Entrust, Zerto 비즈니스 애플리케이션의 무결성 구현 지원

Zerto

Zerto는 재해 복구 기술이 보험 정책이 아니라 경쟁 우위가 되어야 한다는 고유한 신념을 바탕으로 2010년에 설립되었습니다.

Zerto는 현대화와 클라우드 채택 시 동반되는 위험과 복잡성을 IT 탄력성을 통해 제거하여 고객이 IT 혁신을 가속화하도록 지원합니다. 여러 레거시 솔루션을 단일 IT Resilience Platform™으로 대체한 Zerto는 재해 복구, 백업·클라우드 이동성을 간편한 통합 솔루션으로 제공합니다. 엔터프라이즈 규모인 Zerto의 소프트웨어 플랫폼은 상시 고객 경험이 가능하도록 지속적으로 가용성을 제공하는 동시에, 하이브리드 클라우드와 다중 클라우드에서 애플리케이션을 자유롭게 보호, 복구, 이동할 수 있도록 워크로드 이동성을 단순화합니다.

Zerto는 IT 시장을 뒤흔들고 재해 복구의 한계를 뛰어넘었습니다. 또한, 혁신적인 데이터 지속 보호 기술 제품을 개발했으며, 기업들에게 중단 없는 기술이 필수적인 세상에서 단순한 재해 복구 도구 이상의 기업으로 성장했습니다.

> **"다른 공급업체에 비해 Entrust의 구현과 지원 수준이 훨씬 우수합니다. Entrust nShield HSM의 사용과 백업은 훨씬 간편하며 그래픽 사용자 인터페이스(GUI)도 뛰어납니다."**
>
> – Zerto의 기업 IT 인프라 책임자, Nadav Svirsky

ENTRUST.COM/HSM에서 자세히 보기

Zerto

비즈니스적 난관

IT 탄력성의 선두 제공업체인 Zerto는 자체 비즈니스 시스템이 손상에 취약하지 않다는 확신이 필요했습니다. 확신을 얻기 위한 가장 효과적인 전략은 PKI(공개 키 기반 구조)를 신뢰할 수 있는지 확인하는 것이었습니다.

PKI는 디지털 인증서와 공개 키를 생성, 관리, 배포, 사용, 저장 및 취소하는 데 필요한 하드웨어, 소프트웨어, 정책, 프로세스, 절차를 모은 기반 구조입니다. PKI는 사람과 장치, 서비스의 ID를 설정하여 시스템과 리소스에 대한 액세스를 제어하고 데이터를 보호하며 트랜잭션에 대한 책임을 부여합니다. 차세대 비즈니스 애플리케이션은 PKI 기술을 더욱 많이 활용하여 높은 수준의 보증을 제공하고 있는데, 이는 진화하는 비즈니스 모델로 인해 전자 소통의 비중이 커지고 있기 때문입니다. 전자 소통에는 온라인 인증이 필요하고 더 엄격한 데이터 보안 규정 준수가 요구되어 높은 수준의 보증이 필요합니다.

PKI는 디지털 인증서를 사용하여 관련 사용자(개인 키 소유자)와 공개 키를 바인딩합니다. 디지털 인증서는 트랜잭션 중 사용자 간 신원 확인을 용이하게 하는 자격 증명입니다. 여권이 한 국가의 시민으로서의 신원을 인증하는 것처럼, 디지털 인증서는 생태계 내 사용자 신원을 설정합니다. 디지털 인증서로 암호화된 데이터를 전송받는 사용자를 식별하거나 서명자의 신원 정보를 검증하기 때문에, 인증서의 신뢰성과 무결성을 보호하는 것은 시스템의 신뢰성 유지에 필수적입니다. 이는 Zerto 비즈니스 모델, 즉 신뢰할 수 있는 공급업체의 핵심입니다.

기술적 난관

인증 기관(CA)은 사용자의 신원을 인증하는 데 필요한 디지털 자격 증명을 발급합니다. CA는 PKI와 CA 지원 서비스 보안의 토대이므로 정교한 표적 공격의 대상이 될 수 있습니다. CA에 대한 공격 위험을 완화하려면, 물리적·논리적 제어뿐만 아니라 HSM(하드웨어 보안 모듈)과 같은 강화 메커니즘으로 PKI의 무결성을 보장하는 것이 필수적입니다.

Zerto는 Microsoft 플랫폼을 사용하고 있으며 IT 부서는 Microsoft와의 협업을 통해 CA 보호를 위한 모범 방안은 HSM 사용이라는 것을 알고 있었습니다. 독립적으로 인증받은 변조 방지 환경을 제공하는 HSM은 민감한 키와 비즈니스 프로세스를 보호하는 데 필수적입니다.

Zerto

> **Entrust nShield HSM에 CA 보호를 안심하고 맡길 수 있었습니다. 우리 경영진은 위험 감소를 위해서는 투자 가치가 있다고 생각합니다.**
>
> – Zerto의 기업 IT 인프라 책임자, Nadav Svirsky

솔루션

여러 HSM 공급업체를 경험한 Zerto IT 부서는 이번 배포를 담당할 솔루션으로 Entrust nShield® Solo HSM을 선택했습니다. 기업 IT 인프라 책임자인 Nadav Svirsky에 따르면 Zerto는 "다른 공급업체에 비해 Entrust의 구현과 지원 수준이 더 우수하고 Entrust nShield Solo HSM의 사용과 백업은 훨씬 간편하며 그래픽 사용자 인터페이스(GUI)도 뛰어나기 때문에" Entrust를 선택했습니다.

결과

Zerto는 CA를 보호하기 위해 Entrust nShield HSM을 설치하여 얻은 정량화 결과를 공유하지 않습니다. 현재 프로젝트의 초기 목표인 모범 CA 보안 보유를 달성한 것과 관련하여 Svirsky는 "고객은 우리 시스템이 안전하고 신뢰할 수 있다고 확신할 수 있어야 합니다. 안타깝게도 무언가 잘못될 때까지는 데이터 보안의 가치를 알 수 없는 경우가 많습니다. 보안 문제가 생기면 기업의 평판과 실적, 주가 하락으로 이어지죠. Entrust nShield HSM에 CA 보호를 안심하고 맡길 수 있었습니다. 우리 경영진은 위험 감소를 위해서는 투자 가치가 있다고 생각합니다."라고 말했습니다.

Zerto

성능, 안정성 및 보호

비즈니스적 요구

- 내부 데이터 보안 문제의 위험 축소

기술적 요구

- 합리적인 비용으로 CA 서버 신뢰점 확보

솔루션

- Entrust nShield Solo HSM

결과

- 리스크 감소
- Zerto 경영진의 우려 경감

ENTRUST 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명이 넘는 동료 및 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com

Entrust는 미국 및/또는 기타 국가 내 Entrust Corporation 소유의 상표, 등록 상표 및/또는 서비스 마크입니다.
©2020 Entrust Corporation.