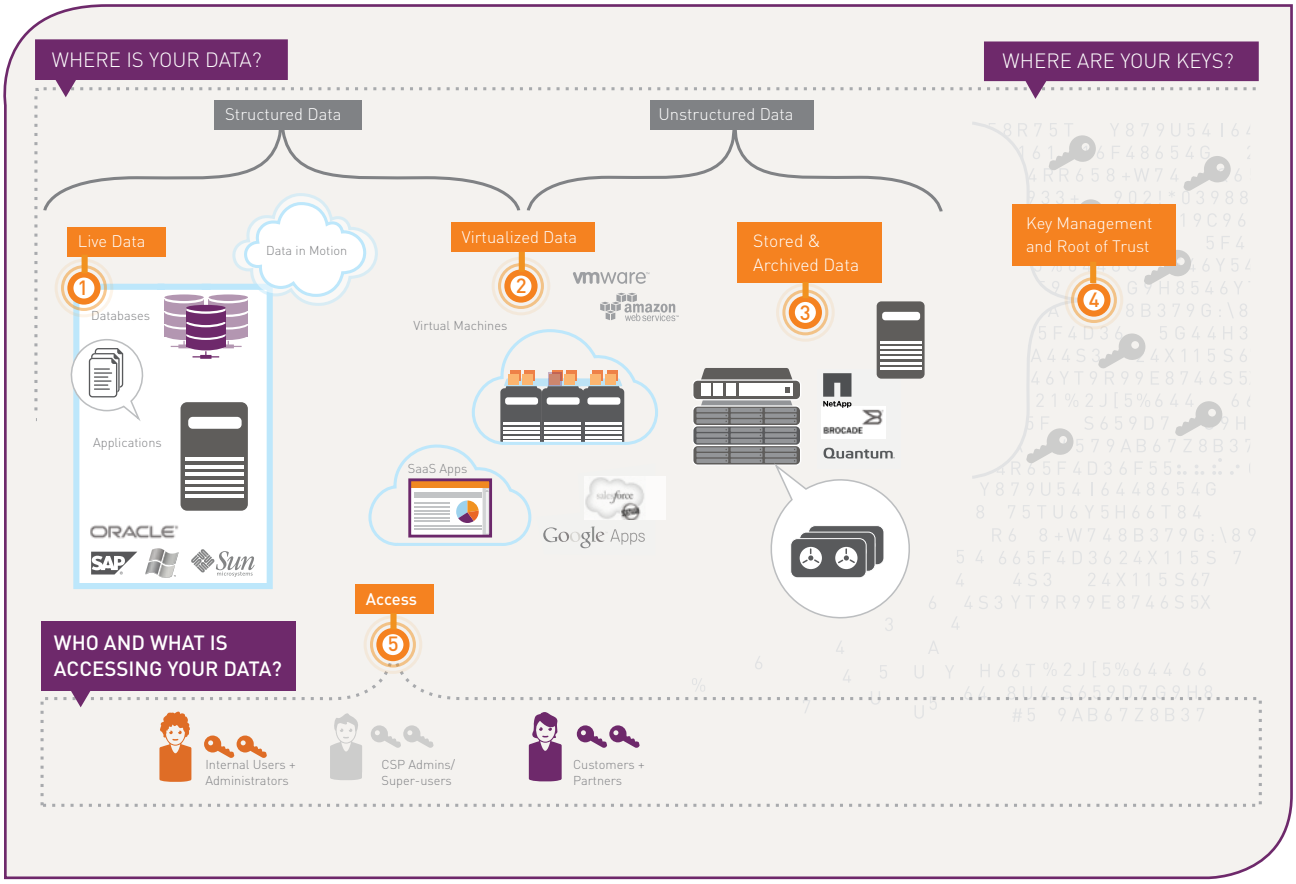
gemalto
security to be free



FAMILY BROCHURE

Sensitive data is everywhere. So are we.

SafeNet Data Protection Solutions from Gemalto

Protecting sensitive data across physical, hybrid and cloud-enabled environments

SENSITIVE DATA IS EVERYWHERE. SO ARE WE.

In a complex and evolving climate of advanced threats, virtualization, regulatory mandates, and mobility, organizations are taking a data-centric approach to protect and control their sensitive information. Gemalto offers the only complete portfolio that provides protection of sensititve data, transactions, and identities from the core to the edge, at all critical points in its lifecycle. From the physical and virtual datacenter to the cloud, Gemalto helps organizations remain protected, compliant, and in control - no matter where their business takes them.

Enabling Protection

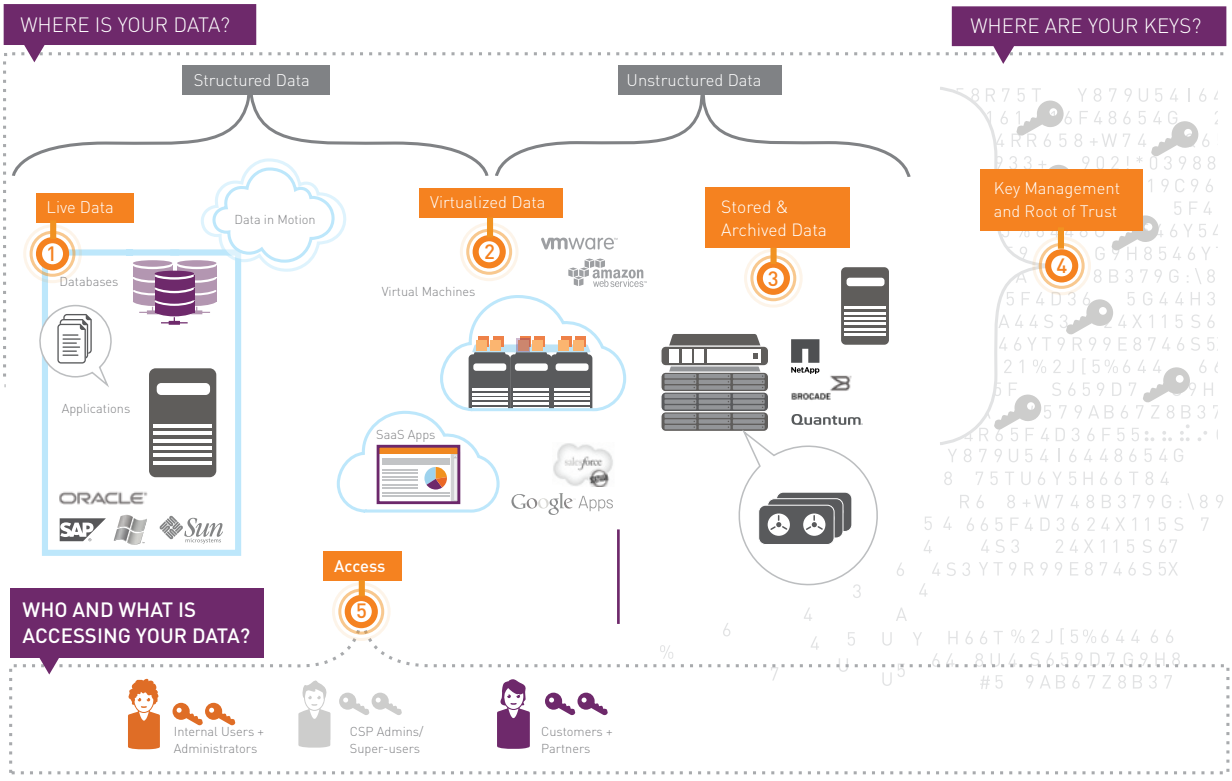
Gemalto helps organizations move past silo constrained encryption and crypto management to centrally and uniformly deploy a data protection solution across the enterprise that scales as needs grow, while effectively controlling security policies. Gemalto's suite of SafeNet solutions deliver unmatched coverage—securing personally identifiable information (PII), intellectual property (IP) and other sensitive data in databases, applications, files and folders, and network attached storage in on-premises, virtual, and public cloud environments, and as it moves across the network to and from these different environments. Gemalto also provides the critical key management needed to effectively and efficiently enable protection across the enterprise wherever data resides. With Gemalto, organizations can apply data protection where they need it, when they need it, and how they need it – consistently and effectively.

SafeNet Crypto Foundation

At the core of this data protection platform is the SafeNet Crypto Management portfolio - a best-in-class crypto foundation that supports the greatest number of organizational use cases both on-premises and in the cloud. Supporting the widest set of technologies and deployment scenarios, this portfolio of key management and key storage solutions provides a centralized cryptographic platform that streamlines encryption deployment, and centralizes policy and key management across the enterprise. Once sensitive information is encrypted, the protected data can pass through your systems transparently, and be persistently available for decryption by authorized users. Gemalto Data Protection solutions deliver the throughput, responsiveness, and availability organizations need for vital cryptographic processing to ensure your data is secure throughout its lifecycle.

The Root of Trust For Sensitive Data

As internal and external risks grow, the primary mechanism to protect data remains encryption. Over and above the requirement to consolidate the organization's crypto foundation and reduce the number of encryption silos, ascertaining that the encryption keys are secure is a fundamental requirement for ensuring that encryption is effective. Ultimately, the success of the organization's efforts to maintain ownership of its data depends on the efficacy of its key ownership efforts and is essential to maintaining control of sensitive data even in shared environments. Interoperability and centralized management enable the crypto foundation to be successfully deployed across the board, while standards-based platforms and adherence to industry regulations help to conform to organizational security requirements, and meet compliance and governance obligations.



GEMALTO PRODUCTS: THE BUILDING BLOCKS FOR THE CRYPTO FOUNDATION

Regardless of the nature of the business, all organizations have sensitive data that must be protected from exposure. The SafeNet crypto foundation from Gemalto enables the protection of sensitive data. The crypto foundation is comprised of a variety of elements, from the extensive encryption engines supported to the type of data they support. With Gemalto's portfolio of SafeNet data protection solutions, you can secure 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) levels, across your on-premises, hybrid and cloud-enabled environments. Gemalto also enables you to secure that data as it moves across the network and between different environments. Gemalto enables you to protect and control sensitive data as it expands in volume, type, and location, while improving compliance and governance visibility and efficiencies through centralized management and policy enforcement. Gemalto's solutions protect growing volumes of data with transparent, fast, granular, network-based encryption, and provide strong access control mechanisms and integrated, centralized key management for separation of duties, privileged administrator risk mitigation, policy enforcement, and data access auditing.

SAFENET KEYSECURE:
ENTERPRISE KEY MANAGEMENT

Enterprise crypto management is a vital component for an effective crypto foundation, allowing organizations to effectively manage their sensitive information wherever it resides. SafeNet's enterprise crypto management solution, SafeNet KeySecure, offers extensive key lifecycle management functionality to ensure that you remain in control of your keys and your data at all times. A highly available, scalable hardware appliance, SafeNet KeySecure enables centralized management of all supported encryption applications across the organization. The SafeNet KeySecure platform enables offloading of all cryptographic activities to specific encryption applications or centralized cryptographic functionalities. Reducing the complexity of security administration, SafeNet KeySecure offers enterprise-ready features such as policy management.

Capabilities such as defining policies which enable granular role-based access controls and a centralized interface for logging, auditing, and reporting are essential to ensuring compliance. For example, SafeNet KeySecure proactively alerts administrators in case of decrypt overuse of any of its connectors, and enable granular authorization controls based on user key permissions. Existing access controls can be automatically retrieved from existing LDAP/Active Directory services and further defined within the administration console to provide an additional layer of access management. SafeNet KeySecure supports a broad range of deployment scenarios including applications and databases in the on-premise and virtual datacenter and in private, hybrid, and public clouds.

As the use of encryption grows, key management is rapidly becoming a critical requirement for the enterprise—helping organizations establish centralized control over data and keys, and reduce cost, complexity, and sprawl.

Built on the OASIS KMIP (Key Management Interoperability Protocol) standard, SafeNet KeySecure delivers high assurance solutions for key management that help customers protect and control their data, address and respond to regulatory requirements, and get the most value out of their investments.

In addition to supporting Gemalto's own line of data protection solutions, SafeNet KeySecure also supports data in SANs for Native Encryption or completed native array encryption with Hitachi Data Systems (HDS), NAS storage such as NetApp NSE (Full Disk Encryption), archived data including HP Enterprise Systems Library (ESL) G3, and Quantum Tape Libraries, and SafeNet HSMs, and any other encryption solutions leveraging KMIP. SafeNet KeySecure helps organizations to leverage their crypto foundation to improve operational efficiency and enhance their overall security posture through its hardware based appliance which includes an embedded FIPS 140-2 Level 3 SafeNet PCIe HSM.

SAFENET HARDWARE SECURITY MODULES:
SECURE CRYPTO KEY STORAGE

At the root of trust of the crypto foundation are the cryptographic keys. The security of these keys is imperative and requires a high assurance solution capable of protecting against ever-evolving data threats. SafeNet Hardware Security Modules (HSM) provide a high-performance, high assurance trust anchor for encryption keys, and an easy-to-integrate application and transaction security solution - a FIPS 140-2 Level 3 validated, CC EAL 4+ certified highly secure platform for the protection of keys throughout the key lifecycle. As a hardware-based solution, HSMs are able to generate extremely secure key material, ensure complete control over key copies, and provide a high level of auditability.

The high security design of SafeNet (HSM) ensures the integrity and protection of crypto keys throughout the key lifecycle. SafeNet HSMs are available in a variety of models and configurations with a wide range of security, performance, and operational capabilities for accelerated encryption, and secure key generation, storage, and backup. With the keys-in-hardware approach, applications communicate with keys stored in the HSM via a client – but keys never leave the HSM. In addition, SafeNet KeySecure can provide visibility into the management of keys within the HSMs too.

SAFENET CRYPTO COMMAND CENTER:
CENTRALIZED CRYPTO RESOURCE MANAGEMENT

IT departments and Service Providers can now quickly and securely expand IT capabilities and streamline their infrastructure in physical, cloud, hybrid cloud and virtual environments with SafeNet Crypto Command Center. This is the market's first solution to fully exploit the benefits of virtualization, including reduced costs and innovation, by provisioning SafeNet HSMs without compromising security or compliance. Together SafeNet Crypto Command Center and SafeNet HSMs combine to form one complete, centralized solution for the management of your crypto HSM resources – a crypto hypervisor that delivers on-demand while ensuring you maintain full control of your encryption services and data.

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. Safenet ProtectV also requires users to be authenticated and authorized prior to launching a virtual machine.

- **Environments:** Cloud-enabled
- **Platforms Supported:** Amazon EC2, Amazon VPC, Amazon GovCloud, Microsoft Azure, VMware vSphere, IBM SoftLayer

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, Cloud-enabled
- **Databases:** Oracle, Red Hat Enterprise Linux, SUSE, Microsoft Windows
- **Big Data:** Apache Hadoop, IBM InfoSphere BigInsights, Hortonworks
- **Databases:** Cassandra, IBM DB2, Microsoft SQL Server, Microsoft SharePoint, mongoDB, Oracle, MySQL, PostgreSQL, Couchbase, and more
- **Cloud Management:** Chef
- **Containers:** Docker

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, Cloud-enabled
- **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, column-level encryption of sensitive data, such as credit card numbers, social security numbers, and passwords, in multi-vendor database management systems. It 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 provides 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, Cloud-enabled
- **Databases:** Oracle, Microsoft SQL Server, IBM DB2

SAFENET TOKENIZATION: APPLICATION-LEVEL TOKENIZATION

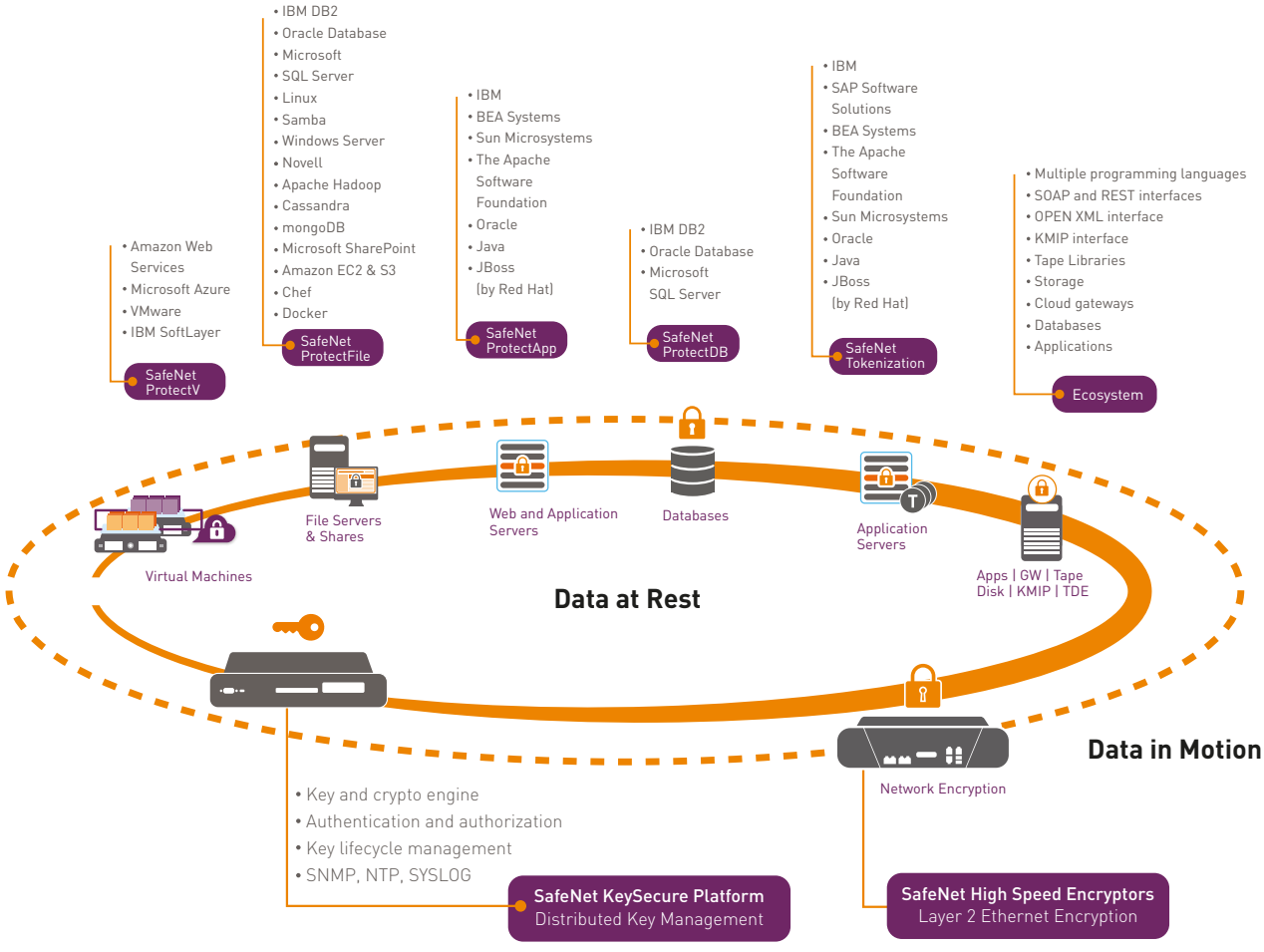
SafeNet Tokenization protects sensitive information by replacing it with a surrogate value that preserves the length and format of the data. The solution can be used to protect primary account numbers (PAN), as well as other sensitive data such as PII and PHI. SafeNet Tokenization also features granular access controls to ensure only authorized users or applications can view protected tokens and data, comprehensive logging and auditing, and requires no changes to applications, databases, or legacy systems.

- **Environments:** On-premises, Cloud-enabled
- **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 HIGH SPEED ENCRYPTORS: NETWORK ENCRYPTION

SafeNet High Speed Encryptors provide proven high-assurance Layer 2 network security for your sensitive data, real-time video and voice, on the move from site to site or multiple sites; data center to data center, back up and disaster recovery; to the last mile, curb or cabinet; on-premises, up to the cloud and back again. As preferred by market leading commercial organizations and governments in over 30 countries, SafeNet High Speed Encryptors are certified to ensure trusted security for Fortune 500 customers across financial institutions, telcos and other commercial organizations. SafeNet High Speed Encryptors provide maximum network performance, with near-zero overhead and microsecond latency, scalable and simple set-and-forget management and low total cost of ownership. True end-to-end, authenticated encryption and state-of-the-art client side key management ensure high-assurance vulnerability protection where your data moves.

SafeNet Data Protection Solutions



The Benefits of a Crypto Foundation

Without a trusted crypto foundation, it is very difficult to manage encryption and maintain security policies. The challenges are compounded when dealing with sensitive data in both physical and virtual datacenters and the cloud. Once a comprehensive crypto foundation supported by products to address the various environments and/or types of data has been implemented an organization can realize a host of advantages and as the organization grows, their data encryption and control solutions can scale with it:

- **Centralized crypto management.** Enterprise-wide encryption policies, cryptographic keys, auditing, logging, and reporting can all be centralized. SafeNet's crypto foundation enables security administrators to define a standard set of criteria, and to mandate a standard set of tools for use wherever encryption is required such as PCI DSS compliance.

- **Standards-based libraries and APIs.** Gemalto's encryption and crytpo management solutions offer a wide range of standard APIs and development libraries to enable easy integration into the organization's existing infrastructure. Using Gemalto's crypto API, security teams can develop an encryption framework, that can be published as a standard that business units and developers can use to secure their data. Gemalto supports the OASIS Key Management Interoperability Protocol, a comprehensive protocol for the communication between enterprise key management systems and encryption systems. Through KMIP standards-based platforms, organizations can simplify key management, ensure regulatory compliance, and reduce operational costs significantly.

- **High availability and redundancy.** Given the central, critical nature of the enterprise crypto management solution, Gemalto solutions enable long term scalability with support for clustering, load balancing, and replication across multiple disaster recovery sites, enabling organizations to ensure critical encryption services always deliver the scalability and availability required.

Conclusion

Gemalto's portfolio of SafeNet encryption and crypto management solutions provide the crypto foundation for delivering encryption across an entire enterprise—centrally and cohesively implementing and managing encryption and key management, from the datacenter to the cloud. Supporting the widest set of technologies and deployment scenarios, Gemalto enables the creation of a centralized cryptographic platform to address the various environments and/or types of data that the organization needs to secure. The Gemalto Crypto Foundation streamlines enterprise wide encryption and key management with unified control, enabling organizations to realize significant benefits in overall security, administrative efficiency, and business agility

The Gemalto crypto foundation enables organizations to realize a host of business 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 readily track and optimize compliance with all relevant security and privacy mandates. 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.** Organizations can leverage proven, repeatable, and documented processes for managing policies and cryptographic keys to minimize upfront costs and ongoing administration efforts.
- **Increased IT and business agility.** By leveraging a cohesive, centrally managed platform, 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, and data is free to move throughout the enterprise to support business objectives—without making compromises in security.

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 safenet.gemalto.com

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free