Entrust helps Zerto establish integrity of its business applications

Zerto

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.

> **Compared to other suppliers Entrust's implementation and support are far better. Entrust nShield HSMs are easier to use and back up, and we also like the graphical user interface (GUI).**
>
> – Nadav Svirsky, Corporate IT Infrastructure Lead, Zerto

Zerto

BUSINESS CHALLENGE

As a leading provider of IT Resilience, Zerto needed assurance that 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.

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.

Zerto

> **Deploying Entrust nShield HSMs to secure our CAs provides us with peace of mind. Our management feels the risk reduction is well worth the investment.**
>
> – Nadav Svirsky, Corporate IT Infrastructure Lead, Zerto

SOLUTION

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

RESULTS

Zerto does not share its quantifiable results from the installation of Entrust nShield HSMs 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, putting in place Entrust nShield Solo HSMs to secure our CAs provides us with peace of mind. Our management feels the risk reduction is well worth the investment."

Zerto

PERFORMANCE, RELIABILITY AND PROTECTION

Business need

- Reduce risk of internal data security problems

Technology need

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

Solution

- Entrust nShield Solo HSMs

Result

- Risk reduction
- Peace of mind for Zerto management

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com