ENTRUST
SECURING A WORLD IN MOTION

5 PRINCIPAIS MOTIVOS AZURE

PARA ADICIONAR UM HSM NSHIELD AO SEUS SISTEMA

1 VOCÊ É RESPONSÁVEL PELOS DADOS DE SEUS CLIENTES

O modelo de responsabilidade compartilhada mostra que, não importa como o serviço em nuvem é fornecido, os dados são sempre de responsabilidade do cliente.

	Infraestrutura como Serviço (IaaS)	Plataforma como Serviço (PaaS)	Software como Serviço (SaaS)
Responsabilidade do cliente	Dados	Dados	Dados
	Aplicação	Aplicação	Aplicação
	Tempo de execução	Tempo de execução	Tempo de execução
	Middleware	Middleware	Middleware
	S/O	S/O	S/O
Responsabilidade do provedor	Virtualização	Virtualização	Virtualização
	Servidores	Servidores	Servidores
	Armazenamento	Armazenamento	Armazenamento
	Networking	Networking	Networking

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

2 AS VIOLAÇÕES DE DADOS ESTÃO AUMENTANDO

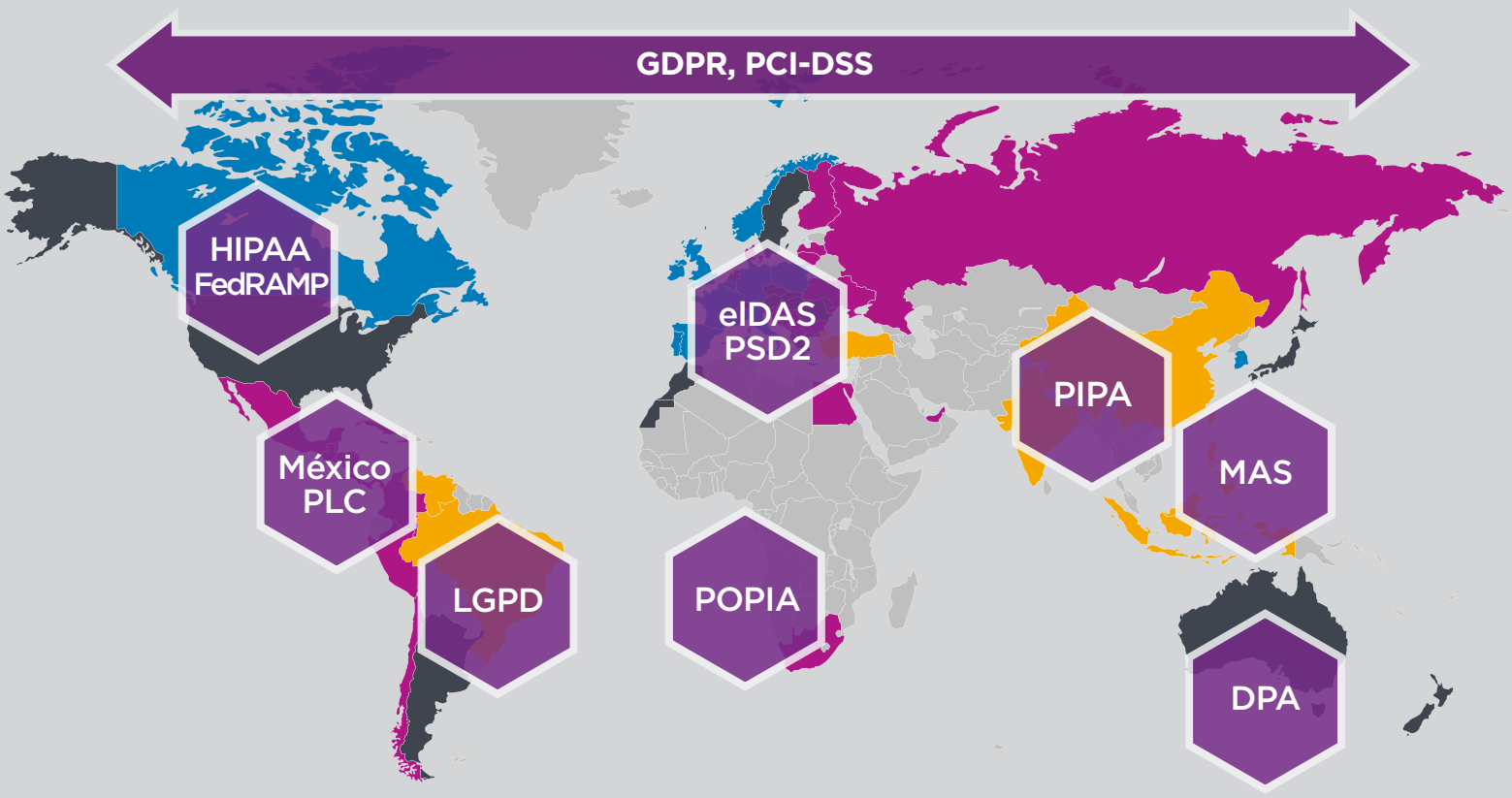
O número relatado de registros expostos de clientes contendo informações de identificação pessoal (PII) aumentaram significativamente de 197,6 milhões para 446,5 milhões em 2018 - um salto de 126%. O número total real de dados expostos é provavelmente maior, pois apenas a metade das violações relatadas revela o número.

Os dados de consumo expostos dispararam em 126% em 2018

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

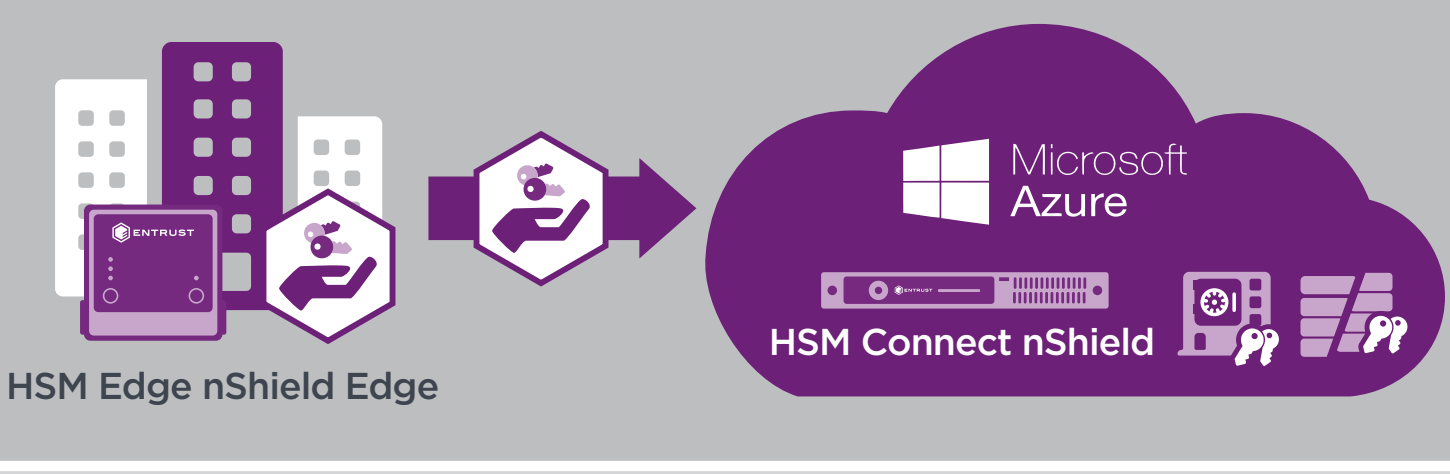
3 É PRECISO SEGUIR AS LEIS DE CONFORMIDADE

No mundo inteiro estão sendo aplicadas novas leis de privacidade, o que significa que as empresas estão enfrentando uma responsabilidade maior e multas maiores. Os módulos de segurança de hardware (HSM) nShield® garantem que você utilize as melhores práticas.



4 O CONTROLE DAS CHAVE É SEU

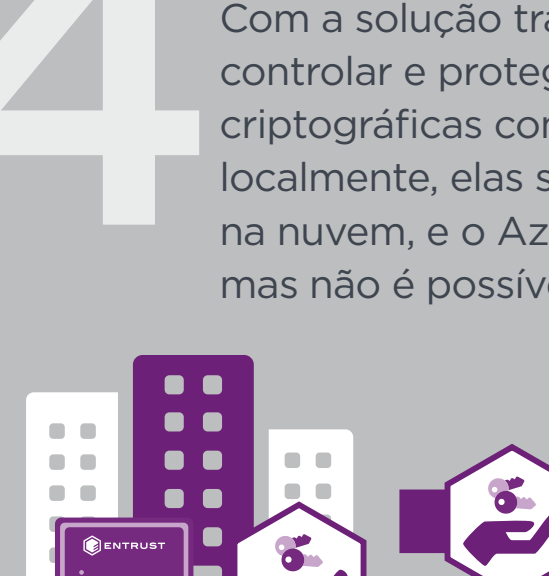
Com a solução traga sua própria chave (BYOK) você pode controlar e proteger os dados na nuvem usando chaves criptográficas com segurança. Você gera suas próprias chaves localmente, elas são transferidas com segurança para os HSM na nuvem, e o Azure as usa para proteger aplicações e dados, mas não é possível vê-los ou fazer mau uso dos mesmos.



HSM Edge nShield Edge

5 VOCÊ ADICIONA UM PROTOCOLO DE SEGURANÇA PARA SUA NUVEM

Os HSM nShield fornecem um ambiente resistente e inviolável para processamento criptográfico seguro, geração e proteção de chaves, criptografia, gerenciamento de chave por HSM e muito mais fornecendo:



- Uma camada extra de segurança para criar uma plataforma segura para aplicações
- Divisão de operações criptográficas e chaves
- Autenticação forte do usuário através de cartões inteligentes
- Controles duplos fortalecidos e separação de funções
- Geração de chaves certificadas e de alto desempenho
- Aceleração poderosa de criptografia e de descarga
- Certificação FIPS 140-2

Clique para assistir nosso vídeo *Bring Your Own Key com Entrust e Microsoft Azure*

Saiba mais em
entrust.com/HSM

ENTRUST
SECURING A WORLD IN MOTION