

POST-QUANTUM CRYPTOGRAPHY (PQC) CAPABILITY DEVELOPMENT REPORT

September 2026

The evidence presented in this report is based on findings collected in July 2026.
The peer review and commentary period took place in August–September 2026.

© 2026 MITRE. All Rights Reserved.

Approved for Public Release; Distribution Unlimited. Case **26-2150**

MITRE

BACKGROUND & OVERVIEW

The development of quantum computers capable of breaking classical cryptography threatens today's digital systems. In response, efforts to migrate to post-quantum cryptography (PQC) have intensified, as seen in recent directives such as Executive Order 14412 and M-26-15, which direct federal agencies to accelerate PQC migration, provide schedules alongside migration planning, and call for assistance to critical infrastructure owners and operators in developing PQC migration plans.

This report supports migration planning by providing a snapshot of PQC solution development maturity across a selected set of critical enterprise technologies that rely on cryptographic capabilities, based on publicly available evidence.[i] The intent is to provide situational awareness of technological maturity to inform migration planning, technology refresh cycles, and long-term investment decisions by identifying which capabilities are beginning to incorporate quantum-resistant cryptographic protections and which remain at earlier stages of development.

Our analysis focuses on claims supporting PQC algorithm integration in solutions, and this report should not be interpreted as an independent evaluation of product security. In our capability assessments, we attempt to reflect claims made by vendors and technology sources about integration of PQC algorithms, particularly in asymmetric cryptography-based solutions. Although PQC algorithm integration alone is not sufficient for product security, it represents an important precondition for solutions being “quantum-safe,” or resistant to cryptanalytic attack by an adversary with access to powerful quantum computers. Overall, knowledge of PQC integration in capabilities can help organizations better plan and evolve their enterprise technologies to meet cryptographic threats.

[i] The evidence presented in this report is based on findings collected in July 2026. The peer review and commentary period took place in August–September 2026.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

PQC Capability Development Overview

Capability	Confidentiality Development	Authentication Development
Web Browsers	Integration	Components Available
Web Servers	Integration	Components Available
VPN/Network Encryption	Integration	Components Available
Platform Assurance	N/A	Components Available
Code Signing	N/A	Integration
PKI/CA Management	Integration	Integration
Volume Encryption	Components Available	Components Available
Cloud Service Connectivity	Integration	Preliminary Integration

Development Definitions

Development Level	Definition
N/A	The capability does not significantly rely on this type of security guarantee.
Blocked	No standards exist to support PQC in this capability for this type of security guarantee.
Enabled	The necessary standards exist to support PQC for this capability and this type of security guarantee.
Components Available	Specialized, capability-specific components exist that incorporate standards-based support for PQC for this type of security guarantee.
Preliminary Integration	A preliminary, limited, or experimental release supports PQC for this type of security guarantee.
Integration	A general release that is fully available to the public and ready to use supports PQC for this type of security guarantee.
Validated Integration	A general release supports PQC for this type of security guarantee, based on a FIPS 140-3 validated module certified to provide those PQC functions.

Note: Each definition describes the capability's development level for the type of security guarantee (Confidentiaility or Authentication) being individually assessed.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

METHODOLOGY

Each capability is evaluated across at least one of two independent security guarantee types: confidentiality development and authentication development. Confidentiality and authentication are evaluated independently because (1) not all capabilities rely on both types of security guarantees, and (2) capabilities may show more progress toward one type of security than the other.

Confidentiality development measures how far a capability has progressed in adopting PQC mechanisms that protect the confidentiality of data, such as quantum-resistant key establishment for encrypted communications.

Authentication development measures progress in adopting PQC mechanisms that allow a party to verify the identity of an entity or the origin and integrity of information through quantum-resistant digital signatures.

This assessment considers only positive progress toward incorporating PQC and therefore excludes technologies that do not rely on asymmetric cryptography at all, as they are not expected to require PQC-related changes. The resulting capability status provides a practical view of where PQC integration is occurring today and where future developments are likely to influence organizational migration planning.

Our research did not focus on pre-selected vendors or products. Rather, a general search was performed for sources discussing progress incorporating PQC into the assessed technical capabilities. We were intentionally broad when considering sources, ensuring that our review did not limit itself to only “major” vendors or products. The claims made within the identified sources were then compared against our development level definitions. For each capability, the overall assessment is based on the highest development level observed in the supporting sources. The inclusion of specific products or vendors in the references should not be interpreted as a listing of the most significant products or vendors in any capability area. References in this report support the assessment of observable maturity and do not endorse products or vendors.

When assessing maturity, we built the development level definitions to reflect common stages of product development found in our research. For the highest level of development, we defined Validated Integration as being FIPS 140-3 validated, as it goes beyond ensuring the use of strong algorithms and provides evidence that the algorithms are being implemented in a controlled manner. For certain organizations, FIPS validation is also a requirement for new capability adoption, which adds to why Validated Integration is the highest level of development in our analysis. We do not separately track the maturity of pure versus hybrid approaches, or the integration of specific key sizes, although, where possible, we articulate the approaches used by the most mature solutions.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

DEFINITIONS

This report presents a cross-section of technical cryptographic capabilities and a current assessment of the PQC development of those capabilities. The term “PQC development” refers to the level of standards-based PQC algorithm integration for quantum-resistant confidentiality and/or authentication. We define PQC development on the following scales for confidentiality and authentication.

Development Level Definitions

Note: Each definition describes the capability’s development level for the type of security guarantee (Confidentiality or Authentication) being individually assessed.

Development Level	Definition
N/A	The capability does not significantly rely on this type of security guarantee.
Blocked	No standards exist to support PQC in this capability for this type of security guarantee.
Enabled	The necessary standards exist to support PQC for this capability and this type of security guarantee.
Components Available	Specialized, capability-specific components exist that incorporate standards-based support for PQC for this type of security guarantee.
Preliminary Integration	A preliminary, limited, or experimental release supports PQC for this type of security guarantee.
Integration	A general release that is fully available to the public and ready to use supports PQC for this type of security guarantee.
Validated Integration	A general release supports PQC for this type of security guarantee, based on a FIPS 140-3 validated module certified to provide those PQC functions.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

Technical Capability Definitions

This report assesses PQC across selected enterprise technology capabilities. These capabilities were selected because they support common enterprise operations and all rely on cryptographic functions to varying degrees. Some capability areas encompass more cryptographic components than others, and certain services and products may support multiple capabilities. Other relevant capability areas will be assessed in future versions of this report, as organizational relevance and available evidence permit. To ensure a consistent assessment, each capability area is defined as follows.

Web Browsers: Client-side software capability to establish, negotiate, and validate secure web sessions using standard web security protocols (e.g., transport layer security or "TLS"), including handshake processing, certificate validation, and enforcement of security policies.

Web Servers: Server-side capability to terminate TLS and handle secure web traffic, including certificate management.

Virtual Private Network (VPN)/Network Encryption: Capability to protect network tunnels and communication links through secure key establishment and authentication mechanisms for data in transit between private endpoints.

Platform Assurance: Capability to ensure hardware, firmware, and operating system integrity through mechanisms such as secure boot, measured boot, attestation, and hardware roots of trust to support trusted computing environments.

Code Signing: Capability to sign and verify signatures of code, software, and updates.

Public Key Infrastructure/Certificate Authority (PKI/CA) Management: Capability to issue, manage, and validate certificates and support lifecycle operations (enrollment, rotation, revocation).

Volume Encryption: Capability to protect data at rest through full-disk or volume-level encryption, including management of encryption keys and access controls.

Cloud Service Connectivity: Capability to securely connect to cloud services and application programming interfaces (APIs) using transport security and identity mechanisms across control and data planes.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

WEB BROWSERS



Confidentiality: Integration

Authentication: Components Available

The web browser ecosystem has made substantial progress in post-quantum confidentiality, while post-quantum authentication remains at the component and experimental stage. For confidentiality, most major browser platforms support hybrid post-quantum TLS key establishment, primarily through X25519MLKEM768, which combines X25519 with ML-KEM-768 (NIST Category 3) and has been enabled by default in several major browsers.[1,2,3,4,7,8] The assessed browser implementations did not demonstrate equivalent mainstream support for higher-strength ML-KEM parameter sets, such as ML-KEM-1024, or pure-PQC TLS key establishment.[9]

Post-quantum authentication integration in web browsers is less mature.[2,5] Developers have identified technical adoption barriers created by the size of post-quantum signatures and certificates.[2] Browser support for X.509 certificate validation using post-quantum signature algorithms was not found. However, vendors have published designs, experimental implementations, and platform support for algorithms such as ML-DSA,[2,3,4,5,10] and browser security libraries increasingly support post-quantum signature primitives.[5] There is also evidence of limited or experimental use of post-quantum signature methods using alternative approaches such as Merkle Tree Certificates in at least one web browser.[3]

Overall, web browsers are capable of delivering post-quantum confidentiality today through post-quantum hybrid TLS, and some components of web browsers incorporate post-quantum signature capabilities.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

WEB SERVERS



Confidentiality: Integration

Authentication: Components Available

The web server ecosystem has progressed toward PQC readiness for confidentiality through hybrid TLS key establishment, as well as some building blocks for post-quantum authentication. Several major web servers support post-quantum hybrid use of ML-KEM in TLS handshakes.[10,13] The evaluated implementations primarily use hybrid TLS groups such as X25519MLKEM768, a NIST Category 3 parameter set combining the classical X25519 key exchange with ML-KEM-768. Support is increasingly available through modern TLS libraries, operating-system TLS stacks, and reverse proxies, with some implementations already deployed in production environments and others available through documented implementation guidance.[11,12,14]

Post-quantum authentication for web servers is less mature than confidentiality. Several vendors provide guidance for deploying PQC certificates and digital signatures through custom software builds, particularly involving OpenQuantumSafe.[11,12,14] These implementations provide ML-DSA support,[12] PQC certificates,[14] and hybrid authentication mechanisms.[11,12] In addition, several cryptographic libraries supporting TLS 1.3 have introduced ML-DSA primitives.[13] However, our research did not find integration into mainstream web server distributions.

Overall, PQC-enabled web-server infrastructure supports hybrid confidentiality deployments today, while PQC-based authentication still depends on custom software builds.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

VPN/NETWORK ENCRYPTION



Confidentiality: Integration

Authentication: Components Available

The VPN/network encryption ecosystem has progressed toward PQC adoption, with confidentiality ahead of authentication. Multiple vendors support ML-KEM or hybrid ML-KEM key encapsulation leveraging either IKE/IPsec or TLS in their VPN products.[15,17,18,19,20] Some products demonstrate integrated deployment through standardized quantum-resistant IKEv2 VPNs using RFC 9242 and RFC 9370, with support for hybrid post-quantum key establishment and interoperability with standards-compliant peers.[15]

For VPN authentication, limited components of PQC currently exist. VPNs rely on authentication to ensure that secure tunnels are only created with trusted endpoints. Our research found that post-quantum building blocks exist, but they do not yet support integration into VPN connections.[16,17] Vendors developing VPN products are still primarily focused on key exchange, hybrid encryption, and tunnel protection rather than post-quantum endpoint authentication.[16,17]

Overall, VPN confidentiality has advanced further than authentication. Organizations can deploy post-quantum confidentiality today through standardized hybrid key establishment, but complete migration depends on more mature PQC digital signature integration.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

PLATFORM ASSURANCE



Confidentiality: N/A

Authentication: Components Available

Technologies enabling platform assurance, such as secure boot, measured boot, attestation, and hardware roots of trust have begun integrating PQC authentication. However, these technologies for platform assurance operate across multiple levels, and the PQC versions of these capabilities are not yet fully integrated.

Trusted Platform Modules (TPMs) are common specialized components of computing platforms that are used as a hardware root of trust, and are a mandatory baseline requirement for some operating systems and networks.

Firmware-based TPMs have standardized support for all ML-DSA parameter sets through software implementation,[21,23] and are secured by post-quantum update mechanisms.[27] As of July 2026, no evidence of commercially available PQC hardware TPM implementations has been identified, but PQC capabilities have been articulated as a needed next step.[21,22,28] Other hardware roots of trust have introduced PQC support into firmware authentication, device identity, and attestation.[26]

Broader platform assurance capabilities remain at an earlier stage of development. Secure boot and firmware signing have well-defined migration approaches[25] and emerging PQC implementations, but integration of these techniques in production boot chains has yet to be claimed. Likewise, operating systems now provide PQC cryptographic primitives that enable future trusted boot and platform integrity services,[24] but our research did not find PQC integrated into mainstream trusted boot, measured boot, or remote attestation workflows.

Overall, platform assurance capabilities are transitioning unevenly. Although they currently demonstrate component-level implementation, challenges remain in integrating those components.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

CODE SIGNING



Confidentiality: N/A

Authentication: Integration

Signing capabilities for code distributions, operating systems, and application software include a broad range of software vendors, certificate authorities, and signing platforms that have incorporated PQC authentication at different rates. Some code signing platforms have already introduced support for post-quantum digital signatures, including NIST-standardized algorithms such as ML-DSA and, in some cases, hybrid[ii] signing approaches.[28,29,30] These implementations demonstrate that practical PQC code signing has progressed beyond experimental implementations. Some certificate and signing infrastructure tools also support issuing and managing post-quantum digital signatures for code signing.[31,32]

Overall, there are PQC-integrated code signing solutions that can be deployed now and that are progressing toward validation.

[ii] The use of hybrid signatures alone does not establish secure hybrid authentication. Hybrid signature constructions introduce design considerations and risks such as stripping or downgrade attacks.[33]

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

PKI/CA MANAGEMENT



Confidentiality: Integration

Authentication: Integration

The PKI ecosystem has transitioned from PQC experimentation to operational deployment, with several major vendors now supporting ML-DSA signatures.[34,35,36] Leading certificate authority platforms support the issuance and management of certificates using NIST-standardized post-quantum signature algorithms, such as ML-DSA [34,35,36,37] and SLH-DSA.[34,36] These capabilities enable post-quantum certificate issuance and hybrid authentication models for enterprise deployments.

Confidentiality in the context of PKI/CA management entails supporting PKI and PQC-based public keys for pure or hybrid ML-KEM in certificate formats. This is less central to the development of PKI/CA management overall, since supporting signature keys in certificate formats is necessary to build PKI chains. There is evidence of PKI capabilities integrating ML-KEM keys into certificate issuance and lifecycle operations.[34]

Overall, PQC support in PKI/CA management capabilities has been integrated for both encryption and signature keys, with deployable solutions available for issuing, managing, and validating certificates and supporting certificate lifecycle operations.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

VOLUME ENCRYPTION



Confidentiality: Components Available

Authentication: Components Available

Current examples of volume encryption capabilities use asymmetric cryptography for volume-key establishment and management, access control, key wrapping, recovery, or disk-encryption key hierarchies,[38,40,41,42] although others use only symmetric cryptography, such as AES-XTS, for protecting data at rest and volume keys, password-based or boot measurement methods for authentication.

Our assessment of the PQC development of volume encryption is based only on progress for solutions currently leveraging asymmetric cryptography. For those technologies, PQC support is in an early stage of transition, present only in components of overall solutions.[39] In some technologies, asymmetric cryptography is tied to TPMs for which PQC support is planned, but actual commercial components are not yet available. In others, asymmetric cryptography is involved optionally in delivering access tokens through FIDO2 (transported over TLS).[42]

Overall, our research indicates that components enabling PQC asymmetric methods for volume encryption are available, but we did not find evidence of early integration.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

CLOUD SERVICE CONNECTIVITY



Confidentiality: Integration

Authentication: Preliminary Integration

Cloud service providers have made some of the most significant progress toward PQC-enabled operations, with stronger PQC integration for confidentiality than for authentication. Several cloud connectivity platforms now implement hybrid TLS using NIST-standardized post-quantum key encapsulation mechanisms.[43,45,46,47,48]

Authentication is less mature across cloud service connectivity technologies. Publicly available implementations of post-quantum digital signatures and certificate capabilities are comparatively limited, and most documented deployments prioritize transport security over replacing classical authentication mechanisms.[44,45,46,47,48] The highest observed development level of authentication is experimental deployment of post-quantum signatures on long-lived TLS connections with support for ML-DSA.[43,44]

Overall, organizations today can adopt hybrid post-quantum confidentiality for select cloud services and connectivity platforms. Post-quantum authentication in the ecosystem shows preliminary integration, with experimental solutions currently being developed.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

ACKNOWLEDGEMENTS

This work was supported by the MITRE Independent Research and Development Program. Portions of this technical data were produced for the U.S. Government under Contract No. FA870225CB001 and W56KGU-18-D-0004, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (FEB 2014).

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

REFERENCES

Web Browsers

1. “Protecting Chrome Traffic with Hybrid Kyber KEM,” Chromium Blog, Aug 10, 2023, https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.
2. "Building a Deployable Post-quantum Web PKI," Chromium Project, Aug 27, 2024, https://www.chromium.org/Home/chromium-security/post-quantum-pki-design/.
3. "Cultivating a Robust and Efficient Quantum-Safe HTTPS," Google Security Blog, Feb 27, 2026, https://blog.google/security/cultivating-a-robust-and-efficient-quantum-safe-https/.
4. "Quantum-Secure Cryptography in Apple Operating Systems," Apple Platform Security, Jan 28, 2026, https://support.apple.com/guide/security/quantum-secure-cryptography-apple-devices-secc7c82e533/web.
5. "PQC Support Documentation," Cloudflare Developers, Jun 24, 2026, https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-support/.
6. "Post-Quantum Cryptography Resources," Google Cloud, (n.d.), https://cloud.google.com/security/resources/post-quantum-cryptography.
7. "Post Quantum Key Agreement Enabled Policy," Microsoft Learn, (n.d.), https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies/PostQuantumKeyAgreementEnabled.
8. "Hybrid Quantum-Secure TLS Deployment (X25519MLKEM768)," Apple Support, Jun 18, 2026, https://support.apple.com/en-us/122756.
9. “Module-Lattice-Based Key-Encapsulation Mechanism Standard,” National Institute of Standards and Technology, Aug 13, 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf.
10. David Benjamin and Joe DeBlasio, “Post-Quantum HTTPS Authentication Roadmap,” Chromium Project, Feb 27, 2026, https://www.chromium.org/Home/chromium-security/post-quantum-auth-roadmap/.

Web Servers

11. Christopher van de Sande, “Post-Quantum Cryptography (PQC) support in NGINX,” NGINX Community Blog, Dec 3, 2025, https://blog.nginx.org/blog/pqc-nginx.
12. “Post-Quantum Cryptography: Building Resilience Against Tomorrow’s Threats,” F5, Mar 25, 2026, https://community.f5.com/kb/technicalarticles/post-quantum-cryptography-building-resilience-against-tomorrow%E2%80%99s-threats/341048.
13. Aabha Thipsay, “Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms,” Microsoft Security Blog, Nov 18, 2025, https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-apis-now-generally-available-on-microsoft-platforms/4469093/replies/4491787.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

14. Mariam John, “Building a quantum-safe web application based on a quantum-safe version of OpenSSL,” IBM Developer, Mar 26, 2024, https://developer.ibm.com/tutorials/awb-building-quantum-safe-web-applications/.

VPN/Network Encryption

15. "Support for Post-Quantum Features," Palo Alto Networks TechDocs, May 27, 2026, https://docs.paloaltonetworks.com/network-security/quantum-security/administration/quantum-security-concepts/support-for-quantum-features.
16. "Securing the Quantum Age," Palo Alto Networks Blog, Aug 13, 2025, https://www.paloaltonetworks.com/blog/2025/08/securing-the-quantum-age/.
17. "Quantum Computing and the Future of Cybersecurity," OpenVPN Blog, Sep 15, 2025, https://blog.openvpn.net/quantum-safe-vpn.
18. "Post-Quantum Cryptography for IPsec Key Exchange," Fortinet, (n.d.), https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/229631/post-quantum-cryptography-for-ipsec-key-exchange.
19. "Enhancing Security with Post-Quantum Cryptography for IPsec Key Exchange (7.6.1)," Fortinet, (n.d.), 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.
20. "Post-Quantum Cryptography IKEv2 Configuration," Cisco, Apr 24, 2026, https://www.cisco.com/c/en/us/td/docs/routers/ios-xe/security-vpn/security-vpn/m-pqc-ikev2.html.

Platform Assurance

21. "The First Firmware TPM with Post-Quantum Cryptography," wolfSSL Blog, May 4, 2026, https://www.wolfssl.com/the-first-firmware-tpm-with-post-quantum-cryptography/.
22. "New Computing Specification Implements PQC Measures to Protect Users from Quantum Attacks," Trusted Computing Group, Mar 22, 2026, https://trustedcomputinggroup.org/new-computing-specification-implements-pqc-measures-to-protect-users-from-quantum-attacks/.
23. "Infineon TPM Features PQC-Protected Firmware Update Mechanism," Infineon Market News, Feb 15, 2022, https://www.infineon.com/market-news/2022/infcss202202-051.
24. "Operating System Security: System Security," Microsoft Learn, (n.d.), https://learn.microsoft.com/en-us/windows/security/book/operating-system-security-system-security.
25. Matthew Stubbs, "Secure Boot Considerations With PQC," PQShield, Nov 21, 2024, https://pqshield.com/secure-boot-considerations-with-pqc/.
26. “Caliptra: A Datacenter System on a Chip (SoC) Root of Trust (RoT),” Open Compute Project, Jul 31, 2025, https://www.opencompute.org/documents/caliptra-2-0-pdf.
27. Michael Burner, “Infineon Advances Physical AI Security Against Quantum-Era Threats with Certified TPM Solution for NVIDIA Jetson Thor,” Infineon, Jun 3, 2026, https://www.infineon.com/press-release/2026/infxx202606-104.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

Code Signing

28. Christian Chisholm, "From Strategy to Architecture: Building a Quantum-Safe Future," Cisco Security Blog, Apr 30, 2026, https://blogs.cisco.com/security/from-strategy-to-architecture-building-a-quantum-safe-future.
29. Clemens Lang, "What's New in Post-Quantum Cryptography in RHEL 10.1," Red Hat Blog, Feb 4, 2026, https://www.redhat.com/en/blog/whats-new-post-quantum-cryptography-rhel-101.
30. "Android 17 Release Notes," Android Developers, Jun 15, 2026, https://developer.android.com/about/versions/17/release-notes.
31. "AWS Private CA Now Supports Post-Quantum Digital Certificates," AWS, Nov 10, 2025, https://aws.amazon.com/about-aws/whats-new/2025/11/aws-private-ca-post-quantum-digital-certificates/.
32. "Post-Quantum Cryptography in AD CS Overview," Microsoft Learn, (n.d.), https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/post-quantum-cryptography-overview.
33. Nina Bindel et al., “RFC 9955: Hybrid Signature Spectrums,” Internet Engineering Task Force, Jul 2026, https://www.rfc-editor.org/info/rfc9955/.

PKI/CA Management

34. "Post-Quantum Cryptography Keys and Signatures," Keyfactor, (n.d.), https://docs.keyfactor.com/ejbca/latest/post-quantum-cryptography-keys-and-signatures.
35. "Post-Quantum Cryptography in AD CS Overview," Microsoft Learn, (n.d.), https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/post-quantum-cryptography-overview.
36. “DigiCert Solutions for Post Quantum Computing,” DigiCert, (n.d.), https://docs.digicert.com/en/platform-overview/digicert-solutions-for-post-quantum-computing.html.
37. “DigiCert Private CA Release Notes,” DigiCert, Feb 12, 2026, https://docs.digicert.com/en/whats-new/release-notes/ca-manager-release-notes.html.

Volume Encryption

38. “NetApp Storage Encryption and NetApp Volume Encryption”, NetApp, (n.d.), https://www.netapp.com/pdf.html?item=/media/19767-ds-3898-netapp-storage-encryption-volume-encryption.pdf.
39. “NetApp Sets New Standard for Cybersecurity at the Storage Layer”, NetApp, (n.d.), https://www.netapp.com/newsroom/press-releases/news-rel-20250429-648807.
40. “BitLocker Overview”, Microsoft, (n.d.), https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**

41. “Intro to FileVault”, Apple Platform Development, (n.d.), https://support.apple.com/guide/deployment/intro-to-filevault-dep82064ec40/web.
42. “Crypttab - Configuration for encrypted block devices,” (n.d.), https://man7.org/linux/man-pages/man5/crypttab.5.html.

Cloud Service Connectivity

43. Sharon Goldberg, Wesley Evans, Bas Westerbaan, and John Engates, "Conventional Cryptography Is Under Threat. Upgrade to Post-Quantum Cryptography in Zero Trust Now," Cloudflare Blog, Mar 17, 2025, https://blog.cloudflare.com/post-quantum-zero-trust/.
44. "Post-Quantum Cryptography (PQC)," Cloudflare Developers, Jul 3, 2026, https://developers.cloudflare.com/ssl/post-quantum-cryptography/#post-quantum-signatures.
45. Alex Weibel, "ML-KEM Post-Quantum TLS Now Supported in AWS KMS, ACM, and Secrets Manager," AWS Security Blog, Apr 7, 2025, https://aws.amazon.com/blogs/security/ml-kem-post-quantum-tls-now-supported-in-aws-kms-acm-and-secrets-manager/.
46. "Istio 1.27.0 Change Notes," Istio Documentation, Aug 11, 2025, https://istio.io/latest/news/releases/1.27.x/announcing-1.27/change-notes/.
47. "Supported Security Policies – Amazon API Gateway," AWS Documentation, (n.d.), https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-security-policies-list.html.
48. "Quantum-Safe Cryptography with TLS for Key Protect," IBM Cloud Docs, Jun 22, 2023, https://cloud.ibm.com/docs/key-protect?topic=key-protect-quantum-safe-cryptography-tls-introduction.

© 2026 MITRE. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case **26-2150**