[PQ]probe

PQPROBE.COM/SCORECARD

PQC Vendor Scorecard

Q3 2026 edition

MEASURED ON THEIR HOSTS

15 of 35

measured vendor products negotiate ML-KEM by default on every customer-facing host scanned. 27 negotiate it on at least one host.

Ottenheimer GmbH Published 5 November 2026
CC BY 4.0

Contents

Key findings	2
Results by category	4
Transitions observed	10
Movement since Q2	10
Regulatory dates	11
Population	12
Method and definitions	15
Sources	17
About this report	21

Key findings

11 measured products carry vendor material saying post-quantum key exchange is deployed. 9 of them negotiate ML-KEM by default on every host scanned.

MEASURED
35
of 53 products, on their customer-facing hosts

BY DEFAULT EVERYWHERE
15
negotiate ML-KEM by default on every host

ON SOME HOST
27
negotiate it on at least one host

SAYS DEPLOYED
9 of 11
whose material says deployed negotiate it by default on every host

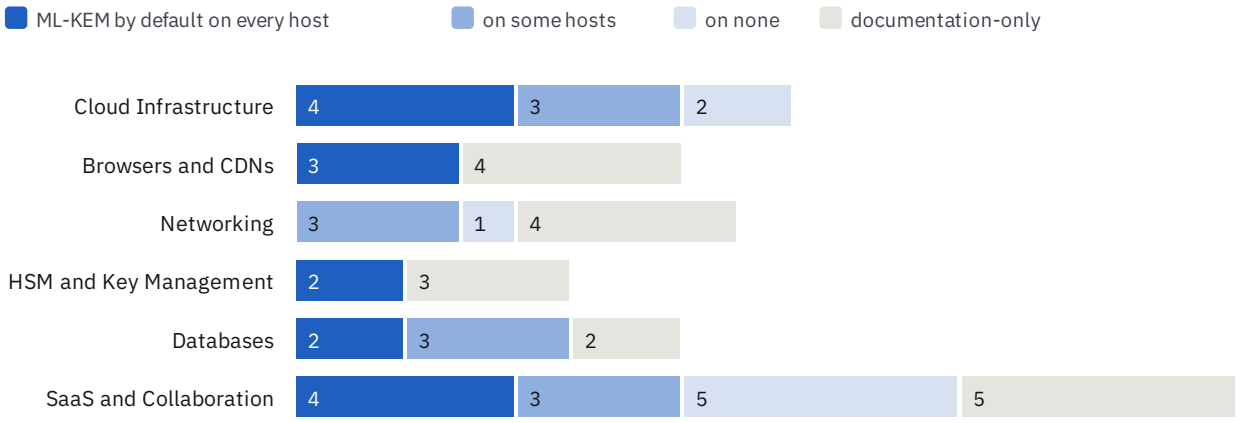
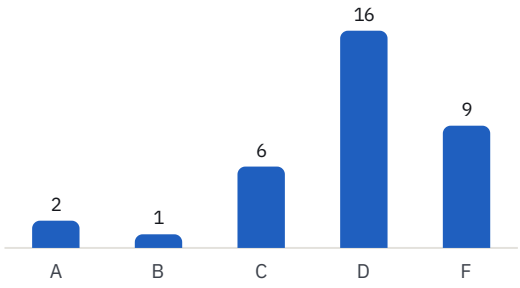


FIGURE 1 Measured products by where ML-KEM is negotiated by default, per category, with the documentation-only products beside.

The scorecard reads 53 vendor products in six categories. 35 are measured on their customer-facing hosts, 123 hosts in all, scanned once a day from a single vantage point on the public internet; 18 are read from vendor documentation alone and marked not measured.

Of the measured products, 15 use ML-KEM by default on every host and 27 on at least one. Across all 53 products, the vendor material reads deployed for 18, available for 9 and announced for 10; 16 have no dated material.

2 products read available although their vendor material says deployed, because their hosts negotiate a classical group by default; the movement table reads them on that effective status.



1 product without a grade: a host did not answer in the window

FIGURE 2 Measured products by grade. A product carries the worst grade across its hosts.

The measured picture is one key exchange group and nothing else. Every post-quantum negotiation in the cohort is X25519MLKEM768. No host negotiates another post-quantum group by default, and no host presented a post-quantum certificate: every leaf certificate is signed with RSA or ECDSA. Twelve products negotiate it on some hosts and not others; the hosts that do not are most often mail hosts and API endpoints. Seven products still accept the pre-standard X25519Kyber768Draft00 on request beside the standard group.

The grade is set by the weakest thing a host still offers. Nine products read F because at least one host still accepts TLS 1.0, TLS 1.1 or a 3DES cipher suite; six of those nine negotiate ML-KEM by default on every host. Google's endpoints, Cloudflare's WARP client API, Signal's storage and CDN hosts, Fortinet's FortiGuard services, Apple's

iCloud Mail exchangers and Tuta's mail exchanger are in that group. A post-quantum key exchange does not raise a grade that a 3DES suite or a protocol version superseded in 2008 holds down.

The vendors whose material says least are not the ones furthest behind. Proton Mail, with no vendor material on its transport, negotiates ML-KEM by default on all five hosts, including both mail exchangers, and reads A on every one. Zoom, Signal's service hosts, Juniper Mist and Google's mail hosts negotiate it on every host that answered, with no vendor statement naming the endpoints. Microsoft 365, Salesforce, Slack, Box, Dropbox and SAP's Cloud Foundry hosts negotiate classical groups on every host.

Results by category

Cloud Infrastructure

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2025	Since Q2
AWS core services (STS, EC2, SES)	available (material: deployed, not by default)	X25519MLKEM768, x25519 / SecP256r1MLKEM768, X25519MLKEM768 (not by default on every host)	SHA256-RSA	none	own	D	measured since 2026-10-29	no	missed	new
Amazon S3	deployed	X25519MLKEM768 / SecP256r1MLKEM768, X25519MLKEM768	SHA256-RSA	none	own	D	ML-KEM negotiated on every scan since measurement began, 2026-10-29	no	met	▷
Azure core services (Resource Manager, Entra ID, Communication Services)	announced	X25519MLKEM768, secp384r1, secp521r1 / SecP256r1MLKEM768, X25519MLKEM768 (not by default on every host)	SHA384-RSA	none	own	D	measured since 2026-06-18; portal.azure.com first post-quantum 2026-09-04, last classical 2026-09-19	no	missed	new
Google Cloud core services (Compute, IAM, Cloud Storage)	deployed	X25519MLKEM768 / X25519MLKEM768	ECDSA-SHA256	TLS_RSA_WITH_3DES_EDE_CBC_SHA	own	F	ML-KEM negotiated on every scan since measurement began, 2026-06-18	no	met	new
Google Workspace (Drive and APIs)	deployed	X25519MLKEM768 / X25519MLKEM768	ECDSA-SHA256	TLS_RSA_WITH_3DES_EDE_CBC_SHA	own	F	ML-KEM negotiated on every scan since measurement began, 2026-10-29	no	met	▲
Google Workspace (Gmail mail hosts)	none	X25519MLKEM768 / X25519MLKEM768	ECDSA-SHA256	TLS 1.0, TLS_RSA_WITH_3DES_EDE_CBC_SHA	own	F	ML-KEM negotiated on every scan since measurement began, 2026-09-12	no	met	▷
Dropbox	none	x25519 / none	ECDSA-SHA384	none	own	D	measured since 2026-10-29	no	missed	▷
Box	none	x25519 / none	SHA256-RSA	none	hosted: Google	C	measured since 2026-06-18	no	missed	▷
Internxt Drive	available (material: deployed, not by default)	X25519MLKEM768, x25519 / X25519Kyber768Draft00, X25519MLKEM768 (not by default on every host)	ECDSA-SHA256, SHA256-RSA	none	hosted: Cloudflare, hosted: OVH	D	measured since 2026-10-29	no	missed	▼

AWS negotiates ML-KEM by default on STS, EC2, every S3 endpoint and KMS, with SecP256r1MLKEM768 accepted on request. The SES submission host is the one AWS endpoint in the population that negotiates x25519, which is why AWS core services read available while the material says deployed. Google negotiates ML-KEM on every Cloud, Workspace and Gmail host, including the MX and the SMTP relay, and reads F on all of them because every Google host still accepts TLS 1.0, TLS 1.1 and, on most, a 3DES suite. Microsoft's Azure hosts negotiate classical groups except the portal, which moved to ML-KEM in September. Dropbox and Box negotiate classical groups on every host and accept no post-quantum group on request. Internxt negotiates ML-KEM on its gateway and drive hosts and x25519 on its API host, which still negotiates TLS 1.2 only.

Browsers and CDNs

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2025	Since Q2
Cloudflare edge, API, WARP and Tunnel	deployed	X25519MLKEM768 / X25519Kyber768Draft00, X25519MLKEM768	ECDSA-SHA256, ECDSA-SHA384	TLS 1.0, none	own	F	ML-KEM negotiated on every scan since measurement began, 2026-06-18	no	met	▷
Akamai edge and control	deployed	X25519MLKEM768 / X25519MLKEM768	ECDSA-SHA384, SHA256-RSA	none	edge: Akamai	A	measured since 2026-06-18; control.akamai.com first post-quantum 2026-07-26, last classical 2026-08-02	no	met	▷
Fastly edge and API	deployed	X25519MLKEM768 / X25519MLKEM768	SHA256-RSA	none	edge: Fastly	D	ML-KEM negotiated on every scan since measurement began, 2026-10-29	no	met	new
Chrome	deployed	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Safari	deployed	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Firefox	deployed	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Edge	deployed	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	new

All three edges negotiate ML-KEM by default on every host. Cloudflare's five hosts include the Tunnel endpoint on port 7844 and the WARP client API; the client API still accepts TLS 1.0 and reads F. Akamai reads A on both hosts. Fastly reads C and D on RSA-signed certificates. The four browsers are read from release notes only: Chrome, Firefox and Edge enable the hybrid group by default, and Apple's platform statement covers Safari on iOS 26 and macOS 26.

Networking

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2026	Since Q2
FortiGate and FortiWeb (FortiOS)	available	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Fortinet cloud services (FortiCloud, FortiGuard, FortiToken Cloud)	none	secp256r1, x25519 / none	SHA256-RSA	TLS 1.0, TLS_RSA_WITH_3DES_EDE_CBC_SHA, none	hosted: CenturyLink Communications, hosted: NTT America, own	F	measured since 2026-10-29	no	missed	new
PAN-OS firewalls	available	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Prisma Access, SASE and WildFire services	announced	X25519MLKEM768, secp256r1, x25519 / X25519MLKEM768 (not by default on every host)	SHA256-RSA, SHA384-RSA	none	hosted: Amazon, hosted: Google	D	measured since 2026-06-18	no	missed	new
Secure Firewall (FTD, ASA)	announced	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2026	Since Q2
Cisco cloud services (Meraki, Umbrella, Webex)	announced	X25519MLKEM768, x25519 / SecP256r1MLKEM768, SecP384r1MLKEM1024, X25519Kyber768Draft00, X25519MLKEM768 (not by default on every host)	SHA256-RSA	none	edge: Amazon CloudFront, edge: Cloudflare, hosted: Meraki, own	C	measured since 2026-10-29	no	missed	new
Junos routers and firewalls	none	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Juniper Mist cloud	none	X25519MLKEM768 / SecP256r1MLKEM768, SecP384r1MLKEM1024, X25519MLKEM768 (not by default on every host)	SHA256-RSA	none	hosted: Amazon	no grade: oc-term.mistsys.net did not answer in the window	measured since 2026-10-29	no	no scan	new

The appliance rows are documentation-only: Fortinet and Palo Alto ship ML-KEM in firmware a customer enables, Cisco has dated targets for FTD 10.5 and ASA 9.25, and Junos documents RFC 8784 pre-shared keys, which are not NIST post-quantum cryptography. On the vendors' own services the picture is mixed. Juniper Mist negotiates ML-KEM on its API, console and device-connect host, with SecP384r1MLKEM1024 accepted on the API; its second device-connect host did not answer a plain TLS connection in the window, so the product carries no grade. Palo Alto's SASE API and WildFire negotiate ML-KEM, Prisma Access's API and the app portal do not. Cisco's Meraki API and Webex negotiate ML-KEM; the Meraki dashboard accepts SecP384r1MLKEM1024 on request but negotiates x25519 by default; Umbrella's dashboard and resolver negotiate classical groups. Fortinet's cloud services negotiate classical groups on every host, the FortiGuard update service still accepts a 3DES suite, and the FortiGuard query service still accepts TLS 1.0 and 1.1.

HSM and Key Management

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2025	Since Q2
Luna HSM	available	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
nShield HSM	available	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
AWS KMS	deployed	X25519MLKEM768 / SecP256r1MLKEM768, SecP384r1MLKEM1024, X25519MLKEM768	SHA256-RSA	none	own	B	ML-KEM negotiated on every scan since measurement began, 2026-10-29	no	met	▷
Google Cloud KMS	deployed	X25519MLKEM768 / X25519MLKEM768	ECDSA-SHA256	TLS_RSA_WITH_3DES_EDE_CBC_SHA	own	F	ML-KEM negotiated on every scan since measurement began, 2026-10-29	no	met	▲
Azure Key Vault and Managed HSM	none	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷

AWS KMS negotiates ML-KEM on its standard and FIPS endpoints in both regions, with SecP384r1MLKEM1024 accepted on the FIPS endpoint, and reads A and B. Google Cloud KMS negotiates ML-KEM and reads F for the same TLS 1.0 and 3DES offering as the rest of Google's hosts. Thales Luna ships ML-KEM and ML-DSA, and Entrust nShield ML-KEM, ML-DSA and SLH-DSA, in firmware a customer installs and enables; by both vendors' own release notes, the firmware that carries them is not the FIPS 140-3 validated firmware. Azure Key Vault and Managed HSM have no Microsoft material naming a post-quantum key type or a date.

Databases

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2025	Since Q2
SQL Server and Azure SQL	none	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Amazon DynamoDB	deployed	X25519MLKEM768 / SecP256r1MLKEM768, SecP384r1MLKEM1024, X25519MLKEM768	SHA256-RSA	none	own	D	ML-KEM negotiated on every scan since measurement began, 2026-10-29	yes	met	▷
Amazon RDS and Aurora	available	X25519MLKEM768 / SecP256r1MLKEM768, X25519MLKEM768	SHA256-RSA	none	own	D	ML-KEM negotiated on every scan since measurement began, 2026-10-29	no	met	▲
MongoDB Atlas	none	X25519MLKEM768, x25519 / SecP256r1MLKEM768, SecP384r1MLKEM1024, X25519MLKEM768 (not by default on every host)	SHA256-RSA	none	hosted: Amazon, own	D	measured since 2026-10-29	no	missed	▷
Managed PostgreSQL	available	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▲
Snowflake	none	X25519MLKEM768, x25519 / X25519Kyber768Draft00, X25519MLKEM768 (not by default on every host)	ECDSA-SHA256, SHA256-RSA	none	hosted: Amazon, hosted: Cloudflare	C	measured since 2026-06-18	no	missed	▷
Oracle Database 26ai and OCI	available	X25519MLKEM768, secp256r1, x25519 / SecP256r1MLKEM768, SecP384r1MLKEM1024, X25519MLKEM768 (not by default on every host)	ECDSA-SHA384, SHA256-RSA	none	edge: Akamai, own	C	measured since 2026-06-18; cloud.oracle.com first post-quantum 2026-07-21, last classical 2026-08-04	no	missed	new

DynamoDB's endpoint negotiates ML-KEM by default and is the one product in the cohort whose every host accepts SecP384r1MLKEM1024 on request. The RDS control plane negotiates it too; the RDS and Aurora data planes are per-instance and read from AWS's material, which makes the hybrid group an opt-in on PostgreSQL 18 and MySQL 8.4. MongoDB Atlas's three cluster hosts on port 27017 negotiate ML-KEM by default and accept all three hybrid groups; the Atlas control plane negotiates x25519. Oracle's identity and IaaS endpoints and the console negotiate ML-KEM, the Autonomous Database endpoint and the OCI email submission host do not. Snowflake's web application negotiates ML-KEM; the trial account's data plane negotiates x25519. The managed PostgreSQL row is read from vendor material: RDS for PostgreSQL 18 allows the hybrid groups when a customer sets them; Azure Database for PostgreSQL and Google Cloud SQL document nothing. No Microsoft material names SQL Server or Azure SQL.

SaaS and Collaboration

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2025	Since Q2
Salesforce platform	announced	x25519 / none	SHA256-RSA	none	hosted: Amazon	D	measured since 2026-06-18	no	missed	▷

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2025	Since Q2
Now Platform	announced	X25519MLKEM768 / X25519MLKEM768	ECDSA-SHA384	none	own	D	measured since 2026-06-18; signon.service-now.com moved to post-quantum between 2026-08-22 and 2026-08-23	no	met	▷
Workday	announced	X25519MLKEM768, x25519 / X25519Kyber768Draft00, X25519MLKEM768 (not by default on every host)	ECDSA-SHA384, SHA256-RSA	none	own	D	measured since 2026-10-29	no	missed	▷
Slack	none	x25519 / none	SHA256-RSA	none	hosted: Amazon	C	measured since 2026-10-02	no	missed	▷
Microsoft 365 (Exchange Online, Teams, SharePoint)	announced	secp384r1, secp521r1 / none	SHA256-RSA, SHA384-RSA	none	own	D	measured since 2026-10-29	no	missed	▷
Zoom end-to-end encryption	available	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Zoom meetings service	none	X25519MLKEM768 / X25519Kyber768Draft00, X25519MLKEM768	SHA256-RSA	none	hosted: Cloudflare	D	measured since 2026-06-18	no	met	new
Signal protocol (PQXDH)	deployed	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Signal service	none	X25519MLKEM768 / X25519Kyber768Draft00, X25519MLKEM768	SHA256-RSA	TLS 1.0, TLS_RSA_WITH_3DES_EDE_CBC_SHA, none	hosted: Amazon, hosted: Cloudflare, hosted: Google	F	ML-KEM negotiated on every scan since measurement began, 2026-10-29	no	met	new
iMessage (PQ3)	deployed	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	▷
Apple push, identity and iCloud Mail	announced	X25519MLKEM768, x25519 / X25519MLKEM768 (not by default on every host)	SHA256-RSA	TLS 1.0, none	edge: Akamai, own	F	measured since 2026-10-29	no	missed	new
SAP Business Technology Platform (Cloud Foundry)	announced	x25519 / none	SHA256-RSA	none	edge: Akamai, hosted: Amazon	C	measured since 2026-10-29	no	missed	new
Tuta Mail service	none	secp256r1, x25519 / none	ECDSA-SHA256, ECDSA-SHA384	TLS 1.0, none	own	F	measured since 2026-06-09	no	missed	new
TutaCrypt end-to-end encryption	deployed	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	new
mailbox.org mail service	none	X25519MLKEM768, x25519 / SecP256r1MLKEM768, SecP384r1MLKEM1024, X25519MLKEM768 (not by default on every host)	SHA256-RSA	none	hosted: Heinlein Support	D	measured since 2026-06-18	no	missed	new

Product	Status	Negotiated by default / supported on request	Certificate signature	Weakest offered	Serving	Grade	History	ML-KEM-1024 hybrid accepted	PQ by default vs CNSA class year 2025	Since Q2
Proton Mail service	none	X25519MLKEM768 / SecP256r1MLKEM768, X25519MLKEM768	SHA256-RSA	none	own	A	measured since 2026-06-09; mail.proton.me moved to post-quantum between 2026-09-17 and 2026-09-18	no	met	new
Post-quantum OpenPGP end-to-end encryption	available	not measured	not measured	not measured	not measured	not measured	not measured	not measured	not measured	new

Proton Mail negotiates ML-KEM by default on its sign-in, webmail, API and both mail exchangers and reads A on all five hosts, with no vendor material on the transport. Zoom's three service hosts and Signal's three service hosts negotiate ML-KEM; two of Signal's still accept TLS 1.0 and read F. Workday negotiates ML-KEM on four of five hosts and x25519 on its API host. ServiceNow's sign-in host negotiates ML-KEM. Microsoft 365 negotiates classical groups on all six hosts, Exchange Online's MX and submission included. Salesforce, Slack and SAP's Cloud Foundry hosts negotiate classical groups on every host and accept no post-quantum group on request. Apple's identity host negotiates ML-KEM; its push host, iCloud Mail's IMAP and submission hosts and all three mail exchangers negotiate x25519, and the exchangers still accept TLS 1.0. mailbox.org's two mail exchangers and submission host negotiate ML-KEM; its sign-in, webmail and IMAP hosts do not. Tuta's app host negotiates secp256r1 and its mail exchanger x25519 with TLS 1.0 still accepted. The end-to-end rows, TutaCrypt, Proton's post-quantum OpenPGP, Signal's PQXDH, iMessage's PQ3 and Zoom's end-to-end encryption, state each vendor's description of its own protocol; the scorecard does not assess key custody or verify the protocol.

Transitions observed

The daily series shows the hosts in the population that moved from classical to post-quantum key exchange during the measurement period, which began in June 2026 for hosts shared with the scanner's other cohorts and on 29 October 2026 for the rest. A host whose last classical reading is after its first post-quantum reading alternated between the two for that interval.

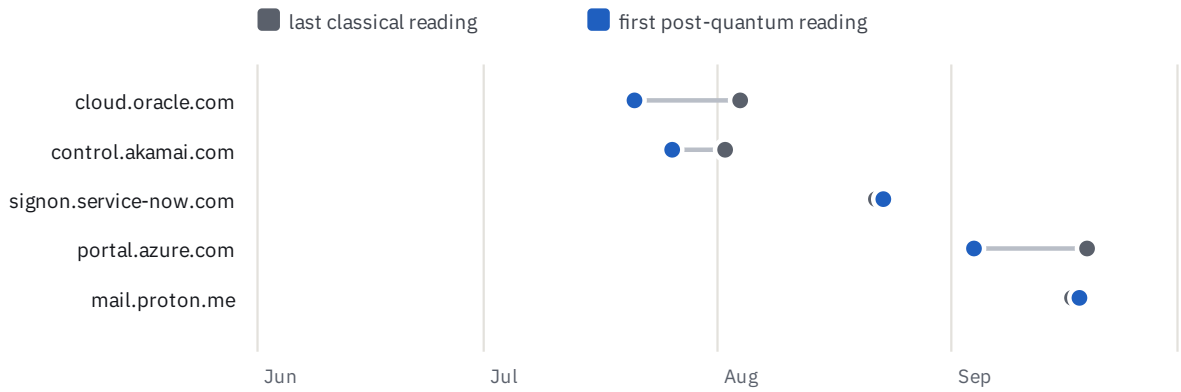


FIGURE 3 Hosts with a classical reading and a post-quantum reading after measurement began.

Host	Product	First post-quantum reading	Last classical reading
cloud.oracle.com:443	Oracle Database 26ai and OCI	2026-07-21	2026-08-04
control.akamai.com:443	Akamai edge and control	2026-07-26	2026-08-02
signon.service-now.com:443	Now Platform	2026-08-23	2026-08-22
portal.azure.com:443	Azure core services (Resource Manager, Entra ID, Communication Services)	2026-09-04	2026-09-19
mail.proton.me:443	Proton Mail service	2026-09-18	2026-09-17

Movement since Q2

Product	Q2 status	Q3 status	Movement	Material
Google Workspace (Drive and APIs)	none	deployed	▲	2026-08-12
Internxt Drive	deployed	available	▼	2025-01-17
Google Cloud KMS	available	deployed	▲	2026-08-12
Amazon RDS and Aurora	none	available	▲	2026-09-24
Managed PostgreSQL	none	available	▲	2026-09-24

19 products are new to this edition: AWS core services (STS, EC2, SES), Azure core services (Resource Manager, Entra ID, Communication Services), Google Cloud core services (Compute, IAM, Cloud Storage), Fastly edge and API, Edge, Fortinet cloud services (FortiCloud, FortiGuard, FortiToken Cloud), Prisma Access, SASE and WildFire services, Cisco cloud services (Meraki, Umbrella, Webex), Juniper Mist cloud, Oracle Database 26ai and OCI, Zoom meetings service, Signal service, Apple push, identity and iCloud Mail, SAP Business Technology Platform (Cloud Foundry), Tuta Mail service, TutaCrypt end-to-end encryption, mailbox.org mail service, Proton Mail service, Post-quantum OpenPGP end-to-end encryption.

Measured against the Q2 edition's corrected statuses, three products improved and one degraded on the effective status. Google Workspace and Google Cloud KMS moved to deployed on Google's August statement and negotiate ML-KEM on every host. RDS and Aurora moved to available on the PostgreSQL 18 announcement. Internxt reads

available because its API host negotiates x25519, although its material says deployed. Of the sixteen measured products new to this edition, Google Cloud, Fastly, Zoom, Signal, Juniper Mist and Proton Mail negotiate ML-KEM by default on every host that answered; Fortinet's cloud services, SAP Business Technology Platform and Tuta's mail hosts negotiate it on none; the other seven negotiate it on some hosts.

Regulatory dates

Authority	Date	Requirement	Source
United States, Executive Order 14412	22 June 2026	Key establishment on federal high-value and high-impact systems by the end of 2030; digital signatures and authentication by the end of 2031.	Securing the Nation Against Advanced Cryptographic Attacks
NSA, CNSA 2.0 and CNSSP 15	CNSSP 15; stated in NSA's FAQ Ver. 2.2, October 2026	CNSA 2.0 in all new acquisitions for National Security Systems by 1 January 2027; equipment and services that cannot support it phased out by 31 December 2030 unless otherwise granted an exception; CNSA 2.0 mandated for use, unless otherwise noted, by 31 December 2031.	Commercial National Security Algorithm Suite 2.0 and Quantum Computing Frequently Asked Questions (NSA, Ver. 2.2); NSA Announces Post-Quantum Cryptography Measures to Safeguard National Security Systems Against Quantum Computing Threats
France, ANSSI	FAQ, undated; position papers 4 January 2022 and 11 October 2023	ANSSI aims at PQC obligations for products entering qualification from 2027. Hybridisation is mandatory in the regulated scope, hash-based signatures excepted.	FAQ cryptographie post-quantique (ANSSI); ANSSI views on the post-quantum cryptography transition; Follow up position paper on post-quantum cryptography
Germany, BSI TR-02102-1	23 January 2026	Sole use of classical key agreement is recommended only until the end of 2031, the end of 2030 for very high protection requirements; classical signatures until the end of 2035.	BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths
European Union	20 January 2026; 11 June 2025	COM(2026) 13 proposes amending NIS2 so that Member States adopt policies for the transition to post-quantum cryptography in their national cybersecurity strategies. The NIS Cooperation Group roadmap of 11 June 2025 recommends completing high-risk use cases by the end of 2030 and medium-risk by the end of 2035.	Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act; A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, Version 1.1 (NIS Cooperation Group)
NSA, CNSA 2.0 equipment classes	September 2022	Support and prefer CNSA 2.0, then use it exclusively: web browsers, servers and cloud services 2025 and 2033; traditional networking equipment 2026 and 2030; operating systems 2027 and 2033; software and firmware signing 2025 and 2030.	Announcing the Commercial National Security Algorithm Suite 2.0 (Cybersecurity Advisory PP-22-1338, Ver. 1.0)
NIST CMVP	21 September 2026; 21 January 2026	FIPS 140-2 certificates move to historical status on 21 September 2026. The average of the last 30 FIPS 140-3 validations is 348 days.	FIPS 140-3 Transition Effort; Cryptographic Module Validation Program (CMVP) Status and Future Plans (David Hawes, NIST)

Population

The population is the Q2 edition's vendor set with Oracle Database and SAP Business Technology Platform added. A host is in a product's row when a paying customer's data or credentials cross it in normal use of that product: sign-in, API, data plane, mail for mail products, tunnel and client-connect endpoints. Marketing sites, documentation, support portals, status pages and corporate mail are not. Where a product has no such host, as with browsers, appliances and end-to-end protocol layers, it is documentation-only.

Cloud Infrastructure

Product	Hosts	Status	Material
Amazon Web Services: AWS core services (STS, EC2, SES)	sts.amazonaws.com, ec2.us-east-1.amazonaws.com, email-smtp.us-east-1.amazonaws.com:587	deployed	2026-04
Amazon Web Services: Amazon S3	s3.us-east-1.amazonaws.com, s3.amazonaws.com, s3.eu-central-1.amazonaws.com	deployed	2025-11-19
Microsoft: Azure core services (Resource Manager, Entra ID, Communication Services)	management.azure.com, login.microsoftonline.com, portal.azure.com, smtp.azurecomm.net:587	announced	2025-08-20
Google: Google Cloud core services (Compute, IAM, Cloud Storage)	compute.googleapis.com, oauth2.googleapis.com, storage.googleapis.com, console.cloud.google.com	deployed	2026-08-12
Google: Google Workspace (Drive and APIs)	www.googleapis.com, drive.google.com	deployed	2026-08-12
Google: Google Workspace (Gmail mail hosts)	imap.gmail.com:993, aspmx.l.google.com:25, smtp-relay.gmail.com:587	none	2026-10-26
Dropbox: Dropbox	api.dropboxapi.com, content.dropboxapi.com, www.dropbox.com	none	2024-06-05
Box: Box	api.box.com, upload.box.com, app.box.com	none	—
Internxt: Internxt Drive	gateway.internxt.com, api.internxt.com, drive.internxt.com	deployed	2025-01-17

Browsers and CDNs

Product	Hosts	Status	Material
Cloudflare: Cloudflare edge, API, WARP and Tunnel	api.cloudflare.com, dash.cloudflare.com, api.cloudflareclient.com, region1.v2.argotunnel.com:7844, www.cloudflare.com	deployed	2026-07-03
Akamai: Akamai edge and control	control.akamai.com, www.akamai.com	deployed	2026-10-28
Fastly: Fastly edge and API	api.fastly.com, manage.fastly.com, www.fastly.com	deployed	2025-04-02
Google: Chrome	documentation-only	deployed	2024-09-13
Apple: Safari	documentation-only	deployed	2026-06-18
Mozilla: Firefox	documentation-only	deployed	2026-10-29
Microsoft: Edge	documentation-only	deployed	2026-05-20

Networking

Product	Hosts	Status	Material
Fortinet: FortiGate and FortiWeb (FortiOS)	documentation-only	available (opt-in)	2025-07-22
Fortinet: Fortinet cloud services (FortiCloud, FortiGuard, FortiToken Cloud)	customerapiauth.fortinet.com, fortigate.forticloud.com, ftc.fortinet.com, update.fortiguard.net, service.fortiguard.net	none	—

Product	Hosts	Status	Material
Palo Alto Networks: PAN-OS firewalls	documentation-only	available (opt-in)	2026-07-20
Palo Alto Networks: Prisma Access, SASE and WildFire services	api.sase.paloaltonetworks.com, api.prismaaccess.com, apps.paloaltonetworks.com, wildfire.paloaltonetworks.com	announced	2026-03
Cisco: Secure Firewall (FTD, ASA)	documentation-only	announced	2026-04-13
Cisco: Cisco cloud services (Meraki, Umbrella, Webex)	api.meraki.com, dashboard.meraki.com, dashboard.umbrella.com, doh.umbrella.com, web.webex.com	announced	2026-07-14
Juniper Networks / HPE: Junos routers and firewalls	documentation-only	none	—
Juniper Networks / HPE: Juniper Mist cloud	api.mist.com, manage.mist.com, ep-terminator.mistsys.net, oc-term.mistsys.net	none	—

HSM and Key Management

Product	Hosts	Status	Material
Thales: Luna HSM	documentation-only	available (opt-in)	2026-07-24
Entrust: nShield HSM	documentation-only	available (opt-in)	2025-08-22
Amazon Web Services: AWS KMS	kms.us-east-1.amazonaws.com, kms-fips.us-east-1.amazonaws.com, kms.eu-central-1.amazonaws.com	deployed	2025-04-07
Google: Google Cloud KMS	cloudkms.googleapis.com	deployed	2026-08-12
Microsoft: Azure Key Vault and Managed HSM	documentation-only	none	2026-05-21

Databases

Product	Hosts	Status	Material
Microsoft: SQL Server and Azure SQL	documentation-only	none	—
Amazon Web Services: Amazon DynamoDB	dynamodb.us-east-1.amazonaws.com	deployed	2026-10-28
Amazon Web Services: Amazon RDS and Aurora	rds.us-east-1.amazonaws.com	available (opt-in)	2026-09-24
MongoDB: MongoDB Atlas	ac-4fecwcj-shard-00-00.dsbyabj.mongodb.net:27017, ac-4fecwcj-shard-00-01.dsbyabj.mongodb.net:27017, ac-4fecwcj-shard-00-02.dsbyabj.mongodb.net:27017, cloud.mongodb.com	none	—
Various: Managed PostgreSQL	documentation-only	available (opt-in)	2026-09-24
Snowflake: Snowflake	oaewtcd-fl05769.snowflakecomputing.com:443, app.snowflake.com	none	—
Oracle: Oracle Database 26ai and OCI	adb.us-ashburn-1.oraclecloud.com, iaas.us-ashburn-1.oraclecloud.com, identity.us-ashburn-1.oraclecloud.com, cloud.oracle.com, smtp.email.us-ashburn-1.oci.oraclecloud.com:587	available (opt-in)	2026-03

SaaS and Collaboration

Product	Hosts	Status	Material
Salesforce: Salesforce platform	login.salesforce.com, api.salesforce.com, test.salesforce.com	announced	2026-03-18
ServiceNow: Now Platform	signon.service-now.com	announced	2026-06-01

Product	Hosts	Status	Material
Workday: Workday	services1.myworkday.com, impl.workday.com, wd5.myworkday.com, wd3.myworkday.com, www.myworkday.com	announced	2026-06-22
Slack: Slack	api.slack.com, app.slack.com, slack.com, wss-primary.slack.com	none	—
Microsoft: Microsoft 365 (Exchange Online, Teams, SharePoint)	graph.microsoft.com, outlook.office365.com, outlook.office365.com:993, teams.microsoft.com, microsoft-com.mail.protection.outlook.com:25, smtp.office365.com:587	announced	2025-08-20
Zoom: Zoom end-to-end encryption	documentation-only	available (opt-in)	2024-05-21
Zoom: Zoom meetings service	api.zoom.us, zoom.us, us02web.zoom.us	none	—
Signal: Signal protocol (PQXDH)	documentation-only	deployed	2025-10-02
Signal: Signal service	chat.signal.org, storage.signal.org, cdn2.signal.org	none	—
Apple: iMessage (PQ3)	documentation-only	deployed	2026-01-28
Apple: Apple push, identity and iCloud Mail	api.push.apple.com, appleid.apple.com, imap.mail.me.com:993, smtp.mail.me.com:587, mx-in.g.apple.com:25, mx-in-hfd.apple.com:25, mx-in-ma.apple.com:25	announced	2025-06
SAP: SAP Business Technology Platform (Cloud Foundry)	api.cf.eu10.hana.ondemand.com, login.cf.eu10.hana.ondemand.com, api.cf.us10.hana.ondemand.com, cockpit.btp.cloud.sap, accounts.sap.com	announced	2026-07-13
Tuta: Tuta Mail service	app.tuta.com, mail.tutanota.de:25	none	—
Tuta: TutaCrypt end-to-end encryption	documentation-only	deployed	2026-08-26
mailbox.org: mailbox.org mail service	login.mailbox.org, office.mailbox.org, mx1.mailbox.org:25, mx2.mailbox.org:25, imap.mailbox.org:993, smtp.mailbox.org:587	none	—
Proton: Proton Mail service	account.proton.me, mail.proton.me, mail-api.proton.me, mail.protonmail.ch:25, mailsec.protonmail.ch:25	none	—
Proton: Post-quantum OpenPGP end-to-end encryption	documentation-only	available (opt-in)	2026-05-05

Method and definitions

Each product has two independent readings and one grade. The status comes from the vendor's own dated material, with the URL and date given. The measured columns come from the product's hosts: the key exchange group negotiated by default and the post-quantum groups supported on request, the leaf certificate signature algorithm, how each host is served, and the grade, all on the days of the cut. Deployed requires post-quantum key exchange negotiated by default on every host; a product whose material says deployed but whose hosts negotiate a classical group by default reads available, is marked as such, and moves on that reading. The grader and its scale are published; nothing in this report is sponsored or sold.

The cohort is scanned once a day by the production scheduler. This report reads the 5 consecutive daily scans from 30 October 2026 to 3 November 2026. The scanner and the grader were the same across the window. Each host is read at its latest graded scan within the cut. A product's grade is the worst grade across its hosts. Per-host results are product output and are not published; the hostname list is.

Weakest offered names the weakest protocol version or cipher suite a host still offers, by the grader's fatal rules (export, NULL, SSL 2.0 and 3.0, DES and 3DES, RC4, TLS 1.0 and 1.1) and from the same enumeration the grade reads; none where nothing offered is below the grade's threshold. No probe was added for it.

History comes from the scheduler's daily series: measured since, the first scheduler scan of the product's hosts; the first post-quantum reading, the first scan on which a host accepted a post-quantum group by default or on request; and the last classical reading, the last completed scan on which it accepted none. A product post-quantum on every scan since measurement began says so. Hosts added to the cohort for this edition were first scanned late on 29 October 2026, UTC, and read measured since that day; the cut begins with the next day's scan. The default-handshake group has been recorded since 12 September 2026; before that the series carries whether a post-quantum group was accepted.

Serving has three values: a named edge operator, where the edge classifier identifies the TLS terminator from its certificate and DNS delegation; own, where the serving address is announced by the vendor's own autonomous system; and hosted, where it is announced by another named operator's network. A lookup that did not answer reads unclassified, never own.

Movement since the Q2 edition is read on the status scale against the Q2 edition's status, corrected where it rested on no vendor source: ▲ improving, ▷ stable, ⧨ degrading. A product the Q2 edition had no row for is marked new. Where a host sits in more than one cohort of the scheduler it is scanned once a day; the product groups it by this report's hostname list.

The ML-KEM-1024 hybrid accepted column reads yes where every host accepts SecP384r1MLKEM1024 on request. This hybrid carries ML-KEM-1024, the CNSA 2.0 parameter set, but NSA's draft TLS profile for CNSA 2.0 requires ML-KEM-1024 alone; the pure ML-KEM groups are not yet probed.

The column Post-quantum by default, against the CNSA 2.0 class year, headed PQ by default vs CNSA class year in the tables, maps each category to its equipment class in NSA's CNSA 2.0 advisory (PP-22-1338, September 2022, Timing section) and reads each measured product against the class's support-and-prefer year on the publication date: met when every host negotiates a post-quantum group by default, missed when the year has come and one does not, not yet due while it is ahead. The reading is any post-quantum group, not CNSA 2.0's ML-KEM-1024. CNSA 2.0 applies to National Security Systems, and the advisory's years are for those systems. The reading changes nothing in the grade.

Status definitions

deployed: post-quantum key exchange is negotiated on the product's customer-facing hosts with no customer action, and the vendor's material says so.

available: the vendor has shipped post-quantum cryptography in the product, but a customer must configure or opt in, including shipped-but-disabled defaults, previews a customer enrols in, and firmware a customer must install.

announced: a dated public commitment with nothing shipped in the product.

none: no dated vendor material naming the product. A press article or a third-party tracker is not material.

Sources

1. Securing the Nation Against Advanced Cryptographic Attacks, 2026-06-22. https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/
2. Product Categories for Technologies That Use Post-Quantum Cryptography Standards, 2026-01-23. https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards
3. Module-Lattice-Based Key-Encapsulation Mechanism Standard, 2024-08-13. https://csrc.nist.gov/pubs/fips/203/final
4. Module-Lattice-Based Digital Signature Standard, 2024-08-13. https://csrc.nist.gov/pubs/fips/204/final
5. Stateless Hash-Based Digital Signature Standard, 2024-08-13. https://csrc.nist.gov/pubs/fips/205/final
6. Announcing the Commercial National Security Algorithm Suite 2.0 (Cybersecurity Advisory PP-22-1338, Ver. 1.0), 2022-09-07. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
7. NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems, 2022-09-07. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3148990/
8. Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations, 2026-03-30. https://arxiv.org/abs/2603.28846
9. How to factor 2048 bit RSA integers with less than a million noisy qubits, 2025-05-21. https://arxiv.org/abs/2505.15917
10. State of the post-quantum Internet in 2025, 2025-10-28. https://blog.cloudflare.com/pq-2025/
11. Bringing more transparency to post-quantum usage, encrypted messaging, and routing security, 2026-02-27. https://blog.cloudflare.com/radar-origin-pq-key-transparency-aspa/
12. Post-quantum ML-DSA certificates for Authenticated Origin Pulls and Custom Origin Trust Store, 2026-06-17. https://developers.cloudflare.com/changelog/post/2026-06-17-pqc-mldsa-aop-cots/
13. The White House's post-quantum executive order is an important milestone. It's time to get to work, 2026-06-23. https://blog.cloudflare.com/post-quantum-eo-2026
14. AWS post-quantum cryptography migration plan, 2024-12-05. https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan
15. AWS Post-Quantum Confidentiality Readiness, 2026-04. https://aws.amazon.com/security/post-quantum-cryptography/aws-pq-readiness-confidentiality/
16. AWS Payments Cryptography announces support for post-quantum cryptography to secure data in transit, 2025-11-21. https://aws.amazon.com/about-aws/whats-new/2025/11/aws-payments-cryptography-post-quantum-data-transit
17. Quantum-safe security: Progress towards next-generation cryptography, 2025-08-20. https://www.microsoft.com/en-us/security/blog/2025/08/20/quantum-safe-security-progress-towards-next-generation-cryptography/
18. Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms, 2025-11-18. https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-apis-now-generally-available-on-microsoft-platforms/4469093
19. Accelerating the quantum-safe timeline (Microsoft Security Blog, Mark Russinovich), 2026-06-30. https://www.microsoft.com/en-us/security/blog/2026/06/30/microsoft-advances-quantum-safe-security-as-the-risk-timeline-shifts/
20. Next '26: Redefining security for the AI era with Google Cloud and Wiz, 2026-04-22. https://cloud.google.com/blog/products/identity-security/next26-redefining-security-for-the-ai-era-with-google-cloud-and-wiz
21. Cloud KMS release notes, 2025-09-23. https://docs.cloud.google.com/kms/docs/release-notes
22. Support for hybrid PQC SSL deep inspection in proxy mode. https://docs.fortinet.com/document/fortigate/8.0.0/new-features/771310/support-for-hybrid-pqc-ssl-deep-inspection-in-proxy-mode
23. Fortinet Introduces FortiOS 8.0 to Expand Secure Networking with Secure AI Controls, Fabric-Based AI Agents, Flexible SASE, and Simplified SD-WAN, 2026-03-10. https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2026/fortinet-introduces-fortios-8-expand-secure-networking-with-secure-ai-controls-fabric-based-ai-agents-flexible-sase-and-simplified-sdwan
24. Post-Quantum Cryptography (PQC) Support (8.0.3). https://docs.fortinet.com/document/fortiweb/8.0.3/administration-guide/426552/post-quantum-cryptography-pqc-support-8-0-3
25. Securing the Quantum Age, 2025-08-14. https://www.paloaltonetworks.com/blog/2025/08/securing-the-quantum-age/
26. Support for Post-Quantum Features, 2026-07-20. https://docs.paloaltonetworks.com/network-security/quantum-security/administration/quantum-security-concepts/support-for-quantum-features
27. Preparing for Post-Quantum Cryptography: The Secure Firewall Roadmap, 2026-04-13. https://blogs.cisco.com/security/preparing-for-post-quantum-cryptography-the-secure-firewall-roadmap
28. How to Become Quantum-Ready Today: Luna HSM v7.9 Delivers Real-World PQC, Validated by Thales PKI Technology Partners, 2025-07-29. https://cpl.thalesgroup.com/blog/encryption/luna-hsm-pqc-quantum-safe-encryption
29. Luna HSM Firmware 7.9.0, 2025-07. https://www.thalesdocs.com/gphsm/luna/7/docs/network/Content/CRN/Luna/firmware/7-9-0.htm
30. Luna HSM Firmware 7.9.1, 2025-09. https://www.thalesdocs.com/gphsm/luna/7/docs/network/Content/CRN/Luna/firmware/7-9-1.htm
31. Modules In Process List, 2026-10-29. https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List
32. Entrust nShield HSMs Post-Quantum Cryptography Algorithms Achieve Validation from the NIST Cryptographic Algorithm Validation Program (Entrust press release, Business Wire copy), 2025-09-10. https://www.businesswire.com/news/home/20250910020412/en
33. nShield Security World v13.9.0 release notes (firmware 13.8.0 with ML-DSA, ML-KEM and SLH-DSA), 2025-08-22. https://nshielddocs.entrust.com/

34. Salesforce Post-Quantum Cryptography, 2026-03-18. https://compliance.salesforce.com/documents/a00Kd00000z7HMjIAM

35. ANSSI views on the post-quantum cryptography transition, 2022-01-04. https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition

36. Follow up position paper on post-quantum cryptography, 2023-10-11. https://messervices.cyber.gouv.fr/guides/en-follow-position-paper-post-quantum-cryptography

37. FAQ cryptographie post-quantique (ANSSI). https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/faq-pqc/

38. Post-quantum cryptography (ANSSI). https://cyber.gouv.fr/en/technological-and-cybersecurity-challenges/post-quantum-cryptography/

39. BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2026-01-23. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=21

40. BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths, 2026-01-23. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=15

41. A Post-Quantum Future for Let's Encrypt, 2026-06-03. https://letsencrypt.org/2026/06/03/pq-certs

42. FIPS 140-3 Transition Effort, 2026-04-13. https://csrc.nist.gov/projects/fips-140-3-transition-effort

43. Cryptographic Module Validation Program (CMVP) Status and Future Plans (David Hawes, NIST), 2026-01-21. https://csrc.nist.gov/csrc/media/presentations/2026/cmvp-status-and-future-plans/images-media/1.4-cmvp_status-hawes.pdf

44. The 2025 State of Post-Quantum Cryptography (PQC) on the Web, 2025-06-26. https://www.f5.com/labs/articles/the-state-of-pqc-on-the-web

45. How Quantum Computing Will Upend Cybersecurity, 2025-10-15. https://www.bcg.com/publications/2025/how-quantum-computing-will-upend-cybersecurity

46. Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act, 2026-01-20. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act

47. Strengthening the EU transition to a quantum-safe world. Technology, market, governance and policy challenges, 2025-12. https://cdn.ceps.eu/2025/12/2025-12-Quantum-TF-report-formatted.pdf

48. Amazon Web Services: AWS core services (STS, EC2, SES), further material. https://aws.amazon.com/security/post-quantum-cryptography/

49. Amazon Web Services: AWS core services (STS, EC2, SES), further material. https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan/

50. Amazon S3 now supports post-quantum TLS key exchange on S3 endpoints, 2025-11-19. https://aws.amazon.com/about-aws/whats-new/2025/11/s3-post-quantum-tls-key-exchange-endpoints/

51. Amazon Web Services: Amazon S3, further material. https://docs.aws.amazon.com/AmazonS3/latest/userguide/pqtls-how-to.html

52. Microsoft: Azure core services (Resource Manager, Entra ID, Communication Services), further material. https://www.microsoft.com/en-us/security/blog/2026/07/10/securing-our-future-july-2026-progress-report-on-microsofts-secure-future-initiative/

53. PQC in Plaintext: Google Cloud's post-quantum cryptography roadmap, 2026-08-12. https://cloud.google.com/blog/products/identity-security/pqc-in-plaintext-google-clouds-post-quantum-cryptography-roadmap

54. Google: Google Cloud core services (Compute, IAM, Cloud Storage), further material. https://docs.cloud.google.com/rust/docs/post-quantum-cryptography

55. Google: Google Cloud core services (Compute, IAM, Cloud Storage), further material. https://cloud.google.com/blog/products/identity-security/how-were-helping-customers-prepare-for-a-quantum-safe-future

56. Google: Google Workspace (Drive and APIs), further material. https://workspaceupdates.googleblog.com/2026/10/google-meet-now-uses-post-quantum-cryptography.html

57. Google: Google Workspace (Drive and APIs), further material. https://knowledge.workspace.google.com/admin/gmail/advanced/ciphers-for-gmail-smtp-tls-connections?hl=en

58. Implementing end-to-end encryption for Dropbox teams, 2024-06-05. https://dropbox.tech/security/end-to-end-encryption-for-dropbox-teams

59. Internxt Becomes The First Cloud Storage With Post-Quantum Cryptography, 2025-01-17. https://blog.internxt.com/post-quantum-cryptography/

60. Internxt: Internxt Drive, further material. https://help.internxt.com/en/articles/10522070-what-encryption-does-internxt-use

61. Post-quantum cryptography (PQC), 2026-07-03. https://developers.cloudflare.com/ssl/post-quantum-cryptography/

62. Cloudflare: Cloudflare edge, API, WARP and Tunnel, further material. https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-to-origin/

63. Cloudflare: Cloudflare edge, API, WARP and Tunnel, further material. https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-and-zero-trust/

64. pqcClientToEdge, 2026-10-28. https://techdocs.akamai.com/property-mgr/reference/ga-pqc-client-to-edge

65. Akamai: Akamai edge and control, further material. https://www.akamai.com/blog/security/future-proofing-internet-akamai-achieves-end-to-end-pqc

66. Akamai: Akamai edge and control, further material. https://techdocs.akamai.com/property-mgr/docs/pqc-origin

67. Future-Proofing TLS Encryption Against Quantum Threats, 2025-04-02. https://www.fastly.com/blog/future-proofing-tls-encryption-against-quantum-threats

68. Fastly: Fastly edge and API, further material. https://www.fastly.com/documentation/guides/getting-started/domains/securing-domains/tls-prerequisites-and-limitations/

69. A new path for Kyber on the web, 2024-09-13. https://security.googleblog.com/2024/09/a-new-path-for-kyber-on-web.html

70. Google: Chrome, further material. https://blog.google/chromium/advancing-our-amazing-bet-on-asymmetric/

71. Google: Chrome, further material. https://support.google.com/chrome/a/answer/10314655

72. Prepare your network for quantum-secure encryption in TLS - Apple Support, 2026-06-18. https://support.apple.com/en-us/122756

73. Apple: Safari, further material. https://developer.apple.com/documentation/safari-release-notes/safari-26-release-notes

74. PostQuantumKeyAgreementEnabled | Firefox administrator reference, 2026-10-29. https://firefox-admin-docs.mozilla.org/reference/policies/postquantumkeyagreementenabled/

75. Mozilla: Firefox, further material. https://www.firefox.com/en-US/firefox/132.0/releasenotes/

76. Mozilla: Firefox, further material. https://www.firefox.com/en-US/firefox/135.0/releasenotes/

77. Microsoft Edge Browser Policy Documentation PostQuantumKeyAgreementEnabled, 2026-05-20. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/postquantumkeyagreementenabled

78. Microsoft: Edge, further material. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-archive-stable-channel

79. Fortinet Advances Quantum-Safe Security to Guard Against Emerging Quantum Threats, 2025-07-22. https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2025/fortinet-advances-quantum-safe-security-to-guard-against-emerging-quantum-threats

80. Fortinet: FortiGate and FortiWeb (FortiOS), further material. https://docs.fortinet.com/document/fortigate/7.6.0/new-features/229631/enhancing-security-with-post-quantum-cryptography-for-ipsec-key-exchange-7-6-1

81. Fortinet: FortiGate and FortiWeb (FortiOS), further material. https://docs.fortinet.com/document/fortiweb/8.0.4/administration-guide/426552/post-quantum-cryptography-pqc-support-8-0-3

82. Fortinet: Fortinet cloud services (FortiCloud, FortiGuard, FortiToken Cloud), further material. https://docs.fortinet.com/document/fortigate/8.0.2/administration-guide/771310/post-quantum-cryptography-support-in-ssl-deep-inspection

83. Palo Alto Networks: PAN-OS firewalls, further material. https://docs.paloaltonetworks.com/network-security/quantum-security/administration/configure-quantum-resistant-ikev2-vpns/configure-post-quantum-ikev2-vpns-with-rfc-9242-and-rfc-9370-hybrid-keys

84. Palo Alto Networks: PAN-OS firewalls, further material. https://docs.paloaltonetworks.com/panorama/new-features/by-version/panorama/12-1

85. New Features - Prisma Access - 6.1 Preferred and Innovation, 2026-03. https://docs.paloaltonetworks.com/prisma-access/new-features/by-version/prisma-access/6-1-preferred-innovation

86. Palo Alto Networks: Prisma Access, SASE and WildFire services, further material. https://docs.paloaltonetworks.com/ngfw/release-notes/12-1/features-introduced-in-pan-os/decryption-features

87. Cisco: Secure Firewall (FTD, ASA), further material. https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.html

88. Cisco: Secure Firewall (FTD, ASA), further material. https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/release-notes/threat-defense/100/management-center-release-notes-10-0.html

89. Webex Suite Meetings Security technical paper, 2026-07-14. https://help.webex.com/article/nhxkyce

90. Juniper Networks / HPE: Junos routers and firewalls, further material. https://www.juniper.net/documentation/us/en/software/junos/pki/pki.pdf

91. Juniper Networks / HPE: Junos routers and firewalls, further material. https://www.juniper.net/documentation/us/en/software/junos/release-notes/22.4/junos-release-notes-22.4r1/topics/new-features/feature-descriptions/vpns-13.html

92. Juniper Networks / HPE: Junos routers and firewalls, further material. https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/quantum-safe-ipsec-vpn.html

93. Thales: Luna HSM, further material. https://thalesdocs.com/gphsm/luna/7/docs/network/Content/CRN/Luna/CRN.htm

94. nShield Security World v13.9.0 Release Notes, 2025-08-22. https://nshielddocs.entrust.com/security-world-docs/v13.9.0/release-notes/release-notes.html

95. Entrust: nShield HSM, further material. https://nshielddocs.entrust.com/release-notes/nshield-security-world-v13-9-6-release-notes.html

96. Entrust: nShield HSM, further material. https://nshielddocs.entrust.com/release-notes/nshield-security-world-v13-9-3-release-notes.html

97. ML-KEM post-quantum TLS now supported in AWS KMS, ACM, and Secrets Manager, 2025-04-07. https://aws.amazon.com/blogs/security/ml-kem-post-quantum-tls-now-supported-in-aws-kms-acm-and-secrets-manager/

98. Amazon Web Services: AWS KMS, further material. https://docs.aws.amazon.com/kms/latest/developerguide/pqtls.html

99. Amazon Web Services: AWS KMS, further material. https://docs.aws.amazon.com/sdkref/latest/guide/pqtls-details.html

100. Google: Google Cloud KMS, further material. https://docs.cloud.google.com/kms/docs/key-encapsulation-mechanisms

101. Key types, algorithms, and operations - Azure Key Vault Managed HSM, 2026-05-21. https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/about-keys-details

102. Microsoft: Azure Key Vault and Managed HSM, further material. https://learn.microsoft.com/en-us/azure/key-vault/keys/about-keys

103. Microsoft: SQL Server and Azure SQL, further material. https://learn.microsoft.com/en-us/sql/relational-databases/security/networking/tls-1-3?view=sql-server-ver17

104. Amazon Web Services: Amazon DynamoDB, further material. https://aws.amazon.com/about-aws/whats-new/2026/09/postgresql-post-quantum-tls-key-exchange/

105. Amazon Web Services: Amazon DynamoDB, further material. https://docs.aws.amazon.com/AmazonRDS/latest/AuroraMySQLReleaseNotes/AuroraMySQL.Updates.848.html

106. Various: Managed PostgreSQL, further material. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL.Concepts.General.SSL.html

107. Oracle AI Database cryptographic roadmap, 2026-03. https://www.oracle.com/security/database-security/crypto-roadmap/

108. Oracle: Oracle Database 26ai and OCI, further material. https://docs.oracle.com/en/database/oracle/oracle-database/26/netrf/parameters-for-the-sqlnet.ora.html

.09. Oracle: Oracle Database 26ai and OCI, further material. https://docs.oracle.com/en/database/oracle/oracle-database/26/nfcoa/encryption.html

.10. Salesforce Post-Quantum Cryptography, 2026-03-18. https://compliance.salesforce.com/en/documents/a00Kd00000z7HMjIAM

.11. Salesforce: Salesforce platform, further material. https://help.salesforce.com/s/articleView?id=002472175&language=en_US&type=1

.12. Salesforce: Salesforce platform, further material. https://help.salesforce.com/s/articleView?id=000380977&language=en_US&type=1

.13. External Key Management Service: Keep Your Encryption Keys, Keep Control of Your Data, 2026-06-01. https://www.servicenow.com/community/platform-privacy-security-blog/external-key-management-service-keep-your-encryption-keys-keep/ba-p/3551900

.14. ServiceNow: Now Platform, further material. https://newsroom.servicenow.com/press-releases/details/2026/ServiceNow-delivers-Autonomous-Security-the-industrys-most-complete-security-offering/default.aspx

.15. Workday's Post-Quantum Cryptography Migration: How We're Securing Your Data for the Future, 2026-06-22. https://medium.com/workday-engineering/workdays-post-quantum-cryptography-migration-how-we-re-securing-your-data-for-the-future-a9106e593c5c

.16. Workday: Workday, further material. https://security.workday.com/

.17. Zoom bolsters security offering with the inclusion of post-quantum end-to-end encryption in Zoom Workplace, 2024-05-21. https://news.zoom.com/post-quantum-e2ee/

.18. Zoom: Zoom end-to-end encryption, further material. https://www.zoom.com/en/blog/guide-to-post-quantum-end-to-end-encryption/

.19. Zoom: Zoom end-to-end encryption, further material. https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408

.20. Zoom: Zoom end-to-end encryption, further material. https://github.com/zoom/zoom-e2e-whitepaper/blob/master/CHANGELOG.md

.21. Signal Protocol and Post-Quantum Ratchets, 2025-10-02. https://signal.org/blog/spqr/

.22. Signal: Signal protocol (PQXDH), further material. https://signal.org/blog/pqxdh/

.23. Signal: Signal protocol (PQXDH), further material. https://signal.org/docs/specifications/mlkembraid/

124. Quantum-secure cryptography in Apple operating systems, 2026-01-28. https://support.apple.com/en-gb/guide/security/secc7c82e533/web

125. Apple: iMessage (PQ3), further material. https://security.apple.com/blog/imessage-pq3/

126. Apple: iMessage (PQ3), further material. https://developer.apple.com/videos/play/wwdc2025/314/

127. Apple: Apple push, identity and iCloud Mail, further material. https://support.apple.com/en-us/guide/security/sec100a75d12/web

128. Leading the Way for Post-Quantum Cryptography, 2026-07-13. https://community.sap.com/t5/security-and-compliance-blog-posts/leading-the-way-for-post-quantum-cryptography/ba-p/14439479

129. SAP: SAP Business Technology Platform (Cloud Foundry), further material. https://community.sap.com/t5/technology-blog-posts-by-sap/quantum-safe-by-default-how-sap-s-4hana-closes-the-door-on-harvest-now/ba-p/14498058

130. Tuta Ensures Post Quantum Cryptography For Email, 2026-08-26. https://tuta.com/blog/post-quantum-cryptography

131. Tuta: TutaCrypt end-to-end encryption, further material. https://tuta.com/blog/celebrating-one-year-pq-launch

132. Tuta: TutaCrypt end-to-end encryption, further material. https://tuta.com/encryption

133. Proton Mail introduces post-quantum encryption, 2026-05-05. https://proton.me/blog/introducing-post-quantum-encryption

134. Proton: Post-quantum OpenPGP end-to-end encryption, further material. https://proton.me/support/mail-post-quantum-protection

135. Proton: Post-quantum OpenPGP end-to-end encryption, further material. https://github.com/ProtonMail/gopenpgp/blob/main/CHANGELOG.md

136. Commercial National Security Algorithm Suite 2.0 and Quantum Computing Frequently Asked Questions (NSA, Ver. 2.2), 2026-10. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

137. NSA Announces Post-Quantum Cryptography Measures to Safeguard National Security Systems Against Quantum Computing Threats, 2026-10-01. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4615285/nsa-announces-post-quantum-cryptography-measures-to-safeguard-national-security/

138. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, Version 1.1 (NIS Cooperation Group), 2025-06-11. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

About this report

Per-host results are not published. A vendor or operator may ask for a re-test of a listed host at hello@pqprobe.com; the answer comes within five business days. The scored products' hosts are scanned once a day, and the Vendor Monitor at pqprobe.com/dashboard/vendors shows each product's current standing beside what its dated vendor material says.

Publisher
Ottenheimer GmbH

Published
5 November 2026

Licence
Creative Commons Attribution 4.0 International (CC BY 4.0)

Contact
hello@pqprobe.com