SECURE TECHNOLOGY ALLIANCE

US Executive Order: Strengthening Information Security with Key Encryption for Data at Rest

SECURE TECHNOLOGY ALLIANCE

US Executive Order: Strengthening Information Security with Key Encryption for Data at Rest

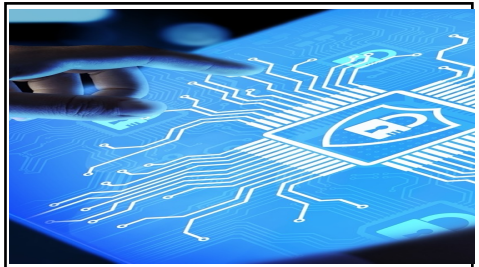
The webinar will start momentarily.

SECURE TECHNOLOGY ALLIANCE

US Executive Order: Strengthening Information Security with Key Encryption for Data at Rest

Manish Upasani, Product Manager | @manishupasani
Mark Azadpour, Sr. WW Security Workload Product Manager | Computesecurity@hpe.com

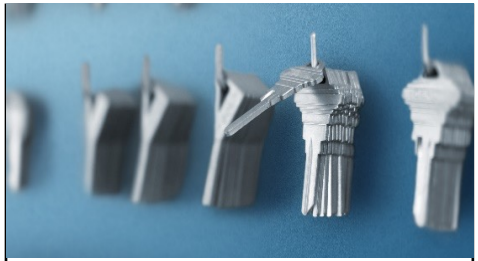
Agenda



Introduction

Federal Mandate

Q&A



Data Encryption &
Key Management

Secure Technology Alliance

Speaker – Manish Upasani

Introducing Your Speaker

utimaco®

Product Manager at UTIMACO

- **Key Management & HSM Portfolio**
- **15+ years industry experience**
- **10+ years UTIMACO product experience**
- **Certifications**
  - CISSP
  - TOGAF Certified
  - CTGA UT
  - CCSK-Plus
  - CEH
  - ECSA/LPT
  - ETA-CPP

Speaker – Mark Azadpour

Introducing Your Speaker

Hewlett Packard Enterprise

Workload Security Product Manager at Hewlett Packard Enterprise

- 20+ years of experience
- Focused on security from user perspective
- Zero trust focused
- CPU assisted security products
- Data at rest, Data in motion & ISV ecosystem execution
- PMP certified
- Security Clearance

Introducing
UTIMACO

SECURE TECHNOLOGY ALLIANCE

Hewlett Packard Enterprise

utimaco®

We Protect…

…people and digital identities **against terrorism and cyber crime**

People and IDs

…financial transactions, data in motion and IoT devices **against theft and sabotage – in the cloud and on premise**

Transactions

Data and Ideas

…digital economy and digital transformation processes **against theft, abuse and manipulation**

With proven, future-proof technology, **products and solutions that meet regulation and compliance standards**

Investments

SECURE TECHNOLOGY ALLIANCE

Hewlett Packard Enterprise

utimaco®

Introducing
HPE

HPE is Your Partner in This Fast Pace Change Environment

HPE ADVANCING THE WAY PEOPLE LIVE AND WORK

BY ENGINEERING EXPERIENCES THAT UNLOCK YOUR FULL POTENTIAL

Growing Risk for **Cybersecurity Attacks**

Mega Trend: Jaw-Dropping Cyber Attacks and Insider Threats

Executive Order

The Latest U.S. Government Reaction

The White House Executive Order on Information Security

THE WHITE HOUSE

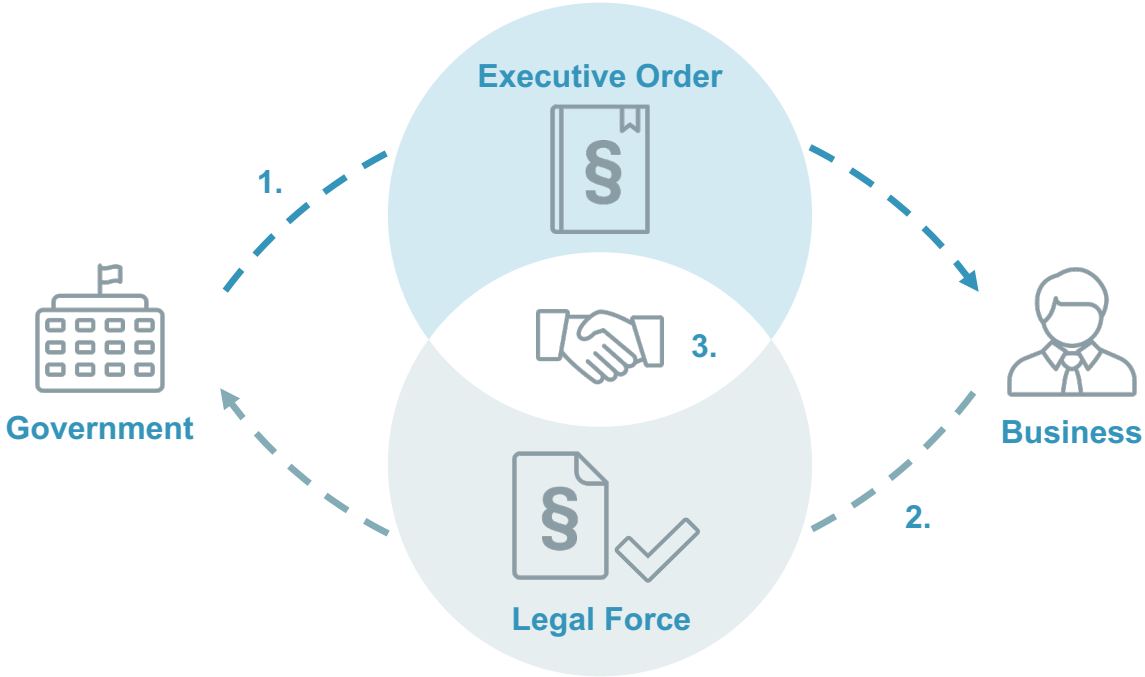
BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws.

Why Information Security may Impact Every Aspect of Your Business



Why Security Affects Every Business

Bad Press & Social Media

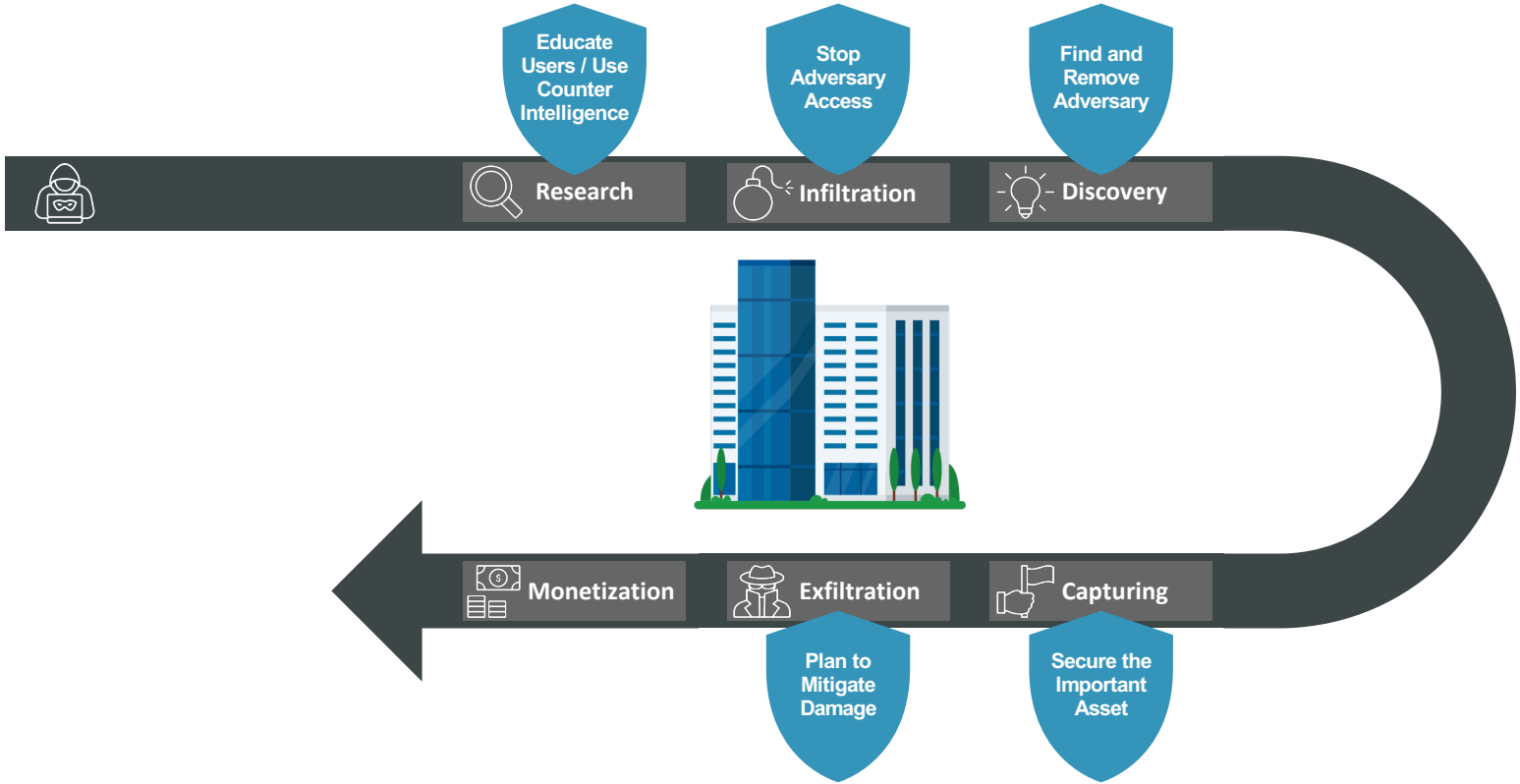
Regulatory Bodies
(e.g. PCI, HIPPA, SOX, FIPS, …)

How Does the Cybersecurity E.O. Affect You?

The Implementation is in Your Organization…

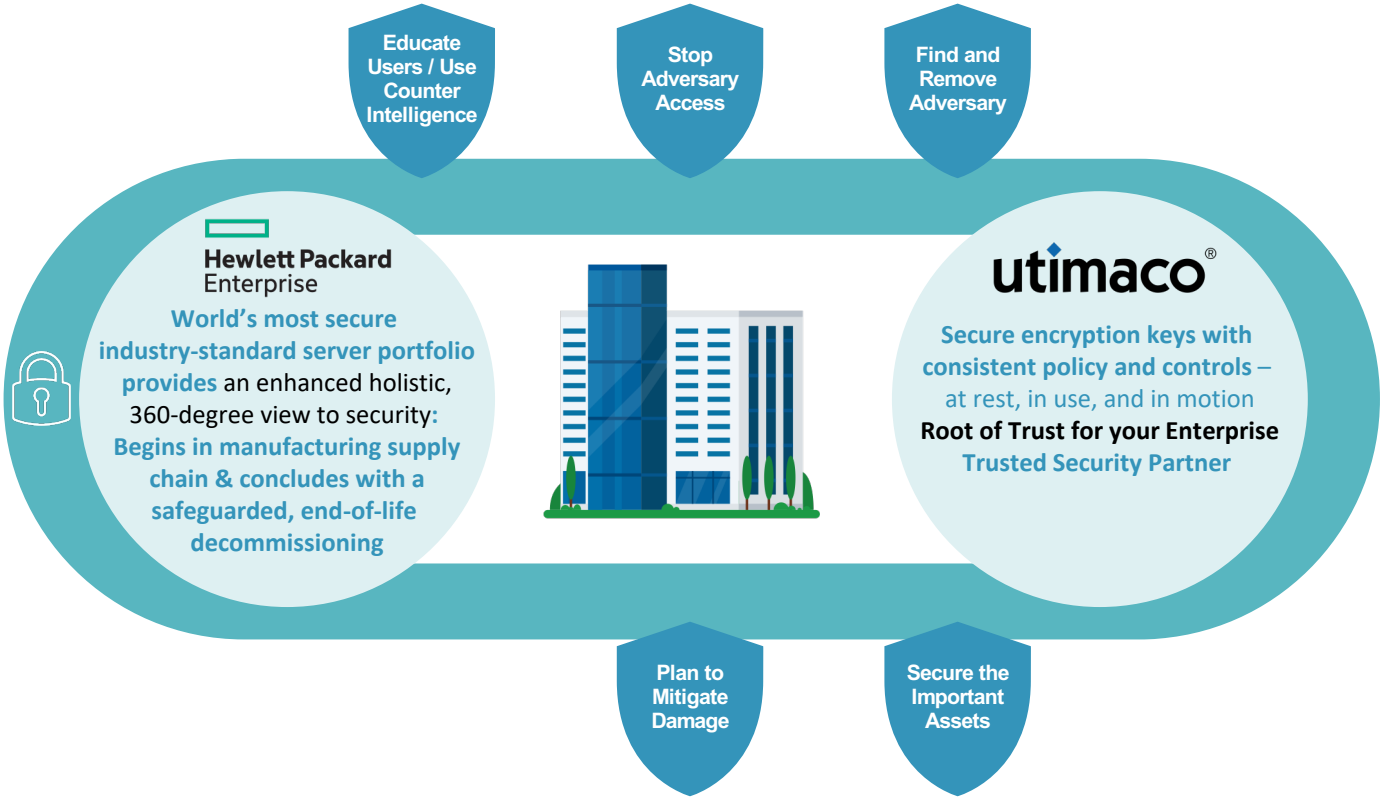
Disrupting the Adversary Ecosystem

Threats and Risks



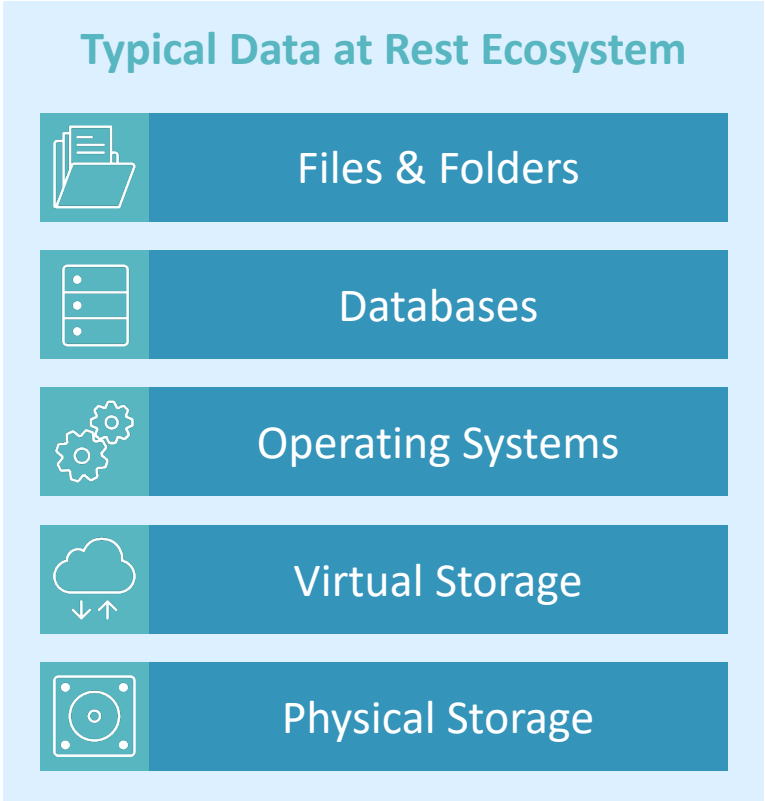
Disrupting the Adversary Ecosystem

Threats and Risks



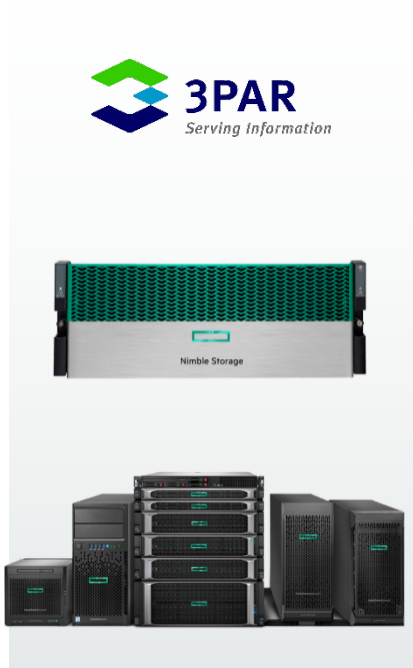
Is Cryptography the Answer to all Cybersecurity Threats?

Data and Information Being Threatened at Different Levels



Is Cryptography the Answer to all Cybersecurity Threats?

Data and Information Being Threatened at Different Levels



Typical Data at Rest Ecosystem

Physical Storage

A Bare Metal Server…

- **Can be stolen** by employees or intruders
- Can **fall into the wrong hands**
- What happens **if the data is not properly migrated?**
- Is it **safe against physical attacks?**

Is Cryptography the Answer to all Cybersecurity Threats?

Data and Information Being Threatened at Different Levels

vmware®

Microsoft Hyper-V

Typical Data at Rest Ecosystem

Virtual Storage

Physical Storage

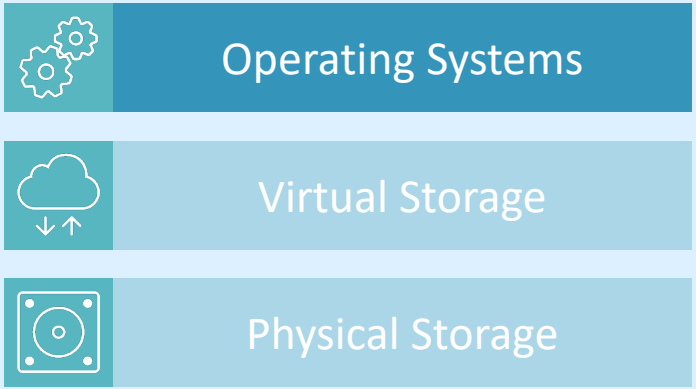
The Virtual HDD…

- **Can be stolen** by the VMWare admin
- Can be compromised by **hypervisor level attacks**
- **Is it safe against Ransomware attacks?**

Is Cryptography the Answer to all Cybersecurity Threats?

Data and Information Being Threatened at Different Levels

Typical Data at Rest Ecosystem



The Operating System…

- Can be attacked at the **application level**
- What happens if the **OS Admin is rogue**
- Is it **safe against logical attacks?**

Is Cryptography the Answer to all Cybersecurity Threats?

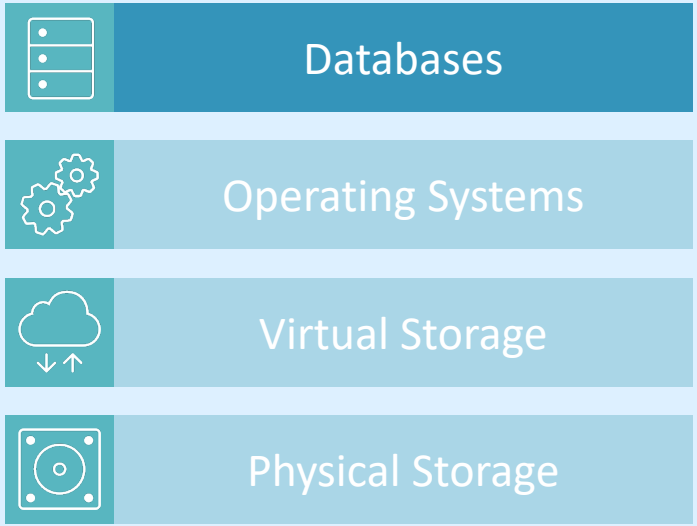
Data and Information Being Threatened at Different Levels

MySQL

IBM Db2

mongoDB.

Typical Data at Rest Ecosystem



The Database…

- SQL injection
- Disgruntled database admin
- Unsecured database dump

Is Cryptography the Answer to all Cybersecurity Threats?

Data and Information Being Threatened at Different Levels

Typical Data at Rest Ecosystem

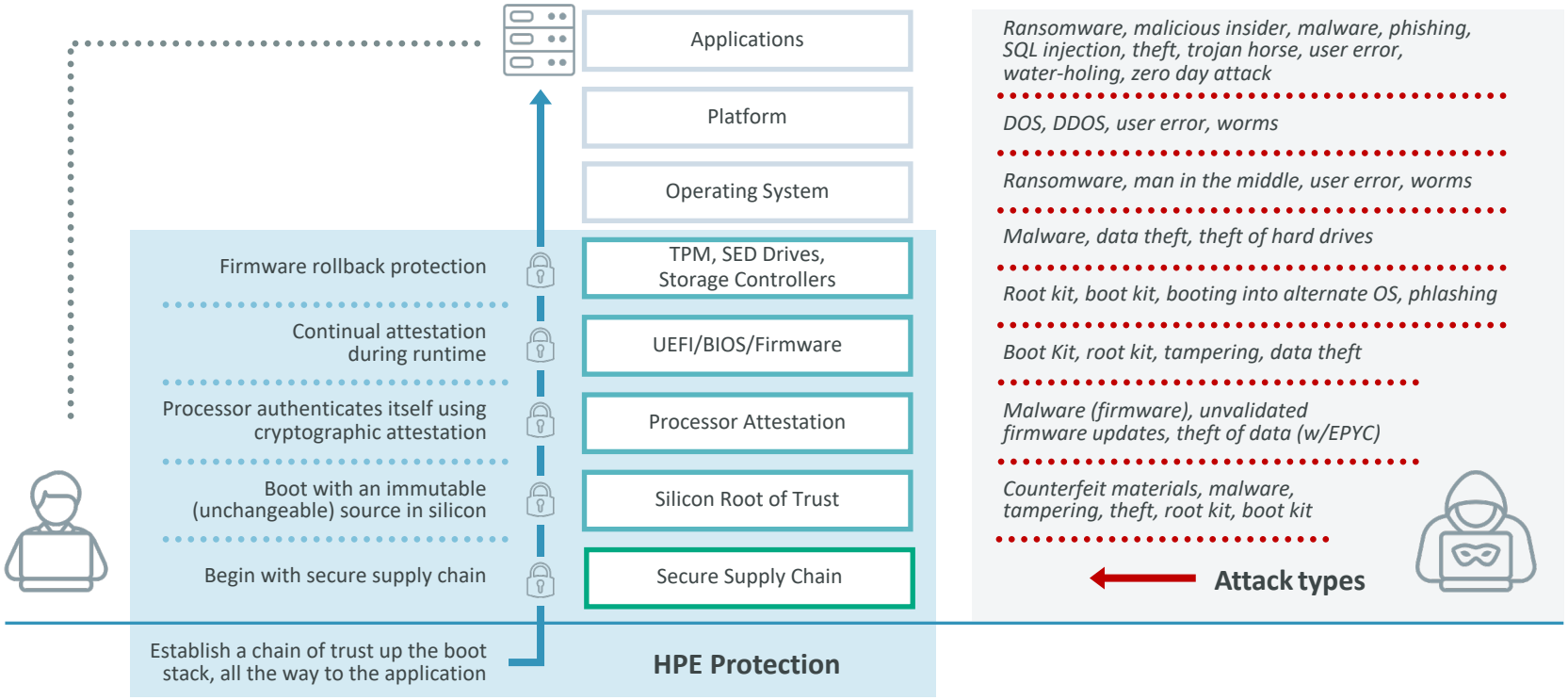
- Files & Folders
- Databases
- Operating Systems
- Virtual Storage
- Physical Storage

Files and Folders…

- What if the **admin misuse** the files?
- Are the **email files secured** properly?
- Are they secured **against ransomware?**
- Are the files and folders **backed up?**

Why Hardware-Based Security is Critical for Enterprise

Security is Only as Strong as the Layer Below the Point of Attack



SECURE TECHNOLOGY ALLIANCE

Hewlett Packard Enterprise

utimaco®

Is Cryptography the Answer to all Cybersecurity Threats?

Now encryption is an easy solution to protect confidential data

- Well-proven **defense against breaches** – highly effective, often mandated as a **must-have investment**
- **Simple** to implement: AES keys, standardized, now embedded, **but…**

Why is Enterprise Key Management a Challenge?

Key management is hard if not done right!

- **Maintain centralized controls:**
  Lose access to keys = lose access to the data
- **Social engineering policy:**
  Who manages the keys?
  What authorization is required for applications?
- **Audit and prove of compliance:**
  Regulatory mandates expect evidence of protection

Can you **coordinate and automate controls** that protect access to keys across enterprise encrypted data, **while maintaining transparent operations?**

Key Manager

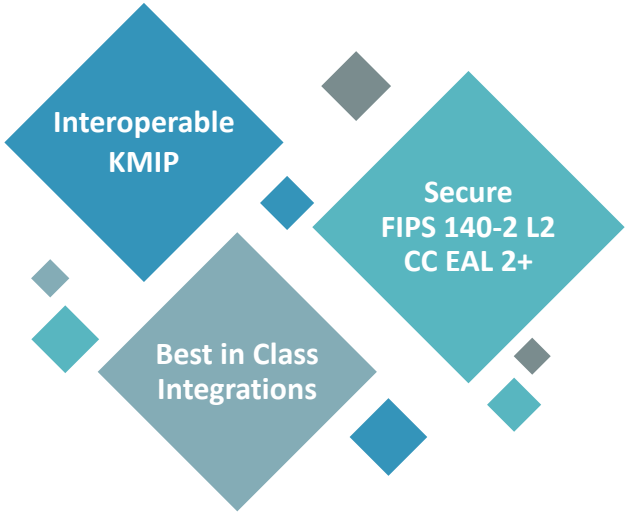
What to Look for…

Secure

- Meetig NIST standards, validated to FIPS 140-2 Level 2, Common Criteria
- Encrypted keys in transit and at rest
- Certificate-based authentication and built-in CA

Manageable

- Configuration and keys replicated across cluster automatically
- Hands-off administration, automated backups and audit logging
- Deploy as a Virtual Machine



Available

- Active-Active cluster
- Automatic key replication, client failover
- Highly redundant hardware

Interoperable

- Support for OASIS KMIP (Key Management Interoperability Protocol)
- No vendor lock-in
- Custom integrations using SDK

Scalable

- Geographically separated clusters across datacenters
- Support for thousands of clients, and millions of keys

Key Manager Integrations

Data-at-Rest Key Management

Business Applications, Data Stores and Processes

Servers
HPE ProLiant

Disk and Tape
3PAR, X7, StoreEver, StoreOnce

Web / Cloud
HPE Hybird / OpenStack

Big Data
Vertica, Zettaset

HPE Nonstop
Applications and Databases

3rd Party
Applications

Mainframe
Applications and Databases

Enterprise
Applications

3rd Party
SaaS Gateways

Production
Databases

HPE Portfolio

KMIP Compliant Partner Ecosystem

SECURE TECHNOLOGY ALLIANCE

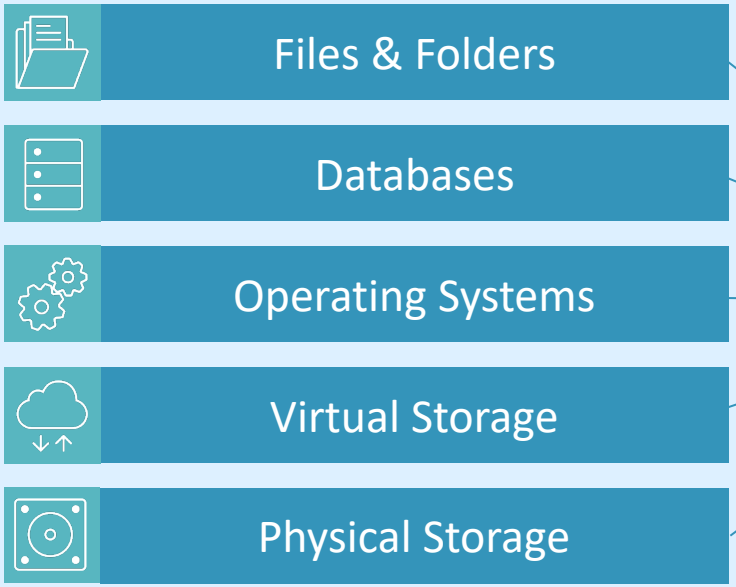
Hewlett Packard Enterprise

utimaco®

Securing the Keys at Different Levels

Securing the Access to Data and Information at Different Levels

Data at Rest in HPE & External Ecosystem



Securing the Keys at Different Levels

Securing the Access to Data and Information at Different Levels

Data at Rest Ecosystem

- Files & Folders
- Databases
- Operating Systems
- Virtual Storage
- Physical Storage

Centralized Secure Key Manager

Securing Keys for Data at Rest

Backup Solution

Tape Storage Solution

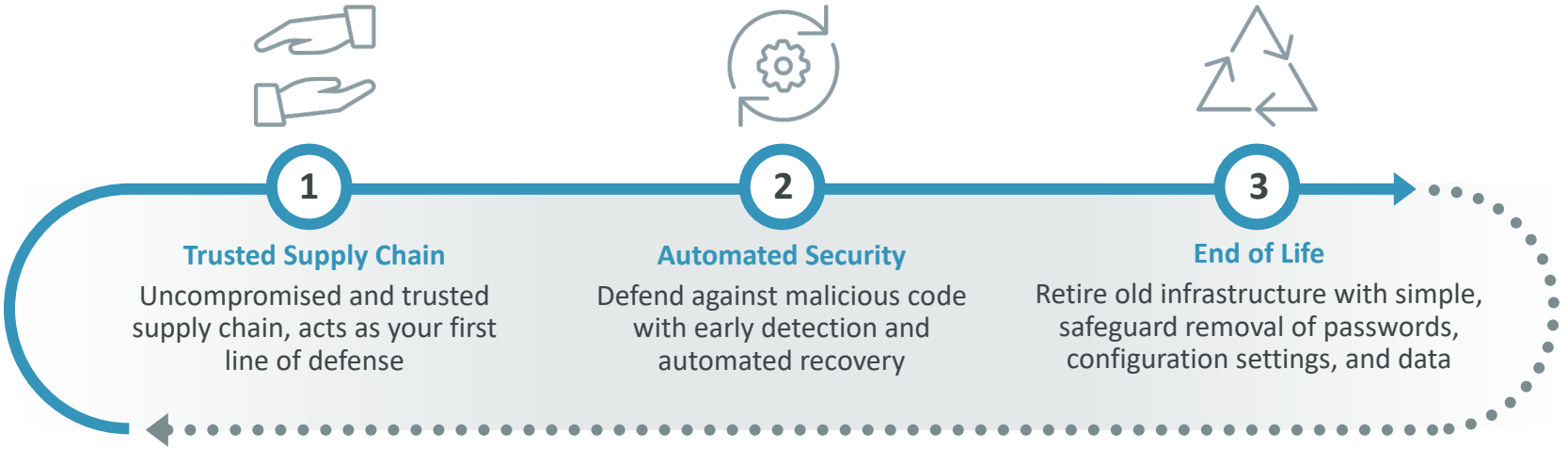
Data Protection Systems

SECURE TECHNOLOGY ALLIANCE

Hewlett Packard Enterprise

utimaco®

Security Protection and Security by Design



DNA of an Ideal Key Management System

Centralized Key Management

Streamline key management **processes**, reduce **costs** and the risk of **human errors.**

Key Availability

Multiple paths to request keys as a failover mechanism should a failure occur – **Resiliency** is vital.

Scalability

Expect the number of keys in use and in archive to grow to millions. **Scalability** is key!

Disaster Recovery

Be able to **recover the key management system** in the event of a complete failure is critical.

Ease of Use

The ability to **group keys, assign roles and policies to these groups** is the only way to manage the high volume of keys.

Raising the Bar

HSM as the preferred method of performing localized key management tasks, protecting the keys and the core operating functions

Deleting a key renders data useless or as good as deleted

White paper: Strengthening Information Security with Strong Key Management
https://bit.ly/3nLkdfs

Brochure: Enhanced Protection for Data at Rest
https://bit.ly/3CQ7fS1

Contact us
hsm@utimaco.com
computeSecurity@hpe.com

SECURE TECHNOLOGY ALLIANCE

Hewlett Packard Enterprise

utimaco®

Q & A

Free 60 Days Trial

For more information, visit:

https://bit.ly/3nLkdfs

https://bit.ly/3Bi5GvC

Thank you

for your attention!

UTIMACO IS GmbH

Germanusstraße 4
52080 Aachen
Germany

Phone +49 241 1696-0
Web hsm.utimaco.com
E-Mail hsm@utimaco.com

UTIMACO Inc.

900 East Hamilton Avenue
Campbell, CA-95008
United States of America

Phone +1 (844) UTI-MACO
Web https://hsm.utimaco.com
E-Mail hsm@utimaco.com