nShield as a Service Cloud Disaster Recovery

Off-site failover as a service to increase redundancy and resiliency for on-premises hardware security module (HSM) estates

Overview

As organizations continue to consider migrating data processing and applications to the cloud, many may not be ready to fully transfer their cryptography outside their controlled perimeter, preferring to keep critical HSM estates on-premises. Deploying HSM backups off-site or having alternate on-premises data centers for high assurance failover can be expensive and labor-intensive when considering the cost of hardware, deployment, management, and maintenance.

Organizations needing to increase redundancy and resiliency of on-premises HSM estates can be faced with this challenge as they try to manage the expense of purchasing additional HSM backup units and the cost of deployment, management, and maintenance. A hybrid approach where the failover HSM is enabled through an off-site managed as a service model can offer a convenient and cost-effective alternative that delivers the increased redundancy and resiliency that the organization needs.

The Solution

nShield as a Service Cloud Disaster Recovery provides an accessible and flexible cloud-based failover capability for on-premises nShield HSM deployments. The solution enables organizations with in-house HSM estates to easily increase the redundancy and resiliency of their deployments, without having to add in-house equipment and personnel resources.

FLEXIBILITY TO MEET YOUR NEEDS WHEREVER AND WHENEVER YOU NEED IT

Entrust nShield as a Service Cloud Disaster Recovery provides the ability to generate, access, and protect your cryptographic keys, while achieving high assurance and data sovereignty within your jurisdiction, wherever and whenever you need it.

Learn more about nShield as a Service at entrust.com

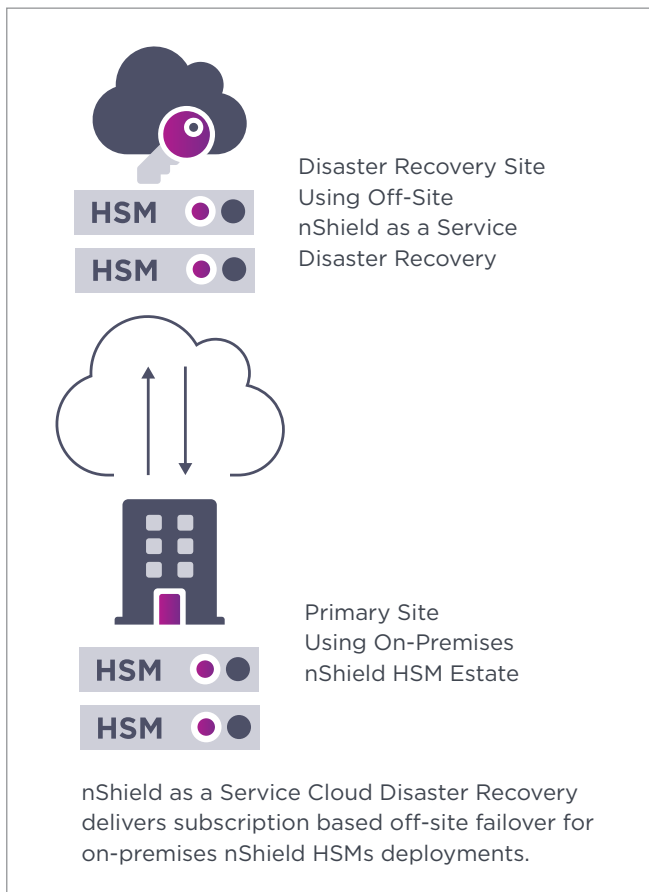# nShield as a Service Cloud Disaster Recovery

Benefits

nShield as a Service Cloud Disaster Recovery requires no changes to organizations' application environment. Customers only need to initialize their dedicated cloud-based HSM into the existing on-premises nShield key management framework, update the configurations to define failover rules, and off they go. Service delivers:

- Certified off-site cryptographic resources

- Increased HSM redundancy and resiliency

- Improved convenience and time to value

Disaster Recovery Site
Using Off-Site
nShield as a Service
Disaster Recovery

Primary Site
Using On-Premises
nShield HSM Estate

nShield as a Service Cloud Disaster Recovery delivers subscription based off-site failover for on-premises nShield HSMs deployments.

Deployment

nShield as a Service Cloud Disaster Recovery requires no additional hardware on-premises or up-front capital investments. The subscription-based pricing model enables organizations to pay for what they need when they need it. The service is offered as a self-managed off-site single HSM with a 99% service level agreement (SLA) licensed for up to 10 client hosts or application integrations. For larger deployments, additional client licenses are available. Because nShield as a Service benefits from the same unique Security World key management framework as on-premises nShield deployments, migrating from on-premises data centers to the cloud for disaster recovery is easy, and can be accomplished quickly. The unified nShield Security World ecosystem delivers scalability and load balancing.

Using a dedicated FIPS 140-2 Level 3 and Common Criterial EAL4+ certified nShield HSM in the cloud means the organization will never share hardware. This allows customers to maintain complete control over back-up capability and their keys, with no impact on compliance audits. Organizations not yet fully migrated to the cloud can begin their journey through this quick and convenient disaster recovery option as they familiarize themselves with further cloud adoption.

nShield as a Service Cloud Disaster Recovery

Features

High Availability: Delivers 99% SLA across cloud backup deployments to ensure failover capability.

Global Coverage: Deployed in data centers around the globe (AU, EU, UK, US), enabling you to back up operations within your jurisdiction to fulfill data sovereignty requirements.

Certified Security: Uses dedicated FIPS 140-2 Level 3 and Common Criteria EAL4+ certified nShield HSMs.

Cost-Effective: Flexible subscription-based service enables you to replace capital expenditures with operational expenditures and pay as you go.

Trusted Execution: CodeSafe functionality is also available, ensuring critical and sensitive processing can be maintained in the event of a disaster.

The Entrust Difference

Entrust has over 20 years' experience delivering proven HSM technology to the world's most security-conscious organizations. Only Entrust features the nShield Security World key management framework that lets customers build and grow their HSM environment, institute granular controls over access and usage of keys, and deliver scalability. With nShield as a Service Cloud Disaster Recovery, organizations can seamlessly add off-site failover to increase redundancy and resiliency.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223