FullProxy

AppViewX

The countdown has started

Certificate lifecycles halved in March 2026. Are you prepared?

Turn the 200-day rule into a foundation for post-quantum security.

Every secure connection your organisation makes - every login, checkout, or device - depends on trust. That trust rests on digital certificates; the unseen machine identities that keep data private and systems authenticated.

From 15 March 2026, all public TLS certificates will be capped at 200 days. This marks the first stage in a series of significant certificate lifecycle reductions that will see expiries at no more than 47 days by 2029.

The reason: a global security upgrade by the major cert authorities in preparation for Post-Quantum Cryptography (PQC). Shorter lifecycles enhance encryption hygiene and reduce risk, bringing you greater protection - but also vastly greater operational demands.

The time to automate cert management is now. Without automation, renewal workloads multiply. With automation, you build crypto-agility that strengthens security and readies you for the quantum era.

Why certificate lifetimes are shrinking

- Long-lived certificates extend the risk window for key compromise.
- Shorter validity forces regular renewal, improving visibility and policy compliance.
- Frequent rotation prepares infrastructures for algorithm changes (like PQC).
- The shift aligns with the NCSC's 2028 PQC-readiness milestone, helping organisations modernise their cryptography in time.

The Road Ahead
A Shorter, Smarter Certificate Lifecycle

Now (As of March 15th 2026)
Renewals twice per year, certificate visibility becomes essential.
200 days

15 Mar 2027
Quarterly renewals, manual processes no longer scalable.
100 days

2029 onward
Monthly renewal cadence, automation becomes unavoidable.
47 days

FullProxy

AppViewX

> “The 200 day rule has been the first real world step toward crypto-agility. It’s not a burden, it’s a blueprint for quantum-ready security.”
>
> Ewan Ferguson, CEO at FullProxy

The Challenge

When certificates shrink, workloads grow

Shorter certificates create a faster renewal cycle. An organisation managing 1,000 certificates may spend over 4,000 hours annually on manual renewals today. Under 47-day certificates, that workload could increase tenfold.

Manual management risks:

- Missed renewals leading to outages and downtime
- Increased human error during frequent change windows
- Lost productivity as engineers firefight
- Gaps in compliance, inventory, and ownership visibility

Without automation, shorter lifespans increase cost and risk. With automation, they become a security accelerator, enforcing discipline, transparency, and crypto-agility across the enterprise.

The Solution

Automate for Agility with AppViewX

FullProxy partners with AppViewX to help you turn these new renewal cycles into a foundation for quantum-ready security.

With AppViewX you can:

- Discover every certificate; public, internal, cloud, and containerised.
- Automate renewal and deployment using ACME and API-driven workflows.
- Integrate seamlessly with F5, Fortinet, and other core infrastructure.
- Maintain continuous compliance through dashboards and audit policies

Outcome: Operational efficiency and crypto-agility.

The Next Step

Build Quantum-Safe Foundations Now

The NCSC advises completing cryptographic inventories by 2028. That process begins today, with crypto visibility, automation, and agility enabled by effective certificate lifecycle management.

In short:

- Shorter lifecycles are strengthening digital trust.
- Automation transforms complexity into resilience.
- PQC readiness starts with better certificate management.

Run a FREE Public Domain Certificate Scan

PUBLIC DOMAIN FREE CERTIFICATE SCAN

Discover unmanaged certificates, assess renewal workload, and begin your PQC ready automation journey with the help of FullProxy and AppViewX.