As sophisticated threats emerge and the risk of data exposure grows, encryption is the critical last line of defense when other security measures fail. Application encryption has become essential as it protects data at the earliest stages of the information lifecycle which helps organizations minimize risk, strengthen security, and meet regulatory and compliance mandates.

**Secure Sensitive Application Data Across Its Lifecycle**

SafeNet ProtectApp provides an interface for key management operations, as well as application-level encryption of sensitive data. The solution can protect both unstructured data types (e.g. Excel and PDF files) and structured data types (e.g. credit card numbers, social security numbers, national ID numbers, passwords). Encryption takes place as soon as data is generated or first processed, and it remains secure across its entire lifecycle no matter how many times it is transferred, backed up, or copied. The solution can be deployed in physical, virtual, and cloud infrastructures to keep data secure as it is migrated from one environment to another—without any modification to existing encryption policies or associated application code.

SafeNet ProtectApp is deployed in tandem with SafeNet KeySecure, a FIPS 140-2 up to Level 3 enterprise key manager, for centralized key and policy management across multiple sites. The solution enables the implementation of granular access controls that separate administrative duties from data and encryption key access. For example, a policy can be applied 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.

**SafeNet ProtectApp Highlights**

- **Transparent, Strong, and Efficient Application Encryption**
  - Protect sensitive data with application-level encryption
  - Securely manage keys centrally in an industry-leading, FIPS-certified enterprise key manager

- **Support for Format Preserving Encryption (FPE)**
  - Flexible key management interfaces
  - Multiple interfaces available for full key management lifecycle

- **Broad Standard and Interface Support**
  - Java, C/C++, .NET
  - XML open interface, KMIP standard
  - Web services, including SOAP and REST

- **Easy Deployment and Management**
  - Deploy in physical, virtual, and public cloud environments
  - Built-in key rotation
  - Customizable sample applications for quick, easy deployment

- **High Performance**
  - Offload cryptographic processing to SafeNet KeySecure
  - Built-in health checking and multi-tiered load balancing

- **Compliance Ready**
  - Ensure separation of duties
  - Track data and key access with auditing and logging tools

![SafeNet ProtectApp and SafeNet KeySecure](image)
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.