

# Channel Partner Playbook

## Data Protection Portfolio





# Thales Cloud Protection and Licensing Story

Today's enterprises depend on the cloud, data and software to keep pace with the cost of doing business in a world that is rapidly digitally transforming. However, they are concerned about business critical and sensitive data being stolen by adversaries such as competitors or cyber criminals. In spite of all their investments in perimeter and endpoint security data breaches continue to occur on a weekly basis. When all else fails, data security has become the last line of defense.

That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive data at rest in on-premises data centers and in public/private clouds, and data-in-motion across wide-area networks. Our solutions enable organizations to migrate to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

We are the worldwide leader in data protection, providing everything an organization needs to protect and manage its data, identities and intellectual property with comprehensive data discovery and classification, data encryption, tokenization, advanced key management, authentication and access management. Whether it's securing the cloud, digital payments, blockchain or the Internet of Things, security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation.

# Contents

4	<b>The people we all rely on to make the world go round – they rely on Thales</b>
6	<b>Providing a safer, more secure world powered by the cloud, data and software</b>
7	<b>Thales Data Protection Portfolio</b>
9	<b>Buyers personas</b>
10	<b>How to Win</b>
10	<b>Ask these questions!</b>
11	<b>Vormetric Data Security Manager</b>
12	<b>Vormetric Transparent Encryption</b>
13	<b>Vormetric Tokenization and Dynamic Data Masking</b>
14	<b>Vormetric Application Layer Encryption</b>
15	<b>Vormetric Enterprise Key Management</b>
16	<b>CipherTrust Cloud Key Manager</b>
17	<b>Protecting Data in Motion</b>
18	<b>Hardware Security Modules</b>
19	<b>General Purpose HSM</b>
19	<b>Thales Luna Network HSM</b>
20	<b>Thales Luna PCIe HSM</b>
21	<b>Thales Luna USB HSM</b>
21	<b>Thales Crypto Command Center</b>
22	<b>Thales ProtectServer PCIe HSM</b>
23	<b>Thales Data Protection On Demand (DPoD)</b>
24	<b>payShield 10K</b>
25	<b>payShield Manager</b>
25	<b>payShield Monitor</b>
25	<b>About Thales</b>

# The people we all rely on to make the world go round – they rely on Thales



10 largest banks in the world



5 largest software companies in the world



10 largest retailers in the world



10 largest healthcare companies in the world



5 largest cloud service providers in the world



10 of the largest manufacturers in the world

Today's enterprises depend on the cloud, data and software in order to be confident in decisive moments.



# What will be your decisive moment to protect your data and software?

Digital transformation is reshaping industries as more and more organizations look to build their businesses using the cloud, data and software. The success of these transformations will ultimately depend on whether these digital services, identities and transactions can be secured and trusted.

At Thales, we are at the heart of making this new digital world possible. As the worldwide leader in digital security, we protect more data, identities, software and transactions than any other company and enable tens of thousands of businesses and organizations to deliver trusted digital services to billions of individuals around the world.



## Cloud Security

---

Confidence in data security is essential, whether it's accessing cloud services or storing data across multiple cloud environments. You can rely on Thales to deliver simple, secure access and encryption solutions to protect sensitive data in any cloud. **How will you secure your data in the cloud?**



## Data Encryption & Key Management

---

Securing sensitive data is a priority for every organization. Whether your data is at rest, in motion, or in use, you can rely on Thales to enable the most effective encryption strategies for your enterprise environments. **Does your enterprise have an encryption strategy?**



## Access Management & Authentication

---

Moving applications to the cloud brings not only increased risks of data breaches but also the challenges of simplifying access for users and enabling compliance. Regardless of the size of your business, you can rely on Thales to deliver secure, trusted access to all cloud services. **Do you have secure access to all of your cloud services?**



## Compliance & Data Privacy

---

Data security regulations present an increasingly complex challenge for global organizations. Wherever you operate and whatever the regulation, you can rely on Thales to help you achieve and maintain compliance, improving your security and managing your risk. **Is your business ready for today's data compliance challenge?**



## Software Licensing & Protection

---

Software is crucial for business performance and new revenue opportunities. As your company shifts from hardware to a software-based business, you can rely on Thales to generate new revenue streams, improve operational efficiency and gain valuable insights from your software. **Can you deliver software the way your customers want to consume it?**

# Providing a safer, more secure world powered by the cloud, data and software

## Data protection against increasing threats

According to the Thales Data Threat Report, 60 percent of organizations have been breached sometime in their history. This is increasingly serious when nearly all organizations will use sensitive data in digitally transformative technologies. However, less than 30% of companies have deployed encryption to protect data in digital transformation environments. Thales helps businesses and organizations defend their data in a digital world where there is no defined perimeter with advanced encryption, key management and tokenization solutions.

## Trusted access in a zero trust world

Traditional security models operate on the assumption that everything inside corporate networks can be trusted. However, given the increasing adoption of cloud services and sophistication of cyberattacks, new security approaches are needed to ensure the individuals accessing cloud services and corporate resources can be trusted, verified and deliver on compliance mandates. Our access management solutions help organizations provide secure, trusted access to cloud services and applications with user friendly single sign-on and robust multi-factor authentication.

## Security for a cloud-first world

The cloud gives organizations the agility and efficiency to instantly introduce new services, expand operations, and enter new markets. But the lack of physical control of infrastructure brings a whole host of data security issues, including privileged user abuse, data leakage, regulatory requirements, and many more. Our solutions help organizations secure their cloud transformation, reduce breach exposure and achieve compliance with encryption and key management solutions that keep you in control of your data in any cloud while also providing simple, secure access to cloud services with integrated access management, authentication and single sign-on.

## Enabling a world powered by software

Just as important as the cloud, software is increasingly crucial for business performance and new revenue opportunities. This is especially true for businesses that are shifting away from hardware as their main revenue driver in favor of software. Our software licensing and monetization solutions help manufactures, device makers and software companies license, deliver and protect their software in order to generate new revenue streams, improve operational efficiency, increase customer satisfaction and gain valuable business insights.

## Security that integrates with your technology ecosystem

With one of the industry's largest data protection technology ecosystems, Thales solutions integrate with the most widely used technologies to protect and secure access to your mission-critical applications and data. Through the Thales partner program, we have established partnerships with more than 500 global technology organizations who are committed to architecting solutions to meet secure cloud and digital transformation initiatives. Thales partners with leading resellers, system integrators, distributors, managed service providers and technology companies to meet the data protection and compliance needs of the most security-conscious organizations around the world.





# Thales Data Protection Portfolio

As security breaches continue with alarming regularity and compliance mandates get more stringent, companies need to protect sensitive data in both on-premises and cloud environments.

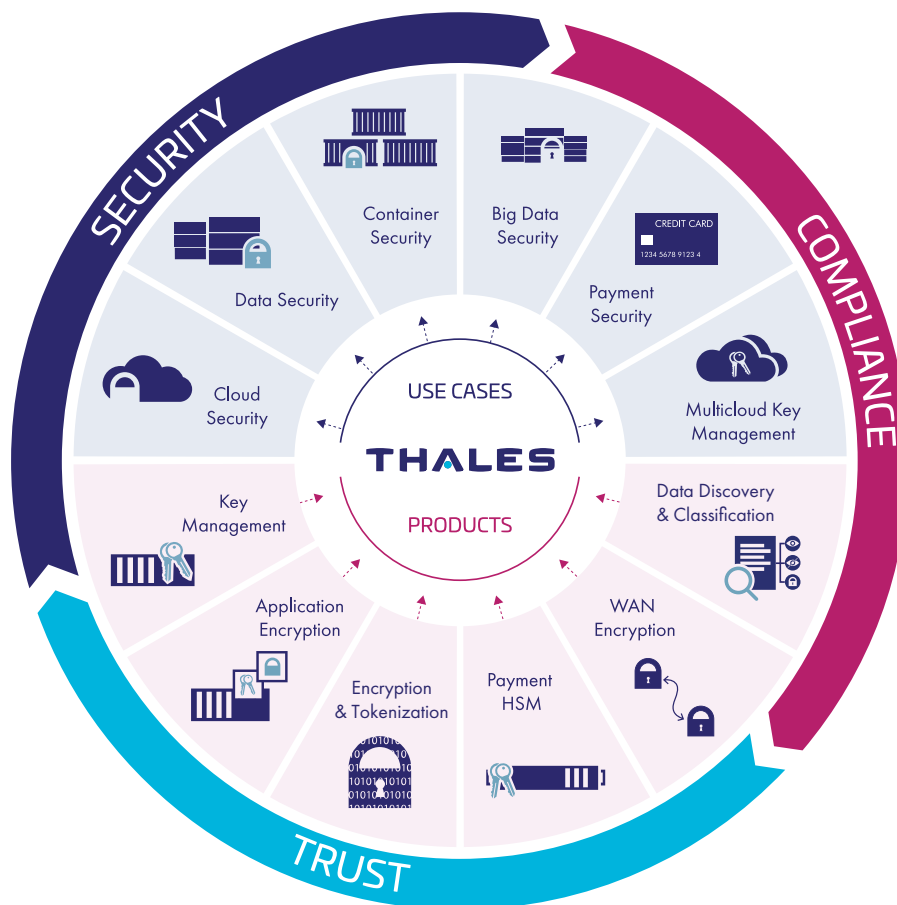
The industry leading portfolio of data protection solutions from Thales allows you to manage data-at-rest and data-in-motion security across the entire IT ecosystem, lowering costs and improving operational efficiencies.

Thales offers advanced data-at-rest products which include data encryption, key management, and tokenization capabilities that enable customers to protect sensitive data wherever it resides - in file servers, databases, applications, on-premises or in cloud and virtual environments.

Our data-in-motion products include high speed network encryptors for your sensitive data, real-time video and voice, as they move from data center to data center or site-to-site, or to back up and disaster recovery sites.

Thales is the market leader in hardware security modules that protect the crypto infrastructure of the most security conscious organizations in the world and act as trust anchors by securely managing, processing, and storing crypto keys inside a hardened, tamper-resistant device available on-premises, in the cloud as a service or as a hybrid solution.

The most trusted brands rely on Thales to help them protect and secure access to their most sensitive information. Whether you're protecting customer PII data, want to leverage hybrid clouds without sacrificing control of your data, or looking to optimize meeting data security and privacy regulations, the Thales Data Protection portfolio has the solutions and services that your organization can trust.



## Thales Data Protection Advantages

- Centralized data-at-rest and data-in-motion encryption and key management policies
- Manage keys for Thales and third-party encryption products to enable bring your own key or encryption use cases
- Consistent security and compliance across physical, virtual, cloud and big data environments
- Single vendor that offers the largest breadth and depth of data protection products
- Only true encryption, key protection and key management solution for hybrid cloud and multi-cloud environments
- Support for emerging technologies including quantum, IoT, Blockchain, 5G and more
- Global support with presence in 68 countries around the world

## Key Benefits

- Strengthen Security and Compliance Thales enables you to address the demands of a range of security and privacy mandates, including the electronic IDentification, Authentication and trust Services (eIDAS) regulation, Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and regional data protection and privacy laws.
- Optimize Staff and Resource Efficiency Our products make administration simple and efficient, offering intuitive web-based interfaces and a variety of application programming interfaces (APIs) including support for REST, Java, .Net, and C. This portfolio enables you to apply key management, data-at-rest and data-in-motion security policies quickly and consistently, while optimizing staff efficiency and productivity.
- Reduce Total Cost of Ownership Overall, the Thales data protection portfolio delivers a comprehensive set of data security products and solutions that easily scale, expand into new use cases, and have a proven track record of securing new technologies. With Thales, you can future proof your data protection investments while reducing operational costs.

## Protecting Data at Rest

The Vormetric Data Security Platform is composed of an integrated suite of products that protect data-at-rest. The platform is built on a common, extensible infrastructure with efficient, centralized key and policy management. It offers capabilities for protecting data in files, databases and containers, securing sensitive assets residing in cloud, virtual and physical environments.

The Vormetric Data Security Platform key attributes:

- Lower total cost of ownership. The Vormetric Data Security Platform makes it simpler and less costly to protect data at rest
- Maximize staff and resource efficiency. The Vormetric Data Security Platform makes administration simple and efficient
- Strengthen data security and compliance. Moving security close to the data is more effective because it minimizes the potential for any surreptitious access

The platform includes:

### Data Security Manager

Vormetric Data Security Manager (DSM) provides the centralized management environment for all Vormetric Data Security Platform products offering policy control as well as secure generation, management and storage of encryption keys. The platform includes a web-based console, CLI, SOAP and REST APIs, and is available up to FIPS 140-2 Level 3 and Common Criteria certified virtual and physical appliances.

### Transparent Encryption

Vormetric Transparent Encryption (VTE) is a set of software agents that run on servers to protect data in files, volumes or databases on-premises, and in hybrid cloud environments. It features hardware accelerated encryption, least-privilege access controls and data access audit logging across data center, cloud and hybrid deployments. It offers extensions for Container Security, Live Data Transformation, Transparent Encryption for Efficient Storage and SAP HANA. VTE also provides integration with security information and event management (SIEM) systems, with pre-packaged dashboards and reports that streamline compliance reporting and speed threat detection.

### Tokenization and Dynamic Data Masking

Vormetric Tokenization Server makes it easy to add format-preserving tokenization to protect sensitive fields in databases and policy-based dynamic data masking for display security. Static data masking and bulk encryption or tokenization is made quick and simple with Vormetric Batch Data Transformation.

### Application Layer Encryption

Vormetric Application Encryption streamlines the process of adding AES and format-preserving encryption (FPE) into existing applications. It offers standards-based APIs that can be used to perform high-performance cryptographic and key management operations.

### Enterprise Key Management

Vormetric Key Manager provides unified key management and secure key storage for third-party Transparent Data Encryption (TDE) and KMIP-compliant clients as well as securely storing certificates.









## Cloud Key Management

CipherTrust Cloud Key Manager manages Bring Your Own Keys (BYOK) and provider created keys for Salesforce, Microsoft Azure and AWS while addressing enterprise needs to meet compliance and best practices for managing encryption

key life cycles outside of their native environments, without the need for enterprises to become cryptographic experts.

# Buyers personas

	 <b>Overall Approver</b>	 <b>Decision Maker</b>	 <b>Implementer</b>	 <b>Recommender</b>
	<b>Business Buyer</b>	<b>Technical Buyer</b>	<b>End User</b>	<b>Key Influencer</b>
<b>Responsible for</b>	Grow revenue, shareholder value, budget control, final approval	IT/Security strategy, technology roadmap, fund allocation, vendor selection	Managing data security operations, evaluates data protection solutions – important stakeholder in making buying decision.	Evaluating and testing data protection and key management solutions. Key influencer in the decision making process.
<b>Drivers</b>	Company's reputation, comply with industry regulations, protect company/customer data	Improve Security, Protect Data, Simplify operations, Reduce IT Cost	Reduce operational complexity, simplify security management and cloud migration, streamline compliance	Ease of deployment/migration, integration and testing with existing applications and legacy data stores.
<b>Risks / Concerns</b>	Business Risks, Data Breaches, Penalties associated with compliance	Sensitive data exposure, operational complexity, compliance audit delays	Management complexity, lack of centralized visibility and control, limited security skills	Lack of centralized management, monitoring, reporting, visibility of sensitive data. Complexity of integration with current data stores.
<b>Considerations</b>	<ul style="list-style-type: none"> <li>Need strong ROI and TCO</li> <li>Buy from vendors with wide inside support</li> <li>Relies heavily on decision makers and influencers</li> </ul>	<ul style="list-style-type: none"> <li>Avoid product silos, technology gaps</li> <li>Select right vendors who reduce complexity, simplify operations</li> <li>Streamline data privacy compliance</li> </ul>	<ul style="list-style-type: none"> <li>Centralized visibility and management across on-premises and cloud</li> <li>Breadth of data protection across data stores</li> <li>Simplify multi-cloud data protection</li> </ul>	<ul style="list-style-type: none"> <li>Support of IT ecosystem at customer site</li> <li>Developer friendly APIs for test &amp; dev</li> <li>Breadth of data protection across data stores</li> </ul>
<b>How our solution helps</b>	<ul style="list-style-type: none"> <li>Reduces business risks with comprehensive data protection</li> <li>Better ROI and operational efficiency with centralized management</li> <li>Coverage across multiple global and regional compliance mandates</li> </ul>	<ul style="list-style-type: none"> <li>Provides comprehensive data protection to reduce complexity</li> <li>Centralized management across on-premises and multi-cloud providers</li> <li>Simplifies compliance with better auditing, monitoring and reporting</li> </ul>	<ul style="list-style-type: none"> <li>Provides centralized key management and data protection across all data stores</li> <li>Unified console to discover sensitive data and protect it from a single pane of glass</li> <li>Simplifies data protection and key management across multiple cloud service providers</li> </ul>	<ul style="list-style-type: none"> <li>Centralized visibility: provides discovery, classification protection, monitoring and alerting capabilities.</li> <li>Simplifies data protection and key management across multiple data stores</li> <li>REST APIs for easy application integration and automating test and dev</li> </ul>

# How to Win

## Business drivers and specific goals

- What are they trying to achieve – business and security objectives, cloud strategy, scalability requirements and budget?
- Do they have to meet any data privacy and industry specific compliance regulations?
- What does their current data storage ecosystem consist of, where is their data located across on-prem. and cloud?
- How are they currently discovering and protecting sensitive data across their enterprise?

Ask these questions!

## Why they should trust Thales

- Market-leading key management, data protection and HSM solutions across financial, healthcare, and gov. sectors
- New Data Discovery solution integrated with data protection offers simplified security and accelerated compliance
- Largest partner ecosystem of storage, server and cloud service provider integrations
- 19 billion Euros revenue, 1+ billion Euros R&D, global presence in 68 countries

## Solutions that meet their needs

- Demonstrate appropriate solutions and how they meet customer's needs
- Best practices for holistic data protection and compliance
- Value Proposition of the solution - benefits, customers, compliance, TCO, etc.
- Differentiators as compared to the key competitors





# Vormetric Data Security Manager

The Vormetric Data Security Manager (DSM) centralizes management and policy for all Vormetric Data Security Platform products. The DSM enables organizations to efficiently address compliance requirements, regulatory mandates and industry best practices, and to adapt as deployments and requirements evolve. The DSM and the products it manages are integrated with user and group identity management systems such as LDAP, Active Directory, local user databases, Hadoop and container environments— offering best-practice management of security policies and deployments.

## Value proposition

- Enables centralized management of data security policies and key management, simplifying training, deployment and operations
- Available in multiple form factors and FIPS 140-2 levels 1-3 validated appliances. Deploy virtual appliances on-premises, in private and public clouds or select high-assurance physical appliances with the data security management tool
- Provision and manage encryption keys for all Vormetric Data Security platform products from Thales, as well as KMIP and other third-party encryption keys and digital certificates

## Smart questions

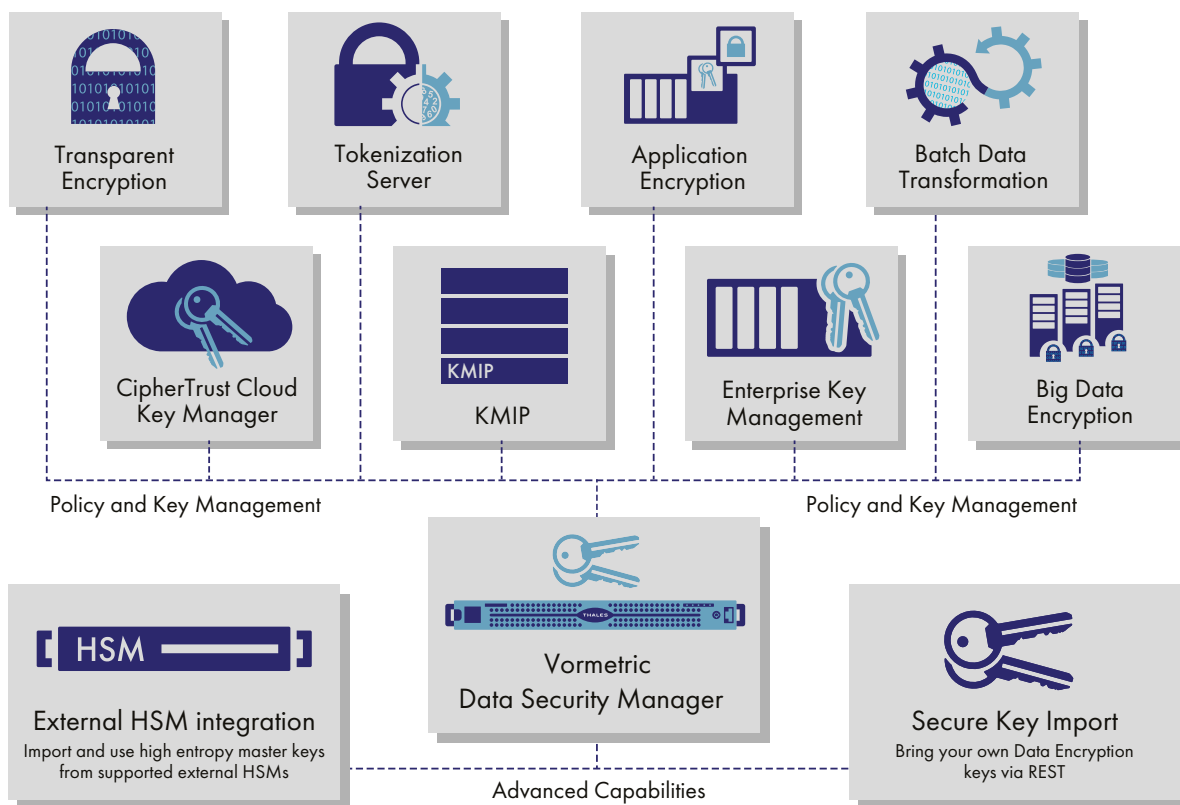
- How are you encrypting sensitive data and managing access control across all your data repositories on file-servers, databases, applications, virtual machines and across cloud providers?
- Do you have a centralized key management solution for managing encryption keys and access control across all these data repositories?
- Does your key management solution come with a built-in HSM or integrated with a network attached HSM for securely storing encryption keys for highest level of assurance?



[Click here to access the Vormetric Data Security Platform brochure](#)



[Click here to access the Vormetric Data Security Platform customer presentation](#)



# Vormetric Transparent Encryption

Vormetric Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging that helps organizations meet compliance reporting and best practice requirements for protecting data, wherever it resides.

This solution's transparent approach protects structured databases, unstructured files, and linked cloud storage accessible from systems on-premises, across multiple cloud environments, and even within big data and container implementations. Designed to meet data security requirements with minimal disruption, effort, and cost, implementation is seamless – keeping both business and operational processes working without changes even during deployment and roll out.

## Value proposition

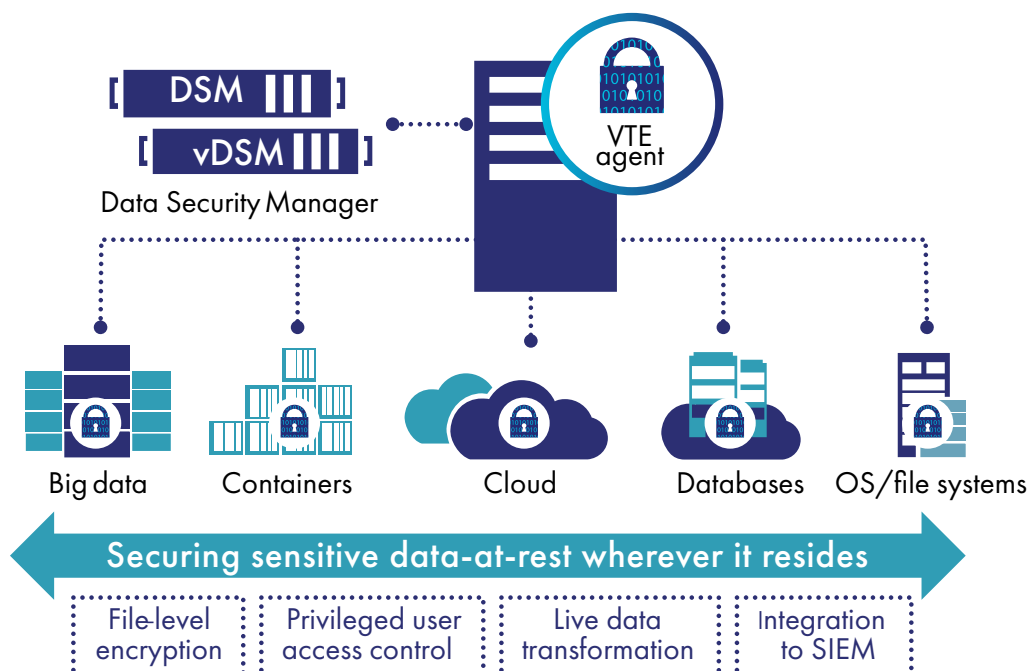
- Achieve compliance with data protection mandates by securing data-at-rest with encryption, access controls and data access audit logging wherever it resides – across multiple clouds, on-premises or within big data and container environments
- Realize data security faster without changing business processes using encryption that is transparent to users, applications and infrastructure
- Simplify data security administration with centralized key management, encryption, and access policies that reach across cloud and data center environments
- Enable administrators to work as usual, but never be exposed to sensitive data with strong privileged user access controls
- Minimize deployment and maintenance downtime by encrypting and re-keying while data is in use with the Live Data Transformation option
- Extend encryption and access controls to big data, container and SAP HANA environments with optional components and licenses

## Smart questions

- What initiatives do you have around data security, encryption and key management?
- Who is responsible for securing your – cloud, big data and container initiatives? What about your databases?
- What strategy do you have at the enterprise level for securing the data target in a breach?



Click [here](#) to access the Vormetric Transparent Encryption product brief





# Vormetric Tokenization and Dynamic Data Masking

Vormetric Tokenization with Dynamic Data Masking reduces the cost and effort required to comply with security policies and regulatory mandates such as the European Union’s Global Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS). You can secure and anonymize sensitive assets—whether they reside in the data center, big data environments or the cloud.

## Value proposition

- Reduce PCI DSS compliance effort and scope by minimizing servers requiring audit and control
- Achieve compliance with privacy mandates by irreversibly masking personal information
- Fully leverage cloud, big data and outsourced models – Replacing sensitive data with tokens enables use without risk or compliance overhead
- Easily enable call center and other applications
- Minimize data security staff training and overhead with a common platform used for other data security applications

## Smart questions

- What data is in your databases that would be critical if taken? How are you protecting those field values now?
- Explain how users access critical field values? Do all users need full access or would partial value be of benefit?
- Do you have a QA, Test or Dev environment that needs to work with a production database, but shouldn’t be exposed to sensitive information? Are you using outside contractors for any of this work?

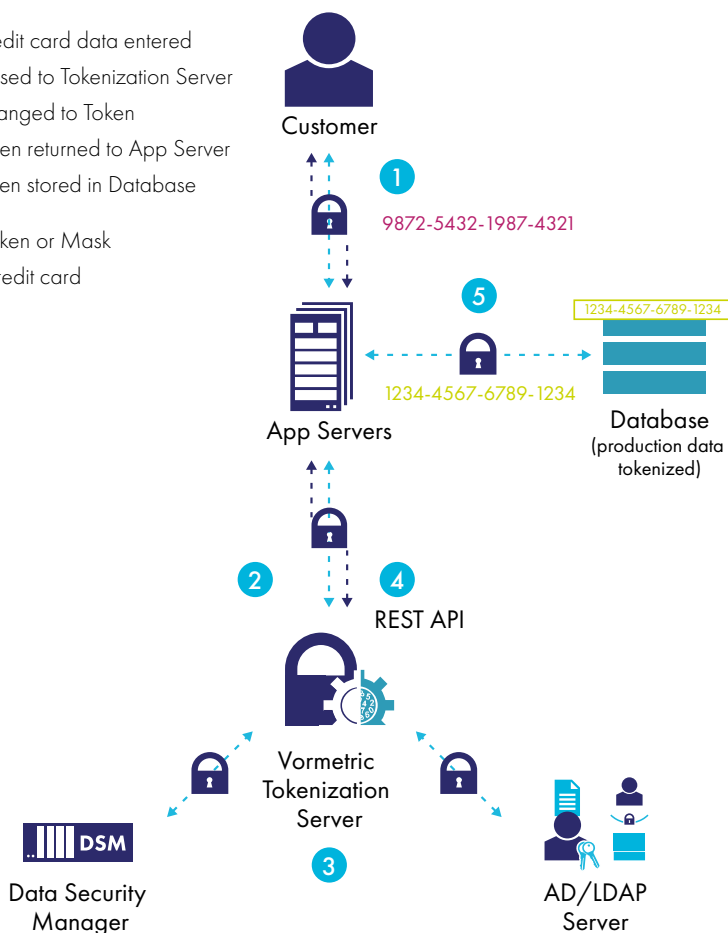


Click [here](#) to access the Vormetric Tokenization with Dynamic Data Masking solution brief

## Typical Tokenization Workflow

1. Credit card data entered
2. Passed to Tokenization Server
3. Changed to Token
4. Token returned to App Server
5. Token stored in Database

- Token or Mask
- Credit card



# Vormetric Application Layer Encryption

Vormetric Application Encryption delivers key management, signing, and encryption services enabling comprehensive protection of files, database fields, big data selections, or data in infrastructure as a service (IaaS) environments. The solution is FIPS 140-2 Level-1 certified, based on the PKCS#11 standard and fully documented with a range of practical, use-case based extensions to the standard. Vormetric Application Encryption accelerates development of customized data security solutions.

## Value proposition

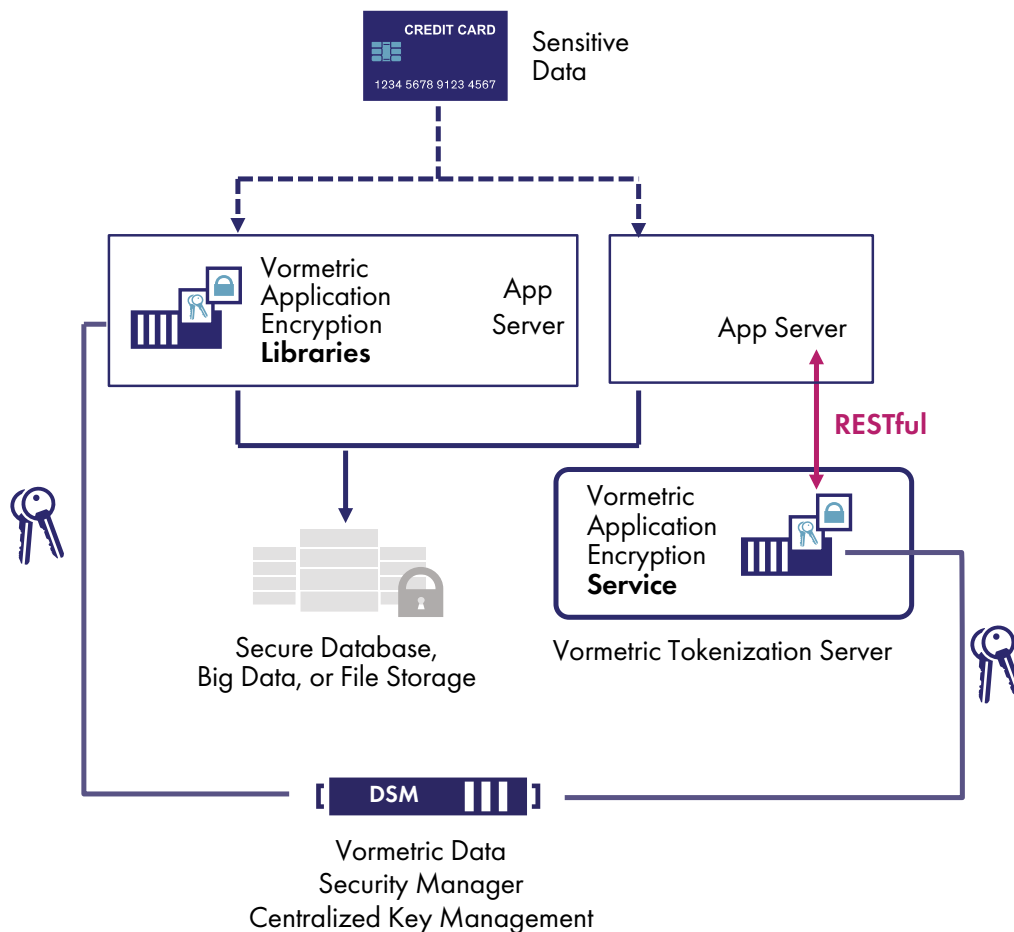
- Fast creation of encryption and key management applications
- Streamline PKCS#11-standard application-level security with simple tools to add key management and encryption to application data flows
- Secure specific fields, protecting sensitive data before it is stored in database, big data or cloud environments
- Centralize key management to secure data from compromised database or cloud administrator, hackers, and subpoenas
- Software development your way: use either RESTful API's or a secure development and runtime environment with high performing PKCS#11 libraries

## Smart questions

- How are your software developers protecting sensitive data using encryption or tokenization in applications today?
- How are your developers securing data in Extract-Translate-Load(ETL) tools, which needs a way to selectively protect data before it gets stored in data repositories?
- Do you have access to PKCS#11 libraries or REST APIs that connects your applications and ETL tools to a centralized key-management and encryption platform?



Click [here](#) to access the Vormetric Application Encryption Architecture whitepaper



**Vormetric Application Encryption Customer Choice:  
Libraries or RESTful**



# Vormetric Enterprise Key Management

With Vormetric Key Management, you can centrally manage keys from all Vormetric Data Security Platform products, and securely store and inventory keys and certificates for third-party devices—including IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE and KMIP-compliant encryption products. Consolidating key management fosters consistent policy implementation across multiple systems and reduces training and maintenance costs.

## Value proposition

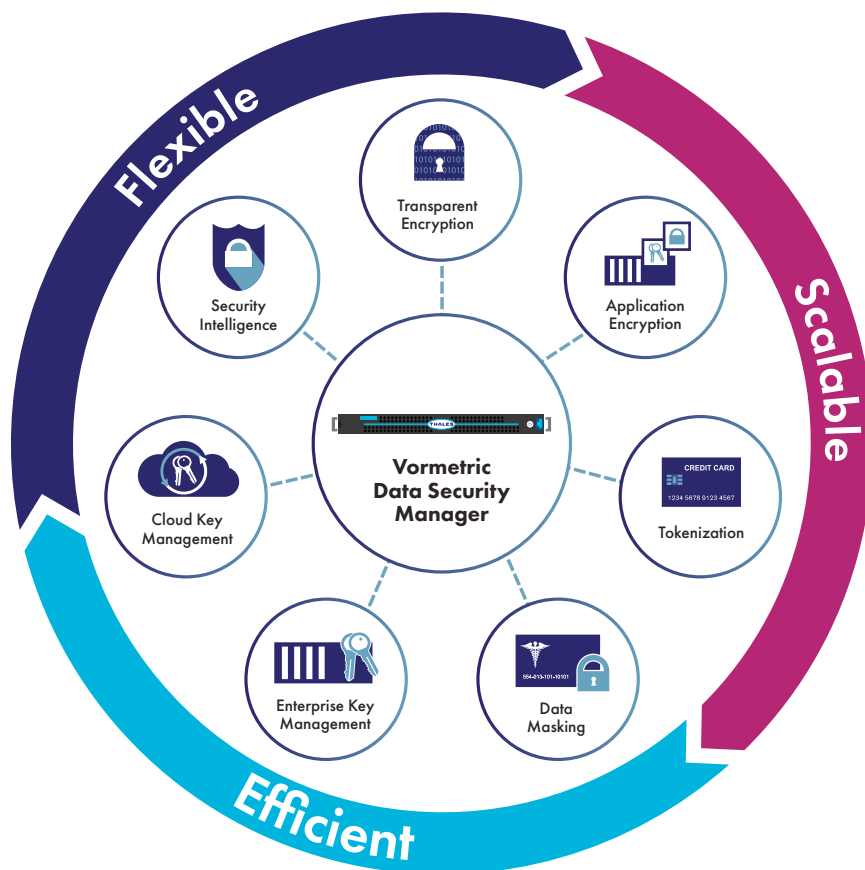
- Simplify key management – Consolidate enterprise encryption key management and certificate storage solutions
- FIPS 140-2 certified – The Vormetric Data Security Manager is FIPS 140-2 certified
- Transparent Database Encryption (TDE) – Consolidate encryption key management for Oracle and Microsoft SQL Server
- Standard API Support – Leverage KMIP APIs for programmatic encryption key management and bulk key vaulting
- Reduce downtime – High availability and proactive notifications of certificate and encryption key expiration reduces application and user downtime
- Centralize reporting – Generate consolidated reports for compliance and simplified auditing of encryption key and certificate usage
- Multi-tenant operations – Role-based administration for compartmentalized management of data security policies, data encryption keys, and audit logs

## Smart questions

- Do you use Microsoft SQL or Oracle Transparent Database Encryption?
- Do you use any storage arrays that offer KMIP-based encryption key management?
- Do you have a need for centralized management of encryption keys or certificates?



Click [here](#) to access the Vormetric Enterprise Key Management white paper



# CipherTrust Cloud Key Manager

For virtually every organization today, the adoption of multiple cloud services continues to expand—and so does the use of encryption. As the proliferation of encryption continues, so do the number of keys, and the potential risks. With the CipherTrust Cloud Key Manager, your organization can establish strong controls over encryption keys and policies for data encrypted by cloud services.

CipherTrust Cloud Key Manager supports a growing list of infrastructure-, platform- and software as a service (IaaS, PaaS and SaaS) providers. SaaS solutions include Microsoft Office365, Salesforce.com and Salesforce Sandbox. Supported IaaS/PaaS solutions include Microsoft Azure, Microsoft Azure Germany and China National Clouds, Microsoft Azure Stack, and Amazon Web Services.

## Value proposition

- Leverage the value of “Bring Your Own Key” services with full-lifecycle cloud encryption key management
- Comply with the most stringent data protection mandates with up to FIPS 140–2 Level 3 validated key origination and storage
- Gain higher IT efficiency with centralized key management across multiple cloud environments, automated key rotation and key expiration management

## Smart questions

- How many cloud services do you use to run your business? Do you have a single scalable data protection platform across cloud services? What about on-premises?
- Do you use encryption provided by cloud platforms? Where are the keys stored?
- Do you need subpoena-proof cloud encryption?
- How do you manage multiple BYOK services? Do you have a flexible and scalable solution for key lifecycle management?



**Azure**      **aws**


**Office 365**      **salesforce shield**




**CipherTrust Cloud Key Manager**

Enhanced Security	IT Efficiency
<ul style="list-style-type: none"><li>• Key control</li><li>• FIPS 140-2 assurance</li><li>• Visibility for compliance</li></ul>	<ul style="list-style-type: none"><li>• Key lifecycle management</li><li>• Automated key rotation</li><li>• Single pane of glass</li></ul>

Multi-Cloud *Bring Your Own Key* Management

 [Click here to access the CipherTrust Cloud Key Manager product brief](#)

 [Click here to access the Multicloud Security Partner sales guide](#)





# Protecting Data in Motion

Thales offers High Speed Encryptors (HSEs) that provide network independent data-in-motion encryption (Layers 2,3 and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our HSE solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception — all at an affordable cost and without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps, with platforms ranging from single to multi-port appliances.

## CN Series

The CN series is a hardened physical network appliance that delivers network layer independent (Layers 2, 3 and 4) data-in-motion encryption. These hardware encryptors are certified for FIPS 140-2 Level 3 and Common Criteria EAL 2 and 4+.

### CN6000 Series

The CN6000 Series encryptors offer variable-speed licenses from 100 Mbps to 10 Gbps. The CN6140 has a multi-port design that makes this encryptor variable, with speed licenses up to 40 Gbps (4x10 Gbps), highly flexible and cost effective.

### Value proposition

- 1 Gbps-10 Gbps Ethernet Encryptor
- Certified to highest commercial standards
- Rack-mountable, fully redundant robust design
- Ideal for private networks and data center interconnects

### CN9000 Series

Delivering 100,000,000,000 bits per second of high assurance and secure encrypted data, the CN9000 Series provides mega data security (100 Gbps), with the lowest latency in the industry (<2µs)

### Value proposition

- First commercial certified 100 Gbps encryptors
- Only multipoint 100G Encryptor on market
- Fully interoperable with CN product family
- Designed for next gen data centers and core networks

### CN4000 Series

The CN4000 Encryptors are versatile and compact, offering 10 Mbps-1 Gbps encryption in a small-form factor (SFF) chassis. The CN4000 series is ideal for branch and remote locations, offering cost effective, high-performance

encryption, without comprising network performance.

### Value proposition

- 10 Mbps-1 Gbps Ethernet Encryptor
- Certified, low-cost, high-performance
- Small form factor ideal for remote locations

## CV Series

The CV series is a hardened virtual appliance that delivers robust encryption for data-in-motion across high speed carrier WANs and SD-WAN links, using Network Function Virtualization (NFV).

### CV1000 Series

The CV1000, the first hardened virtual encryptor, is instantly scalable and may be deployed rapidly across hundreds of network links, providing robust encryption protection for data-in-motion. The Thales Virtual Encryptor CV1000 is a Virtual Network Function (VNF) that delivers an agile network and reduces capital expenditure requirements. Ideal for organizations that are virtualizing network functions and taking advantage of Software Defined Networking (SDN).

### Value proposition

- Hardened virtual appliance
- KeySecure integration
- Supports Transport Independent Mode (TIM)
- Ideal for Software Defined Networks (SDN) and Server-to-Server communications

### Target customers

Organizations with:

- Data Center Interconnect
- Branch Offices/Remote Locations
- Disaster Recovery Sites
- Remote Data Centers
- Cloud Services

## Smart questions

- **Are you encrypting your network?**
  - Yes - What are you using?
  - Considering - Are you considering encrypting at Layer 2?
  - No - Why? Are you aware of the risks and latest breaches?
- **High-level topics to start the HSE conversation**
  - Data Links – Everyone has them. Where are the big pipes? 1G and above
  - Encryption – Everyone knows they need it
  - Do they have a L2 Encryption strategy?
  - Privacy – Who is listening in?



Click [here](#) to access the High Speed Encryptors for Education solution brief

# Hardware Security Modules

Thales offers the industry leading product family of hardware security modules (HSMs), which are the highest performing, most secure and easiest to integrate in the market today. They act as trust anchors to protect the master keys that encrypt your data and digital identities in a high assurance FIPS 140-2 Level 3-certified, tamper-resistant appliance. Thales offers the following types of purpose-built HSMs:

## General Purpose HSM

Luna HSMs come in several form-factors – a network attached appliance, an embedded PCI module, and a portable USB appliance. They can be easily integrated with a wide-range of applications to accelerate general cryptographic operations, secure crypto key life cycles and act as a root of trust for your entire crypto infrastructure. Crypto Command Center is available to centrally monitor and manage multiple Luna HSM crypto resources on-premises, virtual and hybrid cloud environments.

## Cloud HSM

Data Protection On Demand (DPoD) is a cloud-based platform that provides a wide range of Cloud HSM and key management services through a simple on-line marketplace. With DPoD, security is made simpler, more cost effective and easier to manage because there is no hardware to buy, deploy and maintain. Just click and deploy the protection you need, provision services, add security policies and get usage reporting in minutes.

## Payment HSM

payShield 10K delivers a suite of payment security functionality including transaction processing, sensitive data protection, payment credential issuing, mobile card acceptance and payment tokenization. It is used throughout the global payment ecosystem by issuers, service providers, acquirers, processors and payment networks. The payShield 10K has PCI HSM v3 and FIPS 140-2 Level 3 certifications.



# General Purpose HSM

## Smart Questions

- Do you have a data security strategy? How does data encryption form part of that strategy?
- What data encryption do you currently deploy and what does compliance mandates and audit mandates expect you to encrypt?
- Do you have an internal PKI? – How do you securely store the root keys?
- Do you purchase third party SSL and TLS Certificates? – Are they centrally stored for improved security and performance?
- What crypto services do you currently offer? – How do you generate and store the cryptographic keys?

# Thales Luna Network HSM

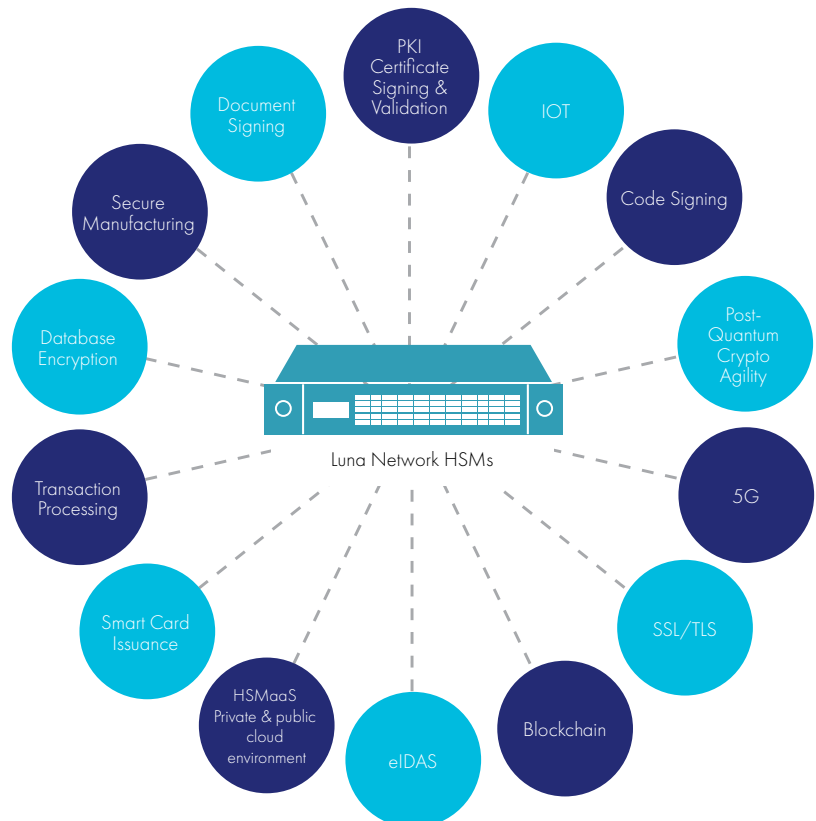
Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in Thales Luna Network HSM - high-assurance, tamper-resistant, network-attached appliances offering marketleading performance. You can integrate Luna Network HSMs into a wide range of applications to accelerate cryptographic operations, secure the crypto key lifecycle, and provide a root of trust for your entire encryption infrastructure.

## Value proposition

- High-assurance, FIPS 140-2 Level 3 validated
- Tamper-resistant network connected HSM appliance
- Hardware root of trust
- Hardware backup
- On-premises solutions
- Centralized crypto management
- Multiple form factors



[Click here to access Thales Luna Network HSM product brief](#)



# Thales Luna PCIe HSM

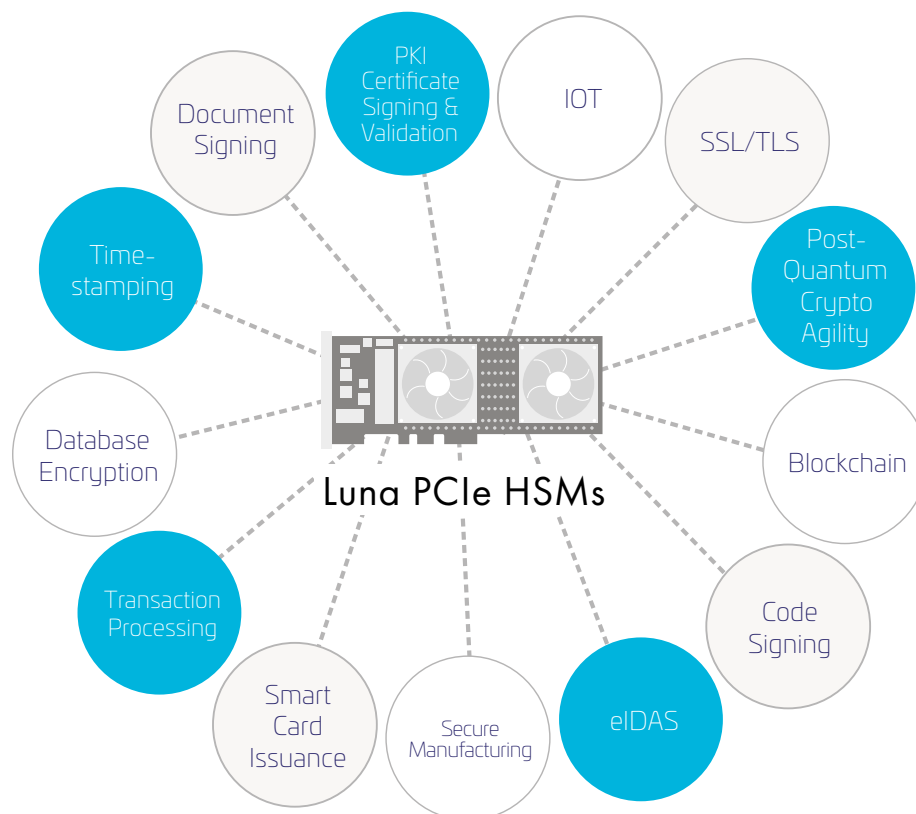
Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in Thales Luna PCIe HSM –high-assurance, tamper-resistant PCIe cards. Provide applications with dedicated access to a purpose-built, high-performance cryptographic processor. Quickly embed this cost-efficient solution directly into servers and security appliances for FIPS 140-2 validated assurance.

## Value proposition

- Server-embedded PCIe card
- High assurance, FIPS 140-2 validated, high performance cryptographic processor
- Keys always remain in FIPS-validated, tamper-evident hardware
- Meet compliance needs for GDPR, eIDAS, HIPAA, PCI-DSS, and more



[Click here to access the Thales Luna PCIe HSM product brief](#)





# Thales Luna USB HSM

Thales Luna USB HSM is a small form factor HSM. Governments, financial institutions, and large enterprises reduce security risks and ensure regulatory compliance with this hardware cryptographic root of trust for data, applications and digital identities. It is well suited for the strong protection of Certificate Authority (CA) root keys and Proof of Concepts (PoCs).

## Value proposition

- Small form-factor USB interface appliance
- Ideal for storing root keys in an offline, secure device
- FIPS 140-2 Level 3 validated



[Click here to access the Thales Luna USB HSM product brief](#)

# Thales Crypto Command Center

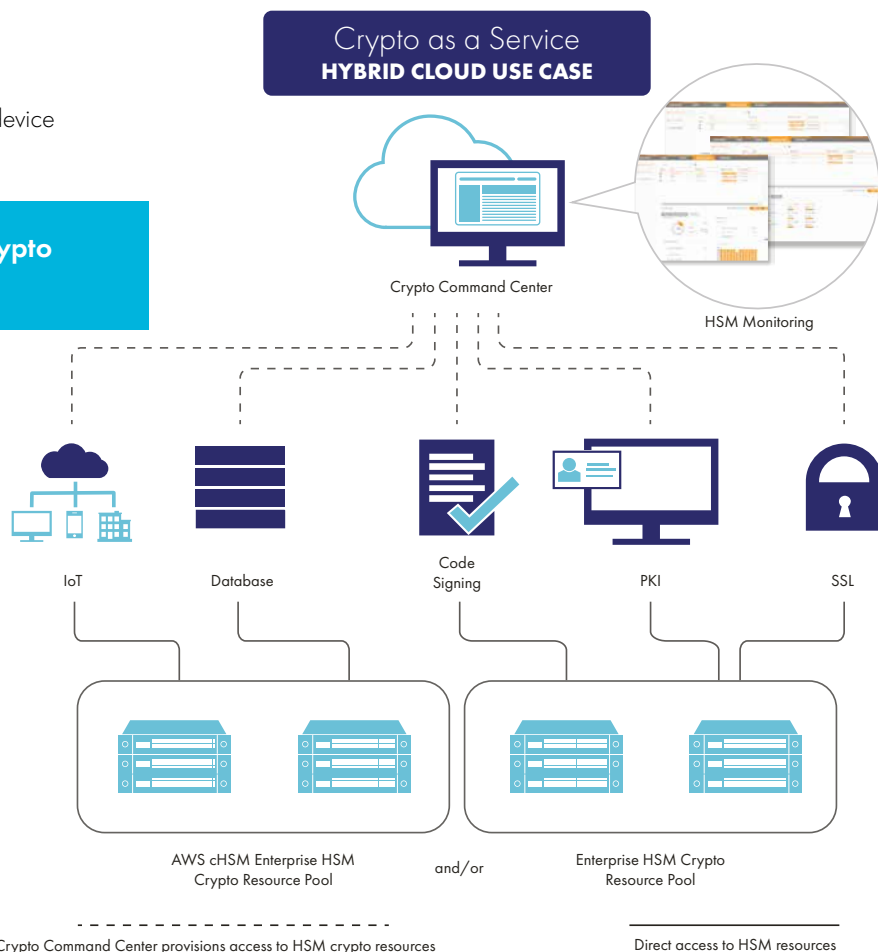
Thales Crypto Command Center centralizes crypto management HSM resources and helps to reduce IT security infrastructure costs. IT security departments and service providers can now quickly and securely expand IT capabilities, gain visibility, and streamline their infrastructure in physical, cloud, hybrid cloud and virtual environments with Thales Crypto Command Center. This is the market's first solution to fully exploit the benefits of virtualization including reduced costs and innovation, by provisioning Thales Luna Network HSMs without compromising security or compliance. Together Thales Crypto Command Center and Thales Luna Network HSMs combine to form one complete, centralized solution for the management of crypto HSM resources - a crypto hypervisor.

## Value proposition

- Small form-factor USB interface appliance
- Ideal for storing root keys in an offline, secure device
- FIPS 140-2 Level 3 validated



[Click here to access the Thales Crypto Command Center product brief](#)



# Thales ProtectServer PCIe HSM

The Thales ProtectServer PCIe HSM provides tamper-protected hardware security for server systems and applications that require high-performance symmetric and asymmetric cryptographic operations. The HSM provide secure storage and a dedicated cryptographic processor to deliver high-speed processing for cryptographic operations and fast transaction speeds. The HSM provides a wide range of cryptographic services, including encryption, user and data authentication, message integrity, secure key storage, and key management for eCommerce, PKI, document management, Electronic Bill Presentation and Payment (EBPP), database encryption, financial EFT transactions, plus many others.

## Value proposition

- Flexible, fully customizable HSM
- Ideal for application developers
- FIPS 140-2 validation
- Multiple form factors



[Click here to access the Thales ProtectServer PCIe HSM product brief](#)





# Thales Data Protection On Demand (DPoD)

Thales Data Protection On Demand is a cloud-based platform that provides a wide range of Cloud HSM and key management services through a simple online marketplace. With Data Protection On Demand, security is made simpler, more cost effective and easier to manage because there is no hardware to buy, deploy and maintain. Just click and deploy the protection required, provision services, add security policies and get usage reporting in minutes. Customers have access to a wide range of security services by simply clicking and deploying what they need to protect dozens of applications and use cases.

## Value proposition

- FIPS certified hardware-based HSM security with the ease of use of cloud services
- SLA – 99.95% availability, ISO 27001 compliant
- Multi-tier management, including complete separation of duties
- Easily integrates with existing apps, IT infrastructure & services
- Up and running in minutes - Point, click, & deploy

## Smart questions

- Do you need a cost effective and streamlined approach for protecting sensitive data, to meet compliance regulations such as GDPR and PCI DSS quickly and effectively?
- Is simple security deployment, with minimal impact on users important to you?



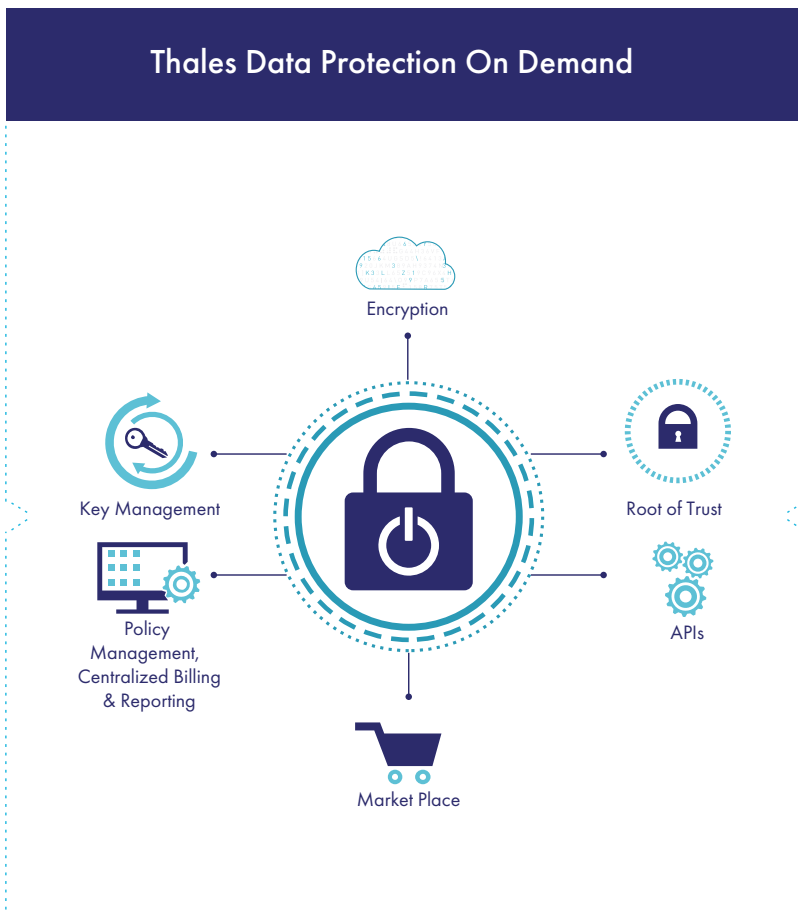
[Click here to access the Thales Data Protection On Demand \(DPoD\) product brief](#)



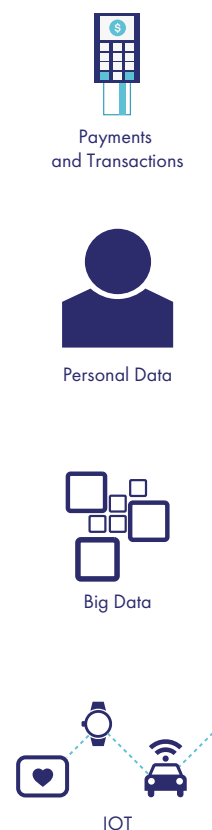
[Click here to access the Thales Data Protection On Demand \(DPoD\) customer presentation](#)

## Data Protection...Now Available On Demand

Protect Everywhere



Protect Everything



# payShield 10K

As markets and digital payment security standards continue to advance, a secure payment infrastructure is crucial to the success of global business. Organizations face many challenges in protecting the rapidly growing volume of digital payments – from transaction processing and country-specific mandates, to card/device issuance and direct-to-mobile (IoT) provisioning. Customers can rely on payShield 10K payment HSM to deliver the protection, performance, and operational efficiency needed to confidently secure digital payments.

## Value proposition

- Protection – Point-to-Point encryption protects payment data and reduces merchant PCI DSS scope
- Performance – Real time payments and Secure Remote Commerce (SRC). ECC algorithm\* supports 3D Secure 2.0, EMV Next Gen, and Software-based PIN entry on COTS device (SPoC)
- Operational efficiency – Reduce costs and streamline existing operations with lower power consumption, faster firmware updates, and broader cryptographic support



Click [here](#) to access the payShield 10K product brief



Click [here](#) to access the payShield 10K customer presentation

## Smart questions

- Which payment applications are you using – in-house or from a Thales ASAP technology partner (and if so, which one)?
- How many types of HSMs are you using in your production data centers?
- What types of cryptographic keys do you need to share with third parties?
- Which online or remote payment solutions do you need to support?
- Have you considered HSM options to help lower your operating costs, including:
  - Remote management using payShield Manager to eliminate most travel to data centers?
  - payShield Monitor for 24 x 7 monitoring of HSM utilization to identify performance bottlenecks?
  - Multiple LMK options to securely share an HSM between multiple applications or tenants?
  - Software performance upgrades to maximize HSM investment?





# payShield Manager

payShield Manager offers local and remote management options for both payShield 10K and payShield 9000 HSMs. It enables remote operation of HSMs via a standard browser interface, leveraging smart card access control to establish secure connections with HSMs. payShield Manager enables key management, security configuration and software and license updates to be carried out remotely.



[Click here](#) to access the payShield Manager product brief



[Click here](#) to access the Top 10 Reasons You Can't Live Without Remote HSM Management product brief

# payShield Monitor

payShield Monitor from Thales eSecurity is a comprehensive HSM monitoring platform that enables operations teams to gain 24x7 visibility into the status of all their payShield HSMs, including those residing across distributed data centers. With this solution, security teams can efficiently inspect HSMs and find out immediately if any potential security, configuration, or utilization issue may compromise their mission-critical infrastructure.



[Click here](#) to access the payShield Monitor product brief



[Click here](#) to access the Top 10 Reasons HSM Monitoring Helps You Avoid Outages product brief

# About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

# THALES

## Americas

Arboretum Plaza II, 9442 Capital of Texas Highway North,  
Suite 100, Austin, TX 78759 USA  
Tel: +1 888 343 5773 or +1 512 257 3900  
Fax: +1 954 888 6211 | E-mail: sales@thalessec.com

## Asia Pacific - Thales Transport & Security (HK) Ltd

Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East  
Wanchai, Hong Kong | Tel: +852 2815 8633  
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

## Europe, Middle East, Africa

350 Longwater Ave, Green Park,  
Reading, Berkshire, UK RG2 6GF  
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550  
E-mail: emea.sales@thales-esecurity.com

> [cpl.thalesgroup.com](https://cpl.thalesgroup.com) <

