cpl.thalesgroup.com

#ThalesNewNormal

Working Initiative

Your Thales Reference Guide

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 undergoing a digital transformation. 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 wherever it resides - at rest in on-premises data centers and in public/private clouds, and data-inmotion 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 discover, protect and control its data, identities and intellectual property with comprehensive data discovery and classification, data encryption, tokenization, access controls, advanced key and crypto 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

This reference guide accompanies the #ThalesNewNormal Working Initiative, designed to give an overview of the Thales portfolio.

For more detailed information please download the Partner Playbooks.

Identity and Access Management Partner Playbook
https://thales.webinfinity.com/content/1093864

Data Protection Partner Playbook
https://thales.webinfinity.com/content/1079137

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

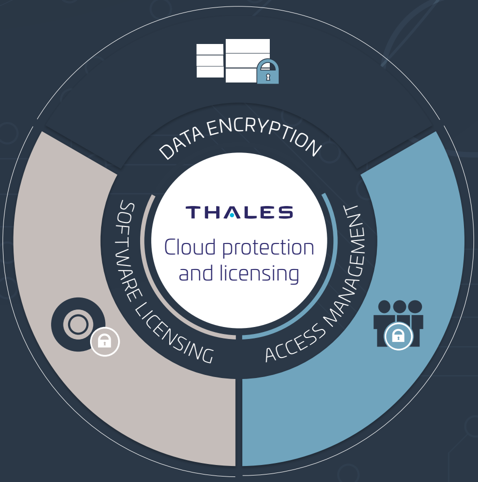
10 largest retailers in the world

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, or managing security as a service. As businesses evolve to encompass hybrid, multi-cloud environments, they need a comprehensive security solution that meets their needs regardless of where their data resides or who manages it for them. You can rely on Thales to deliver simple, data protection, and secure access solutions as a service in the cloud, on-premises or across hybrid environments. How are you securing your data across the hybrid multi-cloud?

Data Discovery & Classification

The crucial first step in compliance is to understand what constitutes sensitive data, where and how it is stored, and who can access it. Data Discovery and Classification enables organizations to get complete visibility of sensitive data across cloud, big data, and traditional environments. Does your organization know how to prevent sensitive data exposure?

Data Encryption

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?

Key Management

Manage encryption keys securely, with separation of duties, and over the entire lifecycle of the keys whether you choose to manage them in your own environments, or bring or hold them in them in the cloud (BYOK/HYOK). How do you ensure that your keys are always secure?

Secure Your Digital Transformation

Digital transformation is increasing the growth of connected devices, and with that comes the challenge of security, privacy, safety and reliability of the underlying systems and information. Additionally, security has become more complex with IoT, and containerized applications are more difficult to secure due to the way microservices and applications are developed, deployed and run. Thales can protect the digital keys and unique credentials on with modern digital security is built. Have you considered a defense-in-depth security approach and how purpose-built security solutions can help?

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? onfidence 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?

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.

Identity and Access Management Handbook

Thales Identity and Access Management Portfolio

Cloud-based applications play a vital role in fulfilling productivity and operational needs in the enterprise. However, as new services are added to an organizations' cloud estate, it becomes more difficult to gain unified visibility into cloud access events, more complex to comply with regulations and more onerous for users to remember multiple credentials. And with cloud applications protected, by default, only with weak static passwords, the risk of a data breach rises.

Thales's award-winning suite of SafeNet Access Management and Authentication solutions allow organizations to effectively manage risk, maintain regulator y compliance, gain visibility into all access events and simplify the login experience for their users. Utilizing policy-based SSO and universal authentication methods, enterprises can securely move to the cloud while maintaining access controls to all corporate resources, regardless of the device being used.

Prevent breaches

Deter unauthorized access and apply universal authentication methods for all apps

Enable cloud transformation securely

Transform your business and operate securely by applying consistent access policies to all on prem and cloud apps

Simplify the login experience

Make it simple for users to log into multiple apps with cloud SSO, elevating trust only when needed

Simplify compliance

Remain compliant as you grow your environment by setting policies that adapt to new regulations

Industries We Address

Government	GDPR, PSN, CJIS-SP
e-Filing Public Services	eIDAS, MCA-21
Healthcare	HIPAA, HITRUST, EPCS
Financial Services	FISMA, FFIEC, PCI DSS
Critical Infrastructure	NERC

Telecom and Service Providers

Manufacturing

Enterprise and More!

Use Cases We Secure

Cloud SSO

SaaS & Cloud

Web Portals

Digital Signature

Local Network Access

VDI

Physical/Logical Access

Endpoint Protection

Remote Access

Email Encryption

Products We Offer

Access Management

SafeNet Trusted Access

Authentication Methods

PKI

Hardware

3rd Party

OTP Push

Kerberos

Pattern Based

Voice

Biometric

Google Authenticator

SMS

eMail

Password

Passwordless

Standards-based Security

Thales's SafeNet Access Management and Authentication solutions offer unparalleled standards-based security:

- FIPS 140-2 validated software and hardware tokens
- Common Criteria certified hardware tokens
- ISO 27001:2013 accreditation
- AICPA SOC-2 recognition
- DSKPP-secured provisioning of software tokens
- ANSSI certified libraries within software tokens
- Hardware-based root of trust
- Field-programmable tokens

Access Management

Over the years, you may have heard a lot about access management. In fact, we tended to use the terms "authentication" and "access management" pretty much to mean the same thing. But in fact there are differences between the two. While authentication validates a user's identity, access management determines that a user has the permission to access a certain resource and enforces the access policy that has been set up for that resource.

Access management is very important when it comes to managing access to cloud resources. Nowadays, a person typically has to access numerous cloud apps throughout the day. This is a hassle for both users and IT: Users have to remember countless passwords; while IT need to endlessly reset forgotten passwords. The solution to this problem is SSO: By having one credential for all cloud apps, users can easily login once to several apps while IT saves precious time over password resets.

Since that single identity is only as secure as the authentication used to verify it, the method of verifying users' identities becomes paramount to maintaining cloud access security. To this end, access management solutions and single-sign on solution offer granular control over the access policies defined per application.

By requiring an additional authentication factor in high risk situations, a frictionless user experience is maintained.

Introduction to Access Management

Authentication and Access Management solutions are composed of Identity Governance and Administration (IGA) functionality and Access Management (AM) functionality. IAM solutions provide a methodic framework for granting (and requesting) access to applications (IGA), enforcing access controls (AM) and ensuring visibility into access events (AM). Given that most organizations deploy the IGA and AM components separately of each other, these disciplines are being increasingly evaluated as distinct, standalone solution families, rather than as composite functionalities of a single Authentication and Access Management suite.

Access management is a functionality that enables determining whether a user has permission to access a certain resource, and enables the enforcement of the access policy that has been set up for that resource.

Access management is implemented based on access policies that are defined by IT administrators and include such information as which groups of users (e.g. Sales, R&D, HR) are allowed access to which cloud applications (e.g. Salesforce, Office 365, Jira, Taleo), as well as the set of user attributes required to access each application (e.g. trusted network, password, OTP).

The access policy can require more or less user attributes to be assessed depending on the sensitivity of a cloud application. These attributes are assessed using riskbased or context-based authentication, which is central to enforcing the different access policies defined for each cloud application. (For more details, see context-based authentication.)

Also central to cloud access management is single sign-on, which enables the use of a single usernameand- password set or 'identity' to log in to all one's cloud applications. (For more details, see single sign-on.)

Visit https://thales.webinfinity.com/content/970662 to learn more and download the Access Management Handbook

Cloud Access Management

Cloud applications are excellent at providing organizations the best technology at a quick time to value, zero maintenance overhead and infinite scalability. The immediate fulfillment and instant productivity provided by cloud apps comes, however, with a price tag. IT departments lose visibility into who is accessing what application, when—and what authentication method is being used.

Compliance risk increases as apps are managed from multiple disparate consoles, while help desk tickets owing to password resets abound.

The most important person in the process—the end user—suffers from password fatigue, frustration and downtime as they fret to keep their copious identities in order.

To address these cloud adoption hurdles, cloud access management solutions have emerged to streamline cloud access provisioning, eliminate password hassles for IT and users, provide a single pane view of access events across your cloud estate and ensure that the right access controls are applied at the right time to the right user.

Visit https://thales.webinfinity.com/content/972955 to access the Access Management Primer fact sheet

Visit https://thales.webinfinity.com/content/970698 to access the 4 Steps to Cloud Access Management guide

Value proposition:

Optimized cloud security - By enforcing scenario-based access controls using finegrained policies, organizations optimize security and reduce the risk of a breach

Ease of Management - Access management provides administrators with a single point of management, a single pane of glass, from which to define access policies once and enforce them throughout

Visibility - Access management solutions enable IT to answer the questions "Who has access to what?" "Who accessed what and when? and "How was their identity verified?" By gaining a central view of access events and visibility into which applications are being accessed also saves businesses money as it enables identifying which app licenses are underutilized

Access Management Benefits - Implementing cloud access management solutions increases enterprise access security, removes the ambiguity associated with cloud security and compliance risk—and no less important—ensures the most frictionless user experience.

Enhanced user convenience - Access management solutions offer cloud single sign on, which lets your users log in just once in order to gain access to all their cloud applications, using the familiar enterprise identity they already use today

Cloud access management ensures that the right people have access to the right applications at the right level of trust

Cloud access management solves the challenges faced by enterprises in their quest for broader cloud adoption.

SafeNet Trusted Access (STA)

Thales offer access management and authentication solutions which prevent data breaches and enable cloud adoption by simplifying and securing access to all your apps. STA is an access management and authentication service. By helping to prevent data breaches and comply with regulations, STA allows organizations to migrate to the cloud simply and securely.

Value proposition

- Prevent breaches - Apply different MFA methods and control accesses for each app while eliminating passwords
- Enable cloud transformation securely - Extend existing access controls to cloud apps and apply consistent access policies to all cloud resources
- Simplify compliance - Prove compliance with a real-time audit trail of who is accessing which app and how
- STA prevents data breaches, allowing organizations to migrate to the cloud simply and securely

STA core capabilities

- Access Management
- Authentication
- Smart Single Sign On

Target customers

- CISO
- IT Manager
- Support
- End User
- Finance

Supported authentication methods

- OTP Push
- OTP App
- OTP Hardware
- Pattern-based authentication
- Out-of-band via email and SMS text messages
- Password
- PKI credentials
- FIDO
- Google Authenticator
- Passwordless authentication
- Biometric
- Voice
- 3rd party

Visit https://thales.webinfinity.com/content/972285 SafeNet Trusted Access product brief

Smart questions

- Organizations who planning to use cloud apps, or that are already using several cloud apps will be the most likely customers for STA. The purpose of the questions below is to help us understand where our customer is in terms of cloud adoption. The first thing to verify is whether the customer already is using an IDaaS or SSO solution. Those that are not, will more likely be potential customers for STA.

Customers who are NOT using an SSO or IdaaS solution:

- How many cloud apps are deployed in your organization?
- Is there a "cloud first / cloud adoption" strategy direction in your organization?   Do you have many issues with users having to manage multiple passwords for the various apps? How do you handle that currently?
- Do you want to be able to apply 2FA and SSO to all cloud apps?
- Customers who ARE already using an SSO or IDaaS solution:
- What are you using today?
- How does it allow you to set policies per application and per user?
- What type of 2FA methods can you use?
- What applications does it protect?
- What additional features would you like to see in your current solution that are not available?
- What types of other solutions are you looking into at this time?
- How are you protecting O365?

Access Management for Leading Applications

SafeNet Trusted Access supports hundreds of applications, including the following:

amazon web services
Office 365
salesforce
IBM Connections
G Suite
zendesk
WordPress
Pulse Secure
box
JIRA
citrix ShareFile
servicenow
f5
BLUE COAT
Drupal
OWA

Thales Authentication Portfolio

Universal Authentication Capabilities

Thales delivers fully-automated, highly secure next generation authentication capabilities with flexible authentication options tailored to the unique needs of any organization. Our platforms support a broad range of authentication technologies and form factors as outlined below:

OTP

- One-time passwords are supported via PUSH notifications generated on mobile devices, on apps installed on desktops and via hardware tokens.

Certificate-based authentication

Thales' range of certificate-based solutions offer strong multi-factor authentication and enable organizations to address their PKI security needs. Thales' virtual smart card solution, hardware smart cards and USB authenticators offer a single solution for strong authentication and high assurance applications such as digital signing and email encryption. They also support network logon, as well as corporate ID badges, magnetic stripes and proximity.

Thales offers a broad range of certificate-based PKI authentication solutions. These include:

- SafeNet IDPrime Virtual - A virtual smart card solution that facilitates mobility by enabling PKI-based security on all devices and reduces the operational overheads associated with hardware based authentication devices.
- Smart Card hardware form factor
- USB token form factor

PKI authentication solutions are enabled by SafeNet Authentication Client middleware and CMS solutions that manage certificate life cycle management and provisioning.

Adaptive authentication

Thales' context-based authentication offers convenient, frictionless strong authentication while maintaining the flexibility and agility to add protection with stronger methods of security in higher risk situations.

Combined with "step-up" authentication, context-based authentication optimizes a layered approach to access security by assessing user login attributes and matching them against pre-defined security policies.

SMS and eMail

- Numerical passcodes can be delivered to all devices via SMS or eMail

Pattern-Based Authentication

Thales' GrIDsure flexible authentication method allows an end-user to generate a one-time password without the requirement for hardware tokens or software applications. GrIDsure tokens work by presenting the end-user with a matrix of cells which contain random characters, from which they select a 'personal identification pattern' (PIP).

FIDO Authenticators

SafeNet FIDO2 Devices offer enterprises strong and secure passwordless authentication to any environment.

SafeNet IDPrime 3940 FIDO (Smart Card) and SafeNet eToken FIDO (USB token enable organizations to secure cloud adoption and bridge secure access across hybrid environments via an integrated access management and authentication offering.

Third Party Authenticators

Thales solutions support OATH tokens and other third party authenticators.

Data Protection Handbook

CipherTrust Data Security Platform

As data breaches continue at alarming rates, securing sensitive data is critical to all organizations. In addition, organizations struggle to stay compliant with evolving global and regional privacy regulations, and securing the cloud in the face of accelerated adoption brought on by the new demand to support tremendous number of remote employees. IT security organizations seek a data-centric solution that secures the data as it moves from networks to applications and the cloud. When perimeter network controls and endpoint security measures fail, protecting data at rest is the last line of defense.

The CipherTrust Data Security Platform integrates data discovery, classification, data protection and unprecedented granular access controls, all with centralized key management. This solution removes data security complexity, accelerates time to compliance, and secures cloud migration, which results in less resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

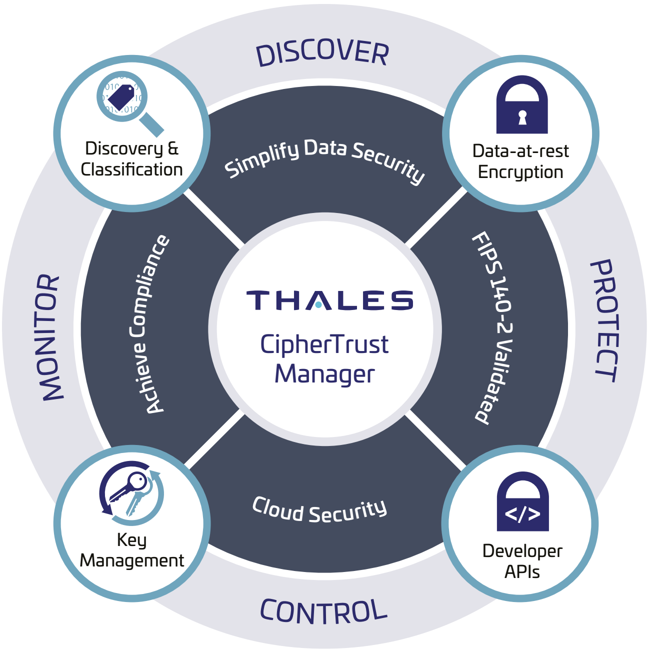
Key Features

- Centralized management console
- Monitoring and reporting
- Data discovery and classification
  - Risk analysis with data visualizationData protection techniques
  - Transparent encryption for files, databases and containers
  - Application-layer data protection
  - Format preserving encryption
  - Tokenization with dynamic data masking
  - Static data masking
  - Privileged user access controls
- Centralized enterprise key management
  - FIPS 140-2 compliant
  - Unparalleled partner ecosystem of KMIP integrations
  - Multi-cloud key management
  - Database encryption key management (Oracle TDE, big data, MS SQL, SQL Server Always Encrypted, etc.)

Compliance

CipherTrust Data Security Platform supports global security and privacy regulations, including:

- GDPR
- PCI DSS
- HIPAA
- SOX/GLBA
- CCPA
- FIPS 140-2
- FISMA, FedRAMP
- NIST 800-53 rev.4
- South Africa POPI Act
- ISO/IEC 27002:2013
- Japan My Number Compliance
- South Korea's PIPA
- India's Aadhaar Act
- Philippine's Data Privacy Act
- Monetary Act of Singapore
- Australia Privacy Amendment



Key Benefits

- **Simplify Data Security.** Discover, protect, and control sensitive data anywhere with next-generation unified data protection. The CipherTrust Data Security Platform simplifies data security administration with 'single pane of glass' centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or in any external provider's infrastructure. Organizations can easily uncover and close privacy gaps, prioritize protection, and make informed decisions about privacy and security mandates before a digital transformation implementation.
- **Accelerate Time to Compliance.** Regulators and auditors require organizations to have control of regulated and sensitive data along with the reports to prove it. CipherTrust Data Security Platform capabilities, such as data discovery and classification, encryption, access control, audit logs, tokenization, and key management support ubiquitous data security and privacy requirements. These controls can be quickly added to new deployments or in response to evolving compliance requirements. The centralized and extensible nature of the platform enables new controls to be added quickly through the addition of licenses and scripted deployment of the needed connectors in response to new data protection requirements.
- **Secure Cloud Migration.** The CipherTrust Data Security Platform offers advanced encryption and centralized key management solutions that enable organizations to safely store sensitive data in the cloud. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager. The CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications. With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise's sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over data, wherever it is created, used, or stored.

CipherTrust Data Security Platform Products

CipherTrust Manager

CipherTrust Manager is the central management point for the platform. It is an industry-leading enterprise key management solution that enables organizations to centrally manage encryption keys, provide granular access controls and configure security policies. CipherTrust Manager manages key lifecycle tasks including generation, rotation, destruction, import and export, provides rolebased access control to keys and policies, supports robust auditing and reporting, and offers development- and management-friendly REST APIs. CipherTrust Manager is available in physical and virtual form-factors that are FIPS 140-2 compliant up to level 3. The CipherTrust Manager can also be rooted to a hardware security module (HSM) such as Thales Luna and Luna Cloud HSM.

CipherTrust Data Discovery and Classification

CipherTrust Data Discovery and Classification locates regulated data, both structured and unstructured, across the cloud, big data, and traditional data stores. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, compliance violations and prioritizing remediation. The solution provides a streamlined workflow all the way from policy configuration, discovery, and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption delivers data-at-rest encryption, privileged user access controls and detailed data access audit logging. Agents protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers in cloud and big data environments. The Live Data Transformation extension is available for CipherTrust Transparent Encryption, providing zero-downtime encryption and data rekeying. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

CipherTrust Application Data Protection

CipherTrust Application Data Protection delivers crypto functions such as key management, signing, hashing and encryption services through APIs, so that developers can easily secure data at the application server or big data node. The solution comes with supported sample code so that developers can move quickly to securing data processed in their applications. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management from developer responsibility and control. In addition, it enforces strong separation of duties through key management policies that are managed only by security operations.

CipherTrust Tokenization

CipherTrust Tokenization is offered both vaulted and vaultless and can help reduce the cost and complexity of complying with data security mandates such as PCI-DSS. Tokenization replaces sensitive data with a representative token, so that the sensitize data is kept separate and secure from the database and unauthorized users and systems. The vaultless offering includes policy-based dynamic data masking. Both offerings make it easy to add tokenization to applications.

CipherTrust Database Protection

CipherTrust Database Protection solutions integrate data encryption for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, IBM DB2 and Teradata databases.

CipherTrust Key Management

CipherTrust Key Management delivers a robust, standards-based solutions for managing encryption keys across the enterprise. It simplifies administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services. CipherTrust Key Management solutions support a variety of use cases including:

- **CipherTrust Cloud Key Manager** streamlines bring your own key (BYOK) management for Amazon Web Services, Microsoft Azure, Salesforce and IBM Cloud. The solution provides comprehensive cloud key lifecycle management and automation to enhance security team efficiency and simplify cloud key management.
- **CipherTrust TDE Key Management** supports a broad range of database solutions such as Oracle, Microsoft SQL, and Microsoft Always Encrypted.
- **CipherTrust KMIP Server** centralizes management of KMIP clients, such as full disk encryption (FDE), big data, IBM DB2, tape archives, VMware vSphere and vSAN encryption, etc.

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.

Target customers

Organizations with:

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

Smart questions

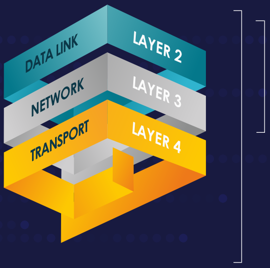
- **Are you encrypting your network?**
  - Yes - What are you using?
  - Considering - Are you considering encrypting at Layer 2?
  - No - Why? Are you aware of the risks and latest breaches?
- **High-level topics to start the HSE conversation**
  - Data Links – Everyone has them. Where are the big pipes?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

Visit https://thales.webinfinity.com/content/971559 to access the High Speed Encryptors for Education solution brief

Network Independent Encryption

Meeting the evolving needs of today's networks.

Concurrent multi-layer encryption



CN Series
Hardware encryption

CV Series
Virtualised encryption

Destination policy based

Data centre

Head office

Branch office

Cloud computing

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.

With Thales Hardware Security Modules, You Can address compliance requirements with solutions for Blockchain, GDPR, eIDAS, IoT, paper-to-digital initiatives, PCI DSS, digital signatures, DNSSEC, hardware key storage, transactional acceleration, certificate signing, code or document signing, bulk key generation, data encryption, and more. Keys are generated, and always stored in the intrusion-resistant, tamper-evident, FIPS-validated appliance, providing the strongest levels of access controls.

Create partitions with a dedicated Security Office per partition, and segment through admin key separation.

Luna General Purpose HSM

Available in a wide range of form factors and performance options, Thales Luna General Purpose HSMs safeguard the cryptographic keys used to secure transactions, applications, and sensitive data.

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?
- Does your HSM provide the ability to address your existing traditional use cases such as code signing, PKI and database encryption, as well as emerging technologies such as Blockchain, 5G, IoT and BYOK?
- Do you have the ability to quickly react to cryptographic threats? Can you implement alternative methods of encryption, ensuring you can migrate your applications to new postquantum algorithms?

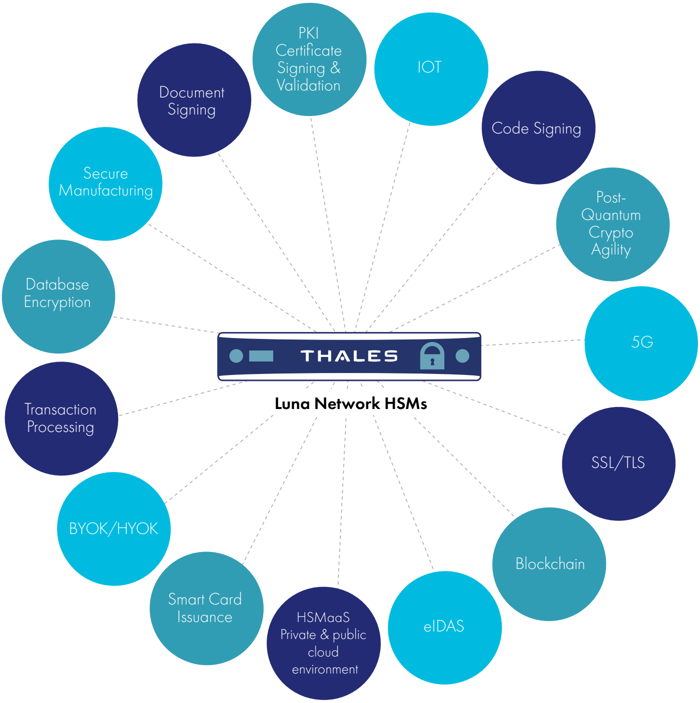
Thales Luna Network HSM

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 market-leading 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. Furthermore, centralize your Luna Network HSM crypto resources and reduce IT security infrastructure costs with Crypto Command Center - a complete monitoring, reporting and management tool for on-premises, hybrid and cloud environments.

Value proposition

- Ensure keys always remain in high assurance FIPS 140-2 Level 3, tamper-evident hardware root of trust
- Protect your organization today and into the quantum era
- Meet high throughput requirements for high performance use cases
- Meet compliance for eIDAS, GDPR, HIPAA, PCI-DSS and more
- Securely backup and duplicate keys in hardware for redundancy, reliability and disaster recovery
- Increase security with multi-person MofN with multi-factor authentication
- Multiple roles for strong separation of duties
- Remotely manage Luna HSMs - no need to travel
- Reduce audit and compliance costs and burdens
- Extend native HSM functionality by developing and deploying custom code within the secure confines of the HSM

Visit https://thales.webinfinity.com/content/972229 to access Thales Luna Network HSM product brief



Thales Data Protection On Demand (DPoD)

The award winning Thales Data Protection on Demand (DPoD) is a cloud-based platform, providing a wide range of Luna Cloud HSM, CipherTrust Cloud Key Management, and payShield Cloud Payment services through a simple online marketplace. Data security is now simpler, more cost effective and easy 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. DPoD is also ideal for Managed Security Providers and Managed Security Service Providers who want to provide their customers unrivaled data-protection-as-a service solutions, bundled with their other cloud and security services.

Value proposition

- Deploy and manage key management and hardware security module services, on-demand and from the cloud
- SLA – 99.95% availability, ISO 27001 compliant
- Focus on services, not hardware
- Deploy in minutes, not days
- Purchase only what you need and reduce costs
- Protect data anywhere
- Real-time reporting and visibility
- Multi-tier management, including complete separation of duties
- Easily integrates with existing apps, IT infrastructure & services

Visit https://thales.webinfinity.com/content/971344 to access the Thales Data Protection On Demand (DPoD) product brief

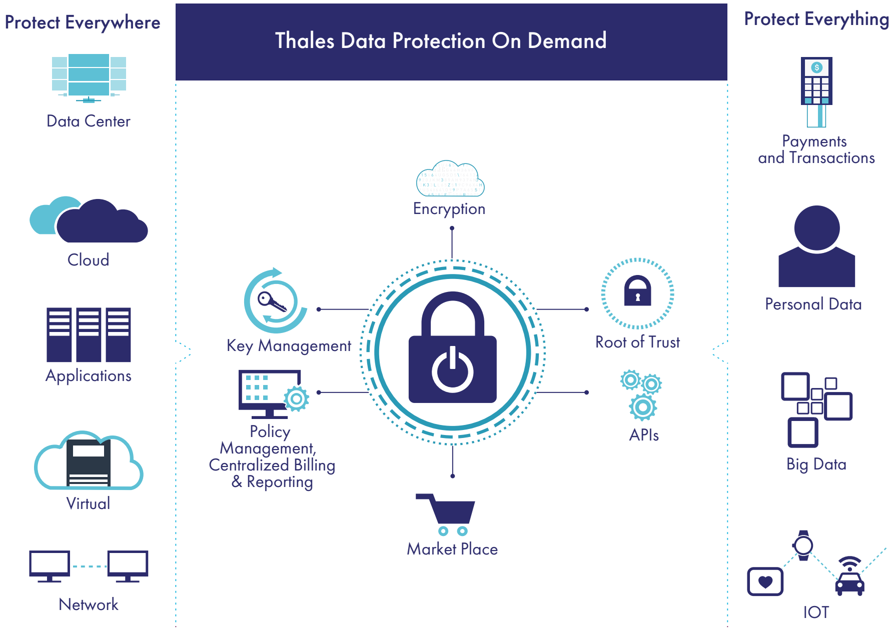
Smart questions

- What is your company strategy around cloud adoption?
- If you use a CSP, how do you feel about the data security provided by the cloud service provider?
- What are your concerns when it comes to securing your data?
- Do you have internal resources to manage the data security?

Visit https://www.youtube.com/watch?v=1E1Fb0xl-8M to view Thales Data Protection On Demand video

Visit cpl.thalesgroup.com/encryption/data-protection-on-demand/marketplace to access the Thales Data Protection On Demand - 30-Day Free Evaluation information page

Data Protection...Now Available On Demand



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

- Optimized for deployment in dark data centers – comprehensive remote management and monitoring underpinned by high resilience and availability
- Operational efficiency – reduce costs and streamline existing operations with lower power consumption, faster firmware updates and broader cryptographic support
- Proven integrations – payShield HSMs work off-the-shelf with the largest number of payment applications from the leading vendors
- Future-proof design – leverage the latest cryptographic functions to support new payment methods while meeting stringent security standards
- Backwards compatible will all legacy Thales payment HSMs – a simple migration path for all payShield 9000 users

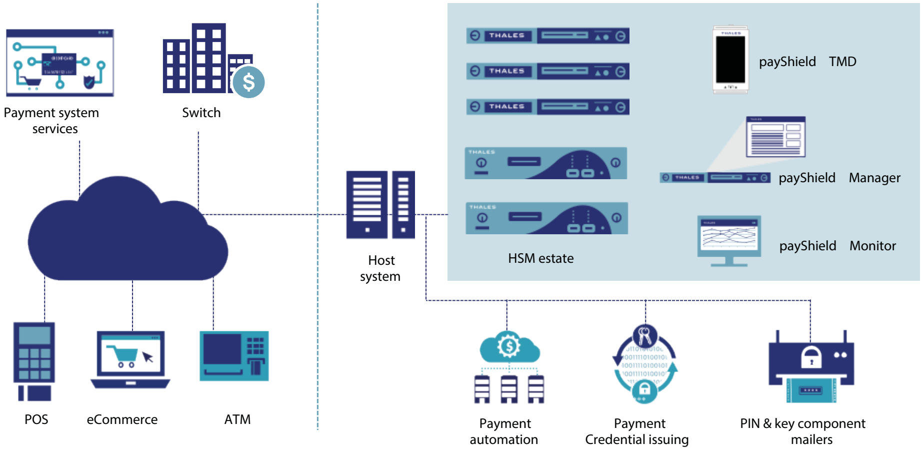
Visit https://thales.webinfinity.com/content/974554 to access the payShield 10K data sheet

Visit https://thales.webinfinity.com/content/974526 to access Top 10 reasons for Migrating to payShield 10K now data sheet

Smart questions

- Which payment applications are you using – in-house or from a Thales Accelerate 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?
  - payShield Trusted Management Device as a more flexible, portable and efficient alternative to a console for key component management?
  - Multiple LMK options to securely share an HSM between multiple applications or tenants?
  - Software performance upgrades to maximize HSM investment?

Visit https://thales.webinfinity.com/explore/284067?search-bar=%7B%22k%22:%22payshield%20 10K%22%7D to access payShield 10K sales enablement tools



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.

About Exclusive Networks

Exclusive Networks is the global 'value creating' specialist distributor for cybersecurity and cloud solutions – the defining and interdependent technologies of the digital era. Its capabilities are backed by best-of-breed vendor portfolios, unparalleled skills and a host of compelling services from pre and post-sales technical support to leasing, training, professional services and global project management. With 50+ offices across five continents and presence in over 100 countries, Exclusive Networks has a unique 'local sale, global scale' model, creating value and enabling partners to achieve global reach, while delivering the value of a locally-focused specialist distributor. More at www.exclusive-networks.com.

Your Partner Team

Identity and Access Management

Grahame Williams - grahame.williams@thalesgroup.com

Ben Willis - ben.willis@thalesgroup.com

Claire Barnes - claire.barnes@thalesgroup.com

Lucy Toms - lucy.toms@thalesgroup.com

Yvonne Mansfield - yvonne.mansfield@thalesgroup.com

Data Protection

Amelia Hicks - amelia.hicks@thalesgroup.com

Andrew Griffiths - andrew.griffiths@thalesgroup.com

Laurence Nutt - laurence.nutt@thalesgroup.com

Luke Cox - luke.cox@thalesgroup.com

Michael Gates - michael.gates@thalesgroup.com

Sunny Toor - sunny.toor@thalesgroup.com

Systems Integrators and Solution Providers

Phil Duerdan - philip.duerden@thalesgroup.com

Andy Cox - andrew.cox@thalesgroup.com

Jeff Williams - jeff.williams@thalesgroup.com

Nilly Pegg - nilly.pegg@thalesgroup.com

Seb Brals - sebastien.brals@thalesgroup.com

Exclusive Networks

Simon Bickers, Thales Vendor Manager
SBickers@exclusive-networks.com

Hannah Woodbourne, Product Sales Specialist
hwoodbourne@exclusive-networks.com

Julie Lewis, Thales Marketing Manager
JLewis@exclusive-networks.com

Partner Resources

Partner Portal:
thales.webinfinity.com

Marketing Accelerate Tool (via partner portal)

BrightTalkWebinar Channel:
www.brighttalk.com/channel/2037/

THALES

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <