NCIPHER

www.ncipher.com

Stronger security and control across your cloud estate

- Access to crypto functionality via APIs speeds app development
- Remote capabilities expedite access to crypto functionality and reduce administrative costs
- HSM-strength protection and control of keys enables stronger cloud security
- BYOK keeps you in control of your data in public cloud environments

Cloud security solutions

CLOUD: RAPID GROWTH, INCREASING RISKS

With 96% of businesses now relying on cloud computing, including 81% that use multiple cloud environments*, cloud adoption is no longer a trend but the new normal. And the benefits are clear as enterprises now find that cloud platforms are able to replicate – or even exceed – the features and benefits found in their on-premises counterparts, without the maintenance and hardware costs.

This requires enterprises to place more emphasis on a critical issue related to cloud computing and storage: how to ensure the integrity and protection of sensitive data.

Traditional approaches to the cloud either place reliance on the cloud service provider for security or simply leave gaps in coverage. Neither option is acceptable in today's business environment, where sophisticated attackers and rigorous compliance mandates have raised the bar for data protection requirements. What's needed instead is a security approach that keeps *you* in control of your data.

*RightScale 2018 State of the Cloud Report

Cloud security solutions

nCipher HSMs and integrated applications from leading technology partners empower our customers with stronger security and control over their cloud environments. Our solutions enable multi-cloud data protection, provide crypto as a service and deliver strong control of business-critical keys, allowing organizations to advance their cloud strategies with confidence.

PRODUCT-SPECIFIC CAPABILITIES

Bring your own key to the cloud

One of the advantages of the cloud is that services can be quickly deployed and scaled on an as-needed basis. In order to secure your data in this environment, you need to control the encryption keys used by cloud applications. Maintaining control over encryption keys and application secrets is essential for enhanced trust and the robustness of the public cloud service.

Encryption in the cloud using keys generated and protected on your premises means you stay in control of your data in public cloud environments. nShield bring your own key (BYOK), based on nShield HSMs, lets you generate strong keys in your on-premises HSM and securely export those keys to your cloud applications, whether hosted in Amazon Web Services, Google Cloud Platform, Microsoft Azure or all three.

Azure Key Vault with enhanced key controls enabled by nShield HSMs

nCipher also partners with Microsoft to deliver a unique version of BYOK, which offers the highest levels of cloud key protection and provides the ability to create your own secure vault in the cloud. With the Azure Key Vault, you use your own nShield HSM to generate and transfer keys securely to an nShield HSM in the cloud owned by Microsoft. The HSM safeguards cryptographic keys independently of the software environment in the cloud. Microsoft holds a local copy of your key, and only appropriately authorized applications within Azure can make use of your key. The key can be replicated between HSMs for disaster recovery, but the hardware does not allow your key to be visible outside the HSMs.

Cryptography as a service

nCipher's RESTful APIs give applications streamlined access to cryptographic key and data protection services, whether those applications reside locally, in the cloud or in a remote data center. As a result you can more easily implement security in both traditional data center and cloud deployments through clientless access to nShield HSMs.

nShield users can implement their key management and crypto functionality independently of their applications and the underlying infrastructure, increasing flexibility and minimizing the time from project inception to application deployment. Furthermore, fine-grained policies can be defined based on both role and user identity, ensuring processes or users can only perform the cryptographic, management or administrative operations assigned to their role and individual identity.

Centralized key management

Your critical business applications and data deserve the strongest security controls, often requiring encryption keys on demand. But managing and protecting encryption keys across disparate applications and teams is a daunting challenge. That's why nCipher partners with leading technology providers like Cryptomathic and Fornetix to deliver high assurance, highly-scalable key management. The nShield HSM provides strong key generation through its high entropy random number generator and the hardened environment provides FIPS and Common Criteria certified protection of the underpinning encryption keys and the security of the entire system.

RELENTLESS FOCUS ON THE CLOUD

nCipher's development team continues to enhance the nShield product line to keep pace with your evolving cloud security requirements. Features enabling your cloud strategy include:

Remote administration and configuration

nShield Connect XC delivers new remote configuration functionality that builds on the product's remote administration features and high availability improvements to meet customer demand for easier management and scalability of their nShield HSMs.

nShield Connect XC customers can avoid time-consuming trips to the data center and remotely perform both routine maintenance and complex configuration tasks such as:

- Upgrading HSM firmware
- Adding a new HSM to their pool
- Initiating and changing an HSM's IP address
- Purging all key material at the end of a usage cycle
- Setting up the Remote File Server

Key isolation

nShield's unique Security World enables applications or users, sharing cryptographic infrastructure resources, to be securely isolated from each other. This flexibility to isolate keys supports cloud strategies, particularly when HSMs are managed centrally and their functions are provisioned to distinct entities, whether they are within the same enterprise or independent clients. As a result, you can more cost-effectively provide access to cryptographic resources by maximizing the utilization of your HSM estate.

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com