securosys

Solution Brief

# Cloudflare Keyless SSL with Securosys Primus HSM

## Enterprise-Grade TLS Protection with Complete Key Custody

## The Challenge: Balancing Cloud Performance with Key Security

Enterprises rely on global web security and content delivery to scale and serve customers worldwide. Traditional CDN deployments meet this need but typically require uploading SSL/TLS private keys to the provider's infrastructure. For regulated organizations such as financial institutions, healthcare providers, and government agencies, this creates a significant challenge. Regulatory requirements and internal policies demand full control over cryptographic keys, making it unacceptable to share private keys with third parties.

As cloud-based security adoption grows, maintaining full key custody becomes more complex. Preserving exclusive control over cryptographic keys therefore requires a different approach. By combining Cloudflare's global Edge network with Securosys' certified HSM infrastructure, organizations no longer need to choose between cloud performance and key custody. Together, Cloudflare and Securosys deliver enterprise-grade protection at global scale while ensuring complete control over cryptographic keys.

## Solution Overview

Cloudflare Keyless SSL with Securosys Primus HSM creates a unique solution which enables TLS termination at Cloudflare's Edge while cryptographic signing remains exclusively within the customer's certified HSM. The integration combines Cloudflare's global network of 330+ data centers with Securosys' FIPS 140 Level 3 certified hardware security modules.

This solution allows organizations to use Cloudflare's security stack without exposing private keys outside tamper-resistant HSM hardware. As part of Cloudflare's Developer Services portfolio, it extends TLS key operations to customer-controlled HSM infrastructure while preserving Edge-based TLS termination and requiring no changes to existing applications. Customers can choose the deployment model that best fits their needs: on-premises Securosys Primus HSMs for maximum control or Securosys CloudHSM for operational simplicity with the same security guarantees.

## Solution Benefits

**Cloud Security Without Key Exposure:** Access Cloudflare's complete security suite while private keys remain exclusively within Securosys HSM hardware. No trade-offs between protection and control.

**Global Performance, Local Compliance:** Cloudflare's 330+ Edge locations ensure global performance, while Securosys HSMs store keys in FIPS-compliant hardware, supporting PCI DSS, HIPAA, GDPR, and other regulatory requirements.

**Minimal Latency Impact:** Session resumption ensures that only new connections require interaction with the key server. Returning visitors connect instantly through Cloudflare's Edge without additional round trips.

**Get started**

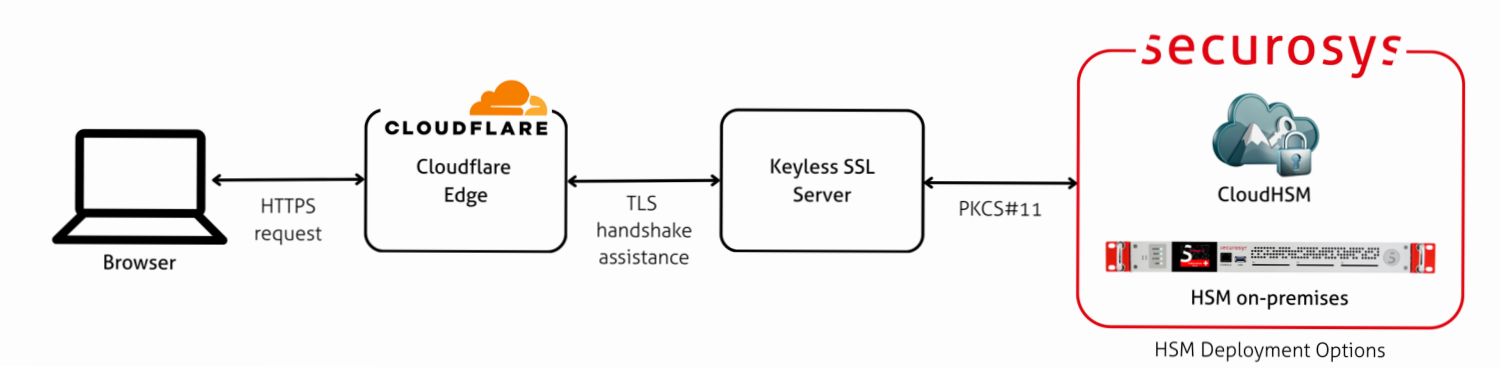
securosys

## How it works

The joint solution is based on a key architectural insight: TLS private keys are required only once per handshake, for a single cryptographic operation. Cloudflare's Keyless SSL protocol delegates this operation to the customer's infrastructure while handling everything else at the Edge.

When visitors connect to a protected website, Cloudflare's Edge server initiates the TLS handshake and securely forwards only the signature request through a mutually authenticated tunnel to the customer's key server. The key server uses Securosys' PKCS#11 provider to communicate with the Primus HSM, which performs the cryptographic operation within its secure boundary and returns only the computed result. The private key material never leaves the HSM, never traverses the network, and never becomes accessible to Cloudflare's infrastructure.

To minimize latency, session resumption ensures that this additional round trip only occurs for new connections. Returning visitors reconnect instantly through Cloudflare's Edge without contacting the key server, delivering performance comparable to traditional CDN deployments.



HSM Deployment Options

## Use Cases

### Upgrade Existing Cloudflare Deployment to HSM-Backed Security

Organizations already using Cloudflare can transition from uploading private keys to Cloudflare's infrastructure to storing them securely in Securosys HSMs. This allows them to continue using the same Cloudflare services while adding hardware-level key protection.

### Geographic Key Sovereignty

Organizations with data residency or sovereignty requirements can deploy Securosys HSMs in specific jurisdictions, ensuring local control over cryptographic keys while still benefiting from Cloudflare's globally distributed Edge network for content delivery and attack mitigation.

### Centralize Key Storage and Management

TLS private keys for multiple websites and applications can be centrally managed within a clustered Securosys HSM deployment, while all traffic is routed through Cloudflare's Edge.

About Cloudflare

About Securosys

CLOUDFLARE | PARTNER NETWORK