Database Encryption: Securing Data-at-Rest

Databases and other forms of data-at-rest storage often contain sensitive information for both customers and employees and are a prime target for attackers. Using hardened data encryption and robust key management, organizations can pursue a number of different strategies to protect this sensitive data. With technology that can be applied across all aspects of this important and multifaceted subject, Futurex's Hardened Enterprise Security Platform provides a versatile, secure, and scalable solution for securing data-at-rest.

With the uptick in major data breaches over the past decade, organizations are racing to secure their databases and other repositories of data-at-rest. Enterprise databases hold invaluable information: proprietary organizational data, employee records, customer details, and other personal protected information. It is no wonder that this information is a high-value target for attackers.

Organizations have placed a premium on securing databases and other systems developed to manage information by storing it in an organized fashion for retrieval at a later time. Several different methods have been developed for securing databases, varying in difficulty of deployment and the level of security they provide.

One of the primary original uses of encryption was to secure data-in-motion, defined as data that is being transferred as messages. These encrypted messages require the use of cryptographic keys in order to be able to decrypt and interpret the information.

Protecting data-at-rest represents a different set of challenges. Data-at-rest includes data which is stored and is not being processed on devices such as network servers, computers, and mobile devices. System and database administrators must walk a fine line between availability and security. Information secured within databases must be available to only certain devices or individuals, preventing access by those who do not have authorization. Depending on the organization and database in question, this can be a complicated undertaking. This authorization hinges on the distribution and management of keys in a cryptographic system.

Key Management for Databases and Applications

Perhaps the most salient objective for system and database administrators to achieve in securing databases is implementing a strong key management solution. Brute force attacks on encryption are, from a practical standpoint, a virtually impossible task, which is why it is not the preferred method of attackers. Encryption keys are often targeted, making the success or failure of a data security infrastructure lie within the policy, procedures, and technology used to manage keys.

At the center of any robust key management infrastructure is the physical cryptographic hardware used to encrypt, decrypt, and store the keys.

It is imperative that keys must be stored in hardware security modules validated to FIPS 140-2 Level 3 or greater and away from the databases they encrypt. If an attacker has access to both the database and the keys encrypting its data, this represents a significant risk to security.

A system's keys can range in volume from hundreds of thousands to tens of millions and beyond. Because of the relative complexity of enterprise-level databases, key management solutions must, in many cases, be robust enough to handle millions of keys. These keys may be used by multiple applications, stored in geographically separated locations. Additionally, when keys expire and must be exchanged, the key management solution must be able to handle the revocation and reissuance of keys to a wide range of devices, servers, users, and applications.

Another key management consideration is the availability of encryption keys. Key management servers must make keys readily available to ensure optimal performance of database systems. In addition to key generation throughput considerations, it is up to system administrators to ensure keys are readily available to authorized applications and devices to ensure optimal system performance and fulfillment of business objectives.

Methods for Securing Databases

Organizations have several approaches at their disposal to secure databases. The choice of methods depends on the environment, the level of security needed, the type of data being protected, and the overall complexity of the system. In some cases, multiple methods can be used simultaneously to secure databases.

Application Layer Encryption

Application layer encryption offers a method of superior control because it captures encryption at the source — in the application. By encrypting it in the highest layer in the system, it limits the instances within the database infrastructure where the data is found as plaintext, thereby limiting the danger of a breach. It is the most granular and secure of the encryption options, but implementing it can be a challenge.

Encrypting Storage Media

Many breaches occur while transferring backup files or other servers from site to site when they are either lost in transit, stolen, or are simply disposed of improperly. To mitigate the risk of breaches under these circumstances, the actual storage media can be encrypted. This method is often used in conjunction with other encryption strategies, like application layer encryption or object-based encryption to secure databases.

Encrypting Objects Stored in Databases

There are several sub-methods that fall under the category of encrypting objects in the actual database:

Transparent Data Encryption: A popular method for encrypting database objects is transparent data encryption, also known as TDE, which automatically encrypts and decrypts the data stored in the database. Organizations may choose to encrypt data at the column, table, or tablespace level of the database, offering increased versatility.

Tokenization: Tokenization is a method of replacing sensitive data with a string of identifying characters known as "tokens" for storage. Two main approaches to tokenizing data are common: a hash-based message authentication code (HMAC) method and an encryption-based method. The encryption method is preferred in cases where the tokenization needs to be reversed for any reason. Tokenization effectively removes the burden of multiple parties storing sensitive data in the clear while still allowing easy access to authorized applications and users.

Futurex Solutions for Securing Databases: The Hardened Enterprise Security Platform

The Futurex Hardened Enterprise Security Platform is a collection of advanced data security solutions that operate together to produce a result far beyond the sum of its parts. These solutions are custom-tailored by Futurex Solutions Architects to our clients' specific ecosystems and can be integrated directly with existing applications and business systems.

The Hardened Enterprise Security Platform represents the pinnacle of data security and is trusted by industry leading organizations worldwide. It has been designed and developed to provide core cryptographic functions for an organization's data security infrastructure, including databases and other instances of data-at-rest. Particular attention has been given to developing solutions that are extensible, scalable and secure.

Best-in-Class Hardware Security Modules

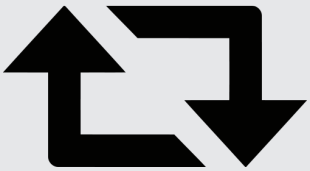
Futurex offers FIPS 140-2 Level 3-certified hardware security modules which can be used to handle encryption and decryption tasks for data-at-rest, including PKCS #11-based integration with enterprise database systems. These hardware security modules offer the fastest transaction processing speeds in the industry with the lowest cost per transaction. Futurex makes a commitment to creating extensible products and to support emerging security trends and technologies. These hardware security modules are equipped with robust logical and physical security features to safeguard sensitive data, as well as an easy-to-use GUI to reduce costs associated with training employees.

Enterprise Key Management Solutions

Key management is a growing responsibility for enterprises managing large volumes of keys and certificates. Futurex's KMES Enterprise Series key management servers are FIPS 140-2 Level 3-validated solutions for managing all aspects of the encryption key lifecycle including creation, management, distribution, and destruction for both symmetric and asymmetric keys in one central, secure location.

Key Management 101

Key management can mean the success or failure of an organization's data security infrastructure. Often enough, organizations don't place enough weight to the policies and procedures that will shape the outcome of their data security infrastructure. Here are important key management ideas to keep in mind.



Don't treat compliance as a checkbox

Observe best practices

Consider your organization as a whole when planning for key management

(Enterprise Key Management Solutions Continued)

Robust, permission-based user controls ensure only authorized users have access to certain keys, supporting industry best practices and allowing an enterprise to manage and store keys securely in one cryptographic system. Other logical support mechanisms enforce best practices of dual control and separation of duties. The KMES Enterprise Series API allows for programmatic automation of repetitive tasks and will incorporate standards outlined in the Key Management Interoperability Protocol (KMIP), ensuring compatibility and easy implementation into existing systems.

Certificate Authority Solutions

Authentication of devices, application, files and other data lies at the heart of modern data security strategies. By creating mutually authenticated environments, organizations seek to secure their sensitive data and that of their customers. With Futurex's KMES Enterprise Series certificate authority solutions, organizations can issue certificates to sign and verify data with a variety of applications. This certificate authority technology has been integrated in large, Tier-1 enterprises all around the world, securing products and services used by millions of people on a daily basis.

System Scalability and Storage

Enterprises are often charged with managing large volumes of keys, certificates, and other objects in their mission to secure their organization's most sensitive data . The SAS9000 Secure Attached Server offers a high-volume, hardware-based data storage and access solution with full integration with other Futurex products. Sensitive information is encrypted and stored directly on the SAS9000's array of hot-swappable, RAID-enabled hard drives until the information needs to be accessed once again.

From large, heavily accessed databases to collections of individual files, the SAS9000 ensures the highest protection of sensitive data by functioning as a network-attached storage server, a fully redundant database server, and more.

Solution Spotlight: The KMES Enterprise Series

Enterprises have been tasked with securing a multitude of encryption keys. The KMES Enterprise Series has been developed to meet this challenge. The KMES Enterprise Series is a customizable, standards-compliant solution for full key and certificate lifecycle management.

- Tamper-responsive physical and logical security
- Object grouping and custom attributes provides a simple, user-friendly method of organizing keys and certificates
- Full integration with Hardened Enterprise Security Platform solutions, enabling centralized management, remote access, and large-scale scalability
- Fully functional graphical user interface, with no command line tasks required for initial setup, regular auditing, firmware upgrades, or maintenance

Secure SSL/TLS Gateway

As plaintext objects travel to and from their storage locations, they pose an easy target for attackers. All communication, whether site-to-site connections or external communications with endpoint devices like computers or point of sale terminals, must be secured. Even networks protected behind a firewall are potentially at risk. The Kryptos TLS Server encrypts these connections, ensuring point-to-point encryption of all transmitted data when it is not housed within the secure confines of an encrypted database.

High Availability Infrastructures

The danger of downtime is a serious concern for enterprises where 24x7x265 uptime is not only expected, but the industry standard. Because of this, core cryptographic infrastructure must support 99.999% uptime as well. As a cornerstone of the Hardened Enterprise Security Platform, the Guardian9000 provides centralized management, custom alerting, and N^{th} degree scalability for an enterprise's data security infrastructure.

The Guardian9000 allows organizations the ability to easily manage, configure, and monitor their encryption and key management hardware, as well as establish a high availability infrastructure with the same functionality for groups of Futurex client devices. This provides full system redundancy in the event of system failure or natural disaster. Multiple Guardian9000 devices can be located in geographically distributed data centers to establish a high availability environment, virtually eliminating the risk of downtime, both planned and unplanned.

Remote Configuration and Management

The Securus, the world's only purpose-built handheld remote configuration and key loading tablet containing a FIPS 140-2 Level 3-validated Secure Cryptographic Device, adds the ability for systems administrators to manage and configure their entire cryptographic infrastructure remotely. Users can perform tasks such as loading master keys and updating firmware from a remote location, eliminating time and money spent for key administrators to travel to various data centers around the globe.

Hardened Enterprise Security Platform

The Futurex Hardened Enterprise Security Platform is a collection of products that work together to provide one complete solution for cryptographic needs, combining to form a solid foundation for an organization's core IT infrastructure.

Guardian9000

Centralized management platform providing intelligent load balancing capabilities, remote management and configuration, high availability and custom alerting

Securus

A purpose-built, tablet-based remote configuration and key loading solution

KMES Enterprise Series

Manages all aspects of asymmetric and symmetric key lifecyle

Excrypt SSP9000 Enterprise Series

An advanced, enterprise-class hardware security module solution

SAS9000

Secure attached storage, supporting system scalability and high-volume encrypted data storage

RKMS Enterprise Series

Remote key distribution for electronic devices, including ATM and POS terminals

Kryptos TLS Server

A solution for securing data-in-motion via an SSL/TLS gateway

VirtuCrypt: Hardened Enterprise Security Cloud Solutions

Building upon this mission and the Hardened Enterprise Security Platform, Futurex has developed additional solutions for securing an organization's databases and data-at-rest. VirtuCrypt's secure, hosted services revolutionize cloud computing, providing an innovative approach by combining the convenience of cloud-based services with the robust physical and logical security of FIPS 140-2 Level 3-validated Secure Cryptographic Devices.

The VirtuCrypt cloud hosting solutions can benefit organizations of all sizes and industries, fulfilling a number of requirements. Using the Hardened Enterprise Security Platform at its core, VirtuCrypt offers cloud-based features such as offsite disaster recovery and redundancy; hosted core cryptographic infrastructure; secure data storage, processing, and validation; and more, all protected using technology hosued within TR-39 and PCI PIN-certified secure facilities.

Establishing a secure facility to house an organization's cryptographic devices is a time-consuming and expensive process. Organizations must ensure their secure facilities are compliant and undergo regular audits. A cloud-based hardened enterprise security service based in SSAE 16 (SOC 1, 2, and 3), PCI DSS, and HIPAA-compliant secure data centers, VirtuCrypt offers the benefits of Futurex's Hardened Enterprise Security Platform without the overhead or effort associated with building, maintaining, and certifying a data facility.

VirtuCrypt is yet another example of dedication to meeting and exceeding security standards in every solution offering, ensures that organizations will benefit from the highest possible level of protection while still enjoying the ease of use that Futurex solutions are known for.

VirtuCrypt: The Hardened Enterprise Security Cloud

VirtuCrypt represents the next generation of secure cloud computing, offering:

Disaster Recovery
VirtuCrypt allows for secure, easily accessible backups of all data

Security
Data is secured by physical and logical security features designed by Solutions Architects

Scalability
More processing capacity is as simple as the click of a button

Convenience
VirtuCrypt offers easy implementation of data security infrastructures without the expense or hassle of setting up a self-hosted system

About Futurex

For over 30 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions.

More than 15,000 customers worldwide have trusted Futurex's Enterprise Security Platform to provide innovative, first-to-market solutions for the secure encryption, storage, authentication, and transmission of sensitive data.

Futurex maintains an unyielding commitment to offering advanced, standards-compliant hardware security modules, key management servers, and general-purpose data encryption technology alongside world class customer service.

FUTUREX

Global Headquarters 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF 800.251.5112 P +1 830.980.9782 F +1 830.438.8782 info@futurex.com
WWW.FUTUREX.COM