

SECURITY SEMINAR

Quantum-Safe Cryptography



Protecting data in the quantum era

PRESENTED BY
Presenter Name

DATE
2026

CONTACT
hello@yourdomain.in

02 Agenda

01 Introduction

02 Architecture

03 Trends

04 Adoption



**Today's secrets need
protection from
tomorrow's computers.**

Why it matters

04 Overview

- ▶ Most encryption relies on hard maths problems
- ▶ Future quantum computers could break some of them
- ▶ New post-quantum algorithms resist quantum attacks
- ▶ Migration takes years, so planning starts now

KEY IDEA

Data stolen today could be decrypted later.

05 | How it works

1 Inventory

Find where crypto is used

2 Assess

Rank systems by risk

3 Migrate

Adopt new algorithms

4 Test

Verify and monitor

06 | Core components

1

Algorithms

Lattice and hash-based schemes.

2

Standards

New published standards.

3

Agility

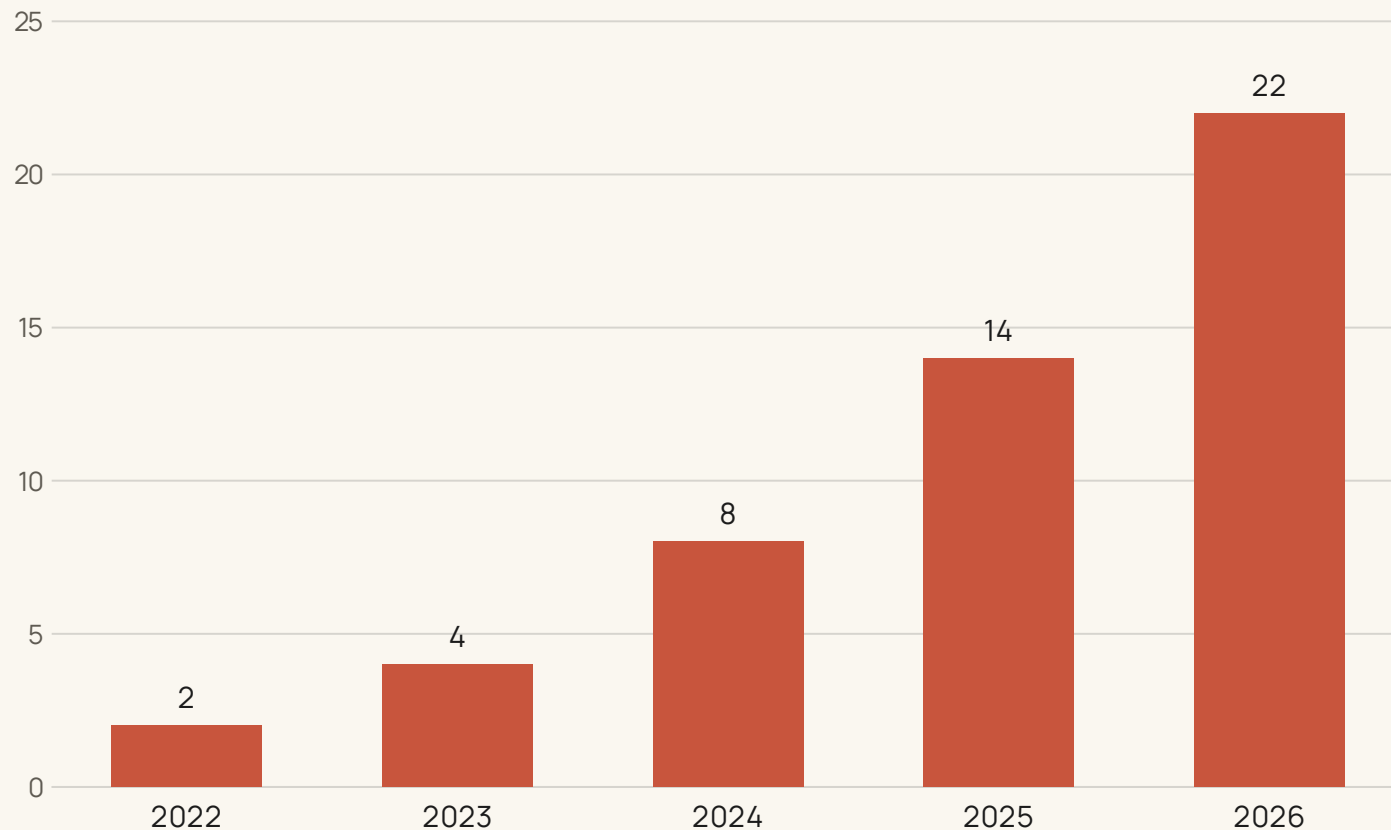
Swap algorithms easily.

07 | Tools and options

Layer	Popular choices	Notes
Key exchange	Post-quantum KEMs	Replace older methods
Signatures	Lattice and hash-based	For certificates
Hybrid	Classical + PQ together	Safe transition

Generic examples; pick what fits your project.

08 Adoption over time



Adoption keeps rising as tools mature (sample data).

Sample data for illustration – replace with your own figures.

09 | Use cases



Image 1

Banking

Secure transactions



Image 2

Government

Long-term secrets



Image 3

Health

Patient records

10 | Benefits and risks

Benefits

- Future-proof security
- Standards available
- Hybrid mode eases transition

vs

Risks

- Larger keys
- Performance overhead
- Complex migration

11 | Best practices

1

Map your crypto

Know every use.

2

Be crypto-agile

Design for change.

3

Start pilots

Test hybrid modes.

12 | Getting started roadmap

Week 1

Learn

Core concepts and a tutorial

Week 3-4

Pilot

One real use case

Week 2

Prototype

Small proof of concept

Month 2

Scale

Standards, monitoring,
training

Questions?

Thanks for your time.

Presenter Name

hello@yourdomain.in

