

## **New nCipher HSM as a Service delivers high-assurance security for organizations adopting cloud-first strategies**

*nShield as a Service provides cryptography on-demand using cloud-based nCipher hardware security modules (HSMs), and allows secure code execution in the cloud*

**Cambridge, UK and Sunrise, FL – September 17, 2019** – nCipher Security, an [Entrust Datacard company](#), announces [nShield as a Service](#), a cloud-based hardware security module (HSM) service that allows organizations to protect sensitive data and applications and helps meet compliance mandates – simply and efficiently, using on-demand cryptography.

“Organizations embracing cloud-first strategies require cloud-first encryption,” said Peter Galvin, vice president of strategy, nCipher Security. “This means remote, automated management at scale, and flexible access control both in the cloud and onsite. nShield as a Service makes it easy to adopt a secure, multi-cloud encryption strategy using the same nShield HSMs organizations deploy onsite today.”

nShield as a Service is ideal for cloud-first strategies, selective cloud migration, or adding HSM capacity to handle workload spikes. The customer experience is consistent and familiar – users interact with the cloud-based nShield® HSMs in the same way as with nShield appliances in their own data centers. And customers utilizing nCipher’s unique secure execution environment to run sensitive application code within a secure FIPS-validated boundary now have that same opportunity using cloud-based as well as on premises HSMs.

Using nShield as a Service, customers can:

- implement Bring Your Own Key and Host Your Own Key solutions with a trusted third party service
- maintain full control over key material and maintain separation of data from the encryption keys
- extend cloud-based cryptography and key management across multiple clouds
- implement secure code execution for cloud-based workloads
- integrate with third party applications in the cloud

“The nShield as a Service launch highlights the synergies we’ve gained since becoming an Entrust Datacard company in June,” Galvin said. “We were able to accelerate and enhance nShield as a Service by combining our HSM and cryptography expertise with Entrust Datacard’s experience in data centers, cloud services and HSM operations. The result is a powerful HSM as a service solution that complements the company’s cloud-based PKI and IoT security solutions.”

“Encryption is a powerful tool,” said Robert Westervelt, Research Director, Security Products, IDC. “Delivering it easily across distributed infrastructure can be very effective in protecting data and applications against cyberattacks. Solutions such as nShield as a Service allow even the largest organizations to secure their public cloud workloads with all the conveniences of software-as-a-service offerings. Now, there are no excuses for not using encryption in the cloud.”

## **How nShield as a Service works**

nShield as a Service uses nShield HSMs to generate, access and protect cryptographic key material separately from sensitive data. All nShield HSMs are managed through nCipher's unique Security World key management architecture that spans cloud-based and on premises HSMs. This lets customers efficiently scale HSM operations while retaining control of their key material, even if they change their cloud service provider.

Organizations can utilize nShield as a Service to supplement or replace on premises HSMs, while keeping the benefits of HSM ownership. The subscription model lets enterprises budget predictably, manage capacity, reduce data center footprint and decrease time spent on routine maintenance and monitoring.

Customers seeking cloud-first solutions can work with market-leading cybersecurity and infrastructure vendors in nCipher's [nFinity Strategic Technology Partner program](#), including F5, IBM, Micro Focus Voltage, Red Hat, Venafi, and Citrix (see quote sheet below). Applications include SSL/TLS, code signing, data and database encryption and more.

## **nCipher Security nFinity Strategic Technology Partners talk about nShield as a Service:**

### **F5**

"F5 has deep experience in application delivery and security services and helps customers protect their critical applications, ensuring they are safe, secure, and available. The launch of nShield as a Service from nCipher Security gives F5 customers enhanced security choices with the ability to achieve data sovereignty on a subscription-based model. Shifting security from a capital to an operational expenditure enables greater flexibility and cost-effectiveness for organizations," said John Morgan, VP & GM of Security at F5 Networks.

### **Rick Robinson, WW Offering Manager, Encryption and Key Management, IBM Security:**

"As enterprises increasingly migrate business processes to the cloud, security continues to be a major concern. Ensuring that critical applications and their underpinning cryptographic keys can be protected and managed throughout their lifecycle is vital. The launch of nShield as a Service from nCipher Security gives our joint customers greater choice and the ability to have subscription-based data sovereignty," said Rick Robinson, WW Offering Manager, Encryption and Key Management, IBM Security.

### **Micro Focus Voltage**

"Data is one of the most abundant and valuable assets for an organization today," said Reiner Kappenberger, Director Product Management, Voltage Data Security at Micro Focus. "However, without reliable ways to protect data at rest, in motion, and in use, these very assets can become liabilities. As Voltage SecureData customers increasingly migrate storage and workloads to cloud-based environments, they are looking to establish an HSM-based root of trust in the cloud that can maintain the highly available, highly performant data-centric solution they currently enjoy. nShield as a Service from nCipher Security, through its support of Voltage SecureData's innovative Stateless

Key Management, enables Micro Focus to offer its customers continuing relief from the burden of traditional key management in both hybrid and zero data center cloud deployments.”

## **Red Hat**

“As a long-standing nCipher Security nFinity technology partner and the world’s leading provider of open source solutions, Red Hat is committed to providing customers with more choices to enhance. nShield as a Service from nCipher will offer expanded choice to our customers in how they pursue IT security to better protect the underlying cryptographic keys that help to secure Red Hat Certificate System and Red Hat OpenStack Platform deployments across the hybrid cloud,” said Keith Basil, Senior Principal Product Manager at Red Hat.

## **Venafi**

“As the leader in machine identity protection, Venafi welcomes the launch of the new nShield as a Service capability from nCipher Security,” said Kevin Bocek, VP Security Strategy and Threat Intelligence at Venafi. “With the number of machines growing exponentially, and the definition of machines expanding to include everything from containers in Kubernetes clusters running in cloud to embedded IoT devices that will be deployed for the next 20 years, securing machine identities is critical for every business and government. The new nShield as a Service delivers the same robust root of trust that customers have come to depend on with on-premises nShield HSMs, adding a subscription-based security alternative that is easy to use, flexible, and cost-effective for organizations no matter their size. This is an exciting development that will help fast DevOps and security teams move at cloud speed to secure TLS and code signing keys certificates.”

## **Citrix**

“At Citrix, we are committed to providing companies with simple and efficient tools that enable them to deploy and manage all of their applications in a unified, secure and reliable manner,” said Marissa Schmidt, Senior Director, Product Management, Citrix. “nCipher nShield HSMs allow our customers to establish a root of trust and facilitate FIPS compliance. And with the addition of nShield as a Service to the nCipher HSM portfolio, they can do it in a more simple and flexible way.”

## **About nCipher Security**

nCipher Security, an [Entrust Datacard company](#), is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business-critical information and applications. Today’s fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business-critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. [www.ncipher.com](http://www.ncipher.com)

Follow us on [LinkedIn](#), [Twitter](#), [Facebook](#) and [Instagram](#) – search nCipherSecurity.

###

For more information please contact:

**nCipher Security**

Megan Nemeš [megan.nemeh@ncipher.com](mailto:megan.nemeh@ncipher.com) +1 408 887 5064

Liz Harris [liz.harris@ncipher.com](mailto:liz.harris@ncipher.com) +44 7973 973648