THALES

thalescpl.com

Digital Transformation for MSPs and MSSPs: How Cloud HSM Can Fuel Your Business Growth

Overview

The IT landscape is rapidly changing. And so is the market for MSPs and MSSPs. Their customers are waking up to the benefits of the cloud and are looking for service partners to guide them through their digital transformation journey.

At the same time, the number of cyber attacks is growing almost exponentially. Virtually every business is potentially at risk. Yet many organizations lack the in-house knowledge and skills to meet the never-ending challenges of regulatory compliance and continually changing cyber threats.

This presents huge opportunities for business growth in the managed services sector, but only to partners who are prepared to embrace the service-based model of the cloud, and particularly multi-cloud and hybrid environments —those who can help their clients make the best use of both on-premises and cloud-based resources, and those with the skills and tools to help their clients overcome the technical complexities of securing their infrastructure.

HSM as a service, or Cloud HSM services, can help MSPs and MSSPs exploit these opportunities as clients adopt a cloud-first approach to IT and review their existing infrastructure requirements.

This eBook will show MSPs and MSSPs how they can use Cloud HSM to optimize security service delivery and bridge the growing skills gap in today's IT workforce, while, at the same time, increase their profitability and build a stronger and more secure service.

But, before we dive a little deeper, let's remind ourselves what Cloud HSM actually is.

What Is Cloud HSM?

Cloud HSM provides exactly the same cryptographic functionality as an on-premises HSM, but is delivered as an as-a-service offering. As with many as-a-service offerings, the capabilities vary, but a well-established Cloud HSM from a reputable vendor should provide a fully managed resource with redundancy, resiliency, and high availability built in as standard. This makes Cloud HSM ideal for those companies that do not have the in-house expertise to perform the complex setup and maintenance of an on-premises hardware deployment.

With Cloud HSM, you can provision services in minutes, rather than weeks. You can scale capacity up and down as your requirements change. And you only pay for the cryptographic resources you actually consume. This gives your clients the flexibility to run pilot projects without committing to large upfront investments.

What's more, Cloud HSM solutions generally offer a service trial so you can assess whether the solution meets your needs before you purchase.

International Data Corporation (IDC) forecasts that the worldwide managed cloud services market will grow at a five-year compound annual growth rate (CAGR) of nearly 18%, with spending reaching $62.8 billion in 2021.

"The managed cloud services market is creating fundamental changes in the outsourcing industry involving the entrance of new providers, partnership ecosystems, investment requirements and opportunities, though also bringing with it some critical challenges to players shifting from a world of non-cloud (legacy) outsourcing to managed cloud services," said David Tapper, vice president, IDC's Outsourcing and Managed Cloud Services program.

https://www.businesswire.com/news/home/20171127005548/en/Worldwide-Managed-Cloud-Services-Demand-Shows-Signs

Cloud HSM solutions are available through both public cloud providers and third-party vendors. The main differences between the two types of offerings are as follows:

Public Cloud HSM

HSM capabilities provided by cloud service providers (CSPs), such as AWS, Microsoft Azure, and Google, provide native integration with other services available on their platforms. However, they are vendor specific, where each provider has its own individual approach to encryption key management. This means they're often less flexible with regards to multi-cloud environments, and especially hybrid environments, due to the technical complexity of integrating different cloud vendors' systems, as well as cryptographic systems.

Third-Party Cloud HSM

Third-party solutions are cloud agnostic. Moreover, those that are more advanced can protect sensitive data in any type of deployment and are equally at home serving on-premises, hybrid cloud, or multi-cloud infrastructures.

They're a particularly good fit for clients with multi-cloud strategies, as they're a simple and consistent way of providing cryptographic security across different environments through centralized management.

Third-party services also tend to be more sophisticated than their public cloud counterparts, offering a higher level of automation for tasks such as backups, load balancing, and scaling.

On-Premises vs. Cloud HSM

Which Is the Most Cost-Effective Solution for Your Application Security?

Download this guide to making a side-by-side TCO comparison of two different HSM options:

Cloud-Based HSM Using SafeNet Data Protection On Demand vs. On-Premises HSM: A TCO Comparison

How Cloud HSM Can Boost Your Business

Cloud HSM will be increasingly demanded by customers, due to rapidly burgeoning compliance requirements, as proof that an organization has full custodianship over its data and encryption capabilities. This is in order to prove to regulatory authorities that the organization can provide an audit trail on demand. This is going to be a massive driver for growth in the MSP/MSSP industry in the coming months/years.

Let's take a look at some of the more practical considerations for both you and your customers of moving to a Cloud HSM or hybrid environment, rather than to traditional on-premises solutions:

The Practical Benefits

- **Ease of use:** Setting up an on-premises HSM is a complex and time consuming process, requiring a high level of technical expertise. By contrast, cloud-based HSMs are relatively simple to manage and configure.
  A mature cloud HSM solution will also provide out-of-the-box interoperability with a wide range of services, such as application development tools, databases, and privileged access management systems.
- **Centralized management:** Choosing the right HSM is an essential element in building your portfolio. Read this blog for more advice. Choosing a Cloud HSM that is designed for MSP/MSSP partners is critical, as being able to manage all your customers from a single central point reduces Total Cost of Ownership and improves the customer experience in the rare case that something does go wrong.
- **Reduced management overhead:** An on-premises HSM requires a significant amount of manual workload involved in patching, scaling, upgrading, monitoring, security auditing, backup, and general housekeeping.
  Cloud HSM takes care of all this for you so that you can provide the same high level of service at a considerably reduced management overhead.
- **Simpler all-in-one pricing:** In addition to the one-off cost of hardware purchase and setup, you may need to factor ongoing expenditures on software licenses and monitoring tools into your expenses. However, Cloud HSM makes cost allocation a breeze, as everything is included in the price.
- **24/7 support:** As an as-a-service solution, Cloud HSM typically comes with 99.95% SLA (Service Level Agreement) support, offering partners fast responses to technical questions, to support your business with expertise and support for the Cloud HSM infrastructure.
- **Built-in redundancy:** With redundancy built in as standard, cloud-based solutions automatically failover to standby HSMs in event of hardware failure. In other words, you can provide a robust cryptographic service without the complexity of configuring and managing a cluster of HSMs.

The Strategic Benefits

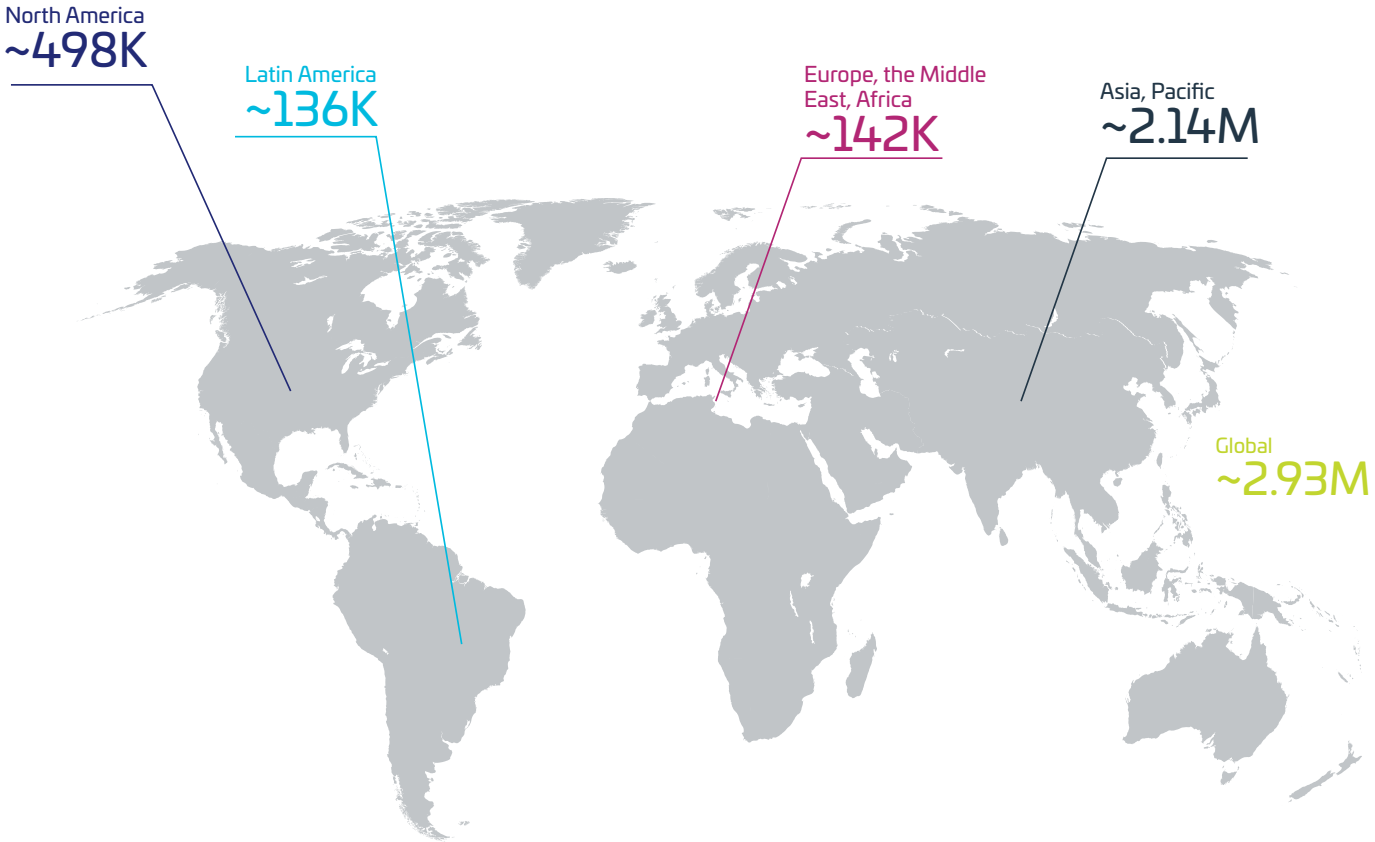
- **Simple to set up and manage:** With Cloud HSM, there is no need for on-site set ups or the delivery/management of hardware.
- **No upfront costs:** Cloud HSM's OPEX pricing model can encourage more sales, as clients don't have to make large upfront investments to bolster their security and there is no costly infrastructure investment to start the service.
- **More affordable:** HSM hardware doesn't come cheap. This can make the cost prohibitive for clients with only modest cryptographic requirements.
  But, with Cloud HSM, you only pay for what you need, so it's particularly cost effective for small-scale deployments. As it's a more affordable alternative to on-premises hardware, adding Cloud HSM to your portfolio can open up doors to new SMB markets.
- **More secure:** Cloud HSM provides the same high level of protection as traditional HSMs for storing your customers' encryption keys and other sensitive information.
  What's more, their keys are stored in a completely separate environment from the data they encrypt, providing an additional level of defense against a breach.
- **Streamlined compliance:** Compliance is not only essential to meeting legislative requirements, but also opens up business opportunities in highly regulated sectors such as healthcare, finance, and federal government.
  However, it can require significant investment in regulatory expertise and compliance management tools. Cloud HSM simplifies this process by doing much of the legwork involved in meeting compliance.
- **Hybrid friendly:** More sophisticated cloud HSM solutions are designed to protect data in any type of environment, so they're perfectly adapted to customers who are adopting a hybrid strategy and need a solution that can help with their migration plans.
- **Regular income stream:** By contrast with the one-off nature of providing on-premises hardware, offering HSM capability as a service-based proposition will bring in regular, reliable, and consistent annuity revenue.
- **Additional revenue opportunities:** You can leverage the different integrations available through your Cloud HSM vendor to develop cross-sell, upsell, and product bundling opportunities.
  For example, you could draw up a menu of security and cryptographic add-ons for common implementations such as CyberArk, Microsoft Active Directory Certificate Services, and Oracle TDE. These can help clients plug gaps in their cybersecurity while, at the same time, drive new revenue to your service-oriented business.

Cloud HSM provides an affordability, rapid deployment, and ease of use that will increase market appeal to smaller organization or projects within a larger enterprise. However, we also need to consider that a cloud-based HSM is not a fit for all organizations, and there are some use cases that still require an on-premises HSM.

The Global Cybersecurity Shortage

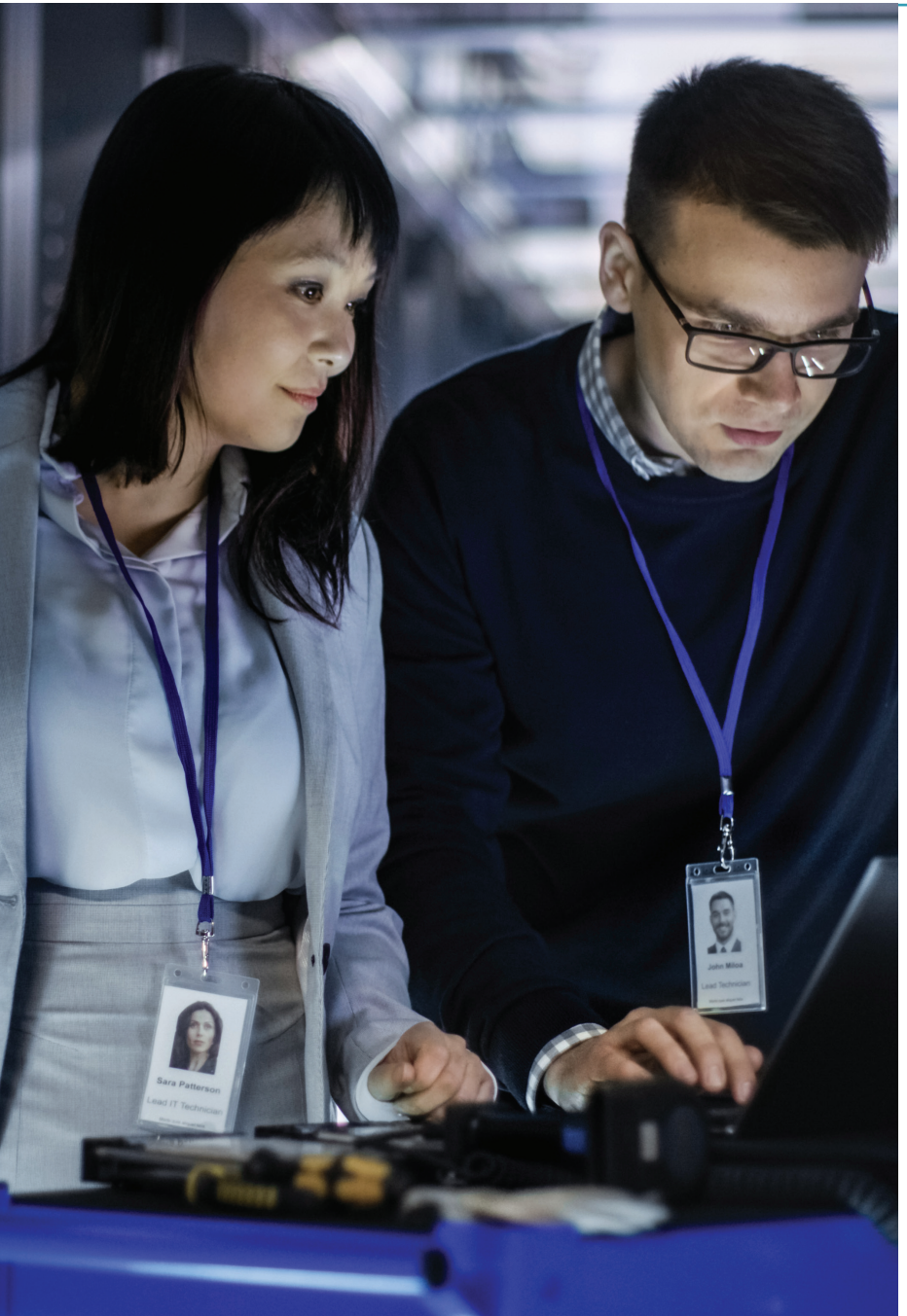
According to recent estimates by security training and certification body (ISC)[2], the worldwide shortage of cybersecurity professionals is rapidly approaching three million.

That's a serious shortfall, but it's great news for MSPs and MSSPs with the expertise to help customers fill the gaps in their cybersecurity knowledge.



The global cybersecurity skills gap

(Image source: (ISC)[2])



Hybrid Cloud: The First Step to Digital Transformation

Many clients begin their digital transformation journey with hybrid cloud, using it as a stepping stone to wider cloud migration—typically developing new applications on the public cloud while supporting legacy workloads on existing on-premises infrastructure. So, having both Cloud and on-premises HSMs in your portfolio will be essential in winning projects and ensuring effective security for your customers.

As their service partner, your role will be to help your clients reap the benefits that hybrid cloud has to offer. These include:

- **Seamless integration:** Most projects that customers have will very likely need an HSM to be integrated with solutions that you are already supplying. By bundling these services together, you create a seamless delivery.
- **Innovation:** Hybrid cloud enables innovation through fast provisioning times, accelerated development, and access to new technologies.
- **Cost savings:** Clients no longer need costly additional hardware to cope with occasional peaks in demand. Instead, they can burst workloads to the cloud whenever they need extra capacity.
- **More flexibility:** Hybrid cloud offers more scope to host applications in the environment where they're best suited.

This is why hybrid cloud will be such an important source of revenue for MSPs and MSSPs in the next few years. It offers huge potential to become a trusted partner, providing expertise in areas such as migration, cost and performance optimization, security and compliance, data lifecycle management, and container technologies.

5-Point Checklist to Partner Success

As organizations migrate their systems to the cloud, they face complex challenges to securing their applications on new, unfamiliar, and dynamic infrastructure.

At the same time, the IT industry is in the throes of a chronic cloud and cybersecurity skills shortage. Companies are turning to trusted service partners in a bid to bridge the knowledge gap and solve their digital transformation problems.

Cloud HSM can play an instrumental role in helping MSPs and MSSPs meet the on-premises and cloud security needs of their clients. But it's still just one part of a much bigger picture.

In this section, we look at some of the other measures service partners should take to support their customers so that they can survive and thrive in a climate of rapid industry change and increasingly more sophisticated cybersecurity threats.

1. Understand Your Customers' Needs

First and foremost, talk to your customers. That way, you'll get a deeper insight into their cybersecurity requirements and how these are changing due to the cloud. For example, you'll get a clearer picture of what data they store, where they store it, and the level of protection it needs and why. As well as gaps in their data security, you'll also identify gaps in their expertise. Together, these will provide the basis for recommending or developing new services to meet their requirements.

Secondly, focus on the use cases where you add value. With the increased focus on regulatory compliance requiring improved auditability, many of the use cases where customers identify a need for key management and HSMs are very closely aligned to the very products and services that MSPs/MSSPs are already supplying. Most partners are finding that the previously high costs and ongoing resource requirements for on-premises HSMs have been prohibitive to customer adoption. By bundling HSMs, key management, and encryption solutions into the portfolio mix, you can enable cross/upsell potential for every sale.

By doing so, you can set yourself, as service provider, apart from traditional resellers, who generally focus on pushing a point product rather than delivering services that address customer needs. The migration to the cloud will demand knowledge about customer business needs and priorities.

2. Empower People

MSPs and MSSPs should equip their workforce with the cloud and security skills they need to meet the challenges customers face as they modernize their infrastructure. With cloud and cybersecurity skills at a premium, you should look beyond traditional talent recruitment by educating your workforce through formal and on-the-job training. Where possible, training should lead to industry-recognized accreditation. This gives staff an incentive to learn, improves job satisfaction, and also enhances the credibility of your business.

Cloud HSM is a great example, where the focus on specific use cases and the simplification of deployment/integration processes means that the need for actual technology knowledge is less prevalent than in the past. Simple online training courses are now available and can add significantly to the skillsets of the technical teams.

3. Advance Processes

As your business shifts its focus towards hybrid and multi-cloud services, you'll need to nurture cloud security knowledge and awareness throughout your organization. In other words, not just your technical team, but also sales, marketing, and frontline customer support.

Moreover, you should consider adopting the ITIL framework (Information Technology Infrastructure Library), a set of best practices for IT service management, as this will:

- Be a key selling point to new prospective customers.
- Ensure you deliver services in line with best practices.
- Open up opportunities with leading public CSPs.
- Provide a strong platform for business growth and change.

This process change, to align with more automated cloud offerings, also covers areas such as order processing and billing—where your business will need to adapt to different paperless methods. Adopting these new processes can significantly cut resource costs and streamline a service partner business.

4. Provide Tools

Tooling will also play an instrumental role in the future success of your business. Leverage tools such as APIs that enable you to integrate partner solutions into your cloud service business processes.

As you expand your customer base, a range of tools will take the strain out of managing security and compliance across a complex array of on-premises and cloud deployments. Others will help you manage your client portfolio or provide a better service — from cost allocation and invoicing, to a CRM system.

And, depending on the nature of your service, you may need tools that:

- Help you control cloud costs.
- Monitor application performance.
- Perform automatic backups.
- Enable application portability across hybrid and multi-cloud environments.
- Automate and streamline the software development process.

5. Develop a Unique Selling Proposition (USP)

Finally, don't forget that prospective customers still need a reason to partner with you, rather than one of your competitors, whether they are an MSP/MSSP offering similar services or one of the large cloud providers—so you'll need to develop a point of difference. That means positioning yourself as the obvious partner choice for a clear segment of the market, rather than simply providing the same service as everyone else.

The best way to identify a USP is to ask yourself the following questions:

- Do you serve clients in a specific industry vertical?
- Do you have expertise in specific technologies?
- Are you locally based or do you offer a worldwide presence?
- Do you provide a better range of services?
- Do you offer a new and unique SLA?
- What other ways can you add value to your proposition?

Conclusion

As more companies adopt hybrid and multi-cloud strategies, they require expertise from MSPs and MSSPs to help them through the minefield of security and compliance concerns that come from migrating workloads between on-premises and clouds.

The cloud security market is in its formative stages and in hyper-growth, making it the perfect time for service providers and security resellers to capture market share with security consultancy and service offerings. Organizations of all sizes are concerned with how they will assure data security and maintain compliance as they deploy hybrid strategies or fully lift and shift workloads into the cloud.

Top areas of concern include HSM root of trust deployment, high-assurance key management, and encryption. These technologies are not only fundamental in establishing trust, security and compliance, but deliver controls that are demanded by auditors and regulators.

Service-based security offerings, such as the right Cloud HSM, will help you get started by addressing many of the challenges you and your customers encounter along the way, and to cement your role as trusted advisor by helping them to overcome concerns about migrating to the cloud/s, and ensure the simple and secure management of keys and data across multi-cloud and hybrid environments.

Building a hybrid portfolio to help customers during the migration period over the next few years will be critical by centrally managing and securing entire cryptographic operations across not just across public cloud services but also other cloud services and on-premises applications.

As a service provider, you can take advantage of the digital transformation, leveraging services such as Cloud HSM to provide a differentiated service to your customers, driving revenue and capturing a high-growth market.

As a service partner in the traditional, or even the transformative IT space, you simply cannot afford to ignore this shift in focus. And now's the time to make that move.

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.

To help customers address the shortage of skilled security professionals at a time of increasing compliance requirements, Thales has developed a new range of data security capabilities delivered as a service.

In 2017, it launched SafeNet Data Protection On Demand, a one-stop marketplace of cloud-based HSM, key management, and encryption solutions. Each service is delivered through a simple, intuitive, web-based interface, fully managed by experienced security professionals and hosted on highly robust and scalable architecture.

SafeNet Data Protection On Demand offers all the Cloud HSM features you'd expect of a mature cybersecurity solution provider and is suited to any type of on-premises, public cloud, hybrid, or multi-cloud environment.

It boasts a growing range of integrations that support the growth of MSPs and MSSPs through upsell and cross-sell opportunities, including options for Microsoft Active Directory, CyberArk, and Oracle TDE encryption key storage.

SafeNet Data Protection On Demand is designed to save you time and money. You do not need high levels of IT or security skills and can deploy any service at the click of a button. What's more, with our usage-based pricing and no hardware to purchase, customers only pay for what they actually consume.

Cloud HSM from Thales, part of the SafeNet Data Protection On Demand cloud-based service, is a simple step to enhance your portfolio.

This is where Thales can help, by giving you BOTH options to fulfilling your customer's' needs and demands. Leverage our market-leading on premises HSMs, together with our groundbreaking Cloud HSM service, to provide the ideal solution for your customers' hybrid environments.

Find Out More

It has never been easier to grow your service offering. Ask Thales how you can add new data security services without making any capital investment, deploying any new hardware, or heavily investing in customer support training.

Your customers rely on you for secure cloud deployments, service providers rely on Thales. Download our product brief to learn more about SafeNet Data Protection On Demand, or visit our online marketplace to start your FREE 30-day product evaluation.

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 814 | E-mail: asia.sales@thales-.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-.com

> thalescpl.com <