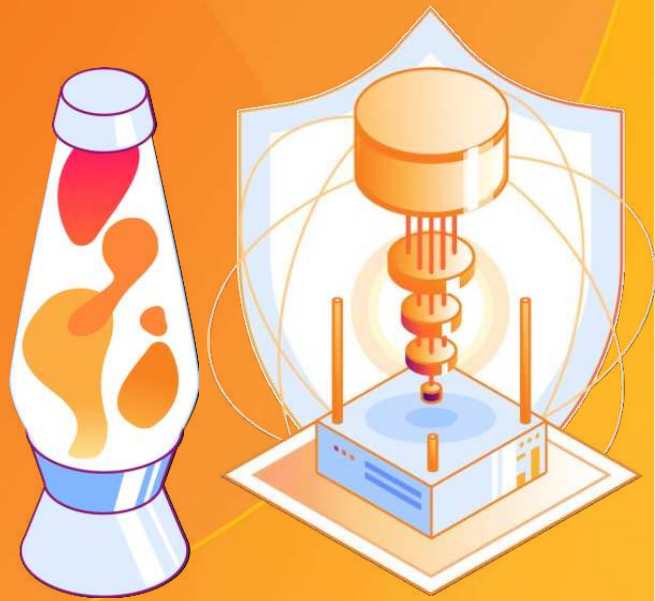
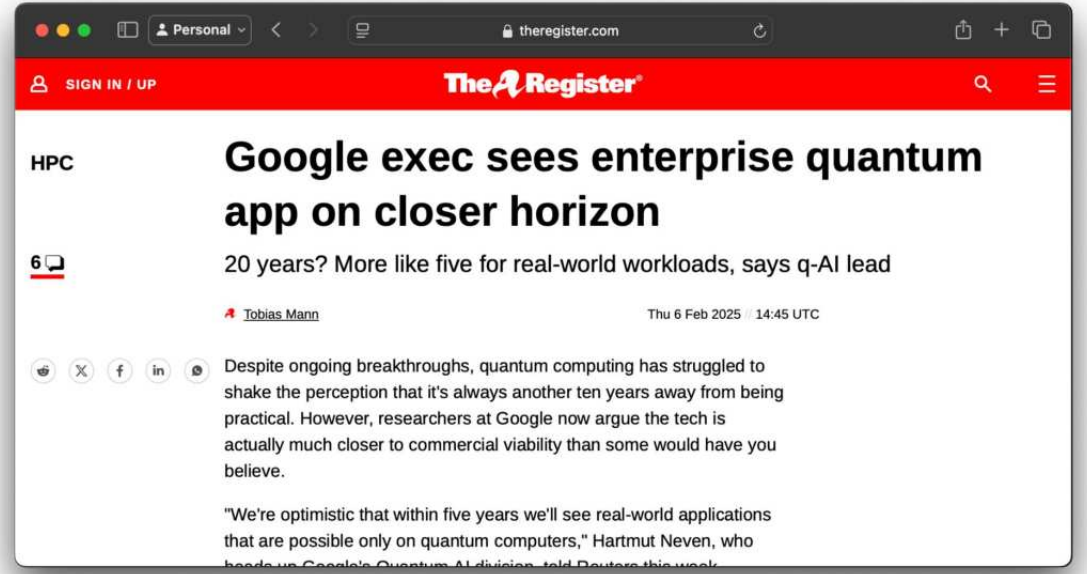
CLOUDFLARE

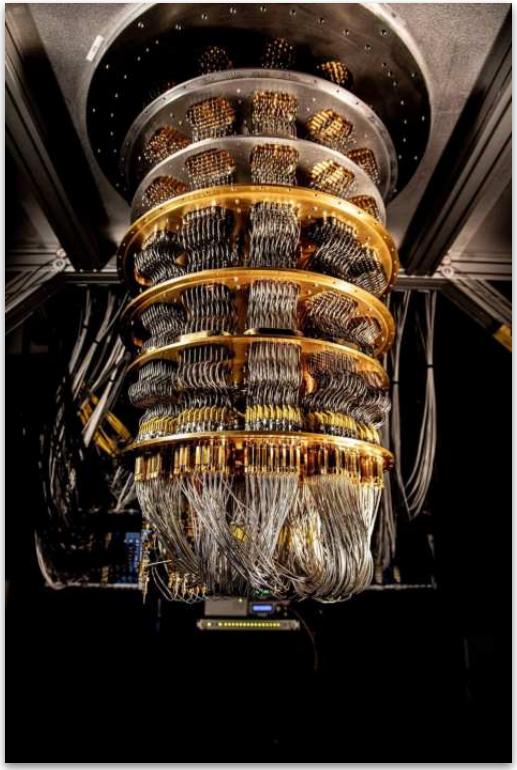
Post Quantum Cryptography at Internet Scale

Sharon Goldberg, PhD
Senior Director, Product



Quantum Computers threaten conventional cryptography (RSA, ECC) that is used everywhere



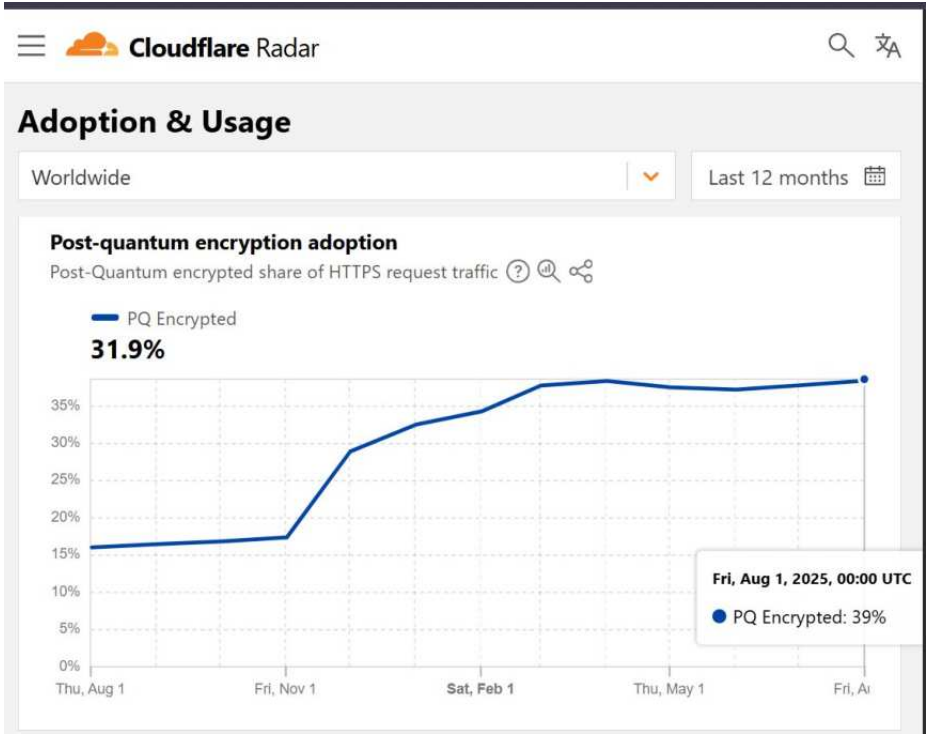


Why Start the Transition to Post Quantum Cryptography?

- **RSA and ECDSA will be deprecated in 2030:** NIST announced that widely-used public-key cryptography algorithms must be deprecated by 2030 and disallowed by 2035.
- **Cost of waiting:** Experience shows that updating cryptographic algorithms is hard and takes years. (See e.g., MD5/SHA1/DES)
- **Harvest Now, Decrypt Later:** Adversaries that store today's encrypted data can decrypt them in the future, when better quantum computers are available.
- **Regulatory Pressure**: Government directives are urging action today (e.g., U.S. NIST, CISA, NSA, EO 14144) .
- **Unknowns:** Many quantum research efforts remain classified.

At Cloudflare, we already run PQC at Internet scale

- **Early Adopter of TLS 1.3 with PQC:** Pioneered PQC trials in 2019 (CECPQ2 with Google Chrome)
- **On by default since 2022:** Secure connection also requires browser support (hybrid ML-KEM with X25519)
- **At Scale:** Over ⅓ of the human traffic into Cloudflare's network already uses post-quantum key agreement today
- **Across our product suite and internal links:** To provide end-to-end quantum safety



Cryptography Landscape

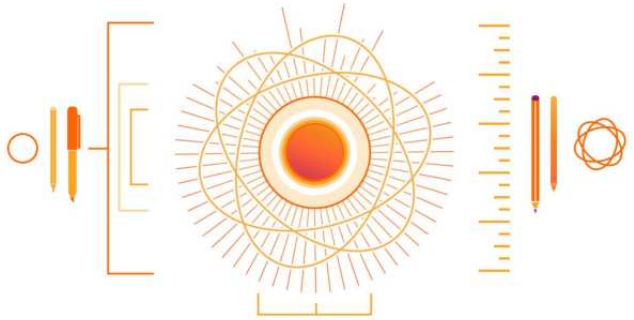
- **Post-quantum key agreement** (TLS 1.3 with ML-KEM)
  - Mature. We use it at scale at Cloudflare today.
  - ML-KEM stops harvest-now-decrypt-later attacks
  - *Vendors have converged to a "hybrid" deployment model where ML-KEM deployed alongside classical ECDH*

- **Post-quantum digital signatures and certificates:**
  - Still being standardized
  - Needed to stop active man-in-the-middle attacks in the future, when we have better quantum computers

- **No need to upgrade symmetric cryptography**
  - *Note: Quantum computers break public-key cryptography (e.g., RSA, ECC, ECDSA) using Shor's algorithm. Symmetric encryption, like AES, is affected by Grover's algorithm but these attacks are impractical. AES-256 and AES-128 are still quantum-resistant due to limitations in Grover's algorithm.*

CLOUDFLARE

Advice on deploying PQC at scale today



- **Start with TLS 1.3 with hybrid ML-KEM.**
  - ML-KEM prevents harvest-now-decrypt-later attacks
  - Hybrid reduces security/compliance risks
  - TLS 1.3 with ML-KEM is very performant
  - No need to upgrade symmetric crypto; 128 bit is still fine
- **No need for specialized hardware**
  - ML-KEM works on regular hardware
  - Quantum Key Distribution (QKD) not necessary or sufficient for security
  - Also, QKD requires vacuum or fiber medium. Doesn't work on cellular, WiFi, etc
- **Start now by tunneling traffic over PQC connections with ML-KEM**
  - Immediate security benefit without needing to upgrading individual systems
- **Make sure your vendors have a cryptoagility plan**
  - Eventually, systems need to be **upgraded to support PQ signatures + certs**
- **Once tunnels are in place, look to upgrade individual systems**
  - Tunnels provide immediate protection against harvest-now-decrypt-later attacks, so you have time to do a cryptography audit and upgrade individual systems.

How to Migrate and When to Start

- **Phase 1: Assessment (Now–6 Months)**
  - Start Now!
  - Inventory most critical assets & identify PQC-ready vendors. (Cloudflare & others)
- **Phase 2: Tunnel traffic over PQ protected connections (with ML-KEM) (6–24 Months)**
  - Gain immediate security against harvest now decrypt later attacks without upgrading
  - Make sure your tunnel provider is building with cryptoagility in mind
    - The tunnel eventually needs to support PQ signatures and certs
  - No need for specialized hardware or Quantum Key Distribution (QKD)
- **Phase 3: Upgrade individual systems to PQC (~24–48 Months)**
  - For traffic at rest
  - For traffic between devices in your local area network
- **Phase 4: Track standards, compliance and cryptoagility**
  - For traffic at rest and inside your local area network

Let Cloudflare shoulder the burden of your upgrade to PQC

By tunneling traffic through Cloudflare, our customers automatically gain protection for harvest-now-decrypt-later attacks using TLS 1.3 with post-quantum key agreement (ML-KEM)

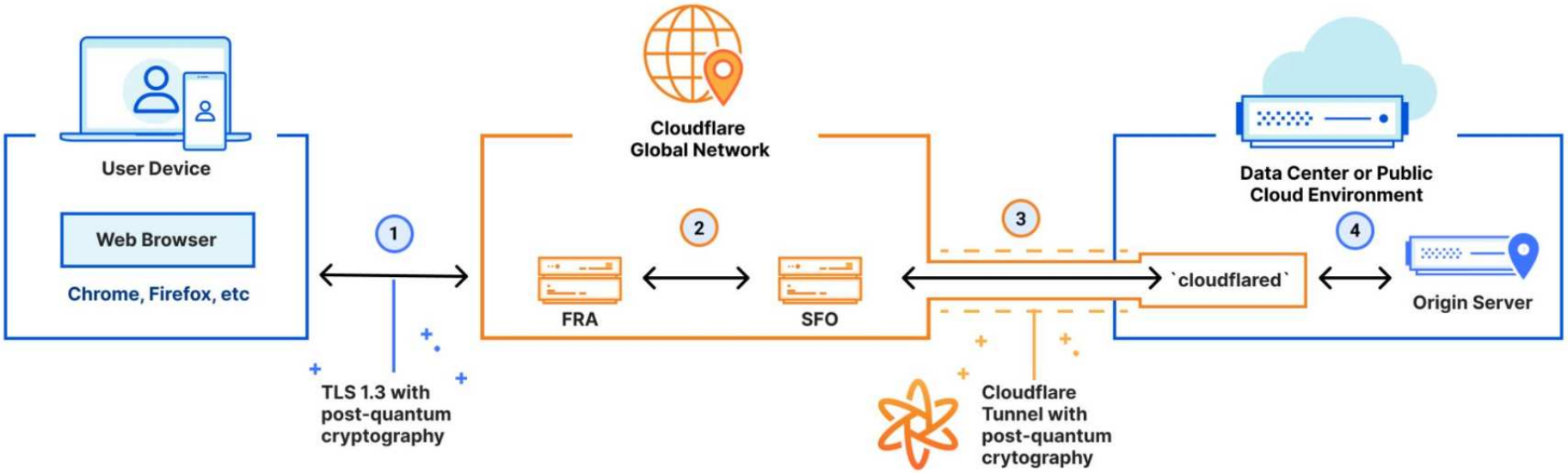
🛡️ Websites and APIs

- All websites and APIs served through Cloudflare are protected by TLS 1.3 with PQC
- Connections back to origin server that use Cloudflare Tunnel are also secured with PQC

🔄 Post-quantum Zero-Trust

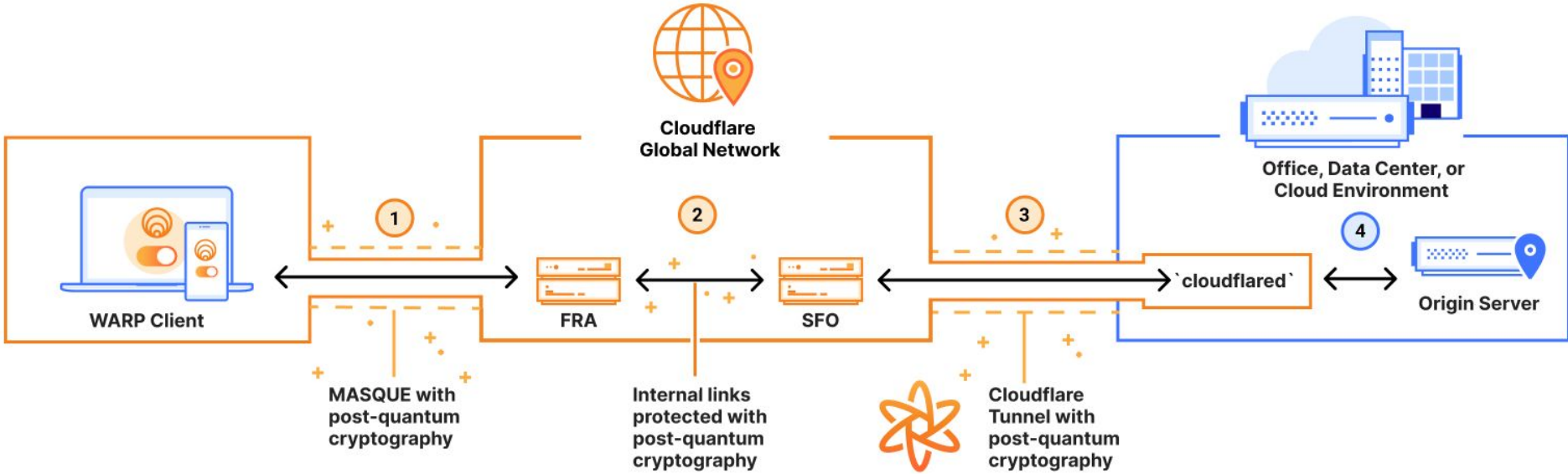
- **Post-Quantum Clientless Access:** Protect employee access to your corporate websites with PQC, even if those websites are not yet upgraded to PQC
- **Post-Quantum VPN / Zero-Trust Network Access:** Tunnel any protocol through quantum-safe Cloudflare tunnels, with WARP client on user devices and Cloudflare Tunnel to corporate office/cloud/datacenter.
- **Post-Quantum Secure Web Gateway (SWG):** A SWG secures access to third-party websites by intercepting and inspecting TLS traffic; connections from browser to SWG are PQC, and from SWG to origin are PQC as long as the origin supports PQC.

Enhancing Web Security with Post-Quantum Cryptography



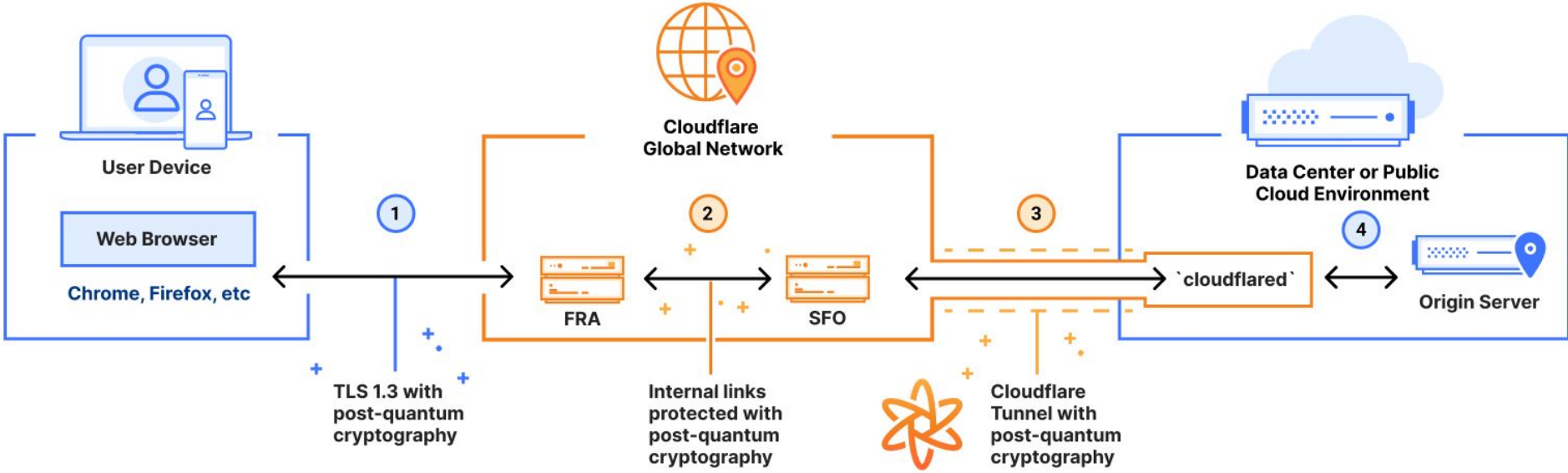
* No immediate need to make changes to origins.

Zero Trust + PQC: Future-Proofing Internal Security



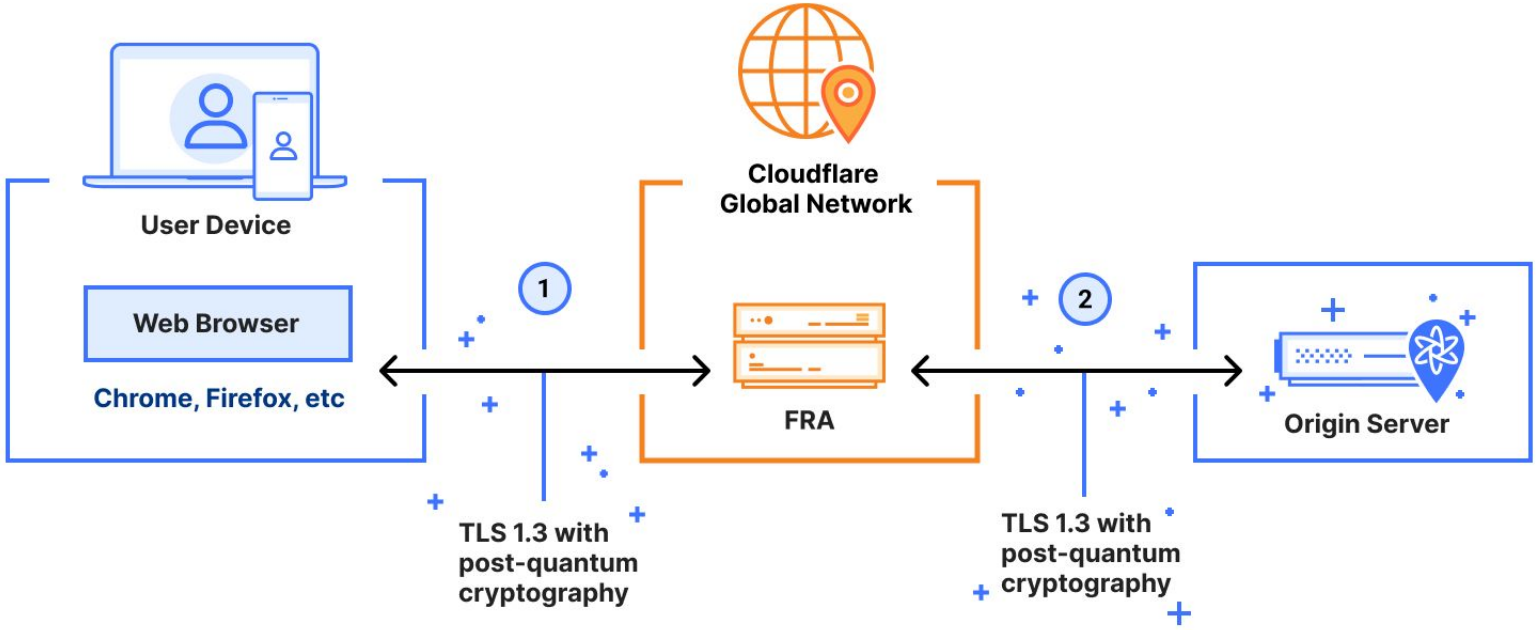
* No immediate need to make changes to origin.

Clientless Access + PQC: Future-Proofing Internal Security

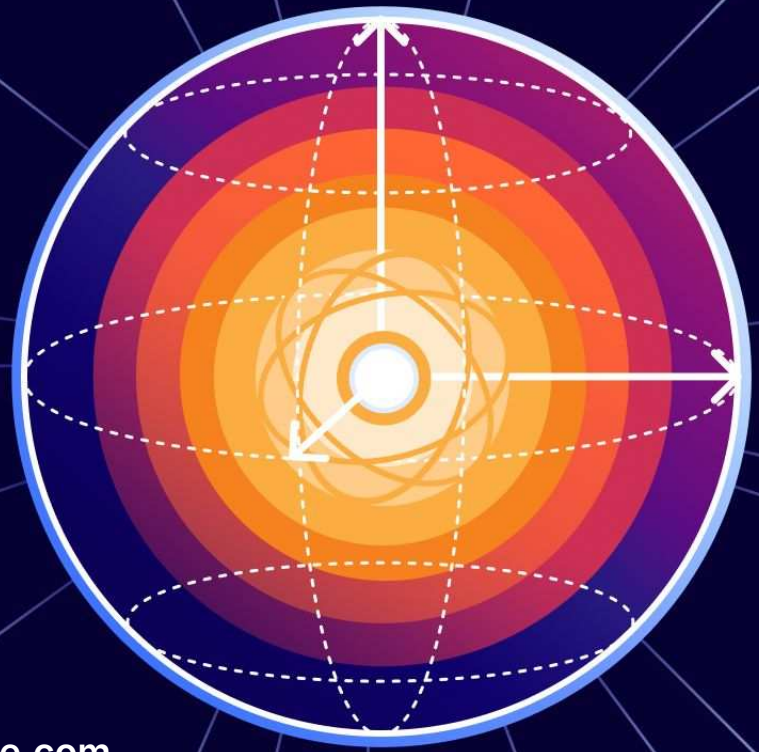


* No immediate need to make changes to origin.

Post Quantum Secure Web Gateway



Thank you!



1 888 99 FLARE

enterprise@cloudflare.com

www.cloudflare.com