WHITEPAPER

Post-Quantum Readiness for DNS and Network Infrastructure

Network infrastructure is frequently left out of post-quantum planning entirely — but encrypted DNS and DNSSEC carry two genuinely different migration timelines that deserve separate attention.

The Infrastructure Layer That Gets Overlooked

Most post-quantum planning starts with applications and data — reasonably, since that's where the highest-value exposure usually sits. Network infrastructure is easy to overlook as a result, but DNS in particular carries two distinct cryptographic concerns that behave very differently under quantum risk, and treating them as one problem leads to the wrong prioritisation.

Encrypted DNS: A Confidentiality Problem, and an Urgent One

Modern encrypted DNS protocols — DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), and DNS-over-QUIC (DoQ) — rely on the same classical key-exchange algorithms (ECDHE, RSA) used elsewhere in TLS and QUIC. That means encrypted DNS traffic captured today is just as exposed to "harvest now, decrypt later" as any other TLS-protected traffic.

The content matters more than it might first appear: DNS query patterns reveal internal service discovery, application dependencies, and user behaviour — the kind of metadata that's individually unremarkable but collectively revealing about how an organisation's systems and users actually behave. Because encrypted DNS shares its underlying cryptography with the broader TLS and QUIC ecosystem, it should generally migrate to post-quantum and hybrid key exchange on the same timeline as the rest of an organisation's TLS infrastructure — not treated as a separate, lower-priority project.

DNSSEC: A Different Problem, on a Different Clock

DNSSEC solves a different problem: it protects the authenticity and integrity of DNS responses — proving a response hasn't been tampered with — rather than confidentiality. Because DNSSEC doesn't encrypt anything, it isn't vulnerable to "harvest now, decrypt later" in the same way; there's no confidential payload to harvest. The quantum risk to DNSSEC is different in kind: a future quantum computer capable of forging signatures could allow an attacker to forge DNSSEC-signed responses at that point in time, not retroactively.

That distinction matters for planning. DNSSEC's migration runway is genuinely longer than encrypted DNS's, and the practical challenge is different too: post-quantum signature schemes tend to produce larger signatures, which has real implications for DNS packet sizes and response performance across a system that was designed around much smaller classical signatures. What DNSSEC needs today is algorithm agility built into the deployment — not a lower priority than encrypted DNS, but a different kind of preparation on a different timeline.

A Practical Sequencing

For most organisations, the sensible order is: bring encrypted DNS into the same hybrid-first TLS/QUIC migration work already underway for other systems, while separately tracking DNSSEC algorithm-agility readiness on a longer horizon aligned with when post-quantum signature schemes have matured enough for widespread DNS deployment.

Don't Let Infrastructure Fall Outside the Inventory

The practical risk with DNS and other network infrastructure isn't usually that the migration is technically hard — it's that it's invisible to a cryptographic inventory focused only on applications and data stores. A CBOM that stops at the application layer will miss it entirely. Enterprise Cryptographic Exposure Management extends discovery to network protocols and infrastructure specifically so that gap doesn't exist.

© 2026 Quantum Sentinel™. All rights reserved.
Registered as a limited company in England and Wales under company number: 17317113. Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.