Optimization

Utilizing Open Standards maximizes interoperability, accelerates broader encryption usage, and lowers the historically high costs of managing encryption.

Enabling the 21st Century Secure Data Revolution

COMPLEXITY REDUCED

Single, Powerful, Integrated

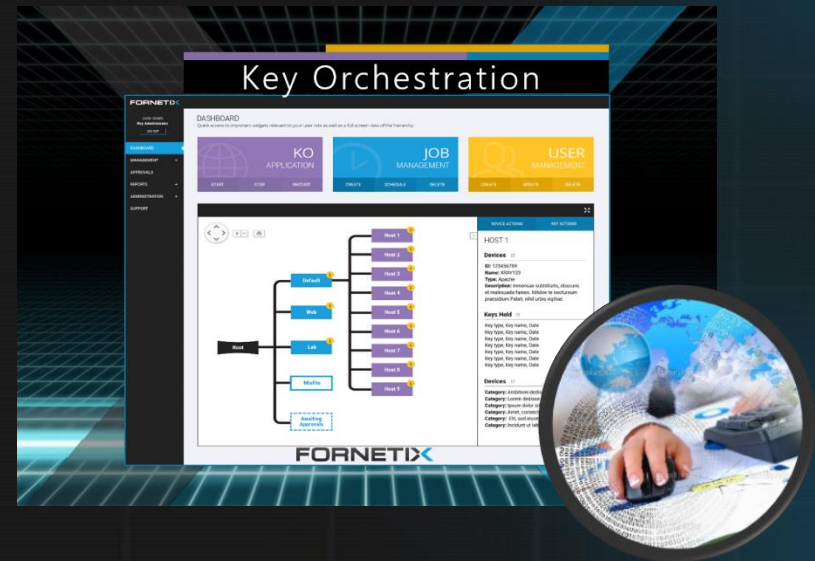
Current Encryption Key
Management
IS DONE MANUALLY!



Grid Views

VS.

Modern Interface
Workflow Automation

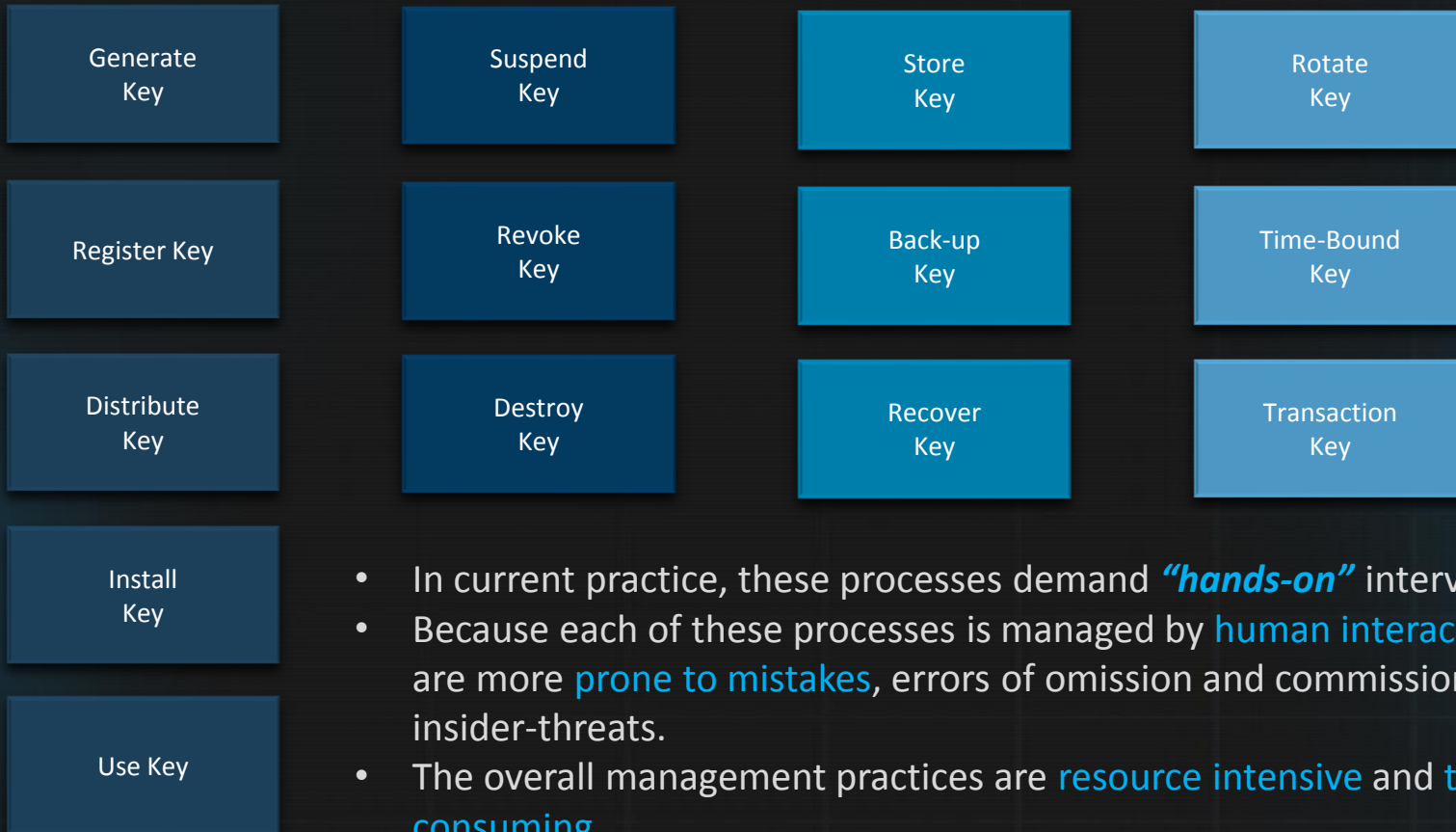


- Multiple, Cumbersome Interfaces
- Operationally Complex
- High Costs, Slow to Innovate
- Scale-adverse

- Unique Tree Structure Interface
- Simple, Easy to Use, Powerful
- Disruptive, Affordable Pricing
- Architected to Scale to Millions

KEY MANAGEMENT - LIFECYCLE

Many Points of Failure



KEY ORCHESTRATION™

Pre-defined, Tested Policy Interface, Tools, and Automation

Audits Key
Generation, from any
approved source

Automatically
Suspends Keys
Rules Violation

Wraps & Stores
Keys
Rules Based

Automated Key
Rotation
Management

Prompts & Manages
Key Registration

Automatically
Revokes Keys
Rules Based -
Alarms, Roles, etc

Supervises & Audits
Back-up
Keys

Time-Bound
Key Supervision
& Auditing

Distributes Key
based on Policy
Instruction

Destroys
Keys
According to Policy

Inherent Key
Recovery tools

Transaction
Key Supervision
& Auditing

Installs Keys
Automatically
according to a Plan

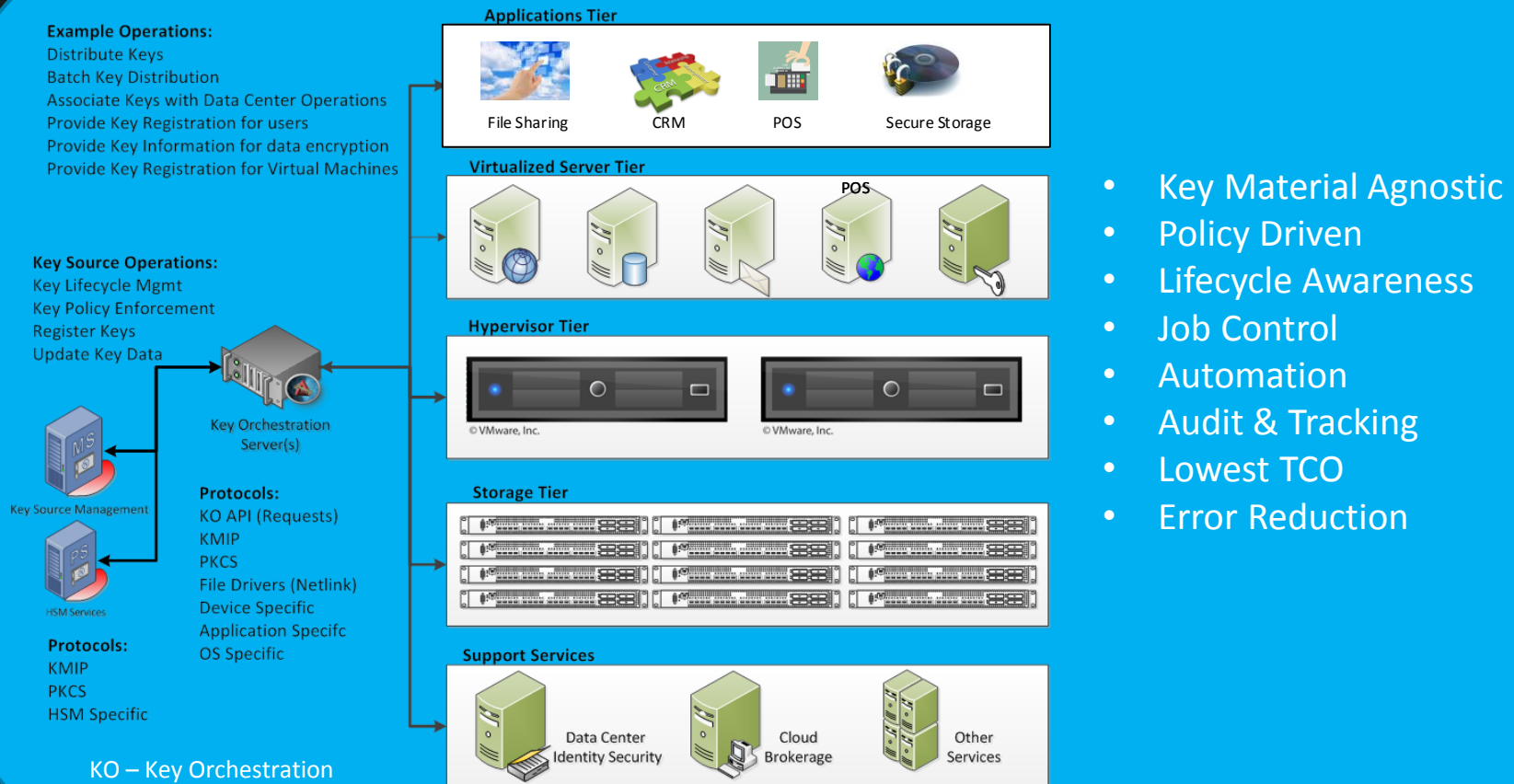
Monitors & Audits
Key Usage

- **Key Orchestration™** plans and stages each element of Key Management in automation, well ahead of execution.
- **Benefits** include testing prior to deployment, greatly reduced operations resources, elimination of most security errors (including insider threats), and substantially reduced time to execute.

USAF SMC Satellite rekey demo: 48 hours reduced to 30 minutes

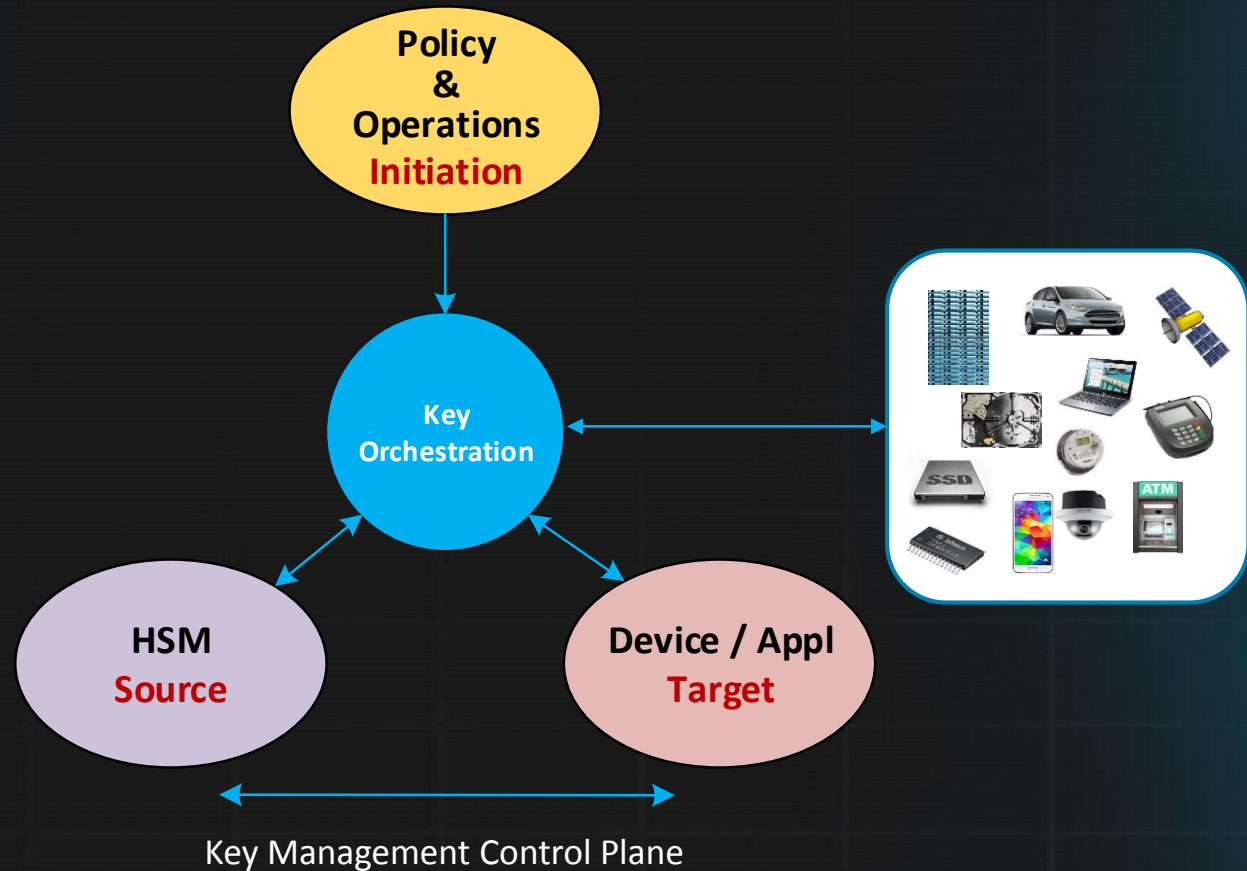
CONSOLIDATED MANAGEMENT

Manage Keys Across Platforms



ORCHESTRATING ENCRYPTION USE

Key Management Control Plane

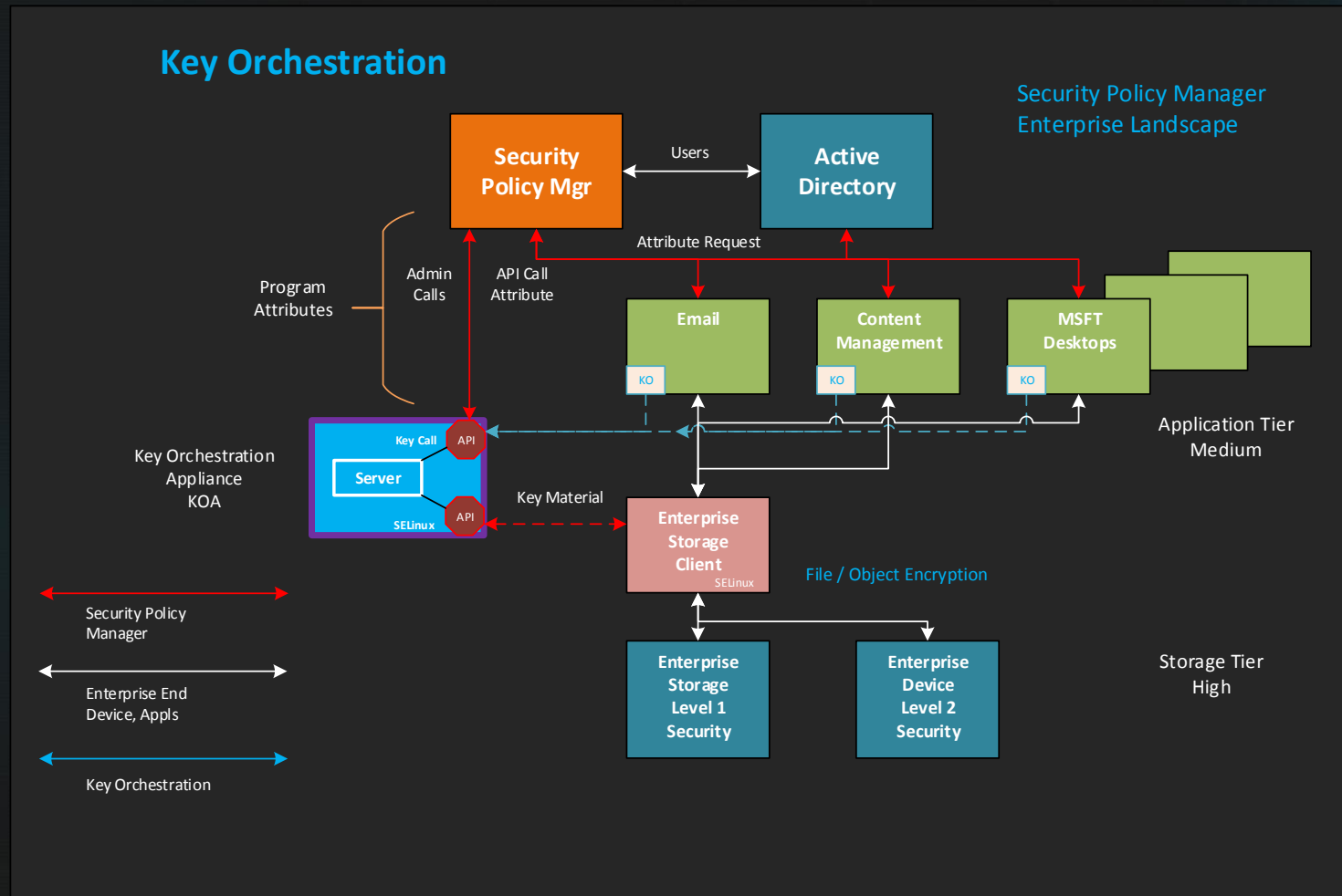


Fornetix Partners
Hardware Security Module

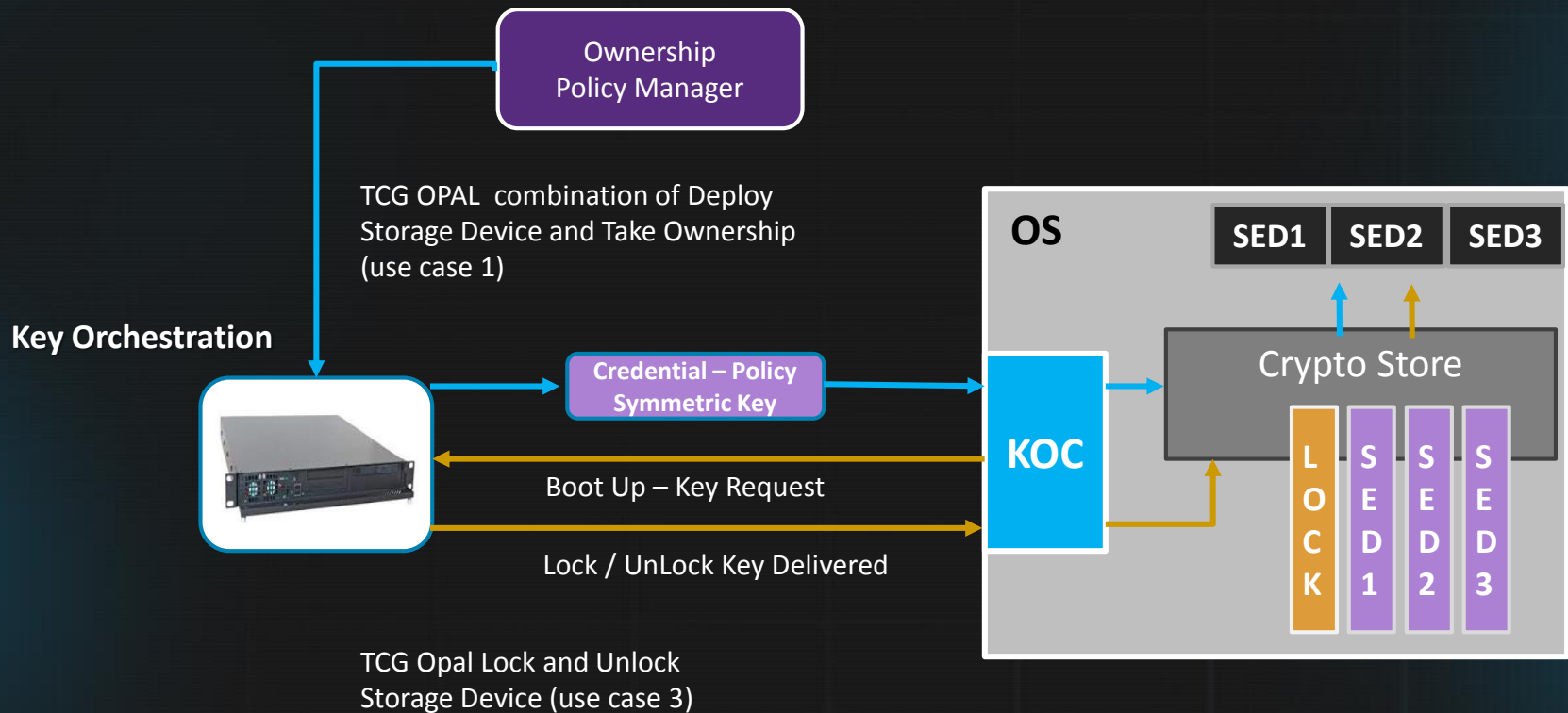


ENCRYPTION IMPLICATIONS

Fine Grained Encrypted Storage



TCG OPAL USE CASES



MONETIZING ENCRYPTION

Enable Encryption as Killer App

Aligning the management of encryption keys with business processes where the use of encryption can now be deployed effectively and efficiently to create new value propositions .

Hard Disk Drive Asset Management

- In-Use Inventory
- Day 1 to EOL

Decommission Auditing

- Proof: Out-of-Use
- Regulatory Compliance

Cryptographic Erase

- HDD/SSD Data “Bricked”
- Encrypt → Destroy Key → Reuse Asset

SECURE DATA REVOLUTION

Historical

2014

Dumb Client

Uni-Directional

- Key Request
Device side Only
- Static Attributes
Single Use
Device Type
Flat Key
Forklift Updates

10s of Thousands

Attribute Barrier™

2015-2018

Smart Client (Fornetix)

Bi-Directional

- Key Request
Either Side
- Dynamic Attributes
Identity
Policy
Location
Federation

100s of Millions

Encryption Horizon™

2020

Micro Client (Fornetix)

Multi-Directional

- Key Request
IoT Intelligence
- Micro Attributes
Chip Level
High Function
High Frequency
Low Latency

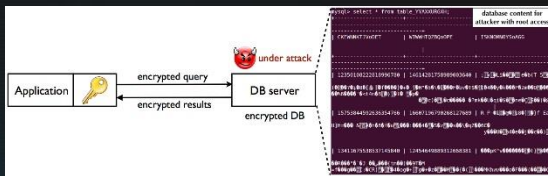
10s of Billions

HOMOMORPHIC ENCRYPTION

Key Orchestration is architected for high scale and ubiquitous encryption functioning across current and future encryption deployment innovations.

CryptDB:

Encrypted database and query processing



Advanced data base systems supporting primary end-user encryption managed data objects, such as CryptDB, will benefit greatly from Fernetix vision of an Encryption Horizon™.

Mylar:

A platform for building secure apps



Key Orchestration's unique alignment of policy, identity, and federation provides for multi-level and cross-group associations of various encryption material, and their respective key usage profiles and techniques.

Advances such as these, portend a larger scale of encryption usage at the high and low end of computing systems and storage.

Thank you!

Bob Guimarin, CEO
bob@fornetix.com

info@fornetix.com
Tel: 703.687.9770