PQC vs. QKD

Which shield fits the problem?

DEFAULT	SPECIAL CASE	LAYERED	REMEMBER
PQC for most systems	**QKD on dedicated links**	**Both when justified**	**QKD never replaces PQC**

PQC	QKD	BOTH	NO IMMEDIATE ACTION
New math in ordinary software. Use for portals, VPNs, APIs, cloud services, certificates, and digital signatures. Think: replace RSA/ECC at scale.	Quantum key establishment on a specialized point-to-point link. Use only when dedicated fiber or quantum optical hardware already exists. Think: narrow, physical, specialized.	QKD for the special link plus PQC for endpoint authentication and the rest of the environment. Think: layered protection, not an either/or choice.	Shared-key protection, offline controls, or short-lived credentials may not need early quantum spending. Think: monitor, do not overreact.

THE THREE-QUESTION DECISION TEST

1. What is failing?
If the problem is RSA/ECC in software, certificates, or signatures → PQC.

2. Is there special hardware?
If there is a dedicated quantum link and the goal is detecting interference → consider QKD.

3. What remains outside the link?
Endpoints, authentication, vendors, applications, and certificates still need PQC.

BOTTOM LINE

PQC is the scalable enterprise migration path. QKD is a specialized networking capability. They solve different problems, and QKD still depends on PQC for authentication.