Solution Brief

THALES

CYBERSECURITY



Top 10 Reasons for Using the Thales payShield Cloud HSM Service

cpl.thalesgroup.com

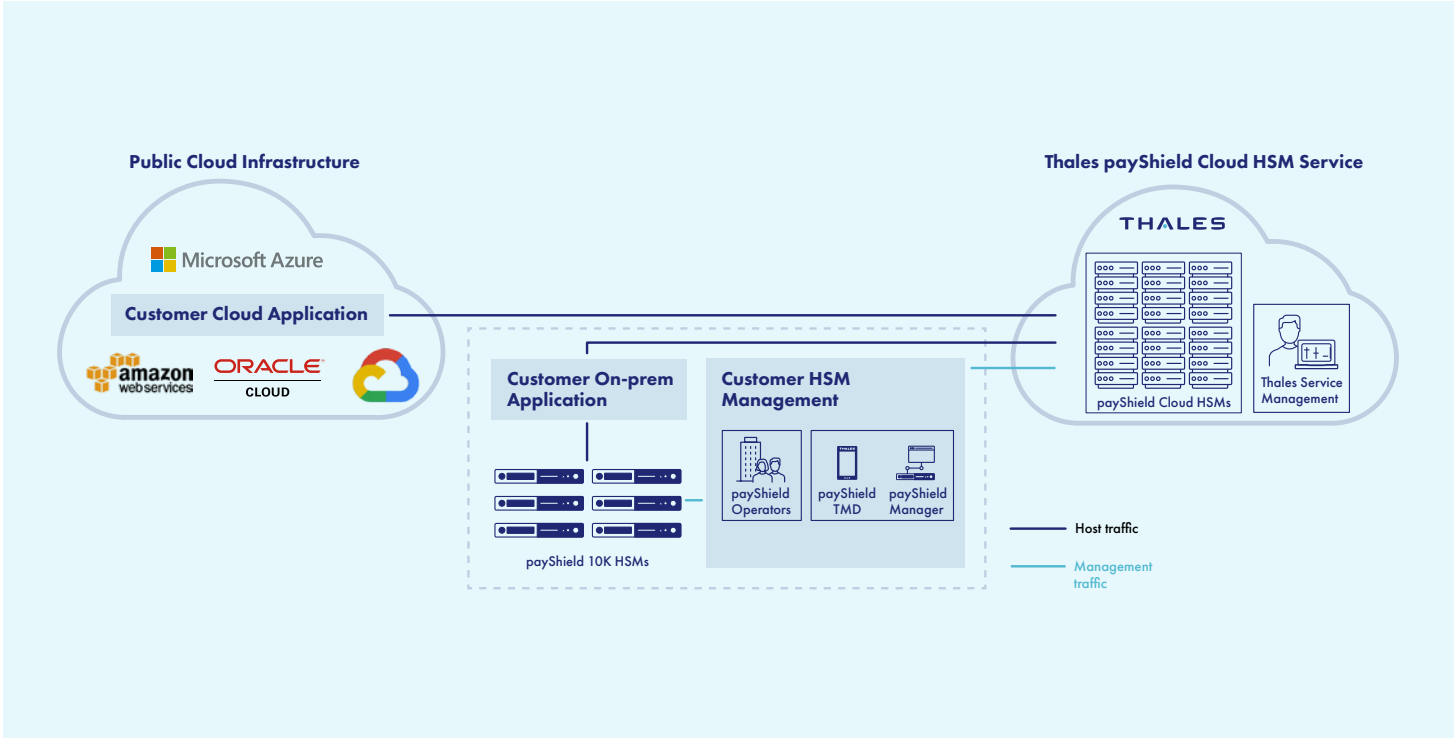


THALES

CYBERSECURITY

Payment hardware security modules (HSMs) play a fundamental role in securing payment transactions. For many years the only option available to the vast majority of financial institutions, payment networks and service providers was to purchase their payment HSMs outright and install, configure, operate and manage them in data centers under their control. Today this perpetual ownership restriction no longer applies organizations have a choice when they select Thales payment HSM technology to meet their security needs – continue to deploy on-prem HSMs, subscribe to a hosted HSM cloud service or take a hybrid approach (which contains a mixture of on-prem and cloud HSMs).

As the recognized market leader, Thales is determined to make it as easy as possible for its existing and new customers to make use of payment HSMs securely hosted in the cloud while ensuring that any longer term migration away from on-prem HSM technology is performed in an efficient, cost effective and low risk manner. payShield Cloud HSM is a hosted service offered by Thales where users have full access to dedicated payShield HSMs under their control via flexible subscription options. This brochure explains the numerous efficiency, flexibility and security benefits associated with the service, helping any potential user to make an informed decision.



Efficiency

1 Bring new applications to market faster

The payShield Cloud HSM service from Thales is designed specifically to help accelerate your ongoing projects by enabling efficient and early access to the payment HSM technology you will need. For new projects it offers you the ability to eliminate on-prem infrastructure dependencies by facilitating a cloud-native environment right from the outset. Through the OPEX subscription model, you avoid having to make significant upfront investments in infrastructure while enabling you to test new concepts quickly with minimal investment or long term commitment. For established users of on-prem payment HSM technology you get the best of both worlds – you can use the cloud HSMs for new applications without disrupting your production environments and in parallel you can plan a longer term migration to the cloud for existing applications.

2 Reduce time for HSM deployment

A significant efficiency benefit of using a cloud HSM rather than an on-prem HSM occurs when you need to deploy an HSM quickly. The cloud service eliminates your involvement in the early activities of a typical deployment phase such as organizing delivery, secure handling, booking data center slots, installation into racks, cabling and performing some preliminary functional tests – all critical and necessary before you can start taking advantage of the device in your development, test or production environment. Thales takes care of all of this on your behalf so that when you need an extra HSM, for whatever reason, you simply start a new subscription – your HSM is ready and waiting, saving you days, if not weeks, in real time.

3 Share service access to staff across multiple geographical regions

When you subscribe to the payShield Cloud HSM service, you gain much more flexibility regarding how each HSM in question can be shared throughout your organization. For example in the development or test phase of a project, all team members (who might be geographically dispersed around the world) can access, configure, manage, monitor and operate any HSM at any time, 24x7, using the extensive remote management capabilities and with no need to host HSMs locally or travel to data centers. In a production environment, country boundaries are eliminated as staff in multiple countries can access the HSM cloud pool in a different country to where they reside while still maintaining the highest levels of security.

4 Manage your cash flow more effectively

The OPEX subscription model associated with the service means that you do not need to fund upfront investments in HSM infrastructure. Your costs are predictable and split into monthly payments. Valuable IT staff are freed up to carry out other tasks. In the future when you need to move to a newer certified model of payShield HSM, you simply update your subscription to utilize the new device. The on-prem challenge of planning a physical swap-out is eliminated when, for audit reasons, a newer hardware model is necessary for ongoing compliance.

Flexibility

5 Add HSMs on demand

A key advantage of the well managed Thales cloud service is that there are always some HSMs unallocated waiting for a user to subscribe. This instant availability to a 'ready-to-deploy' HSM, eliminates the order planning, delivery, installation and basic commissioning of each HSM, enabling you to expand your HSM capacity much more in line with your business growth. For example, you could upgrade to a higher performance subscription or take out additional subscriptions to meet increased capacity demands. The latest base software is always available and you can leverage the Thales Professional Services team to develop and maintain any custom software functionality you may need.

6 Choose from a range of public clouds for application integration

You might begin using the cloud service with your on-prem applications for reasons such as backup or additional processing capacity. Alternatively you may be in the process of migrating your off-the-shelf or home-grown payment applications to the cloud as part of a corporate digital transformation initiative and the cloud HSM is what you need for early integration testing. The Thales data centers where the payShield Cloud HSMs are hosted are present in a range of locations where there is a low latency, high performance and secure communication link to a public cloud service provider (CSP) in close proximity. The Thales service is proven to work seamlessly with applications hosted by the major public CSPs – Microsoft Azure, Amazon Web Services, Oracle Cloud and Google Cloud.

7 Operate a hybrid payment HSM environment

The payShield Cloud HSMs have total backwards compatibility with the on-prem payShield 10K HSMs– no application changes are needed, any existing custom software is supported and the same sets of master keys can be used. There is no need to modify operational or security procedures. Importantly, hybrid estates are both feasible and encouraged. All HSMs can be managed using payShield Manager, payShield Monitor and the payShield Trusted Management Device (TMD) – a consistent set of proven remote management and monitoring tools for use with all Thales payShield HSMs. The mix of on-prem or cloud HSMs can be adjusted relatively quickly to support evolving business needs, giving you maximum flexibility.

Security

8 Gain faster access to the latest certified payment HSM technology

Thales ensures that all its payment HSMs have the latest relevant certifications based on global standards such as PCI HSM and FIPS 140 together with regional standards such as AusPayNet, CB-HSM and GBIC. The cloud service enables you to switch to the latest certified HSM instance seamlessly, irrespective of whether it involves a hardware change or software enhancement. This avoids the challenge of planning for future HSM physical replacement which is inherent in the alternative, traditional perpetual ownership model.

9 Maintain control of your security posture

You retain absolute control of your keys and security configurations with your cloud HSMs – identical to your on-prem payShield HSMs. Thales is not involved in your production security policies or procedures. When you activate your subscription to the service, Thales has no access to your cryptographic keys or sensitive data. If you wish to terminate a subscription, all keys and data are securely erased as part of any associated secure deallocation process before the HSM in question is assigned to another subscriber. You are always in complete control, including when activating additional HSM subscriptions to support the load balancing, disaster recovery and backup needs of your payment application workloads.

10 Leverage secure segregation and sharing capabilities

The HSMs used in our cloud service are single-tenant by design and hence no HSM is shared between service users from different organizations. This provides peace of mind that the HSMs managed through your subscriptions are securely segregated and no one else, which includes Thales, can gain access to your keys or data. In addition, for many years Thales payment HSM customers have taken advantage of the multiple Local Master Key (LMK) feature of the HSM to securely share a single HSM between different applications. The payShield Cloud HSM service offers a similar capability, enabling you to maximize the utilization of each HSM subscription while keeping the keys segregated for your individual applications.

Key Benefits

- Flexibility – simplifies sharing of production HSMs across multiple applications, staff and regions
- Future proof – offers access to the latest certified payShield hardware and software on demand
- Scalability – enables extra HSMs to be added quickly for resilience, backup or capacity
- Cloud agnostic – works seamlessly with fast connections to all major public cloud providers (Microsoft Azure, Amazon Web Services, Oracle Cloud and Google Cloud)
- Cash flow – avoids up-front investment by offering a flexible, monthly subscription service to improve cash flow

About payShield

payShield is constantly evolving to help secure your business transactions. For more information visit our website.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

© Thales - October 2026 • AC. v9