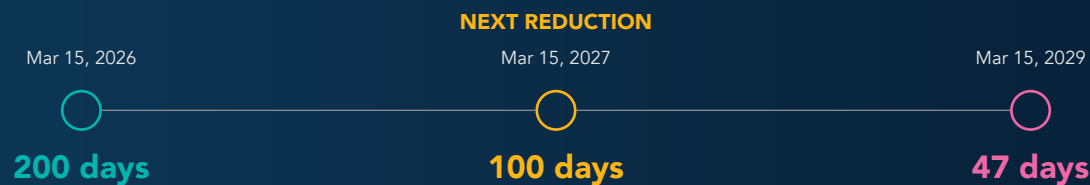




The SSL Landscape: Six-Month Checkpoint

What the Forbes Global 2000 data says
about readiness for 100-day certificates

The life-cycle reduction is accelerating



Secure Sockets Layer (SSL) certificates used to be valid for 10 years. Over the past 15 years, this has been shortened to its current life cycle in a bid to strengthen trust and reduce exposure from compromised keys. The latest decision in 2025 was to eventually bring it down to 47 days in phases. The first phase began on March 15, 2026, reducing life cycles from one year to 200 days.

The 200-day certificate life-cycle phase is already exposing the operating model that enterprises will carry into the next reduction. Six months in, the landscape

shows progress—but not yet a fully automated operating model, signaling future challenges for enterprises.

At this six-month checkpoint, CSC's analysis of approximately 246,100 certificates on the core domains of Forbes Global 2000 companies shows a market still balancing legacy one-year certificates with much shorter validity periods. The question now isn't whether certificate operations will become more frequent, but whether inventory, ownership, and automation are mature enough before the move to 100-day certificates on March 15, 2027.



246,100
certificates analyzed

Across the core domains of the Forbes Global 2000.



55.8%
use 3+ providers

More than half of companies still manage certificates across three or more providers.



41%
are 1-year certificates

Some companies have yet to feel the full impact of shorter-term certificates.

Readiness signal

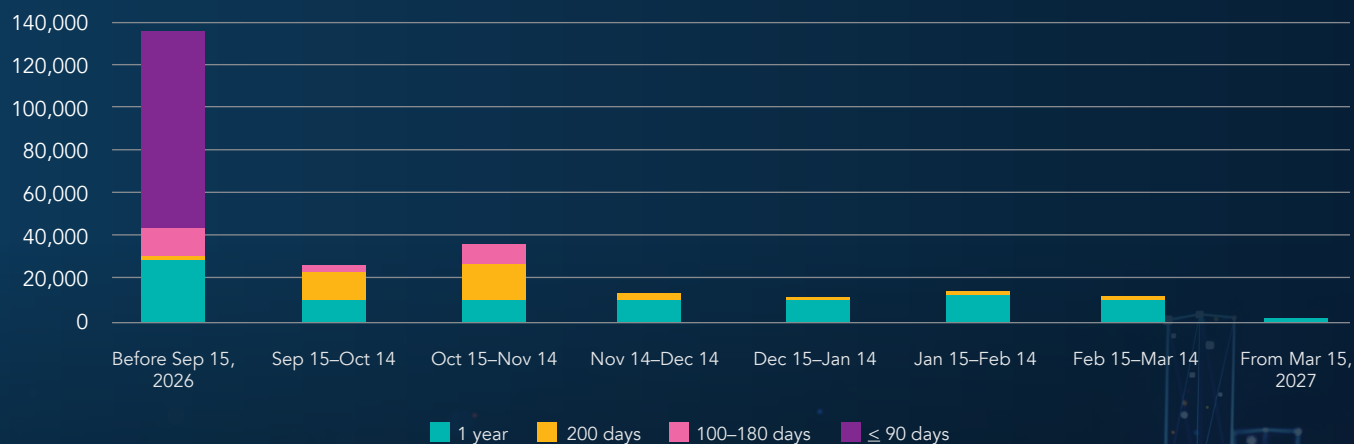
The next phase is operational, not theoretical.

CSC's 2025 [The SSL Landscape](#) warned that fragmented certificate management amplifies risk as life cycles shorten, because teams must manage multiple provider touchpoints at greater frequencies, increasing the likelihood of oversight. The report recommended standardizing processes, educating teams, consolidating where practical, and automating the full workflow. This 2026 data makes those recommendations more immediate.

Operational pressure

About 41% of the certificates analyzed have a one-year validity, suggesting that some companies may not have been impacted yet by shorter-term certificates. However, at the six-month checkpoint on September 15, 2026, 31% of those will be due for renewal with certificates that have a maximum validity of 200 days and will have to be renewed twice a year.

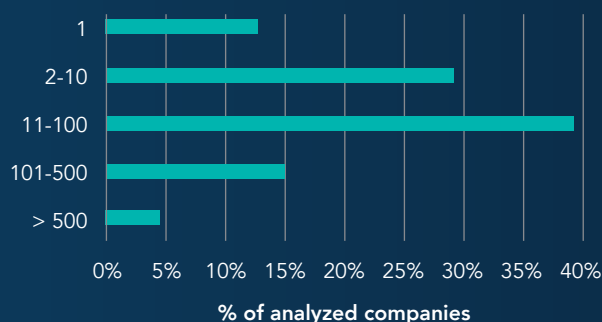
Certificates renewing in upcoming months*



Shorter life cycles multiply routine renewal activity. The critical test is whether certificate discovery, validation, issuance, installation, and monitoring can run consistently without manual bottlenecks.

Certificate portfolio sizes are not small

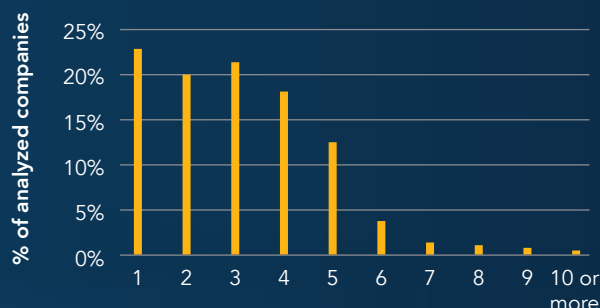
Number of certificates on the main domain



According to our research, 58.6% of companies have more than 10 certificates on their main domain, and roughly one in five have more than 100. A few companies had over 15,000 certificates each. At that scale, spreadsheets and ad-hoc ownership are difficult to sustain; complete inventory and automated renewal workflows become foundational controls. Even before accounting for certificates beyond the core domain, the data points to an inventory problem that becomes materially harder as renewal windows compress. Any missed renewal could result in the disruption of applications, sites, and more. This can lead to losses in revenue, reputation, and trust.

Provider sprawl is still common

Number of certificate providers used on the main domain



Only 24.2% of analyzed companies use a single provider on their main domain. A further 55.8% use three or more providers, reinforcing [the earlier landscape report](#) finding that fragmented management creates multiple points of risk with scattered inventory, differing renewal timeframes and notices, and inconsistent processes—a concern that grows as renewal and validation tasks become more frequent.

Similar to previous findings, about 44% of certificates are with Let's Encrypt, Google, and Amazon, which provide low-cost domain validation (DV) certificates. These low-cost DV certificates are highly accessible, attracting both legitimate companies and malicious actors. As a result, they are the certificate type most frequently associated with fraudulent domains taken down by CSC's Enforcement Team.

Readiness for 100 days

Best practices need to become the default

The data point to a mixed picture: Enterprises are managing substantial certificate portfolios, but provider fragmentation remains common. With the next life cycle reduction due March 15, 2027, the remaining runway should be used to remove manual dependencies.



Centralize inventory.

Know every certificate, its owner, provider, validity period, and deployment point. Discovery should cover the full workflow, not only certificates already visible to the central team.



Standardize and document.

Shorter life cycles reward repeatability. Define approval, validation, issuance, installation, monitoring, and exception processes before automating them.



Avoid multiple automation implementations.

Multiple providers can mean multiple portals, application programming interfaces (APIs), renewal rules, and troubleshooting paths. Consolidation can simplify both automation and operational response.

The six-month checkpoint serves as a warning against complacency. As certificate life cycles continue to shrink, standardizing and automating certificate management helps organizations keep pace. With clearer visibility across expanding portfolios, they can better manage provider sprawl and strengthen security controls.

Request a consultation to explore CSC certificate management solutions tailored to your organization's evolving needs.

[CONTACT CSC NOW](#)



Let's talk 800-927-9800 | cscdbs.com

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSecSM platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve. Visit **cscdbs.com**.

This document is provided by CSC for information purposes only and does not constitute an offer, invitation, or inducement to contract. The information herein does not constitute legal, tax, regulatory, accounting, or other professional advice, and therefore one should seek appropriate professional advice before considering a transaction as described in this document. No liability is accepted whatsoever for any direct or consequential loss arising from the use of this document.