ENTRUST
SECURING A WORLD IN MOTION

TOP 5 REASONS TO ADD AN NSHIELD HSM TO YOUR AZURE DEPLOYMENT

1 YOU ARE RESPONSIBLE FOR YOUR CUSTOMER DATA

The shared responsibility model shows that regardless of how the cloud service is delivered, data is always the customer's responsibility.

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Customer responsibility	Data	Data	Data
	Application	Application	Application
	Runtime	Runtime	Runtime
	Middleware	Middleware	Middleware
	O/S	O/S	O/S
Provider responsibility	Virtualization	Virtualization	Virtualization
	Servers	Servers	Servers
	Storage	Storage	Storage
	Networking	Networking	Networking

Source: https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

2 DATA BREACHES ARE INCREASING

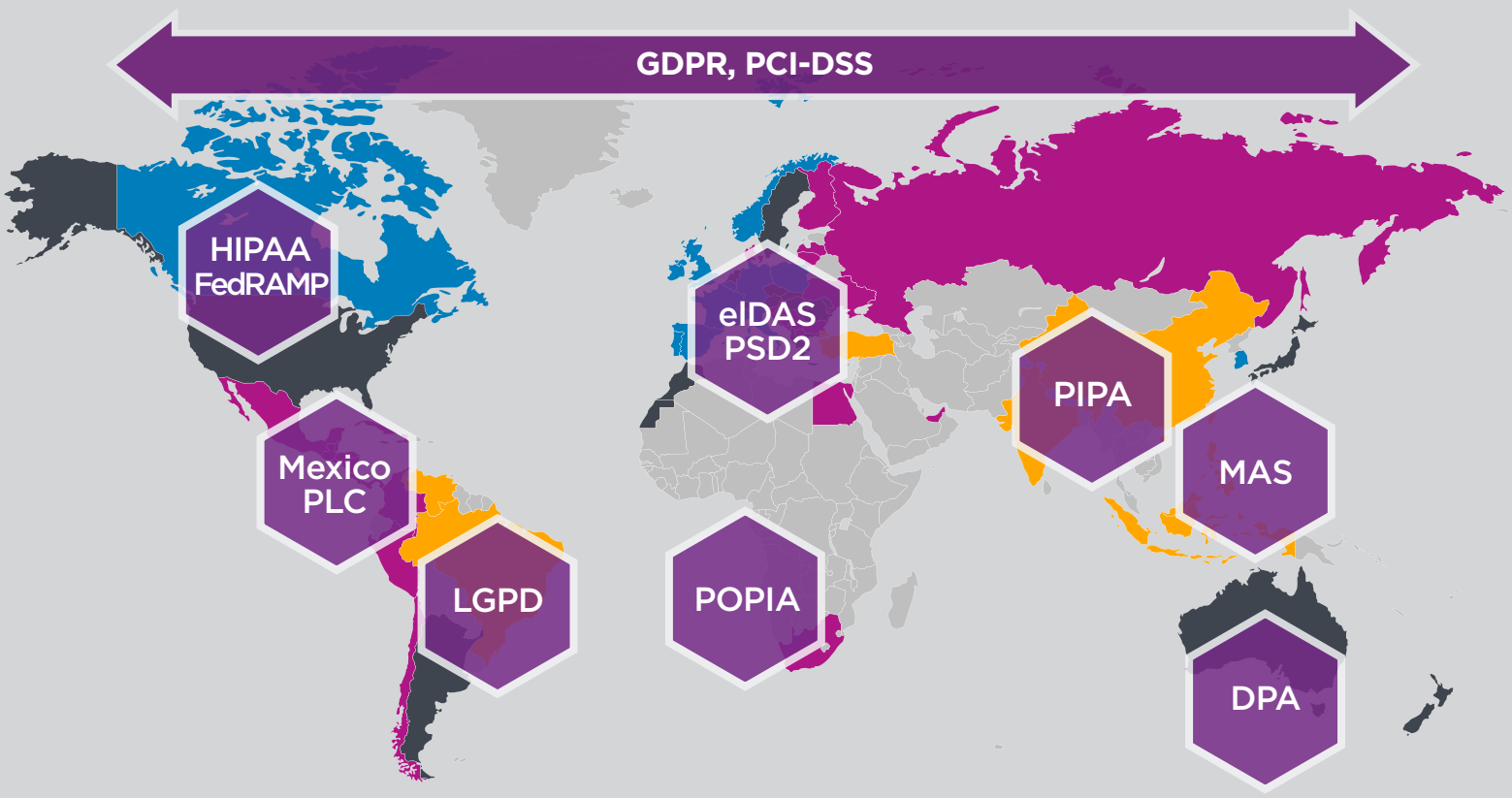
The reported number of exposed consumer records containing personally identifiable information (PII) significantly increased from 197.6 million to 446.5 million in 2018 – a 126% jump. The actual total number of records exposed is likely higher, given that only half of reported breaches disclose the number.

Exposed consumer data skyrocketed 126% in 2018

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

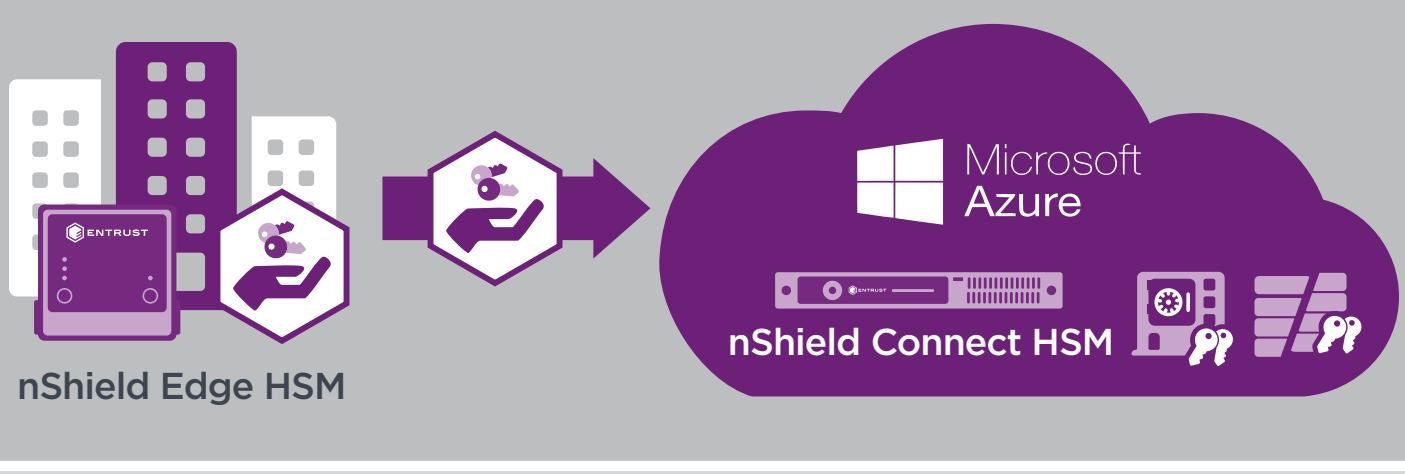
3 YOU NEED TO MEET COMPLIANCE REGULATIONS

New privacy regulations are being enforced across the globe meaning companies are facing increased responsibility, accountability and heavier fines. nShield® hardware security modules (HSMs) ensure you are using best practices.



4 YOU REMAIN IN CONTROL OF YOUR KEYS

With bring your own key (BYOK) you can control and protect data in the cloud using cryptographic keys securely. You generate your own keys on-premises, the keys are securely transferred to HSMs in the cloud, and Azure uses the keys to secure applications and data but cannot see or misuse them.



nShield Edge HSM

5 YOU ADD A ROOT OF TRUST TO YOUR CLOUD

nShield HSMs provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, HSM key management and more, providing:

- An additional layer of security to create a secure application platform
- Isolation of cryptographic operations and keys
- Strong user authentication via smart cards
- Enforced dual controls and separation of duties
- Certified, high performance key generation
- Powerful cryptographic acceleration and offload
- FIPS 140-2 certification

Click to watch our video *Bring Your Own Key with Entrust and Microsoft Azure*

Learn more at
entrust.com/HSM

ENTRUST
SECURING A WORLD IN MOTION