THALES eSECURITY: SECURING YOUR DIGITAL TRANSFORMATION
Enterprises are committing to a digital transformation initiative by embracing new opportunities and building revenue by leveraging all digital technology offers in terms of connectivity, stability and efficiency. While this transformation offers many opportunities and benefits, it also poses significant challenges around data security and ensuring that the data is trusted and reliable.

Only Thales eSecurity has the technology, experience and resources to deliver trust throughout the information landscape so companies can embrace digital transformation while maintaining business agility.

Our data security platform provides encryption, advanced key management, tokenization, authorization, privileged user control and hardware security module (HSM) solutions that protect data in any environment. This is complemented by a professional services team that is expert at helping customers get the most from their investment quickly, with minimal downtime.
40+ Years of securing the world’s most sensitive data

Deep expertise and track record in applied cryptography

9 of the Fortune 10 are customers

80% Protection of the world’s card transactions

Security for 4 of the five largest energy companies

130+ Partnerships with leading technology providers of cloud computing, digital payments and more

Security for 19 of the 20 largest banks

Long-standing history of industry certifications and validation

Protection of the world’s card transactions

Partnerships with leading technology providers of cloud computing, digital payments and more

Common Criteria

FIPS Level 3 Validated

140-2

Long-standing history of industry certifications and validation

Asap

Alliance for Solution and Application Providers
Data security core principles

DATA PROTECTION MUST BE BOTH EFFECTIVE AND EFFICIENT
Great data protection solutions are designed for today’s dynamic organizations and must require minimal human intervention, have minimal impact on performance or data availability and adapt easily as business processes change and scale over time. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and meeting the highest standards of certification for high assurance solutions.

DATA SECURITY IS ALL ABOUT THE DATA
An organization’s most sensitive data requires increasingly stringent protection from loss and from outsider and insider attacks. With today’s highly integrated systems, organizations must know where their data is stored, how and where it moves and which applications use it – then design a protection strategy that follows the data. Thales provides a comprehensive portfolio of data security solutions that can meet your needs for protecting data wherever it resides.

Structured and unstructured data at rest
In motion and in use
Within and across devices
Across processes, platforms and environments
YOUR DATA IS ONLY AS SECURE AS YOUR KEYS

Cryptography protects data effectively only if keys are secure and well managed. From low-volume, infrequently used applications to high-volume, on-demand applications, key management is a critical component of an organization’s ability to protect data from malicious attacks while ensuring that the data is available for use. Thales provides key management and protection designed to meet your specific security requirements.

- High assurance certified key storage
- Centrally managed keys and policies
- Comprehensive API and protocol support
- Role-based management and monitoring

BOTH LOGICAL AND PHYSICAL CONTROLS ARE NEEDED TO PROTECT THE MOST SENSITIVE INFORMATION

With the rise of insider attacks and innovative malware, including advanced persistent threats, organizations can no longer rely on perimeter tools to protect cryptographic processes. Thales eSecurity’s portfolio features certified, tamper-resistant hardware in diverse forms that add a critical layer of protection for sensitive applications and information, limiting access and reducing opportunity for insider attacks.

THE BEST DATA PROTECTION STRATEGIES MINIMIZE COMPLIANCE COST AND COMPLEXITY

Complying with privacy and data protection mandates – including disclosing breaches when they occur – should be a straightforward byproduct of implementing an effective data protection solution and add minimal overhead to an organization’s data security efforts. Thales’ extensive compliance expertise enables us to design solutions that reduce the scope and cost of your compliance efforts while securing the information on which you and your auditors rely.
The data security platform

Thales eSecurity offers powerful technology solutions that feature a complete range of Hardware Security Module, encryption, digital signing, key management, tokenization, access and privileged user control solutions.

- Integrated technology provides advanced data encryption with policy-based access controls for the widest range of servers, applications and environments
- Centralized key management enables organizations to address security policies and compliance mandates across databases, files and big data environments, regardless of asset location – virtual, physical, or cloud
- High scalability with products that can be deployed individually while centralizing management access and oversight
- A single platform, management and infrastructure set for all solutions that reduces the cost and complexity of protecting data
GENERAL PURPOSE HARDWARE SECURITY MODULES

nShield is a family of hardware security modules (HSMs) that protect the cryptographic operations and data of enterprise applications. They provide a certified, hardened, tamper-resistant environment that safeguards cryptographic processing and keys for applications that require a high level of trust. nShield HSMs are FIPS 140-2 Level 2 and Level 3 certified and are available in three form factors:

- nShield Connect: a network-attached appliance for high-performance data center environments
- nShield Solo: a PCIe server-embedded card for high-volume applications
- nShield Edge: a USB-connected model for portable, low-volume and developer applications

All nShield HSMs integrate with the unique Security World architecture, a specialized key management framework, from Thales. With this proven technology, you can combine different nShield HSM models to build a unified ecosystem that delivers scalability, seamless failover and load balancing.

PAYMENT HARDWARE SECURITY MODULES

Thales payment HSMs are used extensively throughout the global payment ecosystem, playing a fundamental security role in supporting user authentication, card authentication and sensitive data protection processes.

Thales payShield 9000 supports payment applications for contact chip, contactless chip and mobile secure elements. The solution addresses evolving standards from EMVCo, PCI SSC, GlobalPlatform and Multos International. The Payment Card Industry Hardware Security Module (PCI HSM) specification defines a set of logical and physical security compliance standards for HSMs specifically for the payments industry. The payShield 9000 HSM from Thales eSecurity was one of the first HSMs to be successfully validated against the PCI HSM standard.

Supporting all major payment applications including technologies such as host card emulation, secure element provisioning, mobile point of sale (POS) and mobile payments security, Thales payment solutions are used in an estimated 80% of payment card transactions worldwide.

KEY MANAGEMENT

Thales key management solutions are a family of products based on FIPS 140-2 certified platforms that help you manage your keys securely and separately from the applications that use them. Customers use our key management products as a complement to their application vendor’s or their own native encryption to gain greater control over their keys using centralized, streamlined interfaces.

- The Vormetric Data Security Manager, available as a virtual or hardware appliance, serves as the foundation for key management for KMIP Clients, Oracle and Microsoft SQL databases using TDE, Key Management as a Service for cloud, bring your own key (BYOK) and vaulting services
- nShield BYOK, based on nShield HSMs, lets customers generate strong keys in their on-premises HSMs and securely export these keys to their cloud applications, whether hosted in Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure or all three, to gain greater control over their keys in the cloud

PKI AND DIGITAL CERTIFICATES

Products and services from Thales can help to ensure the integrity, performance and manageable of your PKI. By securing the process of issuing certificates and proactively managing signing keys, you prevent their loss or theft, thereby creating a high-assurance foundation for digital security. When you add nShield HSMs to your PKI, you are deploying independently certified, tamper-resistant devices that are used to secure some of the most sensitive keys and business processes in the organization—a
By taking advantage of products, expertise and services from Thales, you will be able to operate PKIs confidently.

**CODE SIGNING**

Designed for software vendors of all sizes and for enterprises that develop their own code, the Thales Code Signing Solution is a comprehensive solution that enables you to implement high assurance, high-efficiency code signing processes to protect your software from tampering and bring appropriate governance to your software publishing practices. Combining tamper-resistant nShield HSMs with services from Thales ASG, the Thales Code Signing solution is backed by our extensive expertise in code signing best practices.

**ENCRYPTION**

The Vormetric Data Security Platform can effectively manage data-at-rest security across your entire organization. Built on an extensible infrastructure, the Vormetric Data Security Platform is composed of several products that can be deployed individually, while offering efficient, centralized key and policy management. As a result, your security teams can address your data security policies, compliance mandates and best practices, while reducing administration effort and total cost of ownership.

The platform offers capabilities for protecting and controlling access to databases, files and containers—and can secure assets residing in cloud, virtual, big data and physical environments.

**ADVANCED FILE AND DATABASE ENCRYPTION**

Vormetric Transparent Encryption protects data with file and volume level data-at-rest encryption, access controls and data access audit logging without re-engineering applications, databases or infrastructure. The solution mitigates the risk of insider threat, malware and advanced persistent threats (APTs) with privileged user access controls that limit the scope of damage that stolen or abused admin credentials can be used for. Deployment is simple, scalable and fast, with agents installed above the file system on servers or virtual machines to enforce data security and compliance policies. Vormetric Application Encryption offers APIs to simplify the addition of encryption to applications and Vormetric Batch Data Transformation delivers static data masking and initial encryption or tokenization of existing databases’ sensitive data. Policy and encryption key management are centralized and secured by the Vormetric Data Security Manager for the entire Vormetric product line.

**TOKENIZATION WITH DYNAMIC DATA MASKING**

Vaultless Tokenization with Dynamic Data Masking reduces the cost and effort required to comply with security policies and regulatory mandates such as PCI-DSS by delivering capabilities for database field tokenization and dynamic display security. Now you can efficiently address your objectives for securing and anonymizing sensitive assets—whether they reside in data center, big data, container or cloud environments. Utilized with a simple RESTful API, the solution can be implemented quickly. Virtual appliance form factors enable deployment at cloud providers or on-premises with secure key storage on the Data Security Manager.

**MULTI-CLOUD SECURITY**

Thales eSecurity technologies and solutions can help you fulfill data protection responsibilities as you migrate workloads to multiple cloud providers. We partner with cloud providers to help you protect data in any multi-cloud strategy – public, private or hybrid. Cloud-friendly solutions enable you to:

- Bring your own encryption to Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP) compute instances, or get advanced encryption services from over 30 managed service providers worldwide. Or you can implement Tokenization with Dynamic Data Masking at multiple public cloud providers. Either way, encryption keys are stored safely in the Vormetric Data Security Manager deployed at your favorite cloud provider or on your premises.

- Control encryption keys for cloud-vendor provided encryption with the CipherTrust Cloud Key Manager or you can Bring Your Own Key to AWS, Azure or GCP, to ensure both regulatory compliance and implement best practices for data
The Data Security Partner Program is an ecosystem of global technology organizations and leaders who are committed to architecting solutions to meet digital transformation objectives. Thales partners with leading resellers, system integrators, OEMs, managed service providers and technology companies to meet the data protection needs of security-conscious organizations around the globe.

**THALES CHANNEL PARTNER PROGRAM**

The Thales Channel Partner Program provides resellers with the tools, training, support and resources to ensure successful delivery of leading data protection solutions based on Thales products. With multiple tiers available based on sales targets and business plans, our program is designed to foster teamwork, commitment and success.

**THALES ALLIANCE FOR SOLUTION AND APPLICATION PROVIDERS (ASAP) PROGRAM**

The Thales Alliance for Solution and Application Providers Program is designed to forge valuable technology and business relationships with leading technology vendors. These products have been tested for interoperability and integration so that customers can deploy with confidence and improve their overall data security posture.

**THALES CLOUD PARTNER PROGRAM**

The Thales Cloud Partner Program enables service providers to deliver best-in-class data-centric security services to end customers. The program is available for infrastructure-, platform- and software-as-a-service providers, as well as managed service providers, cloud service providers and hosting service providers.
Thales eSecurity services

Thales eSecurity offers a broad range of market-leading data protection products, related professional data security services and training — all of which are designed to help your organization safeguard its most sensitive information and business processes while complying with regulations and industry mandates.

Drawing on the company’s more than 40 years of global experience protecting data for enterprises and governments around the globe, our independently certified hardware and software products deliver an ideal blend of high assurance and operational efficiency—so you never have to make tough tradeoffs between security, performance and agility. Our global technical support and customer service team provide a world class service, with expert support engineers available to resolve technical and product related queries. Complementary services delivered by data protection experts in the Thales Advanced Solutions Group (ASG) can accelerate deployments, increase your confidence, improve your knowledge of best practices and maximize return on your investment in data protection solutions.

PKI PROFESSIONAL SERVICES
Design, deploy and manage world-class PKIs.

CUSTOM CRYPTOGRAPHIC SOLUTIONS
Leverage our knowledge to protect your customers.

PRODUCT DEVELOPMENT
Complete important data protection projects quickly and correctly.

TRAINING & CERTIFICATION
Learn security best practices.
About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn’t just reduce risk, it’s an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization’s digital transformation. Thales eSecurity is part of Thales Group.