cpl.thalesgroup.com

THALES

Cloud-based HSM using SafeNet Data Protection On Demand vs. on-premises HSM: A TCO Comparison

Choosing the Most Cost-Effective Solution for Your Crypto Security

White Paper

Contents

Cloud-based HSM vs. on-premises HSM - how do you choose the right option for your organization's crypto security? And how do you compare the total cost of ownership (TCO) of an upfront on-premises HSM investment with a pay-as-you-go (PAYG) cloud-based HSM service? In this paper, we run through a checklist of features you should consider when making your choice of HSM. Then we focus on the primary costs you should include in your side-by-side TCO calculation. Finally, we present a working example that shows you what your TCO evaluation might look like.

Overview

As enterprises step up their cybersecurity to protect the increasing disparate IT systems, meet contractual obligations and comply with new data protection regulations, the need to secure data using mechanisms such as encryption has become an essential part of everyday life. For most organizations this means that the hardware security module (HSM) will become pervasive and play an increasingly important role in safeguarding sensitive key materials that are used to protect important data encryption and management applications and online transactions.

But a traditional on-premises HSM is a significant financial and resource investment. As a result, hard-pressed CIOs or IT directors with tight IT budgets and ever scarce resources may find it difficult to justify the expenditure or find the right level of skills to build and support the infrastructure.

At the same time, the IT landscape is changing, as organizations gradually migrate their applications from on-premises data centers to the cloud. Well respected Forbes magazine reports that 83% of Enterprise workloads will be cloud based by 2020, and many other media reports highlight Enterprises committing "all-in" strategies to take them to the cloud. The security requirements for these moves and the on-going number of breaches (see: https://breachlevelindex.com) have heightened the focus on securing encryption and key management policies. This has led to the emergence of a new type of HSM solution, HSM as a Service or cloud HSM, which is based on the on-demand delivery model of the cloud.

Thales has developed a unique HSM as a Service solution called SafeNet Data Protection On Demand (DPoD), which is a cloud-based platform providing a wide range of on-demand HSM, key management and encryption services through a simple online marketplace. This service complements Thales's market leading on-premises SafeNet Luna and Payment HSM offerings and its extensive portfolio of data protection solutions.

But how do you know which is the right option for your organization? And how do you compare the total cost of ownership (TCO) of an upfront on-premises HSM investment with a pay-as-you-go (PAYG) cloud-based HSM service?

In this paper, we run through a checklist of features you should consider when making your choice of HSM. Then we focus on the primary costs you should include in your side-by-side TCO calculation. Finally, we present a working example that shows you what your TCO evaluation might look like.

But first let's look at the differences between the two HSM models.

On-Premises HSM and SafeNet Data Protection On Demand

On-Premises HSM and SafeNet Data Protection On Demand (which we will call DPoD in this document) are exactly the same cryptographic technology, but delivered in different ways.

On-premises HSM is currently the more familiar model, where the customer purchases the hardware upfront, installs and configures it on-site and is responsible for managing the device(s) throughout their lifecycle.

By contrast, DPoD is a fully managed resource, where the Thales has built a scalable HSM platform in its own data centers from which it delivers secure cryptographic services as a SaaS offering. The DPoD service comes pre-configured with redundancy, resiliency and high availability built in as standard.

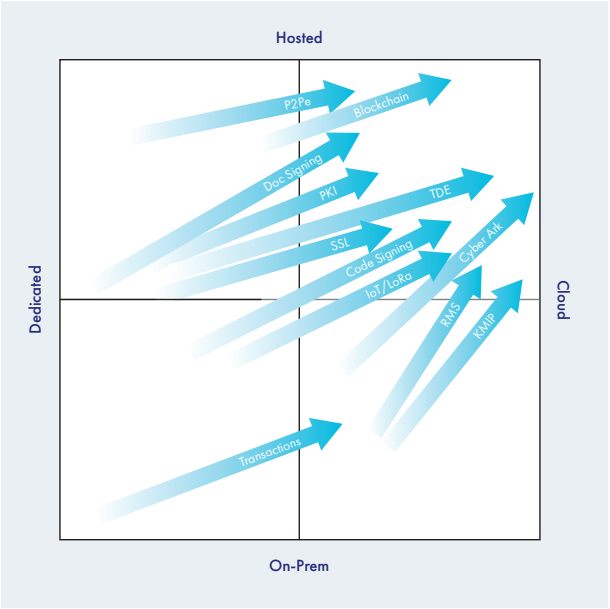
In general, the choice between comparable on-premises HSM and DPoD offerings will largely come down to the overall long-term cost of ownership. But each model is also more suited to specific use cases and customer requirements.

On-Premises HSM

On-premises HSMs remain essential to organizations that need sole control over encryption keys and policies. They also make sense where they're used to serve secure applications hosted in the same on-premises data center. This reduces latency by keeping the hardware components used by an application closer together, provided it is all on one site.

In addition, some organizations will prefer their own dedicated on-premises HSM for applications with intensive cryptographic operations, owing to architecture constraints or higher security and/or performance requirements.

The figure below shows how some of the applications that HSMs are used for are becoming increasingly relevant to DPoD – the arrow shows progress over the next 2-3 years and so the closer to the top right hand corner and the darker the arrow, the more suitable the application is for a cloud based HSM service. As can be seen, this means that cloud has an immediate relevance for different applications or use cases and other use cases will follow over the next 2-3 years as cloud HSM services increase in relevance. Until that point it is therefore likely that many organizations will end up with hybrid infrastructures.



HSM Applications

Usage over the next 2-3 years

Data Protection On Demand

SafeNet Data Protection On Demand (DPoD), like other cloud HSM services, is ideal for a wide range of applications, DevOps, SecOps, smaller departmental requirements, start-ups and SMBs, all of which may not have the budgets or in-house expertise to perform the complex setup and maintenance of an on-premises deployment. In addition, many larger organizations although they have the resources in house, may choose to leverage the benefits of a cloud service and choose to expand their offerings with a cloud HSM for reasons such as scalability and OpEx only expenses. DPoD is well suited to virtually any organization that wants to leverage the on-demand, agile and elastic benefits of the cloud, regardless of size or available resources.

You can take advantage of product trials before committing to a particular vendor. You can run pilot projects without large upfront investments. You can provision services in minutes rather than weeks. And you can scale resources up or down as your capacity requirements change.

With cloud based HSM services you have a choice of two main types of service:

Public Cloud HSM Services

These are the public cloud vendors' in-house HSM offerings. While leading cloud platform providers Azure and AWS offers both a single-tenant solution CloudHSM and a multi-tenant alternative Key Management Service (KMS), others tend only to offer multi-tenant solutions. Common examples include Oracle Key Vault and Google Cloud KMS. In this paper we focus on the HSM technology only.

Public cloud HSM service offerings typically focus on simplicity at the expense of functionality. What's more, they're cloud vendor specific. So they're generally only suited to organizations that are committed to a single cloud provider.

Third-Party HSM Services

Third-party HSM services, such as DPoD, support a range of cloud platforms through a centralized management portal. This makes them better suited to organizations with multi-cloud strategies, helping them to overcome the logistical complexity of different key management methods for each cloud environment.

They're often more sophisticated than public cloud HSM services, offering a higher level of automation for tasks such as on-line backups, load balancing and scaling.

Some types of third-party cloud HSM services come in the form of a click and deploy online marketplace of modular services. DPoD is a leading example of this type of service. These allow you to purchase only the solutions you need for your specific use case and thereby reduce your data protection costs. Services range from general key management and encryption to more specific applications such as key vault, digital signing and Oracle TDE key encryption key (KEK) storage.

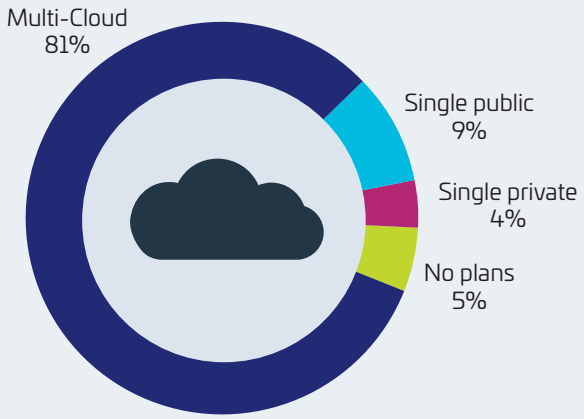
Pivotal Role of Third-Party Cloud HSM Services

According to RightScale's 2018 State of the Cloud Report, **81%** of enterprises now have a multi-cloud strategy.

This well-established trend towards multi-cloud IT highlights the importance of DPoD solutions that can work across a wider range of cloud environments.

Enterprise Cloud Strategy

1,000+ employees



Source: RightScale 2018 State of the Cloud Report

Feature Checklist

Before you make any side-by-side comparison, you'll first need to decide what features you actually need.

All HSMs, whether on-premises or cloud based, should meet the bare minimum requirements, such as:

- Secure storage of cryptographic material
- Secure cryptographic execution environment (key generation, management, function execution)
- Strong separation of duties
- Strong segregation of logical data and credentials (in multi-partition / multi-tenant cases)
- Certified physical and logical security mechanisms (tampering, protection against attacks)
- Mechanisms for event logging and audit reporting
- Secure APIs to access the HSM (PKCS#11, RESTful and others)

But, not all HSMs are created equal. They have different levels of functionality, security, ease of use, etc. – all of which can have a knock-on effect on your TCO.

Here are some of the typical features you may want to put high on your priority list:

Security: With different levels of compliance such as provided by FIPS and Common Criteria, certification is the easiest way to spot-check the security of a device. However, it's important to remember that although the certification means the hardware meets specific criteria, it doesn't necessarily guarantee security. Another way to gauge the security of the device is to consider the reputation of the HSM vendor and look at what other companies are using its products. Or in the case of cloud service providers, you may also want to consider their focus on physical and logical security as well as certifications such as ISO27001 and SOC2.

Geographic Location: Compliance requirements may dictate where data can reside, and how that data can be shared, even within an organization. Some organizations are very conscious of choosing cloud HSM services that are specific to a geography such as Europe or North America.

Crypto Agility: Industry standard algorithms are generally recommended over proprietary, but some use cases mandate the use of specific algorithms or algorithm families. For compliance purposes, old algorithms may be occasionally blacklisted or deprecated. An HSM will provide a number of symmetrical and asymmetrical crypto algorithms that will be used for symmetric /asymmetric encryption, signing, timestamping, authentication and other functions. Organizations such as NIST, ANSI industry boards like GSMA (for machine to machine, IoT), or ETSI (telecom standards, smartcards) and other might specify certain algorithms/interfaces for their relevant applications and industries. Talk to your vendor about their support for future technologies such as Quantum.

Random Number Generation (RNG): The use of certified random number generators can be a factor for compliance with certain regulations or requirements, so check that the vendor uses an approved or certified process.

Key Backup: The backup of key material should only be done to an environment with the desired security level as is provided by the HSM. The ability to manage remote backups or key material replication is also an important factor.

User Interface: Most of the HSM administration is done via command line, although "Crypto Management" interfaces are often available to facilitate the HSM management,
HSM client deployment and other lifecycle activities. This dictates a familiarity with HSMs that most organizations do not have – or the acquisition of the requisite skills which
can be beyond the core competencies, not to mention budgets, of many organizations. In addition, even large organizations with onsite HSM teams to manage their existing appliances may not choose to expand their capacity when their requirements change.

Application Integration: A wide choice of integrations is going to be important because as your IT operations grow and compliance requirements change it is likely that you will need to secure more than just the initial application, therefore choose a vendor with multiple proven integrations that will serve you well into the future.

Automation: In addition to building the HSM infrastructure, the deployment and on-going management of the solution is a significant part of the operation. In order to do this effectively, it is recommended to find a cloud HSM service that offers automation of at least some of the processes such as deploying the clients, integrating the clients and managing on-going updates.

Key migration: The ability to transfer existing keys into the new environment is important in maintaining continuity of service for your applications. Some HSMs can provide simple migration capabilities today.

Key Cost Factors

So now you've decided on the HSM features your applications and security posture need, you can compare the TCO of an on-premises solution with DPoD on a
like-for-like basis. The following are the most important cost factors you'll need to consider:

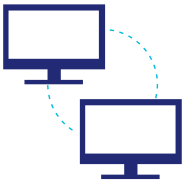
HSM Hardware

A typical on-premises deployment will serve a number of mission-critical applications. So, to ensure resiliency and high availability, it generally comprises a pair of HSMs and a backup HSM at each geographical location.

All this represents a significant investment in infrastructure and configuration. On the other hand, a cloud-hosted HSM solution like DPoD is ready for immediate use and requires no additional hardware.

Crypto Management Tool

A crypto management tool is a hypervisor for managing a network of HSMs. It provides centralized management of HSM resources, such as partitioning, troubleshooting, monitoring and alerting. It is also an important aspect in terms of the orchestration and automation of the deployment of the HSM clients into the applications environments. Much of this type of capability is included within DPoD as standard.



Network and Infrastructure

Building an infrastructure to support a resilient IT service is a major consideration when looking at comparing on-premises versus cloud based services. This also therefore relevant to an HSM build-out – where items such as networks, routers, load-balancers, servers and much more will be required to support the resilient HSM requirements of an organization.

An additional consideration reported by many customers is the time taken to get network teams to prepare the infrastructure for the deployment of on-premises HSMs – something that is not required (or is much simpler) when using a cloud based service. For a cloud-based service like DPoD all you require is access to the IP addresses and ports.

Security

Wrapping a secure infrastructure around your HSMs will be an important factor in mitigating all risks, so looking closely at firewalls, anti-virus and other aspects of keeping these elements patched and current will be a significant resource overhead and risk factor. All of this has been built into SafeNet Data Protection on Demand.

Data Center Environment

Dedicating rack space, power, environmental aspects and resources to putting a resilient HSM infrastructure in place will mean looking at where your DC's should be located, internetworking between those sites and resources to manage and monitor those environments.

Payment Model

An on-premises HSM purchase, based on the CAPEX model, can range from around a few thousand to many thousands of dollars, depending on the level of functionality and security you require.

By contrast, the OPEX approach of a service like DPoD provides a more manageable way to finance cryptographic key security. Not only that, but you only pay for the capacity and services you actually need or use – many customers rarely use all of the capacity of their HSM.

These different payment models also require different approaches to calculating TCO in terms of the cost of capital etc.

Setup

Setting up an on-premises HSM is no easy challenge and requires a significant financial investment in manpower to procure, configure and deploy to a production environment. This can take days or even weeks. But, with DPoD, you can be up and running in a matter of minutes. Not only does this drastically reduce labor costs but also increases your business agility, helping to improve the bottom line through lower project cost and/or faster times to market.

Software

In addition to your crypto management tool you'll also need the software to access the functionality of your HSMs. This may require separate licenses for each partition or HSM service, as well each client that accesses your hardware.

Your licensing costs can soon mount up in a large enterprise configuration, as you'd assign logically separate HSM services to different applications and on-premises locations and build (and maintain) your licensing accordingly)

With DPoD, you don't need to worry about calculating software licenses separately, as everything is included in the price.

Application Integration

As part of your TCO calculation, you should estimate the amount of work involved in integrating your applications. Integrating in-house systems with any type of HSM may prove time-consuming and challenging.

A good HSM vendor will provide clear documentation on how to integrate its product with common applications. DPoD for example offers out-of-box interoperability with a wide range of services, such as databases, storage and application development tools.

However, even with DPoD you should look carefully at the integration or migration aspects of your environment when calculating your TCO.

Technical Knowledge and Training

Managing an on-premises HSM platform requires a high level of technical expertise. So you should also include the cost of staff training or skills recruitment in your TCO evaluation. This is also true of the deployment of your HSM infrastructure.

By contrast, a cloud-based HSM requires far less technical know-how, with SafeNet Data Protection on Demand, Thales maintains the hardware for you. This makes DPoD a particularly more cost-effective option for organizations that are relatively new to cryptographic security.

Compliance

Compliance is not only essential to meeting legislative requirements but also opens up more business opportunities from highly regulated sectors, such as healthcare, finance and federal government.

On-premises compliance with security standards such as GDPR, FIPS, PCI-DSS and others can be a complex undertaking that requires deep regulatory knowledge and lengthy processes. Most of this work is automatically covered when you use a recognized cloud-based HSM service like SafeNet Data Protection On Demand, helping to reduce the TCO compared with an on-premises deployment.

This is particularly true when certification to SOC2 and ISO27001 standards are important to the business, its alignment to industry regulations and its processes.

Operational Management

Your TCO comparison should also cover the area which commonly has the highest impact, namely the cost of operational management. For example, your on-premises figure should allow for the manual workload involved in patching, scaling, upgrading, monitoring, security auditing, backup and general housekeeping.

Although DPoD will free you up from many time-consuming operational tasks, you'll still need to account for some lifecycle administration, such as user account and permission management. We have included these in our TCO calculations later in this document – indicating the differences between on-premises and DPoD.

Service Level

What level of SLA do you require? Most businesses will be satisfied with a guaranteed 99.95% SLA for their HSM architecture. In addition to the hardware costs of building a resilient and highly available on-premises HSM deployment to support such an SLA, you'll also need to invest in people and tools to maintain optimum service levels. Your TCO calculation should therefore also include the cost of providing technical support and incident resolution, holiday cover for expert resources and any ongoing maintenance contract.

In the case of DPoD, most of this is the responsibility of Thales and included in your contract, as set out in its Service Level Agreement (SLA).

At a Glance Comparison

	On-Premises HSM	DPoD Service
Hardware	Range of hardware required, including a resilient pair and backup HSM per site, a crypto management platform and network infrastructure.	Delivered through fully redundant cloud architecture. No hardware required.
Payment Model	High upfront cost (CAPEX).	Usage-based billing (OPEX) with no upfront cost.
Setup	Complex setup and configuration.	Rapid click and deploy.
Software	Licenses may be required for each HSM partition and use of HSM client software.	Included in cost.
Client deployment	Complex and time-consuming deployment of the integration client. Quality of product documentation varies with manufacturer.	Out-of-box deployment of a wide range of services, such as databases, storage and application development tools.
Technical Knowledge and Training	High level of in-house expertise required.	Fully managed by highly trained and experienced security professionals. Easy-to-use front-end interface. Minimal cryptographic knowledge required.
Compliance	Complex undertaking requiring deep regulatory knowledge and investment in additional services such as compliance consultants and monitoring tools.	Responsibility of DPoD provider.
Operational Management	High manual workload, including regular patching, scaling, upgrading, monitoring, security auditing, backup and general housekeeping.	Fully automated managed solution with low operational overhead.
Service Level	Investment in people and third-party tools and services to provide technical support, incident resolution and holiday cover for expert resources.	High standards of SLA with 24x7 support.

Illustrative Example

Once you've identified the key factors you need to consider in your TCO comparison you can start collating the figures for your cost analysis.

One-Off Costs

First build up a list of one-off costs for each deployment model. For your on-premises HSM calculation, you'll need to include the upfront costs of hardware [and any perpetual software licenses]:

- A resilient pair of HSMs
- A backup device
- A crypto management tool

You will then need to estimate the time and cost for setup work:

Design and planning of installation Installation, configuration and integration

- Testing and handover
- Staff training

We have included in this document some of the areas you should look at closely, and the calculations we show later in this document provide real life examples of what this looks like, based on some typical projects that we have been involved in.

Now let's move onto your annual costs.

Annual Costs

Your on-premises HSM calculation will include the cost of:

- Crypto management server software licenses to provide a simple GUI based management platform
- HSM partition charges to allow multiple use cases to utilize your HSM platform
- HSM client licenses which are used to integrate with your applications
- Ongoing support licenses

You'll also need to estimate the ongoing cost of systems and infrastructure management. The calculation will be very specific to your organization. However, the following example, based loosely on our own internal cost analysis, highlights the most important costs you'll need to consider:

Cost area	Description of Consideration
Incident resolution	Resolving faults within the infrastructure – either from the service desk or from automated tools (e.g. performance, disk space, user support)
Change installation	Implementing changes within the infrastructure, adding disk, service packs, memory, etc.
System documentation	Documenting the infrastructure, maintaining the documentation and the configuration.
Virus/security management	Ensuring solutions and updates are deployed to protect the server and the infrastructure.
Reporting	Monitoring server and infrastructure performance and availability, etc.
Housekeeping	Clearing/archiving log files, general file management, storage reclaim, etc.
Performance capacity management	Ensuring ongoing server availability and capacity.
System software upgrades	Ensuring latest patches are implemented, preventative analysis and execution.

Security audit	Checking security logs, maintaining service integrity etc., implementing and maintaining security policy.
Print administration	File and print server management.
User administration	Managing user accounts, MAC, permissions.
Storage management	Storage connectivity, resilience, failovers, etc.
Token administration	Managing provisioning, deployment, revocation and other life-cycle events.
System monitoring	Ongoing monitoring using system tools and reports, correlation and investigation.
Back-up operations	Back-up and storage of the application, as well as user data. Includes: monitoring of tapes; storage; off-site operations.
Team leadership	Managing the team who supports the server, application, infrastructure, help desk, escalation processes, etc.

In addition to these resources you will likely require a Crypto team to manage the ongoing operational aspects of your HSM infrastructure. The following are areas that we have found are common across our customer base:

HSM client management	Managing provisioning, deployment of updates, etc.
HSM management	Managing provisioning, deployment of updates, etc.
Team management	Managing the team who support the server, application, infrastructure, help desk, escalation processes, key ceremonies, etc.

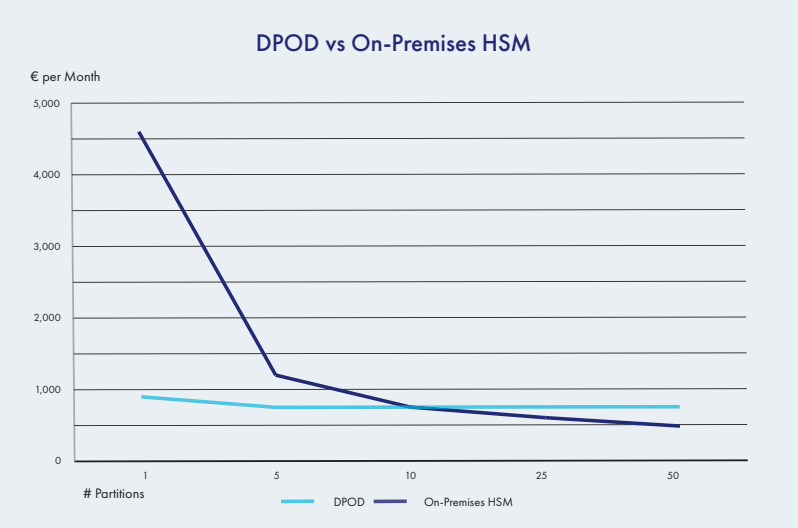
TCO Calculation

To complete your calculation, you'll need to combine these one-off and annual costs as well as the administration/management costs into a TCO figure for each deployment model.

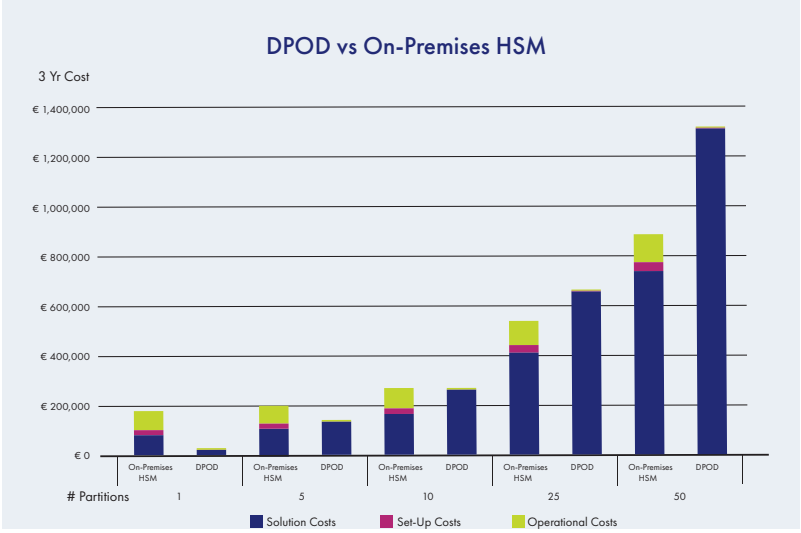
The below example, based on our own internal cost analysis, converts these costs into an annual figure by spreading them over a three-year period.

Some organizations will have only modest HSM needs, while others will be intensive HSM users. So our first example below provides calculations for a range of HSM requirements – from 5 use cases or up to 50 and shows the monthly costs that would likely arise. In summary, for organizations looking to deploy small to medium sized DevOps projects or shared service environments and for organizations such as SMB's a DPoD based service holds great appeal for up to 12-15 individual use cases.

The alternative figure below takes a slightly different approach and demonstrates the differences between on-premises HSM and DPoD based deployment, but showing the areas of cost. This will allow you to make an initial assessment of the investment differences between the solution and the additional resources, which is essential in determining the level of in-house skills required:



The results of our simple TCO comparisons are based on our own assumptions about the typical cost of implementing each HSM solution over a three-year period. Although they show that DPoD is considerably more economical than an on-premises HSM for small to medium scale installations, costs will vary from organization to organization. So it's essential you perform your own cost analysis before making an informed purchasing decision.



Nevertheless, the results clearly demonstrate that DPoD is particularly cost-effective in certain deployments where you may only need to secure cryptographic services for a limited number of applications. And that makes sense, given that an on-premises solution requires significant investment in hardware and setup at any scale of deployment.

Conclusions

Cloud based HSMs such as DPoD have their place where the upfront investment or skills required to deploy a device far outweigh the investment in an HSM or an additional HSM if you are considering expansion of your existing HSM estate... or are beyond the reach of an organization such as an Small Medium Business (SMB/SME).

One of the most important decision criteria is the availability of and/or the cost of funding the capital investments of an on-premises solution. The analysis clearly shows that it is important to look at the long term TCO and balance that with up-front investments. For many smaller businesses or even department/project oriented requirements the budget availability can be a highly significant decision factor in selecting the appropriate solution. This can also apply to large organizations such as tier-1 banks for example, that although they have onsite expertise to manage their existing HSMs, may consider expanding their options through cloud-based HSM services in order to take advantage of all the benefits of a cloud service.

Skills availability is an additional consideration that affects may customer decisions. The availability and on-going cost of employing crypto-aware resources is a primary consideration of many businesses as they consider the on-premises versus cloud/outsourcing options, where the analysis shows a significant skills requirement for implementing and maintaining on-premises solutions – something that many organizations recognize and is a primary driver for the move to cloud.

The previous graphs show that an on-premises solution would appear more favorable once you exceed over 15-20 partitions or individual use cases. So for the majority of organizations who are using HSMs for only a limited number of applications then a solution such as DPoD would be highly cost-effective.

It is essential to consider the application or use case that the HSM is to be used for. On-premises HSMs are more suited to high volume transactional requirements, where the latency of cloud could constrict performance and response times. However, the majority of use cases for most businesses should be able to benefit from using cloud based HSM services such as DPoD.

The real benefit of a broad scope data protection solution such as DPoD comes from when you are considering other security and data protection applications such as control and ownership of keys, key management or encryption of data at rest such as data held in virtual machines or in folders or files. The managing such diverse data protection assets lends itself to using a cloud based platform that can provide a single pane of glass management, orchestration and deployment capability. To deploy on-premises solutions for such diverse environments could potentially cost multiple times the cost of a cloud based service.

Many customers see significant benefits in cloud based services coming from the ease and speed of setting up and managing projects or sandbox environments, where on-premises solutions require multiple changes network changes, infrastructure adjustments, resource scheduling etc.

In summary, in addition to some compelling Total Cost of Ownership benefits demonstrated by the previous graphs, a cloud based solution such as SafeNet Data Protection On Demand can deliver significant benefits to smaller organizations or projects and easily achievable benefits to organizations of all sizes seeking a simple, easy to deploy and manage cloud-based HSM service.

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

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: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> cpl.thalesgroup.com <