ENTRUST
SECURING A WORLD IN MOTION

5 TOP MOTIVI
PER AGGIUNGERE UN HSM NSHIELD A UN DEPLOYMENT AZURE

1 LA RESPONSABILITÀ DEI DATI SPETTA AL CLIENTE

Il modello di responsabilità condivisa mostra che è sempre il cliente a essere responsabile dei dati, indipendentemente dal tipo di servizio cloud.

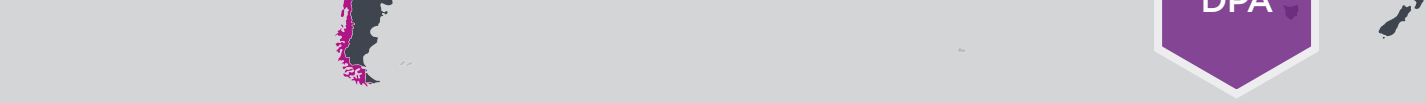
	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Responsabilità del cliente	Dati	Dati	Dati
	Applicazione	Applicazione	Applicazione
	Runtime	Runtime	Runtime
	Middleware	Middleware	Middleware
	OS	OS	OS
Responsabilità del provider	Virtualizzazione	Virtualizzazione	Virtualizzazione
	Server	Server	Server
	Archiviazione	Archiviazione	Archiviazione
	Networking	Networking	Networking

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

2 LE VIOLAZIONI DEI DATI SONO IN AUMENTO

Nel 2018, il numero di dati esposti contenenti informazioni sull'identità dei consumatori è passato da 197,6 milioni a 446,5 milioni, un aumento significativo pari al 126%. Il dato effettivo è probabilmente più elevato, poiché la cifra esatta viene rivelata soltanto nella metà dei casi di violazione riportati.

L'esposizione dei dati dei consumatori è aumentata del 126% nel 2018



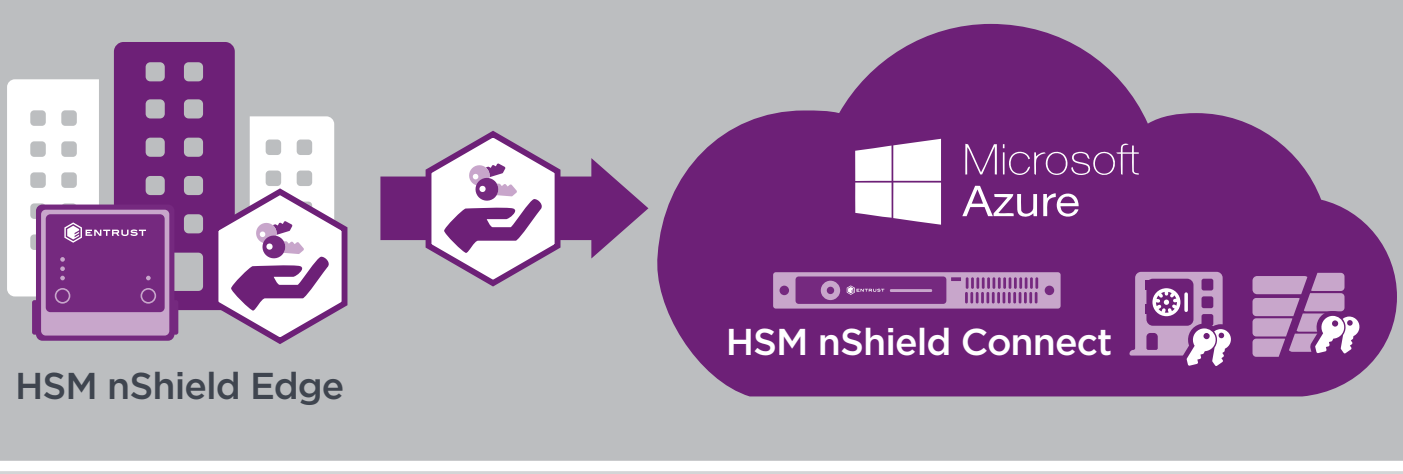
Fonte: Identity Theft Resource Center www.idtheftcenter.org/2018-data-breaches

3 CONSENTE ALLE IMPRESE DI RISPETTARE GLI OBBLIGHI DI CONFORMITÀ NORMATIVA

In seguito all'introduzione di nuove normative sulla privacy in tutto il mondo, le aziende devono fare i conti con maggiori obblighi e responsabilità, rischiando sanzioni più severe. Gli hardware security module (HSM) nShield® garantiscono la conformità alle best practice.

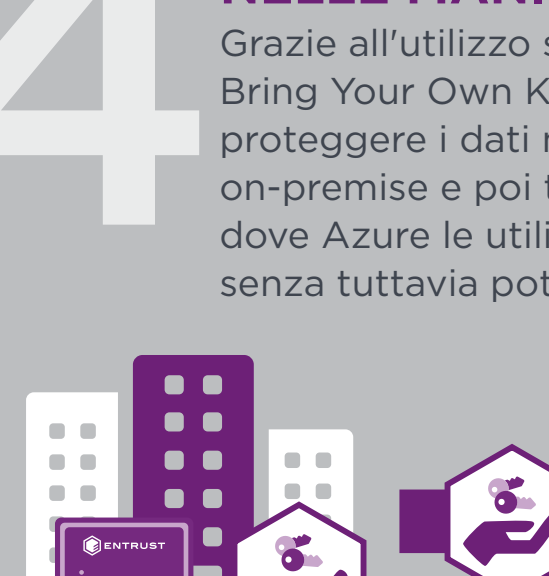
4 LASCIA IL CONTROLLO DELLE CHIAVI NELLE MANI DELLE AZIENDE

Grazie all'utilizzo sicuro delle chiavi crittografiche, i modelli Bring Your Own Key (BYOK) consentono di controllare e proteggere i dati nel cloud. Le chiavi vengono generate on-premise e poi trasferite in tutta sicurezza agli HSM nel cloud, dove Azure le utilizza per proteggere le applicazioni e i dati, senza tuttavia poterle vedere o utilizzare in maniera impropria.



5 AGGIUNGE UNA ROOT OF TRUST AL CLOUD

Gli HSM nShield forniscono un ambiente temprato a prova di manomissione per eseguire attività sicure di elaborazione crittografica, generazione, protezione e gestione delle chiavi, crittografia e molto altro, offrendo:



- Un livello di protezione aggiuntivo per la creazione di una piattaforma applicativa sicura
- Isolamento delle chiavi e delle attività crittografiche
- Autenticazione a più fattori con smart card
- Doppi controlli e separazione delle responsabilità
- Generazione delle chiavi certificata e ad alte prestazioni
- Accelerazione e offload crittografici efficaci
- Certificazione secondo lo standard FIPS 140-2

Fai clic qui per guardare il nostro video sulla *soluzione Bring Your Own Key di Entrust e Microsoft Azure*

Scopri di più su
entrust.com/HSM

ENTRUST
SECURING A WORLD IN MOTION

Entrust è un marchio, un marchio registrato e/o un marchio di servizio di Entrust Corporation negli Stati Uniti e/o in altri Paesi. ©2020 Entrust Corporation. Tutti i diritti riservati.