Solution Showcase

The CipherTrust Cloud Key Manager for Multi-cloud Environments

Date: February 2018 **Author:** Doug Cahill, Senior Analyst

Abstract: The broad use of multiple cloud services, including software-as-a-services (SaaS) applications and infrastructure-as-a-service (IaaS) platforms, has become the new normal of corporate computing. Users are increasingly relying upon these cloud-delivered applications and cloud-resident workloads for business-critical purposes, resulting in sensitive data being stored across multiple public cloud environments and on-premises, resulting in both multi- and hybrid clouds. As such, the same enterprise-class data security and compliance tools and processes employed to protect on-premises data to meet and maintain compliance with industry regulations must be applied to this hybrid- and multi-cloud reality.

While many cloud services now offer native and third-party encryption options, including bring your own key (BYOK), challenges remain, such as operationalizing encryption key lifecycle management centrally, across multiple cloud services. The CipherTrust Cloud Key Manager from Thales eSecurity, offered as a service and as a customer-managed implementation, provides the ability to separate encrypted data from its encryption keys for organizations seeking the combination of compliance, enhanced security, and operational efficiency to protect data assets in a multi-cloud environment.

Compliance and Operational Key Management Challenges for Cloud-resident Data

Today, multiple IT meta trends, including mobility and cloud adoption, are simultaneously and fundamentally changing how corporate data is stored, accessed, and secured, challenging perimeter-centric security models and complicating compliance with industry regulations. At the same time, the threat landscape continues to evolve with bad actors employing new attack vectors and methods and internal threats exercising new data exfiltration techniques. But one constant remains: Security should be applied as close to the data as possible, an especially relevant consideration for data stored by cloud services in physical locations into which the customer lacks visibility and control.

Multi-cloud Adoption Increases Cloud Data Security Concerns

IT is evaluating many new projects through the lens of cloud-first initiatives, which is driving the wide adoption of cloud services. In fact, according to ESG research, 74% of IT professionals surveyed said that their organizations currently use software-as-a-service.[1] While the use of multiple SaaS applications has been commonplace for years, the use of services from multiple infrastructure-as-a-service providers has grown in popularity as well. In fact, 81% of the participants in

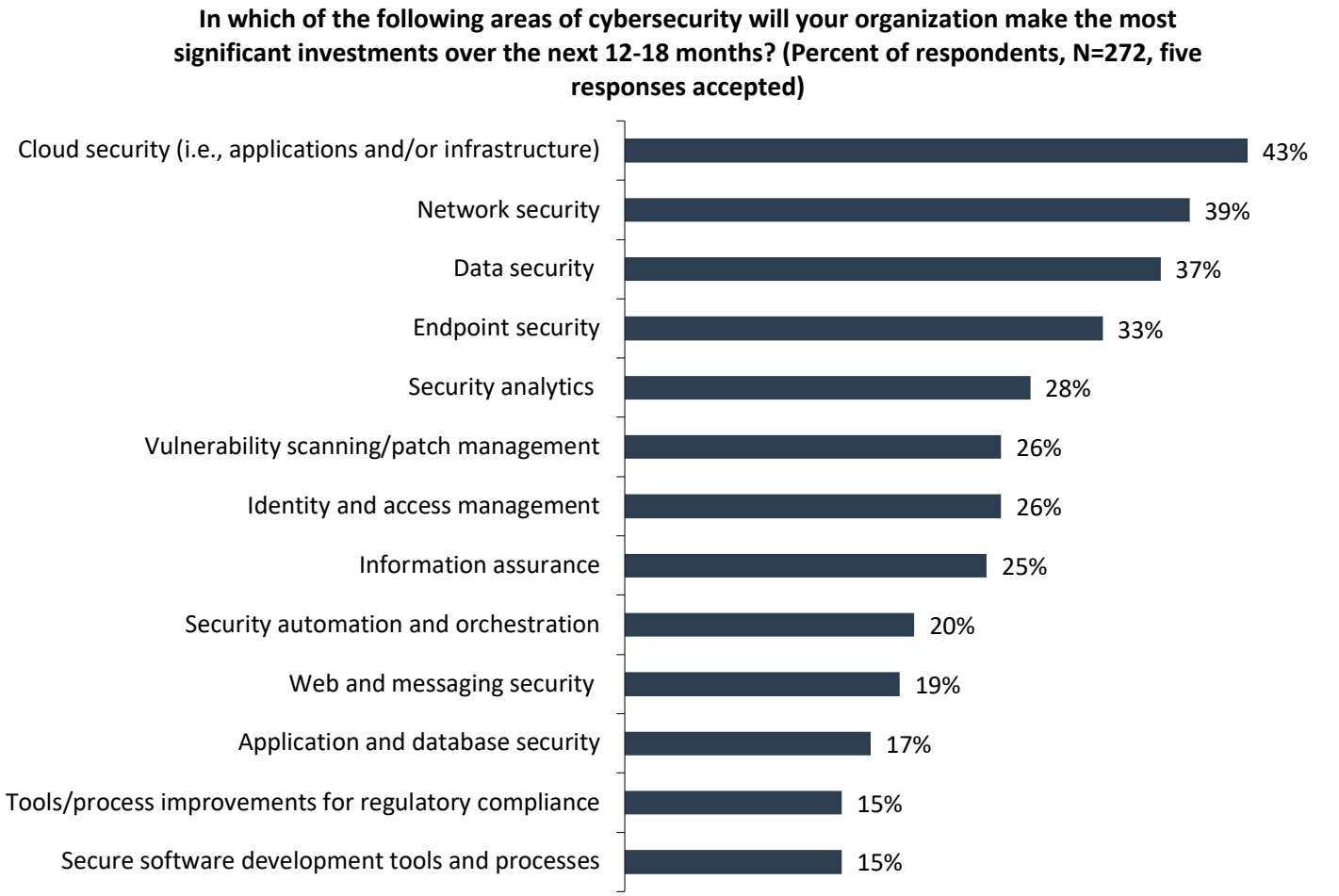
[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

This ESG Solution Showcase was commissioned by Thales eSecurity and is distributed under license from ESG.
© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

research conducted by ESG who indicated they are using IaaS services report consuming these services from two or more cloud infrastructure services providers.

This broad consumption of cloud services has created an acute concern around storing sensitive data in one or more public clouds due to its strategic and, thus, intrinsic value to a company. As such, it's not surprising that previously conducted ESG research revealed that more than half (53%) of respondents surveyed indicated they were very concerned about storing sensitive data in the cloud.[2] And in the context of multi-cloud adoption, the top challenge cited by participants in the same research was maintaining strong and consistent security *across disparate cloud computing technologies and services*. In response, according to ESG research, both cloud security and data security are two of the most commonly selected areas of cybersecurity in which organizations expect to make significant investments in 2018 (see Figure 1).[3]

Figure 1. Areas of Significant Investment Related to Cybersecurity in 2018



Source: Enterprise Strategy Group

Complicating Compliance

Many regulations are infrastructure-agnostic in that they require organizations to apply the same processes and controls independent of whether the data in scope is on-premises, in the cloud, or both. For example, PCI DSS requires dual control with respect to the separation of data and keys, as well as separation of duties in the form of role-based access to key management software. PCI DSS, along with GLBA/FFIEC and FISMA, requires the use of NIST-certified AES encryption and FIPS 140-2-compliant key management. Meeting and maintaining compliance with such industry regulations can be

[2] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.
[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

complicated by the prevalent use of cloud services. Furthermore, regional laws and regulations that govern data sovereignty and privacy, including the European Union's General Data Protection Regulation (GDPR), are increasingly relevant to conducting business internationally, typically requiring both access controls and custodianship of data and keys.

Cloudy Key Management and Custodianship

While many cloud service providers (CSPs) offer native encryption, that capability, in and of itself, does not address all use cases or compliance requirements. Co-located decryption keys provide access to encrypted data and raise questions and concerns over separation of duties, lack of dual controls between data and keys, and operational aspects of key management including key rotation, deactivation, and more. For these and many other reasons, industry best practices, such as those from the Cloud Security Alliance, simply state that encryption keys should be held remote from the cloud provider. If the CSP holds the keys, then the customer should be rightfully concerned about what happens in the case of a court serving the CSP a subpoena requiring access to the data. Key management and clarity on which party—the CSP or the customer—should be the custodian of the keys is an important factor for security professionals given prescribed guidelines and regulatory requirements.

The Requirements for Multi-cloud Key Management

Some CSPs address a subset of cloud encryption issues with bring-your-own-key (BYOK) services to give customers more control over their keys, but centralization across cloud services and additional capabilities are required.

Coverage across Multiple Cloud Services

The ongoing shortage of cybersecurity skills, and the need for the definition and application of consistent security policies and controls across disparate environments, make support for multiple cloud services a central requirement for modern encryption key management solutions. While most organizations subscribe to dozens, and often hundreds, of cloud applications, those which store sensitive data, such as customer relationship (CRM) and office productivity software, are the types of SaaS apps that are most relevant. Multi-cloud key management platforms should also support multiple IaaS platforms.

Separation of Data and Keys

Augmenting a BYOK service should allow organizations to implement the encryption best practice of separating the location of data from that of the decryption keys. This best practice of data and key separation is a compliance requirement for many industry regulations. However, such separation does not address the issue of custodianship, also a compliance requirement for some industry regulations.

Deployment Flexibility via Management Plane and Vault Delivery and Location Options

Customer-managed does not necessarily mean custodianship. Cloud-delivered encryption services allow for customer-dedicated vaults in the form of a hardware security module (HSM), but the keys in that HSM still reside in the CSP's data center when in use. Organizations most sensitive to this fact are typically those subject to certain industry regulations that require them to be the physical custodians of their keys. Extending a CSP's BYOK capability should include the option of deploying the management server and key vault on-premises where the customer controls the backup and usage of the keys.

For those organizations that do not require on-premises key creation and store, an "as a service" (XaaS) offering eliminates the need for on-premises infrastructure and the associated CapEx for infrastructure and OpEx of managing that environment. As use of the service grows and additional resources are required, key-management-as-a-service (KMaaS)

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

automatically scales to meet that demand. Cloud-delivered KMaaS services can also simplify key management by providing a centralized control plane for anywhere, anytime access to the key management user interface.

Extending BYOK with Flexibility of The CipherTrust Cloud Key Manager for Multi-clouds

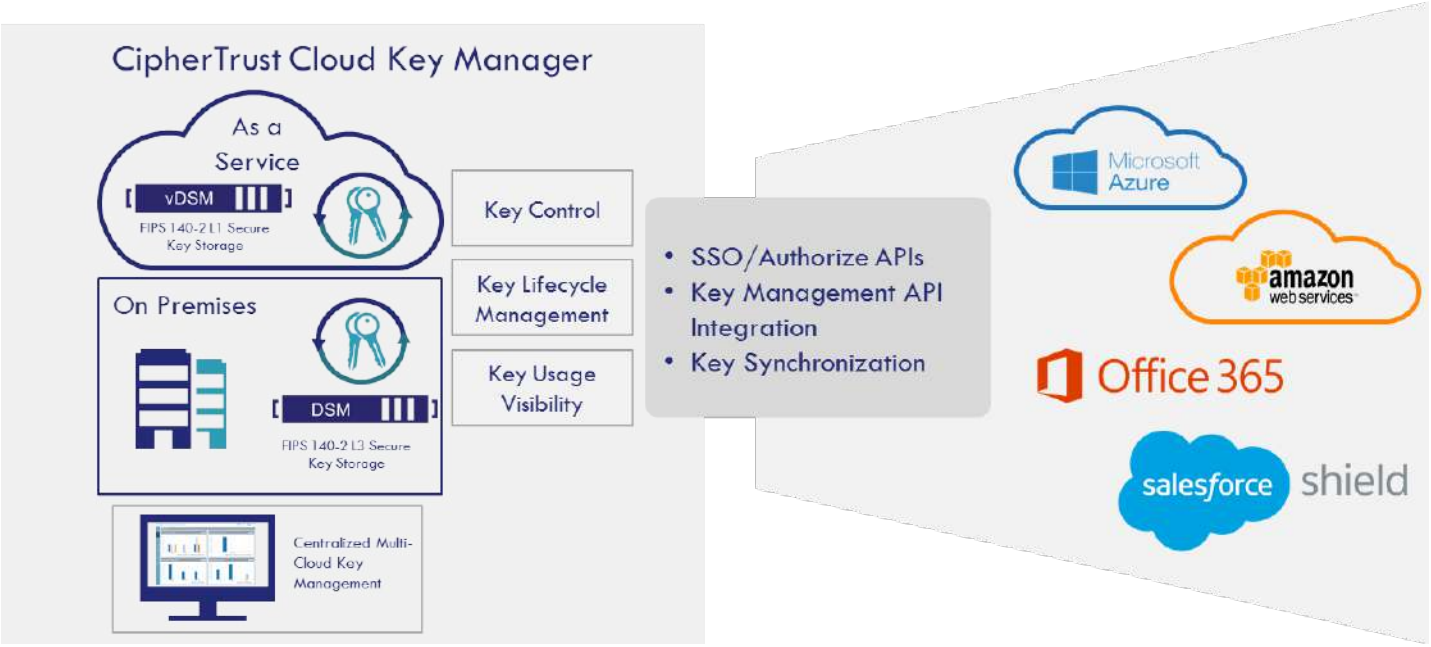
The CipherTrust Cloud Key Manager from Thales eSecurity extends native BYOK offerings with full capabilities across multiple cloud services, and is offered as a service and in customer-management deployment modes.

Support for Multiple Cloud Services

The CipherTrust Cloud Key Manager allows organizations to bring their own encryption keys and centrally manage the lifecycle of those keys across many of the most broadly used and business-critical cloud services (see Figure 2).

- Software-as-a-service (SaaS): The CipherTrust Cloud Key Manager supports Salesforce.com via integration with Salesforce Shield's BYOK service as well as Microsoft's Office 365 office productivity suite.
- Infrastructure-as-a-service (IaaS): The CipherTrust Cloud Key Manager supports and extends the BYOK services of both Amazon Web Services (AWS) and Microsoft Azure.

Figure 2. CipherTrust Cloud Key Manager for Multiple Cloud Services



Source: Thales eSecurity

On-premises and as a Service Implementation Options

Thales eSecurity offers two deployment models for the separation of the control path and data path. Both offer FIPS 140 compliant key protection.

- CipherTrust Cloud Key Manager is offered as a service in the cloud for both the management and storage of customer-created encryption keys. It has a subscription-based pricing model that aligns with SaaS models, allowing organization to treat all of the associated costs as operational expenses.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- CipherTrust Cloud Key Manager can also be deployed on-premises or as a private cloud single-tenant solution for both the management plane and encryption key vault. This implementation option can be partially subscription-based with the customer managing and deploying both or either the management plane and/or the key vault in a public cloud; for example, via the use of an Amazon Machine Image (AMI).

These flexible deployment options represent a notable consideration for organizations evaluating key management solutions for cloud-resident data: Some customers can opt for the efficiencies of a service, others can choose the on-premises option when custodianship of the keys is a requirement for internal security policies or compliance considerations, while a third group can leverage full-cloud but single-tenant. Regardless of whether an organization chooses on-premises or "as a service," it can take advantage of cloud-like utility-based subscription licensing. In addition to licensing, both solutions share the same easy-to-use graphical user interface to remove much of the complexity often associated with key management. The result is centralized key management across multiple cloud services that can simplify compliance and regulation audits for PCI DSS, FISMA, HIPAA, and the upcoming GDPR.

RBAC-based Key Management Lifecycle Management

The CipherTrust Cloud Key Manager provides a full set of key management functionality including: key creation, rotation, deactivation, and revocation. These management capabilities also include the ability to automatically sync key stores to facilitate migrating cloud-resident keys to customer-managed key store vaults. To ensure such key management activities are authorized, Thales integrates with federated login APIs to enable tenant secret management based on cloud provider, rather than local database, controls.

The Bigger Truth

The foundational concept in cloud security is the shared responsibility model that defines the demarcation line of the division of labor between the cloud service provider and the customer for securing and protecting the cloud service. For all types of cloud services, from infrastructure platforms to software-as-a-service, the model is clear: The customer is responsible for securing data that is stored in a public cloud. While CSPs offer some native controls, including the ability to encrypt data, upload your own keys via a BYOK service, and store those keys in either a multi-tenant environment or dedicated HSM, the customer is responsible for both employing these services and managing the process. The use of multiple, discrete, native data encryption-related services increases management complexity while customers in certain industries also require the ability to store encryption keys on-premises to meet regulatory compliance requirements, which, together, create the requirement for efficiency and flexibility.

With the CipherTrust Cloud Key Manager, which supports multiple SaaS apps and IaaS platforms, Thales has delivered on operationalizing the management of encryption keys to efficiently and effectively protect data assets stored by critical cloud services that increasingly represent the core of modern IT environments. The combination of visibility into key usage and management, along with the optionality of cloud-delivered and on-premises deployment models, will help organizations satisfy auditors when it comes to meeting and maintaining compliance. By providing both as a service in the cloud and on-premises versions, customers have options for leveraging the agility of the cloud, while meeting and maintaining compliance.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.