

Securing data at rest white paper

An enterprise strategy for data encryption and key management



Introduction: The data security imperative	2
Enterprise data-at-rest security landscape today	2
Challenges of enterprise stored data (data-at-rest) encryption	3
Current approaches to key management	4
The enterprise key management appliance	5
Implementation model-enterprise key management appliance	6
Time to elevate key management to enterprise level	7
For more information	8

Introduction: The data security imperative

The data residing on your storage systems and media, data-at-rest, presents serious security concerns. Regulations and various mandates around the globe are putting the burden on companies and government entities to protect the private information they store.

Increasingly, companies are being required to publicly disclose breaches that put individual's private data at risk, be it a customer, employee, shareholder, partner, or other stakeholder. And it is not just in the United States where laws like California's SB1386, which requires public disclosure when unencrypted private data is potentially exposed, are being rolled out state by state. In Europe, the EU Data Protection Directive and Japan's PIP Act protect the rights of individuals when handling personal information for commerce and the rendering of service. Expect regulations like these to get more stringent and spread more widely as breaches proliferate. For companies that operate in multiple countries, protecting the privacy of personal data presents a growing challenge.

The solution to the data privacy and corporate data protection challenge has been identified—encryption. To meet the various privacy mandates and compliance requirements, enterprises have to encrypt their data-at-rest. This means backup tapes containing an organization's important data need to be encrypted with a key. Very soon, organizations will have dozens, hundreds, thousands, and potentially millions of encryption keys that must be managed, secured, and protected. These encryption keys must always be available so the data can be recovered, even in the event of a system disruption or major disaster.

The technology to perform data encryption is widely available. What organizations need is enterprise key management to protect keys while ensuring key availability under all circumstances.

This white paper reviews today's enterprise data-at-rest privacy/security landscape and examines challenges of enterprise encryption and key management. It also assesses the current approaches to key management, introduces the concept of appliance-based enterprise key management, and identifies evaluation criteria for such an appliance. Finally, it describes the HP approach to enterprise key management and provides an enterprise implementation model to simplify key management deployment.

Enterprise data-at-rest security landscape today

Judging whether there are more security breaches now than in the past is hard. However, what is clear is that security breaches are getting more attention, if for nothing else than laws mandating public disclosure when a security breach potentially exposes unencrypted private data. Whatever the cause may be, the costs associated with security breaches are high. The state of Ohio reports spending over \$2 million on a security breach resulting from a single lost tape. The headline grabbing breach at TJX Stores, which compromised the privacy of almost 46 million records, has cost this retailer approximately \$150 million to date and the price tag is still climbing. The retail, financial, healthcare, and government sectors handle more private, personal data and thus feel even greater pressure to protect private data. In addition, enterprises need to keep their financial records and other proprietary information confidential until they are ready to be released or destroyed.

Although data encryption is the agreed upon solution for ensuring the privacy of personal data in the company's care, there is no agreement on the best place to implement encryption. Encryption can be deployed across the enterprise data center infrastructure stack. Some companies implement it high in the stack, at the application level, where they can achieve broader coverage and control. Others encrypt data low in the stack, at the storage device itself or tape library, for the speed and ease of deployment. The invention of the HP StorageWorks LTO-4 Ultrium 1840 Tape Drive with built-in encryption makes implementing encryption especially convenient. In truth, companies deploy encryption at multiple points in the stack to achieve the right balance of coverage, control, speed, and ease for their situation.

Similarly, there are numerous encryption products from a wide range of vendors that may provide acceptable encryption and simple key management. Companies are likely to implement multiple products. Many of these, however, are immature and expensive and may entail migration risks, especially when an organization wants to extend its key management efforts enterprise-wide.

Even at this early stage in large-scale encryption deployment, the following two points are essential.

1. With encryption being applied in multiple places and with the use of multiple products, organizations need an enterprise encryption key management strategy that spans multiple system domains—storage, applications, networks—to ensure end-to-end privacy, from the desktop to the data center.
2. With disparate encryption technology being deployed, enterprise-wide key management is critical for allowing organizations to centrally manage, protect, and make available all their encryption keys if they are to avoid the cost of individually managing and protecting thousands of different keys being generated and used in multiple places.

Only a centralized approach based on automated enterprise management, protection, and high-availability practices enables organizations to deal with the rapid proliferation of encryption keys. Otherwise, organizations face nightmare scenarios of lost keys and the resulting loss of data and other confidential intellectual property along with the spiraling cost of ensuring data privacy.

Challenges of enterprise stored data (data-at-rest) encryption

Encryption is a known entity and is not difficult to implement. The leading encryption algorithms and standards have proven to be reliable, stable, and remarkably effective over the long term. Encryption products are readily available, and AES-256 encryption provides ironclad protection that ensures data privacy. However, without the correct key, it becomes virtually impossible to render AES-256 encrypted data usable. Encrypted data without the key is nothing more than unintelligible garbage.

According to best practices, every time an organization stores or backs up data it should encrypt the data with a different key. Very quickly, enterprises have many keys to manage and protect. The challenge then is not encrypting the data, but managing and safeguarding what quickly becomes large volumes of keys, which are subject to theft, loss, or destruction. When it comes to key management, therefore, companies face a number of challenges:

- Too many keys in too many places
- Keys at risk of loss or theft
- Difficult key recovery
- Complex key management

When companies are encrypting a small amount of data using a few encryption devices, it is possible to manually manage and protect the few keys. However, key management becomes unwieldy as soon as multiple disparate encryption solutions are deployed or the number of encrypting devices proliferates across the enterprise. Complicating matters is the fact that the loss of a key is tantamount to losing the data. Keys, therefore, need to remain accessible for the useful life of the data. For data-at-rest, the useful life could be decades.

An encryption key is just another piece of important corporate data. The IT industry already knows how to safeguard important data for long periods of time. The healthcare industry, the financial services industry, and manufacturers of durable goods routinely store data for decades. Now, the lessons IT learned in terms of data scalability, reliability, availability, accessibility, and manageability must be applied as part of an enterprise-wide key management infrastructure solution. In short, companies need an effective way to centrally protect and manage keys independent of where and when encryption occurs.

Current approaches to key management

Although it is clear that centralized, automated enterprise key management is needed, the current approaches to key management are far from enterprise-class. Rather, they are tactical. Today, organizations generally perform key management in one of two ways or a combination of both. Consider tape encryption as an example:

1. Application-based—The application, often the tape backup application, manages the key.
2. Library-hosted—The tape library or backup server generates and manages the key locally.

Each of these approaches provides basic key management. Tactical in nature, they are architecturally unable to scale to enterprise levels, unable to accommodate other encryption client types beyond tape, and lack capabilities that enable them to comply with various higher level security certifications, such as the FIPS 140-2 Level 2 and higher validations. Their key management also entails considerable manual intervention.

With today's heightened interest in encryption, organizations need to reassess the tactical approach to key management. Specifically, companies need to evaluate their key management strategies against the following criteria:

- How secure is it—This goes beyond simple access control by addressing both the physical and logical hardening of the system, such as disabling unnecessary processes in the OS or reinforcing the locks on the physical key repository itself.
- How well does it scale—Certainly, scalability needs to effectively handle thousands, tens of thousands, or ultimately millions of keys, but it also needs to span multiple locations, devices, and applications.
- How automated is it—Key management quickly grows beyond what an administrator or team of administrators can handle manually and requires policy-based automation.
- How failure proof—Any system can go down, including key management systems so a key management strategy needs a clustering architecture, redundancy, and replication failover to ensure that even if one node is unavailable for any reason, keys can be accessed through an alternate site to ensure uninterrupted access to the data. Advanced clustering architectures would have both device and path failover and possibly even load balancing capability.
- How far does it go in supporting government security specifications—FIPS 140-2 is currently the most stringent cryptographic accreditation, but even lesser specifications require capabilities such as audit trails, separation of roles and responsibilities, and other best practices.

The current approaches to key management do not sufficiently address these criteria. Although they provide basic key management, they simply fall short for enterprise-scale privacy and data protection. For more information, see Table 1. Key management assessment.

The enterprise key management appliance

So, what does enterprise-scale key management need to look like? HP believes it looks like a key management solution that scales because the volume of encrypted data and types of encrypting clients quickly expands. It replicates and clusters for reliability and high availability to reduce the danger of lost or inaccessible keys. It also protects keys through system hardening and secures policy-based automation and control. Finally, it offers simplified, centralized management since protecting data already is complex and resource intensive.

Based on the preceding identified criteria, HP envisions an enterprise-class key management appliance delivering the following capabilities:

- Policy-based automation to minimize the amount of labor involved as key volume surges
- Solid security, including a hardened device, to protect access to keys and device administration
- Cluster redundancy to ensure reliable and highly available access to keys
- Backup copies of keys to further protect keys and ensure availability even in the face of system disruptions and disasters
- Seamless integration with applications, databases, and encryption devices
- Open and standards-based to ensure key management interoperability in heterogeneous environments (while there are no key management interoperability standards yet, HP is working on the standards with other vendors)

Although many vendors offer key management solutions and more will as the magnitude of the need becomes apparent, very few of these vendors have the enterprise-class infrastructure experience, technology, and strategy to deliver true enterprise-class key management. In the end, enterprise-class key management has to come from industry leaders like HP that have the breadth of technology, products, services, experience, and strategy along with a proven track record in enterprise-class computing.

Table 1. Key management assessment

Key Management Approach	Advantages	Disadvantages
Enterprise appliance	Centralized management Hardened Automated, policy-driven Clustered, replicated, failover Open Support for FIPS 140-2	Higher initial cost More complex deployment
Application/ISV based	Lower acquisition cost Simple to deploy	Does not scale well Not standards-compliant Costly to administer Limited replication failover Very proprietary
Native/Encryption Device based (Local)	Lower acquisition cost Simple to deploy Fast encryption	Does not scale well Not standards-compliant Costly to administer Limited replication failover Very proprietary

HP has introduced an appliance-based enterprise key management offering, HP Secure Key Manager, featuring both a hardened cabinet (dual bezel pick resistant locks and tamper-evident enclosure) and hardened software (closed Linux kernel) for maximum security and key protection. Since it is an appliance, it is easy to deploy and efficient to centrally administer on an enterprise scale. The architecture is designed to allow support over time beyond tape to accommodate encryption keys for other storage and infrastructure devices and applications.

Organizations will be able to centrally manage keys throughout the data lifecycle, and the appliance will offer transparent key archival and timely key retrieval. Automatic policy-based key generation reduces both the administrative burden and the likelihood of error while secure identity-based control will safeguard access to the appliance itself. Multi-site high availability is achieved through appliance clustering and automatic key replication, which ensures the safety and availability of keys in the event of system interruptions or disasters.

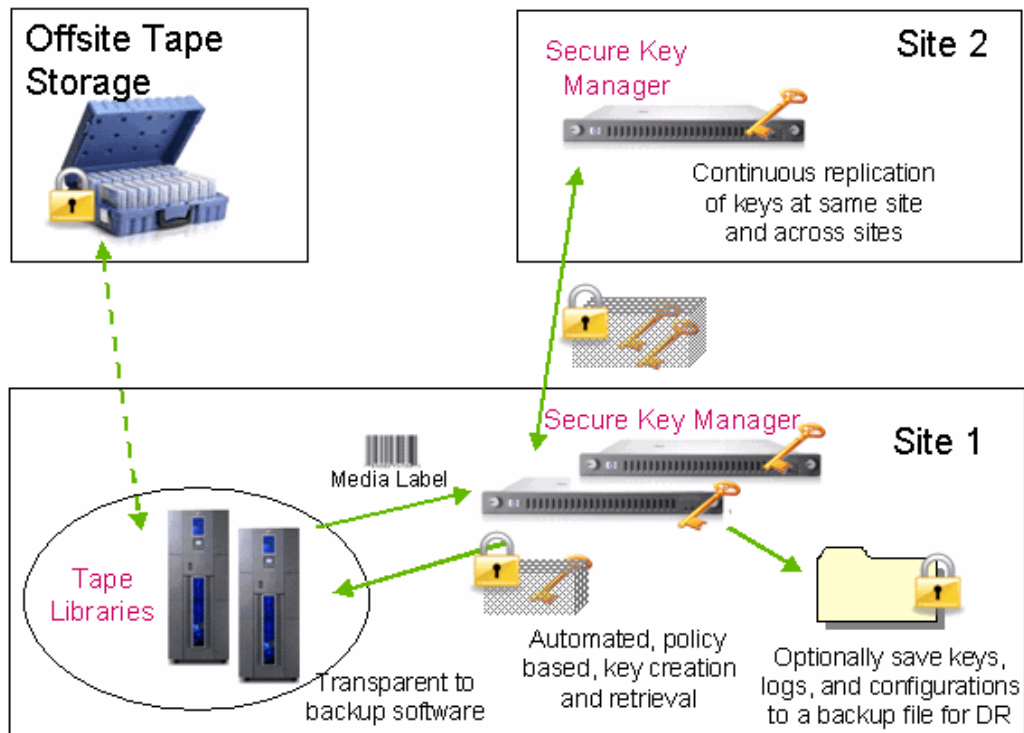
For organizations that strive for compliance with various mandated security validations, such as FIPS 140-2, the key management appliance offers tamper-evident hardware and digital signing of logs for auditors. In addition, its identity-based access control enforces security best practices, such as the separation of roles between storage administrators and security officers.

Implementation model-enterprise key management appliance

The implementation and deployment of an enterprise-class appliance is simpler than expected. The following describes the implementation of enterprise key management using the Secure Key Manager configured as three nodes spread across two sites: a primary site (2 nodes) and a remote site (1 node) to protect keys for encrypted tapes.

- Site 1 consists of a pair of Secure Key Manager nodes clustered together. A security officer enrolls the tape libraries as clients to the key management cluster and creates the key management policies. Keys are automatically replicated between the nodes on site. Then the libraries automatically retrieve keys from the Secure Key Manager using identifiers based on the media ID.
- Site 2 consists of one Secure Key Manager node. Keys are automatically replicated from Site 1 to the node on Site 2 and continuously updated.
- Each node in the cluster can have library connectivity.

Figure 1. Implementation model



The encrypted data on tape cartridges is stored off site, and the keys for future decryption are archived on each of the nodes and in backup files. In the event the primary site is disrupted, key management automatically shifts (failover) to the secondary site. For audit and compliance purposes, a record of key management operations and key usage is logged and digitally signed. The payoff from Secure Key Manager comes from the centrally automated, secure, and high availability of keys for its encryption clients.

Time to elevate key management to enterprise level

From a data-at-rest perspective, encryption key management is a relatively new development. Early products may initially meet needs in very simple environments with homogeneous security policies, but device-hosted, native or application-based key management cannot deliver a strategic enterprise caliber solution to the problem. However, the importance of privacy and the cost to those companies that fail to protect the privacy of personal data they store have become so great that encryption and key management must be raised to the strategic level. Enterprise-wide encryption of data-at-rest is now a strategic imperative.

While key management on an enterprise scale can be challenging, a centralized, automated appliance can speed deployment and reduce the management overhead as it delivers reliable, scalable, highly available key management on true enterprise scale. The risks of lost keys, compromised keys, and slow or incomplete key recovery and the corresponding loss of data that implies are just too great for anything but an enterprise key management strategy based on a centralized, hardened appliance.

For more information

- Information about HP StorageWorks products and solutions is available at www.hp.com/go/StorageWorks.
- Information about HP storage security solutions is available at www.hp.com/go/encryption.

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA1-6170ENW, October 2007

