ENTRUST
SECURING A WORLD IN MOTION

TOP 5 중요한 이유

왜 NSHIELD HSM을 AZURE 배포에 추가해야 할까요

1 고객 데이터에 대한 책임은 귀하에게 있습니다

책임 분담 모델은 클라우드 서비스 제공 방식에 관계없이 데이터가 항상 고객의 책임임을 보여줍니다.

	서비스로서의 인프라(IaaS)	서비스로서의 플랫폼(PaaS)	서비스로서의 소프트웨어(SaaS)
고객 담당	데이터	데이터	데이터
	애플리케이션	애플리케이션	애플리케이션
	런타임	런타임	런타임
	미들웨어	미들웨어	미들웨어
	OS	OS	OS
제공자 담당	가상화	가상화	가상화
	서버	서버	서버
	저장소	저장소	저장소
	네트워킹	네트워킹	네트워킹

출처: https://gallery.technet.microsoft.com/Shared-Responsibilities-81d091

2 데이터 침해 증가

보고된 바에 의하면, 개인식별정보(PII)를 포함하는 소비자 정보의 노출 건수는 2018년 197.6백만 건에서 446.5백만 건으로 크게 늘어나 126% 급증한 것으로 나타납니다. 보고된 건의 50%만 침해 수를 밝히는 것을 고려하면, 실제 노출된 소비자 정보는 더 많을 가능성이 큽니다.

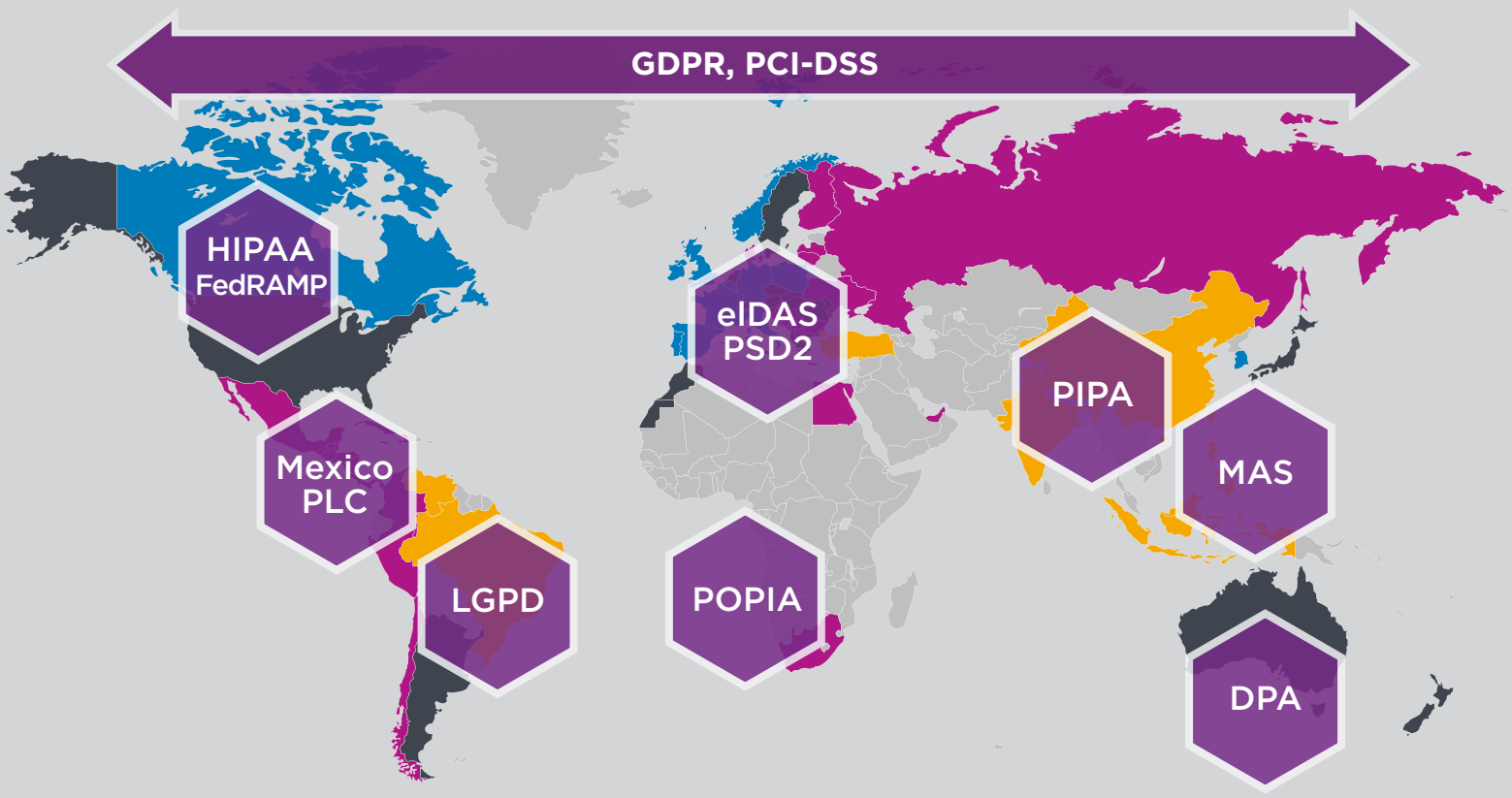
2018년 126% 폭등한 고객 데이터 노출

197.6백만 → 446.5백만

출처: Identity Theft Resource Center www.idtheftcenter.org/2018-data-breaches

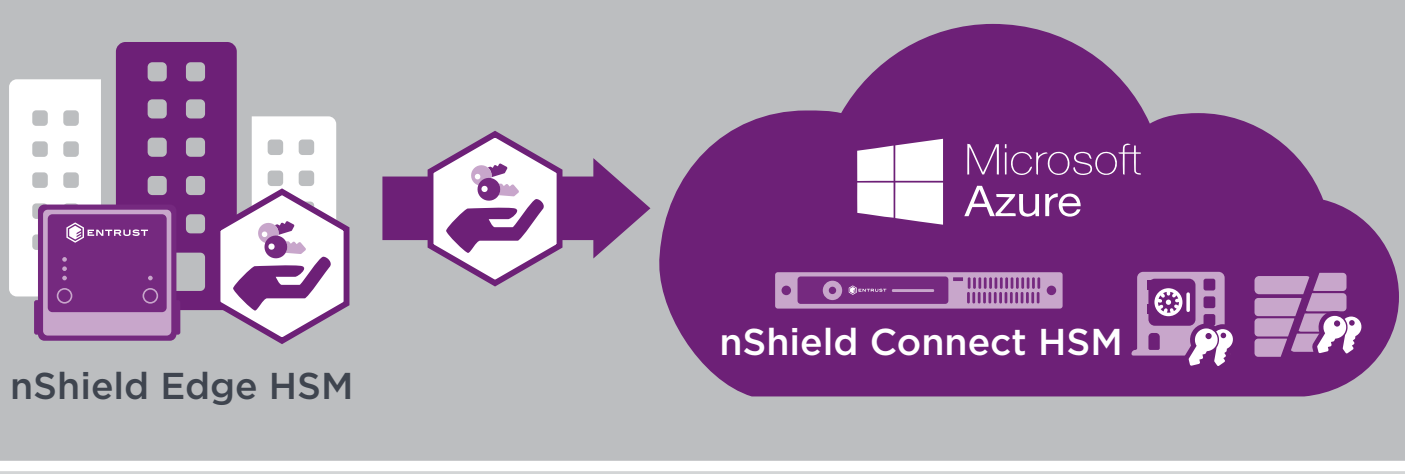
3 규정 준수 필요

전 세계적으로 개인정보 관련 법규가 새롭게 시행되면서 기업은 책임감, 관리책임 및 강화된 벌금에 직면하고 있습니다. nShield® 하드웨어 보안 모듈(HSM)은 귀사가 모범 사례를 이용할 수 있도록 보장합니다.



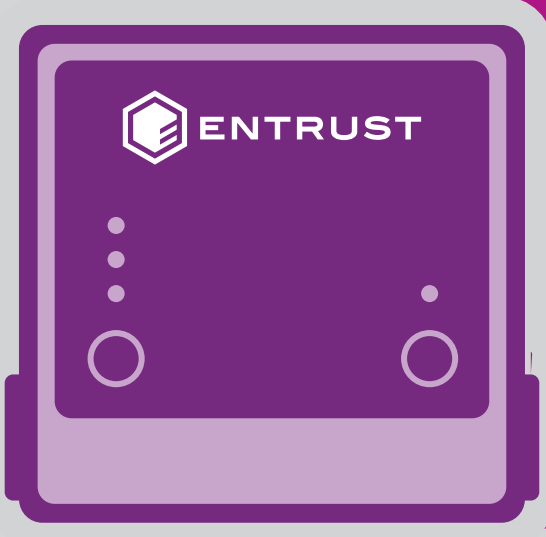
4 자체 키 관리 가능

BYOK(Bring Your Own Key)를 이용하여 암호키를 안전하게 보호함으로써 클라우드상의 데이터를 통제하고 보호할 수 있습니다. 귀사는 온프레미스에서 자체 키를 생성하고, 이 키는 클라우드의 HSM으로 안전하게 전송되며, Azure는 키를 사용하여 애플리케이션과 데이터를 보호하지만 이를 보거나 오용할 수는 없습니다.



5 클라우드에 신뢰점 구현

nShield HSM은 안전한 암호화 처리, 키 생성 및 보호, 암호화, HSM 키 관리 등에 적합한 강력한 변조 방지 환경과 함께 다음과 같은 이점을 제공합니다.



- 안전한 애플리케이션 플랫폼을 만드는 추가 보안 계층
- 암호화 작업과 키 분리
- 스마트 카드를 통한 강력한 사용자 인증
- 강화된 이중 제어 및 역할 분리
- 인증된 고성능 키 생성
- 강력한 암호화 가속화 및 오프로드 작업
- FIPS 140-2 인증

동영상 시청하기: *Entrust와 Microsoft Azure와 함께 하는 Bring Your Own Key*

entrust.com/HSM
에서 자세히 보기

ENTRUST
SECURING A WORLD IN MOTION