Sophisticated threats and the risk of data exposure are increasing, making encryption an essential last line of defense when other security mechanisms fail. Encryption is also a core requirement in meeting many regulatory mandates, and is of vital importance as organizations look to address the security challenges they face when migrating sensitive data to virtualized and cloud environments. To be completely protected, enterprises must deploy a solution that secures the applications and data that drive their operations.

The Gemalto Solution for IBM

Gemalto and IBM have a solution to the security challenges faced by organizations that need to protect their sensitive data. Townsend Security Alliance AES400 encryption provides application encryption to IBM i for Power Systems platforms while Gemalto provides the key management for ongoing administration. By applying encryption at the application level, all assets – from structured data in a database file to unstructured data in a word processing file - will be secured immediately. This enables organizations to minimize risk by protecting high-value data across its entire lifecycle, no matter how many times it is transferred, backed up, or copied.

IBM i for Power Systems (including AS/400, iSeries, and System i)

IBM i is an integrated operating environment run on the IBM Power Systems server platform. Organizations can take advantage of the infrastructure’s flexibility and resilience to run business applications with minimal setup and investment. IBM i is versatile enough to support virtual workloads; over 3,000 solutions from third-party ISVs; and a wide variety of IBM solutions such as DB2 and WebSphere. Enterprises deploy IBM i on Power Systems platforms to lower their operational costs while running applications from a high-performance infrastructure.

Key Benefits

- **Immediate encryption:** The sooner a sensitive asset is encrypted, the less chance that asset has to be exposed.
- **Automated key rotation:** Fully automated key rotation reduces the complexity and cost associated with manual key rotation and potential re-keying of data.
- **Secure data throughout its lifecycle:** Once application data is encrypted, it does not matter whether it is backed up on-premises, replicated, or stolen; only authorized users holding the appropriate encryption keys will be able to view and use the data. Even data encrypted and stored in virtual machines will remain secured in the event the image is copied or stolen.
- **Key management simplified:** Centralized key management by SafeNet KeySecure reduces the strain of administrative resources. Administrators can manage keys for the entire security infrastructure from one location, which reduces the complexity of the security structure and the amount of time needed for proper management and oversight.

Townsend Security Alliance AES400 and SafeNet KeySecure

Townsend Security Alliance AES400 is an application encryption solution that secures data as soon as it is generated, helping organizations meet their security and compliance obligations. SafeNet ProtectApp works with SafeNet KeySecure to centralize encryption and key management.

SafeNet KeySecure and Townsend Security Alliance AES400 can encrypt applications running on IBM i, through a comprehensive set of encryption and decryption APIs. The encryption and decryption of application data is transparent to end users irrespective of the back-end database or file system they are using, or the number of times and locations encrypted data is backed up, stored, or copied. From unstructured data, such as Excel files and PDFs, to structured data, such as credit card number database fields, Townsend Security Alliance AES400 provides protection to a wide range of sensitive information.
Securing cryptographic processing in a hardware appliance

- When Townsend Security Alliance AES400 is deployed with SafeNet KeySecure, all cryptographic processing is securely conducted on the KeySecure appliance. Alternatively, keys can be pulled to the IBM environment for local crypto processing in a safe fashion.
- The appliance is built specifically for optimizing the performance and security of processing-intensive cryptographic operations. By conducting all operations on the appliance, and never letting encryption keys leave the hardware, Gemalto’s SafeNet line of products preserves the integrity of the organization’s cryptographic infrastructure. Administrators can account for their keys at all times, and trust that unauthorized users won’t ever have access to encryption processes.
- In addition, ProtectApp offers load balancing, connection pooling, SSL connections, and key caching to optimize scalability and throughput to reduce impact on overall performance.

Conclusion: Best-in Class Security Intelligence and Key Management

Gemalto and IBM make securing data easy, from the moment it is generated, despite the ever-increasing sophistication of attacks and the growing complexities of IT environments. This solution ensures that data is always secure and the application environment is thoroughly monitored so potential threats are addressed before they become a problem. Organizations now have a tool to sift through the massive amounts of security data in their networks for actionable insights, while also protecting valuable resources through encryption and centralized key management. To learn more, visit www.safenet-inc.com/partners/ibm/

About Gemalto’s SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

©Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. SB (EN) Jun 28, 2016 - Design: ELI

Key Management at the Application Level
Townsend Security Alliance AES400 and SafeNet KeySecure

Key features

Centralized key management
SafeNet KeySecure centralizes the management and storage of cryptographic keys (for example, symmetric and asymmetric encryption keys, passwords, and certificates) in a secure, FIPS 140-2 Level 3-validated, tamper-proof appliance. Management tools and capabilities such as key versioning streamline time-consuming tasks, including key rotation. KeySecure enables enterprise key management for Townsend Security Alliance AES400, the entire portfolio of SafeNet encryption products, as well as a growing list of products supporting the OASIS Key Management Interoperability Protocol (KMIP) standard. By providing centralized administration of keys, policies, logging, auditing, and reporting functions, KeySecure simplifies management, helps ensure regulatory compliance, and maximizes security.

Policy management and separation of duties
Administrators can set authentication and authorization policies that dictate which applications can be accessed in the clear by a particular user or set of users. These controls provide administrators with tighter governance of sensitive data. Policy-driven security using granular access controls provides a vital layer of protection to help organizations comply with the separation of duties between IT and security administrators that is required in many security mandates.

Logging, auditing, and reporting
SafeNet KeySecure records all key state changes in centralized logs, simplifying auditing and reporting access to data and encryption keys. By tracking this information from one platform, organizations increase security around their data and can readily demonstrate their compliance with industry mandates and government regulations.

Securing Data on IBM i: Gemalto Encryption Solutions for IBM i for Power Systems - Solution Brief