WHITEPAPER

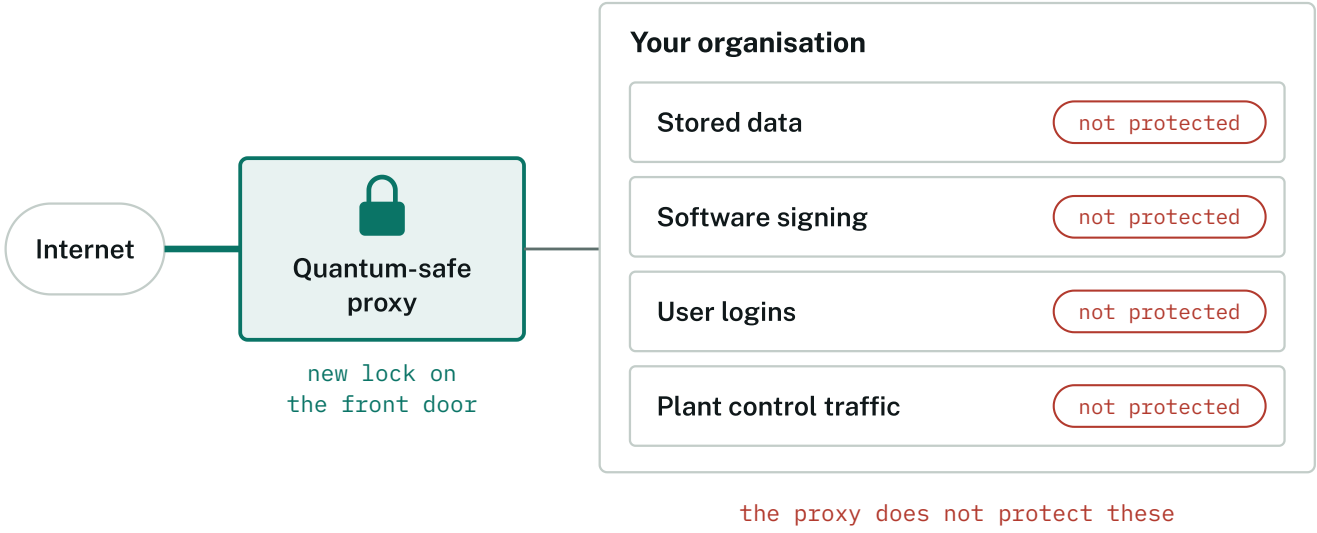
Beyond the Proxy

What a quantum-safe internet boundary leaves exposed

Many organisations are making their internet connections quantum-safe by placing a new proxy in front of them. A proxy is a server that sits between the internet and your systems and handles their encryption. It protects one thing: traffic crossing the internet boundary. Everything behind it stays as exposed as before. For example, in December 2025, a coordinated attack in Poland exploited unprotected internal systems despite internet-facing VPN devices being in place, allowing attackers to disrupt plant operations (CERT Polska, 2026). Figure 1 shows the idea in one picture. This paper shows what the proxy leaves out, and how to find each exposure on your network.

ClaveQ · Quantum Clave Ltd 9 sections · ~15 min read Accurate as of October 2026

FIGURE 1 · A NEW LOCK ON THE FRONT DOOR



A quantum-safe proxy changes the lock on the front door. The systems behind it remain unchanged.

01 *Executive summary*

AT A GLANCE

- A quantum-safe proxy protects only data transmitted over the internet boundary, but it does not safeguard internal or local network traffic within the organisation.
- Stored data, software signing, user logins and plant control traffic stay exposed.
- Keep the proxy, and pair it with discovery — a process that systematically identifies and inventories where cryptography is applied across your systems — so you can see what exposures remain unaddressed.

A quantum-safe proxy upgrades the encryption on internet connections. It is one of the quickest, lowest-risk steps an organisation can take towards post-quantum readiness. On its own, it is a partial fix. It protects only traffic that crosses the internet boundary, and only while the proxy stays in the path.

Four elements remain unaddressed:

Stored data. Databases and backups still use pre-existing encryption methods, leaving stored data vulnerable to future quantum attacks.

Code and firmware signing. These processes remain unupgraded, so attackers could exploit legacy signing algorithms once quantum capabilities emerge.

User login tokens. Tokens continue to be signed with conventional mechanisms, leaving them exposed to signature forgery in a quantum era.

Internal network traffic. Control communications inside industrial environments are not routed through the proxy, so they remain unprotected.

Treating the proxy as a complete solution therefore leaves multiple high-value attack surfaces exposed.

Keep the proxy. It is the right first move for internet-facing connections. Pair it with **discovery**: a full inventory of where cryptography is applied, in what forms, and what assets it secures. That shows the residual exposures the proxy alone will not address, so they are understood rather than assumed away.

02 *Attackers are already inside critical networks*

Harvest now, decrypt later means copying encrypted data today and keeping it until a quantum computer can decrypt it. Copying does not require a quantum computer to exist. It needs an attacker with access to the traffic and the patience to keep it. State-sponsored groups already sit inside the networks and providers that carry long-lived, sensitive traffic. Their access lasts years.

CISA ADVISORY AA24-038A · FEB 2024

Volt Typhoon

PRC government-backed actors pre-positioned themselves on the IT networks of US communications, energy, transportation and water organisations, in some cases for at least five years. The agencies assessed this as preparation for disruptive or destructive attacks in the event of a major crisis or conflict with the United States.

Source: cisa.gov/aa24-038a ↗

NSA · CISA · FBI & PARTNERS ADVISORY AA25-239A · AUG 2025

Salt Typhoon

PRC government-backed actors, operating since at least 2021, target the backbone and provider-edge routers of major telecommunications providers and modify them to keep long-term access.

Source: cisa.gov/aa25-239a ↗

NSA · FBI · CISA · JAPAN ADVISORY AA23-270A · SEP 2023

BlackTech

A PRC-linked group modifies router firmware undetected and exploits routers' domain-trust relationships to pivot from international subsidiaries to headquarters in Japan and the US.

Source: cisa.gov/aa23-270a ↗

NCSC-UK & PARTNERS ADVISORY AA26-113A · APR 2026

China-nexus covert device networks

China-nexus actors, including Volt Typhoon and Flax Typhoon, hide the origin of their traffic behind covert networks of compromised routers and IoT devices. One, Raptor Train, infected more than 200,000 devices worldwide in 2024.

Source: cisa.gov/aa26-113a ↗

No quantum computer was used in any of these campaigns, and no cryptographically relevant one exists yet. However, the advisories say that attackers already have access to critical network infrastructure. Specifically, the Salt Typhoon advisory says the actors passively collect packet captures from specific ISP customer networks, and in some instances enable traffic mirroring on compromised routers. Such access is the gap a proxy leaves open. While quantum-safe proxies protect encrypted data in transit at the network boundary, they cannot stop an attacker who already has access to internal network infrastructure from

capturing that data. If traffic were captured and kept, it would remain vulnerable to future quantum decryption, so organisations would be exposed once quantum computers become viable. These findings show the precondition for 'harvest now, decrypt later': attackers already hold long-term access to networks that carry sensitive traffic, and one group has captured traffic from customer networks. They do not show that anyone is keeping that traffic to decrypt it later, so treat that step as a plausible risk, not a documented campaign.

Five exposed points, and the public evidence

Figure 2, in section 03, marks five points where attackers can reach what a quantum-safe proxy leaves exposed. Public incident reports show markers 1 and 2 in use today, and show attackers capturing traffic on compromised routers, though not traffic behind a proxy. None of the incidents below involved breaking encryption. Once inside the boundary, the attackers found control protocols with no built-in security, and in Poland a default login.

On 29 December 2025, coordinated attacks in Poland hit at least 30 wind and solar farms, a large combined heat and power (CHP) plant and a manufacturing company. CERT Polska found that every affected farm had an internet-facing VPN device that accepted logins without multi-factor authentication. At a smaller CHP plant that heats about 50,000 residents, the attackers moved from a wind farm's VPN, over the distribution grid operator's private mobile data network, into the plant's control network. Their way in was a PLC with its own cellular modem, still on its default administrator login. They connected to three Siemens PLCs using the S7 protocol, and plant staff reported that the PLCs were put into STOP. A steam turbine and the plant's process-water treatment stopped. The outage was short, and no customer lost heat or electricity.

Attackers are patient, and learn the plant first. In Poland they scanned the private network from 18 December and opened S7 sessions to the three PLCs on 25 December, four days before the shutdown. In one confirmed compromise, Volt Typhoon actors collected "diagrams and documentation related to OT equipment". Unencrypted control traffic hands a listener the same map: which devices exist, what they control and how they talk. Defenders can listen to the same traffic first, and see what an attacker would see.

Ukraine shows the same pattern. On 23 December 2015, attacks on three electricity distribution companies cut power to about 225,000 customers for several hours. The attackers appear to have had access more than six months before, and US ICS-CERT reported that they operated breakers remotely, partly over VPN. In December 2016, an attack on a transmission substation cut power to part of Kyiv for about an hour. ESET and Dragos linked it to Industroyer, malware built to send commands in substation control protocols. In April 2022 a successor, Industroyer2, was aimed at high-voltage substations; CERT-UA reported the attack was prevented. In January 2024, attackers sent Modbus commands, which normally carry no built-in security, to the controllers of a district heating company in Lviv, probably using FrostyGoop malware. The company supplied heating to over 600 apartment buildings, and customers were without heating for almost two days in sub-zero temperatures.

03 *What a proxy protects, and what it leaves alone*

A TLS-terminating proxy ends each client's TLS connection and opens a new one to the service behind it. Placing such a proxy between the internet and a public-facing service and configuring it for hybrid **X25519MLKEM768** key exchange strengthens security. In this hybrid scheme, both a classical key exchange algorithm (X25519) and a post-quantum algorithm (ML-KEM) run in parallel; the result is a session key derived from both, so the traffic is protected unless both algorithms are broken. Even if one — such as X25519 — becomes vulnerable to quantum attacks, the session remains secure because of ML-KEM's strength. Traffic harvested on that path is then protected against later decryption by a quantum computer. Chrome on desktop has offered this key exchange by default since version 131, and Cloudflare supports it. X25519 on its own is not quantum-safe. The ML-KEM half is the part that matters.

The protection ends at the proxy. Four kinds of exposure sit outside it, and there is one deployment risk to plan for.

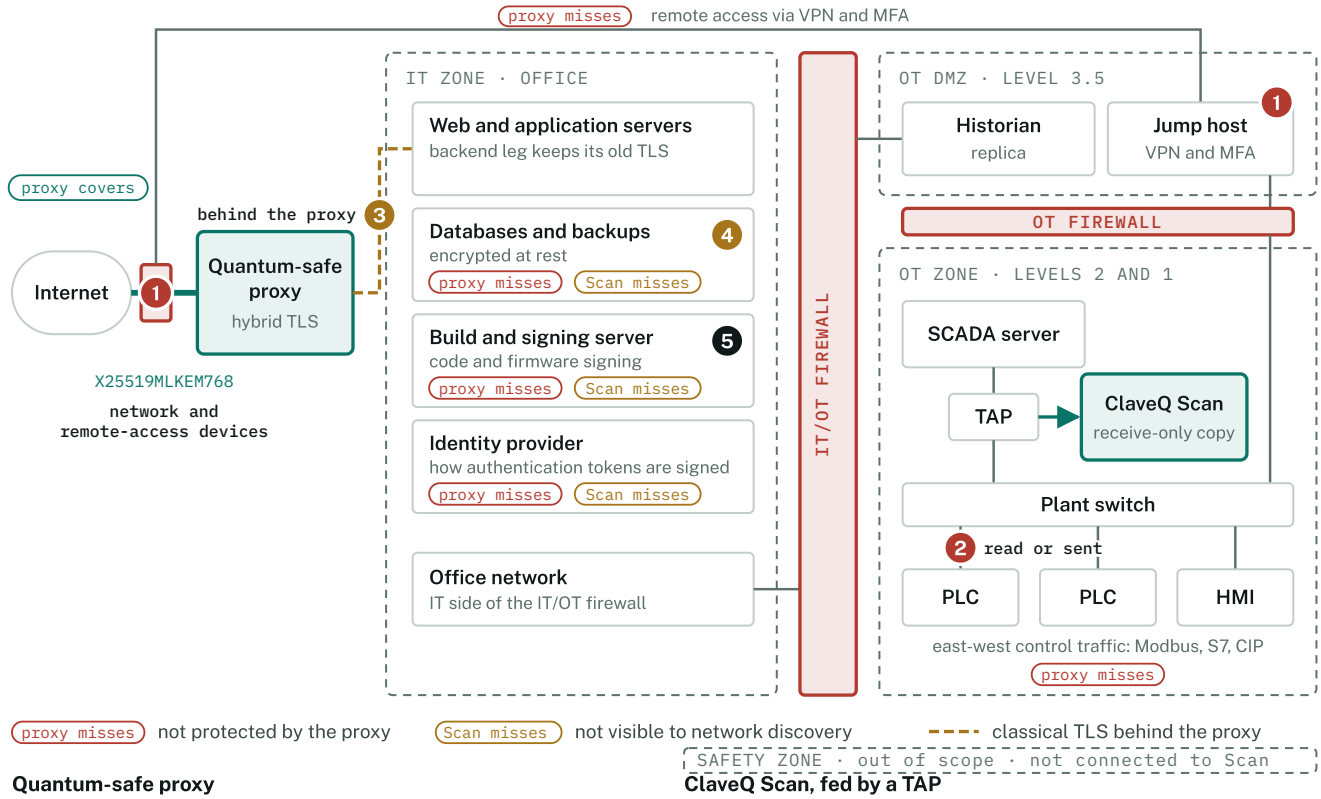
Data at rest and long-retention archives

To clarify the limitations of proxy-based protection, distinguish between data in transit and data at rest, especially in the context of long-term data retention. A proxy protects data in transit. However, data encrypted at rest with keys wrapped or exchanged using RSA or ECC — such as data stored in databases or backups — remains just as vulnerable. Consider a healthcare organisation that must retain patient records confidentially for decades. If those archives rely solely on classical encryption, a future quantum adversary could later decrypt sensitive information that was harvested today. This scenario shows why, for long-term confidentiality, the unmitigated risk to data at rest can outweigh the risks addressed by upgrading data in transit.

Internal, east-west traffic

Network engineers use the terms 'north-south' and 'east-west' to distinguish different types of data movement: 'north-south' traffic refers to data that moves across the boundary between an organisation and external networks (such as the internet). In contrast, 'east-west' traffic refers to data exchanged internally between systems within the same network or site. Most proxies are positioned at the internet boundary, meaning they primarily manage and secure north-south traffic. So these proxies do not affect communications within the organisation's internal network (such as service-to-service calls and database connections). In industrial environments, messages exchanged between the supervisory control and data acquisition (SCADA) system and programmable logic controllers (PLCs), as well as communications between multiple PLCs, are considered east-west traffic and do not traverse the internet-facing proxy. Widely used industrial protocols like Modbus TCP and DNP3 generally do not employ Transport Layer Security (TLS) encryption.

FIGURE 2 · WHAT A QUANTUM-SAFE PROXY COVERS VS WHAT NETWORK DISCOVERY SEES



Quantum-safe proxy

Covers: TLS between the internet and the proxy.

Misses: data at rest, code signing, how tokens are signed, and all east-west and OT traffic.

ClaveQ Scan, fed by a TAP

Sees: cryptography negotiated on the tapped link, including OT protocols that carry no encryption.

Does not see: data at rest, code signing, token signatures, or any link it is not given a copy of.

KEY · EXPOSED POINTS, BY WHEN THE ATTACK PAYS OFF

NOW, NO QUANTUM COMPUTER NEEDED

1. **Network and remote-access devices.** Routers, firewalls, VPNs and cellular routers, used to copy traffic or as the way in, including links that bypass these firewalls.
2. **Plant control traffic.** Unencrypted traffic (Modbus, S7 and similar) that an attacker could read, or commands sent from a foothold inside.

HARVEST NOW, DECRYPT LATER

3. **Behind the proxy.** Traffic sent on with classical encryption, recorded and kept until a quantum computer can decrypt it.
4. **Stored data.** Databases and backups with RSA- or ECC-wrapped keys, copied today.

AFTER A QUANTUM COMPUTER EXISTS

5. **Software and firmware signing.** Signatures forged.

Simplified for illustration. The firewalls do not change the encryption on connections that cross them.

- **What the TAP sees:** only the SCADA server's link to the plant switch, so Scan sees that server's traffic with the PLCs, the HMI and the OT DMZ.
- **What it does not see:** HMI-to-PLC and PLC-to-PLC traffic (needs a mirror port or more TAPs), the second path on a redundant network, and stored data or signing (4 and 5).
- **What it does not do:** detect intrusions or block attacks.
- **Not drawn:** Level 3 site systems, the Poland-case link that routes around the firewalls, the safety system's interfaces (its zone is drawn, out of scope), and the engineering workstation and standby

SCADA server.

What if the proxy sits at the IT/OT boundary?

It can, and it upgrades TLS that crosses between office and plant. Because it opens a new connection on the plant side, that leg still runs on whatever the plant device supports. Control traffic between PLCs and SCADA normally stays inside the plant, out of the proxy's sight.

Code signing and firmware

Nothing on a network path changes software updates, firmware images, or build artefacts signed with RSA or ECDSA. Migrating a signing pipeline to ML-DSA, SLH-DSA, or, for firmware, the hash-based schemes LMS and XMSS starts with knowing which certificate authorities, hardware security modules (HSMs), and build systems are involved. Discovery is significant here because identifying all existing signing mechanisms and their dependencies is a prerequisite for effective migration. Without a comprehensive inventory, organisations risk leaving vulnerable legacy signatures unaddressed, undermining overall cryptographic resilience.

Authentication and identity

JSON Web Tokens (JWTs), SAML single sign-on assertions, Kerberos tickets and the HSMs that hold root keys work independently of the transport layer. A proxy can carry a token over a quantum-safe channel. It cannot change how the token was signed.

Handshake size and compatibility

Post-quantum key-exchange material is far larger than classical: an ML-KEM-768 encapsulation key is 1,184 bytes, against 32 bytes for an X25519 public key. A TLS ClientHello that offers a post-quantum key share no longer fits in a single packet, and some servers and middleboxes fail when it arrives in two. Test client and network-path behaviour before you switch on post-quantum cryptography (PQC) at a proxy.

04 *Discovery versus proxy remediation*

The two do different jobs. A proxy changes what is negotiated on a connection. Discovery tells you what exists to be changed, and which parts of it a proxy at the internet boundary cannot reach.

EXPOSURE	DISCOVERY (ALL METHODS COMBINED)	PROXY REMEDIATION
Internet-edge TLS transport	Identifies legacy cipher suites and key exchange in use	Offers hybrid or PQC TLS directly
Cryptographic inventory (CBOM)	Maps the cryptographic assets in use	No visibility
Data at rest	Flags long-retention encrypted assets	None
Code and firmware signing	Finds the signing certificates and CAs in scope	None
Internal, east-west and OT traffic	Extends the inventory behind the internet boundary	Usually out of path

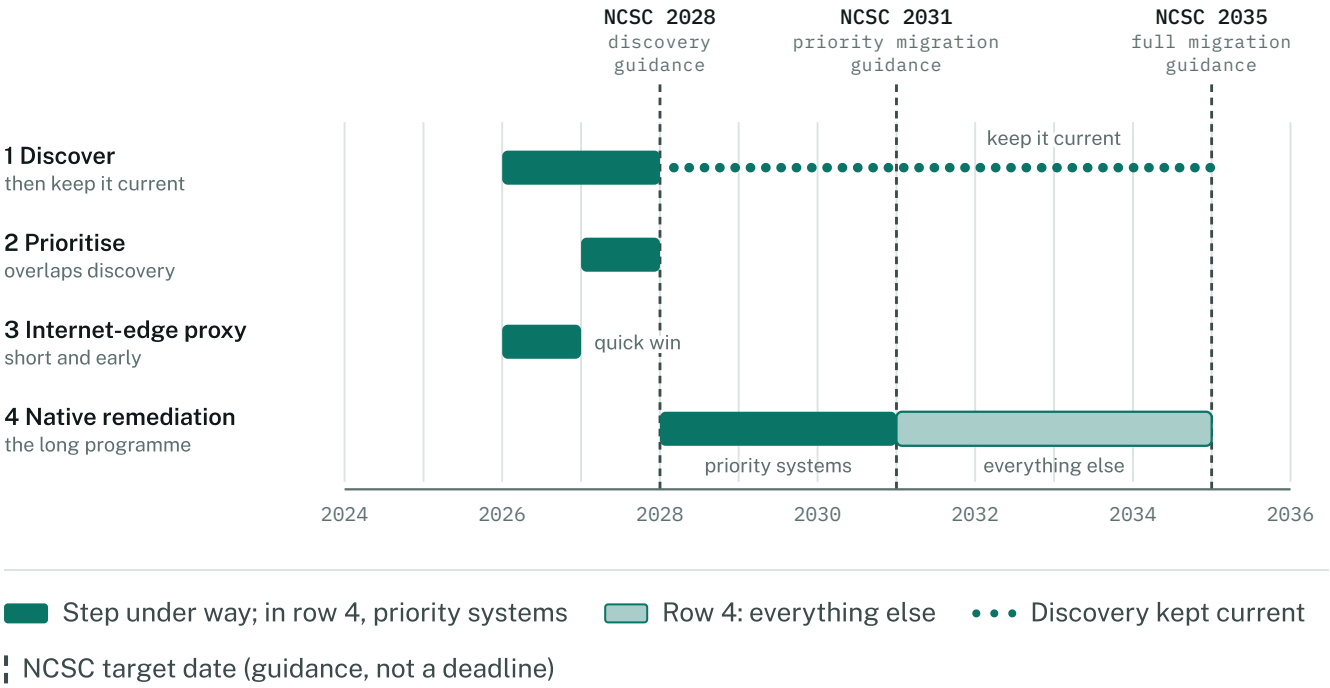
No single discovery method fills the whole middle column. Section 06 sets out which method reaches which row.

To decide what comes first, use the test usually credited to Michele Mosca. Take X, the number of years the data must stay secret. Add Y, the years it will take to migrate the system that protects it. Compare the total with Z, the years until a cryptographically relevant quantum computer exists. If $X + Y$ is greater than Z, data harvested today will still matter when it can be read. Migration for that system is already late. Discovery tells you which systems fail the test. A proxy is one of several fixes you apply once you know.

Figure 3 shows the order. The proxy is a short early step, and native remediation is the long programme that runs to 2035 on the illustrative timeline.

05 *A staged migration plan*

FIGURE 3 · THE PROXY IS A SHORT EARLY STEP; NATIVE REMEDIATION IS THE LONG PROGRAMME



Illustrative. Real timings depend on your inventory.

01

Discover.

Build a cryptographic inventory, or Cryptography Bill of Materials (CBOM), encompassing network traffic, certificates, and, where applicable, code-signing and data-at-rest assets. Developing a full CBOM presents several practical challenges, including identifying all cryptographic mechanisms in heterogeneous and legacy environments, mapping encryption use across distributed systems, and ensuring visibility into assets that may operate outside centralised management. For instance, a CBOM might reveal that a backup database uses RSA-2048. NIST's draft transition plan (NIST IR 8547 ipd, November 2024) deprecates RSA at 112 bits of security strength after 2030 and disallows it after 2035. Addressing these challenges often requires a combination of automated scanning tools, manual audits, and coordination with multiple stakeholders to ensure accuracy and completeness. For each finding, record the algorithm in use and how long the data it protects must remain confidential, as this information is critical for planning effective migration strategies.

02

Prioritise by data lifespan.

Apply the $X + Y > Z$ test above. Long-retention, high-sensitivity data goes to the front of the queue, no matter how safe it looks today.

03

Deploy a proxy at the internet boundary.

Terminate hybrid PQC TLS (X25519 with ML-KEM-768) for internet-facing services. This measure is quick to deploy and reduces harvest-now-decrypt-later risk for that class of traffic; however, teams should first assess compatibility along the entire network path, as some servers and middleboxes may not support the larger handshake sizes introduced by post-quantum key exchange.

04

Remediate natively, over time.

Key remediation actions include upgrading backend services, hardware security modules (HSMs), data-at-rest encryption, and signing authorities to utilise NIST-approved algorithms (ML-KEM, ML-DSA, and SLH-DSA) as identified through the cryptographic inventory. Organisations should also consider defence-in-depth strategies, such as network segmentation and hardware-based security enclaves, while maintaining compensating controls for systems that remain dependent on quantum-vulnerable cryptography during a phased migration. Prioritise remediation measures based on the inventory findings and select them with operational needs, system compatibility, regulatory requirements, and overall risk tolerance in mind.

> **The recurring mistake** is treating step 3 as the whole programme. The proxy is the quickest step to complete and the easiest to show a board, which is why it gets mistaken for completion. Steps 1 and 2 tell you how much is left.

06 *Network discovery, and where Scan fits*

Cryptographic discovery splits across layers. Each needs a different method.

Firmware and binary static analysis
Shows what shipped, which may differ from what runs.

Receive-only, protocol-aware network capture
Reads the cryptography negotiated on the wire, across IT and industrial protocols. This is Scan's layer.

Generic deep-packet inspection
The same capture method, usually tuned for asset and behaviour visibility. Cryptographic detail varies by product.

Agent- and filesystem-based IT inventory
Strong for certificates and keys on disk in enterprise IT and cloud. NIST SP 800-82 warns that host-based agents can affect the performance of OT devices and calls for extensive testing first.

Scan takes a copy of the traffic from a network TAP or, where a TAP cannot be fitted, from a switch mirror (SPAN) port. It decodes IT and OT protocols, including those that were never encrypted, down to the cipher suite and key exchange in use. It reads the server certificate where the protocol sends it in the clear, as TLS 1.2 and earlier do. TLS 1.3 encrypts the certificate, so Scan cannot see it there and rates those sessions from the key exchange. Each connection whose cryptography Scan can read gets a rating such as quantum-safe, quantum-vulnerable or unencrypted. Connections it cannot read are reported as unobserved, a coverage statement rather than a finding. Scan also reports how much of the traffic it saw in both directions, as a guide to how complete the capture was.

The output is a **Cryptography Bill of Materials** in CycloneDX 1.7, the version Ecma International publishes as ECMA-424 (2nd edition). Our test suite checks that output against the official CycloneDX 1.7 schema on every code change. Findings map, as advisory context for your compliance team, to IEC 62443, NERC CIP (North America), CNSA 2.0 and the EU Cyber Resilience Act. They are not a compliance determination. Migration phases are set against the NCSC timeline.

Why a TAP, and what we measured

Plant security teams ask one question first: can this device ever transmit onto my process network? A software setting is a weak answer. A TAP gives a physical one, because its monitor port is receive-only by design. As ClaveQ Scan is in private beta, validation has been conducted on a dedicated bench rig rather

than a live production site. Capture through a TAP has been tested on that rig. Mirror-port (SPAN) configurations and virtualised sensor deployments, such as NUC or VM environments, remain to be tested.

So the monitor port is receive-only by design, and Scan reads the same handshakes the endpoints negotiate. That guarantee covers the monitor path only. The appliance also has a management port; on a site, connect it to a separate network that you choose. The TAP carries a risk of its own too. It sits in the cable, so fitting it means a short outage, and some TAPs drop the link when they lose power. NIST SP 800-82 raises the same concern about in-line network probes. We do not call this arrangement passive without that caveat. On a live site, plan the fitting as a managed change. Choose a TAP specified to pass traffic without power, and expect that a copper link may still drop briefly while it renegotiates. Give the TAP a power supply of its own, separate from the appliance. Where no outage is acceptable, a switch mirror (SPAN) port avoids breaking the cable, but it is still a configuration change: test it first, raise it through change control, and check that the switch can mirror the link without dropping packets. A mirror port is not receive-only by design. Whether a mirror port can transmit depends on the switch configuration.

Sized for an industrial computer

Our appliance runs on a DIN-rail industrial computer. Its memory use grows with the size of the capture, so size the hardware to the traffic you expect.

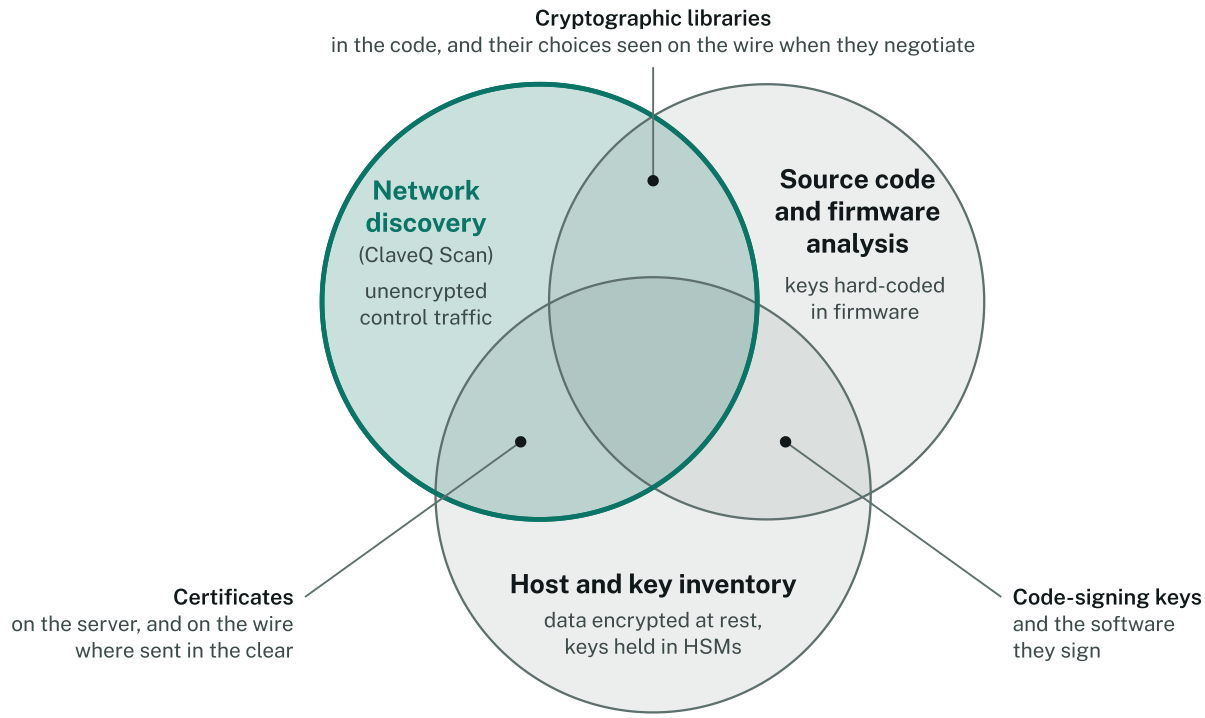
What one testbed network carried

We also decoded a capture from SWaT, the water-treatment testbed run by iTrust at the Singapore University of Technology and Design, recorded in December 2019. SWaT is a research testbed, so this says nothing about any operator's estate, though it shows the kind of finding an inventory turns up.

Scan is one layer of the picture. It does not inventory data encrypted at rest or the keys that sign your code. It shows what a proxy cannot: the cryptography running across this network today, and how much of it is already exposed. That matters most where agents and active scanning are least welcome, which includes the water and energy sectors named in the Volt Typhoon advisory.

Figure 4 shows three ways to find cryptography: network discovery, source-code and firmware analysis, and host and key inventory. Each finds what the others miss, and they overlap where they share certificates, cryptographic libraries and signing keys.

FIGURE 4 · THREE WAYS TO FIND CRYPTOGRAPHY, AND WHERE THEY OVERLAP



Network discovery (ClaveQ Scan): this set only, not the other two

Illustrative. Scan covers one set: the cryptography on the links it is given a copy of. It does not replace source-code and firmware analysis or a host and key inventory.

07 *The regulatory backdrop*

Government guidance sets the same order of work. The UK NCSC's migration guidance sets three target dates: by 2028, define migration goals, carry out a full discovery exercise and build an initial plan; by 2031, complete the highest-priority migration activities; by 2035, complete migration of all systems, services and products. These are guidance, and they assume you know what you are migrating well before 2031.

NIST published its first three post-quantum standards in August 2024: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA). With these standards, approved algorithms are largely defined, enabling organisations to plan migrations with clarity on cryptographic options. However, the main challenge now is practically identifying where legacy, quantum-vulnerable algorithms remain in use across complex infrastructures. This uncertainty requires discovery and inventory work to ensure critical systems and data are not left reliant on quantum-vulnerable cryptographic schemes, so organisations need to map existing cryptographic deployments alongside the adoption of new standards.

Under the EU Cyber Resilience Act, manufacturers must report actively exploited vulnerabilities from 11 September 2026, and the main obligations apply from 11 December 2027. In the UK, the Cyber Security and

Resilience (Network and Information Systems) Bill was before the House of Lords, at report stage, in October 2026. An inventory of the cryptography in use is the starting point for the NCSC timeline, and it makes the CRA's security requirements easier to evidence.

08 Conclusion

A quantum-safe proxy is a sound first step for internet-facing connections, and it should go in early. It upgrades the encryption that crosses the boundary, but it does not protect stored data, code signing, login tokens or the traffic inside your network.

Closing the rest of the gap takes three steps. First, find where cryptography is used across the network, storage, signing and identity, so you know what the proxy leaves exposed. Second, rank that exposure by how long the data must stay confidential, and start with the data that must last longest. Third, replace the classical algorithms over time, working towards the NCSC's guidance dates of 2028, 2031 and 2035.

None of the incidents in Section 02 involved breaking encryption. The near-term work is to see what is exposed today and reduce it, while planning post-quantum protection for the long-lived data.

Keep the proxy. Pair it with discovery. Then plan the migration in stages, starting with the data that cannot wait.

09 Glossary

CBOM (Cryptography Bill of Materials)
An inventory of the cryptography in use, where it runs and what it protects.

Cryptographically relevant quantum computer
A quantum computer powerful enough to break the encryption most systems use today.

CycloneDX
An open standard file format for listing software components, including cryptography.

East-west traffic
Traffic between systems inside one site, such as a control server polling a controller.

Forward secrecy
Stealing a server's long-term key later does not let anyone decrypt sessions recorded earlier.

Harvest now, decrypt later
Copying encrypted data today and keeping it until a quantum computer can decrypt it.

HMI (human-machine interface)
The screen operators use to watch and run a plant process.

Mirror (SPAN) port

A switch port set to send out a copy of traffic from other ports.

ML-DSA

A post-quantum method for digital signatures, standardised by NIST in 2024.

ML-KEM

A post-quantum method for agreeing encryption keys, standardised by NIST in 2024.

OT DMZ

A buffer network between office and plant, holding systems both sides need to reach.

PLC (programmable logic controller)

A rugged computer that directly controls plant equipment such as pumps and valves.

Post-quantum cryptography (PQC)

Encryption methods designed to stay secure against a future quantum computer.

Proxy

A server between the internet and your systems that handles their encryption.

SCADA

The control-room system that monitors plant controllers and sends them commands.

TAP (test access point)

A small device fitted to one cable that copies its traffic to a monitor.

TLS

The standard encryption that protects web and many other network connections.

---

10 Sources

#	PUBLISHER	DOCUMENT	DATE	SUPPORTS
1	CISA, NSA, FBI and partners	Advisory AA24-038A, Volt Typhoon ↗ (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)	7 Feb 2024	§02 Volt Typhoon pre-positioning and OT diagrams collected in one confirmed compromise; §06 water and energy sectors
2	NSA, CISA, FBI and partners	Advisory AA25-239A, Salt Typhoon ↗ (https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a)	27 Aug 2025	§02 Salt Typhoon router access and packet capture
3	NSA, FBI, CISA, NPA and NISC	Advisory AA23-270A, BlackTech ↗ (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a)	27 Sep 2023	§02 BlackTech router firmware and domain trust
4	NCSC-UK and partners	Advisory AA26-113A, China-nexus covert networks ↗ (https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a)	23 Apr 2026	§02 covert device networks and Raptor Train

#	PUBLISHER	DOCUMENT	DATE	SUPPORTS
5	CERT Polska (NASK)	Energy Sector Incident Report, 29 December 2025 ↗ (https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/)	30 Jan 2026	§02 Poland: scale of the attacks; VPN without multi-factor authentication at every affected farm
6	CERT Polska (NASK)	Follow-up report on the December 2025 energy sector incident ↗ (https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/)	8 Aug 2026	§02 smaller CHP plant: route in, PLC on its default login, reconnaissance dates, S7 sessions, PLCs in STOP, outcome
7	E-ISAC and SANS ICS	Analysis of the Cyber Attack on the Ukrainian Power Grid (archived copy) ↗ (https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf)	18 Mar 2016	§02 Ukraine 2015: access more than six months before; outages of several hours
8	US ICS-CERT (now CISA)	IR-ALERT-H-16-056-01, Cyber-Attack Against Ukrainian Critical Infrastructure ↗ (https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01)	25 Feb 2016	§02 Ukraine 2015: three distribution companies, about 225,000 customers, remote operation, partly over VPN
9	ESET	Industroyer: Biggest threat to industrial control systems since Stuxnet ↗ (https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/)	12 Jun 2017	§02 control protocols with no built-in security; Ukraine 2016: part of Kyiv without power for an hour; Industroyer built to send commands
10	Dragos	CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations (archived copy) ↗ (https://nsarchive.gwu.edu/sites/default/files/documents/3869008/Dragos-CRASHOVERRIDE-Analyzing-the-Threat-to.pdf)	Jun 2017	§02 Ukraine 2016: transmission substation, 17 December 2016
11	ESET	Industroyer2: Industroyer reloaded ↗ (https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/)	12 Apr 2022	§02 Ukraine 2022: Industroyer2 attempt against high-voltage substations
12	CERT-UA	Sandworm (UAC-0082) cyberattack on Ukrainian energy facilities, INDUSTROYER2 and CADDYWIPER (CERT-UA#4435), in Ukrainian ↗ (https://cert.gov.ua/article/39518)	12 Apr 2022	§02 Ukraine 2022: attack prevented
13	Dragos	Impact of FrostyGoop ICS Malware on Connected OT Systems (intelligence brief) ↗ (https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology)	Jul 2024	§02 Ukraine 2024: January 2024; over 600 apartment buildings supplied with heating; almost two days; sub-zero temperatures
14	Dragos	How to Protect Against FrostyGoop: ICS Malware Targeting Operational Technology ↗ (https://www.dragos.com/blog/protect-against-frostygoop-ics-malware-targeting-operational-technology/)	23 Jul 2024	§02 Ukraine 2024: Lviv; Modbus commands sent to heating controllers; FrostyGoop likely used
15	MITRE ATT&CK	Campaign C0041, FrostyGoop Incident ↗ (https://attack.mitre.org/campaigns/C0041/)	Accessed 12 Oct 2026	§02 Ukraine 2024: district heating company; Modbus commands; loss of heating

#	PUBLISHER	DOCUMENT	DATE	SUPPORTS
16	SANS Institute	What's the Scoop on FrostyGoop: The Latest ICS Malware and ICS Controls Considerations ↗ (https://www.sans.org/blog/whats-the-scoop-on-frostygoop-the-latest-ics-malware-and-ics-controls-considerations/)	9 Aug 2024	§02 Modbus normally has no built-in security
17	Google Security Blog	A new path for Kyber on the web (Chrome 131, ML-KEM) ↗ (https://security.googleblog.com/2024/09/a-new-path-for-kyber-on-web.html)	13 Sep 2024	§03 Chrome default hybrid key exchange
18	Cloudflare	Post-quantum cryptography (X25519MLKEM768) ↗ (https://developers.cloudflare.com/ssl/post-quantum-cryptography/)	Accessed 11 Oct 2026	§03 Cloudflare support for X25519MLKEM768
19	NIST	FIPS 203, Table 3: ML-KEM key and ciphertext sizes ↗ (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf)	Aug 2024	§03 handshake size (ML-KEM-768)
20	IETF	RFC 7748, X25519 ↗ (https://www.rfc-editor.org/rfc/rfc7748)	Jan 2016	§03 handshake size (X25519)
21	tldr.fail	Servers that fail on large post-quantum ClientHellos ↗ (https://tldr.fail/)	Accessed 11 Oct 2026	§03 handshake size and compatibility
22	Mosca, M.	Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy 16(5), 38–41 ↗ (https://doi.org/10.1109/MSP.2018.3761723) (preprint: Cryptology ePrint Archive 2015/1075 ↗ (https://eprint.iacr.org/2015/1075))	Sep 2018	§04 X + Y > Z test; §05 step 2
23	NCSC	Timelines for migration to post-quantum cryptography ↗ (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines)	20 Mar 2025	§05 Figure 3 markers; §07 NCSC target dates 2028, 2031, 2035
24	NIST	IR 8547 ipd, Transition to Post-Quantum Cryptography Standards (initial public draft) ↗ (https://doi.org/10.6028/NIST.IR.8547.ipd)	Nov 2024	§05 CBOM example; Table 2 RSA and ECDSA transition dates. Draft: not final
25	NIST	SP 800-82 Rev. 3, Guide to Operational Technology Security ↗ (https://csrc.nist.gov/pubs/sp/800/82/r3/final)	Sep 2023	§06 host-based agents and in-line probes in OT
26	Ecma International	ECMA-424, CycloneDX 1.7 (2nd edition) ↗ (https://ecma-international.org/publications-and-standards/standards/ecma-424/)	Dec 2025	§06 CBOM format
27	Guarino, Faramondi, Setola, Flammini	Hardware-in-the-loop water distribution testbed (WDT) dataset, IEEE DataPort ↗ (https://doi.org/10.21227/rbvf-2h90)	4 May 2021	§06 appliance sizing test (testbed capture used)
28	iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design	SWaT dataset ↗ (https://www.sutd.edu.sg/itrust/itrust-labs/datasets/)	Capture Dec 2019	§06 SWaT control-network findings

#	PUBLISHER	DOCUMENT	DATE	SUPPORTS
29	NIST	First 3 finalised post-quantum encryption standards ↗ (https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards)	13 Aug 2024	§07 FIPS 203, 204 and 205
30	European Commission	EU Cyber Resilience Act ↗ (https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)	Updated 7 Sep 2026	§07 CRA dates
31	UK Parliament	Cyber Security and Resilience (Network and Information Systems) Bill ↗ (https://bills.parliament.uk/bills/4035)	Status at 9 Oct 2026	§07 UK Bill stage

See it on your own network

Scan is in private beta for operational-technology and critical-infrastructure operators in water, energy, healthcare and manufacturing. It takes its copy of traffic from a network TAP or a mirror port, and you get a standards-based CBOM you can act on.

See the papers at claveq.com →

COPYRIGHT AND TERMS OF USE

Copyright	© 2026 Quantum Clave Ltd, trading as ClaveQ. Company no. 17340121. All rights reserved, except as below.
Sharing	You may copy and share this paper in full and unmodified, with this notice intact. Please do not edit it, remove our name, or sell it.
Quotations and sources	Quotations from published sources are reproduced with attribution for the purposes of review and comment. Named products and organisations belong to their owners; mention does not imply endorsement.
Datasets	The SWaT dataset is provided by iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design, and is credited where it is used in this paper.
Trade mark	ClaveQ® is a registered trade mark of Quantum Clave Ltd in the United Kingdom.
Disclaimer	This paper is general information, accurate as of October 2026. It is not legal, regulatory or compliance advice. Check current guidance before acting on it.

© 2026 Quantum Clave Ltd, trading as ClaveQ · Company no. 17340121

Accurate as of October 2026 · claveq.com