cpl.thalesgroup.com

THALES
Building a future we can all trust

Your Data. Their Cloud.

Leveraging the Cloud without Relinquishing Control

White Paper

Contents

Executive Summary

In today's organizations, digital transformation is a vital imperative—and cloud services offer a proven path to accelerate an organization's repositioning to thrive in the digital economy. A successful digital transformation demands that organizations address security, privacy, and compliance objectives. This white paper looks at the factors driving the need to expand the use of cloud services, the critical security, privacy, and compliance objectives that organizations must address, and the core security capabilities required to leverage the cloud without relinquishing control.

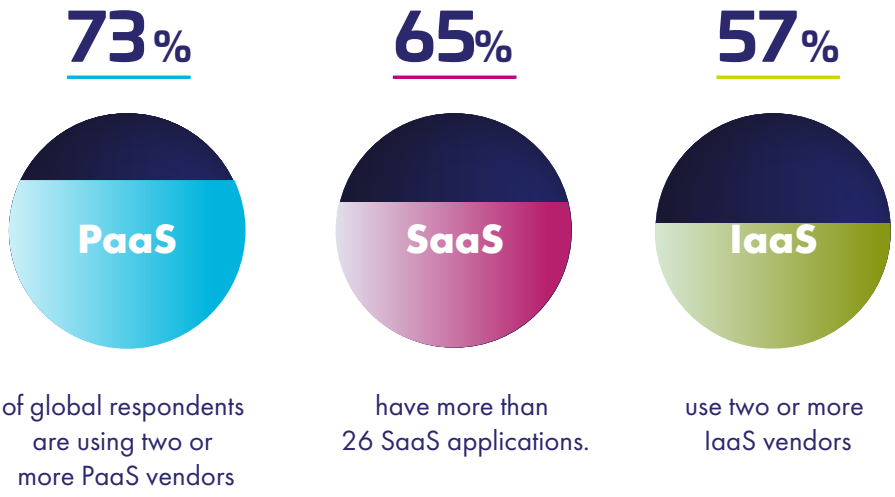
Growth of cloud services is integral to meeting the digital transformation imperative

Today, delivering optimized customer experiences (CX) remains a consistent, vital mandate. Increasingly, optimizing CX means providing high-quality, rewarding, and consistent digital experiences to satisfy a user base that has high expectations and is quick to defect when their expectations aren't met.

Perhaps more than any other approach or technology, cloud services represent a foundational building block for successful digital transformation. This includes all modalities of Infrastructure, Platform, and Software-as-a-Service in public, private, and hybrid forms.

According to the 2021 Data Threat Report, produced by 451 Research for Thales, 73% percent of global respondents are using two or more PaaS vendors, 57% use two or more IaaS vendors, and 65% have more than 26 SaaS applications[1].

1 Thales Data Threat Report 2021 https://cpl.thalesgroup.com/data-threat-report



Critical security demands in cloud environments

The massive adoption of multiple flavors of cloud services creates a complex hybrid IT environment for security executives to manage, and exacerbates cyber security and compliance challenges. While digital transformation is critical, so too is ensuring compliance, combatting cyber threats, and guarding against the risks posed by privileged users.

Compliance with regulations

In recent years, the number and scope of regulatory requirements have increased for organizations in a broad range of industries. The landmark European Union General Data Protection Regulation (GDPR), was followed by the California Consumer Privacy Act (CCPA), and the General Data Protection Law or LGPD in Brazil. And these are just the beginning. In multiple countries, the legislatures and working groups are in the final stages of considering bills and mandates governing privacy matters.

Data sovereignty rules (keeping data within sovereign boundaries, even when in the cloud) create an additional level of complexity. The Schrems II ruling in 2020 invalidated the EU-US Privacy Shield, which regulated the transfers of personal data between the US and European Union. Multi-national enterprises the world over now must take extra care to not allow the export of regulated data -- which is easier said than done. If an employee based in the US accesses sensitive data associated with a European citizen, according to Schrems II, accessing the data is considered an "export."

Further, financial services must comply with multiple rules, including those in the global Payment Card Industry Data Security Standard (PCI DSS) or regional guidelines such as the Monetary Authority of Singapore (MAS) Advisory on Cyber Security Risks in the Public Cloud. Government agencies must comply with national regulations such as the Federal Information Security Management Act (FISMA), healthcare providers with the Health Insurance Portability and Accountability Act (HIPAA), and the list goes on.

Guarding against cyber attacks

Cyber attackers continue to get more sophisticated and tenacious, massive data breaches continue to multiply, and guarding against data breaches continues to be a mandate after services are migrated to the cloud.

While cloud infrastructure security is a focus area for Cloud Service Providers, cybersecurity is not their primary business. Security controls for Cloud Service Providers are notoriously tough to figure out and can be easy to overlook[2]. Cloud infrastructure can be susceptible to ransomware, an ever-growing threat striking organizations large and small.

A report published by the research firm IDC found that 80% of the enterprises in the study had experienced at least one cloud data breach in the past 18 months, and nearly half (43%) reported 10 or more breaches[3].

> "only 17% of enterprises indicated that they have protected a majority of their sensitive data in the cloud with encryption."

One of the main causes of cloud data breaches is that while cloud usage continues to grow, the level of security in the cloud does not. Protecting applications at login access points, and protecting data with mechanisms such as encryption do not appear to be scaling up with the increased use of the public cloud. In the 2021 Thales Data Threat Report, only 17% of enterprises indicated that they have protected a majority of their sensitive data in the cloud with encryption, and just 55% have implemented MFA in any form.

In competitive markets, breaches can render organizations responsible for significant penalties in terms of fines, negative publicity, and lost customers. Further, the direct costs associated with these breaches continue to grow. One global study found that the average cost of a data breach grew 10 percent over the previous year and is now $4.24 million[4].

2 Wall Street Journal, "Human Error Often the Culprit in Cloud Data Breaches"
3 Security Magazine, "Nearly 80% of Companies Experienced a Cloud Data Breach in Past 18 Months"
4 IBM, "2021 Cost of a Data Breach Study by Ponemon"

Guarding against privileged user abuse

While guarding against external cyber-attacks is essential, that is not the only risk that needs to be addressed. The persistent reality is that one rogue administrator can expose the business and its data to significant risks. The Verizon Data Breach Report of 2021 shows that "Privileged User Abuse" is by far the most common vector for cyberattacks in the world[5].

> "only 48% of enterprises use Multi-Factor Authentication (MFA) to authenticate privileged users."

Privileged users/accounts are at the greatest risk because they provide access to an organization's most sensitive accounts.

Further, it takes no more than a port left open inadvertently, or a firewall configured incorrectly, for an organization to experience a major breach. One analyst firm estimated that over the next several years, at least 95% of cloud security failures will be the customer's fault[6].

Still, even with these clear facts, only 48% of enterprises use Multi-Factor Authentication (MFA) to authenticate privileged users. Worse still, 39% of enterprises said they haven't even deployed an integrated system that provides policy-based access, cloud single sign on (SSO) authentication[7].

Avoiding accidental data leaks

When you outsource a major part of your IT infrastructure to anyone, cloud service provider or otherwise, you risk putting all your data eggs in one security basket. Sometimes that basket has a hole in it. Aside from breaches caused by active hacks by malicious entities, there are numerous cloud security incidents traced back to configuration errors, user misunderstandings, and just embarrassing gaps in operational procedures. Sadly, this is a common problem associated with the cloud because such complexity is hidden within layers of abstraction and virtualization. It is easy to tweak a single configuration and have access fall open somewhere unseen. This is compounded by the fact that cloud deployments are being done more and more by users inexperienced in operations or IT security.

Obstacles to cloud security

As the prior sections illustrate, establishing strong security controls in cloud environments is vital for compliance, and guarding against external cyber-attacks, internal mistakes, and abuse. Addressing the cloud environment poses a unique set of challenges:

1. By definition, sensitive data and applications reside outside of a traditional corporate perimeter, which means many of an enterprise's legacy perimeter-based security approaches and technologies no longer apply.
2. Today's hybrid environments breed complexity because security teams have to contend with traditional on-premises environments and an increasing array of hybrid and cloud services. The speed of change has led organizations to "bolt-on" security point products or use cloud-native security to meet specific security or compliance requirements – even when it means no longer owning your access security and authentication. Consequently, IT must manage even more siloed data security solutions protecting different platforms and different environments.
3. While cloud providers may offer security capabilities, these are not a complete solution to maintain security and control across your organization's deployments on-premises and in multiple clouds. One CSP's capabilities invariably will not apply to another cloud vendor's environment or on-premises implementation. Further, each cloud model offers different levels of controls, so, for example, the controls that work in an IaaS environment won't necessarily be practical in a SaaS deployment. The gaps are compounded when customers use apps in multiple clouds and manage security across hybrid environments.

Ultimately, when security teams are forced to implement security controls in a siloed, piecemeal fashion, they contend with inefficiencies, inconsistencies, high management overhead, excessive costs, gaps and loss of control.

5 Verizon Data Breach Report of 2021

6 Gartner, "Is the Cloud Secure?" March 27, 2018, Kasey Panetta,

7 Thales Identity and Access Management Index 2021

The CSP shared responsibility model

The shared responsibility model delineates what the cloud customer is responsible for and what your cloud service provider (CSP) is responsible for. The CSP is responsible for security "of" the cloud—think physical facilities, utilities, cables, hardware, etc. The customer is responsible for security "in" the cloud—meaning network controls, identity and access management, application configurations, and especially the security of the data.

		On-prem	IaaS	PaaS
Application elements are specific to the customer's business, so they are the customer's responsibility	Application user access management	✔	✔	✔
	Application-speicific data assets	✔	✔	✔
	Application-specific logic and code	✔	✔	✔
Workload responsibility depends on IaaS vs PaaS model (PaaS often referred to as "Serverless")	Application / platform software	✔	✔	✔
	Operating system and local networking	✔	✔	✔
	Virtual machine / server instance	✔	✔	✔
Lower-level infrastructure is more generic and commodotized, and the provider assumes responsibility	Virtualization platform	✔	✔	✔
	Physical hosts / servers / compute	✔	✔	✔
	Physical and perimeter network	✔	✔	✔
	Physical datacenter enironment	✔	✔	✔

✔ Customer ✔ Provider

Source: Cloud Security Alliance web site: Shared Responsibility Model Explained

As the graphic above illustrates, no matter what model of cloud service an organization uses, the organization that owns and grants access to the apps and data is ultimately responsible for the security of the apps and data. Security controls need to be applied to ensure compliance and to document and demonstrate compliance, for data that is not stored or managed by their internal organization. This includes enforcing separation of duties, access controls, multi-factor authentication and high assurance key controls.

Key cloud security requirements

Security teams tasked with securing workloads, apps and data sets across cloud environments must address several specific objectives. Sensitive data needs to always remain confidential and secure, including when it is on premises, in the cloud, or in transit. This requires controls that persist, for example, to safeguard assets even after hardware or virtual resources are decommissioned, or if the cloud service provider (CSP) is subpoenaed.

Controls must be put in place that guard against enterprise or CSP administrators maliciously or inadvertently exposing sensitive assets. Within multi-tenant cloud environments, security teams also need to ensure data can't be accessed by other tenants.

To be pragmatic, solutions must be aligned with the following characteristics:

- **Comprehensive, unified coverage.** Security teams need to be able to establish centralized controls that enable efficient and consistent application of policies for access controls, encryption, and key management. Security teams need a unified platform that offers central, convenient controls over complex, distributed environments, including on-premises and multiple cloud providers.
- **Data-centric.** Data security today needs to recognize not only that data is the most valuable asset of the organization, but also that it is proliferating exponentially. Data-centric security protects the data itself regardless of the applications using the data, the environments where the data resides, or the networks the data crosses.
- **High assurance.** Encryption and key management systems employed need to deliver the highest levels of availability and performance, as well as certified, proven security. Access management needs to enforce access controls at every access point, allowing only verified administrators to access privileged accounts while enforcing less stringent access controls for less sensitive applications and regular users.

Deployment approaches

It is not enough to check a box for core security capabilities by relying on minimal features —products and services need to be assessed against real needs and threats.

As security teams look to establish a comprehensive, unified approach to security across all their distributed environments, they must address key questions within each of the primary security areas:

- **Data encryption.** Who provides the protection: the organization, the CSP, or a managed security service provider (MSSP)? Are protection mechanisms employed at the application level or infrastructure level? How is encryption supported upstream and downstream from the cloud environment?
- **Key custodianship.** Where are the keys stored: in the key vault of the CSP, or a centralized enterprise key management system controlled by the customer (whether on-premises or in the MSSP's cloud)? How secure are the key storage platforms?
- **Access control.** Does the customer or the CSP define and enforce access control policies? Are the CSP's identities used or are the customers' single sign-on mechanisms employed? Under what conditions is MFA being used? Are context-based adaptive access policies evaluating risk conditions continuously and enforcing authentication where needed?

These questions are imperative as decision-makers consider which specific approach to pursue. In the following sections, we offer a high-level overview of six potential deployment approaches that can be adopted.

Approach #1: Customer manages data protection

In IaaS environments, customers can establish a high level of control over the underlying infrastructure. With today's solutions, customers have a range of options in terms of where they house their key management capabilities and their access security and authentication, including on-premises, in a private cloud, at a trusted third-party service providers' facility such as an MSSP, or in an encryption vendor's environment. When running workloads in an IaaS environment, security teams can retain the key management and access security and authentication capabilities outside of the cloud environment that hosts the applications.

Advantages

From a security standpoint, teams can do everything they are accustomed to in managing their on-premises environments while leveraging the benefits of cloud and other service provider models. Because policies for access controls, encryption, and key management and keys remain in the customer's control, this approach helps security teams apply stricter authentication to guard against the risks posed by admins and privileged users in the cloud provider's environment. In addition, this approach offers a way to address an organization's compliance mandates, including any data residency requirements that may be in effect. Once data is encrypted, it can be moved to multiple environments and geographical regions, but the keys used to encrypt and decrypt the data can remain in a central region, always under the organization's control.

Approach #1 At a glance

Cloud environment: IaaS

Approach:

- Key management and root of trust remain under customer's control.
- Access security and authentication at the login point for admins remain under customer's control.

Approach #2: CSP-provided encryption

Compared to IaaS environments, customers have fewer options for establishing security controls in PaaS environments. In these cases, customers can use the encryption mechanisms offered by PaaS vendors, while instituting some levels of control over keys. Within this high-level approach, security teams can choose from:

- Bring your own key (BYOK). In this case, the customer generates the encryption keys and provides them to the CSP. The CSP manages the keys within its key vault.
- Hold your own key (HYOK). Here the customer generates and holds the encryption keys for their cloud data. Organizations have full ownership and sole control of encryption keys while leveraging cloud services.
- Control your own Access Security and Authentication. Here a customer owns and controls their IAM instead of relying on the CSP. Organizations have full ownership and sole control of their identity and access management.

Advantages

Through this key management approach, customers can define and upload master keys, and in some cases, associated key management and encryption policies, while leveraging the key management and encryption capabilities offered by the CSP. In this way, security teams can start to implement uniform controls across multiple clouds. Teams can also strengthen security by setting and enforcing policies around key rotation and expiration.

Through the shared responsibility approach, customers control their IAM, reducing the threat surface, avoiding "threat inheritance," reducing the risk of third parties accessing their data, and ensuring directory flexibility. Security teams also implement uniform controls across multiple clouds with a consistent login experience for customers and Admins, and stricter authentication as needed.

Approach #2 At a glance

Cloud environment: PaaS

Approach:

- Customer generates keys, while CSP manages keys and encryption.
- Customer enforces access security and authentication at the login point for admins and users.

Approach #3: Key broker services

Today, many SaaS vendors and independent brokers offer cloud-access security services that include key management and brokering options. Organizations can employ these services while managing keys in their own central key management platform.

Advantages

With this approach, customers can leverage all the benefits of SaaS offerings, while retaining control over who can access the data held in these environments. Customers can set and enforce key management policies across the key management lifecycle. This approach offers a range of protections. For example, even if the SaaS provider is subpoenaed, the customer can still retain control over whether data is disclosed.

Approach #3 At a glance

Cloud environment: SaaS

Approach:

The customer uses a key broker service offered by a third-party vendor such as an MSSP or SaaS vendor.

Approach #4: Double key encryption

Cloud Service Providers work together with third-party security vendors to enable organizations to protect their most sensitive data while maintaining full control of their encryption keys. The solution uses two keys to protect data. One key is in the customer's control in a certified root of trust and a second key is stored securely at the CSP.

Advantages

Both keys are required to access protected data, ensuring that CSP and other third parties never have access to the protected data on their own. Organizations in highly regulated industries such as financial services, government, and healthcare can comply with regulations such as GDPR, HIPAA, and Schrems II.

Approach #4 At a glance

Cloud environment: All

Approach:
Customers have sole control over who has permission to access keys to decrypt protected data.

Customer held keys are maintained in the customer's environment and remain separate from the CSP.

Approach #5: Authentication everywhere

Cloud Service Providers and third-party security vendors provide services to enable organizations to protect their most sensitive data. It is the customer's responsibility to understand their security landscape, plug all authentication gaps and make sure all apps are protected with authentication.

Advantages

The authentication everywhere approach is relevant for all types of cloud environments, offers the benefit of consistent protection and user experience for all apps, leverages existing on prem solutions as needed, and does not require rip and replace.

Through the shared responsibility approach, customers control their IAM, reducing the threat surface, avoiding "threat inheritance," reducing the risk of third parties accessing their data, and ensuring directory flexibility. Security teams also implement uniform controls across multiple clouds with a consistent login experience for customers and Admins, and stricter authentication as needed.

Approach #5 At a glance

Cloud environment: All

Approach:

The customer plugs all authentication gaps and makes sure all apps are protected with authentication regardless of the IDP and SSO solution deployed.

Approach #6: All of the above

Through utilizing this approach, customers can employ centralized key and access security management to control data, access and authentication across all their hybrid cloud deployments.

Advantages

Through this approach, organizations can realize the benefits of centralized controls, including centrally and uniformly defining and enforcing policies for access controls, encryption, and key management, and securely managing keys throughout their lifecycle. At the same time, organizations can adapt approaches to fully capitalize on the specific options and advantages offered by various cloud vendors and models.

Through the shared responsibility approach, customers control their IAM, reducing the threat surface, avoiding "threat inheritance," reducing the risk of third parties accessing their data, and ensuring directory flexibility. Security teams also implement uniform controls across multiple clouds with a consistent login experience for customers and Admins, and stricter authentication as needed.

While cloud services offer compelling advantages to organizations pursuing digital transformation objectives, they also pose unprecedented challenges from a security and compliance standpoint. By employing the approaches above, organizations can establish the capabilities required to maximize the benefits of a range of cloud services and models, while addressing their critical compliance mandates and security objectives.

Approach #6 At a glance

Cloud environment: All

Approach:

Customer establishes central key and access security management that is used to control data, access and authentication across all cloud models and vendors.

Cloud security methodology

As IT and security teams map out their cloud security strategies, they should go through the following steps:

1. Identify sensitive data and applications and where they reside

Start with a complete, current picture of all the enterprise's sensitive assets, including private employee and customer records, intellectual property, financial records, account information, and more. Also determine exactly where these assets are located, including the physical location and the type of environment.

2. Determine the risks

For each sensitive asset category and location, delineate the specific risks they are exposed to. Determining vulnerabilities to external cyber attackers as well as to privileged users. Ascertain any compliance risks as well.

3. Understand the level of data control by deployment type

Ensure approaches are aligned with the specific characteristics of the deployment environment and model. For example, if pursuing a host-your-own-key approach in a PaaS environment, specify what types of key management policies can be attached to keys being delivered to the PaaS vendor.

4. Define an overall cloud strategy

Whether your organization has a cloud-first strategy, is mostly on-premises, or is using hybrid environments, it's important to define the overall security strategy and ensure it crosses all environments and platforms, etc. Once the strategy is established, evaluate and deploy the right level of security for different assets based on sensitivity, privacy, risk, etc.

5. Establish an approach for centralized custodianship of keys, access, and policies

Depending on the organization's existing IT landscape, as well as its security and business objectives, the specifics of the security posture may vary. However, organizations will be best served by establishing a central key management and access management solution that will help predict, prevent, and respond to dynamic cybersecurity threats. This could be an on-premises, in the cloud, or hybrid combination that best meets their needs. As long as the solution is centralized, the organization can ensure continuity and consistency throughout.

6. Deploy the best available controls

Based on their current environment, IT and security teams will need to establish a mix of controls that optimize and deliver security and operational efficiency. As outlined above, encryption, key management, and access control capabilities will need to be managed in an increasingly centralized, unified manner.

7. Monitor the evolution of cloud capabilities

The cloud services market is seeing rapid innovation, and the number of vendors and offerings continues to proliferate. Once organizations have established an optimal approach to cloud service usage and security controls, it will be important to stay abreast of market evolution. This should include regular monitoring of existing vendors to make sure decision-makers are apprised of new capabilities and offerings that become available. Executives should also monitor the market more generally to identify new vendors and offerings that may deliver compelling advantages, whether from a security, efficiency, or cost-savings standpoint.

How Thales solutions can help

Thales offers an integrated, comprehensive set of solutions that deliver central, unified, and efficient capabilities for securing apps and data across all environments, including on-premises, multiple clouds, and across the entire hybrid IT landscape. With Thales solutions, organizations can implement granular information security controls that optimize the availability, integrity, and confidentiality of sensitive digital assets.

1. Discover all sensitive data

Usually, the first step in a data security strategy is finding sensitive or regulated data. This can be particularly difficult in a multi-cloud environment, where the data spans platforms. CipherTrust Data Discovery and Classification, part of the CipherTrust Data Security Platform, finds and classifies both structured and unstructured data on premises and in the cloud. Without knowing what sensitive data is stored in the cloud, how it's stored, and why it's there, it isn't possible to apply effective key management and encryption policies and controls to protect the data.

2. Protect data and access

Protect data-at-rest

The CipherTrust Data Security Platform integrates industry-leading data protection solutions across a variety of data stores, platforms, and IT environments. These solutions enable security teams to apply the right security control for sensitive data in virtually any situation.

The CipherTrust Data Security Platform integrates industry-leading data protection solutions across a variety of data stores, platforms, and IT environments. These solutions enable security teams to apply the right security control for sensitive data in virtually any situation.

- **Transparent encryption**
  For data-at-rest encryption, particularly for IaaS systems, CipherTrust Transparent Encryption delivers privileged user access controls, powerful industry-leading encryption, and advanced features and extensions including detailed audit logging of data access. Transparent Encryption protects data in files, database volumes, and other repositories and enable the use of data during encryption and rekeying operations with patented Live Data Transformation.

- **Tokenization**
  CipherTrust Tokenization replaces sensitive data with a representative token so the original sensitive data remains inaccessible to the database administrator and unauthorized users. Tokenization is ideal for implementing enhanced security at a database field level when using PaaS services in the cloud. And because CipherTrust Tokenization is REST-based, it's easy to integrate into applications and cloud orchestration.

- **Application data protection**
  The CipherTrust Data Security Platform supports additional controls for data. CipherTrust Application Data Protection delivers cryptographic functions, such as key management, signing, hashing, and encryption services through APIs, so developers can easily integrate these complex operations into their applications running in the cloud or on premises, particularly at the PaaS level.

- **Database protection**
  CipherTrust Database Protection provides column-level data encryption for databases, without the need to alter code or applications. Pre-integrated solutions save customers time and effort when delivering encryption and key management for Oracle, Microsoft SQL Server, IBM DB2, and Teradata.

SureDrop is an enterprise-class, cloud-based, or on-premises solution for secure file sharing collaboration. Secure by design, SureDrop is developed for organizations that have strong security policies around file storage, but still need the productivity benefits of a full-featured file-sharing solution.

Protect data-in-motion

Thales High-Speed Encryptors (HSE) 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. Thales network encryption 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.

Protect cryptographic keys

Achieve compliance and scale to meet high-performance use cases, by confidently securing critical environments with high-assurance FIPS 140-2 Level 3-validated Thales Luna HSMs. Securing the keys for data at rest and in transit, Luna HSMs act as trust anchors to protect the master keys that encrypt your data, digital identities, and transactions. Thales offers a range of market-leading HSMs including:

- **General purpose HSMs**
  Thales Luna General Purpose HSMs are the foundation of trust for an organization's overall digital security ecosystem including devices, identities, and transactions. Thales Luna HSMs ensure the integrity of your cryptographic keys and functions, protecting them within a variety of form factors including a network-attached appliance, an embedded PCIe card, a portable USB appliance, and a Cloud HSM service. Simplify integration and development with a wide variety of APIs, superior performance, and hundreds of out-of-the-box technology partner applications to secure crypto key life cycles and operations.

- **Cloud-based HSMs**
  Thales Data Protection on Demand (DPoD) is a cloud-based platform providing a wide range of Luna Cloud HSM, CipherTrust Key Management (key broker), and payShield Cloud (P2PE) services through a simple online marketplace. Data security is now 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 reports in minutes.

Protect access to apps and privileged accounts

Thales SafeNet Trusted Access is a cloud-based identity and access management (IAM) service that acts as the trusted identity provider for public and private clouds. SafeNet Trusted Access provides the ability to securely deploy an IAM solution across an organization's entire environment, including a variety of clouds.

SafeNet Trusted Access protects cloud resources at the log-in point by using authentication, conditional access, and enforcing policy-based access controls every time a user logs into an app.

- **Policy-based access management for cloud platforms**
  You can avoid threat inheritance from the cloud by using an external IAM solution to protect your access security and authentication— you remain in control even if the cloud's back end is breached. An added benefit of using an external IAM service is that by segregating security, you can choose a solution that supports multiple clouds, so that when your business needs require support for multiple clouds, you aren't locked into a single cloud vendor.

- **2FA compliance**
  Various compliance regulations require two-factor authentication (2FA) for managing cloud resources. SafeNet Trusted Access supports a broad range of contextual and MFA methods allowing organizations to offer the right level of authentication while maintaining an optimal user experience.

- **Cloud SSO and MFA for administrators and customers**
  In addition to enabling compliance with regulations, SafeNet Trusted Access improves productivity for IT administrators and customers by enabling remote provisioning of authentication and access controls to users, wherever they reside, by providing support for Cloud SSO and MFA in public and private clouds.

3. Control data and access security

Centralized key management

CipherTrust Manager

CipherTrust Manager is the central management point for the CipherTrust Data Security Platform. It manages key lifecycle tasks, including generation, rotation, destruction, import and export; provides role-based access control to keys and key management policies; and supports robust auditing and reporting. It can run as a native virtual machine on AWS, Microsoft Azure, Google Cloud, VMware, Microsoft HyperV, and more. Additionally, native support of CipherTrust Cloud Key Manager on CipherTrust Manager streamlines key management across multiple cloud infrastructures and SaaS applications

Many cloud providers understand that customers require control of their keys, and support Bring Your Own Key (BYOK) options. While BYOK enables customers to better control their keys in the cloud, BYOK becomes a challenge with a multi-cloud strategy, given varying APIs and methods. Using CipherTrust Cloud Key Manager, security teams can manage BYOK across cloud environments from a single pane of glass.

Key management as a service

CipherTrust Key Management Services on the Thales Data Protection on Demand (DPoD) platform provide BYOK capabilities as a cloud-based service. With DPoD, you can ensure simple and secure control of your keys and related security policies for encryption within your cloud service providers, IaaS and PaaS environments, and SaaS vendors.

The key broker enables you to retain control of your keys and align your key management policies across environments. The key broker serves as a custodian of keys, providing a consolidated key management directory to manage, search, and audit all keys. Using the Key Broker, you can design and enforce key management policies, helping to ensure compliance.

Control access to apps and accounts

We recommend you control access by performing 2FA or MFA authentication using a Thales authenticator app, software authenticator or hardware authenticator used in conjunction with the Thales SafeNet Trusted Access policy-based IAM.

SafeNet Trusted Access is a cloud-based access management solution that makes it easy to manage access to both cloud services and enterprise applications with an integrated platform combining single sign-on, multi-factor authentication and scenario-based access policies. SafeNet Trusted Access provides a single pane view of access events across your app estate to ensure that the right user has access to the right application at the right level of trust.

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

Building a future we can all trust

Contact us

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

> cpl.thalesgroup.com <