EQUINIX

Do You Know Where Your Customers' Data Is?

A Retailer's Guide to Data Governance

INTERACTIVE

Table of Contents

EQUINIX

Evolving IT Architectures Introduce Security Challenges

Retailers modernizing their architectures struggle to manage data security

Retailers can’t afford to wait.

Retailers are eager to adopt modern hybrid cloud architectures to deliver the experiences customers have come to expect. However, they must ensure they protect massive amounts of sensitive personal data as it moves to cloud-based infrastructures.

Data breaches continue to pose serious threats.

According to IT Governance, in the first five months of 2019, over 7.2 billion Personally Identifiable Information (PII) records were breached.[1] Security regulations and the need to avoid damaging public relations fallout mean retailers must prioritize security above all else.

Retailers must secure and protect PII data.

To comply with the California Consumer Protection Act (CCPA), the General Data Protection Regulation (GDPR) and other regulations, retailers must protect customer data at any state.

The General Data Protection Regulation (GDPR) identifies encryption as an effective method by which to achieve a risk-based approach to data security (Article 32, GDPR).

1 Dan Rafter, “Data breach: Could your email account be compromised?“ NortonLifeLock, 2020.

EQUINIX

CHALLENGE

Data: Here, There and Everywhere

Protecting PII no matter its state or location

Retail rewards and loyalty programs work.

According to the Harvard Business Review, loyalty leaders grow revenues roughly 2.5x as fast as other companies in their industries.[1]

However, they have a cost.

The third-party vendors that provide these services collect, process, transmit and store vast amounts of PII at each point of purchase. A large retailer collects data on roughly one million transactions per hour.

PII must be protected.

The California Consumer Protection Act (CCPA) in the U.S., General Data Protection Regulation (GDPR) in Europe, and other data protection regulations mandate that PII data must be secured and protected whether in use, in transit or at rest.

The challenge is protecting data outside of your organization.

The vendors that run the rewards programs are also collecting and storing your customers' data. To comply with security regulations, you must ensure your cloud vendors are also following appropriate security protocols.

1. Rob Markey, "Are You Undervaluing Your Customers?" Harvard Business Review, Jan.–Feb. 2020.

EQUINIX

CHALLENGE

To Protect PII, Encrypt It

A best-practice approach to securing PII against loss or compromise

Protect sensitive data with encryption.

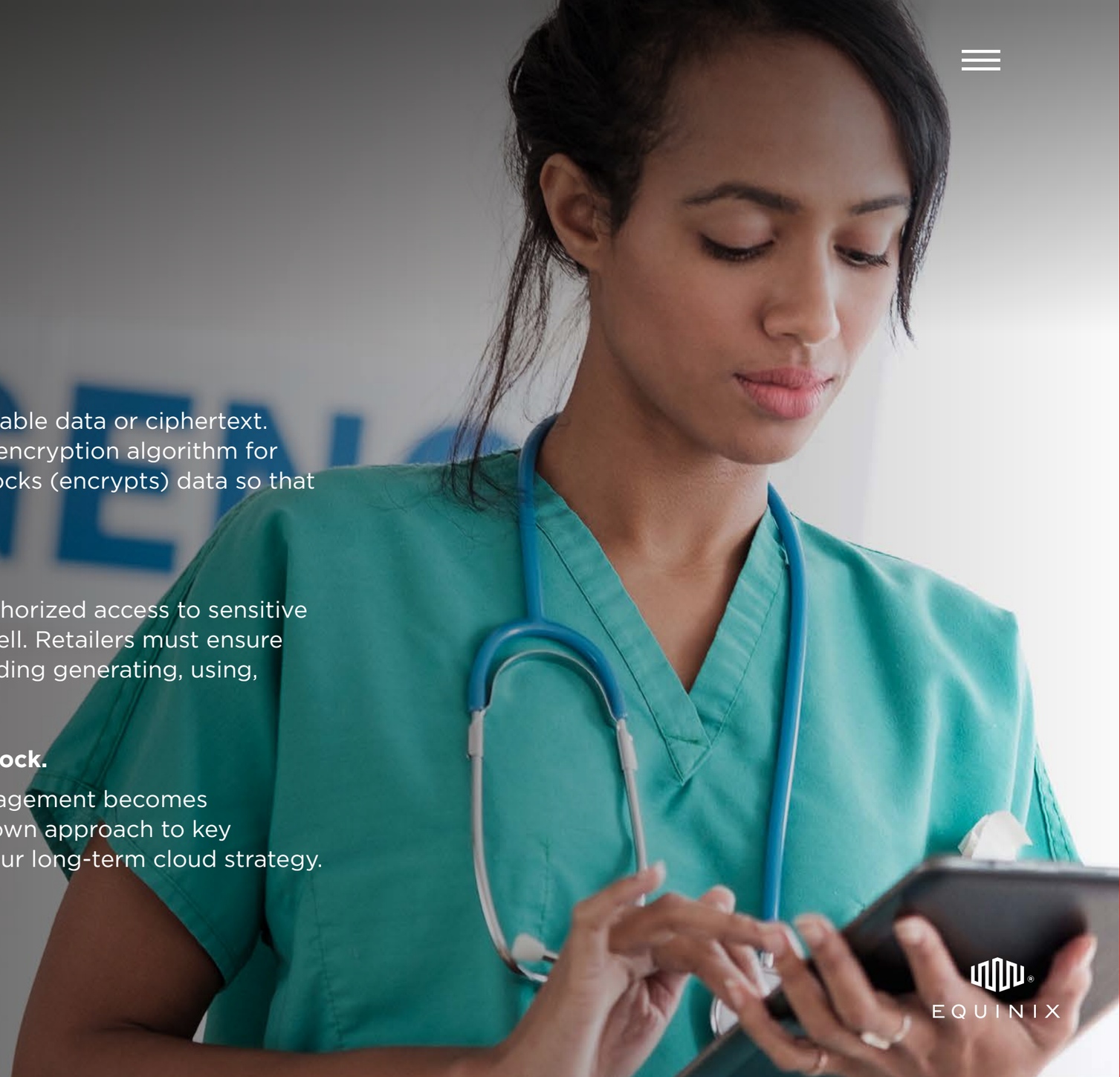
Encryption encodes plaintext or readable data into unreadable data or ciphertext. Encryption keys are random strings of bits used within an encryption algorithm for scrambling and unscrambling data. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

Encryption keys must be managed and protected.

Encryption key management is crucial to preventing unauthorized access to sensitive information. If keys are compromised, PII data can be as well. Retailers must ensure they manage the full life cycle of cryptographic keys, including generating, using, storing, archiving and deleting keys.

Effective key management is encryption's biggest roadblock.

As enterprises transition to the cloud, encryption key management becomes more challenging, as each cloud environment requires its own approach to key management. Your key management strategy should fit your long-term cloud strategy.



EQUINIX

CHALLENGE

Encryption Key Management Approaches

Traditional HSM vs. cloud-based KMS? Both are problematic when it comes to multicloud environments

Multiple cloud provider key management tools increase complexity.

Legacy Hardware Security Modules (HSMs) offer robust cloud-neutral encryption and key management, but they are also complex and require significant ongoing management to implement and support. Additionally, as retailers move to the cloud, they no longer control HSM selection and provisioning. The cloud provider assumes responsibility for its part of HSM, and the business is required to use key management tools for specific vendors. If you work with a single cloud provider, this can work; however, managing multiple cloud provider key management tool results gets complicated.

A strictly cloud-based approach is also problematic.

Cloud-based Key Management Services (KMSs) scale easily as data and processing demands grow. They provide encryption keys to encrypt data stored in the cloud provider's data center and offer reporting and auditing features for regulatory compliance. Again, this strategy works well with a single cloud provider, but is difficult to manage across multiple clouds. More concerning, however, is that a KMS approach diminishes data security by storing and managing encryption keys and data in the same entity—the cloud provider. Best practices recommend encryption keys and data be managed by separate entities so that a breach of encrypted data produces only ciphertext and a breach of keys is worthless without access to the data.

SOLUTION

Cloud-Neutral HSM Delivered as a Service

What if you could have KMS-like simplicity with the security of HSM?

HSM as a Service offers robust, cloud-neutral security capable of managing the entire encryption key life cycle for private, public or hybrid cloud environments, including those offered by leading providers such as AWS, IBM, Azure, Oracle and Google.

A cloud service is always available and scales to match your needs.

HSM as a Service features enterprise-level access controls and audit logging for compliance requirements. Most importantly, it offers a single, centralized way to simplify provisioning and control of encryption keys in any number of multicloud environments.

As a best practice, a strong key management solution should:

- Ensure compliance with data privacy regulations, including the CCPA.
- Work across any SaaS provider in the cloud or on-premises.
- Scale across multiple metros and/or countries.
- Include HSM-grade security, without the HSM capital expense.
- Keep keys and data separate.

SOLUTION

Equinix SmartKey®: HSM Re-Imagined

A cloud-based HSM provides simple, secure and scalable key management

Data privacy + granular control

Equinix SmartKey powered by Fortanix is based on Intel Software Guard Extensions (SGX), a technology that protects application code and data from disclosure or modification. This core technology removes the need for legacy HSMs and provides application integration and development tools for today's cloud environments.

Best in class

The recipient of the InfoSec 2019 Hot Company Cloud Security Award and Publishers Choice SaaS/Cloud Security Award, SmartKey is a globally distributed, cloud-based HSM that provides encryption, key management and tokenization as a service. SmartKey simplifies key management without sacrificing security.

SOLUTION

Benefits of Equinix SmartKey®

Reduce your risk of regulatory fines

Ensure your customer data is encrypted to avoid mandatory notifications to data protection regulators of potential data breaches.

Get started with zero upfront cost

A low subscription fee based on usage means you don't have to pay for engineers to implement or run the system on an ongoing basis.

Access your keys whenever, wherever

Keys are stored at the digital edge (in the cloud or on-premises), in close proximity to your applications and data for the lowest possible latency.

Achieve instant disaster recovery

Keys, certificates and secrets are instantly replicated among all HSM nodes within each of the metros across a service region, so they are always available and accessible, ensuring maximum uptime.

Migrate data seamlessly

SmartKey allows for rapid and easy application integration, regardless of whether data resides in the cloud or on-premises.

Achieve complete key secrecy

Only SmartKey customers have access to their keys, removing the risk of key compromise from service providers and governments both foreign and domestic, where both the key and the data are stored in shared infrastructure.

Eliminate the risk of data breaches

Through unified key management, encryption and tokenization, SmartKey helps to eliminate the risk of PII data breaches, as data is encrypted, both in transit and at rest.

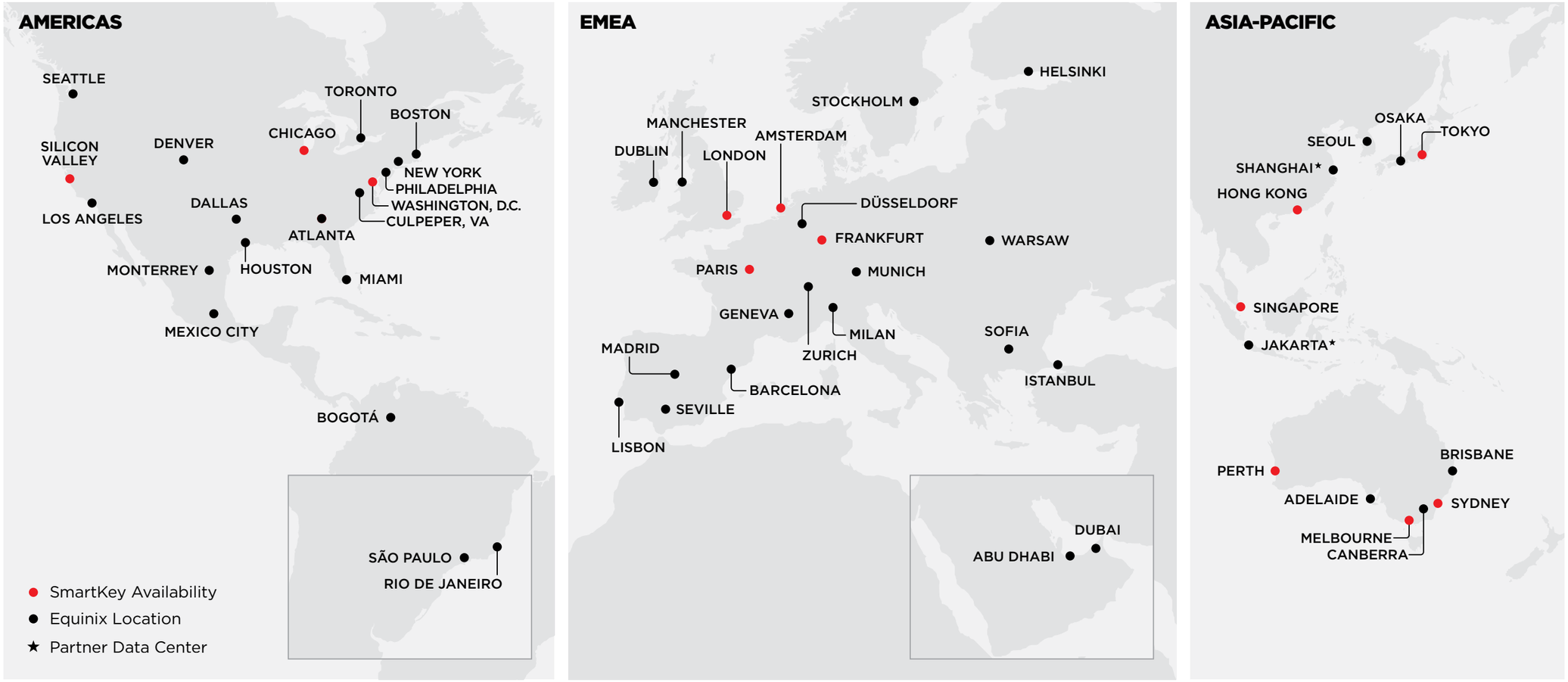
Integrate easily with your systems

Compatible with a large number of interfaces (including RESTful APIs, PKCS#11, CNG, JCE and KMIP), allowing easy integration with existing and future systems.

EQUINIX

SOLUTION

Equinix SmartKey® Availability Zones



USE CASE

Multicloud Encryption Key Management

Challenge

A large food manufacturer with data spanning multiple clouds found storing and managing encryption keys in a hybrid/multicloud environment expensive, time-consuming and complex. The company's legacy KMS solution couldn't support other cloud environments, and multiple services were required to manage security objects like keys, certificates and secrets.

USE CASE

Multicloud Encryption Key Management

Solution

Equinix SmartKey provided a single repository and interface to manage all the company's keys, certificates and secrets across multiple clouds. This simplified provisioning, storage and management of keys across public, private and hybrid clouds and external HSM systems, and improved the company's security posture by separating keys from associated data.

Benefits

- Cloud-native, cloud-neutral.
- Compatible with all major CSPs.
- Eliminates risk of key compromise in shared infrastructure.
- Offers non-disruptive method to migrate keys from HSMs.
- Create/revoke all keys through SmartKey interface.

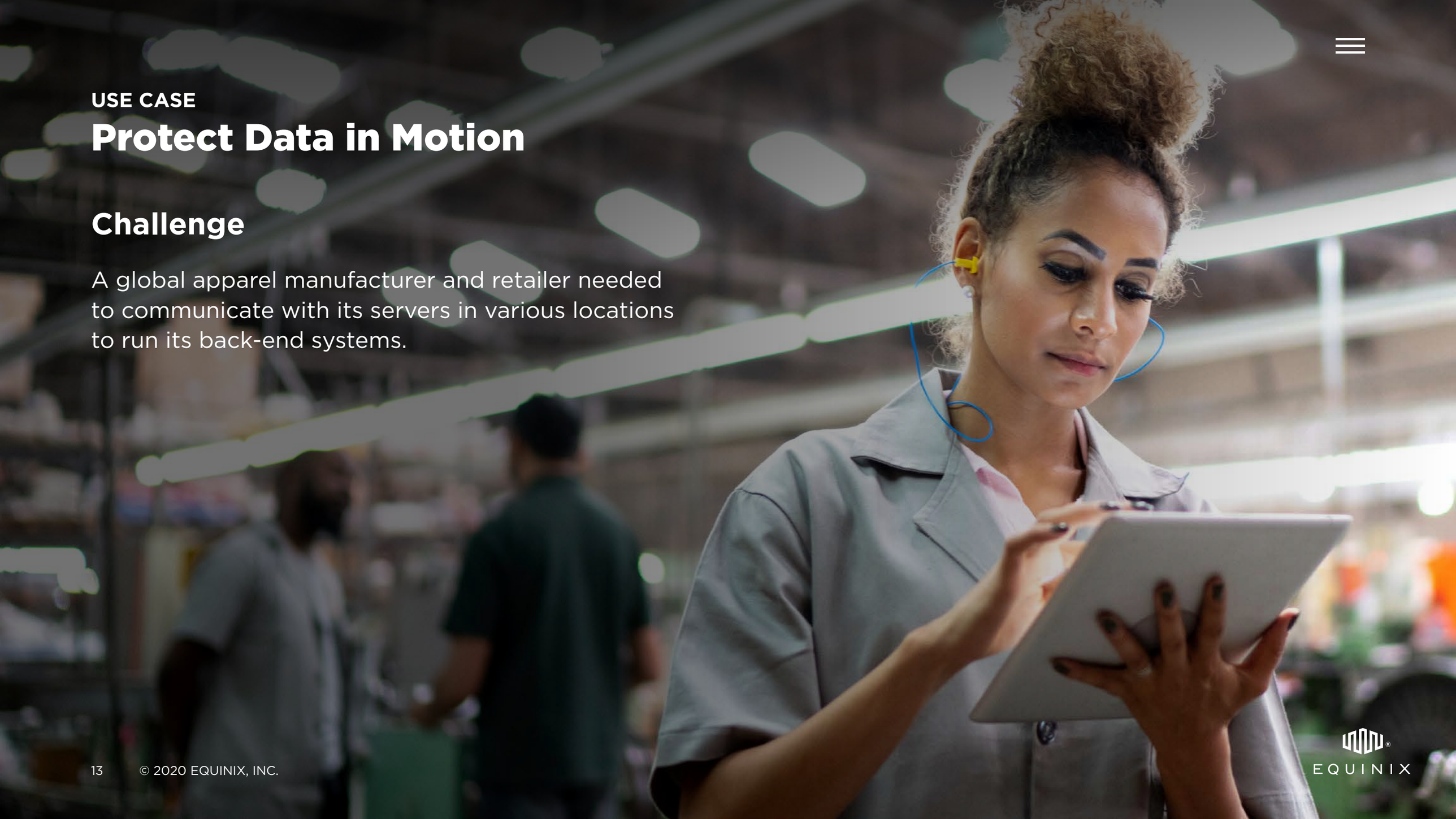
EQUINIX

USE CASE

Protect Data in Motion

Challenge

A global apparel manufacturer and retailer needed to communicate with its servers in various locations to run its back-end systems.



EQUINIX

USE CASE

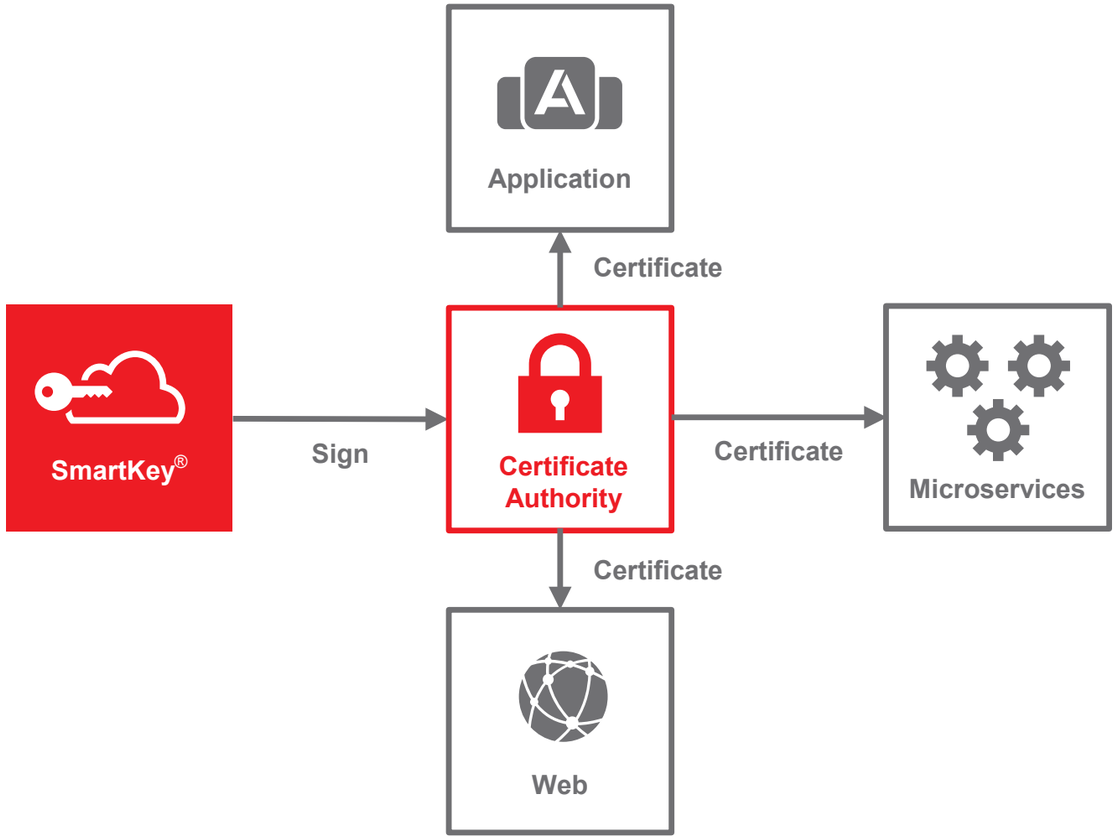
Protect Data in Motion

Solution

The retailer used Public Key Infrastructure (PKI) to enable secure communications by identifying and authenticating the servers so they could be authorized to talk to each other. SmartKey generates and manages the public and private keys that are used to sign digital certificates used in PKI.

Benefits

- Entire solution, including KMS, runs inside HSM secured with Intel SGX.
- Distributed active/active design ensures uptime and provides seamless scalability in capacity or performance with no downtime.
- Encrypted connections between distributed servers with centralized tamper-proof logging.
- Analytics on the logs provide insights and help detect threats.



USE CASE

Keep Customer PII Data Safe

Challenge

A global restaurant chain with over 48,000 locations across 140 countries uses a third-party vendor to manage gift cards, digital marketing and customer loyalty programs that leverage customer PII. To remain compliant and protect customers, the retailer needed to encrypt data in many locations and systems, including restaurants, HQ, third-party vendors and cloud. The retailer used multiple point security tools to address requirements, which was expensive, inefficient and hard to manage.

EQUINIX

USE CASE

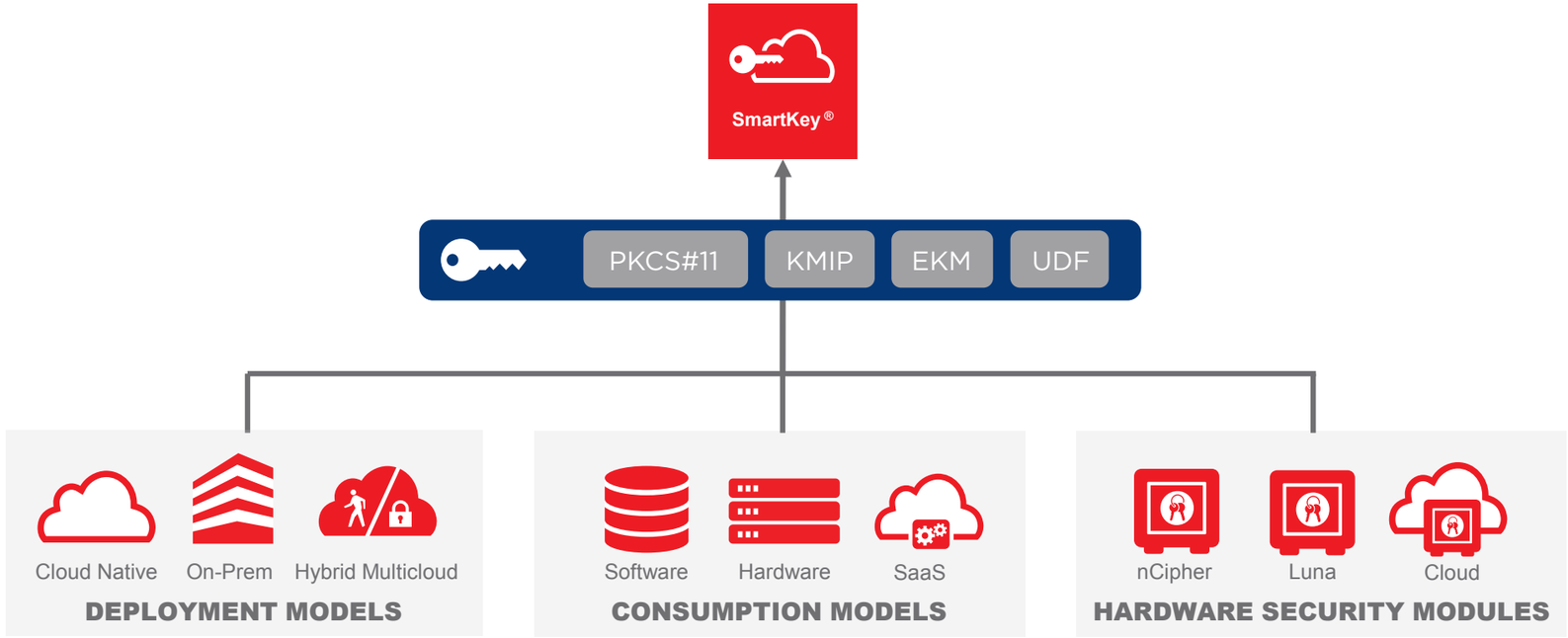
Keep Customer PII Data Safe

Solution

As a distributed HSM as a Service offering, Equinix SmartKey provided the retailer a secure location to store all objects required to secure sensitive data located in the cloud and on-premises.

Benefits

- Met regulatory compliance for PII.
- Consolidated multiple security technologies by using a single service across multiple applications and use cases.
- Global solution with no upfront CAPEX requirements.



Equinix SmartKey

Get the convenience of cloud without the risk

Unified key management, encryption and tokenization across multiple clouds and vendors is here.

Stay compliant and leverage powerful encryption capabilities without slowing down your data. Available on Platform Equinix®, SmartKey stores keys in a cloud-neutral environment at the digital edge, close to your cloud service provider and carriers. Simplify the provision, storage and control of encryption keys, and protect your data on any cloud in the world.

Start your secure journey to PII compliance today.

Schedule a SmartKey demo now.

Equinix.com/Contact-Us/Sales

EQUINIX