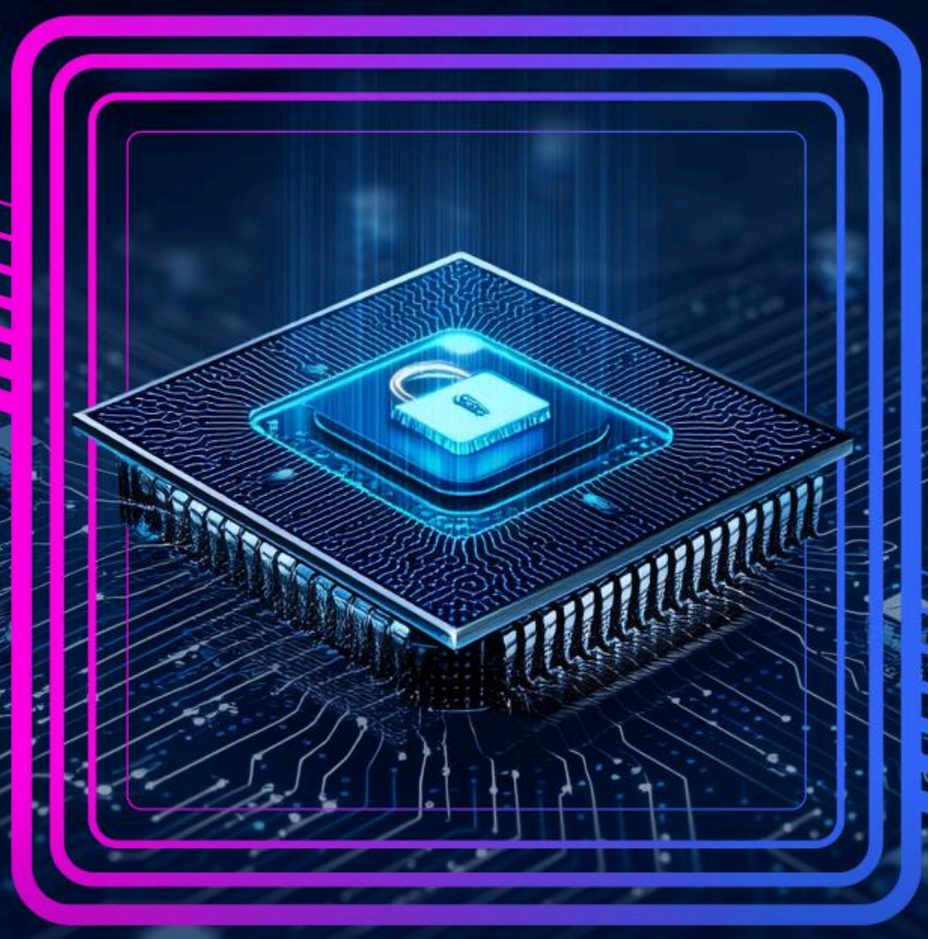
The Quantum Tipping Point



WHAT EVERY CXO SHOULD HAVE ON THEIR RADAR

The greatest risk isn’t what happens when encryption breaks. It's waiting too long to prepare. Here’s how to act now before response options narrow.

THE BUSINESS RISK IS ALREADY HERE

The greatest quantum risk isn’t suddenly going to appear on the day encryption breaks. It's the years of inaction beforehand, happening right now, that pose the biggest threat. Sensitive data stolen today may be decrypted in the future, while post-quantum migration takes years to plan and execute. Waiting for certainty about when quantum disruption will happen means accepting growing exposure as your response options narrow. Organizations that act now can **reduce risk on their terms.** Those that delay may be **forced to respond under pressure.**

The date of disruption is uncertain. The lead time to prepare for it is not.

THE COST OF WAITING EXTENDS BEYOND ENCRYPTED DATA

RISK	BUSINESS IMPACT
CONFIDENTIALITY	Data with long-term value could be exposed years after it is stolen.
TRUST	Compromised digital signatures could erode confidence in critical systems, users and transactions.
COMPLIANCE	Organizations that postpone action may struggle to meet future post-quantum requirements on time.

Three-step framework

Most organizations understand the quantum risk. The challenge is knowing where exposure exists and how quickly it needs to be addressed. This framework helps identify, prioritize and reduce risk before response options narrow and growing disruption becomes harder to manage.

The challenge isn't knowing when quantum disruption will arrive.
It's being ready when it does.

01 **SEE IT**	**GOAL** Identify critical exposure before it becomes a business liability.	**ACTIONS** Map where cryptography is used and identify the systems, assets and dependencies that would be hardest to protect if migration timelines accelerate.	**OUTCOME** Clear visibility into where action (and investment) is needed first.
02 **CONTAIN IT**	**GOAL** Reduce risk while transition is underway to avoid reactive decisions.	**ACTIONS** Prioritize phased migration based on business impact, focusing first on critical data, systems and long-lived information at greatest risk.	**OUTCOME** Reduced exposure and greater control throughout the transition.
03 **SUSTAIN IT**	**GOAL** Build resilience for a future of continual cryptographic change.	**ACTIONS** Design systems with centrally governed, policy-driven cryptography that can be updated without disruptive re-engineering.	**OUTCOME** Long-term agility without repeated transformation or re-platforming projects.

MOVE FROM VISIBILITY TO CONTROL

The question isn't whether to prepare. It’s whether you can afford to wait. Few organizations can. Reduce exposure now, before quantum readiness becomes a costly race against time.

For more information read our whitepaper that translates the quantum threat into a practical executive plan — so your organization can migrate in a controlled, sequenced way before options narrow.

Download now

©2026 Zscaler, Inc. All rights reserved.

zscaler™