



Menlo Post-Quantum Cryptography (PQC) Support

Securing Today's Web Traffic Against Tomorrow's Quantum Threats

Three Things to Know

- **Harvest now, decrypt later may already be happening:** The NSA has publicly warned that adversaries may already be collecting encrypted data today, banking on future quantum computers to decrypt it. Long-lived sensitive data is exposed the moment it's captured, not the moment it's decrypted.
- **The timeline is shrinking:** Multiple independent estimates now place the arrival of a quantum computer capable of breaking today's encryption somewhere between 2030 and 2035, and that window has narrowed sharply in just the last few years. Adversarial use of quantum decryption is expected to follow closely once that capability exists.
- **Migration takes years:** Migrating an entire security stack to quantum-resistant cryptography is a multi-year effort. NIST finalized its first post-quantum cryptography standards, including ML-KEM, in August 2024 — and Menlo has already adopted it, well ahead of any confirmed deadline.

The Quantum Threat

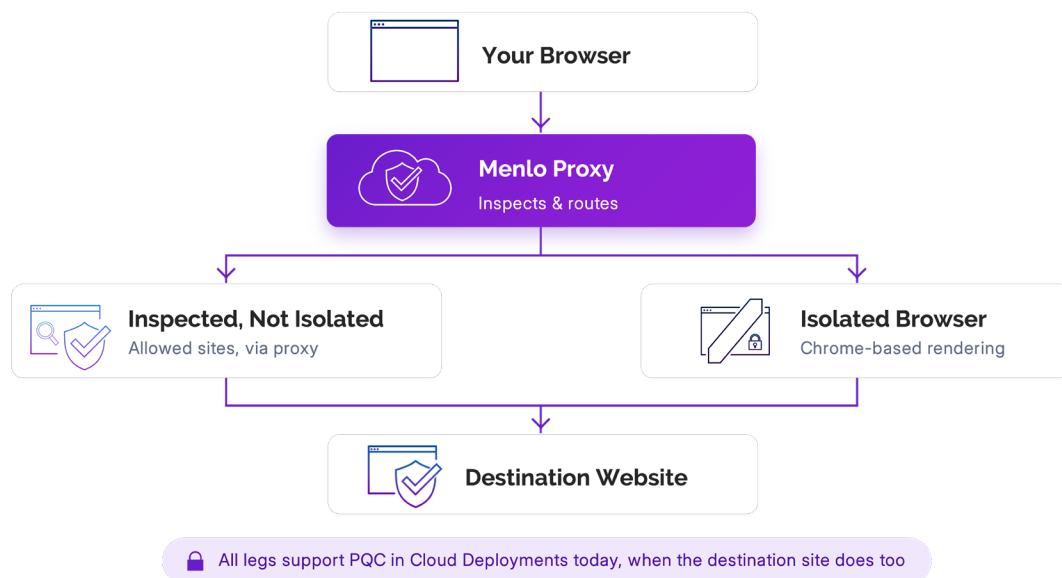
Quantum computers powerful enough to break today's encryption don't exist yet, but the resources needed to build one keep shrinking, and expert estimates for when they might arrive keep getting closer. Meanwhile, adversaries can already capture encrypted web traffic today and simply wait to decrypt it later, a tactic known as harvest now, decrypt later. Any organization handling data that needs to stay confidential for years, such as government records, health information, or trade secrets, faces exposure long before a quantum computer actually arrives.

Migrating web traffic to quantum-resistant cryptography is not a one-time switch: it depends on both ends of every connection being upgraded, which takes years to complete across an entire organization. Waiting until a quantum computer is confirmed to exist is waiting too long — by then, any traffic captured today is already permanently exposed. The migration needs to start now.

Delivering Hybrid Post-Quantum Cryptography Across Every Leg of the Browsing Session

Menlo Security supports X25519MLKEM768, a hybrid key exchange that combines two methods at once: the current classical method (X25519, an elliptic-curve technique widely used across the industry today) and MLKEM, the new NIST-standardized quantum-resistant method. Both sides of a connection need to support the hybrid approach for it to actually be used. When the destination server doesn't support it, the connection isn't left unprotected — it simply falls back to the classical method alone, the same encryption relied on across the web today. When the destination server does support the hybrid approach, the connection gets the benefit of both methods at once: protected against today's threats and, going forward, against tomorrow's quantum ones. This runs over TLS 1.3 and uses FIPS-approved algorithms throughout.

How Menlo Supports PQC Across A Browsing Session



With our latest proxy architecture, PQC support now spans every leg of the connection in Cloud deployments: the client to Menlo, and Menlo to the destination website, whether that traffic is inspected by the proxy or additionally routed through Menlo's isolated cloud browser. Because Menlo terminates and re-establishes each TLS connection itself, that traffic remains fully inspected even when it's encrypted using PQC — moving to quantum-resistant encryption does not create a blind spot for security teams.

Key Capabilities:

- **End-to-end PQC coverage:** Menlo PQC support now spans the full path of a browsing session, and that traffic stays fully inspected throughout, even when it's encrypted using PQC.
- **Hybrid classical + PQC key exchange:** Menlo combines two methods at once: a proven classical method with a new quantum-resistant one, so the connection is protected by both at the same time. Post-quantum digital signatures are a separate technology and are not yet in use anywhere — not by Menlo, and not by any public Certificate Authority or major browser. This is an industry-wide gap today, not a Menlo limitation.
- **FIPS-approved cryptography:** Menlo's PQC implementation uses FIPS-approved algorithms — cryptographic methods that meet the U.S. government's Federal Information Processing Standards (FIPS), a common bar many regulated industries require. Our commercial product does not run in a certified FIPS mode, but the same approved algorithms are used regardless, so there is no material difference in the cryptography applied. There are no additional licensing requirements.
- **Crypto visibility, with more on the roadmap:** Menlo has underlying visibility into TLS versions and cryptographic algorithms in use, including which connections are classical versus PQC or hybrid. Policy controls for TLS/cryptographic configuration and dedicated PQC readiness reporting are not generally available today; Menlo can help assess migration readiness using existing browser-version telemetry to flag clients too old to support PQC.
- **No endpoint changes required:** PQC support lives in Menlo's proxy and isolation infrastructure, not on the endpoint. Users keep working in their browser of choice, and IT teams have no new client software to install, configure, or manage in order to benefit from it.
- **Cloud and on-prem coverage, with on-prem catching up:** PQC support spans both legs of the connection in Cloud deployments. In Private Cloud/On-Premises deployments, the isolated-browser-to-destination leg already supports PQC; support for the client-to-proxy leg is on the roadmap.

Get Ahead of the Quantum Threat with Menlo Security

Menlo's PQC support, built on the Menlo Secure Cloud Browser, helps enterprises stay ahead of the migration to quantum-resistant cryptography without adding complexity for users or IT teams, all from the same platform already securing browsing, application access, and enterprise data.

No one can say exactly when quantum computers will be capable of breaking today's encryption, but data captured today can be decrypted later, which makes waiting for certainty the riskiest option. Menlo Security is building PQC support into the same cloud-native architecture that already secures browsing and application access, so customers can begin their migration journey now, without reactive, last-minute changes once the timeline becomes clearer.

To learn more about securing the ways people work, visit menlosecurity.com or email us at ask@menlosecurity.com.

About Menlo Security

Menlo Security is the pioneer of the Browser Security Platform (BSP), the industry's first infrastructure designed to govern a hybrid workforce of humans and autonomous AI agents. By centering the browser as the new enterprise operating system, Menlo provides a "Guardian Runtime" that resolves the unique risks created when AI agents operate at machine-speed without human skepticism. The Menlo platform enables the agentic enterprise to scale AI with confidence, providing universal connectivity to legacy data and unified zero-day threat prevention across every session. Trusted by over 1,000 global enterprises—including eight of the ten largest financial institutions and major government agencies—Menlo protects over 8 million users and millions of simultaneous AI agent sessions. Headquartered in Mountain View, California, and backed by investors including JPMorgan Chase, American Express Ventures, and Vista Equity Partners, Menlo is securing the browser for the agentic age. Learn more at www.menlosecurity.com.

Work without worry and move business forward with Menlo Security. © 2026 Menlo Security, All Rights Reserved



Learn more: <https://www.menlosecurity.com>
Contact us: ask@menlosecurity.com

