

## nCipher Security helps Zerto establish integrity of its business applications

*Founded in 2010, Zerto has been built on a unique vision that disaster recovery technology should not be an insurance policy, but a competitive advantage.*

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption through IT resilience. By replacing multiple legacy solutions with a single IT Resilience Platform™, Zerto combines disaster recovery, backup and cloud mobility in a simple, converged solution. With enterprise scale, Zerto's software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds.

Zerto has disrupted IT markets and pushed the bounds of disaster recovery. The company has developed its innovative product on continuous data protection technology, and, in a world where uninterrupted technology is non-negotiable for enterprises, become much more than just a tool for disaster recovery.

### BUSINESS CHALLENGE

As a leading provider of IT Resilience, Zerto management needed assurance its own business systems weren't vulnerable to compromise. The most effective strategy for doing so was to ensure its Public Key Infrastructure (PKI) was trusted.

A PKI infrastructure is a set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public keys. PKIs help establish the identity of people, devices, and services – enabling controlled access to systems and resources, protection of data, and accountability in transactions. Next generation business applications are becoming more reliant on PKI technology to guarantee high assurance as evolving business models are becoming more dependent on electronic interaction requiring online authentication and compliance with stricter data security regulations.

In order to bind public keys with their associated user (owner of the private key), PKIs use digital certificates. Digital certificates are the credentials that facilitate the verification of identities between users in a transaction. Much as a passport certifies one's identity as a citizen of a country, the digital certificate establishes the identity of users within the ecosystem. Because digital certificates are used to identify the users to whom encrypted data is sent, or to verify the identity of the signer of information, protecting the authenticity and integrity of the certificate is imperative to maintain the trustworthiness of the system. This was essential to Zerto's business model as a trusted vendor.

# Zerto



*“Compared to other suppliers nCipher’s implementation and support are better, nShield Solo is easier to use and back up, and we also like the nShield’s graphical user interface (GUI).”*

*“nShield Solo HSM securing our CAs provides us with peace of mind. Our management feels the risk reduction is well worth the cost of installing the nShield Solo HSM.”*

– Nadav Svirsky, Corporate IT Infrastructure Lead, Zerto



## TECHNICAL CHALLENGE

Certificate authorities (CAs) issue the digital credentials used to certify the identity of users. CAs underpin the security of a PKI and the services they support, and therefore can be the focus of sophisticated targeted attacks. In order to mitigate the risk of attacks against CAs, physical and logical controls as well as hardening mechanisms, such as hardware security modules (HSMs) have become necessary to ensure the integrity of a PKI.

Zerto uses a Microsoft platform and IT knew from working with Microsoft that best practice to secure its CAs was to use an HSM. Offering an independently certified, tamper-resistant environment, HSMs are an integral part of securing sensitive keys and business processes.

## SOLUTION

Zerto's IT team had experience with multiple HSM vendors and chose nCipher Security's nShield Solo. According to Nadav Svirsky, Corporate IT Infrastructure Lead, Zerto chose nCipher over other vendors because "Compared to other suppliers nCipher's implementation and support are better, nShield Solo is easier to use and back up, and we also like the nShield's graphical user interface (GUI)."

## RESULTS

Zerto does not share its quantifiable results from the installation of the nShield Solo to protect its CAs. In reference to now having best practice CA security, which was the initial goal of the project, Svirsky notes "Our customers need to be confident that our systems are secure and trustworthy. Unfortunately, you frequently cannot see the value of data security until something goes wrong. Then you see a company's reputation, sales and share price drop. So, having the nShield Solo HSM securing our CAs provides us with peace of mind. Our management feels the risk reduction is well worth the cost of installing the nShield Solo HSM."

## PERFORMANCE, RELIABILITY AND PROTECTION

### Business need

- o Reduce risk of internal data security problems

### Technology need

- o Secure root of trust for CA servers at a reasonable cost

### Solution

- o nShield Solo HSM

### Result

- o Risk reduction
- o Peace of mind for Zerto management

## ABOUT NCIPHER SECURITY

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security, a leader in the general purpose hardware security module (HSM) market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the 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, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. [www.ncipher.com](http://www.ncipher.com)

Search: nCipherSecurity



nCipher - June 2019 - Zerto

[www.ncipher.com](http://www.ncipher.com)

