# ENCRYPTION IS KEY

Picture credit: Getty

**Marcella Arthur** *explains why the continuing growth of the hybrid cloud calls for a radical reappraisal of key security*

**The cloud opens up huge vistas of opportunity through increased agility, flexibility, efficiency and cost-saving. Yet as cloud migration increases and workloads are distributed in different locations across hybrid infrastructures, the security complications multiply, especially in relation to encryption and key management. These are serious considerations that have significant cost implications, which multiply as more organisations develop complex cloud environments. The 2020 IBM Ponemon Cost of a Data Breach Report puts the average cost of a data breach at $3.86-million and the average length of time to detect and contain at 280 days. But security complexity and cloud migration drive up the damage to as much as $4.15-million.**

There is no question that the use of hybrid cloud is accelerating. In the first quarter of this year, global spending on shared cloud infrastructure rose by almost 12 percent, according to market intelligence company IDC, amounting to more than $10-billion, while spending on dedicated cloud infrastructure rose nearly 15 percent to hit $4.8-billion. Almost half (46 percent) of the latter figure was invested on-premises, reflecting how hybrid deployments are becoming the norm.

IDC estimates that more than 90 percent of enterprises worldwide will be relying on a mix of on-premises/dedicated private clouds, multiple public clouds and legacy platforms to meet their infrastructure needs by 2022. A survey by professional services giant Accenture at the end of last year found 60 percent of its top banking clients have adopted a multi-cloud strategy. The typical enterprise may now use as many as 1,200 different clouds including commonplace applications or systems such Microsoft Exchange or Salesforce.

As confidence increases, more organisations are not just migrating existing workloads, they are launching greenfield applications in the cloud, believing the gains outweigh the potential security drawbacks. Gartner expects public cloud investment to reach $332-billion this year, driven not just by the obvious advantages of the cloud and growth of remote working during COVID, but also by the near-universal uptake of SaaS applications and increased adoption of virtualisation, edge computing and containerisation. Enterprises are also preparing in a serious way for 5G and the adoption of AI and machine learning applications.

**More than 90 percent of enterprises worldwide will rely on a mix of on-premises/dedicated private clouds, multiple public clouds and legacy platforms by 2022**

With many enterprises keeping their most sensitive data on-premises, highly complex hybrid infrastructures are inevitable, especially for multi-national companies concerned about data sovereignty or where the history of the business involves extensive merger and acquisition activity. Enterprises may also enter national markets where one vendor predominates or where customers and suppliers insist on a certain provider. Google, for example, is the first of the big three cloud companies to launch a data centre in Indonesia and is increasing market-share in the country. In the Asia-Pacific region, however, Google, AWS and Microsoft compete with local vendors including Ali Cloud, Tencent and Huawei, making it more likely some enterprises in the region will have multiple clouds.

These hybrid infrastructures multiply the problems of encryption and key management. For a decade, enterprises have been using sticking-plaster solutions in an attempt to manage their growing number of encryption keys, employing hardware security modules (HSMs), manual inventories and native encryption services from the cloud vendors. This has seldom been easy and is certainly sub-optimal. The inability to secure and manage the cryptographic keys that protect their data across a multitude of scenarios has the potential to bring their organisations to an extremely costly standstill. In any case, reliance on physical hardware alone is challenging in an increasingly virtualised world.

One of the drawbacks with the use of multiple clouds is that each deployment requires a different key to match the encryption system used by the provider. Every app therefore needs its own encryption, its own protection from malware and its own authentication. Keys have dependencies on the applications they are looking to authenticate, each having been written to specific cloud requirements.

The creation and management of these keys is time-consuming, especially when hardware remains intact. Enterprises often lack the ability to manage their entire cryptographic system across all the locations hosting their apps. Organisations with complex infrastructure and high volumes of sensitive data, such as banks, often resort to manual inventories with separate portal log-ins to keep track of which keys work with which applications on different cloud vendors' systems around the world.

When organisations cannot manage their keys across disparate sites, security is compromised. CISOs lack any real oversight of keys, who is using them and for what purpose, or how requirements are changing. If criminals or malicious insiders copy, destroy or ransom data, they are unlikely to know until the damage is done.

Cloud providers have, however, made great strides in developing the strength of their keys and have made them simple to use. Yet many dangers persist. If a key is inadvertently deleted, for example, there is no real possibility of undoing it and the data is lost, with potentially catastrophic consequences. Many cloud companies lack automated back-up or retention policies and do not have key rotation, which although laborious, is necessary for security. There are often problems inserting key material into key management systems or HSMs. Auditability is also often poor, which substantially increases the manual workload for organisations in heavily regulated industries.

More fundamentally, having the keys held by the same entity that holds the data is contrary to any notion of best practice. Whenever encrypted data is stolen it is because the criminals have stolen the keys first. Effectively, enterprises are abdicating responsibility for security when they put their trust in cloud providers' key protection systems.

Developers and solution architects take on the biggest migration risk. The painstaking work that it took to develop an application once, may have to be repeatedly refactored to ensure that keys work anywhere in the cloud, at any time. Applications must be refactored to work with the cloud provider's own system, with new APIs in each case.

Refactoring, as everyone knows, not only eats up time, but is also very costly, requiring significant levels of skill. It hinders time-to-market and if a cloud provider changes the way it runs its systems, an application must be refactored again. The trap for many organisations is that their developers become overstretched through the effort of having constantly to refactor their applications. Dev teams will stress the advantages of sticking with one cloud provider. This may make sense for them, but makes it difficult for enterprises to maximise the agility and efficiency benefits of cloud-agnosticism. The enterprise is no longer free to use whichever provider is most suitable to its needs and purposes at the time. Besides the obvious vulnerability that comes from cyber criminals penetrating the cloud vendor's security to gain access to its customers' data, there is also the risk of vendors having to comply with government warrants for disclosure.

**IT'S UNDERSTOOD THAT THE TYPICAL ENTERPRISE NOW USES AS MANY AS 1,200 DIFFERENT CLOUDS**

What enterprises need is a single pane of glass to manage all keys – a third-party platform that sits above the hybrid infrastructure that gives CISOs full visibility. This is a platform that application developers can write to, offering them flexibility and crypto agility. It will also allow organisations to override the need to refactor numerous applications to ensure their compatibility across each cloud environment. Such a solution must be based on multi-party computation (MPC), which is a sub-field of cryptography.

With an MPC platform, the technology splits a secret key into two or more pieces and places them on different servers and devices. As all the pieces are required to obtain any vital information about the key, but are ultimately not assembled, hackers must breach all the servers and devices to access the system. Strong separation between devices (for example, different administrator credentials and environments), provides a very high level of key protection. This allows organisations to synchronise key management across many data environments and applications, swiftly wiping out the single point of failure.

This hybrid approach to key management supports each enterprise's unique combination of infrastructures, physical and virtual, and includes HSM and cloud-specific applications. It creates a virtual mesh of key management and protection devices, wherever they are – in any

data centre and any cloud, both for management and consumption of cryptographic services.

The fact is that competitive pressures and the drive for efficiency and innovation compel most enterprises to use hybrid infrastructure, making it highly advantageous from a security point of view, for the applications to be 'ignorant' of where the key material is. The application API does not have to call a specific cloud provider. CISOs can use this platform to regain control, setting policy that both governs and enables authorised individuals' use of keys.

## GARTNER EXPECTS PUBLIC CLOUD INVESTMENT TO REACH AS MUCH AS $332-BILLION THIS YEAR

This is a huge advantage for multi-national enterprises that increasingly rely on complicated hybrid infrastructures, allowing them to continue migrating to the cloud to drive the innovation they need for competitive advantage, without compromising security.

Adopting MPC third-party key management gives enterprises using hybrid cloud or multi-cloud infrastructures the single-pane-of-glass visibility that is essential for security and surveillance, providing data about all keys and digital assets, how they are stored, who is using them and how they are programmed.

This gives control that complies with various data protection and data privacy regulations such as GDPR. A good example that illustrates this is data-shredding, where an organisation uploads highly sensitive data to the cloud and is obliged to delete it after a certain time. How can the organisation ensure the data was eliminated from all instances, backups, servers in all relevant regions? This may be a difficult undertaking, but holding the master encryption key separately from the cloud makes it much easier. Delete the master key, and the encrypted data in the cloud is instantly shredded and cannot be recovered.

Neither is it possible for a rogue user to get round policy governing data-access, even if they work for a cloud provider. In other words, the adoption of a third-party cryptographic key platform founded on MPC technology removes much of the risk that currently accompanies the mass migration to the cloud at enterprise level.

### SINGLE SIGN-ON SECURITY

For organisations such as banks that have high volumes of sensitive data in the cloud which they must use for customer-facing applications and secure transactions, an MPC key management platform enables single sign-on security. This eliminates the repeated requirement for multi-factor authentication, which annoys consumers using digital wallets or mobile banking applications. Banks have much to gain from a key management platform. They operate in a highly regulated environment, where audits and due diligence are essential. They use tokenisation and code-signing to secure data throughout the transaction cycle, and many have enterprise blockchain and other distributed ledger technologies, which introduce a further layer of assets to manage securely.

The hybrid cloud is now an essential part of enterprise infrastructure and will remain so for the foreseeable future as the world becomes both increasingly globalised and more complex. If enterprises are to streamline their management and increase the security of the increasingly vast amounts of data held and used in the cloud, they must think much harder about how they use encryption keys. Relying on manual inventories or cloud-native key management systems is not a route to either the most optimal security or a cost-effective use of resources. Not only is refactoring highly costly, but it is also a drain on an organisation's time and energy. All enterprises want to avoid the huge financial and reputational damage of a data breach, but with ever-growing cloud complexity, MPC technology is by far the most effective solution to do so ●

**Marcella Arthur**, Vice President Global Marketing Unbound Technologies, has spearheaded two successful IPOs and led the global marketing and channel strategy of several of the world's technology innovators and IT security vendors, including Sybari, Mimecast and Microsoft.

**Enterprises often lack the ability to manage their entire cryptographic system across all the locations hosting their app**