

SafeNet ProtectApp

Application-level encryption and key management



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.

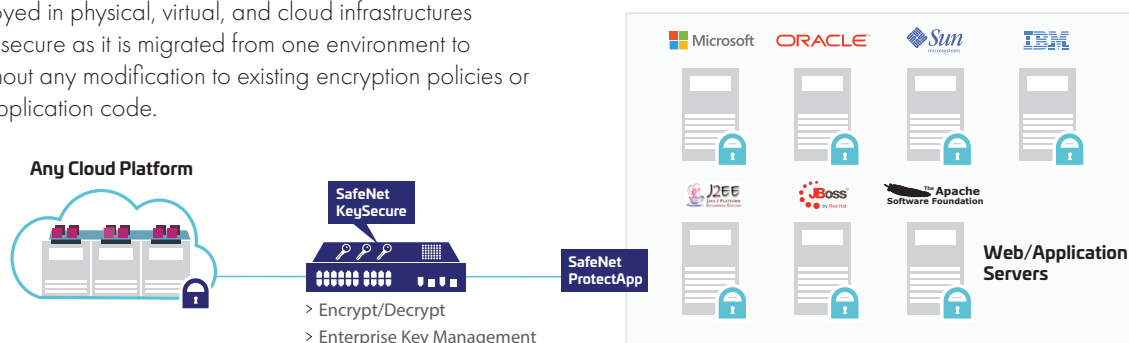
Secure sensitive application data across its lifecycle

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 and SafeNet KeySecure



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

How SafeNet ProtectApp benefits your business

With SafeNet ProtectApp, your organization can enjoy a number of significant benefits:

Strengthen Security and Ensure Compliance

SafeNet ProtectApp enables your organization to maximize security of data in applications running in physical, virtual and cloud data centers. Comprehensive logging and auditing capabilities let you track access to encrypted data and keys so you can effectively address your internal policies and all relevant regulatory mandates—including encrypting personally identifiable information (PII) and credit card information to comply with privacy mandates and the Payment Card Industry Data Security Standard (PCI DSS).

Centralize and Streamline Security Administration

Through its integration with SafeNet KeySecure, SafeNet ProtectApp provides the comprehensive coverage and integration that enables security teams to move away from disparate, point-based encryption deployments. Your teams can centrally manage policies and keys, and, as a result, realize significant improvements in efficiency and productivity.

Leverage the Cloud Securely

SafeNet ProtectApp, together with SafeNet KeySecure, enable your organization to move forward with its cloud and virtualization initiatives—in any cloud provider—so you can fully leverage the business benefits without compromising security. You maintain full control and ownership of your data and encryption keys at all times.

Speed Time to Deployment

With its adherence to open standards, flexible integration support, sample applications, and central management, SafeNet ProtectApp enables streamlined integration and fast deployment.

Optimize Server Performance

By managing processing-intensive cryptographic operations on dedicated encryption appliances, SafeNet KeySecure offloads this workload from application servers, which helps your organization deliver fast responses to users and customers, and fully leverage your existing software and hardware investments.

Native Encryption Ecosystem

SafeNet ProtectApp APIs use open standards whose flexibility lets you join native encryption solutions (e.g. Linux Unified Key Setup (LUKS), MongoDB, Oracle TDE) with SafeNet KeySecure—the industry's leading enterprise key manager—for fully consolidated key management across the organization. Sample code and SDKs make it easy for developers to incorporate encryption and key management into their applications.

Technical specifications

Web Application Servers

- Apache Tomcat, IBM WebSphere, JBoss, Microsoft IIS, Oracle WebLogic, SAP NetWeaver, Sun ONE, and more

Cloud and Virtual Infrastructures

- Works with all major cloud platforms, including AWS, Azure, IBM Cloud, Google and VMware

Development Libraries and APIs

- Java, C/C++, .NET
- XML open interface, KMIP standard
- Web services: SOAP and REST

Encryption Algorithms

- Including 3DES, AES-256, SHA-256, SHA-384, SHA-512, RSA-1024, RSA-2048, RSA-3072, RSA-4096

Supported Platforms for ICAPI Provider

- Red Hat Enterprise Linux 5.4 and above
- Microsoft Windows 2003, 2008 R2, and 7 in both 32-bit and 64-bit

Certificates

- X509, PKCS1, PKCS8, PKCS12
- Export, Import, MonitorSize and Weight