Gemalto's SafeNet Encryption Connectors

A Complete, Enterprise-ready Encryption Platform

Data is delivering more value than ever before to enterprises around the globe. However, as the data organizations produce, process, and store grows, it becomes a prime target for hackers and malicious attacks. Encryption is a critical last line of defense because it applies protection directly to the data wherever it resides–in today's distributed enterprise.

Comprehensive Data Protection for Your Enterprise

Gemalto offers a complete, enterprise-ready platform that provides centralized and uniform data protection across your on-premises, virtual, and public cloud environments, including hybrid implementations. Gemalto's data-at-rest solutions enable you to:

> **Protect and control access to your data**
With Gemalto's portfolio of SafeNet Encryption Connectors, you can encrypt and control access to sensitive structured and unstructured data at all levels of the enterprise data stack, including the application, database (column or file), file-system, full disk (virtual machine), and network attached storage levels.

> **Protect and manage your keys**
All of the SafeNet Encryption Connectors work with Gemalto's FIPS 140-2 up to Level 3 validated SafeNet KeySecure enterprise key manager for centralized key and policy management across multiple sites. For optimal security, keys are stored separately from the protected data.

In addition to data-at-rest protection, Gemalto's SafeNet High Speed Encryptors (HSE) enable you to encrypt the sensitive data flowing across your network or between data centers.

GEMALTO'S PORTFOLIO OF SAFENET ENCRYPTION CONNECTORS

Gemalto SafeNet ProtectApp
> Application-level encryption

Gemalto SafeNet ProtectDB
> Column-level database encryption

Gemalto SafeNet ProtectFile
> File system-level encryption

Gemalto SafeNet Tokenization
> Application-level tokenization

Gemalto SafeNet ProtectV
> Full disk virtual machine encryption

Gemalto SafeNet StorageSecure
> Remote network attached storage encryption

SafeNet ProtectApp: Application-Level Encryption

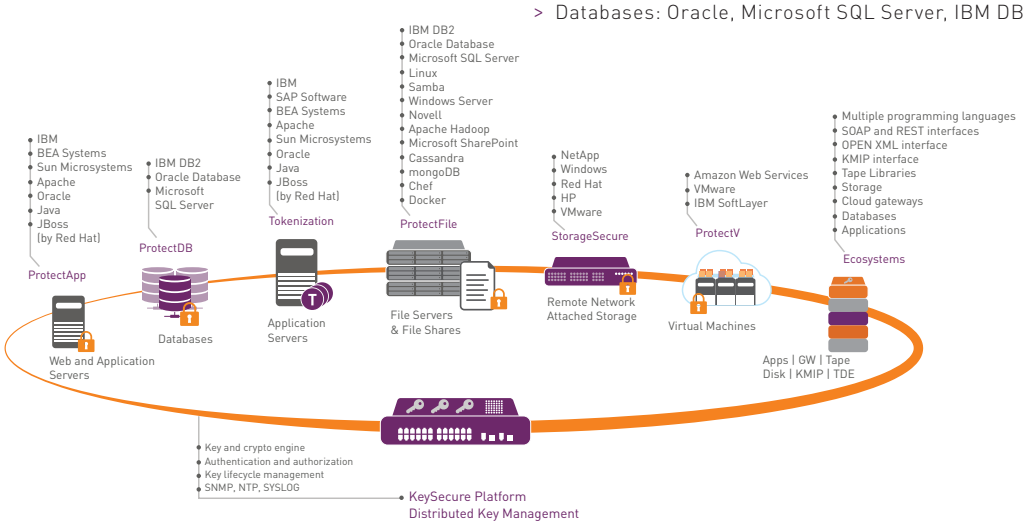
SafeNet ProtectApp provides an interface for key management operations, as well as encryption of sensitive data. Once deployed, application-level data is kept secure across its entire lifecycle, no matter where it is transferred, backed up, or copied. Using ProtectApp APIs, both structured and unstructured data can be secured in multi-vendor application server infrastructures. SafeNet ProtectApp also features granular access controls to ensure only authorized users or applications can view protected data, built-in, automated key rotation and data re-keying, comprehensive logging and auditing, and the ability to offload encryption to SafeNet KeySecure for external processing power.

> 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 ProtectDB: Column-level Database Encryption

SafeNet ProtectDB provides efficient and transparent column-level encryption of sensitive data, such as credit card numbers, social security numbers, and passwords, in multi-vendor database management systems. SafeNet ProtectDB also features the ability to define granular access controls 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. In addition, the solution features built-in and automated key rotation and data re-keying, comprehensive logging and auditing, and the ability to offload encryption to SafeNet KeySecure for external processing power.

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



SafeNet ProtectFile: File System-level 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 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: AIX, Centos, Oracle, Microsoft Windows, Red Hat Enterprise Linux (RHEL), SUSE, Ubuntu
- 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 Tokenization: Application-Level Tokenization

SafeNet Tokenization protects sensitive information by replacing it with a surrogate value that preserves the length and format of the data. The solution tokenizes numeric and alphanumeric data and returns tokens in an unlimited number of formats. SafeNet Tokenization is used to address a wide range of use cases, including securing primary account numbers to achieve PCI DSS compliance and protecting other sensitive data such as personally identifiable information (PII). It can be applied in big data, as well as other scenarios that require static data masking or the exposure of production databases to non-production environments, such as testing, development, staging, research, etc. SafeNet Tokenization features granular access controls to ensure only authorized users or applications can view protected tokens and data, comprehensive logging and auditing, and requires no changes to application, databases, or legacy systems.

- 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 ProtectV: Full Disk Virtual Machine Encryption

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. Once deployed, the solution enables enterprises to maintain complete ownership and control of data and encryption keys by keeping it safeguarded and completely isolated from the cloud service provider, tenants in shared environments, or any other unauthorized party. ProtectV also requires users to be authenticated and authorized prior to launching a virtual machine.

- Environments: Virtual, Public Cloud
- Platforms Supported: AWS, VMware, IBM SoftLayer

SafeNet StorageSecure: Remote Network Attached Storage Encryption

SafeNet StorageSecure is a network attached storage encryption solution that connects to Ethernet networks. The solution secures file data stored on NAS servers using CIFS/NFS file sharing protocols, and block data. Backups or replicas of the file shares remain encrypted, adding security to secondary and off-site storage. While SafeNet StorageSecure can securely store all encryption keys and associated parameters in hardware, it can also be deployed with SafeNet KeySecure for centralized key management of those keys, as well as other heterogeneous encryption keys.

- Environments: On-premises
- Clients: Windows 7/8, Windows Server, VMware ESXi, RedHat (RHEL)
- Storage Arrays: NetApp FAS, HP StoreEasy, Windows Server, RedHat (RHEL)
- Antivirus Scanners: TrendMicro, McAfee

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto 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 newly expanded portfolio of SafeNet Identity and Data Protection solutions enables 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.

GEMALTO.COM

gemalto
security to be free