ENTRUST
SECURING A WORLD IN MOTION

TOP 5 GRÜNDE
FÜR DIE BEREITSTELLUNG EINES NSHIELD HSM IN IHRER AZURE-UMGEBUNG

1 SIE TRAGEN DIE VERANTWORTUNG FÜR DIE DATEN IHRER KUNDEN

Das Shared-Responsibility-Modell zeigt, dass unabhängig von der Bereitstellung des Cloud-Dienstes der Kunde stets die Verantwortung für die Daten trägt.

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Verantwortung des Kunden	Daten	Daten	Daten
	Anwendung	Anwendung	Anwendung
	Laufzeit	Laufzeit	Laufzeit
	Middleware	Middleware	Middleware
	Betriebssystem	Betriebssystem	Betriebssystem
Verantwortung des Anbieters	Virtualisierung	Virtualisierung	Virtualisierung
	Server	Server	Server
	Storage	Storage	Storage
	Netzwerk	Netzwerk	Netzwerk

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

2 DATENVERSTÖßE NEHMEN ZU

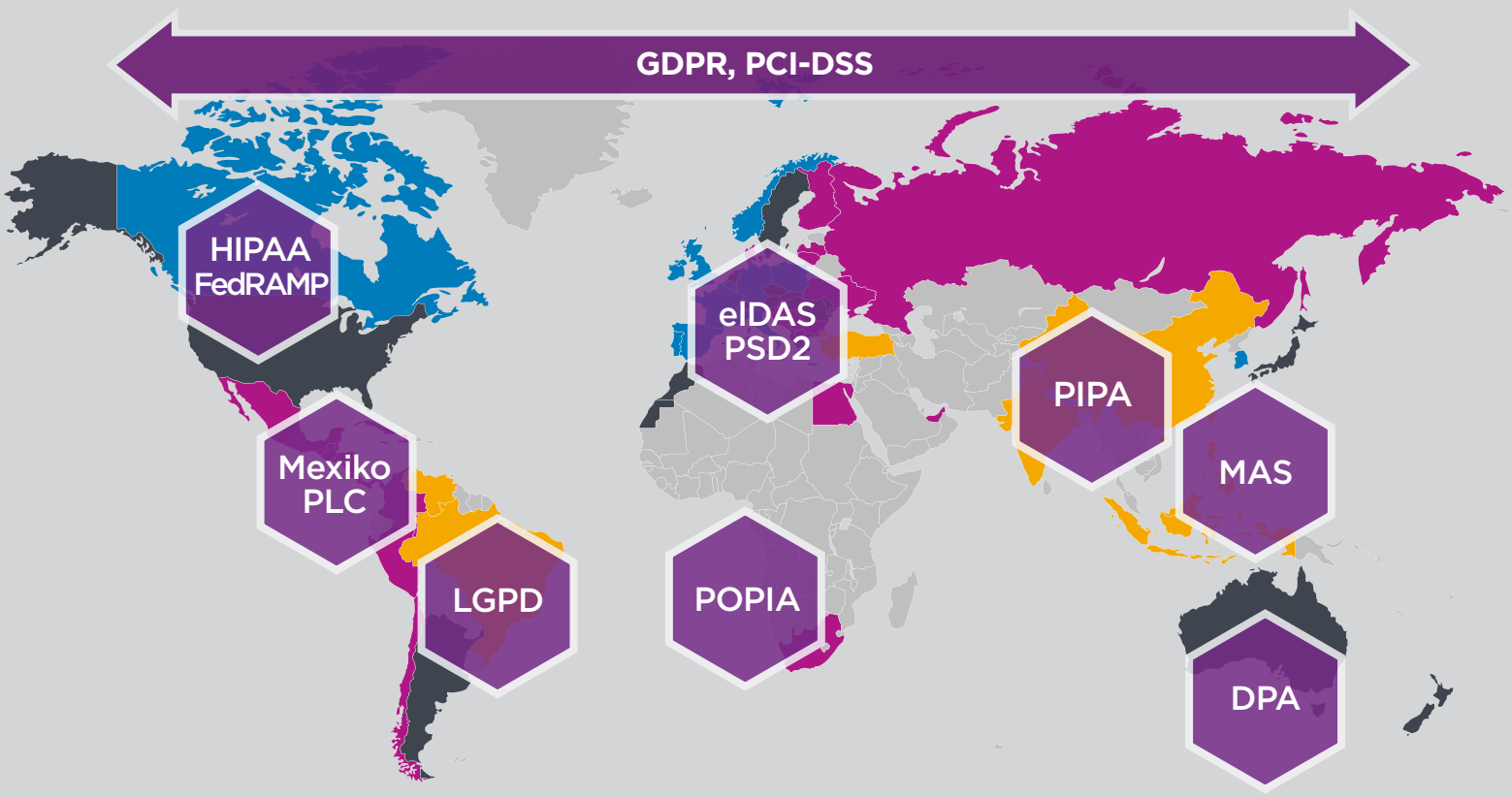
Stetig werden mehr Verbraucherdatensätze mit personenbezogenen Informationen offengelegt. 2018 stieg die Zahl von 197,6 Millionen auf 446,5 Millionen – ein Anstieg von 126 %. Die tatsächliche Gesamtzahl der offengelegten Datensätze ist wahrscheinlich höher, da nur bei der Hälfte der gemeldeten Verstöße die Anzahl angegeben wurde.

Im Jahr 2018 stieg die Zahl der offengelegten Verbraucherdaten sprunghaft um 126 %

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

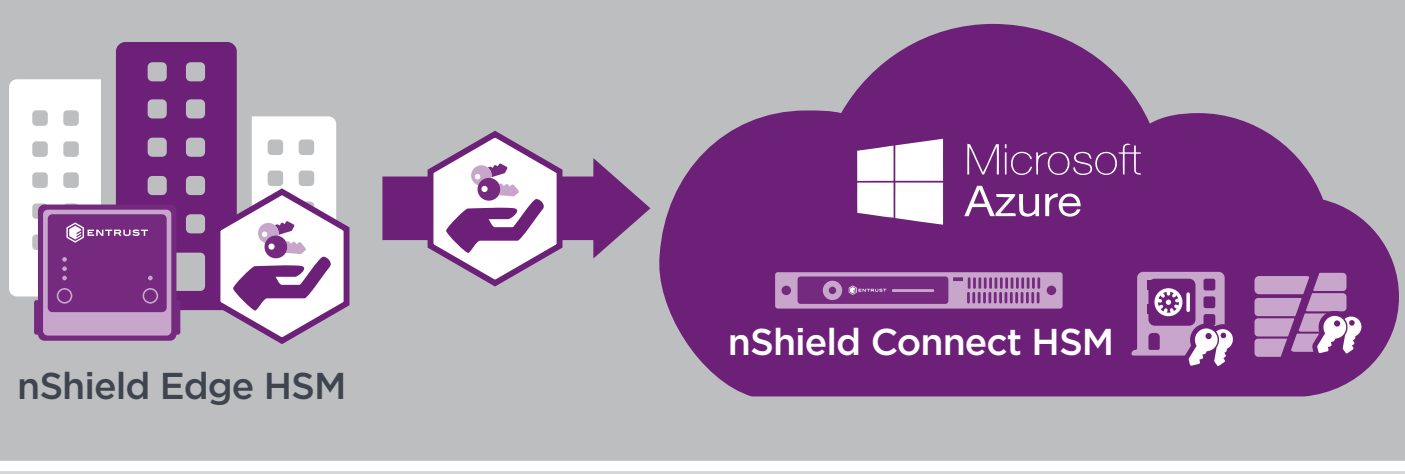
3 REGULATORISCHE VORGABEN MÜSSEN ERFÜLLT WERDEN

Weltweit werden neue Datenschutzbestimmungen eingeführt. Das bedeutet auch mehr Verantwortung, Rechenschaftspflicht und höhere Strafen für Unternehmen. nShield®-Hardware-Sicherheitsmodule (HSM) haben sich in diesem Zusammenhang bewährt.



4 SIE HABEN DIE KONTROLLE ÜBER IHRE SCHLÜSSEL

Mit Bring Your Own Key (BYOK) können Sie Daten in der Cloud mit kryptographischen Schlüsseln sicher kontrollieren und schützen. Sie erstellen Ihre eigenen Schlüssel On-Premises. Diese Schlüssel werden anschließend sicher auf HSM in der Cloud übertragen, wo Azure sie nutzt, um Anwendungen und Daten zu sichern, ohne sie dabei sehen oder missbrauchen zu können.



5 SIE STELLEN EINEN VERTRAUENSANKER FÜR IHRE CLOUD BEREIT

nShield HSM stellen eine gehärtete, manipulationssichere Umgebung für geschützte kryptographische Verarbeitung, Schlüsselerstellung und Schutz, Verschlüsselung, HSM-Schlüsselverwaltung und vieles mehr bereit, die Folgendes bietet:

- Eine zusätzliche Sicherheitsebene für eine sichere Anwendungsplattform
- Isolierung kryptographischer Operationen und Schlüssel
- Starke Benutzerauthentifizierung über Smartcards
- Durchführung von Doppelkontrollen und Aufgabentrennung
- Zertifizierte, hochleistungsfähige Schlüsselerstellung
- Leistungsstarke kryptographische Beschleunigung und Auslagerung
- FIPS 140-2-Zertifizierung

Mehr dazu in unserem Video *Bring Your Own Key with Entrust and Microsoft Azure*

Weitere Informationen auf
entrust.com/HSM

ENTRUST
SECURING A WORLD IN MOTION