pqprobe.com

[PQ]probe PQC Vendor Scorecard

Q2 2026 Edition

Who Ships, Who Talks, and Who Hopes You Won't Check

Davi Ottenheimer
Ottenheimer GmbH

July 2026

Contents

Introduction

This scorecard puts major technology vendors into CISA's product categories — the framework that separates products where PQC should be deployed now from those in active transition — and probes their reality versus their announcements. It covers cloud infrastructure, browsers and CDNs, messaging, networking hardware, databases, SaaS and collaboration, cloud storage, and — new in Q2 — HSM and key management.

We built a toolkit to answer the question that matters in post-quantum migration: what is actually negotiated at the endpoint right now? Not what is planned. Not what is available in a developer preview. What is protecting data in transit today? You can test it at pqprobe.com.

This is the second quarterly edition. The Q1 edition (February 2026) established the baseline. This edition tracks what moved, what did not, and what entered the scorecard for the first time.

CISA Framework

CISA divides the world into products where post-quantum key establishment should already be deployed, and products that are actively transitioning.

Table 2 — Deploy PQC now: Cloud PaaS/IaaS, chat and messaging apps, web browsers and servers, endpoint data-at-rest/full-disk encryption.

Table 3 — Actively transitioning: Networking hardware and software, SaaS, telecommunications, operating systems and hypervisors, identity and access management, email and collaboration, databases, SIEM, and continuous diagnostics.

Table 2 products — closest to the user's data in transit — have made the most progress. Table 3 products, where infrastructure complexity is highest, are largely still at the announcement stage. That gap is the story this scorecard tracks.

What Changed Since Q1

Between February and July 2026, three developments compressed the quantum timeline and changed vendor positions across the scorecard.

The quantum timeline was shortened. In March 2026, Google Quantum AI published a 57-page whitepaper demonstrating a 20x reduction in the resources needed to break 256-bit elliptic curve cryptography. ECC-256 can now be attacked with fewer than 500,000 physical qubits in minutes, not hours. Combined with Craig Gidney's June 2025 work reducing RSA-2048 to fewer than one million superconducting qubits, both major classical algorithm families are on a compressed path. Cloudflare moved its full post-quantum target to 2029 in response. Google set the same date.

The US deadline became law. On June 22, 2026, Executive Order 14412 set binding deadlines for federal high-value and high-impact systems: key establishment by the end of 2030, digital signatures and authentication by end of 2031. Federal contractors must comply with post-quantum FIPS by the end of 2030. The one-year gap between the two dates reflects the infrastructure reality this scorecard has tracked since Q1: key exchange is deployable now, authentication is harder.

Networking vendors shipped products. The networking hardware category changed the most. In Q1, the scorecard listed Fortinet as the only vendor with NIST-compliant PQC in the data path. That was incomplete: Palo Alto had shipped PAN-OS 12.1 Orion in August 2025 with all three NIST PQC standards, but the Q1 scorecard did not reflect it. After Q1, Cisco published a product roadmap with ML-KEM in Secure Firewall (FTD 10.5 / ASA 9.25) targeted for GA in late 2026, and ML-DSA following in 2027. Fortinet extended its lead with FortiOS 8.0 and FortiWeb 8.0.3. The networking category moved from "fragmented" to "converging."

HSM vendors cleared the firmware gate. Both Thales (Luna v7.9) and Entrust (nShield v13.8.0) now ship ML-KEM, ML-DSA, and SLH-DSA in production firmware with CAVP validation. The remaining bottleneck is combined FIPS 140-3 validation with PQC algorithms, which gates CA issuance of PQC certificates and federal procurement. That validation averages 500+ days in the current CMVP queue.

Origin adoption is passive. Cloudflare launched origin-server PQC tracking on Radar in February 2026. The number: approximately 10% of origins support X25519MLKEM768, up from under 1% at the start of 2025. Support means the server advertises the group; the negotiated rate is lower and Cloudflare does not publish it. Client-side adoption passed two-thirds. The gap between edge and origin remains the defining measurement problem in PQC, and it validates the "false floor" thesis from Q1: the number everyone cites measures the CDN, not the infrastructure behind it.

Regulatory Landscape

The regulatory picture has sharpened considerably since Q1. Five jurisdictions now have binding or near-binding PQC deadlines:

Jurisdiction	Key Exchange Deadline	Signatures Deadline	Source
United States	2030 (federal KEX)	2031 (federal auth)	EO 14412 (June 2026)
CNSA 2.0 (NSS)	2030 (signing, networking); 2033 (all)	2030 (sw/fw); 2033 (all); 2035 (pure PQC)	CNSSP-15
France (ANSSI)	2027 (cert gate)	2027 (cert gate)	ANSSI certification policy
Germany (BSI)	2030 (high-sens)	2031 (classical end)	BSI TR-02102
EU Roadmap	2030	2035	COM(2026) 13 / CEPS
FIPS 140-2 sunset	**Sep 21, 2026**	—	NIST CMVP

The FIPS 140-2 sunset on September 21, 2026 is the nearest deadline. After that date, remaining FIPS 140-2 validated certificates move to the Historical list and no longer satisfy federal procurement requirements. Organizations still on FIPS 140-2 modules face a double migration: to FIPS 140-3 and to PQC simultaneously. FIPS 140-3 validated modules with PQC algorithms are not yet widely available — both Thales and Entrust have submissions in the CMVP queue, but the average validation now takes over 500 days.

The ANSSI 2027 certification gate is the earliest PQC-specific deadline. Starting in 2027, ANSSI will not certify security products without post-quantum capabilities. This is a vendor gate, not a deployment gate — it tests whether the product can do PQC, not whether deployed servers negotiate it. The distinction matters: certified is not deployed.

Scorecard Summary

The summary table tracks movement from Q1. One category improved, one is new, two are stable, two did not move.

Category	Q1 Readiness	Q2 Readiness	Movement	The “Probe Gap”
Browsers / CDNs	✅ High	✅ High	▷ STABLE	Over 65% of traffic uses PQC at edge. ~10% of origins support PQ; negotiated rate is lower.
Cloud Infra	⚠️ Medium	⚠️ Medium	▷ STABLE	KMS/edge ready; databases and M365 still classical.
Networking	⚠️ Fragmented	✅ **Converging**	▲ **IMPROVING**	Cisco roadmap published. Fortinet extends lead. Palo Alto corrected from Q1.
HSM / Key Mgmt	—	⚠️ **Mixed**	**NEW**	Hardware ships PQC; FIPS validation + cloud KMS lag.
Databases	❌ None	❌ None	▷ UNCHANGED	Zero native PQC at any database endpoint.
SaaS / Collab	❌ None	❌ None	▷ UNCHANGED	Salesforce published compliance doc; endpoints still classical.

> *A grade is a snapshot. Trajectory is what matters. The networking category is the proof: three vendors moved in five months.*

Table 2: PQC Shipping

A. Cloud Infrastructure

The hyperscaler picture is stable from Q1, with incremental progress.

AWS continues the most methodical rollout. ML-KEM hybrid PQ-TLS is GA on KMS, ACM, Secrets Manager, S3, ALB/NLB, and CloudFront. AWS is phasing out pre-standard CRYSTALS-Kyber in 2026, migrating all endpoints to finalized ML-KEM. ML-DSA is now available for digital signatures in KMS (CreateKey, Sign, Verify). The AWS-LC cryptographic library is, to our knowledge, the only open-source module with FIPS 140-3 validated PQC. AWS also added PQ-TLS to Payments Cryptography in November 2025, extending coverage to regulated financial workloads.

Microsoft continues its Quantum Safe Program. SymCrypt supports ML-KEM and ML-DSA across Windows Server 2025, Windows 11, and .NET 10. Azure Key Vault is tracking PQC features through 2026–2027, but Managed HSM does not yet support PQC key types natively — PQC operations require external HSMs via the BYOK path. Azure Front Door and Application Gateway are adopting hybrid ML-KEM for TLS. Microsoft accelerated its internal migration target from 2033 to 2029 on June 30, 2026.

Google Cloud has ML-KEM and ML-DSA in preview for Cloud KMS. At Next 2026, Google announced Quantum Safe Key Imports in preview. Cloud HSM (Marvell NITROX-based) does not yet support PQC at the hardware protection level. Google’s internal target is full PQC migration by 2029.

The finding from Q1 holds: key exchange is deployed at the edge. Digital signatures and PQC certificates are not. The certificate bottleneck is now more specific: HSM vendors have the firmware, but FIPS 140-3 validation with PQC is still in the CMVP queue, which gates CA issuance.

B. Web Browsers and CDNs

Client-side adoption has passed 65%. Over 65% of browser traffic to Cloudflare now uses post-quantum key exchange, up from 52% in December 2025. Apple shipped ML-KEM by default in iOS/iPadOS/macOS 26 (September 2025), closing the last major browser gap.

Cloudflare shipped ML-DSA certificate support for origin connections in June 2026, enabling end-to-end post-quantum authentication between Cloudflare's edge and origin servers. They also became the first SASE platform with full PQ encryption (February 2026). The origin-server tracking they launched on Radar confirms the false-floor thesis: approximately 10% of origins support X25519MLKEM768 versus over 65% of traffic at the edge. Support means the server advertises the group; the share of connections that negotiate it is lower, and Cloudflare does not publish that figure.

Akamai made PQ from edge-to-origin default for all customers on January 31, 2026, as announced. PQ for client-to-edge is now default in Q1 2026.

Let's Encrypt committed to Merkle Tree Certificates for post-quantum authentication, identifying hybrid key exchange as the near-term server operator priority. Chrome is pursuing the same MTC path rather than adding post-quantum X.509 certificates to the Chrome Root Store — a decision that moved the migration target for authentication.

C. Messaging

No change from Q1. Apple iMessage (PQ3, March 2024) and Signal (PQXDH, September 2023) remain fully operational with post-quantum key agreement. This category is complete.

Table 3: Transitioning

Table 3 is where the Q2 scorecard diverges most from Q1. Two vendors shipped product. One published a compliance document. And a new category — HSM and Key Management — enters the scorecard.

A. Networking Hardware

The biggest change in the entire scorecard. In Q1, one vendor shipped PQC in the data path. In Q2, three are shipping or have committed to shipping by year-end.

Fortinet extended its lead. FortiOS 8.0 added PQC SSL deep inspection in proxy mode, allowing FortiGate to perform TLS inspection on hybrid ML-KEM connections. FortiWeb 8.0.3+ added ML-KEM and ML-DSA via OpenSSL 3.5 integration, with PQC configurable for both client-side and server-side TLS. Fortinet remains the only networking vendor with NIST-compliant PQC shipping across multiple product lines (FortiGate, FortiWeb) in production today.

Palo Alto Networks shipped PAN-OS 12.1 Orion in August 2025 with support for all three NIST PQC standards: ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205), plus non-standardized

algorithms including HQC, Classic McEliece, BIKE, and Frodo. Quantum-safe VPN tunnels and SSL/TLS sessions are available. The Cipher Translation proxy actively re-encrypts classical traffic into ML-KEM at the network edge, making legacy applications quantum-safe without code changes. Palo Alto also introduced PQC-optimized hardware. The Q1 scorecard incorrectly categorized Palo Alto as a discovery tool only. This has been corrected.

Cisco moved from a strategy blog to a published product roadmap. ML-KEM support is targeted for GA in Secure Firewall Threat Defense (FTD) 10.5 and ASA 9.25 in late 2026. ML-DSA follows in FTD/ASA 11.0 in H2 2027, along with broader coverage for inline traffic inspection. Recent hardware platforms (Secure Firewall 1200 and 6100 series) have the hardware prerequisites for PQC Secure Boot. Platforms released before 2025 are being evaluated but most are expected to lack the hardware support. This is substantive progress: specific product names, specific firmware versions, specific timelines.

Juniper Networks / HPE remains unchanged: QKD-based pre-shared keys via RFC 8784, not NIST PQC.

Vendor	PQC in Data Path	NIST Algorithms	Q1 / Q2	Status
Fortinet	✅ ML-KEM + ML-DSA	✅ FIPS 203+204	▲ Extended	FortiOS 8.0 + FortiWeb 8.0.3
Palo Alto	✅ ML-KEM + ML-DSA + SLH-DSA	✅ FIPS 203+204+205	Q1 correction	PAN-OS 12.1 Orion (Aug 2025)
Cisco	⚠️ Late 2026 target	⚠️ Committed	▲ Roadmap	FTD 10.5 / ASA 9.25 targeted
Juniper/HPE	❌ QKD only	❌	▷ UNCHANGED	RFC 8784 PPK

B. Databases: Still Unprotected

The database category has not moved since Q1. No major database vendor has deployed PQC to a connection endpoint. This remains the most significant gap in the scorecard given the HNDL exposure of long-lived data.

Microsoft SQL Server / Azure SQL — no PQC at the endpoint. SymCrypt has PQC, Schannel does not. “Data platforms” remain in the final phase of the Quantum Safe Program.

AWS RDS / Aurora / DynamoDB — no PQC at the endpoint. ALB/NLB PQ-TLS provides a proxy workaround for the client-facing leg. AWS continues its HTTPS endpoint rollout but has not named database services in the near-term schedule.

MongoDB Atlas — no public PQC roadmap. TLS 1.0/1.1 hard cutoff completed July 31, 2025; TLS 1.3 rollout described as in progress.

PostgreSQL — OpenSSL 3.5 (April 2025) includes ML-KEM. No managed PostgreSQL service offers PQC at the database endpoint.

Snowflake — complete silence. No announcements, no roadmap, no documentation.

Database Vendor	PQC at Endpoint	PQC via Proxy	Q1 / Q2	Timeline
MS SQL / Azure SQL	❌	⚠️ OS primitives	▷	Final QSP phase

Database Vendor	PQC at Endpoint	PQC via Proxy	Q1 / Q2	Timeline
AWS RDS/Aurora/DynamoDB	❌	✅ ALB/NLB	▷	HTTPS endpoint rollout continues
MongoDB Atlas	❌	❌	▷	No public roadmap
PostgreSQL (managed)	❌	⚠️ Self-hosted possible	▷	OpenSSL 3.5+ required
Snowflake	❌	❌	▷	No public roadmap

C. SaaS & Collaboration

The SaaS category remains at zero endpoint deployment with one notable change: Salesforce published a PQC compliance document.

Salesforce published a Post-Quantum Cryptography compliance document on March 18, 2026, covering multiple services including core Salesforce Services, Commerce Cloud, and Data Cloud on both First Party and Hyperforce infrastructure. The document acknowledges HNDL risk and describes Salesforce's PQC posture. It is behind a login wall, so independent verification of claims is not possible. But this is the first concrete PQC-specific compliance artifact from any major SaaS vendor — a movement from "educational only" to structured disclosure. No ML-KEM at the endpoint.

Zoom shipped post-quantum end-to-end encryption for meetings (ML-KEM-768, Zoom 6.0.10+) in May 2024. This is application-layer E2EE for meeting content, not ML-KEM negotiated in the TLS handshake to zoom.us. The Q1 scorecard listed Zoom as having no announcements. That was incorrect.

ServiceNow, Workday, Slack have not changed from Q1. No PQC deployment, no roadmaps.

Microsoft 365 (Teams, Outlook, SharePoint, OneDrive) remains in QSP Phase 3. Endpoints are not negotiating PQC. Microsoft accelerated its Quantum Safe Program timeline from 2033 to 2029 on June 30, 2026, and shipped TLS hybrid ML-KEM key exchange on Windows 11 and Windows Server 2025 on July 14, 2026. The ML-KEM groups are disabled by default and require explicit admin configuration. The migration target is now public and closer than Q1 reported, but no Microsoft 365 service endpoint negotiates PQC today.

SaaS Vendor	PQC at Endpoint	Q1 / Q2	Status
Salesforce	❌	▲ Compliance doc	PQC compliance doc published; endpoint still classical
ServiceNow	❌	▷	Discovery tool via Keyfactor; own product classical
Workday	❌	▷	Complete silence
Microsoft 365	❌	▲ Timeline accelerated	QSP target moved to 2029; endpoints still classical
Zoom	⚠️ E2EE only	Q1 correction	PQ E2EE for meetings (May 2024); TLS endpoint classical
Slack	❌	▷	No announcements

D. Cloud Storage

Every file uploaded to cloud storage over classical TLS is interceptable in transit. A file encrypted at rest with AES-256 on the provider's servers is irrelevant to an adversary who captured it during upload.

Amazon S3 remains the only major cloud storage provider with PQC in transit (ML-KEM hybrid PQ-TLS since November 2025).

Google Drive remains on classical TLS despite Google's PQC work in BoringSSL and Cloud KMS. **OneDrive and SharePoint** are waiting on Microsoft's QSP Phase 3 (2027+). **Dropbox** and **Box** have no PQC deployment or timeline.

Internxt, a small European provider, continues to claim first-mover status for post-quantum encryption alongside zero-knowledge client-side encryption.

Storage Vendor	PQC in Transit	Q1 / Q2	Status
Amazon S3	✅ ML-KEM (Nov 2025)	▷	GA — the leader
Google Drive	❌	▷	Waiting on Workspace rollout
OneDrive / SharePoint	❌	▷	QSP Phase 3 (~2027+)
Dropbox	❌	▷	No announcements
Box	❌	▷	No announcements
Internxt	✅ (claimed)	▷	Startup — claims first PQC cloud storage

E. HSM & Key Management (New Category)

This category enters the scorecard in Q2 because HSMs are the infrastructure layer that gates whether PQC certificates and signatures can exist. A CA cannot issue an ML-DSA certificate if its signing HSM does not support ML-DSA. An enterprise cannot deploy PQC key management if its KMS does not support ML-KEM key types. The HSM and KMS layer sits underneath every other category in this scorecard.

Thales Luna HSM — ML-KEM, ML-DSA, and SLH-DSA are native in firmware v7.9+ (July 2025), fully integrated without requiring external Functionality Modules. Quantum-resistant key wrapping and unwrapping supports ML-KEM and ML-DSA for secure key exchange with third-party systems. LMS/HSS support enables quantum-safe code signing per CNSA 2.0. Luna v7.9.2 has been submitted for FIPS 140-3 validation with PQC. The Luna HSM partner ecosystem (DigiCert, Venafi, EVERTRUST, Keyfactor) has tested PQC certificate issuance workflows. Thales also ships PQC in its High Speed Encryptors via field-upgradable FPGAs.

Entrust nShield — ML-KEM, ML-DSA, and SLH-DSA are native in firmware v13.8.0 (August 2025). CAVP validated for all three algorithms in September 2025. The nShield 5 includes an FPGA-based cryptographic accelerator designed for PQC acceleration via firmware updates. Submitted for FIPS 140-3 Level 3 validation through CMVP. Entrust also offers PQC-ready PKIaaS and nShield as a Service (nSaaS) with ML-DSA support.

AWS KMS — the most advanced cloud KMS for PQC. ML-KEM hybrid PQ-TLS for connections to KMS (GA across all regions). ML-DSA for digital signatures (CreateKey, Sign, Verify). AWS-LC is FIPS 140-3 validated with PQC. AWS CloudHSM uses Marvell NITROX — PQC support depends on Marvell firmware updates. In November 2025, AWS also launched ML-DSA certificate issuance in AWS Private Certificate Authority,

enabling organizations to issue PQC-signed certificates within their private PKI without waiting for public CA readiness.

Azure Key Vault — PQC features rolling out through 2026–2027 via SymCrypt. ML-KEM and ML-DSA key types are supported in some tier/region combinations. Managed HSM does not natively support PQC key operations — PQC requires external HSMs via BYOK. Azure AD (Entra ID) token signing remains classical. Microsoft's internal target was accelerated from 2033 to 2029 in June 2026.

Google Cloud KMS — ML-KEM-768 and ML-DSA in preview (not GA). Cloud HSM (Marvell NITROX) does not support PQC at the hardware protection level. Quantum Safe Key Imports announced at Next 2026. No SLA coverage for PQC features in preview.

HSM / KMS	ML-KEM	ML-DSA	FIPS 140-3 + PQC	Status
Thales Luna	✅ Native (v7.9+)	✅ Native (v7.9+)	⚠️ Submitted	Production firmware; FIPS pending
Entrust nShield	✅ Native (v13.8+)	✅ CAVP validated	⚠️ Submitted	CAVP done; FIPS 140-3 pending
AWS KMS	✅ GA (PQ-TLS)	✅ GA (Sign/Verify)	✅ AWS-LC validated	Most advanced cloud KMS
Azure Key Vault	⚠️ Partial (via SymCrypt)	⚠️ Partial	❌	Rolling out 2026–2027
Google Cloud KMS	⚠️ Preview	⚠️ Preview	❌	Preview only; no HSM PQC

> *The FIPS 140-3 validation bottleneck is the single most underreported constraint in PQC migration. Until HSM vendors clear the CMVP queue, CAs cannot issue FIPS-validated PQC certificates, and regulated enterprises cannot deploy PQC key management under federal procurement rules.*

What the Scorecard Reveals

The four patterns from Q1 continued, with two new ones.

1. **Key exchange leads; authentication waits.** Unchanged. Every vendor that has shipped PQC has shipped key exchange (ML-KEM). Post-quantum certificates are not deployed anywhere in production for public TLS authentication. The FIPS validation bottleneck for HSMs now explains part of the delay.
2. **The library is ready. The product isn't.** Unchanged. Microsoft has PQC in SymCrypt but not in Azure SQL, Teams, or Outlook. Google has PQC in BoringSSL and Chrome but not in Cloud HSM or Google Drive. The library-to-product gap persists.
3. **The edge is a false floor.** Validated with data. Cloudflare's own origin-server tracking shows roughly 10% PQ support behind the edge, and the negotiated rate is lower, against over 65% of traffic at the edge. The number most organizations cite for PQC adoption measures CDN posture, not infrastructure posture. The origin negotiated key exchange is the number that responds to migration work.
4. **Your SaaS vendors control your timeline.** Unchanged. Salesforce published a compliance document; endpoints remain classical. No SaaS vendor has deployed PQC.
5. **Networking moved the fastest.** *New findings.* The networking category had the most vendor movement of any category in Q2. Fortinet extended its lead across multiple product lines, Cisco published specific product roadmaps with firmware targets, and the Palo Alto correction brought PAN-OS 12.1 Orion (shipping since August 2025) into the scorecard. This is what vendor competition looks like when regulatory pressure and customer demand converge.
6. **The validation queue is the invisible bottleneck.** *New findings.* HSM hardware vendors have PQC in firmware. Cloud KMS services are adopting it. But the CMVP validation process — averaging 500+ days — prevents the certificates, signatures, and key management that depend on validated HSMs from reaching production. This queue, not algorithm research or vendor willingness, is now the binding constraint for PQC authentication.

What This Means for PQC Preparedness and Migration

1. **Probe your vendors again.** Vendor positions changed in five months. If you assessed networking vendors in Q1, reassess now. Cisco moved from a strategy blog to a published product roadmap. Palo Alto was already shipping PQC in the data path when Q1 was published. Fortinet extended to new product lines. Your networking refresh cycle should reflect this.
2. **Separate your KEX and auth timelines.** EO 14412 gives you until 2030 for key establishment and 2031 for authentication. These are two different migrations with different dependencies. Key exchange is a software update. Authentication depends on the FIPS validation queue, CA readiness, and client support for PQC certificates. Plan accordingly.
3. **Track the FIPS 140-2 sunset.** September 21, 2026 is two months away. If your organization procures under federal rules and your cryptographic modules are still on FIPS 140-2, you face a procurement gap regardless of PQC.
4. **Ask your HSM vendor about their CMVP timeline.** If your PKI depends on Thales or Entrust HSMs, the FIPS 140-3 + PQC validation is the gate for production PQC certificates. Get your

vendor's expected validation date. If they can't give you one, factor the 500+ day average into your migration plan.

5. **Don't wait for your database vendor.** This recommendation from Q1 is now stronger. Five months passed and zero database endpoints moved. Proxy-based approaches (PQ-TLS-capable load balancers) remain the only workaround.
6. **Use the origin number, not the edge number.** If your organization reports PQC adoption using Cloudflare or CDN statistics, you are reporting edge posture, not infrastructure posture. Probe your origin servers directly. Approximately 10% support PQ, but the negotiated rate is lower. Edge share of traffic is not the same metric as origin share of servers.
7. **Add HSM/KMS to your vendor questionnaire.** If your PQC migration plan depends on key management, add question 6 to the appendix: can your KMS perform ML-KEM key operations within a FIPS 140-3 validated boundary today?

This scorecard should look different again in Q3. The FIPS 140-2 sunset will have passed. The first FIPS 140-3 + PQC validations may land. Cisco's December 2026 commitment comes due. The question remains the same: is your organization tracking trajectory, or waiting for a snapshot?

Sources

1. Executive Order 14412, “Securing the Nation Against Advanced Cryptographic Attacks,” June 22, 2026
2. CISA: “Product Categories for Technologies That Use Post-Quantum Cryptography Standards,” CISA.gov, January 23, 2026
3. NIST FIPS 203/204/205: ML-KEM, ML-DSA, and SLH-DSA standards, August 2024
4. CNSA 2.0 / CNSSP-15: NSA Commercial National Security Algorithm Suite 2.0
5. Google Quantum AI: “Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities,” whitepaper, March 30, 2026
6. Craig Gidney: RSA-2048 resource estimates for superconducting qubits, June 2025
7. Cloudflare: “State of the post-quantum Internet in 2025,” Cloudflare Blog, September 2025
8. Cloudflare: Post-quantum origin tracking on Radar, February 2026; ML-DSA origin certificates, June 2026
9. Cloudflare: “The White House’s post-quantum executive order,” Cloudflare Blog, June 2026
10. AWS: PQC Migration Plan and service endpoint rollout, updated 2026; Payments Cryptography PQ-TLS, November 2025
11. Microsoft: Quantum Safe Program roadmap; SymCrypt PQC APIs GA, November 2025; Azure Key Vault PQC tracking 2026–2027
12. Google Cloud: Quantum Safe Key Imports preview, Next 2026; Cloud KMS ML-KEM/ML-DSA preview, September 2025
13. Fortinet: FortiOS 8.0 PQC SSL deep inspection; FortiWeb 8.0.3 PQC support via OpenSSL 3.5
14. Palo Alto Networks: PAN-OS 12.1 Orion, FIPS 203/204/205 support, quantum-safe VPN tunnels, cipher translation proxy
15. Cisco: “Preparing for Post-Quantum Cryptography: The Secure Firewall Roadmap,” Cisco Blogs, April 2026; FTD 10.5 / ASA 9.25 targets
16. Thales: Luna HSM v7.9 PQC firmware, July 2025; v7.9.1 ML-KEM/ML-DSA key wrapping, September 2025; FIPS 140-3 submission
17. Entrust: nShield 5 CAVP validation for ML-DSA/ML-KEM/SLH-DSA, September 2025; FIPS 140-3 Level 3 submission
18. Salesforce: Post-Quantum Cryptography compliance document, compliance.salesforce.com, March 18, 2026
19. ANSSI: 2027 certification gate for PQC in security products
20. BSI: TR-02102 classical encryption end date 2031; high-sensitivity recommendation 2030
21. Let’s Encrypt: Merkle Tree Certificates commitment for post-quantum authentication, 2026
22. NIST CMVP: FIPS 140-2 sunset September 21, 2026; average FIPS 140-3 validation timeline 500+ days
23. F5 Labs: PQC browser adoption analysis (93% Chrome+Firefox vs. 57% with Safari), June 2025
24. BCG: “How Quantum Computing Will Upend Cybersecurity,” November 12, 2025
25. EU PQC Roadmap: COM(2026) 13; CEPS Task Force Report, December 2025

Appendix A: Vendor PQC Readiness Questions

Use these questions in procurement reviews, vendor risk assessments, and contract renewals. Questions 1–5 are from Q1. Question 6 is new for Q2, targeting HSM and key management vendors.

#	Question	What You're Testing	Use When
1	**Protocol Level.** Your roadmap mentions ML-KEM support. Is it negotiated at the service endpoint today? If we probe your API endpoint with a PQC-aware TLS 1.3 client, will we see a hybrid ML-KEM key exchange?	Library support vs. live deployment.	Any vendor claiming PQC readiness.
2	**CBOM.** Can you provide a Cryptographic Bill of Materials for this service? We need to verify which components rely on classical signatures and which have a path to crypto-agility.	Whether the vendor knows where their own crypto lives.	Infrastructure, PaaS, key management.
3	**HNDL Shelf Life.** If your platform is compromised in 2029 by an adversary with a quantum computer, what is your plan for the harvest-now-decrypt-later risk to the backups you are taking today on our behalf?	Forces reasoning about data longevity, not just current-state encryption.	SaaS vendors holding long-lived data.
4	**Certificate Integrity.** What is your timeline for supporting PQC-signed certificates? Do you have a plan to move away from classical RSA/ECC roots of trust?	Looking beyond key exchange toward full post-quantum authentication.	Cloud providers, identity/SSO vendors, CAs.
5	**Migration Control.** Can we toggle PQC security policies via configuration, or are we locked into your global migration timeline?	Whether you're a pilot or a passenger in your own migration.	Databases, PaaS, TLS/connection policies.
6	**HSM Validation.** Can your KMS perform ML-KEM key encapsulation and ML-DSA signing within a FIPS 140-3 validated cryptographic boundary today? If not, what is your CMVP submission timeline?	Whether PQC key operations run inside a validated HSM or outside it via BYOK/software. The distinction determines audit posture.	Any vendor managing cryptographic keys on your behalf. Critical for regulated industries.

This scorecard is updated quarterly. Next edition: Q3 2026.

Start continuous post-quantum migration tracking across your organization's external attack surface today.

pqprobe.com