pqprobe.com

[PQ]probe PQC Vendor Scorecard

Q1 2026 Edition

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

Davi Ottenheimer
Ottenheimer GmbH

February 2026

Contents

Introduction

If you're building a post-quantum migration plan, you've probably run into the same problem everyone else has: nobody knows which vendors are shipping PQC, which ones are just talking about it, and which ones are suspiciously quiet. The information is scattered across dozens of analyst calls, blog posts, press releases, and roadmap documents — when it exists at all.

We built a toolkit to answer the question that matters in quantum migration: **what's actually happening right now?** Not what's planned for 2029. Not what's available in a developer preview. What's actually protecting your data today for tomorrow. You can test it at pqprobe.com.

This scorecard puts major technology vendors into CISA's January 2026 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.

Category	Readiness	The "Probe Gap"
Browsers / CDNs	✅ **High**	Client-side is solved; certificates are the bottleneck.
Cloud Infrastructure	⚠️ **Medium**	Edge services are ready; core data platforms are trailing.
Networking	⚠️ **Fragmented**	Fortinet is shipping; others are strategizing or using QKD.
Databases	❌ **None**	Critical HNDL risk with almost zero native PQC support.
SaaS / Collaboration	❌ **None**	Zero-control zone; entirely dependent on slow vendor cycles.

CISA Framework

CISA divides the world into products where post-quantum key establishment should already be deployed, and products that are actively transitioning. The distinction tells you where to direct your attention.

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.

The gap between these two tables is the story. Table 2 products — the ones closest to the user's data in transit — have made the most progress. Table 3 products, where the infrastructure complexity is highest, are largely still at the announcement stage.

Table 2: PQC Shipping

A. Cloud Infrastructure

The hyperscalers are the clearest success story so far, and the progress is real.

AWS has been the most methodical. ML-KEM hybrid post-quantum TLS is generally available on KMS, ACM, and Secrets Manager since May 2025. Amazon S3 endpoints followed in November 2025, and Application and Network Load Balancers now offer opt-in PQ-TLS security policies. AWS published an explicit migration plan in January 2025 committing to ML-KEM on "all AWS services with HTTPS endpoints over the coming years," naming ELB, API Gateway, and CloudFront as upcoming. Their AWS-LC cryptographic library was the first open-source module to include ML-KEM in a FIPS 140-3 validation. The engineering is serious, the rollout is staged by criticality, and they're phasing out the pre-standard CRYSTALS-Kyber in favor of a finalized ML-KEM across all endpoints in 2026.

Microsoft launched its Quantum Safe Program in August 2025 with a three-phase roadmap: foundational components, then core infrastructure services, then everything else. ML-KEM and ML-DSA are GA in Windows Server 2025, Windows 11, and .NET 10 as of November 2025. The SymCrypt cryptographic library — which underpins Azure, Microsoft 365, and Windows — now supports both algorithms. Their self-imposed deadline: early adoption by 2029, full transition by 2033, two years ahead of most government targets.

Google Cloud has ML-KEM and ML-DSA in preview for Cloud KMS and other services, building on their broader work with Chrome and BoringSSL.

What's notable across all three: key exchange is deployed. Digital signatures and PQC certificates are not. This is the right order of operations — key exchange addresses the harvest-now-decrypt-later threat — but it means authentication remains classical everywhere.

B. Web Browsers and CDNs

The highest adoption numbers are browser vendors and CDN providers, who can deploy changes server-side without waiting for customer action. **Chrome** (131+, November 2024), **Firefox** (135+, February 2025), and **Safari** (26, September 2025 with macOS Tahoe/iOS 26) all negotiate ML-KEM in TLS handshakes by default. Edge uses Chrome's implementation. The client side is solved for modern browsers.

Fastly began rolling out ML-KEM support across its CDN fleet in April 2025, reporting about 5% of clients using PQC at launch. The deployment is automatic for TLS 1.3 customers — no configuration required.

Cloudflare reported that 52% of TLS traffic to its network used post-quantum key exchange as of December 2025. That's the single largest PQC deployment in the world by traffic volume. Their implementation uses ML-KEM-768 hybrid with X25519 over TLS 1.3, and they've published extensive technical documentation on the rollout.

Akamai launched PQC for client-to-edge connections in September 2025 (opt-in) with plans to make it default in Q1 2026. They separately enabled PQC from edge-to-origin servers as an opt-in feature, defaulting for all customers on January 31, 2026. Notably, Akamai's implementation is backward-compatible — you can enable PQC even if your origin server doesn't support it yet.

The web infrastructure story is strong on key exchange but shares the same gap as cloud: no post-quantum certificates. The industry consensus is that PQC certificates won't be practical before 2027, which means server authentication still relies on classical signatures everywhere.

C. Messaging

Apple iMessage deployed PQ3, a post-quantum protocol, in March 2024. **Signal** deployed PQXDH, a hybrid PQC key agreement protocol, in September 2023. Both are fully operational and require no user action. This category is effectively complete for the two most security-conscious consumer messaging platforms.

Table 3: Transitioning

This is where writing a scorecard gets awkward. Table 3 products comprise most enterprise infrastructure, and the gap between marketing and implementation is wide.

A. Networking Hardware

The networking hardware category reveals the sharpest contrasts between vendors.

Fortinet is the standout. FortiOS 7.6, released July 2025, includes native ML-KEM support (ML-KEM-512, -768, and -1024, all FIPS 203 compliant) for IPsec VPN key exchange on FortiGate next-generation firewalls and Secure SD-WAN. The implementation includes algorithm stacking for defense in depth and hybrid mode for gradual migration. It ships at no additional cost to existing customers. The caveats: IPsec was the initial PQC use case (7.6.1), with SSL VPN PQC (TLS-based, including hybrid X25519-MLKEM768) following in FortiOS 7.6.5. No post-quantum digital signatures yet. No PQC in FortiSASE or cloud-delivered services. But among networking hardware vendors, Fortinet is the only one with NIST-compliant PQC algorithms shipping in production products today.

Cisco published a strategy blog on February 5, 2026, framing a two-pillar approach: Secure Communications and Secure Products. The post estimates CRQCs “may begin to emerge before 2035, if not sooner” — a timeline notably more conservative than what intelligence agencies with classified access are signaling through their 2027–2030 deadlines. The post outlines principles and workstreams but does not include specific product names, deployment timelines, or algorithm commitments.

Palo Alto Networks launched Quantum-Safe Security on January 30, 2026 — a discovery and risk assessment tool built into their existing firewall platform. It ingests telemetry from PAN-OS and Prisma Access to build a real-time cryptographic inventory (CBOM) and provides remediation guidance. The “Cipher Translation” feature can proxy-encrypt legacy traffic into ML-KEM at the network edge. This is valuable as a migration tool, but Palo Alto’s own product is not a PQC data-path solution — it observes and remediates the cryptography of other products.

Juniper Networks (acquired by HPE for $13.4 billion in July 2025) represents the most interesting claim-versus-reality case. They market “quantum-safe” IPsec VPNs on SRX Series Firewalls. But the implementation uses RFC 8784 Post-Quantum Pre-shared Keys distributed through out-of-band mechanisms — primarily Quantum Key Distribution (QKD) devices from partners. This is not NIST PQC. There is no ML-KEM key exchange in the IKE/IPsec handshake.

Vendor	Shipping PQC in Data Path	Native NIST Algorithms	Protocol	Status
Fortinet	✅ ML-KEM	✅ FIPS 203	IPsec VPN + SSL VPN (7.6.5)	GA (July 2025)
Cisco	❌	❌	—	Strategy only (Feb 2026)
Palo Alto	❌ (discovery tool)	❌	—	Discovery tool GA (Jan 2026)
Juniper/HPE	❌ (QKD, not PQC)	❌	IPsec (RFC 8784 PPK)	Partnership/demo stage

Note: RFC 8784 (Pre-shared Keys) via QKD is a different architectural path than the NIST-standardized ML-KEM. It requires expensive out-of-band hardware that most enterprises cannot scale.

B. Databases: The Crown Jewels Are Unprotected

Databases are arguably where the HNDL threat matters most. They contain the records with the longest shelf life — healthcare data, financial records, intellectual property — exactly the kind of data worth harvesting today for decryption later. Yet the database category has the weakest PQC deployment of any CISA category.

Microsoft SQL Server and Azure SQL Database have no PQC-aware TLS configuration. SQL Server Central noted explicitly in November 2025 that "there's nothing out there yet about implementation into SQL Server." The building blocks exist — ML-KEM and ML-DSA are in SymCrypt, in CNG, in .NET 10 — but they haven't propagated to the Schannel TLS stack that SQL Server on Windows uses, or to Azure SQL Database's connection endpoints. Microsoft's Quantum Safe Program roadmap lists "data platforms" in the final phase of their transition. That puts actual Azure SQL PQC deployment realistically at 2027–2029.

AWS RDS, Aurora, and DynamoDB are in a similar position. Despite AWS's industry-leading PQC rollout across security services and storage, database endpoints are not in the first or second wave. The ALB/NLB PQ-TLS announcement in November 2025 offers a partial workaround: if you front your database with a Network Load Balancer, you can get PQ-TLS on the client-facing leg. But the NLB-to-RDS connection behind it remains classical, and direct-connect database clients get no benefit.

MongoDB Atlas is still catching up on current-generation TLS. MongoDB only completed its fleet-wide TLS 1.3 rollout in early 2025 and finished deprecating TLS 1.0/1.1 in July 2025. There is no public PQC roadmap, no announcement, and no mention of post-quantum cryptography anywhere in MongoDB's product documentation.

PostgreSQL presents a different challenge. As open-source software, PostgreSQL's TLS depends on the underlying OpenSSL library. OpenSSL 3.5+ (April 2025) includes ML-KEM support, so in theory a self-managed instance could negotiate PQC. In practice, no one does this — standard OS packages ship older OpenSSL versions, and no managed PostgreSQL service offers PQC at the database endpoint.

Snowflake is completely silent on post-quantum cryptography. No announcements, no roadmap, no documentation mentioning PQC. For a platform that warehouses some of the most sensitive analytical data in the enterprise, this is a significant blind spot.

Database Vendor	PQC at Endpoint	PQC via Proxy/LB	PQC Certificates	Timeline
Microsoft SQL Server / Azure SQL	❌	⚠️ OS primitives exist	❌	"Data platforms" = final QSP phase
AWS RDS / Aurora / DynamoDB	❌	✅ ALB/NLB opt-in	❌	"All HTTPS endpoints over coming years"
MongoDB Atlas	❌	❌	❌	No public roadmap
PostgreSQL (managed)	❌	⚠️ Possible self-hosted	❌	Depends on OpenSSL 3.5+ adoption
Snowflake	❌	❌	❌	No public roadmap

C. SaaS & Collaboration

If databases hold the crown jewels, SaaS and collaboration platforms are where the daily work product lives — the emails, the documents, the messages, the tickets. CISA's Table 3 explicitly lists SaaS and email/collaboration as categories in active transition. The reality: not a single major enterprise SaaS or collaboration vendor has deployed PQC to their product endpoints.

Salesforce has invested in quantum computing research and published educational content about quantum risks. But there is no PQC deployment on any Salesforce product endpoint. No ML-KEM in the TLS handshake when your CRM connects to api.salesforce.com.

ServiceNow has partnered with Keyfactor to offer cryptographic posture management integrated into ServiceNow's Vulnerability Response module. This is a discovery and remediation workflow tool. But ServiceNow's own platform endpoints don't negotiate PQC. The tool helps you inventory other people's crypto problems while running on classical TLS itself.

Workday has published nothing on post-quantum cryptography. No blog posts, no roadmap, no product announcements. For a platform that processes payroll, benefits, and HR data for millions of employees, the silence is notable.

Microsoft Teams, Outlook, and Microsoft 365 sit in an interesting position. The SymCrypt library underneath supports ML-KEM and ML-DSA. But the Quantum Safe Program roadmap lists Microsoft 365 services in the third phase. Teams, Outlook, SharePoint, and OneDrive endpoints are not negotiating PQC today. Microsoft's own timeline suggests 2027 at the earliest.

Zoom, Slack, and Dropbox have published nothing — no roadmaps, no acknowledgments, no timelines.

BCG's November 2025 analysis is revealing: it explicitly categorizes "vendor-managed external systems (such as Salesforce, Workday, and Microsoft Teams)" as systems that "can be addressed later," grouping them with "internal noncritical systems (such as HR dashboards and expense tools)." Whether that's the right risk assessment for your organization depends on how long the data in those systems needs to remain confidential.

SaaS / Collaboration Vendor	PQC at Endpoint	PQC Roadmap	HNDL Acknowledged	Status
Salesforce	❌	❌	⚠️ Educational only	No deployment or timeline
ServiceNow	❌	❌ (discovery tool only)	✅ Via Keyfactor	Discovery tool GA; own product classical
Workday	❌	❌	❌	Complete silence
Microsoft 365 (Teams/Outlook)	❌	✅ QSP Phase 3	✅	Platform primitives ready; services ~2027+
Zoom	❌	❌	❌	No announcements
Slack	❌	❌	❌	No announcements

D. Cloud Storage

The HNDL threat is usually discussed in terms of stored data being decrypted later. But there's a more immediate version: every file uploaded to cloud storage over classical TLS is interceptable in transit. A file encrypted at rest with AES-256 on your storage provider's servers is irrelevant to an adversary who captured it during the upload.

Amazon S3 is the notable standout. S3 endpoints have had ML-KEM hybrid PQ-TLS since November 2025. This makes S3 one of the clearest examples of the gap between cloud infrastructure and cloud application providers.

The rest of the field hasn't started. **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+). **Box** has no PQC deployment or timeline.

The one outlier in consumer/SMB storage is **Internxt**, a small European provider claiming to be the first cloud storage with post-quantum encryption alongside zero-knowledge client-side encryption.

Storage Vendor	PQC in Transit	Zero-Knowledge Encryption	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

What the Scorecard Reveals

Four patterns emerge when you map vendor announcements against actual deployment:

Key exchange leads; authentication waits. Every vendor that has shipped PQC has shipped key exchange (ML-KEM) only. Post-quantum digital signatures (ML-DSA) and certificates are not deployed anywhere in production for TLS authentication. The certificate ecosystem — CAs, browsers, PKI infrastructure — is not ready for PQC signatures. This is the right sequence for addressing HNDL, but it means the integrity side of the quantum threat is unaddressed across the board.

The library is ready. The product isn't. Microsoft has ML-KEM and ML-DSA in its core cryptographic library. That's available on every Windows Server and .NET application. But SQL Server doesn't use it. Azure SQL Database doesn't negotiate it. The gap between "available in the crypto library" and "negotiated by your product's TLS stack" can be years. Platform vendors announcing PQC in their foundational libraries are telling the truth — but the products you actually connect to haven't caught up.

Monitoring beats assessment. Point-in-time crypto inventories become stale immediately. What organizations need is continuous monitoring of whether their migration is actually progressing. Are your connections negotiating PQC key exchange this month that they weren't last month? Is a configuration change causing regression? This is the "are you getting better or worse?" question — the one that static assessments can't answer.

Your SaaS vendors control your timeline. For infrastructure you own — servers, networking hardware, databases — you can deploy PQC when the technology is ready. For SaaS, you can't. Your Salesforce connection gets PQC when Salesforce ships it. Your Teams calls get PQC when Microsoft enables it. This is a fundamentally different risk posture, and most organizations haven't accounted for it in their migration planning.

What This Means for PQC Preparedness and Migration

Verify what your vendors claim. Probe your actual connection endpoints. Don't rely on vendor roadmaps or platform-level announcements. The difference between "our crypto library supports ML-KEM" and "your database connection negotiates ML-KEM" is the difference between a marketing claim and actual protection.

Start where PQC is available. Cloud service APIs (especially AWS KMS, S3, and security services), web traffic through modern CDNs, and browser-based applications already benefit from PQC key exchange. Make sure your clients and SDKs are configured to negotiate it.

Watch the infrastructure layer. Networking hardware is where the most varied vendor landscape exists. Fortinet is years ahead of its competitors in shipping NIST-compliant PQC. Cisco and Palo Alto are in the announcement and discovery phases. Juniper's QKD approach is architecturally distinct from what CISA and NIST recommend. Your networking refresh cycle should factor in which vendors actually have PQC in the data path.

Don't wait for your database vendor. Database endpoints are the last to get PQC, even though databases hold the data most worth protecting over long time horizons. Consider proxy-based approaches (like PQ-TLS-capable load balancers) as bridge solutions while database vendors catch up. And pressure your vendors — they need to know that "data platforms in the final phase" is not an acceptable answer for organizations holding data with decades-long sensitivity requirements.

Ask your SaaS vendors the hard question. Your organization almost certainly has sensitive data in Salesforce, Workday, ServiceNow, or Microsoft 365. Ask each vendor: when will your API and web endpoints negotiate ML-KEM? If they can't answer, factor that into your vendor risk assessments. You have no workaround for SaaS — you can't proxy your way to PQC when the endpoint is vendor-controlled.

Treat file transfers as HNDL exposure. Every file uploaded to cloud storage over classical TLS is a potential HNDL target. For your most sensitive documents, consider routing to storage endpoints that already support PQ-TLS (like S3) or applying client-side encryption as a bridge measure.

Track trajectory, not snapshots. A single probe tells you where you are. Repeated probes over time tell you whether you're making progress, standing still, or regressing. The organizations that reach their CNSA 2.0 deadlines will be the ones that treated migration as a continuous measurement problem, not a one-time assessment.

This scorecard should look very different in six months. Vendors are moving, standards are solidifying, and the compliance deadlines are getting closer. The question isn't whether PQC deployment will happen across these categories — it's whether your organization will know when it does.

Sources

1. CISA Tables 2 & 3: “Post-Quantum Cryptography: CISA’s Guidance for Federal Agencies,” CISA.gov
2. NIST FIPS 203/204/205: ML-KEM, ML-DSA, and SLH-DSA standards, published August 2024, NIST.gov
3. CNSA 2.0 / CNSSP-15: NSA Commercial National Security Algorithm Suite 2.0, with 2025/2026/2030/2033/2035 deployment timelines
4. Cloudflare: “State of the post-quantum Internet in 2025,” Cloudflare Blog, October/November 2025
5. F5 Labs: PQC browser adoption analysis (93% Chrome+Firefox vs. 57% with Safari), June 2025
6. AWS: “ML-KEM post-quantum TLS now supported in AWS KMS, ACM, and Secrets Manager,” AWS Security Blog, May 2025; S3 PQ-TLS announcement, Amazon S3 User Guide
7. Google Cloud: “Post-quantum cryptography for Cloud KMS,” Google Cloud documentation
8. Microsoft: “Post-Quantum Cryptography APIs Now Generally Available,” Microsoft Community Hub, November 2025; “Quantum-safe security: Progress towards next-generation cryptography,” Microsoft Security Blog, August 2025
9. Apple: “Prepare your network for quantum-secure encryption in TLS,” Apple Support; macOS Tahoe 26 released September 2025
10. Fortinet: “Fortinet Advances Quantum-Safe Security,” Fortinet Newsroom, July 22, 2025; FortiOS 7.6 New Features Guide
11. Cisco: “Facing the Quantum Threat: Cisco’s Strategic Approach to PQC,” Cisco Blogs, February 5, 2026
12. Palo Alto Networks: “Quantum-Safe Security” product page, Quantum Security Dashboard GA January 2026
13. Juniper Networks: Quantum Key Distribution partnerships and documentation
14. MongoDB: “Advancing Encryption in MongoDB Atlas,” MongoDB Blog, March 2025
15. BCG: “How Quantum Computing Will Upend Cybersecurity,” BCG Publications, November 12, 2025
16. EU PQC Roadmap: “Strengthening the EU Transition to a Quantum-Safe World,” CEPS Task Force Report, December 2025
17. Europol / FS-ISAC: Second Joint Report on PQC, migration prioritization guidelines

Appendix A: Vendor PQC Readiness Questions

Use these questions in procurement reviews, vendor risk assessments, and contract renewals. Each targets a specific gap identified in this scorecard.

#	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. Separates marketing from measurable reality.	Any vendor claiming PQC readiness.
2	**Cryptographic Bill of Materials.** Can you provide a CBOM 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. A vendor who can't inventory it can't migrate it.	Infrastructure, PaaS, and any vendor handling 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 the vendor to reason about data longevity, not just current-state encryption.	SaaS vendors holding long-lived data: HR, financial, healthcare, legal.
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?	Signals you're looking beyond key exchange toward full post-quantum authentication.	Cloud providers, identity/SSO vendors, certificate authorities.
5	**Migration Control.** Can we toggle PQC security policies via configuration, or are we locked into your global migration timeline?	Determines whether you're a pilot or a passenger in your own migration.	Databases, PaaS, any service where you manage TLS or connection policies.

This scorecard is meant to be updated quarterly.

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