gemalto
security to be free

Protect Your Sensitive Data

A Step-by-Step Guide to Finding the Right SafeNet Data Protection Solution for Your Organization

So, You Need to Encrypt Your Sensitive Data?

Your data is in high demand, and you know it needs data-centric protection. With so many encryption options available, how do you find the right solution to protect your organization's sensitive data?

An enterprise-ready encryption solution should provide the following:

- **Comprehensive encryption offering:** Avoid isolated islands of encryption across the enterprise. A comprehensive solution can encrypt sensitive data wherever it resides, including structured and unstructured data at rest and data in motion.
- **Centralized encryption and key management:** A centralized solution will enable you to protect and manage both the data and keys. Secure the data by encrypting or tokenizing it, while controlling access to the protected data. Protect keys by managing the full key lifecycle (generation, distribution, rotation, deletion, etc.) and establishing granular policies to control access to the data. To be a truly secure solution, it is imperative keys are stored separately from the data.
- **Cloud-ready security:** Take advantage of the efficiency and flexibility of the cloud while keeping your data secure. An enterprise-ready encryption solution should enable you to maintain control and ownership of your data and encryption keys not only on-premises, but also across virtual, public cloud, and hybrid environments.
- **Transparent performance:** With the high demand for data, an encryption solution must operate without disruption to business operations, application performance, or end-user experience.

With Gemalto's portfolio of SafeNet Data Protection solutions, you can deploy a unified and efficient data protection platform that can be leveraged to secure all data types residing in or moving between your physical, virtual, cloud and hybrid environments.

How to Find the Right SafeNet Data Protection Solution for Your Organization

We've made it quick and easy to pinpoint the solution(s) that best fit your data protection needs. To get started, consider where your sensitive data can be found across your on-premises, cloud, or virtual environments – both at rest and in motion.

Data at Rest

There is sensitive data located in any of the following places:

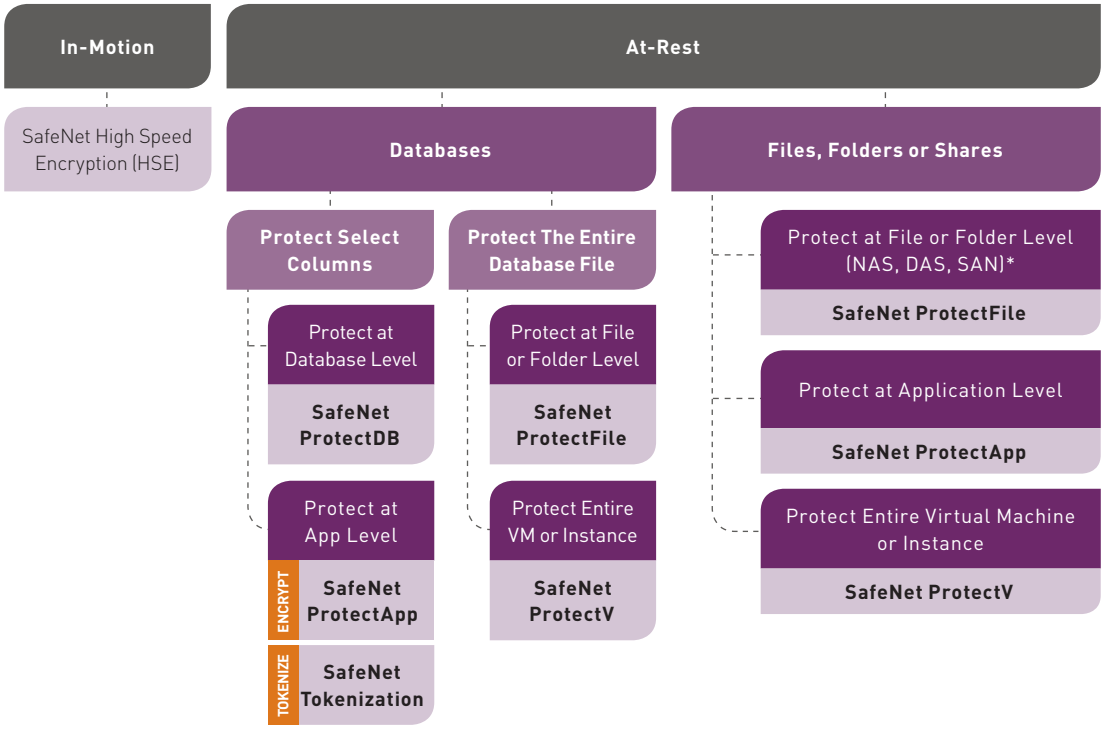
- Application and web servers
- File servers
- Databases

Data in Motion

There is sensitive data flowing across your network and/or between data centers.

Read on to follow our step-by-step guide or click on any item in the chart below to skip ahead to a specific step or learn more about a solution.

Where is your sensitive data?



NAS – Network attached storage
DAS – Direct attached storage
SAN – Storage area network

Protecting Your Data at Rest

If you have sensitive data at rest, it will typically reside in two places:

> Databases

> Files, folders, and shares

Databases

Your sensitive data assets residing in databases can be encrypted in two ways:

Option 1: Protect Select Columns in the Database

If you have sensitive data that resides within specific fields of a database, such as credit card numbers, social security numbers, email addresses, etc., this may be the best option for you.

Recommended Products

To protect structured data, SafeNet solutions that apply protection at the column-level within the database, or the application-level by encrypting or tokenizing the data before it is stored in a database. The following solutions are deployed with SafeNet KeySecure for centralized key management and work across on-premises, cloud, and virtual environments.

SafeNet ProtectDB

Column-level database encryption

SafeNet ProtectApp

Application-level encryption

SafeNet Tokenization

Application-level tokenization

Option 2: Protect the Entire Database File

If you have database exports, archives, and backups that contain sensitive information, encrypting the entire database file may be the best option for you.

Recommended Products

To protect the entire database file, SafeNet solutions encrypt data at the file-level, encrypt the entire virtual instance or machine, or complement encryption capabilities native to the database. All solutions are deployed with SafeNet KeySecure for centralized key management.

SafeNet ProtectFile

File system-level encryption

> Support for on-premises, cloud, and virtual environments

SafeNet ProtectV

Full disk encryption of virtual machines

> Supported cloud platforms include Amazon Web Services, VMware, Microsoft Azure and IBM SoftLayer

Transparent Data Encryption (TDE)

Native database transparent encryption

> Complements native encryption in Oracle and Microsoft SQL databases

> Ensures keys are stored separate from the data

Files, Folders, and Shares

If you have sensitive information located in files, folders, or shares in on-premises, virtual, and cloud environments, SafeNet products can apply protection to data in specific files and folders, to data at the application level, and to the entire virtual instance or machine.

Option 1: Protect Data at the File System-level

To protect files and folders on a file server, SafeNet solutions apply transparent and automated file-system level encryption of server data-at-rest in the distributed enterprise, including Direct Attached Storage (DAS), Storage Area Network (SAN), and Network Attached Storage (NAS) servers using CIFS/NFS file sharing protocols. The solution is deployed with SafeNet KeySecure for centralized key and policy management and works across on-premises, virtual, public cloud, and hybrid environments.

Recommended Product

SafeNet ProtectFile
File system-level Encryption

Option 2: Protect Data at the Application-level

Another option for protecting specific files is to apply protection at the application-level by encrypting select files and folders before they are stored on the file server. The SafeNet solution is deployed with SafeNet KeySecure for centralized key and policy management and works across on-premises, virtual, public cloud, and hybrid environments.

Recommended Product

SafeNet ProtectApp
Application-level Encryption

Option 3: Protect the Entire Virtual Machine or Instance

If you have large quantities of sensitive data to secure in a public cloud environment as a result of migrating your data center to the cloud, running a hybrid cloud environment, or bursting to a public cloud when applications running in a private cloud or data center need additional compute power, encrypting the entire virtual machine or instance may be the best option for you. The solution is deployed with SafeNet KeySecure for centralized key and policy management and enables complete ownership of data and keys even in shared, multi-tenant environments. Supported platforms include Amazon Web Services, VMware, Microsoft Azure, and IBM SoftLayer.

Recommended Product

SafeNet ProtectV
Full Virtual Machine or Instance Encryption

Protecting Your Data in Motion

Increasing network speeds, new cloud and remote data center services, and more accessible network pricing introduces both advantages and security threats to organizations. The availability of greater bandwidth allows us to exchange information faster and more frequently, but the huge growth of often-sensitive data volumes transmitted across networks presents real risks.

The risks are real – from malicious attacks to innocent errors in transmission. Data networks are not inherently safe. And, with the exponential growth in information-rich data transmission and the rapid increase in data networks, the risks have never been greater.

Officially certified by independent international testing authorities, hardware-based data encryption at Layer 2 is the most effective way to protect data on the move, and that's because it's the only security solution that travels with the data on your own network, your service provider's network or any other network.

At the data network level, traditional Internet Layer 3 (IPSec) security is not well suited to modern environments. It is complex to manage, does not scale well to larger settings, and with its considerable overhead, can compromise network performance by up to 50%. Ultimately, it delivers a less efficient cost per gigabyte.

Compared to Layer 3 (IPSec) encryption, Layer 2 networks can be secured and encrypted with dedicated appliances without any loss of speed and performance, minimal management, and greater reliability. This results in a comparatively lower cost per gigabyte.

Layer 2 Network Encryption

If you have sensitive data in motion that needs protecting, high speed encryption is the best option for you.

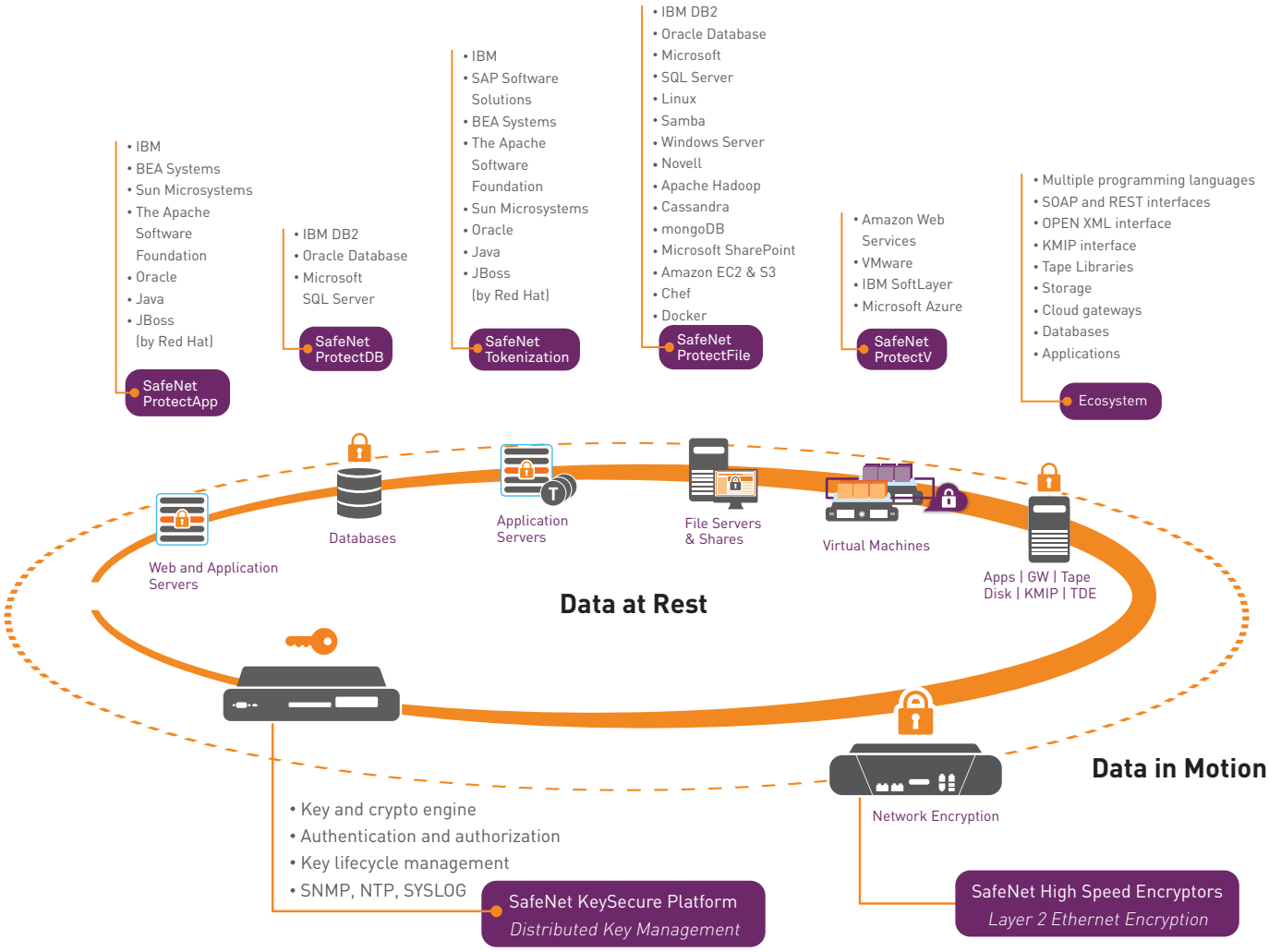
Recommended Product

SafeNet High Speed Encryptors: Network encryption

Comprehensive Data Protection for Your Enterprise

Gemalto offers a complete, enterprise-ready portfolio of SafeNet data protection solutions to keep your sensitive data at rest and data in motion secure. Based on the unique needs of your business, you can apply the right solutions where you need them, when you need them, and how you need them. This holistic approach enables you to meet your organization's immediate data security needs today, while investing in a solution that provides robust security, a growing ecosystem, and the scalability necessary to build a trusted framework for the future.

SafeNet Data Protection Portfolio



SafeNet Data-at-Rest Encryption Solutions

Protection of Sensitive Data at the Application-level

SafeNet ProtectApp: Application-level Encryption

SafeNet ProtectApp provides an interface for key management operations, as well as **encryption of sensitive data**. Once deployed, application-level data is encrypted as soon as it is generated or first processed and kept secure across its entire lifecycle, no matter where it is transferred, backed up, or copied.

Deployed in tandem with SafeNet KeySecure for centralized enterprise key management, SafeNet ProtectApp provides robust security and scalability. The solution enables the implementation of granular access controls that decouple administrative duties from data and encryption key access. For example, you can apply a policy to ensure that no single administrator can make a critical configuration change without additional approval.

SafeNet ProtectApp features built-in, automated key rotation and data re-keying, and can also perform a wide range of cryptographic operations including encryption, decryption, digital signing and verification, secure hash algorithms (SHA), and hash-based message authentication code (HMAC). The solution provides a single interface for logging, auditing, and reporting access to protected data and encryption keys.

- Environments: On-premises, Virtual, Public Cloud
- Web application servers: Apache Tomcat, IBM WebSphere, JBoss, Microsoft IIS, Oracle WebLogic, SAP, NetWeaver, Sun ONE, and more
- Development Libraries and APIs: Java, C/C++, .NET, XML open interface, KMIP, web services (SOAP and REST)

SafeNet ProtectApp Solution Spotlight Location Intelligence Business Maps Secure Route to Cloud

Customer problem

A leader in mapping and location intelligence business data opted to migrate its workloads to the cloud. The company needed a solution to encrypt data in Amazon S3 environments, and centrally manage and own its encryption keys to ensure data privacy and comply with various data privacy laws protecting personally identifiable information.

Solution

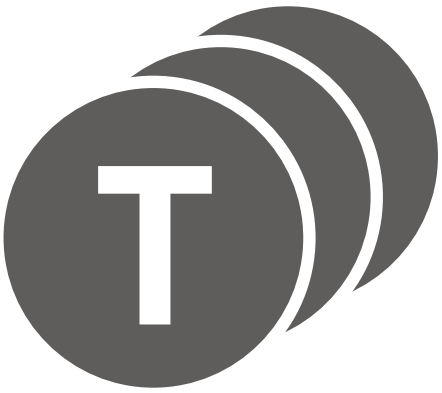
The company deployed SafeNet ProtectApp and SafeNet Virtual KeySecure for centralized key and policy management, as well as encryption of data in Amazon S3. The solution ensures the company is able to make data available to its customers, while still meeting regional and corporate data compliance regulations. Working together, SafeNet KeySecure and SafeNet ProtectApp provided many benefits to the organization including: management and cost savings by enabling a secure route to cloud, extensive logging and auditing, as well as automated key rotation; reliability and availability, including disaster recovery support; and the ability to scale and improve performance based on demand.

SafeNet Tokenization:
Application-level Tokenization Service

SafeNet Tokenization protects sensitive data (primary account numbers, social security numbers, phone numbers, passwords, email addresses, etc.) by replacing it with a unique token that is stored, processed or transmitted in place of the clear data.

Using **Format Preserving Tokenization** (FPT), SafeNet Tokenization preserves the length and format of the sensitive data. The solution is also flexible in its ability to support a variety of token formats, such as last four, first six, custom formats, and regular expression. In addition, SafeNet Tokenization utilizes Web APIs for easy deployment, requires no changes to existing databases and applications, and is extremely scalable across multiple datacenters in distributed environments.

Deployed with SafeNet KeySecure hardware or virtual appliance for key and policy management, SafeNet Tokenization provides a single, centralized interface for logging, auditing, and reporting access to protected data, keys, and tokens. For added security, SafeNet Tokenization also features built-in, automated key rotation and data re-keying. Compliant with PCI Tokenization Guidelines and VISA Tokenization Best Practices, SafeNet Tokenization is an ideal solution for organizations with high compliance costs as it significantly reduces



regulatory scope, facilitates the annual audit process, and results in reduced total cost of ownership.

- Environments: On-premises, Virtual, Public Cloud
- Token Vault Databases: Microsoft SQL Server, Oracle, MySQL
- APIs: Web services (SOAP, REST/JSON), Java, .NET
- Data Types: Unlimited support
- Token Formats: Broad support, including regular expressions and customized formats

SafeNet Tokenization Solution Spotlight:
Quick Service Restaurant Franchise Protects Data with Tokenization

Customer problem

A leading quick service restaurant franchise found its data in high demand across the organization. It needed to secure data as it moved through business analytics and intelligence systems to ensure customer and financial information remained secure in production and non-production databases in their virtual environment.

Solution

SafeNet Tokenization and SafeNet Virtual KeySecure was selected to tokenize the sensitive data to securely enable analysis by various teams throughout the organization, while maintaining control of keys in a virtual environment. The flexibility of the solution enabled the seamless integration with many of their existing applications and database platforms.

Protection of Sensitive Data at the Column-level

SafeNet ProtectDB: Column-level Database Encryption

From credit card information, patient data, and social security numbers to customer email addresses, enterprises often store their most valuable information assets in databases. SafeNet ProtectDB provides **transparent column-level encryption** of structured data residing in databases.

SafeNet ProtectDB enables large amounts of sensitive data to be moved in and out of the data stores rapidly by efficiently encrypting and decrypting specific fields in databases that may contain millions of records. The solution is extremely scalable and works across on-premises, virtual, and cloud environments.

The solution is deployed in tandem with SafeNet KeySecure for centralized key and policy management. SafeNet ProtectDB also features granular access controls that can be defined by role, user, time of day, and other variables, including the ability to prevent database administrators (DBAs) from impersonating another user with access to sensitive data.

For added security, SafeNet ProtectDB features built-in, automated key rotation and data re-keying, as well as a single interface for logging, auditing, and reporting. The solution enables isolation of sensitive data in a shared infrastructure, separation of duties, and improved compliance with a variety of regulations including, but not limited to, credit card numbers for Payment Card Industry Data Security Standard (PCI DSS).

- Environments: On-premises, Virtual, Public Cloud
- Databases: Oracle, Microsoft SQL Server, IBM DB2

SafeNet ProtectDB Solution Spotlight: Leading Insurance Provider Achieves PCI DSS Compliance

Customer problem

A leading insurance provider wanted to deploy a strong data protection strategy to comply with PCI DSS requirements and safeguard customer data, such as credit card numbers, telephone numbers, and other structured data residing in databases.

Solution

The company selected SafeNet KeySecure and SafeNet ProtectDB to address their current data security needs, while providing the foundation to support future risk and compliance challenges. To meet the PCI DSS requirement, the company took advantage of SafeNet KeySecure, an enterprise key manager that delivers the highest level of data security available in a commercial solution and covers the broadest variety of data types. It offers a unified platform with data encryption and granular access control capabilities that can be applied to databases, applications, mainframe environments, as well as individual files. SafeNet ProtectDB provides them with the flexibility to encrypt data at the column level within databases and also helps avoid the risks of "privileged-user" access by ensuring separation of administrative duties.

Protection of Sensitive Data at the File System-level

SafeNet ProtectFile: File Encryption

SafeNet ProtectFile provides transparent and **automated file-system** level encryption of server data at rest in the distributed enterprise, including Direct Attached Storage (DAS), Storage Area Network (SAN), and Network Attached Storage (NAS) servers using CIFS/NFS file sharing protocols.

The solution encrypts unstructured, sensitive data on servers, such as credit card numbers, personal information, logs, passwords, configurations,and more in a broad range of files, including word processing documents, spreadsheets, images, database files, exports, archives, and backups, and big data implementations.

SafeNet ProtectFile is deployed in tandem with SafeNet KeySecure for centralized key and policy management. The solution features granular access controls to ensure only authorized users or processes can view protected data, including the ability to prevent rogue administrators from impersonating another user with access to sensitive data. In addition, the solution provides built-in, automated key rotation and data re-keying and comprehensive logging and auditing.

- Environments: On-premises, Virtual, Public Cloud
- Platforms: Oracle, Red Hat Enterprise Linux, SUSE, Microsoft Windows
- Big Data: Apache Hadoop, IBM InfoSphere BigInsights
- Databases: Cassandra, IBM DB2, Microsoft SQL Server, Microsoft SharePoint, mongoDB, Oracle, MySQL, PostgreSQL, or any database, file, folder or shares
- Cloud Management: Chef
- Containers: Docker

SafeNet ProtectFile Solution Spotlight: Consumer Electronics Brand Keeps Intellectual Property on Lock Down

Customer problem

A well-known manufacturer of consumer electronics required a solution to secure design work and other intellectual property. The company desired a solution that was able to encrypt unstructured data files, such as word processing documents, spreadsheets, images, designs, and more, while applying policies to ensure only authorized users could access this critical information.

Solution

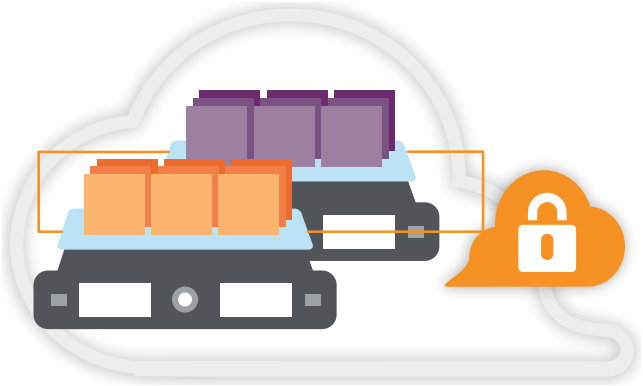
The company deployed SafeNet ProtectFile to encrypt its highly sought-after intellectual property in combination with SafeNet KeySecure for centralized key and policy management. SafeNet ProtectFile ensures the teams working on these highly sensitive projects can collaborate productively with the confidence that their files remain secure. When designers or product architects create a design document, it is first encrypted by the SafeNet ProtectFile and stored. The file can only be accessed by authorized users or applications based on policies set by administrators.

Protection of the Entire Virtual Machine or Instance

SafeNet ProtectV: Full Disk Encryption of Virtual Machines

SafeNet ProtectV is a high-availability solution that **encrypts sensitive data within instances, virtual machines, as well as attached storage volumes** in virtual and cloud environments. SafeNet ProtectV works with SafeNet KeySecure or SafeNet Virtual KeySecure to ensure strong, centralized key management. Once deployed, the solution enables enterprises to maintain complete ownership and control of data and encryption keys.

With SafeNet ProtectV, data is safeguarded and completely isolated from the cloud service provider, tenants in shared environments, or any other unauthorized party. Through SafeNet ProtectV's centralized management console, enterprises can audit and obtain compliance reporting on users accessing secured data.



- Environments: Virtual, Public Cloud
- Platforms Supported: Amazon Web Services, VMware, IBM SoftLayer, Microsoft Azure

SafeNet ProtectV Solution Spotlight: Global Financial Services Firm Secures Data in the Cloud

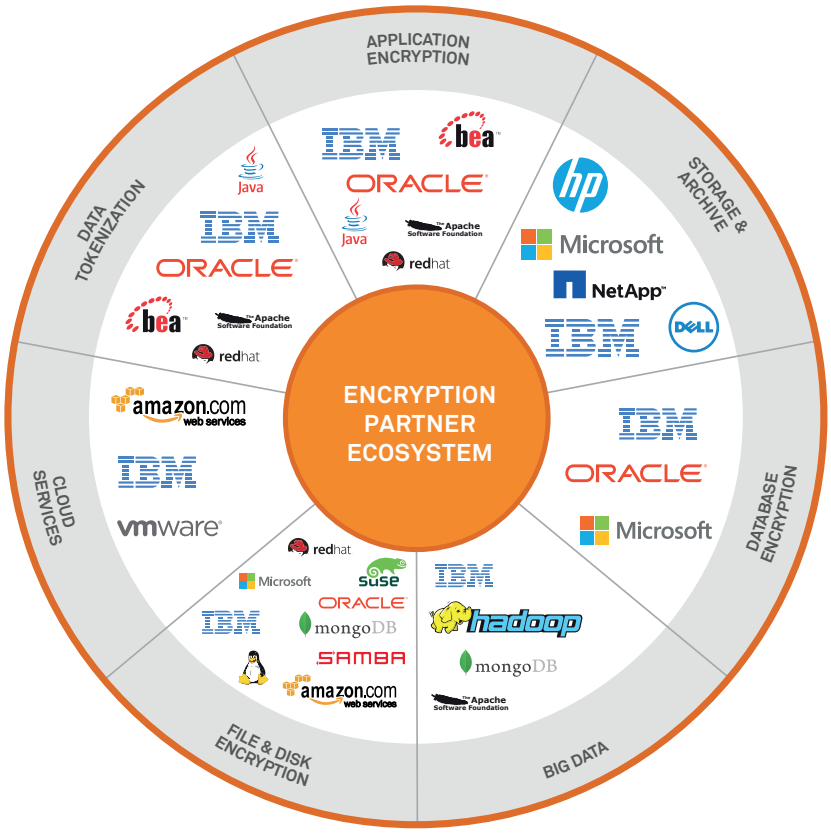
Customer problem

A leading global financial services firm wanted to deploy a single, third-party data security solution that included both encryption and key management to protect sensitive financial information – both internal organization data and customer data. The solution needed to run not only Amazon, but offer the flexibility to support future cloud service providers. They also wanted to be more elastic with their resources and test secure cloudbursting, or the ability to leverage the public cloud when an on-premises datacenter required additional compute power to support spikes in demand during the business day. A final requirement was the ability to deploy a single solution that would also support future cloud service providers and additional users, as needed.

Solution

SafeNet ProtectV and SafeNet Virtual KeySecure were deployed to provide strong encryption and key management and support secure cloudbursting. As a security-conscious company, the organization did not want to rely on Amazon's key management and encryption solutions. They selected SafeNet solutions as they were independent from the cloud service provider and enabled them to maintain complete ownership and control of their data and encryption keys at all times. SafeNet ProtectV was also able to meet the organization's requirements to encrypt the entire virtual machine instance, including attached storage volumes, as well as require authorization of a user before launching a virtual machine.


KEY MANAGEMENT PARTNER ECOSYSTEM
BACKUP & STORAGE
commvault
FalconStor
Symantec
STORAGE & ARCHIVE
NUTANIX
TantaCmm
BROCADE
Quantum
IBM
NetApp
DELL
Hitachi Data Systems
DATABASE ENCRYPTION
MySQL
ORACLE
Microsoft
IBM
SIEM TOOLS
ABOVE SECURITY
hp
RSA SECURITY
IBM
FILE & DISK ENCRYPTION
PKWARE
ViaSat
IBM
TERADATA
Raising Intelligence
CLOUD SERVICES
amazon.com web services
Dropbox
servicemesh
Google
CLOUD ENCRYPTION GATEWAYS
skyhigh
BLUE COAT
CSC servicemesh
CipherCloud
Trust in the Cloud


ENCRYPTION PARTNER ECOSYSTEM
APPLICATION ENCRYPTION
IBM
bea
ORACLE
Java
Java
The Apache Software Foundation
redhat
STORAGE & ARCHIVE
hp
Microsoft
NetApp
IBM
DELL
DATABASE ENCRYPTION
IBM
ORACLE
Microsoft
BIG DATA
IBM
hadoop
mongoDB
The Apache Software Foundation
FILE & DISK ENCRYPTION
redhat
Microsoft
suse
ORACLE
IBM
mongoDB
SAMBA
amazon.com web services
CLOUD SERVICES
amazon.com web services
IBM
vmware
DATA TOKENIZATION
Java
IBM
ORACLE
bea
The Apache Software Foundation
redhat

SafeNet Data-in-Motion Encryption Solution

High Speed Encryption:
SafeNet High Speed Encryptors (HSE)

In addition to its data-at-rest solutions, Gemalto delivers the world's leading certified high speed encryptors to secure data in motion. Gemalto ensures the most secure data-in-motion protection, maximum performance, near-zero overhead with "set and forget" management, and lowest total cost of ownership for speeds up to 10 Gbps. The first choice for Layer 2 encryption, our solutions are field-proven to secure data in transit for governments, defense agencies, global financial transactions networks, and the world's biggest cloud services providers.

Gemalto's high speed encryption solutions protect data in motion, including time-sensitive voice and video streams, as well as metadata for enterprise and government organizations.

SafeNet High Speed Encryptors Solution Spotlight:
Multinational Telco Secures Customers' Video, VoIP and Data in Motion

Customer Problem

A multinational telecommunications company provides telecommunications and IT services to corporate clients (commercial and government) across the globe. These clients require that their information in transit, including high bandwidth live video streaming, remains secure. Types of applications that require this include: legal proceedings via video link, confidential internal organization meetings such as earnings calls for global companies, and live remote supervision of border controls. Network data quality is a central factor in customers' relationships with service providers, and security needs to be seamless, so as not to negatively affect the entire user experience. Video in particular places significant demands on networks, and customers are unable to compromise on quality issues such as latency, jitter or packet loss

Solution

The broad range of available SafeNet High Speed Encryptors (HSE) suited the telco's different customer requirements, such as certifications and attractive pricing for large scale deployments. SafeNet HSEs deliver high speed Layer 2 encryption while meeting the most demanding requirements for secure network performance for data, voice, and video in large scale deployments. The solution is ideal for real time applications, providing very low latency and near zero overheads. Easy to deploy, SafeNet HSEs offered a much better return than alternate solutions the telco considered such as Layer 3 that include encryption but with very high overheads or MACsec which was only designed for LAN-based "hop-by-hop" network connections. Neither solution scales to meet the telco's requirements today, or into the future. With SafeNet Layer 2 encryption, the telco's customers get what they pay for from their networks, and the company can deliver the value-added services that help fuel improved customer satisfaction, reduce churn, and enhance retention.

SafeNet KeySecure: A Vital Component for Building an Effective Crypto Foundation

SafeNet KeySecure is a FIPS 140-2 validated enterprise key manager that provides extensive functionality to ensure that you remain in control of your keys and data at all times. Supporting the widest set of technologies and deployment scenarios, SafeNet KeySecure enables the creation of a centralized cryptographic service that enables you to streamline encryption deployments across your enterprise. Once data is encrypted, the centralization of policy and key management means that this data can pass through your systems transparently, and be available persistently for decryption by authorized users. Scalable to millions of records and trillions of transactions, SafeNet KeySecure delivers the throughput, responsiveness, and availability organizations need for vital cryptographic processing and enterprise key management. This means you can ensure consistent and unified security policies, regardless of where secured data is located across your on-premises, virtual, public cloud, and hybrid environments.

Central Key Management and Administration

SafeNet KeySecure offers a long-term solution that enables organizations to build a foundation and streamline the key management efforts associated with encryption—while at the same time strengthening the security of the sensitive data that has been protected with encryption.

Comprehensive IT Infrastructure Support

SafeNet KeySecure seamlessly integrates with the suite of SafeNet encryption connectors, including SafeNet ProtectApp for application-level encryption, SafeNet ProtectDB for column-level encryption, SafeNet ProtectFile for file system-level encryption, SafeNet ProtectV for encryption of virtual machines and instances, and SafeNet Tokenization for application-level tokenization. SafeNet KeySecure enables strong access controls to be applied to ensure sensitive data is secured wherever it resides.

Standardized Integration and Third-Party Key Management

SafeNet KeySecure also offers a wide range of standard APIs, development libraries, and support for the Key Management Interoperability Protocol (KMIP) standard—giving organizations optimal deployment efficiency, no matter when, where, and how they integrate encryption. With SafeNet KeySecure, security teams can develop a common encryption framework, and publish set standards that business groups and developers can easily work with to leverage encryption, without having to become cryptographic experts.

Gemalto's Portfolio of SafeNet Identity and Data Protection Solutions

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core. Gemalto's portfolio of 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 safenet.gemalto.com
Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free