Data Protection

Securing What Makes You Unique

Joseph Pindar, CISSP
Principal Solution Specialist - Storage
Trends in Data and Storage Security

Regulations
- PCI, EU Data Protection Laws
- Privacy Regulations impose financial penalties
- Proactive security measures have compelling ROI

IP Protection
- Protect Intellectual Property and digital assets
- Strengthen access controls
- Auditing and logging of user IP access
- Protect against political risk

Business Trends
- Controlling data access with outsourced IT
- Cost savings by moving data to “The Cloud”
- “Big Data” changes the way data is being stored
Where to Encrypt Data?

- **Host**
  - ProtectApp
  - ProtectDB
  - ProtectV

- **Network**

- **Storage**
  - StorageSecure

- **Media**
  - Self-Encrypting Drives & Tapes
Transparent “Bump in the Wire” Encryption
Transparent “Bump in the Wire” Encryption

Executive
HR
Finance
Sales

StorageSecure

\storage\finance
\storage\sales

Storage

Windows AD / LDAP

Isolated Data
Not So Fast… What About Your Keys?

- Encryption is the only time proven, trusted, compliant way to control access to and protect high value data.

- BUT as they say…. Encryption is easy, managing it and making it work in scale is hard.

Gartner® says:

“As the use of encryption grows and various solutions are deployed, key management becomes exponentially critical and complex. Mismanagement of keys can expose an organization to unnecessary risk.”
KeySecure: Single Point of Key Management
KeySecure: How it works.

KeySecure handles every aspect of key management.

An Admin Console allows central definition, management and monitoring of key ownership and user access controls.

- Enable purge and delete key upon pre-set expiration policies
- Assign permissions and key ownership to privileged users based on roles
- Automate key rotation and other critical functions
- Enable authenticated clients to set and modify key attributes
- Provide a secure method to distribute keys
- Allow key attributes to be modified (create/delete/rotate) by authenticated key owners
- Maintain high availability and usage
Use Case: Privileged User Risk Mitigation
Where Can Sensitive Data Be Accessed?

Problem: How do we ensure sensitive data is only accessed at approved locations?
“IP Restriction” limits access to the Geneva office on a per folder basis.
No Single Administrator Can Grant Themselves Access to Sensitive Data

1. AD / LDAP admins control who has access
2. Admins must work TOGETHER to allow access
3. StorageSecure also controls local ACLs
4. StorageSecure works with AD / LDAP
5. Head Office

Windows AD / LDAP

Geneva
The Data Owner Decides Who Can Access Their Sensitive Data
Use Case: Compliant Data Protection

StorageSecure

SalesForce.com

HR

Intellectual Property

CMS

Clients

On Premise

Off Premise

(cluster/ failover)
Use Case: Archival Protection
Why Are People Using The Cloud?

Costs 74% less than onsite

(Forrester, 2011)

$150 per TB/year

(AWS Glacier, 2013)
Use Case: Writing Secure Data to Amazon S3

Sensitive or PII Data

StorageSecure & AWS iSCSI Gateway

Amazon Web Services

SafeNet
Use Case: Encrypted Objects as an Archive
SafeNet KeySecure
Enterprise Key Management

- **Enterprise Key Lifecycle Management**
  - Centrally managed, consolidation of keys
    - store, manage, generate, distribute, rotate, backup, activate, deactivate, and destroy
  - Up to 1 million keys per cluster
  - High Assurance Level

- **Standard based approach: OASIS KMIP**

- **Brodest Coverage in Industry**
  - NAS – StorageSecure
  - SAN - Brocade Encryption Solutions (BES and FS8/18)
  - KMIP support (NSE/FDE, Quantum Tape Library and other 3rd Party support)
  - Cloud-enabled (KMIP-based)

- **SafeNet LUNA SA (HSM) and PCI Card Management**

- Hardware- based, secure key replication across multiple appliances
- Active-Active mode of clustering
- Geo distribution support
- Highly scalable for cloud implementations
- LDAP/Active Directory Integration and Syslog forwarding
- Heterogeneous solutions: SFNT and non-SFNT devices, applications, databases, storage devices, SAN switches, tape libraries, HSM, network and endpoint devices, etc.
SafeNet StorageSecure
Next Generation Storage Encryption

- **Transparent deployment**
  - No agent or application/database changes
  - Native support for NAS:
    - NFS (UNIX/Linux)
    - CIFS (Windows)
    - Files servers (Windows, UNIX, AIX, Solaris)
  - Native support for IP-SAN:
    - iSCSI

- **Hardware-based security**
  - High reliability and availability: Clustering
  - Centralized key management: Integrated with KeySecure

- **S220 – 1Gbit Interfaces, S280 – 10Gbit Interfaces**

- **FIPS 140-2 Level 3 (validation in process)**
Děkuji