PCI Security Standards Council

Elevating Security

A Case Study in Moving Payment Cryptography to the Cloud

Adam Cason, Vice President, Global and Strategic Alliances, Futurex
Steve Wilson, Senior Consultant, Encryption Services, Global Payments

globalpayments

FUTUREX

Payment Security and the Cloud in 2023

- 86% of companies have reported increasing cloud initiatives between 2020 and 2023*
- Priorities have shifted from learning and planning to **implementing**
- Factors promoting cloud adoption for payment security workloads:
  - Cloud-centric considerations in PCI Security Standards
  - Increasing comfort with legislative and regulatory frameworks
  - Multitenancy technology adoption in the HSM world
  - Cryptographic modernization initiatives
  - Competitive positioning and speed of innovation

**https://www.accenture.com/us-en/insights/cloud/cloud-outcomes-perspective*

PCI Security Standards Council®

Global Payments' Move to the Cloud

The Business Case

The Challenge

Technology

Business

Architecture

PCI Security Standards Council

Spotlight on Hardware Security Modules

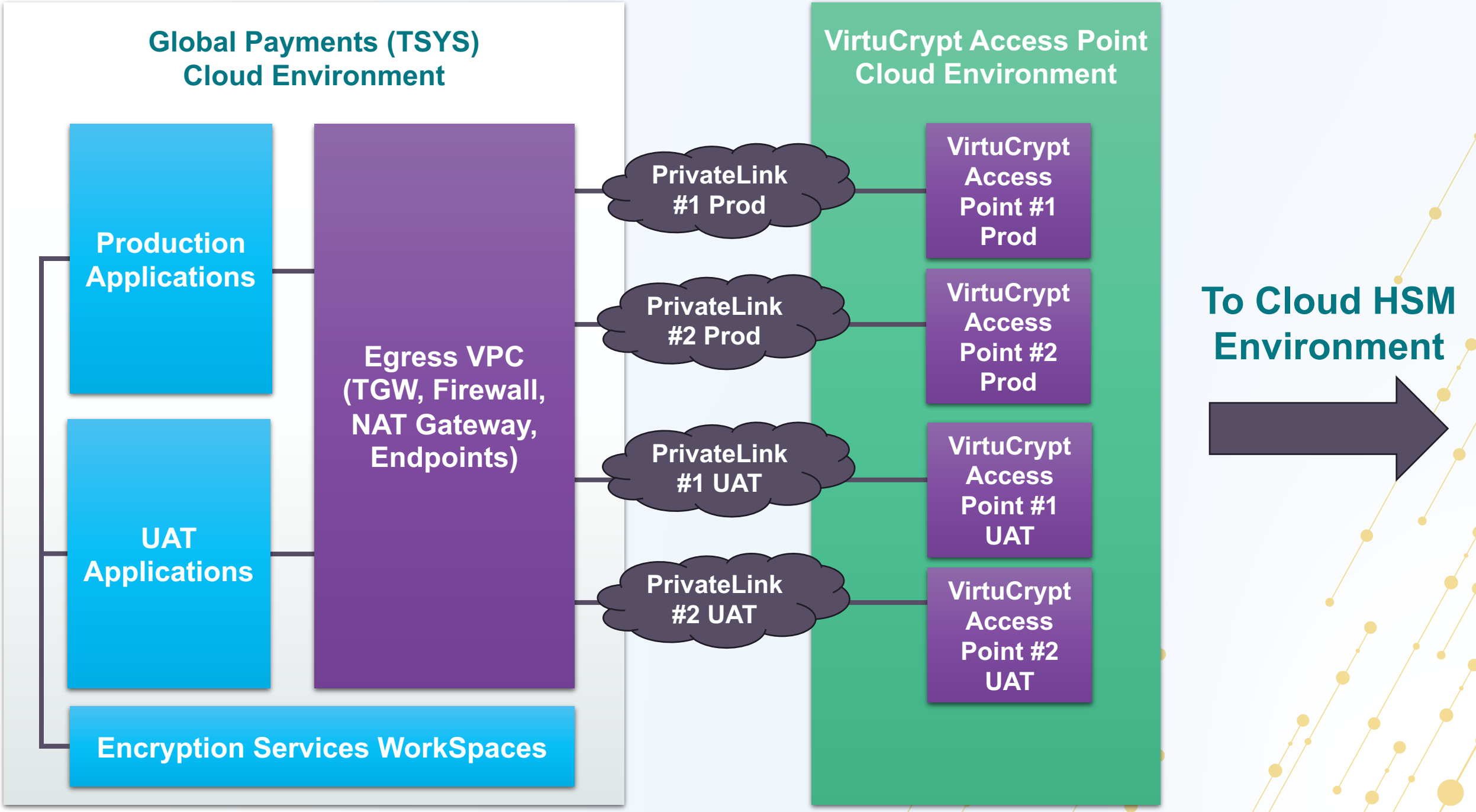
HSMs are purpose-built security devices that protect sensitive data in transit, in use, and at rest through the use of physical security measures, logical security controls, and strong encryption. They are validated or reviewed under standards such as PCI PTS HSM and FIPS 140-2/3 Level 3.

- #1 On-Premises
- #2 Private Cloud
- #3 Multi-Tenant Cloud or HSM-as-a-Service
- #4 Hybrid

PCI Security Standards Council

The Solution

- Payment applications moved into public cloud
- HSMs moved into Futurex HSM-as-a-Service environment
  - Development
  - User Acceptance Testing (UAT)
  - Production
- On-demand provisioning of HSM resources
- Geographic (data residency) and latency considerations
- Key management continued to be managed through TSYS Encryption Services team
- Elastic scalability for throughput growth over time


Global Payments (TSYS)
Cloud Environment
Production Applications
UAT Applications
Encryption Services WorkSpaces
Egress VPC (TGW, Firewall, NAT Gateway, Endpoints)
PrivateLink #1 Prod
PrivateLink #2 Prod
PrivateLink #1 UAT
PrivateLink #2 UAT
VirtuCrypt Access Point Cloud Environment
VirtuCrypt Access Point #1 Prod
VirtuCrypt Access Point #2 Prod
VirtuCrypt Access Point #1 UAT
VirtuCrypt Access Point #2 UAT
To Cloud HSM Environment

To Cloud Environment (Payment Applications)

VirtuCrypt Cloud HSM Environment

Each environment contains TLS CryptoTunnels, CryptoBalancers, and dedicated physical HSMs (PCI PTS HSM and FIPS 140-2 Level 3). Each physical HSM runs multiple virtual HSMs.

Production Data Center #1

Production Data Center #2

UAT Data Center #1

UAT Data Center #2

TSYS Encryption Services

Key Management
PCI PTS HSM and FIPS 140-2 Level 3

Cloud HSM Management
Web Portal

Key Management

- How do general-purpose HSMs approach key management?
- What makes key management for payments so special?
- Key management methods for HSM-as-a-Service
  - Bring Your Own Key (BYOK)
  - Vendor-provided key administration services
- What should service providers share with customers?
  - Attestations of Compliance (AoC)
  - Responsibility matrices
  - Communication and coordination with assessment firms

Key Takeaways and Cloud Considerations

- Reallocate internal resources to more valuable functions
- Retain flexibility for emerging trends and initiatives
- Rapidly expand into strategic markets
- Enable business units to focus on core competencies
- Unblock migration of workloads to public cloud providers
- In addition to PCI SSC requirements, also achieve compliance with regional data protection mandates

PCI Security Standards Council

Thank You

Questions? Contact Us

acason@futurex.com

SteveWilson@tsys.com

Europe Community Meeting 2023

PCI Security Standards Council