The Future Pillars of Cyber Security: Post-Quantum Cryptography and Zero Trust Architecture

I. Executive Summary

This report compares two new technologies in cyber security: Post-Quantum Cryptography (PQC) and Zero Trust Architecture (ZTA). PQC is a mathematical algorithm designed to protect global data privacy against the fast-approaching threat of quantum computers.[1] ZTA, on the other hand, is a big-picture security structure that deals with current risks caused by traditional network boundaries disappearing due to cloud use and remote work.[2]

The analysis finds that PQC and ZTA work together and need each other. While PQC solves the future encryption problem, ZTA provides the necessary setup, clear view, and continuous management required to successfully put PQC algorithms into place across complicated business networks. Organisations aiming for strong, long-term security must include PQC migration planning in their ZTA strategies, viewing both as essential, company-wide change programs rather than small technical projects.

II. Introduction to Emerging Cyber Security Technologies

A. Contextualising the Modern Threat Landscape

The traditional security models, like the “castle and moat” model that rely on trusting users and devices inside the company network, no longer work effectively because of modern operations.[3] The wide use of cloud computing, many Internet of Things (IoT) devices and the rise of remote work have broken down old network boundarys.[2] This change means security must move closer to the data and users, no matter where they are.

At the same time, a new serious threat is facing the core of digital security. The potential arrival of powerful quantum computers. These devices are expected to be able to run programs that could easily break the standard public-key encryption (like RSA and ECC) that protects almost all digital information today.[1] This risk is made worse by the "harvest now, decrypt later" (HNDL) attack. Here, attackers collect huge amounts of currently encrypted data, storing it in the hope that a quantum computer will be able to decrypt it later.[1]

B. Selection Rationale: PQC and ZTA

To handle these two problems, I have chosen Post-Quantum Cryptography and Zero Trust Architecture for this report.

PQC is changing fast, shown by the finalisation of its main standards by the U.S. National Institute of Standards and Technology (NIST) in 2024.[6] Although not yet used everywhere, PQC is a necessary basic change that will affect every system that uses public-key encryption.

ZTA, explained in documents like NIST Special Publication 800-207, is quickly replacing older network boundary models. With government support and wide acceptance by large cloud providers like Google, Azure and AWS, ZTA offers a smart way to achieve immediate operational strength.[7] Comparing PQC and ZTA shows us how cybersecurity strategies must grow in both technical and management areas.[9]

III. Post-Quantum Cryptography (PQC): A Foundational Layer

A. Overview of the Technology: What is PQC?

PQC, also called quantum-resistant cryptography, involves new mathematical algorithms designed to be safe from attacks by both regular computers and future quantum computers.[1] It is relevant to know that PQC is different from quantum cryptography (QC). QC uses quantum physics and needs specialised hardware to secure only specific communication links. PQC, however, uses regular computer hardware to run new, hard maths problems that powerful quantum machines are not expected to be able to solve.[4]

PQC efforts mainly focus on algorithms based on problems that are hard for both types of computers, mostly using structured lattices.[11] In 2024, NIST released the final versions of the first three PQC standards [6]:

- **ML-KEM:** This lattice-based code, from the Kyber family, is meant to replace public-key systems like RSA and ECC for creating security keys. It has small keys and runs fast.[11]
- **ML-DSA:** This code, from CRYSTALS-Dilithium, is the main standardised algorithm for digital signatures.[6]
- **SLH-DSA:** This code, from Sphincs+, uses a different, hash-based maths approach. It is an important backup method in case the main lattice-based codes have security issues.[6]

B. Current State of Development and Adoption (PQC)

The NIST standards mark a key moment, turning PQC from a theory into a required step for security. Governments and organisations are increasingly being told to create full lists of their encryption use and detailed PQC change plans with set deadlines.[12]

Governments and security leaders around the world are treating the HNDL threat seriously.[13] The need for action is clear in pilot programs, such as those run by the UK's National Cyber Security Centre (NCSC). These programs, which check major consulting firms like IBM and Capgemini, are helping industries find all their encryption types and create migration plans. This shows a move towards big, co-ordinated deployment efforts.[13] Large internet companies, like Cloudflare, have already reached goals where most user-based traffic is protected by post-quantum encryption, showing that early, large-scale use is possible today.[15]

C. Applications in Cyber Security (PQC)

The main use of PQC is to protect data for the long term. PQC ensures that highly important, long-lasting sensitive data such as patient records, financial information, or government secrets are secure against the HNDL attack model.[1] If this data is captured today, PQC makes sure it remains private even when a powerful quantum computer is built in the future.

Beyond general data protection, PQC is vital for securing critical parts of the internet, including the core of Public Key Infrastructure (PKI), the security layer for web communications (TLS/SSL), and Virtual Private Networks (VPNs). Also, because lattice-based schemes rely on certain maths concepts, they are key to new privacy technologies like Fully Homomorphic Encryption (FHE), which lets people perform calculations on encrypted data without needing to unlock it first.[11]

D. Advantages and Limitations (PQC)

A main advantage of PQC is that it is evidently quantum resistant, offering long-term security by using maths problems that are too challenging for quantum machines.[11] Also, speed tests of the standardised algorithms have proven to be effective. Codes like Kyber (ML-KEM) are noticeably faster than older types like RSA and ECDH in certain jobs, especially key exchange speed. This makes them good choices for PQC TLS protocols.[16]

However, moving to PQC has big challenges. The whole process is complicated and costly, frequently called one of the most complex change programs the industry has faced in decades.[12]

PQC often causes bandwidth and speed trade-offs because its security keys and signatures are much larger than ECC's. These larger data sizes use up more bandwidth and require network and infrastructure changes, especially where computing resources are limited.[13]

A huge practical problem is the immature vendor market. While the algorithms are standardised, the related technology, such as Hardware Security Modules (HSMs), database encryption tools, and TLS libraries, does not yet fully support PQC. This creates problems when different systems need to work together (interoperability issues) in multi-cloud or hybrid networks, and it increases the risk of being stuck with one vendor (vendor lock-in) if organisations use non-standard, custom solutions sold as quantum-safe.[12]

E. Security Implications and Challenges (PQC)

The biggest challenge in PQC migration is not the maths of the algorithms, but the lack of organisational management and clear visibility of all encryptions used. Many organisations, especially in areas like finance, have a scattered encryption setups and no single list of all cryptographic items.[12] Without this centralised view, finding and replacing every vulnerable algorithm across old systems becomes a "near-impossible task".[12] This lack of encryption 'cleanliness' means that even with standardised solutions available, organisations cannot effectively map the necessary updates to their systems.

This problem makes the risk posed by regulatory deadlines against an uncertain threat timeline worse.[12] Regulators are demanding PQC transition plans, but the lack of a clear date for when powerful quantum computers arrive causes some institutions to hesitate and delay.[1] Since changing encryption across an entire business can takes years, delaying planning increases the risk of missing compliance deadlines and being exposed to HNDL attacks for longer.

Finally, there is a shortage of the right skills. The small number of engineers globally with hands-on experience in lattice-based or hash-based cryptography means that organisations face serious talent shortages.[12] This shortage forces many to rely on outside help or vendor tools, which can increase the risk of using non-standard methods or becoming locked into one vendor.

IV. Zero Trust Architecture (ZTA): A Strategic Framework

A. Overview of the Technology: What is ZTA?

Zero Trust Architecture is a strategic security model built on the basic rule of "never trust, always verify".[2] It stops giving automatic trust to users or devices inside the network boundary, instead requiring strict and continuous identity checks for every access request, no matter where the person or device is.[2]

ZTA uses flexible, rule-based systems that look at factors like user identity, device health, and application permissions to make instant access decisions.[7] The ZTA plan, as defined by NIST, is built on three main ideas [2]:

1. **Continuously Verify:** Access is never given automatically; the system must constantly check and authorise every attempt to connect to a resource.
2. **Limit the Blast Radius:** Using micro segmentation, ZTA limits how different parts of the network, applications, or individual tasks can talk to each other. This ensures that if a security breach happens, the attacker's ability to move sideways and cause wide damage is severely reduced.[2]
3. **Assume Breach:** ZTA works based on the clear assumption that some systems are already compromised or that a breach will happen. Security controls therefore focus on stopping the spread, reducing the damage, and responding quickly, instead of just preventing the initial entry.[21]

B. Applications in Cyber Security (ZTA)

ZTA is the required security structure for today's decentralised business. It safely supports staff working from anywhere and systems spread across multiple clouds, solving the security gap left by the death of the traditional network boundary.[19]

ZTA is very good at reducing current, serious threats [2]:

- **Ransomware:** By making sure that breaking one part (like running bad code) doesn't automatically break the other (like stealing an identity), ZTA keeps things safer.
- **Supply Chain Attacks:** ZTA reduces the risk from unmanaged devices or outside users with high-level access by forcing strict checks on the device's health before allowing access.[7]
- **Insider Threats:** Constantly checking and watching user behaviour helps find and reduce threats from internal people who are compromised or malicious.[2]

Additionally, ZTA fits perfectly with strict global rules like GDPR, HIPAA, and PCI-DSS.[21] By requiring constant checking, encryption, logs of activity, and detailed access control, ZTA helps organisations stay compliant and avoid penalties.[22]

C. Advantages and Limitations (ZTA)

The main benefit of ZTA is better security by making the system harder to attack and limiting the damage if a breach occurs.[19] By bringing together many security and network tasks into one system, ZTA can also lead to less complexity and cost over time, making IT simpler and management easier.[23]

Despite these positives, deploying ZTA is hard. High initial setup and integration costs are a big problem, especially for Small and Medium Enterprises (SMEs).[22] Implementing a full ZTA means spending heavily on upgrading infrastructure and identity systems, often requiring the replacement or complex setup of older systems that don't work with flexible access rules.[20]

The model only works if it overcomes major complexity and operational challenges.[20] Organisations must first get a full, clear view of all data, resources, and work processes across the entire environment to correctly identify everything that needs access control and monitoring.[20] Also, the strict, continuous security checks needed by ZTA can cause staff to push back and create operational friction, especially when job roles are complicated or change often, leading to access being denied.[20]

D. Security Implications and Challenges (ZTA)

How well ZTA works depends a lot on the quality of its basic data (identity, device health, and asset list). A key security risk comes from the ZTA Policy Engine (PE). The PE is the 'brain' of the architecture, making instant decisions based on rules and threat information.[24] While ZTA tries to decentralise control, if the Policy Engine is not set up correctly, it could become a single point of failure (SPOF).[24] If a centralised PE is compromised, it could potentially give access everywhere, undoing the benefit of micro segmentation.

Additionally, putting ZTA in place naturally reveals and worsens existing problems in a business's asset and management methods. If the list of assets or encryption is incomplete, which is a common issue in the PQC context [12], the ZTA policy engine cannot enforce the necessary 'least-privilege' access, making its micro segmentation much less effective. Building reliable and secure trust checking remains a hard problem in decentralised ZTA, requiring systems to combine different data sources for accurate, continuous security checks.[24]

E. Case Studies or Examples (ZTA)

ZTA is no longer just a theory; it is now a standard for secure work. Many important U.S. government departments use ZTA principles and vendors for their security, following strict federal rules like the Secure Cloud Computing Architecture (SCCA) standard and FIPS 140-2 compliance.[26]

In business, major cloud companies have fully internalised ZTA. Google famously started using Zero Trust after a serious government-sponsored attack, making it a deep part of its systems. Microsoft Azure uses its position as a major identity provider to offer a key Zero Trust 'policy engine' system.[8] This wide use by large cloud companies confirms ZTA's importance in securing cloud-based work. ZTA's flexibility is also shown by new research looking at how it can work with blockchain to secure interactions in new digital places, such as the Metaverse.[27]

V. Comparative Analysis: ZTA and PQC

A. Fundamental Differences in Nature and Scope

PQC and ZTA deal with security at completely different parts of the technology setup.

PQC is a basic encryption standard. It focuses on the mathematical heart of security, the algorithms. PQC's reach is global and affects all systems, making sure the content of data and communication methods (like TLS) are secure, no matter the network or cloud design.[11]

ZTA is a strategic security plan. It focuses on setting rules and structure. ZTA is about how resources are accessed, managing who can log in, what they can do, and how the network is split up, all based on the context.[29] It acts as a security model that sets the rules for how things should be done, while PQC provides the strong encryption tools used within that model.

B. Comparison Matrix

Comparative Analysis of PQC and ZTA

Criteria	**Post-Quantum Cryptography (PQC)**	**Zero Trust Architecture (ZTA)**
Primary Objective	Long-term data privacy and integrity against quantum computers (HNDL threat).[1]	Limiting the area an attack can affect and the damage inside current decentralised networks.[19]
Core Mechanism	Mathematical complexity (lattice problems).[11]	Continuous identity verification, micro segmentation, and minimum access rights.[2]
Implementation Scope	Deep technical layer (Cryptography, Protocols, Hardware Security Modules (HSMs)).	Company-wide rules, identity management, and network splitting.[7]
Timeline Urgency	Strategic, long-term preparation (years of change required before Q-day).[1]	Immediate need driven by current cloud and remote work threats. [2, 23]
Required Agility	Cryptographic Agility (ability to rapidly swap encryption codes).[30]	Policy Agility (ability to rapidly adjust access controls based on context).[24]

C. Similarities and Shared Principles

Despite their differences, PQC and ZTA share key ideas needed for modern security. Both technologies are built on an assumption of compromise. PQC assumes today's strong encryption will eventually be broken by future quantum abilities, requiring an active change now.[5] ZTA also assumes the network boundary is already compromised or that a breach will happen, leading it to check every request constantly.[21]

Both also need high levels of flexibility and continuous modernisation. PQC requires 'crypto agility', the ability to easily change encryption codes and libraries as new standards appear or old ones are broken.[30] ZTA demands 'policy agility', the ability to quickly change access rules based on changes in the threat environment and user behaviour.[24]

D. Potential Synergies and Conflicts

The way ZTA and PQC work together is a key development in cybersecurity.[31] PQC is the what (the security required), and ZTA is the how (the system and structure for delivery).

Synergies

1. ZTA Helps PQC Happen: Moving to PQC is a complex, long-term business change that needs a full list of all encryption and centralised control over how encryption works.[12] A good ZTA implementation forces organisations to fix these exact management weaknesses. By requiring the ID of every resource to enforce micro segmentation, ZTA accidentally creates the necessary organisational maturity, clear view, and standardised control structure needed for successful PQC deployment.[20] The flexibility and 'crypto agility' that are part of a true ZTA are basic steps for PQC to protect endpoints, applications, and network traffic.[30]

2. PQC Makes ZTA's Security Stronger: ZTA needs strong encryption to protect important data everywhere (stored or moving).[7] PQC directly improves the Data Security part of ZTA by making sure the encryption used cannot be broken by a quantum computer.[5] So, ZTA makes the 'harvest' part harder (by restricting access and movement), and PQC makes the 'decrypt' part harder (by strengthening the encryption itself).[5]

Conflicts

The main conflict is speed overhead. ZTA's constant checks and detailed policy checks already slow things down a little. PQC, especially because of its larger key and signature sizes, can add more delays or processing demands in some applications or older systems.[5] Applications designed long ago might not cope with the extra computing load from complex, multi-layered encryption needed for both Zero Trust checks and quantum resistance.[5] Security teams must balance the complexity of the algorithms (to maximise security strength) against the required speed targets, as procedures that are too complex can slow the system down.[28]

VI. Conclusion and Recommendations

A. Synthesis of Findings

Post-Quantum Cryptography and Zero Trust Architecture are essential improvements for the future of cybersecurity. PQC addresses the basic threat to encryption from quantum computing, requiring a smart, active change to protect long-lived data from HNDL attacks. ZTA addresses the immediate, structural threats from working in decentralised ways, providing a necessary structure for detailed access control and containing breaches.

The successful move to PQC depends on the good organisational practices and structural flexibility that a solid ZTA implementation provides. By combining these two new technologies, organisations can handle both immediate operational risks and long-term future threats at the same time, building a single, lasting security foundation.

B. Recommendations for Integration and Future Strategy

Based on the technical needs, organisational issues, and ways they work together, here are the recommendations for combining PQC migration into a ZTA strategy:

1. **Focus on Encryption Inventory and Discovery:** Include the work of finding all encryption use directly in the ZTA planning stage. This uses the ZTA need for complete visibility of resources to create a full list of all vulnerable encryption instances, focusing on systems with the most valuable data first, before applying PQC protection.[5]
2. **Make Crypto Agility a ZTA Policy Rule:** Ensure the ZTA Policy Engine is built to be cryptographically flexible. The system must support hybrid encryption (old codes alongside PQC codes) during the transition and allow for fast, standardised changes to

algorithms (like updating Kyber versions) as NIST makes changes and the vendor market grows.[17]

3. **Manage Speed Trade-offs with Specific Testing:** Acknowledge the possible combined effect of ZTA checks and PQC complexity. Closely test how PQC codes affect speed in busy or resource-limited parts of the ZTA network. Security rules must find the right balance between maximising encryption strength and keeping application speed and delay times acceptable.[28]
4. **Reduce Single Points of Failure in the Security Brain:** While ZTA requires centralised control of the policy, the parts that feed into it should be decentralised. Lower the risk of the Policy Engine being a single point of failure by tightly segmenting the network around the PE and using decentralised systems for trust checking to get continuous, reliable data input.[24]
5. **Keep Business-Wide Regulatory Alignment:** Treat both ZTA implementation and PQC migration as essential, compliance-driven programmes. Following the ZTA plan (NIST SP 800-207) and the PQC migration standards (NIST FIPS 204/205) ensures a consistent and standardised approach across the entire security setup.[6]

Works cited

1. New Draft White Paper | PQC Migration: Mappings to Risk Framework Docs | NIST, accessed on November 6, 2025, https://www.nist.gov/news-events/news/2025/09/new-draft-white-paper-pqc-migration-mappings-risk-framework-docs
2. What is Zero Trust? - Guide to Zero Trust Security - CrowdStrike, accessed on November 6, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/
3. Zero Trust Architecture vs. Traditional Perimeter Security: What's the Difference? - Akitra, accessed on November 7, 2025, https://akitra.com/zero-trust-architecture-vs-traditional-perimeter-security/
4. What Is Post-Quantum Cryptography? | NIST, accessed on November 7, 2025, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography
5. Zero Trust and PQC Build a Stronger Security Foundation - GDIT, accessed on November 6, 2025, https://www.gdit.com/perspectives/latest/zero-trust-and-pqc-build-a-stronger-security-foundation/
6. NIST Releases First 3 Finalized Post-Quantum Encryption Standards, accessed on November 7, 2025, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
7. Adopting Zero Trust Principles with CISA's Maturity Model - Zscaler, accessed on November 7, 2025, https://www.zscaler.com/blogs/product-insights/adopting-zero-trust-principles-cisa-s-maturity-model
8. Zero Trust Security: The Business Benefits And Advantages - Forrester, accessed on November 8, 2025, https://www.forrester.com/zero-trust/
9. Emerging Cybersecurity Trends & Technologies - EC-Council University, accessed on November 6, 2025, https://www.eccu.edu/blog/the-latest-cybersecurity-

technologies-and-trends/

10. Post-quantum cryptography (PQC) - Google Cloud, accessed on November 7, 2025, https://cloud.google.com/security/resources/post-quantum-cryptography
11. What Is Post-Quantum Cryptography (PQC)? A Complete Guide - Palo Alto Networks, accessed on November 9, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc
12. PQC Migration Challenges & Compliance Risks for Financial ..., accessed on November 10, 2025, https://www.cryptomathic.com/blog/pqc-migration-challenges-compliance-risks-for-financial-institutions
13. Eight firms blessed by the NCSC for PQC migration planning - The Stack, accessed on November 7, 2025, https://www.thestack.technology/eight-firms-blessed-by-the-ncsc-for-post-quantum-cryptography-overhauls/
14. NCSC shares update on Post-Quantum Cryptography pilot scheme - techUK, accessed on November 8, 2025, https://www.techuk.org/resource/ncsc-shares-update-on-post-quantum-cryptography-pilot-scheme.html
15. State of the post-quantum Internet in 2025 - The Cloudflare Blog, accessed on November 10, 2025, https://blog.cloudflare.com/pq-2025/
16. Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms, accessed on November 8, 2025, https://arxiv.org/html/2503.12952v1
17. A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing - arXiv, accessed on November 10, 2025, https://arxiv.org/html/2508.00832
18. Lattice-Based Cryptography - ISARA Corporation, accessed on November 6, 2025, https://www.isara.com/blog-posts/lattice-based-cryptography.html
19. What Is Zero Trust Architecture (ZTA)? Benefits and Best Practices | Fortinet, accessed on November 10, 2025, https://www.fortinet.com/resources/cyberglossary/zero-trust-architecture
20. The Limitations of Zero Trust Architecture and How to Overcome Them - Terranova Security, accessed on November 6, 2025, https://www.terranovasecurity.com/blog/limitations-of-zero-trust-architecture
21. What Is Zero Trust Architecture? Key Elements and Use Cases - Palo Alto Networks, accessed on November 7, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
22. Zero-Trust Security Market is expected to generate a revenue of USD 124.50 Billion by 2032, Globally, at 16.7% CAGR: Verified Market Research®, accessed on November 8, 2025, https://www.prnewswire.com/news-releases/zero-trust-security-market-is-expected-to-generate-a-revenue-of-usd-124-50-billion-by-2032--globally-at-16-7-cagr-verified-market-research-302603990.html
23. What Is Zero Trust? | Benefits & Core Principles - Zscaler, accessed on November 9, 2025, https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust
24. Zero Trust Architecture: A Systematic Literature Review - arXiv, accessed on November 7, 2025, https://arxiv.org/html/2503.11659v1
25. Theory and Application of Zero Trust Security: A Brief Survey - PMC - PubMed Central, accessed on November 8, 2025,

https://pmc.ncbi.nlm.nih.gov/articles/PMC10742574/

26. Zero Trust Architecture for Government | F5, accessed on November 7, 2025, https://www.f5.com/solutions/use-cases/zero-trust-architecture-for-government
27. Zero Trust Architecture: A Systematic Literature Review - arXiv, accessed on November 8, 2025, https://arxiv.org/html/2503.11659v2
28. Architecture strategies for encryption - Microsoft Azure Well-Architected Framework, accessed on November 9, 2025, https://learn.microsoft.com/en-us/azure/well-architected/security/encryption
29. Security Models and Architecture - TechTarget, accessed on November 7, 2025, https://media.techtarget.com/searchSecurity/downloads/29667C05.pdf
30. Bridging Post-Quantum Cryptography and Zero Trust Architecture - SandboxAQ, accessed on November 9, 2025, https://www.sandboxaq.com/post/bridging-post-quantum-cryptography-and-zero-trust-architecture
31. Beyond Passwords: Evaluating Post-Quantum Cryptography in Zero Trust Architectures - IJIRT, accessed on November 19, 2025, https://ijirt.org/publishedpaper/IJIRT183040_PAPER.pdf