STATE OF SSL

2026

Global Website Security Intelligence Report

First Edition — March 2026

193.4 million certificates · 362.6 million domains · One mandate that changes everything

Insights powered by Dataprovider web intelligence data

Created by
Alex Wong

Table of Contents

About This Report

This week, the internet changed.

On March 15, 2026, the CA/Browser Forum’s Ballot SC-081v3 took effect — the most significant structural change to SSL certificate management in the history of the public web. Maximum certificate validity dropped from 398 days to 200 days. Domain validation reuse periods shortened to 199 days. Every certificate issued from today forward operates under a compressed lifecycle that demands automation, visibility, and active management in a way that annual renewals never did.

The timing of this report is not coincidental.

The State of SSL 2026 is a data-driven analysis of 193.4 million active SSL certificates across 362.6 million domains — the most comprehensive publicly available snapshot of the global SSL market at the exact moment the mandate takes effect. The data reveals structural shifts already underway in the SSL ecosystem — changes that will influence how certificates are issued, sold, and managed over the coming years.

Four takeaways frame everything that follows:

• **193.4 million** valid SSL certificates globally as of February 2026 — up 12.4% year-over-year

• **362.6 million** total domains tracked — the full universe against which certificate coverage is measured

• **46.5 million** domains with invalid SSL — growing nearly three times faster than valid certificate growth

• **22.4 million** domains with open database ports exposed to the public internet — up 48.7% year-over-year

This report is written for three audiences: PKI and SSL resellers building or scaling a certificate practice, managed service providers advising customers on security infrastructure, and Certificate Authorities who want an independent, data-led view of where the market stands and where it is moving.

The data comes from Dataprovider’s global web intelligence database — real domains, real certificates, real infrastructure signals, every data point traceable to a live hostname. Analysis and narrative by Alex Wong, Wow Wong. Full methodology is in Appendix C.

This analysis is informed not only by the data itself, but by years spent working across the SSL ecosystem — alongside certificate authorities, reseller channels, and hosting providers responsible for deploying and managing certificate infrastructure at scale. The goal is not simply to document what is happening in the market, but to interpret what these shifts mean for the operators responsible for selling, securing, and maintaining the infrastructure behind it.

This is the first edition of an ongoing annual series. Regional editions covering North America, Europe, Asia-Pacific, Latin America, and India will follow. The story behind the global numbers is different in every market — those editions will tell each one in full.

SSL in 2026 — Industry Overview

I have spent over two decades in the SSL and PKI industry. I have watched this space evolve from the days when an EV certificate with a green browser bar was the gold standard of digital trust, to today where nearly half the internet runs on free, automated certificates that renew every 90 days. A lot has changed. But one thing never has: you are only as strong as your weakest link.

SSL certificates are the digital keys of the modern internet. They validate identity. They encrypt communication. They are the gatekeepers deciding what gets in and what stays out — machine to machine, server to server, device to network. Every API call, every automated process, every microservice in your infrastructure relies on certificates to function.

As organizations have grown more complex, the number of certificates required to operate has exploded. And yet most organizations still have no centralized system to track them all. That gap between having certificates and actually managing them is where things go catastrophically wrong.

The opportunity in this moment is real and significant. The mandate is driving urgency that was not there before. Customers who have been coasting on annual renewals are about to face a fundamentally different operational reality. The resellers, MSPs, and CAs who get ahead of this conversation — who build automation, visibility, and managed renewal into what they offer — will be in the strongest position in this market in years.

But urgency cuts both ways. As a reminder of what happens when those gaps are left unaddressed:

Brand	Year	What Happened	Impact
Ericsson	2018	Expired software certificate in network equipment	Mobile network outages across 11 countries, ~32M users affected
LinkedIn	2018	Expired SSL certificate on mobile app	Mobile app login failures globally
Microsoft Teams	2019	Expired authentication certificate	3-hour outage, 20M daily users locked out
Xero	2022	Expired SSL certificate	Accounting platform inaccessible to thousands of businesses
Google Voice	2021	Certificate configuration failure	4-hour global outage
GitHub	2023	Expired RSA SSH host key	Widespread connection failures across developer toolchains
Outlook / Microsoft 365	2023	Expired authentication certificate	Global email and calendar access disruption

Around 81% of companies have experienced a certificate-related outage in the past two years. The cost is not just technical recovery — it is customer trust, revenue loss, and reputational damage that rarely shows up in a single line item but accumulates over every incident.

Source: Sectigo Certificate Outage Infographic, 2024.

SSL Is Critical — But Not Enough Alone

Here is the uncomfortable truth this report will show: having an SSL certificate does not mean you are secure. The data reveals millions of websites running valid, active SSL certificates while simultaneously running deprecated servers, unsupported PHP versions, outdated WordPress installations, and open database ports exposed to the public internet.

A lock on the front door does not make your house safe if the windows are open. SSL secures the transport layer — it encrypts the connection between the user and the server. It says nothing about what is running on that server, whether the software is patched, or whether the data behind it is protected from every other direction an attacker might approach from.

For resellers and managed service providers, this gap is not just a warning — it is an opportunity. Your customers need more than a certificate. They need visibility across their entire certificate estate, automated renewal so nothing slips through, and a trusted advisor who can see the full picture and act on it. The SSL certificate is the beginning of the security relationship. This report will show how much room there is to build on it.

The Boom Is Already Here

This report is a baseline captured at a moment of fundamental structural change in the SSL industry. The CA/Browser Forum Ballot SC-081v3 formally passed on April 11, 2025. Starting March 15, 2026 — this week — the maximum SSL certificate lifespan begins dropping, with further reductions already on the calendar.

2024	**March 2026**	**2027**	**2029**
Max 398 days	Max 200 days	Max 100 days	Max 47 days
~1 renewal/year	*~2 renewals/year*	*~4 renewals/year*	*~8 renewals/year*

That means the same website that renewed its certificate once a year in 2024 will need to renew it nearly eight times a year by the end of this decade. The volume growth this drives is already visible in the data — 193.4 million active certificates, up 12.4% year-over-year, and the mandate has only just taken effect. As renewal cycles compress further, issuance volume accelerates with them. This is the floor.

For organizations managing certificates manually today, the math on 47-day certificates simply does not work. For resellers and MSPs, the channel opportunity in automation, managed renewal, and certificate lifecycle management has never been more clearly defined. The window to get the right infrastructure and the right conversations in place is open now — and it will not stay open indefinitely.

Certificate Lifecycle & the 200-Day Mandate

The shift to shorter validity periods is not on the horizon — it is already happening, and the data proves it. As of February 2026, 98.3% of all valid certificates globally expire within 200 days. A year ago that figure was 95.1%.

Within 200 Days vs Long-Validity, Feb 2025 vs Feb 2026

Metric	Feb 2025	Feb 2026
Within 200 days	163.7M (95.1%)	190.1M (98.3%)
After 200 days	8.4M (4.9%)	3.2M (1.7%)
Total valid certs	172.1M	193.4M

The long-validity certificate population collapsed 61.5% year-over-year — falling from 8.4 million to just 3.2 million. The market has already moved. The remaining 3.2 million long-validity certificates are the last of a format being phased out of existence.

What the headline number does not show is the technical precision of exactly how the 200-day rule works in practice — and why the margin for error is smaller than most organizations realize.

> ### Why 200 Days Is Not Actually 200 Days
>
> The 200-day certificate mandate sounds straightforward. It is not. Each stage of the issuance process operates on its own clock — and each clock is slightly shorter than the one before it:
>
> **200 days** — the maximum a certificate can be valid. This is the number everyone quotes. But the certificate cannot exist without the domain authorization that underpins it.
>
> **199 days** — the maximum a domain validation record can be reused under SC-081. Domain authorization must pre-date the certificate and expire after it.
>
> **198 days** — the window Sectigo and other leading CAs apply to DCV reuse internally, providing a one-day buffer against the 199-day limit to prevent compliance failures.
>
> **+24 hours** — the Maximum Merge Delay: the time a Certificate Transparency log has to formally record the pre-certificate after the CA submits it.
>
> The result: a certificate issued right at the edge of each window is already at risk before it is deployed. Organizations relying on manual renewal processes have almost no margin for error anywhere in this chain.

Source: Tim Callan, Root Causes Podcast — Certificate Lifecycle Management.

Who Is Holding the Last Long-Validity Certificates

The 3.2 million remaining long-validity certificates are not evenly distributed. Where they sit — and who is responsible for renewing them — defines both the urgency of the coming transition and the opportunity for CAs and resellers who move first.

CA	Long-Validity Count	% of 3.2M Total	% of CA's Own Portfolio
Sectigo Limited	**1,348,425**	**41.6%**	**26.2%**
Amazon	592,364	18.3%	36.6%
GoDaddy.com	373,033	11.5%	0.9%
Actalis S.p.A.	328,818	10.1%	33.8%
DigiCert Inc	186,174	5.7%	2.5%
GlobalSign nv-sa	129,370	4.0%	25.1%

Sectigo's position at the top of this table is both an opportunity and a structural risk. With 41.6% of all remaining long-validity certificates globally and one of the deepest reseller channel networks in the industry, no other CA has more to gain — or more to lose — from how the next 12 to 24 months play out.

That concentration reflects how Sectigo built its market: through a broad, active reseller channel that sold the majority of these certificates on multi-year terms. Those same resellers are now the first point of contact when renewal conversations begin — a natural advantage for the partners who have already built or adopted modern automation and lifecycle management tooling.

For those who have not, the renewal wave creates a different kind of pressure. Customers facing 200-day renewals for the first time will quickly identify whether their current provider can manage that operationally. The ones who can will deepen the relationship. The ones who cannot will create an opening.

Amazon's 592,364 long-validity certificates are almost certainly tied to AWS Certificate Manager infrastructure designed to auto-renew — but the 36.6% portfolio concentration warrants verification that ACM handles the transition seamlessly across all certificate types and configurations.

Actalis, which grew 67% year-over-year, likely issued a significant portion of its long-validity certificates to newer customers just before the mandate cutoff dates took effect — making near-term renewal outreach an immediate priority.

DigiCert's exposure is smaller in volume but carries disproportionate operational complexity. Of their 186,174 long-validity certificates, 25,789 are OV and 2,842 are EV — enterprise customers with procurement cycles, legal validation requirements, and manual renewal processes built for annual or biennial terms. EV in particular requires human-in-the-loop revalidation that cannot be automated. For DigiCert's enterprise customer base, the transition to shorter validity is less a technical problem than an organizational one — and the advisory firms and consultants who can help navigate that complexity are well positioned to deepen those relationships now.

The Wildcard Problem

Wildcards represent 6.8% of the total valid certificate market — but 31.5% of all remaining long-validity certificates. They are dramatically overrepresented in the legacy population, and for a straightforward reason: wildcards were historically sold as multi-year certificates precisely because their value proposition — covering unlimited subdomains with a single certificate — was amplified by longer validity. Fewer renewals, less management overhead.

Under 200-day validity terms that logic inverts. A wildcard covering 50 subdomains now needs to be renewed every 200 days — and eventually every 47 days — touching every system that depends on it each time. Without automation in place, that is not a certificate management problem. It is an infrastructure change management problem.

Germany and Italy: The Geographic Outliers

Long-Validity Certificates by Country, Top 10

Country	Long-Validity Count
United States	889,894
Germany	630,181
Italy	321,613
United Kingdom	210,659
Japan	129,686
China	117,926
Spain	106,427
France	97,573

Country	Long-Validity Count
Netherlands	79,284
Canada	72,086

Germany holds 19.4% of all long-validity certificates globally — 630,181 certificates — despite representing only 7.23% of global SSL volume. DigiCert holds 33.4% of the German market — a concentration more than eight times DigiCert's global average — which explains both Germany's outsized long-validity count and why Germany is the most important non-US market for enterprise CA revenue.

Italy is the more surprising entry. Italy does not feature prominently in overall SSL volume but holds 9.9% of all long-validity certificates globally. This likely reflects a combination of slower automation adoption and local CA preferences among Italian enterprises and financial institutions.

The Reseller Channel Is the Critical Variable

The underlying theme of this section is not technical — it is operational. The majority of long-validity certificates sitting in the table above were sold through reseller channels, often on multi-year terms. When these certificates expire under the new 200-day maximum — and they will, systematically, over the next 12 to 24 months — the reseller who issued them is the most natural point of contact for renewal, migration, and the managed renewal conversation that comes after.

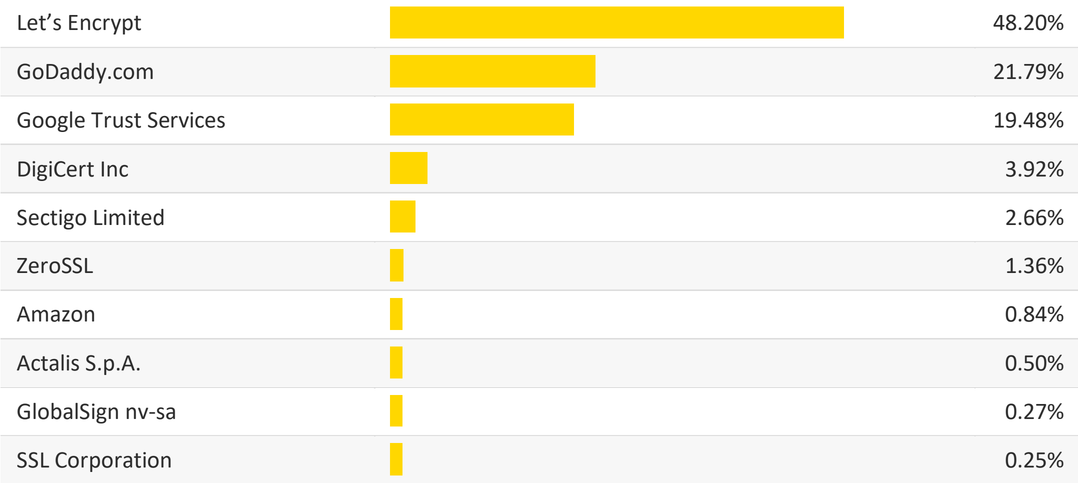
When these certificates expire under the new 200-day maximum — and they will, systematically, over the next 12 to 24 months — the reseller who sold them is in the best position to manage the transition. The reseller who is proactive — who reaches out before expiry with a clear renewal or migration path — owns that customer relationship through the next renewal cycle and beyond.

Certificate Authority Market Share

193.4 million active SSL certificates — up 12.4% year-over-year

The global SSL market now covers 193.4 million active certificates — up 12.4% from 172.1 million a year ago. Growth is not evenly distributed. The top three CAs — Let’s Encrypt, GoDaddy, and Google Trust Services — account for 89.5% of all certificates. The remaining 10.5% is split across seven other CAs in the top 10, plus a long tail of smaller issuers.

CA Market Share — Feb 2026 vs Feb 2025



#	Certificate Authority	Feb 2026	Share	Prior Share	YoY
1	**Let’s Encrypt**	93.2M	48.20%	47.37%	+14.4%
2	GoDaddy.com	42.1M	21.79%	27.40%	−8.7%
3	Google Trust Services	37.7M	19.48%	15.35%	+42.8%
4	DigiCert Inc	7.6M	3.92%	4.55%	−2.6%
5	Sectigo Limited	5.1M	2.66%	1.84%	+59.5%
6	ZeroSSL	2.6M	1.36%	1.17%	+30.6%
7	Amazon	1.6M	0.84%	0.71%	+33.1%
8	Actalis S.p.A.	0.97M	0.50%	0.34%	+65.2%
9	GlobalSign nv-sa	0.52M	0.27%	0.29%	+4.6%
10	SSL Corporation	0.48M	0.25%	0.01%	+∞

Nearly Half the Internet Runs on Free

Let’s Encrypt now holds 48.2% of the global certificate market — 93.2 million certificates. Nearly one in every two SSL certificates on the internet costs nothing and renews automatically. That is a remarkable achievement for internet security at the macro level and a fundamental market reality that every CA and reseller has had to adapt to.

Free certificates come with important limitations that the headline number does not show. There is no warranty, no support, no vetting of the organization behind the domain, and no centralized management by default. In most enterprise environments, Let’s Encrypt certificates create what the industry calls Shadow PKI — certificates spinning up across development environments, cloud instances, and containerized infrastructure, completely invisible to the security team. No one knows they exist until something breaks. The data later in this report will show that a significant share of domains running Let’s Encrypt certificates are simultaneously running vulnerable, outdated, or misconfigured infrastructure. The certificate is valid. The site is not safe. Having a free lock does not make your house secure — and for customers who think free is good enough, that is the conversation worth having.

Sectigo: From Comodo’s Shadow to No. 2 Commercial CA

Sectigo: From Comodo's Shadow to No. 2 Commercial CA

For anyone who has been in this industry long enough to remember the Comodo era, Sectigo's current position is worth pausing on. The rebrand in 2018 was not just cosmetic — it marked a genuine shift in strategy, moving the business beyond high-volume DV into a broader product portfolio and a more deliberate focus on the reseller channel.

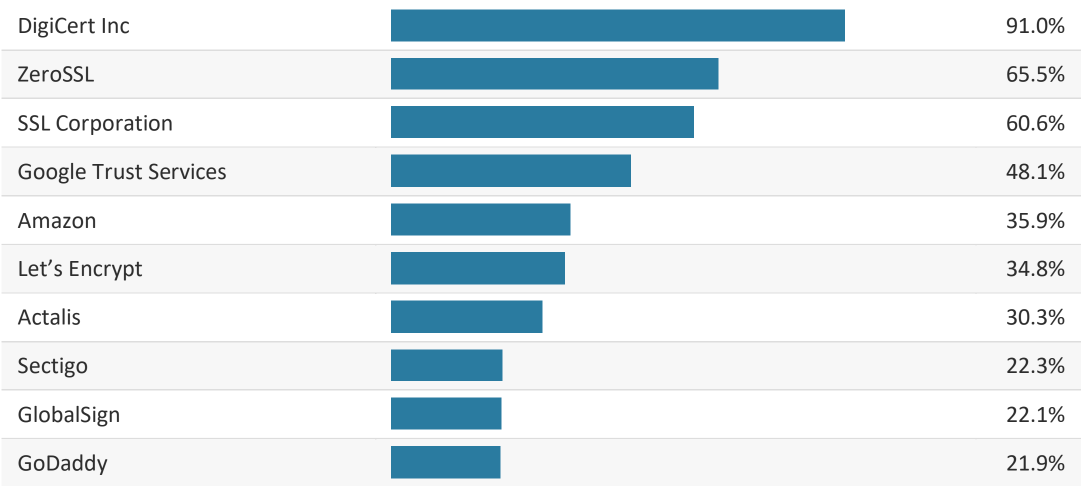
That repositioning shows in the numbers. Sectigo now holds 2.66% global market share, up from 1.84% a year ago — the strongest growth rate among established paid CAs in the top 10, adding nearly 2 million certificates year-over-year. In a market increasingly polarised between free automated issuance and DigiCert's enterprise end, Sectigo has carved out a growing mid-market position that is harder to replicate than the volume numbers suggest. For resellers and MSPs, that mid-market focus matters — Sectigo has built more of its commercial infrastructure around the channel than any other paid CA in the top 10, and that shows in product accessibility, partner tooling, and pricing that works for the SMB and mid-market customers that make up most of their customer base.

The 200-day mandate is the first real test of whether that channel depth translates into retention at scale. The next edition of this report will tell us how well it held.

DigiCert: Smaller Numbers, Bigger Footprint

DigiCert holds 3.9% of the global certificate market by count — but that number dramatically understates their actual presence in enterprise infrastructure. 91% of DigiCert’s valid certificates sit on domains that do not respond to public web crawlers. The next highest is ZeroSSL at 65.5%. Most CAs sit between 20–35%.

Non-Responsive Domain % by CA



This is not a data anomaly — it is a deliberate strategy. DigiCert has moved deeper into enterprise infrastructure: certificates for internal systems, APIs, private networks, load balancers, IoT devices, and machine-to-machine communication that was never intended to be publicly accessible. These are environments where organizations actively block external crawlers as a security measure. DigiCert’s web-visible market share significantly understates their real footprint. The enterprise infrastructure, private networks, and machine identity space is the high-stakes end of the certificate market, and DigiCert has deliberately positioned itself there.

GoDaddy: The Biggest Story Nobody Is Talking About

GoDaddy enters 2026 holding 21.79% global market share — still the second largest CA by volume — but the trajectory tells a different story. Twelve months ago GoDaddy held 27.4%. That is a 5.6 percentage point drop in a single year, in a market that grew 12.4%. GoDaddy did not just lose share — they lost absolute certificate volume while every other CA in the top five grew.

A sharp volume drop in March 2025 — approximately 8 months before the SC-081 mandate — suggests GoDaddy may have begun transitioning away from legacy certificate configurations that inflated their numbers. Whatever the cause, the trajectory is clear: GoDaddy is losing share faster than any other major CA. For resellers and competing CAs, GoDaddy's declining trajectory represents the clearest channel opportunity in this dataset — customers actively moving away from one of the market's largest providers, looking for alternatives.

Certificate Types — DV, OV & EV

When the SSL industry was built, the hierarchy of certificate types carried real meaning. DV was entry level — it proved you controlled the domain but said nothing about who you were. OV went further, verifying the organization behind the domain. EV was the premium tier — the green address bar, the company name visible in the browser, the highest level of publicly verifiable trust. Customers understood the difference and made deliberate purchasing decisions based on it. That world is effectively gone.

Type	Share	Count
Domain Validation (DV)	**99.808%**	**193.1M**
Organization Validation (OV)	0.175%	338K
Extended Validation (EV)	0.018%	34K

For every OV or EV certificate active on the internet today, there are approximately 570 DV certificates. The gap is not closing — it is widening.

OV: Where Paid Certificates Still Have a Home

OV is declining — down 2.95% year-over-year — but the story of who is still buying OV certificates tells you exactly where the paid CA opportunity lives.

CA	OV Share
DigiCert Inc	**38.4%**
Sectigo Limited	18.0%
GlobalSign nv-sa	11.6%
Others	32.0%

DigiCert leads at 38.4%, Sectigo at 18%, GlobalSign at 11.6% — the established paid CA hierarchy. But look further down the list and you find Hellenic Academic and Research Institutions CA, Internet2, Cybertrust Japan — institutional and regional players serving specific compliance or national requirements that free automated CAs structurally cannot meet.

OV has retreated into well-defined niches: regulated industries, academic institutions, government-adjacent organizations, and markets where local or sectoral requirements mandate organization verification. Financial services, healthcare, government contracting, legal — anywhere a compliance or audit framework requires proof of who is behind the domain, not just that someone controls it. In those environments OV is not declining — it is the only option.

The commercial case for OV requires a compliance or regulatory driver. If your customer has one, OV remains the right conversation. If they do not, the honest answer is that DV achieves the same browser result for less cost and less friction. Knowing which customer is which is the entire skill.

EV: The Slow Extinction of a Premium That Lost Its Visual

EV certificates are down to just 33,933 globally — 0.018% of the market — and the monthly trend shows consistent decline every single month for 14 months without interruption or recovery.

CA	EV Share
DigiCert Inc	**43.2%**
Sectigo Limited	18.3%

CA	EV Share
GlobalSign nv-sa	9.1%
Others	29.4%

The cause is well understood in the industry: when Apple, Google, and Mozilla removed the green address bar from browsers between 2018 and 2019, they removed the only visual differentiator that made EV meaningful to end users. Without the green bar, an EV certificate looks identical to a DV certificate in the browser. The premium evaporated overnight. What remains — dominated by DigiCert and Sectigo — is largely legacy contracts and compliance-driven purchases in regulated industries where EV is still mandated by internal policy rather than external requirement.

The monthly trend line says the rest. EV is not stabilizing. The question is not whether it will continue declining — it will. The question is what eventually replaces it as a verifiable signal of organizational identity online. That conversation is happening in the industry, but no answer has arrived yet.

A Clear Dividing Line

The data draws a clean and permanent line. Free and automated CAs — Let's Encrypt, Google Trust Services, ZeroSSL — are present exclusively in the DV tier. They issue no OV, no EV, and by design never will. Validation beyond domain control requires human review, organizational vetting, and legal accountability that the free automated model cannot support. The paid CA market — DigiCert, Sectigo, GlobalSign — owns OV and EV entirely. Any customer with a compliance requirement or organizational identity need that goes beyond basic domain control still has to go through a paid CA.

DV is no longer a tier — it is the market. The commercial conversation has shifted from selling validation level to helping customers manage the growing volume of certificates they already have, and addressing the vulnerabilities a valid certificate does nothing to protect against.

Domain Types & Deployment Patterns

If the previous section showed what kind of certificates are being issued, this section shows how they are being deployed across the internet — and the year-over-year shifts here are some of the most dramatic in the entire report.

Domain Type	Feb 2025	Feb 2026	Change
Single-Domain	73.97%	83.38%	+26.67%
Multi-Domain (SAN)	19.81%	9.80%	−44.42%
Wildcard	6.22%	6.82%	+23.22%

A note on how this data is counted: each figure represents the number of unique root domains carrying that certificate type on their primary hostname — not the total number of certificates issued. A multi-domain SAN certificate covering ten properties still registers as one record against the root domain it is deployed on. The counts reflect deployment reality across the internet, not issuance volume from CAs.

The Multi-Domain Collapse

Multi-domain SAN certificates collapsed 44.4% year-over-year

The single most striking data point in this section: multi-domain SAN certificates collapsed 44.4% year-over-year — losing 15.1 million certificates in twelve months.

Multi-Domain SAN Certificates — Quarterly Volume

Period	Avg Volume	Trend	Notes
Q1 2025	33.0M		Jan–Mar avg; decline begins mid-quarter
Q2 2025	29.4M		Apr–Jun avg; steady fall continues
Q3 2025	24.6M		Jul–Sep avg; accelerated drop
Q4 2025	19.3M		Oct–Dec avg; approaching floor
Feb 2026	18.9M		Latest snapshot

Multi-domain SAN certificates were designed for a specific enterprise problem: cover multiple domains or subdomains — www, mail, vpn, portal, api — under a single certificate with a single renewal event. One certificate, one management action, one renewal date. In a world of annual renewals that was operationally elegant. In a world moving toward 200-day and eventually 47-day renewals, the logic reverses entirely. When one domain on the certificate needs to change or one renewal is missed, the entire certificate must be reissued — touching every property it covers simultaneously. The operational overhead at high renewal frequency becomes unsustainable.

Organizations are simplifying ahead of the mandate — migrating to single-domain certificates that can be managed, renewed, and replaced independently without cascading risk across other properties. The 44.4% collapse is not customer loss. It is certificate strategy changing in real time, driven by the same automation pressure that is reshaping the entire market.

For resellers managing enterprise customers still running large SAN deployments, this is an active migration conversation. The customer has a problem they may not have fully articulated yet — and the solution is a combination of certificate restructuring and automation tooling.

Single-Domain Wins. Wildcard Grows.

Single-domain certificates grew 26.7% year-over-year — adding 34 million certificates and jumping from 74% to 83.4% of the global market. This is the simplest certificate format: one certificate, one domain, one renewal event. Single-domain certificates are the native format of ACME protocol automation, the default output of Let's Encrypt, and the architecture that scales cleanly as renewal cycles shorten. For the vast majority of websites — small business, e-commerce, personal sites, SaaS landing pages, any single-property web presence — single-domain is the right answer and the market has moved decisively in that direction.

Wildcard certificates grew a steady 23.2% — from 10.7 million to 13.2 million — with notable acceleration in December 2025 and January 2026. Wildcards secure all subdomains under a root domain with a single certificate: one wildcard for *.company.com covers dev.company.com, staging.company.com, api.company.com, and every other subdomain simultaneously. The use case is specific and growing: cloud-native architectures with subdomain proliferation, SaaS platforms spinning up customer-specific subdomains dynamically, CDN configurations, microservices environments, and development pipelines where new subdomains appear and disappear faster than individual certificates can be managed.

The wildcard growth story has a clear buyer profile — it is not the small business market. It is the cloud infrastructure and SaaS operator market, where the alternative to a wildcard is managing dozens or hundreds of individual certificates across a constantly changing subdomain landscape. For resellers with customers in that segment, wildcard certificates paired with automation tooling is a high-retention, recurring revenue conversation.

The acceleration in late 2025 is worth watching. It likely reflects organizations making deliberate architecture decisions ahead of the 200-day mandate — choosing wildcards as a complexity-reduction strategy before renewal frequency forces the issue. The next edition of this report will show whether that acceleration continues or plateaus once the immediate mandate pressure has been absorbed.

The Same Story From a Different Angle

One pattern connects the domain type data back to the certificate type section: paid CA customers choosing OV certificates are proportionally more likely to be running multi-domain SAN or wildcard deployments. The customer managing a complex multi-property domain estate — multiple brands, multiple services, internal and external-facing systems — is almost always a paid CA customer with an OV or occasionally EV certificate. The customer automating basic HTTPS coverage across a simple web presence is almost always on DV.

Domain type and validation tier tell the same underlying story from different angles: the market has split cleanly into two segments. Volume, automation, and simplicity on one side. Complexity, compliance, and managed infrastructure on the other. The commercial opportunity for paid CAs and their resellers lives entirely in the second segment — and the domain type data helps identify exactly who those customers are before the conversation starts.

Invalid SSL — The Hidden Growth Story

193.4 million valid SSL certificates. The industry points to that number as evidence that the web is getting more secure. The mandate is working. Adoption is up. The story is positive.

46.5 million domains are carrying invalid SSL certificates — up 31.75% year-over-year

The number that does not make the announcement is this: **46.5 million domains are carrying invalid SSL certificates right now** — and that figure grew **31.75% year-over-year**, nearly three times faster than valid certificate growth. The SSL market is expanding in both directions simultaneously: more valid certificates and more broken ones, accelerating in parallel.

> *For every 4 domains with a valid certificate, there is 1 with a broken one.*

And it is about to get harder to manage, not easier. Certificate growth alone does not equal improved security. As certificate lifetimes shorten and the number of certificates increases, the operational burden grows faster than many organizations are prepared for. Visibility and lifecycle management — not certificate issuance — are becoming the real challenge.

The same mandate driving valid certificate growth — shorter validity periods and more frequent renewals — also increases the surface area for failure. Today organizations renew certificates roughly once per year. At **200 days**, that becomes roughly twice per year. At **47 days**, nearly eight times per year.

Every renewal cycle introduces another opportunity for automation to fail, a DNS record to be misconfigured, a notification to be missed, or a script to break silently with no human in the loop to catch it.

The **31.75% growth in invalid certificates** suggests the market is already struggling to keep up with annual renewals. The coming lifecycle compression will stress that further — and the organizations without proper certificate lifecycle management in place will feel it first.

Status	Feb 2025	Feb 2026	Growth
Valid SSL	172.1M	193.4M	+12.37%
Invalid SSL	35.3M	46.5M	+31.75%

How Certificates Go Invalid

Invalid certificates do not appear from nowhere. They follow predictable and recurring patterns — which means they are also predictable and preventable:

- **Expiry without renewal** — the most common cause. No one was tracking the renewal date, the notification email went to a departed employee, the auto-renewal script failed silently, or the domain was simply forgotten. The certificate expires and the domain continues serving traffic under a broken trust signal.
- **Misconfiguration** — the certificate exists and is valid, but it is incorrectly installed: deployed on the wrong domain, missing intermediate chain certificates, or covering a hostname that does not match what the browser is requesting. The certificate is technically fine. The deployment is broken.
- **Self-signed certificates never replaced** — indicated in the data by the presence of Internet Widgits Pty Ltd as an issuer — the default placeholder name in OpenSSL. These are development or internal certificates that were stood up temporarily and never properly replaced with publicly trusted certificates.
- **Revocation** — triggered by CA mis-issuance, key compromise, or compliance failure. The certificate was valid when issued. An event occurred that made it unsafe to trust. The CA revoked it.
- **Hosting panel defaults** — some hosting environments issue SSL automatically on provisioning but do not manage renewals. When the initial certificate expires, nothing replaces it unless the customer or reseller intervenes.

Who Holds the Invalid Certificates

CA	Invalid Count	% of Total Invalid
Let's Encrypt	**13,103,867**	**28.19%**
GoDaddy.com	10,529,066	22.65%
Sectigo Limited	6,763,269	14.55%
DigiCert Inc	2,905,549	6.25%
GlobalSign nv-sa	1,257,719	2.71%
Cloudflare	1,013,737	2.18%
Internet Widgits Pty Ltd	925,472	1.99%
ZeroSSL	749,517	1.61%

Internet Widgits Pty Ltd is the default OpenSSL placeholder issuer — indicating self-signed certificates deployed in production and never properly replaced.

Let's Encrypt and GoDaddy together account for over half of all invalid certificates globally — a direct reflection of volume dominance. The more certificates you issue, the larger your share of the lapsed pool will be. That is expected. What the distribution also reveals is a specific failure mode in automated free certificate environments: when the automation breaks — a failed ACME challenge, a changed DNS record, a misconfigured renewal script — there is no human in the loop to catch it. The certificate expires silently. The domain owner may not know for days, weeks, or longer.

> *The automation that makes free certificates scale is the same mechanism that makes their failures invisible.*

Not All Invalid Is Equal — But Some of It Is Dangerous

Not every invalid certificate represents an active threat. A parked domain, a decommissioned staging environment, an abandoned project — invalid SSL on a domain with no live traffic is a data point, not a crisis. The risk is proportional to whether the domain is actively serving users.

For domains that are live and serving traffic, an invalid certificate creates a specific and layered set of problems:

- **User trust destruction** — browsers display immediate security warnings. Most users stop. Those who click through are signalling to any attacker monitoring the network that certificate warnings on this domain are being ignored.
- **Man-in-the-middle exposure** — an expired certificate that continues serving traffic creates an interception window. During exactly the period when users are being warned that something is wrong and proceeding anyway, the connection is at its most vulnerable to redirection to a malicious endpoint.
- **API and system-level failures** — applications, integrations, and services that rely on certificate validation to confirm identity do not click through warnings. They fail silently or throw errors that propagate through connected systems. Invalid SSL in an enterprise environment is not just a browser problem — it is an integration risk.

Who Fixes It and How

Invalid certificates do not fix themselves. Responsibility sits at two levels — and for resellers and MSPs, one of those levels is yours.

① CA Responsibility

Revoked certificates — triggered by mis-issuance or key compromise. The CA notifies the domain owner of record, which may be a hosting provider, registrar, or reseller — not the end customer actually affected.

② Reseller / MSP Responsibility

Expired, misconfigured, and self-signed certificates — responsibility sits with whoever manages the domain. In a reseller or MSP context, that means you. Certificate monitoring is the baseline of responsible management.

Type	Trigger	Who Acts	Resolution
Expired	Renewal date missed	Domain owner / reseller	Renew certificate
Misconfigured	Wrong domain, chain incomplete	Domain owner / reseller	Reinstall, check SANs
Self-signed	No CA-issued cert in place	Domain owner / reseller	Replace with CA-issued cert
Revoked	Mis-issuance / key compromise	CA + domain owner	CA notifies; replace required

> *Invalid SSL is only one layer. The Security Risk section later in this report shows how far the gap extends beyond the certificate — into open database ports, outdated software, and infrastructure that a valid certificate does nothing to protect.*

Global Distribution

SSL infrastructure is not evenly distributed. The top 10 countries account for 72.6% of all valid certificates globally — 140.5 million of 193.4 million. The United States alone holds 42.9% of the entire global total.

Top 10 Countries by Valid SSL — February 2026

United States	82,939,088
Germany	13,977,639
Canada	8,270,011
United Kingdom	7,452,442
China	6,318,158
Japan	6,123,808
France	4,291,183
Netherlands	4,084,013
India	3,741,811
Brazil	3,255,957

Three observations worth pulling from this data:

Germany punches above its weight. At 7.23% of global SSL volume, Germany is the clear number two — and the only country outside North America with meaningful scale. This reflects both the size of the German commercial web and a strong cultural and regulatory preference for paid, high-assurance certificates. DigiCert holds 33.4% of the German market — more than eight times its global average of 3.9% — making Germany the single most important non-US market for enterprise CA revenue.

France and the Netherlands are Let's Encrypt territory. Both countries show Let's Encrypt dominance at 74–76% market share, well above the global average of 48.2%. The paid CA opportunity in these markets is narrow and concentrated in compliance-driven segments.

India and Brazil are the growth frontier. Both countries are underrepresented relative to their internet user populations — India at 1.93% of global SSL volume, Brazil at 1.68%. Let's Encrypt is absorbing nearly all new SSL growth in both markets. The paid CA opportunity is limited to enterprise and regulated segments today, but the absolute scale of both markets makes them worth watching closely as digital infrastructure investment accelerates.

Full CA breakdowns by country are included in Appendix A. Regional report editions covering each market in depth are available separately.

Hosting Company SSL Coverage

SSL coverage rates vary dramatically depending on one factor above all others: whether the hosting provider manages certificates on behalf of their customers or leaves it to the customer to manage themselves.

Hosting Company	Valid SSL	Without SSL	% Secured
Cloudflare, Inc.	33,667,464	3,198,355	91.33%
Squarespace, Inc.	8,116,398	<1,159,315	>87.5%
Google LLC	13,379,283	2,048,846	86.72%
Amazon.com, Inc.	56,608,869	20,270,490	73.63%
Hostinger	6,100,401	2,145,896	73.98%
SEDO GmbH	6,624,686	2,426,511	73.19%
Hetzner Online	3,611,945	2,977,660	54.81%
OVH SAS	2,863,105	3,354,144	46.05%
Linode, LLC	2,547,356	4,752,564	34.90%
1&1 Internet SE	2,686,107	7,821,567	25.56%

Three observations worth noting:

Managed platforms cluster at the top. Cloudflare at 91.3%, Squarespace at over 87.5%, Google at 86.7% — every provider in the top three handles certificate provisioning automatically as part of their platform. The customer does nothing. The certificate exists. When SSL management is removed from the customer's responsibility, coverage approaches 90%.

Infrastructure providers expose the gap. 1&1 at 25.6%, Linode at 34.9%, OVH at 46.1% — providers where the customer manages their own server environment show coverage rates that are a fraction of their managed counterparts. Amazon at 73.6% sits in the middle: a mix of managed services like CloudFront and Elastic Beanstalk pulling the number up, and raw EC2 instances where certificate management is entirely the customer's problem pulling it down.

SEDO is the outlier worth explaining. SEDO is primarily a domain parking and aftermarket platform — meaning a significant portion of its SSL-covered domains are parked pages, not active websites. Its 73.2% coverage rate reflects automated certificate provisioning on parked inventory rather than active web properties. The number is real; the context matters.

> *The gap between managed and unmanaged hosting SSL coverage is not a customer behaviour problem — it is a product design problem. Platforms that automate certificates achieve near-universal coverage. Platforms that do not, don't.*

Registrar SSL Coverage

Domain registrars sit at a unique point in the certificate relationship — they are where domains are born, but certificate management is often handled elsewhere. The top 10 registrars collectively account for 59% of all valid SSL certificates globally.

Registrar	Valid SSL	% Secured
GoDaddy.com	**47,120,148**	**72.14%**
Namecheap	11,240,930	73.11%
Squarespace (combined)	6,940,870	—
Tucows	6,682,634	71.53%
GMO Internet	4,169,252	67.63%

Registrar	Valid SSL	% Secured
Hostinger	3,779,169	69.88%
Wix.com	3,027,408	—
NameBright	2,797,904	—
Dynadot	2,691,325	—

Note: Squarespace appears as two separate registrar entities in the data (Squarespace Domains LLC + Squarespace Domains II LLC), combined here at 6,940,870. Where % Secured is marked —, the without-SSL count fell below the top 10 threshold for those registrars, indicating strong coverage.

Three observations from this data:

GoDaddy's registrar scale dwarfs everyone else — and is declining. At 47.1 million valid SSL certificates, GoDaddy holds 24.4% of all valid SSL certificates among registrar-managed domains. That is a remarkable concentration — and it is declining. The March 2025 volume drop visible in the CA data is reflected here as well. Whatever the cause, the registrar with the largest single book of SSL business in the world is shrinking it.

Hostinger is the fastest-growing registrar in this dataset. Up 88.2% year-over-year — adding 1.77 million valid SSL certificates in twelve months. Hostinger's growth reflects aggressive expansion into markets where its price point and bundled hosting plus SSL value proposition resonate strongly: Eastern Europe, Southeast Asia, and Latin America. The growth trajectory puts Hostinger on a path to challenge the top-five registrars by SSL volume within the next reporting cycle.

Platform registrars outperform on coverage. Squarespace and Wix do not appear in the top 10 without-SSL table — which indicates near-universal SSL coverage across their registered domain base. When the registrar is also the hosting platform, certificate management collapses into a single automated step. The coverage gap is a problem for registrars who are pure registrars. It largely disappears for registrars who also manage the hosting layer.

Note: GoDaddy's sharp volume drop in March 2025 — visible in the CA market share trend data — is equally visible in the registrar data. The cause remains under validation.

Security Risk Beyond the Certificate

Every section in this report so far has measured certificates — how many exist, who issued them, how long they last, and whether they are valid. This section measures something different: what is running behind those certificates on the live, actively responding web.

All metrics below are measured on live, actively responding websites. Domains users are visiting right now. Not parked pages, not staging environments, not decommissioned infrastructure. Active websites with real traffic.

SSL secures the communication channel. It does nothing to protect against what an attacker finds when they look past the padlock.

What the Data Found

Vulnerability	Feb 2026 Count	YoY Direction
Open database ports	22,439,171	▲ +48.69%
Unsupported PHP versions	6,350,971	▼ −23.34%
Deprecated Nginx	2,781,862	▼ −13.52%
Outdated WordPress (v2–v5)	1,593,708	▼ −31.69%
Deprecated IIS	677,345	▼ −25.38%
Deprecated Apache	305,277	▼ −19.36%

Most of what this data shows is moving in the right direction. Outdated WordPress down 31.7%. Unsupported PHP down 23.3%. Deprecated server software declining across every category measured. The web is getting cleaner — slowly, but measurably. One number is not.

22.4 million domains have publicly exposed database ports — up 48.7% year-over-year. While every other vulnerability category is declining, direct database exposure is accelerating. A valid SSL certificate and an exposed database port can exist on the same domain simultaneously. One does nothing to mitigate the other.

Knowing More Than Your Customer

The reseller or MSP who can show a customer their full vulnerability surface — not just their certificate status, but their open ports, their deprecated software, their unpatched CMS — is having a fundamentally different conversation than the one that starts and ends with certificate renewal.

This data exists at domain level. That means for any customer portfolio it is possible to know right now which domains have valid SSL and which do not, which have open database ports and which are clean, which are running deprecated server software and which are current. That is a complete security posture report, domain by domain, across an entire managed customer base.

The certificate is the starting point. This data shows how much further the conversation can go.

Key Takeaways

1. The certificate volume boom is already underway — and the mandate will accelerate it further. 193.4 million active certificates, up 12.4% year-over-year, with renewal frequency set to double, then quadruple, then increase eightfold by 2029. Every compression in validity period is a multiplication in issuance volume. This is the floor, not the ceiling.

2. 200 days is not as simple as it sounds. The mandate sets certificate validity at 200 days. Domain validation reuse is capped at 199 days. Leading CAs apply a 198-day internal buffer. CT log recording adds up to 24 hours. Each of these clocks runs simultaneously and independently. Organizations relying on manual renewal processes have almost no margin for error anywhere in this chain.

3. Nearly half the internet runs on free certificates — and that changes the commercial conversation. The paid CA market is not competing for volume. It is competing for the specific customers who need what free certificates structurally cannot provide: warranty, support, OV/EV validation, centralized lifecycle management, and the human accountability layer that automated issuance removes.

4. The multi-domain SAN collapse is a signal, not an anomaly. A 44.4% decline in multi-domain certificates in a single year reflects deliberate architectural change ahead of mandate pressure. Enterprise customers are restructuring their certificate portfolios now. The reseller who is in that conversation owns the migration.

5. 3.2 million long-validity certificates remain — and the window to act on them is closing. Sectigo holds 41.6% of them. Amazon holds 18.3%. GoDaddy holds 11.5%. These are not abstract numbers — they are specific customer renewal conversations waiting to happen, in the next 12 to 24 months, through the reseller channels that originally sold them.

6. Invalid SSL is growing three times faster than valid SSL — and shorter validity will make it worse. 46.5 million invalid certificates, up 31.75% year-over-year. Every compression in renewal frequency is another opportunity for automation to fail silently. The organizations that struggle to manage annual renewals today will struggle harder at 200 days, harder still at 47 days.

7. Valid SSL and secure infrastructure are not the same thing. 22.4 million open database ports — up 48.7%. 6.4 million domains running unsupported PHP. Valid certificate, exposed infrastructure. The padlock is not a security audit. It is the beginning of one.

8. The reseller opportunity is in owning the full security conversation. Not selling more certificates — managing more of the customer's security surface. Certificate lifecycle management, vulnerability monitoring, proactive renewal, infrastructure visibility. The data in this report exists at domain level. That means it is actionable, customer by customer, across every managed portfolio in the channel.

What This Means

The SSL ecosystem is not shrinking — it is evolving. Encryption has become universal, but the operational complexity behind it is increasing. As certificate lifetimes compress and infrastructure becomes more distributed, the organizations that succeed will be the ones that treat certificate management as an operational discipline rather than a periodic task.

About the Author

Alex Wong has spent over two decades working at the intersection of SSL, PKI, and the channel business. He has held senior roles across the certificate supply chain — from CA partnerships and reseller operations to managed security services and product strategy. He has seen the industry from every angle: the CA building the product, the reseller selling it, and the enterprise trying to manage it at scale.

Today Alex works as a consultant and advisor to organizations navigating the certificate lifecycle management transition — helping resellers build scalable PKI practices, advising CAs on channel strategy, and publishing independent analysis of where the market is and where it is going.

Appendix A — Country Detail: CA Breakdown by Country

United States — Total Valid: 82,939,088

Rank	CA	Count	% of Country
1	Let's Encrypt	34,961,150	42.15%
2	GoDaddy.com	33,767,515	40.71%
3	Google Trust Services	9,635,948	11.62%
4	DigiCert Inc	1,488,496	1.79%
5	ZeroSSL	995,820	1.20%
6	Sectigo Limited	986,956	1.19%
7	Amazon	696,420	0.84%
8	SSL Corporation	98,809	0.12%
9	Starfield Technologies	64,382	0.08%
10	DigiCert	52,986	0.06%

Germany — Total Valid: 13,977,639

Rank	CA	Count	% of Country
1	Let's Encrypt	5,407,406	38.69%
2	DigiCert Inc	4,662,036	33.35%
3	Sectigo Limited	2,057,537	14.72%
4	Google Trust Services	991,218	7.09%
5	ZeroSSL	543,728	3.89%
6	Starfield Technologies	123,943	0.89%
7	GoDaddy.com	119,236	0.85%
8	Amazon	34,013	0.24%
9	Hellenic Academic & Research Inst. CA	6,609	0.05%
10	SSL Corporation	5,810	0.04%

Japan — Total Valid: 6,123,808

Rank	CA	Count	% of Country
1	Let's Encrypt	2,941,255	48.03%
2	GoDaddy.com	2,293,410	37.45%
3	Google Trust Services	371,492	6.07%
4	GlobalSign nv-sa	168,556	2.75%
5	Amazon	119,393	1.95%
6	Japan Registry Services Co.	76,399	1.25%
7	DigiCert Inc	57,662	0.94%

Rank	CA	Count	% of Country
8	ZeroSSL	29,154	0.48%
9	Sectigo Limited	18,587	0.30%
10	CloudSecure Corporation	15,298	0.25%

United Kingdom — Total Valid: 7,452,442

Rank	CA	Count	% of Country
1	Let's Encrypt	3,534,068	47.42%
2	GoDaddy.com	1,567,998	21.04%
3	Google Trust Services	1,397,777	18.76%
4	Sectigo Limited	380,863	5.11%
5	Amazon	258,249	3.47%
6	DigiCert Inc	217,376	2.92%
7	ZeroSSL	27,842	0.37%
8	Starfield Technologies	18,735	0.25%
9	SSL Corporation	9,997	0.13%
10	DigiCert	9,320	0.13%

Remaining Markets Summary — Top CA by Country

Full CA breakdowns for all markets are available in the regional editions of this report. Summary below shows #1 CA by volume per country, February 2026.

Country	Total Valid SSL	#1 CA	CA Share
Canada	8,270,011	Let's Encrypt	46.3%
China	6,318,158	Google Trust Services	43.7%
France	4,291,183	Let's Encrypt	74.7%
Netherlands	4,084,013	Let's Encrypt	76.2%
India	3,741,811	Let's Encrypt	61.2%
Brazil	3,255,957	Let's Encrypt	69.2%

Appendix B — Long-Validity Certificate Deep Dive

Table 8B: Long-Validity by SSL Type

SSL Type	Long-Validity Count	% of Long-Validity	% of Type's Total
Domain Validation	3,162,719	97.45%	1.64%
Organization Validation	75,236	2.32%	22.21%
Extended Validation	7,656	0.24%	22.56%

Table 8C: Long-Validity by Domain Type

Domain Type	Long-Validity Count	% of Long-Validity
Single-Domain	2,011,172	61.96%
Wildcard	1,020,822	31.45%
Multi-Domain	213,617	6.58%

Table 8D: Long-Validity by Country (Top 10)

Rank	Country	Long-Validity Count	% of Long-Validity
1	United States	889,894	27.42%
2	Germany	630,181	19.42%
3	Italy	321,613	9.91%
4	United Kingdom	210,659	6.49%
5	Japan	129,686	3.99%
6	China	117,926	3.63%
7	Spain	106,427	3.28%
8	France	97,573	3.01%
9	Netherlands	79,284	2.44%
10	Canada	72,086	2.22%

Table 8E: Per-CA Breakdown by SSL Type (Top 6 CAs)

CA	DV	OV	EV	Total	% of CA Total
Sectigo Limited	1,333,837	13,317	1,271	1,348,425	26.22%
Amazon	592,364	0	0	592,364	36.64%
GoDaddy.com	371,848	909	276	373,033	0.88%
Actalis S.p.A.	328,657	152	9	328,818	33.83%
DigiCert Inc	157,543	25,789	2,842	186,174	2.46%
GlobalSign nv-sa	117,152	11,592	626	129,370	25.09%

Appendix C — Methodology & Data Notes

Data source: Dataprovider global web intelligence database

Reporting period: February 2026 (current) vs February 2025 (YoY comparison)

Primary filter: primaryhostname = Yes — unique root domains only, excluding subdomains

Universe: 193,414,826 valid certificates across 362,576,303 total domains

Section 13 vulnerability metrics: filtered to response = Available — live responding websites only

Open database ports: openports field uses EQUALS predicate — domains with multiple exposed ports may be counted more than once. Treat as directional upper bound.

Hacked WordPress count (4): severe undercount due to crawl methodology — Dataprovider detects via homepage generator meta tag only. Treat as indicative only.

SSL Corporation top 10 entry: reflects VikingCloud portfolio acquisition — not organic growth

Domain type counting methodology: figures represent unique root domains carrying that certificate type on their primary hostname, not total certificates issued by type

Registrar data: Squarespace appears as two separate registrar entities (Squarespace Domains LLC + Squarespace Domains II LLC) — combined figure used throughout for clarity

198-day DCV buffer: Sectigo-specific implementation. SC-081 mandates 199-day maximum domain validation reuse. Sectigo applies 198 days internally. Source: Sectigo Knowledge Base, 2026.