thalescpl.com

THALES

Best practices for secure cloud migration

Leveraging Cloud Security Alliance security guidance

White Paper

Contents

Executive summary

This white paper is intended to aid readers in forming a cloud security strategy and data migration plan when adopting public cloud services. Security Guidance Version 4.0 from the Cloud Security Alliance offers mature recommendations for those looking to adopt public cloud services. But as the guidance offers a 'cloud agnostic' approach across SaaS, PaaS and IaaS services, the advice often lacks focus. In this paper we coalesce into actionable advice recommendations across disciplines and customer use cases, paying particular attention to data protection and encryption key management.

Introduction

Organizations of every size from every vertical – including government agencies from local to federal level – are moving all or part of their workloads to public cloud services. The revenue growth for the major cloud providers reflects this modern gold rush as we see $15B and $18B annual revenues for Azure and AWS respectively.

Cloud consumers are largely past the question of whether public cloud services are secure, or if they can reasonably implement governance and regulatory controls over systems and data they bring into the cloud. Cloud service providers and a handful of their very public customers have proven that they can. But the question of how to secure systems and data persists. Given the diversity of corporate IT challenges and variety of application services they support, mapping a security strategy to cloud services is a complex task.

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing". CSA has gathered a diverse group of globally-distributed business stakeholders with deep expertise in all facets of cloud security, and from this community produced a clear and actionable set of recommendations. As companies struggle to understand migration and security for cloud, the CSA is the go-to source of information. Recently the CSA released "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0", a major enhancement to the previous edition.

However, the guidance is focused around disciplines like applications, network, legal and identity. The cloud vendors implement security as silos for individual services (e.g., file, server, database). In contrast, most customers seek cross-discipline strategies to address the use cases they are most interested in, and prefer a unified model that applies wherever their data may reside. In this paper our goal is to help readers bridge these gaps, mapping the CSA guidance to buyers' most important data security challenges, and outline coherent strategies that meet their objectives.

Thales is well positioned to provide this perspective as we serve thousands of customers around the globe, and our security technologies—through our partnerships with major cloud vendors—are integrated into or available for those providers. Our products enhance cloud native capabilities, offering customers a unified security management interface for the cloud challenges they face today, as well as bringing security capabilities either not available from the cloud vendors or providing multi-cloud solutions that are not typically in the interests of public cloud provides to offer.

Section 1: Data protection use cases and CSA security guidance version 4.0

Version 4.0 of the CSA security guidance represents a significant update, reflecting the many changes in both how enterprises deploy applications and infrastructure within cloud services, as well as the advancement of security capabilities offered by cloud vendors. These changes have altered the world's perception of what is possible with cloud services. In essence, Cloud offers the world new architectures, operational models, and tools designed to work in these elastic, on-demand, API-driven environments.

Security should be viewed as an extension of these same fundamentals. Security Guidance v4.0 reflects real world changes in how we automate and orchestrate security, and a mature view of how to blend cloud native and third party security technologies to meet regulatory, data governance and security challenges. Thales believes our delivery of an integrated data security solution meshes with the guidance, with technologies, architectures and operational models that work equally well across Software, Infrastructure and Platform services.

The following are sample use cases and pain points cloud customers most commonly communicate to our systems engineers and professional services advisors. In each one, we note sections of security guidance that pertain. For each use case potential Thales data protection solutions are suggested. It is helpful to have open a copy of Security Guidance v4 while you read this paper. You can download at: cloudsecurityalliance.org/guidance/#_overview.

Thales cloud data protection solutions overview

To understand references to products in this paper, here is an overview of Thales cloud data protection solutions:

Many Thales cloud data protection solutions are components of the Vormetric Data Security Platform. The Vormetric Data Security Manager, at the core of the platform, provides centralized encryption key and encryption policy management for these components of the Vormetric Data Security Platform:

- Vormetric Transparent Encryption offers advanced file-and volume-level encryption deployable from on-premises through hybrid cloud for IaaS. It provides privileged user access controls, container-aware data protection, security intelligence through data access logging, and Live Data Transformation, which enables use of databases and file systems while they are undergoing encryption.
- Vormetric Tokenization with Dynamic Data Masking and Vormetric Application Encryption enable data protection higher in the computer stack, are cloud-friendly and are compatible with cloud database user-defined functions (UDFs).
- The CipherTrust Cloud Key Manager offers centralized, multi-cloud key lifecycle management for IaaS, PaaS and SaaS providers that support bring your own key (BYOK) capabilities.

How do I extend my existing security and data controls to the cloud?

Security Guidance

Beyond managing risk through contracts (Section 2.1 Data Governance), you can exercise control over your data stored within cloud resources. Several cloud services are intended to overlap or replicate from your on premise systems to cloud services, allowing for greater consistency in management and data governance. Identity Management is central to this approach, with Domain 12 of the guidance outlining strategies for replicating or sharing identities, as well as access control options like Single Sign-On and Federated Identity across cloud providers. Supplementary controls over data access are provided by BYOK; you can import your own keys into software based key management systems, or into dedicated Hardware Security Modules provided by the cloud vendor.

Relevant Thales solutions

The CipherTrust Cloud Key Manager from Thales offers:

- Multi-cloud key management with SSO
- FIPS-140-2-compliant key generation and storage
- Per-cloud-provider key activity logging in support of domain 4

In addition;

- Vormetric Transparent Encryption provides data access logging aggregated by the Data Security Manager
- Vormetric Tokenization Server logs activity to a local or remote syslog server

Both logging systems can be forwarded to any Security Information and Event Manager (SIEM).

How do I protect data as I move and store it in the cloud?

Security Guidance

There are three basic strategies to accomplish this: Encrypt data prior to transport, use encryption with both transport and storage services, or use data-centric security. Subsection 5.1.2 of the guidance is meant to show how each of these strategies work when moving—and using—data in the cloud. The idea is that you want to define your data governance strategy, and understand the tradeoffs of these methods, prior to implementation. Section 11 of the guidance discusses the specific technologies to support each of these strategies. If you choose to encrypt prior to moving data to the cloud, or have an enterprise-wide encryption solution in place, you'll either want to mirror on-premise keys and encryption capabilities for data access in the cloud, blend on-premise with cloud native services, or bring your existing encryption to the cloud in place of cloud native services. If you choose to encrypt at the services layer, for transport (e.g., TLS, VPN) and data storage (e.g., volume, object, database) you can leverage cloud native capabilities or your preferred encryption solution to secure each service that data comes into contact with. Data centric security tools like masking and tokenization can transform data prior to cloud migration.

While some static masking solutions are non-reversible, if you need to reverse tokens into original data values, you will either need to do so on-premise or bring your existing tokenization service to the cloud for de-tokenization requests. But any of these three approaches will provide secure transport and storage of data, and can be used to replicate information to multiple cloud service models.

Relevant Thales solutions

If your on-premises key and encryption capabilities are based on Vormetric Transparent Encryption from Thales, you can readily mirror those capabilities by bringing your own encryption (BYOE) to public cloud providers, or request encryption services based on Vormetric Transparent Encryption from any of nearly 30 cloud services providers worldwide.

Vormetric Tokenization or Batch Data Transformation can both mask data prior to migration to the cloud or in the cloud. Further, dynamic data masking -- that is, masking content dynamically based on user, group, or role, based on, for example Active Directory or LDAP entries, enables masking or presentation of different data fields, or section of data fields, to different users.

How do I ensure the cloud provider does not access my data?

Security Guidance

Most cloud providers are just as fearful of rogue administrators accessing your data as you are, as this type of 'Black Swan' event could severely affect their reputations and valuations. As such they go to great lengths to ensure their administrators cannot access customer data, encryption keys and systems without prior approval and full audit controls. But it remains a risk, however small. More probable is the risk that the cloud vendor be compelled to provide access under court order described in Domain 3: Legal Issues, Contracts and Electronic Discovery. Your Risk Management (Domain 2) and Information Governance (Domain 5) plans will need to account for these risks. For extreme cases where you must minimize or exclude all access by the cloud provider or hostile external parties accessing your information, combinations of cloud services, bring your own encryption, and data management controls such as tokenization with data masking as a form of data redaction, can provide full segregation and protection.

Most Infrastructure as a Service providers now offer—at an added expense for compute nodes—'Trusted Execution Environments'. Code and data are passed fully encrypted to these servers, and only decrypted below the hypervisor layer, as it's loaded into secure hardware, so no other processes may examine—or alter—the data or code.

Couple trusted execution with the ability to either bring your own encryption, bring your own keys (e.g., BYOK for SaaS, PaaS, IaaS as described in Domain 11) and key management (e.g., Bring Your Own Encryption for PaaS/IaaS as described in Domain 10 and 11) software, you have full control over data storage and data in use.

Relevant Thales solutions

As noted in Security Guidance, either bringing your own encryption or managing your own keys is a solution for the black swan or subpoena event, with varying effectiveness:

- If you bring your own encryption to the public cloud, then by definition you have 100% control of your encryption keys
- You can bring your own keys to public cloud providers, discussed below. This protects your data from the cloud provider and subpoena issues to the extent discussed at left
- If you purchase advanced encryption from a Thales Service Provider Partner, their architecture may determine your control of encryption keys. Vormetric Transparent Encryption enables service providers to devolve key management to each customer

Can I use my own encryption keys in the cloud? Is BYOK an option?

Security Guidance

The short answer is "Yes you can". Many major SaaS, PaaS and IaaS vendor offers the ability to import keys from your on-premises HSM into a key vault or cloud HSM, fully described in Domain 11. The level of integration varies between cloud vendors and whether or not you opt for on-premises or cloud HSMs. You may need to manually perform the import, but you are provided up to FIPS 140-2 Level 3 security. From there the cloud provider derives keys from the master key you imported to encrypt data contained in various services (e.g., object, volume, database).

Relevant Thales solutions

The CipherTrust Cloud Key Manager provides full key lifecycle management for a growing list of IaaS/PaaS and SaaS providers and solutions. Key sourcing and storage is available in up to a FIPS 140-2 Level 3-certified appliance, or fully in software with FIPS 140-2 Level 1 certified virtual appliance.

How do I enforce data residency policies, and specifically, comply with GDPR?

Security Guidance

The guidance dedicates a significant portion of Domain 3 (Legal Issues, Contracts and Electronic Discovery) to outline your responsibilities for EU security concerns in general and GDPR compliance specifically. This will provide a good roadmap of what data you need to account for and what controls to implement. We recommend that the basic controls you use for any Personally-Identifiable Information (PII)-regulated data controls are a good place to start with GDPR as the controls and types of data are similar. This is briefly discussed in Domain 11. We also recommend use of Identity Management, encryption and key management for multiple mechanisms to enforce the Cross-border Data Transfer Restrictions, so in the event data is moved, it can be rendered inaccessible. You will need to collect both cloud logs for access controls, as well as the logs from your own applications and services, to fulfill your requirement on Accountability. The guidance has extensive comments on what logs to collect, and how to create secure logging architectures and monitoring behavior from logs in Domain 7 (infrastructure Security), Domain 9 (Incident Response), and Domain 10 (Application Security).

Relevant Thales solutions

Thales solutions including advanced encryption and tokenization enable effective, simple-to-deploy solutions for GDPR articles 32 and 34 related to:

- Pseudonymisation and encryption of personal data
- Assessing the effectiveness of your security measures
- The unauthorized access to personal data
- Crypto-shredding with key revocation

As mentioned above, Thales encryption and tokenization solutions offer a range of data access logging for integration with SIEM systems. The logging mechanisms in the Vormetric Data Security Manager, Vormetric Transparent Encryption Agents, and Tokenization server support monitoring architectures as described in Domains 7, 9 and 10.

How do I track and monitor data access and usage?

Security Guidance

Monitoring is another topic discussed in almost every domain of the guidance, but very few concrete examples of how to accomplish monitoring are provided. Also unstated is that logging capabilities are somewhat new for most public cloud vendors, and monitoring these logs for security related events or compliance reports is decidedly nascent. Cloud vendors are getting better at it, but the log files seldom represent a full picture of activity. Be realistic: If you want to monitor in the cloud, you will need a blend of cloud and third party tools. The primary need is to collect a combination of the service logs and the identity logs provided by the cloud, in addition to log files from the servers, containers and applications you run. That means you will need to leverage all sources, and possibly even use a data warehouse or logging tool to supplement event storage.

The good news is that some of the clouds now provide the ability to filter and route the events they generate, and they offer the ability to create basic security policies that, in effect, monitor cloud events, and provide alerts when conditions are witnessed within the logs. Again, these are basic monitoring capabilities, and it is likely that you will either need to move a portion of the log data back on premises to monitor, alert and generate reports or create that infrastructure in the cloud. It is common to see application logs, syslog and web gateway events all streamed to a Hadoop cluster, Elastic Stack, Splunk or even SIEM installations running in the cloud. These installations then leverage the same reporting and analytics capabilities used on-premises and provide a consistency of reporting.

Relevant Thales solutions

As part of any comprehensive logging strategy as suggested by Security Guidance, one benefit of bringing your own encryption to the cloud with Vormetric Transparent Encryption is its comprehensive data access logging which, combined with supported SIEM solutions, becomes, effectively, an additional layer of security intelligence.

Similarly, applications utilizing Vormetric Tokenization can themselves log activity, or the Tokenization Server can provide logging to SYSLOG and whence to SIEM.

Finally, applications written with Vormetric Application Encryption can log their activities to SYSLOG and whence to SIEM.

Can I secure containers in the cloud or across different clouds?

Security Guidance

Container security is covered briefly Domain 8 (Virtualization and Containers), specifically in section 8.1.4. It touches on four areas—infrastructure security, management plane, image repository and container content security. Infrastructure is critical as a poorly secured OS allows access to all data and secrets on a server, or even take control of the server itself.

Container management is typically performed by what are called 'Orchestration Managers', the most common of which are Kubernetes and Swarm; both are non-cloud native and, unfortunately, very insecure by default. Bootstrapping new containers requires issuing credentials and secrets to access data needed to operate. Image repositories, both from major vendors and cloud native systems, do provide secure image stores as well as digital signature capabilities to ensure container images have not been tampered with.

Again, unfortunately, the guidance gives you a few road signs directing you to areas that need attention, but lacks tools and specifics instructions. To close these gaps the guidance recommends leveraging secrets management technologies to issue credentials to containers at runtime, and transparent disk or file encryption to store sensitive data only accessible by the containers you deem appropriate. The guidance also recommend leveraging code/container signature systems provided by the container repository, and enforcing that the container orchestration system can only use approved containers in the registry. And if you specify your own OS to run containers atop, just as Domain 8 advises for virtual servers, you need to spend considerable time making sure the OS is a secure variant configured for container use. Cloud Identity and Access controls will gate who can access or administer both the containers and the surrounding container infrastructure and security tools. The cloud vendor will offer logs for access which you can bundle with orchestration logs to examine activity.

Relevant Thales solutions

Per Security Guidance recommendations, Thales offers unique in-container security for data at rest. Supported container environments include Docker and Red Hat OpenShift. Vormetric Container Security is an extension to Vormetric Transparent Encryption that extends the feature set from files and volumes to the interiors of containers. When configuring Vormetric Transparent encryption, the administrator can apply specific encryption and data access policies on storage objects in each container.

The benefits of container security in the cloud are the same as for files and volumes: centralized, multi-cloud security with data access logging, granular controls and both data and container portability across cloud vendors.

Section 2: Cloud migration risks and potential mitigations

Mapping typical use cases to the Security Guidance book is important because the guidance offers a balanced perspective, disassociated from cloud service vendors' financial goals, which may not be consistent with your best interests. Cloud vendors operate in an increasingly competitive market. They have addressed most security and compliance impediments which hindered customer acceptance, and are now seeing rapidly increasing adoption rates. Fierce competition has erupted to land customers quickly. In some ways this benefits customers directly (e.g., driving prices down), but also presents the primary risk to customers: that cloud vendors underplay cloud migrations challenges. Most advise customers to simply mirror their on-premises environment into the cloud, using the same in-house architecture and security. This "Lift and Shift" recommendation is attractive, making the cloud feel comfortable and familiar, but neither reduces costs nor improves security. In reality the cloud can offer better security at a lower cost, but requires a degree of re-architecture and re-imagining security controls to meet both goals.

As another mechanism to utilize Security Guidance v4.0, here is a checklist of cloud migration risks that are common running themes and apply to most—if not all—sections.

Vendor lock-in: Lock-in is a reality with cloud services. While PaaS and IaaS vendors offer similar features (e.g., storage, compute, virtual networking, functions, container support and so on) each native API is proprietary. You can architect applications (e.g., abstraction layers, generic terraform templates) and leverage 3rd party technologies (e.g., bring your own encryption (BYOE) (and keys), bring your own keys (BYOK) key management, or Kubernetes container orchestration) for cross-platform services, but a certain amount of lock-in is unavoidable. Thales can help you manage many of the challenges of vendor lock-in and embrace a cost-effective multi-cloud strategy.

Lift and shift: Cloud vendors encourage you to embrace the cloud, and to make it seem less daunting, claim you need only to "lift and shift" your existing IT systems to the cloud. The guidance repeats that lift and shift is a bad idea. That's partially because if your internal security is bad today, don't be surprised that it's still bad when you move it to cloud. But beyond bringing your existing problems with you, this approach fails to leverage native cloud security, elasticity and resiliency features. Thales, or many of our Cloud Service Providers worldwide, can assist you in avoiding, or perhaps making the best of, "lift and shift."

Shared responsibility: This is a key focus of Security Guidance 4.0 as it is important to understand where your security responsibilities begin (and end), and that you should avoid outsourcing data governance responsibilities or think the provider will do this for you. Carefully review vendor-published security controls and service level agreements. Depending upon the cloud service, you're likely to be surprised what vendors do not provide; for example, some will not share events logs to support Incident Response. Any item not clearly spelled out in documentation must be remediated through contracts in order to address risks. Anything outside cloud provider stated security coverage is your responsibility. We find ourselves reminding customers that data security responsibility is in their hands, even with cloud-native encryption, because everything that occurs in cloud compute instance operating systems, is in their, not the cloud vendors, hands. Paraphrasing an Amazon Web Services blog: Cloud vendors [Amazon] are [is] responsible for security of the cloud and customers are responsible for security in the cloud. Other public cloud vendors have similar discussions of shared responsibility.

Multi-account issues: The guidance advises using many different user accounts to support cloud operations, specifically segregation of accounts for administration, development, quality assurance and IT job functions. Part of this recommendation is because cloud accounts are free of charge; you pay only for the resources you consume in each account. Another part is because it's a great way to compartmentalize users and job functions, making it easier to secure, easier to audit and easier to remediate in the event of an account compromise. But this creates new problems in sharing of user certificates, identity tokens, encryption keys, and other sensitive information. But you can find exceptions with third party solutions. For example, if you "Bring Your Own Encryption" with Vormetric Transparent Encryption, you can centrally manage it across any number of accounts – or even across multiple clouds, with the Vormetric Data Security Manager. Similarly the CipherTrust Cloud Key Manager from Thales can manage encryption keys for vendor-provided encryption across key vaults, accounts and even clouds.

Hybrid cloud: The reality is most organizations will run in a hybrid cloud model for some time, with public cloud supplementing on-premises IT. It's important to ensure connections to cloud services are secure, and should not form a bridge (i.e: effectively flatten) your network. But the guidance puts significant focus on meeting compliance and use of customer managed keys as a common root of trust across clouds. And for many users of the guidance, moving to the cloud does not obviate the need for FIPS 140-2-compliant hardware support for encryption and key management operations. Many cloud providers now offer some form of access to HSMs in the cloud, allowing you to meet compliance mandates and bring your own keys to the cloud. And this is an area where Security Guidance fails to recognize, again, Bring Your Own Encryption, which offers FIPS 140-2 secure key storage combined with advanced encryption, seamlessly from your premises to the cloud.

Unintentional data availability: New cloud customers are typically not familiar with cloud native functions, how they work, or their default settings. For example, many firms had sensitive data 'leaked' as they assumed AWS S3 'buckets' were private, when in fact the default setting was publicly available. And with powerful orchestration and automation capabilities, it is quite easy for well-intentioned administrators to automate database and disk backups, which automatically move all private data to a publicly available storage medium. Great care must be taken to ensure that repositories are secure and private prior to moving data into them. Thales can help with many of the challenges that cloud users face in this regard: First is S3: Encryption for S3 applies to the data stored within the service, not when it is extracted or copied. However, as S3 permissions and encryption capabilities are confusing, with misconfigurations resulting in high profile breaches, it's a best practice to encrypt content before it is moved into S3. This ensures data is protected even if it is replicated across regions or copied to different storage mediums. A potential solution for protecting S3 storage buckets is to leverage the Amazon Storage Gateway in combination with Vormetric Transparent Encryption. The Storage Gateway can present S3 buckets as NFS or SMB "mounts". Any Windows or Linux Server, in cloud or on premises, equipped with a Vormetric Transparent Encryption Agent, can apply advanced encryption and comprehensive data access controls on S3 buckets. Turning to backups: an optional feature of Vormetric Transparent Encryption (bring your own encryption) provides for automated key versioning coupled with data rekeying (decrypting with the old key and re-encrypting with new key). But backups are occasionally not "live", so they can't be rekeyed. No problem: when the backup set is brought "live", we read the key version, retrieve the key from the DSM, and can decrypt the backup with a key that could be many versions back.

Data residency: The General Data Protection Regulation (GDPR) from the European Parliament and Council has brought new urgency to data privacy and a real-world examination of what data residency means and how to meet these requirements. The guidance discusses data privacy in most sections, and dedicated most of another to GDPR. While data management requirements for GDPR are both complex and company specific, most existing data protection programs built atop encryption, tokenization and good logging will meet both PII and data privacy sections of GDPR. Additionally, key management controls can ensure that encryption keys—and by proxy decryption or cyber-shredding of sensitive customer data—are only available in specific geographic regions to ensure compliance. Thales has been readying customers for GDPR for several years, and, as discussed above, offer encryption, tokenization and key management solutions that fulfill many GDPR data residency and privacy mandates.

Key ownership and access: There remain both trust and privacy concerns around key usage in cloud services. Domain 11 of the guidance focuses on Data Security and Encryption, but does not cover some of the concerns voiced regarding cloud vendors—perhaps compelled by legal order—accessing customer encryption keys. Major cloud service providers offer key management and elastic HSM support. Vendors can access keys in the native key management system; they cannot access keys in the HSM. But the difficulty comes from this: All key operations are performed on derived keys, so even if customer root keys are protected, some of the derived keys may be accessed by the cloud provider. For customers who feel at risk in this area, they can optionally bring their own encryption, and therefore keys, to the cloud.

Data centric security: Cloud vendors offer security features built into services, and focus on protecting the service, not the data. Data Centric Security ensures that data is protected regardless of underlying cloud security. In fact no cloud vendors provides tokenization, format preserving encryption or masking technology. The guidance notes these technologies as both very useful in augmenting cloud security, but should be foremost considerations when a service cannot meet your security, privacy or regulatory requirements.

For these reasons the new Cloud Security Alliance Security Guidance book, offering a cloud neutral security recommendations, is essential for customers who are considering, or who have already, moved to public cloud services.

Appendix A: How the Thales product suite meets guidance

Security Guidance 4.0 covers 14 different domains of cloud security, offering a very broad set of security disciplines to consider. To help the reader focus on how Thales can aid transition to public cloud and offer both complementary and unique capabilities, in this appendix we outline specific products that address 4.0 recommendations. While we offer products and services applicable to all domains, this appendix focuses on specific capabilities within the broad eco-system of security tools and technologies.

One quick consideration before we dive in: The CSA offers tools beyond Security Guidance such as the Cloud Controls Matrix (CCM) and Consensus Assessment Initiative Questionnaire (CAIQ), which themselves are essential for creating security and compliance requirements for cloud deployments. Version 4.0 of the CCM and CAIQ will be released mid-2018, at which time we will provide updated mapping to these new compliance and security frameworks. As the latest version of Security Guidance is a significant step forward and upon which this paper is based, we forgo mapping Thales solutions to the CCM and CAIQ until the newest versions of those documents are available.

Thales products aid users in cloud security and operations in the following domains:

Domain 4: compliance and audit management

Summary of Domain 4 Domain 4 focuses on the need for compliance as a means to validate awareness of—and adherence to—corporate, contractual and regulatory obligations. Audits are a key tool for proving (or disproving) compliance, and supporting non-compliance risk decisions. That said, the logging and reporting capabilities for public cloud offer a different, and often incomplete, picture of activity. While some issues can be mitigated through contract negotiations and risk reduction strategies, to provide full audit reports, you'll need to supplement cloud native logs with application layer logs for critical applications and data usage.

Thales solutions for Domain 4 Thales solutions offer logging features in support of audits or compliance assurance. The Vormetric Data Security Manager provides detailed logs. This means all key management functions and administrative actions, commonly central audit areas of interest, are logged. Customers can configure the DSM to deliver their audit logs to their SIEM, security analytics or general logging platforms. The previous two logs could be considered "management plane" logs. In addition to those, Vormetric Transparent Encryption can be instructed to log increasingly detailed data access logs, which are aggregated and de-duplicated by the DSM. These "data plane" logs detail when users and applications access data, under what policies the requests were handled, and if access requests were permitted or denied. The logs will even expose when a privileged user submits a command like "switch user" in order to attempt to imitate another user. Aggregating data plane logs across multiple hosts and correlating in a SIEM can enable very early detection of an infection spreading horizontally in a cloud.

Domain 5: Information governance

Summary of Domain 5 Information Governance is one of the more complex subjects covered in the guidance. It covers a myriad of concerns including data ownership, multi-tenancy, jurisdictional constrains on how data is secured, data privacy and proper methods to destroy unused or unwanted data. The guidance provides an entire Data Security Lifecycle to show how to meet data governance concerns under every possible use case, from creation to destruction.

Thales solutions for Domain 5 There are several technologies that address security and privacy concerns in all phases of the Data Security Lifecycle, such as data encryption, tokenization and data masking. By obfuscating data and only exposing the original values to fully authenticated users, these technologies address every phase of the lifecycle by securing data in use, at rest, as it is shared, archived and destroyed.

The Vormetric Data Security Platform from Thales provides encryption, key management, tokenization and dynamic data masking to tackle all of these challenges. The platform's architecture enables customers to implement their own security policies and address Security Guidance recommendations, for databases, files and big data nodes in private, public, or hybrid cloud environments as well as on-premises.

While data encryption provides solid protection against disclosure of data, regardless of where that data may reside, data encryption keys remain a challenge for data stored in the cloud. The main risk of utilizing vendor-provided encryption is key management. Bring Your Own Key (BYOK), supported by the CipherTrust Cloud Key Manager, is a good first step in ensuring security for encrypted data. Bring Your Own Encryption (BYOE), provided by Vormetric Transparent Encryption and the Vormetric Data Security Manager, provides in-depth controls that reflect more Security Guidance requirements such as data access controls as defined in Domain 5 functions, actors and controls. Using BYOE, customers define which user accounts and applications can access data, what particular data they can access, when they can access it, and in what manner or form. Access rights are enforced for all users, even for those administrators with root-level permissions. And data access control is performed within the operating system, integrated with AD or LDAP controls. Control in the operating system is critical, in that vendor-provided encryption occurs **below** the operating system, presenting clear text to the operating system. Since infections exploit operating systems and applications, and the shared security model stops below operating systems, it becomes almost imperative to BYOE.

BYOK and BYOE deliver data protection and segregation at multiple levels to safeguard and ensure the confidentiality of your data. By ensuring the segregation of data, duties, encryption keys, and management of the encryption solution, Thales provides controls that address data governance and data privacy requirements.

Finally, Thales BYOK and BYOE solutions enable cyber-shredding. Customers can destroy any of their own encryption keys. By doing so, they effectively remove the ability of anyone to decrypt and access the data associated with those keys. Data that is misplaced or inadvertently copied remains inaccessible once the encryption keys have been destroyed.

Domain 8: virtualization and containers

Summary of Domain 8 Cloud services, public or private, all leverage virtualization technologies to promote elasticity and multi-tenancy. In addition, most public clouds offer support for running your own applications and services within containers. These technologies are key to cloud services, but change the threat landscape when compared to their physical 'bare metal' counterparts. Public cloud security for compute, storage and networks are handled by the cloud vendor. For containers however, it's still the early days, with minimal container security from the cloud vendors. Just as important, many operations teams still do not fully understand the threats to containers, which need to be addressed.

Thales solutions for Domain 8 The Vormetric Container Security extension to Vormetric Transparent Encryption extends encryption, data access controls and data access logging to Docker and OpenShift containers used in the cloud or on-premises. The Container Security extension helps address security challenges in two ways:

- Containers often run with root level systems permissions (For Docker, by default – elsewhere, when specifically enabled), resulting in administrators having full access to container images and system data. Encryption with data access controls enables privileged users such as Docker or OpenShift cluster administrators to work as usual, without exposing sensitive information
- Encryption also aids enforcement of data security policies in dynamic container environments, especially elastic cloud services. Granular encryption in containers enables users to maximize the benefits of using them in any environment from on-premises to hybrid or public cloud, without compromising data security

Domain 10: application security

Summary of Domain 10 Domain 10 of the guidance focuses on how application security is different in the cloud, and covers how to leverage cloud native functions to address many technical challenges with application security. DevOps techniques, when leveraged in public cloud, radically changes our ability to secure applications. What the guidance does not mention is that applications remain the principal gateway and consumer of data. And as described in Domain 5, when looking at data security through the lens of the Data Security Lifecycle, leveraging encryption at the application layer tackles data at rest, data in use and data in transit by default. When the application decides what a user can access and what remains protected, you have ultimate control over data security and access policy adherence.

Thales solutions for Domain 10 You can encrypt specific files or database columns in infrastructure- or platform-as-a-service (IaaS or PaaS) environments with Vormetric Application Encryption deployed on, for example, front-end web servers. Vormetric Application Encryption is based on the PKCS#11 standard, leveraging the Vormetric Data Security Manager for secure key generation and storage. Another choice for application-layer security is Vormetric Tokenization with Dynamic Data Masking. Offering data tokenization including format-preserving encryption (FPE) along with both static and dynamic data masking, tokenization can be requested from nearly anywhere in the IaaS/PaaS stack using convenient RESTful APIs.

Domain 11: data security

Summary of Domain 1 Domain 11 is a critical section of the guidance as it's the one area that, not matter what type of public cloud you adopt (e.g., SaaS, PaaS, IaaS), data security is largely your concern and your concern alone. The vendor will focus on securing their infrastructure or platform, but the data is yours, and you need to take extra steps to secure it. The guidance again focuses on The Data Security Lifecycle as a means to understand where security controls should be implemented and prescribes a mixture of encryption, architecture and access controls as a means to protect data.

Thales solutions for Domain 11 Data security is where the full portfolio of Thales products come into play.

First, data encryption is at the heart of the Vormetric Data Security Platform. Security Guidance, the Cloud Controls Matrix, and the Consensus Assessment Initiative Questionnaire all identify data encryption as an ideal security control for data protection primarily because it is a data-centric control. Data encryption is a persistent control that remains in effect wherever the encrypted data is created, used or stored. Even in the event the encrypted data is misplaced or unauthorized copies are made, the data remains encrypted and unreadable. Thales offers a range of products that encrypt data in various places in the stack and in various ways. And it is cost effective and more importantly, multi-cloud friendly, in that key management for all encryption solutions is centered in the Vormetric Data Security Manager, which can be deployed on-premises or in popular public cloud environments. Regardless of where the DSM is deployed, if it can reach a server running either Vormetric Transparent Encryption, Application Encryption, or the Tokenization Service, data access controls and key management are simple and easy.

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@thalesesec.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: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalescpl.com <