gemalto
security to be free

WHITE PAPER

Encryption as an IT Service

A Streamlined, Repeatable Model for Centralized, Enterprise-wide Encryption

Introduction

More compliance mandates. More security threats. More deployments. For today's enterprise security teams, there continues to be more of everything—except time and money of course. It is within this context that information security has become both an increasingasset and liability.

In order to meet their charters, security teams have become more reliant on encryption and tokenization, particularly for sensitive data, such as personally identifiable information, human resources files, financial data, and all intellectual property. All too often, however, information security deployments are undertaken during urgent "fire drills"—responses to new mandates, threats, or breaches that have tight timelines and specific near-term objectives.

However, the problems are here to stay. Given the disjointed nature of these encryption and tokenization deployments, organizations must contend with security "islands"—disparate, isolated encryption approaches. Today, it is not uncommon for organizations to have dozens of unrelated, sometimes even overlapping encryption platforms deployed across the enterprise, particularly as data is stored in a variety of locations on-premises and in the cloud. This is simply not sustainable in the long term. Following are a few reasons:

- **Costly, complex administration.** Security administration is time-consuming, costly, and complex, especially when implemented and administered on specific siloed systems rather than across the enterprise on a single platform.
- **Inconsistent security policy enforcement.** As more isolated systems are deployed, it becomes even more difficult to enforce uniform security policies across the organization.
- **No repeatable process.** With every new application and mandate, the security organization, and the rest of the business start over—investing time and effort in defining, architecting, and building a new encryption/tokenization system from scratch.
- **Inhibited data and business workflow.** Encryption deployments run counter to the increasing interconnectedness of corporate applications and workflows. Sharing sensitive data across multiple departments can introduce security gaps, as well as complexity and latency, into critical business processes.
- **Audit challenges.** With each new isolated encryption platform that is deployed, the process of tracking compliance status, preparing for audits and being audited grows even more time consuming. Silos of information need to be sifted through, aggregated, and analyzed.

Encryption as an IT Service

To counter the encryption challenges faced by organizations today, enterprise IT teams can offer their companies centralized key management, encryption, and tokenization, including auditing and compliance capabilities, as an IT service. Taking advantage of the "as-a-service" concept to make data encryption as simple as possible, IT can combine resources to provide their "customers" the ability to manage their encryption in a way that enables them to meet their data security and compliance requirements simply, cost-effectively, elastically, and, of course, securely across different solutions, data centers, geographies, or environments, or all of these areas.

By enabling IT to serve as the encryption service provider, encryption and key management can be centralized but distributed. This means that consistent security policies can be set across the organization's varied encryption solutions and updated as needed automatically, with ease. Standards can be maintained throughout. The encryption service provider can utilize their knowledge effectively to provide high-level APIs with consistent security parameters across the organization. The encryption service consumers, whether they are the business units and developers or the actual applications, databases, or file servers registered to the "service", can benefit from the economies of scale and security provided.

As efforts are consolidated in a "one-stop-shop" service, "build once" solutions can be replicated effectively and overlapping encryption solutions can be avoided. For example, developers don't decide on key types or sizes, as they are already abstracted by APIs, ensuring that security remains in the hands of the security experts. Auditing and compliance tracking is also simplified as it is centralized.

Gemalto SafeNet Solutions: Enabling Encryption as an IT Service

Gemalto provides a centralized solution that enables organizations to move past silo-constrained encryption and begin to deploy encryption as an IT service centrally, uniformly, and at scale across the enterprise. SafeNet solutions from Gemalto deliver unmatched coverage—securing databases, applications, file servers, and storage in the traditional data center, virtualized environments, and the cloud, and as the data moves between these different environments. Gemalto also provides the critical key management needed to effectively and efficiently enable protection across the enterprise. With Gemalto, organizations can apply data protection where they need it, when they need it, and how they need it—according to the unique needs of their business.

Armed with these capabilities, organizations can realize a host of benefits:

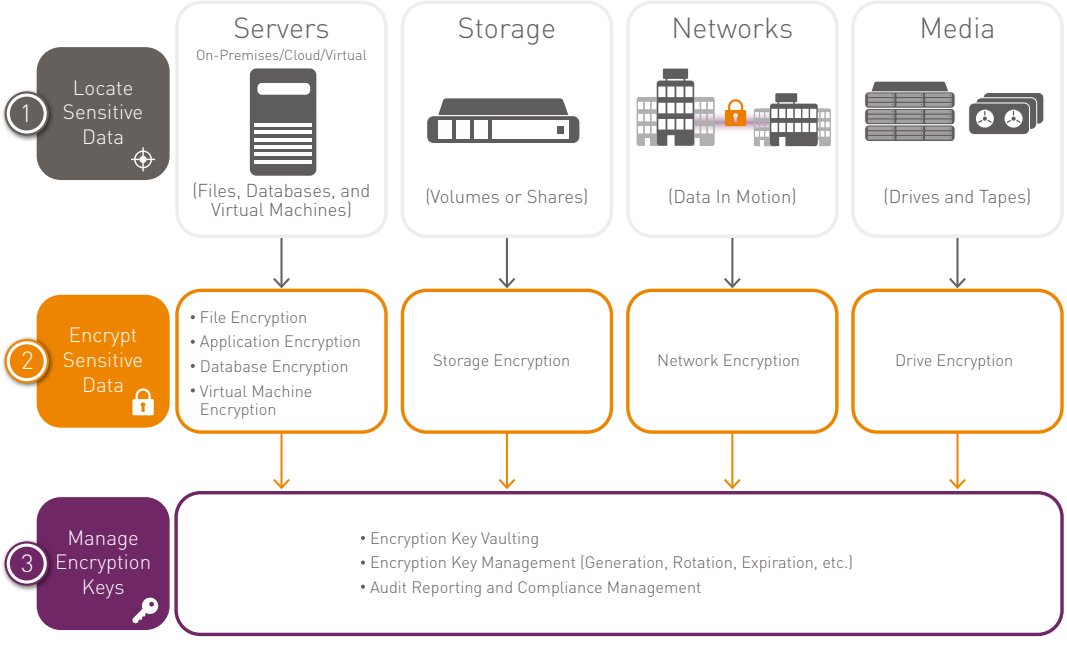
Strengthen security. With Gemalto, security policies can be both centrally managed and broadly deployed. As a result, administrators can more practically and effectively ensure security policies are being enforced. Sensitive cryptographic keys and administrative controls, rather than being broadly distributed, are in tightly secured, centralized, purpose-built security mechanisms.

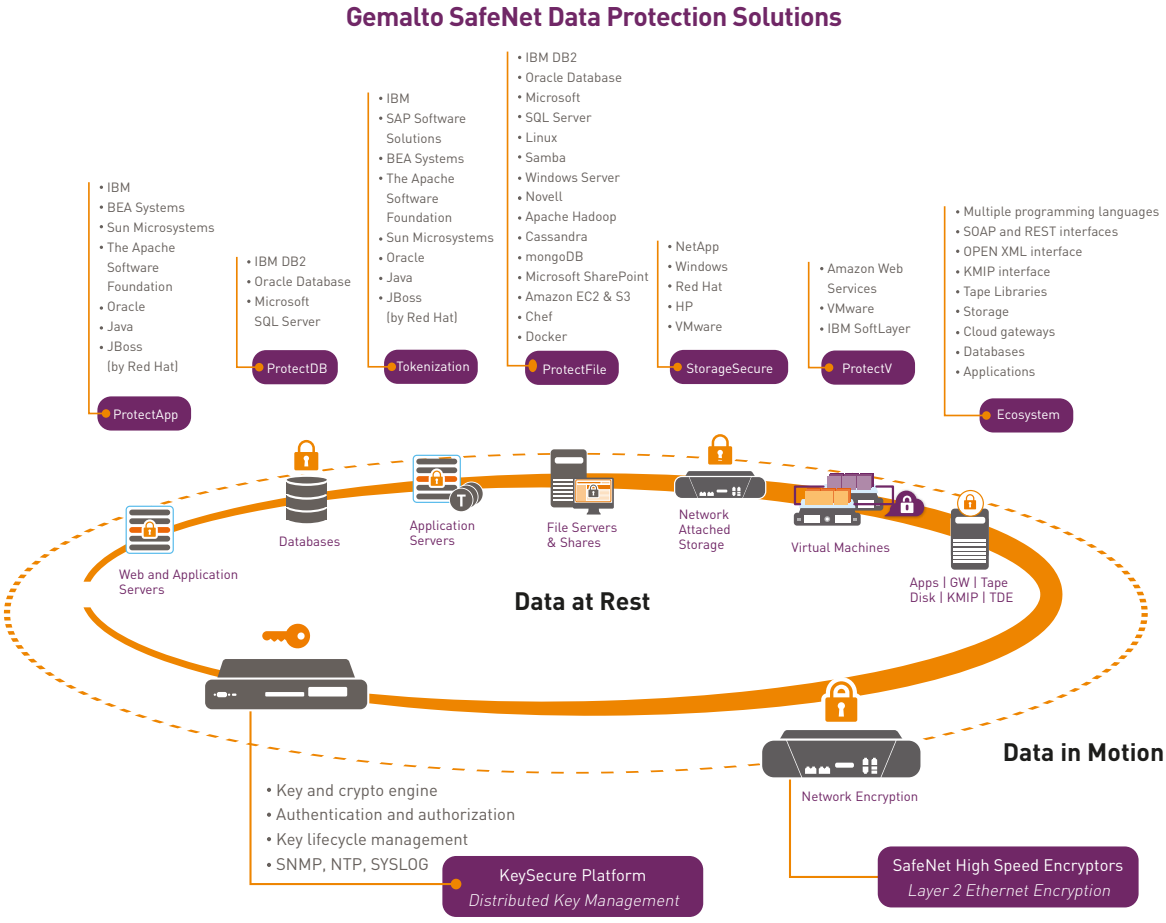
Strengthen compliance and reduce audit costs. With a unified, cohesive view of cryptographic activity across an enterprise, organizations can much more readily track and optimize compliance with all relevant security and privacy mandates. Tokenization in particular enables reduced audit scope. Auditors and internal administrators can leverage a single interface and repository to verify compliance status—which dramatically reduces audit durations and costs.

Reduce security and IT costs. Instead of investing a lot of money and effort in reinventing the wheel each time a new encryption project becomes necessary, organizations can leverage proven, repeatable, and documented processes. With centralized, efficient processes for managing policies and cryptographic keys, both upfront cost and ongoing administration efforts are minimized.

Increased IT and business agility. By leveraging a cohesive, centrally managed platform, and rolling encryption out as an IT service, IT and security teams can become much more nimble in adapting to changing requirements and challenges. New encryption services can be rolled out quickly and effectively. Rather than being stuck in isolated islands, data is free to move securely throughout the enterprise to support business objectives—without making any compromises in security. Business units can more quickly add the new services and capabilities they need, without requiring IT or team members to become experts in cryptography.

Steps to Secure Sensitive Data Everywhere





SafeNet Solutions from Gemalto: Delivering the Key Capabilities for Encryption as an IT Service

Gemalto SafeNet KeySecure is the foundation for delivering encryption as an IT service. Supporting the widest set of technologies and deployment scenarios, SafeNet KeySecure enables the creation of a centralized cryptographic service that streamlines enterprise wide encryption deployment. 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 appliances deliver the throughput, responsiveness, and availability organizations need for vital cryptographic processing and enterprise key management. This means you can ensure consistent security policies across all your encryption platforms, regardless of where they reside - on premises in your physical or virtual data center, or even in the public cloud.

Central Key Management and Administration

Gemalto offers a long-term solution that enables organizations to significantly streamline the key management efforts associated with encryption—while at the same time strengthening the security of the sensitive data for which encryption has been employed to protect. SafeNet KeySecure can centrally manage keys and policies for encrypted data across an enterprise.

Comprehensive IT Infrastructure Support

SafeNet KeySecure supports the broadest range of deployment points—including from applications, databases, file servers and storage, endpoints, third-party key management, and more. Further, SafeNet KeySecure can secure sensitive data wherever it resides—whether in the traditional data center, virtualized environments, or the cloud.

Standardized Integration and Third-Party Key Management

SafeNet KeySecure 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 SafeNet Products: The Building Blocks for Encryption as an IT Service

With Gemalto solutions, organizations can secure sensitive information, wherever it resides.

Data at Rest

Gemalto SafeNet ProtectApp: Application-level Encryption

SafeNet ProtectApp offers robust encryption of data at the application layer, including the industry's most widely used web application servers and enterprise applications. Through SafeNet ProtectApp's use of standard APIs and libraries, such as Java, .NET, C/C++, XML, and web services (SOAP/REST), organizations can integrate application encryption with minimal effort. The solution works with SafeNet KeySecure for centralized key and policy management and can be deployed across on-premises, virtual, public cloud, and hybrid environments.

Gemalto SafeNet ProtectDB: Column-level Database Encryption

Gemalto delivers powerful protection of sensitive corporate and customer information stored in databases. SafeNet ProtectDB delivers transparent column-level encryption of sensitive data stored in databases, across on-premises, virtual, public cloud, and hybrid environments. SafeNet ProtectDB allows for separation of duties and "M of N" policies, which prevent any single administrator from making critical configuration changes without additional approvals of other administrators. This solution works across multiple DBMS environments, is transparent to applications, and is deployed in combination with SafeNet KeySecure for centralized key and policy management. Packages are available for Oracle, Microsoft SQL Server, and IBM DB2 across Windows, Linux, Solaris, HP-UX, AIX, and IBM i/OS platforms.

Gemalto SafeNet Tokenization: Application-level Tokenization Service

SafeNet Tokenization offers organizations a significant opportunity—a way to significantly reduce the number of systems, applications, and users that can access sensitive or regulated data—and so dramatically reduce audit and security costs. SafeNet Tokenization offers a variety of integration options, providing customers with the flexibility to choose the right security technique for their environment. The tokens are created using Format Preserving Tokenization (FPT), maintaining the length and format of the original data, yet masking the actual information, or some of it. SafeNet Tokenization offers multiple options for FPT, minimizing the changes and adaptations that applications undergo when implementing a tokenization solution. With FPT, the solution enables IT organizations to ensure all applications and user interactions will continue to operate transparently after tokenization is employed. SafeNet Tokenization can be deployed across on-premises, virtual, public cloud, and hybrid environments.

Gemalto 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. 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.

Gemalto SafeNet ProtectFile: File System-level Encryption

SafeNet ProtectFile provides transparent and automated file-system-level encryption of sensitive data at rest on servers in the distributed enterprise—either on-premises or in cloud or virtualized environments. SafeNet ProtectFile encrypts sensitive data at rest that may include application data (configurations, passwords, logs), database data (data files, backups), big data, or data in folders (documents, images, media files, such as intellectual property and human resources or payroll files). SafeNet ProtectFile supports Microsoft Windows and Linux file servers and can be deployed across on-premises, virtual, public cloud, and hybrid environments.

Gemalto SafeNet ProtectV: Full Disk Encryption of Virtual Machines

SafeNet ProtectV is a high-availability encryption solution that secures sensitive data in cloud and virtual environments. The solution encrypts data within instances, virtual machines, and storage volumes, and uses strong key management capabilities to ensure enterprises maintain complete ownership and control of their data. 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. The solution can be deployed in the following virtual and cloud environments: Amazon Web Services, VMware, and IBM.

Data-in-Motion Security

Gemalto SafeNet High Speed Encryptors (HSE): Network Encryption

In addition to its data-at-rest solutions, Gemalto delivers the world's leading certified high speed encryptors to secure data in motion. SafeNet HSEs ensure 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. SafeNet High Speed Encryptors protect data in motion, including time-sensitive voice and video streams, as well as metadata for enterprise and government organizations.

SafeNet High Speed Encryptors allow enterprises and service providers to deploy best in class security and performance with true end-to-end network encryption regardless of the routing and switching fabric deployed in their networks. SafeNet HSEs operate in any network topology including fully meshed environment, support multicast traffic, enable variable speeds (10M to 10G) across multiple links, while securing and optimizing the performance of your data in motion. Most metro and long haul networks rely on network equipment from multiple vendors and SafeNet HSEs provide "bump-in-the-wire" encryption capabilities to preserve this capital investment by interoperating with all network equipment vendors.

Whether your requirements are for datacenter-interconnect, site-to-site connectivity, data back-up, disaster-recovery, or you want to be able to move your data to the cloud securely, SafeNet HSE ensures transparent encryption as your data moves across the network.

Conclusion

Encryption has become a core asset for organizations seeking to sustain compliance with regulatory mandates and safeguard their sensitive assets. However, deploying and administering dozens of disparate encryption platforms isn't sustainable—presenting negative implications for cost, administrative overhead, and business agility. Further, treating each new encryption initiative as an isolated, one-off event only exacerbates these issues over time. To build a sustainable security foundation, organizations need to employ encryption as an IT service—centrally and cohesively implementing and managing encryption across an entire enterprise. By doing so, organizations can realize significant benefits in overall security, administrative efficiency, and business agility.

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.

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

GEMALTO.COM

gemalto
security to be free