VirtuCrypt – UAT and Development

Cloud payment HSM

Why VirtuCrypt – UAT and Development?

- Streamlined integration and billing via multiple methods, including signup through the Amazon Web Services (AWS) Marketplace.
- Full redundancy and high availability across worldwide data centers, with service-level agreement (SLA)-backed uptime of up to 99.999%.
- Secure communication directly from an AWS virtual private cloud (VPC) to VirtuCrypt, with no direct internet routing.
- Accessible from multiple AWS regions as well as from applications managed on-premises or in other clouds.
- On-demand provisioning and clustering of cloud payment HSMs.

Product overview

VirtuCrypt uses Futurex's Federal Information Processing Standards (FIPS) 140-2 Level 3 and payment card industry hardware security module (PCI HSM) validated technology. VirtuCrypt cloud payment HSMs can perform cryptographic operations required for user assistance testing (UAT), proof of concept, and payment applications development. This includes all functions available on the Futurex payment HSMs used for various payment application use cases. These include point-to-point encryption (P2PE) functions (cardholder data decryption, cardholder data translation), PIN and offset generation, and online and mobile PIN management. Also included are Europay, Mastercard, and Visa (EMV) key generation and derivation, mobile payment token issuing, PIN translation and verification, and EMV card validation. Additional validation points are card verification value (CVV) validation, point-to-point encryption (P2PE), and all related key management functions.

Product features

Hybrid deployment

Hybrid deployment with on-premises payment application and Futurex HSMs as well as VirtuCrypt cloud payment HSMs.

Full industry compliance

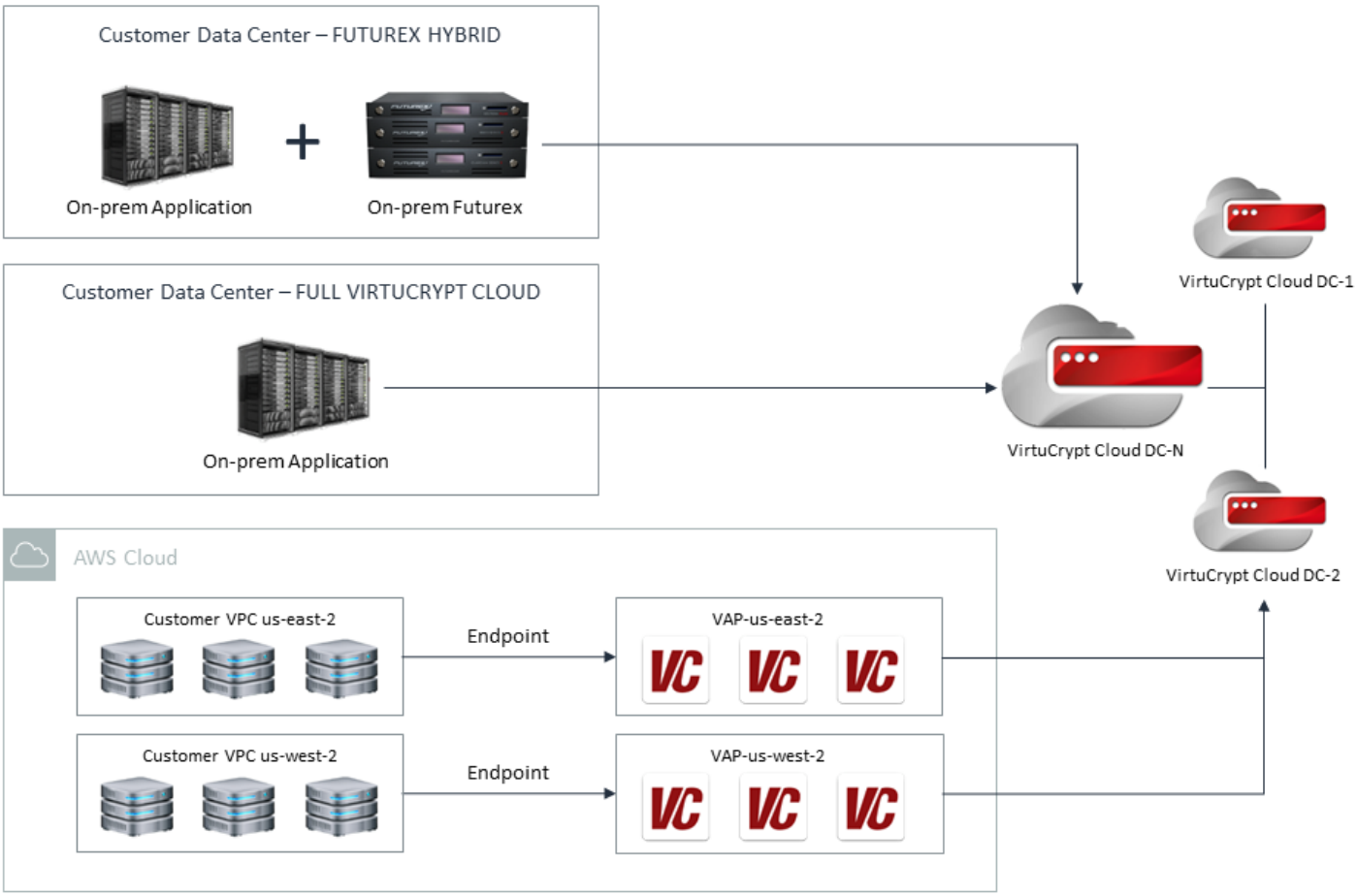
VirtuCrypt's cloud payment HSM service exclusively uses Futurex's FIPS 140-2 Level 3 and PCI HSM validated HSMs. The service ecosystem has received payment card industry data security standard (PCI DSS), payment card personal identification numbers (PCI PIN), P2PE, and VISA PIN/technical report (TR-39) certifications.

Fully-hosted cloud option

VirtuCrypt offers payment applications hosted in multiple AWS regions, connecting through VirtuCrypt Access Points (VAP) to VirtuCrypt cloud payment HSMs. Enables full redundancy, high availability, and expansion over time.

How it works

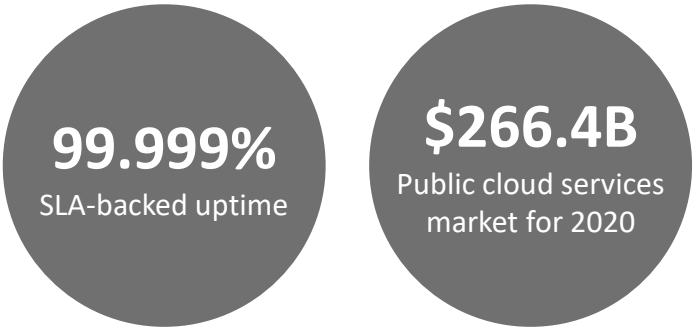
Organizations can connect to VirtuCrypt's cloud payment HSM service in a number of different ways. The most important initial decision for organizations is to determine where they wish to host their payment applications and HSM infrastructure. VirtuCrypt supports a range of different methods outlined in the diagram below. It also offers solutions architects available to advise organizations on the architecture that best fits their needs and goals.



Differentiators

- Payment card industry hardware service module (PCI HSM) and Federal Information Processing Standards (FIPS) 140-2 Level 3 validated cloud payment HSM.
- Services audited under payment card personal identification numbers (PCI-PIN), payment card industry point-to-point encryption (P2PE), and PCI data security standard (PCI-DSS) standards.
- Streamlines and expedites the proof of concept and development process.

Data Points



Additional Resources

- Cloud Payment HMS solutions page
- Case studies
- Schedule a demo

Solution available in AWS Marketplace