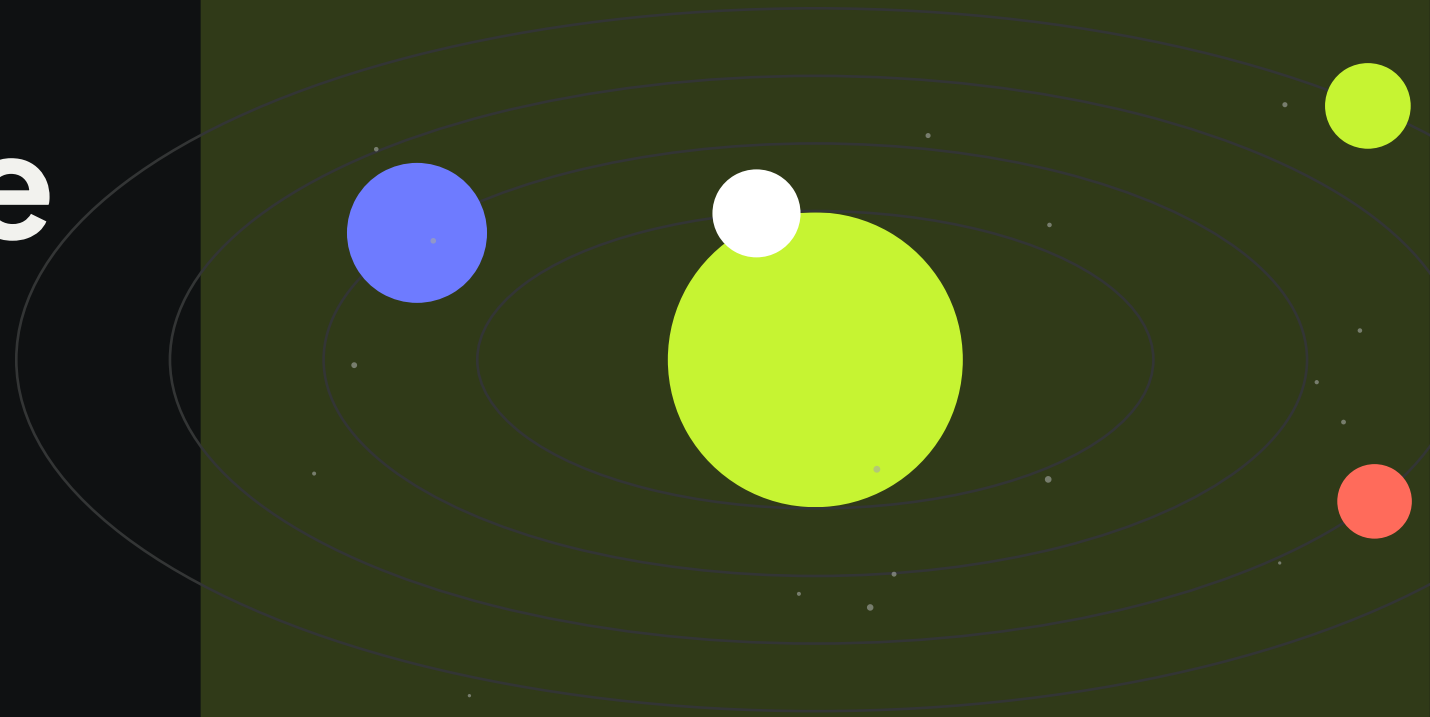


SECURITY SEMINAR

Quantum-Safe Cryptography

Protecting data in the quantum era



PRESENTED BY
Presenter Name

DATE
2026

CONTACT
hello@yourdomain.in



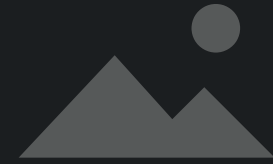
Agenda

01 Introduction

02 Architecture

03 Trends

04 Adoption



Image

SECTION 01

INTRODUCTION

KEY IDEA

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

Why it matters



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

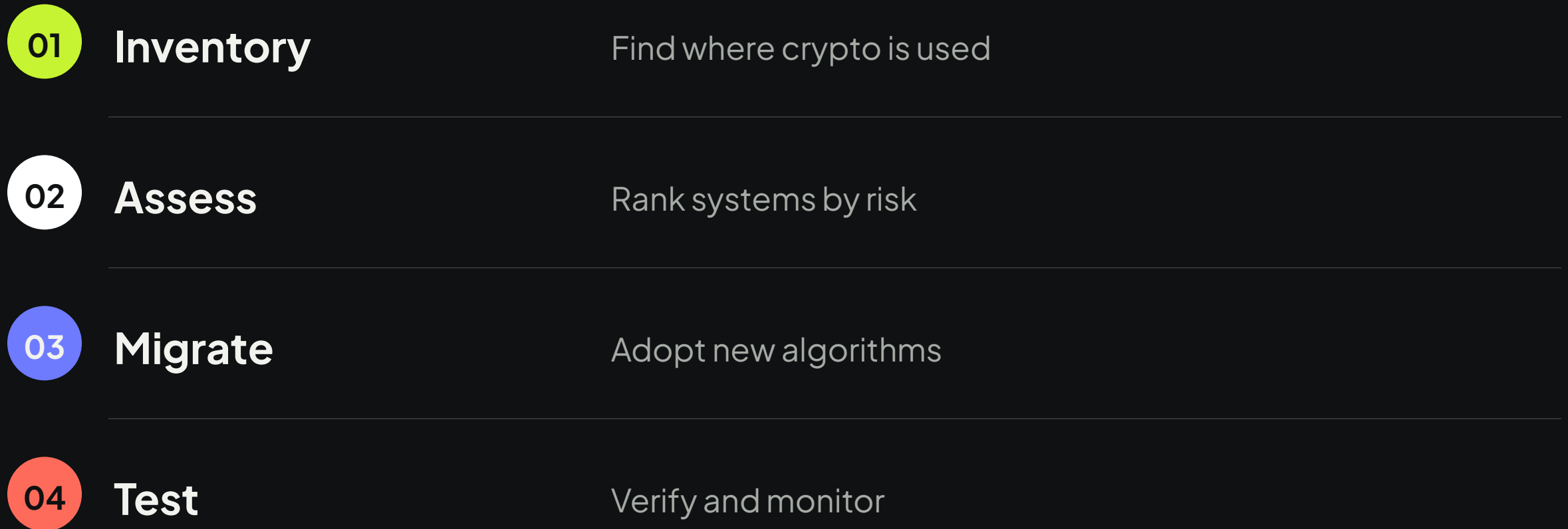
**Data stolen today
could be decrypted
later.**

SECTION 02

ARCHITECTURE



How it works





Core components

01

Algorithms

Lattice and hash-based schemes.

02

Standards

New published standards.

03

Agility

Swap algorithms easily.



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

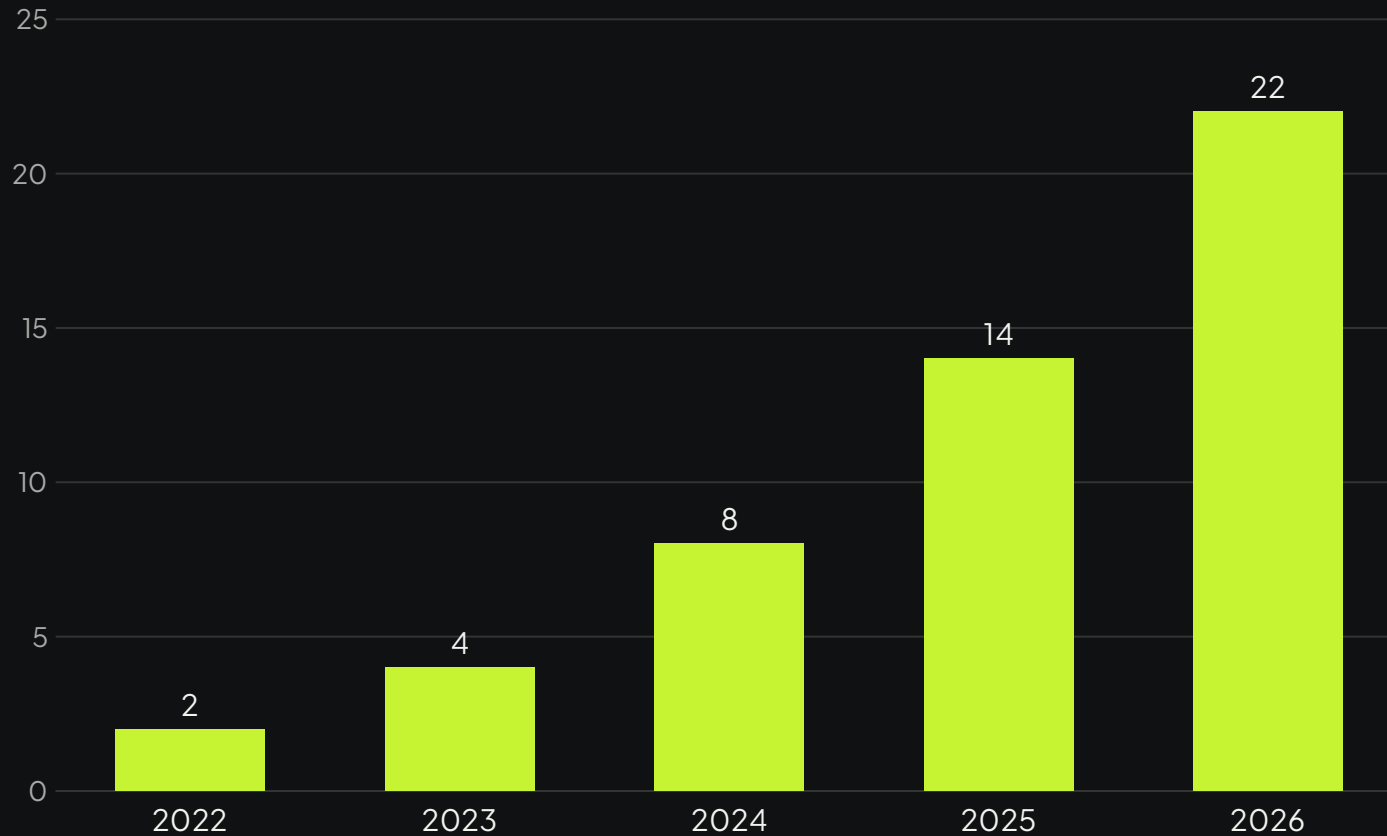
Generic examples; pick what fits your project.

SECTION 03

TRENDS

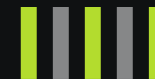


Adoption over time



Adoption keeps rising as tools mature (sample data).

Sample data for illustration — replace with your own figures.



Use cases



Image 1

Banking

Secure transactions



Image 2

Government

Long-term secrets



Image 3

Health

Patient records

SECTION 04

ADOPTION



Benefits and risks

Benefits

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

vs

Risks

- Larger keys
- Performance overhead
- Complex migration



Best practices

01

Map your crypto

Know every use.

02

Be crypto-agile

Design for change.

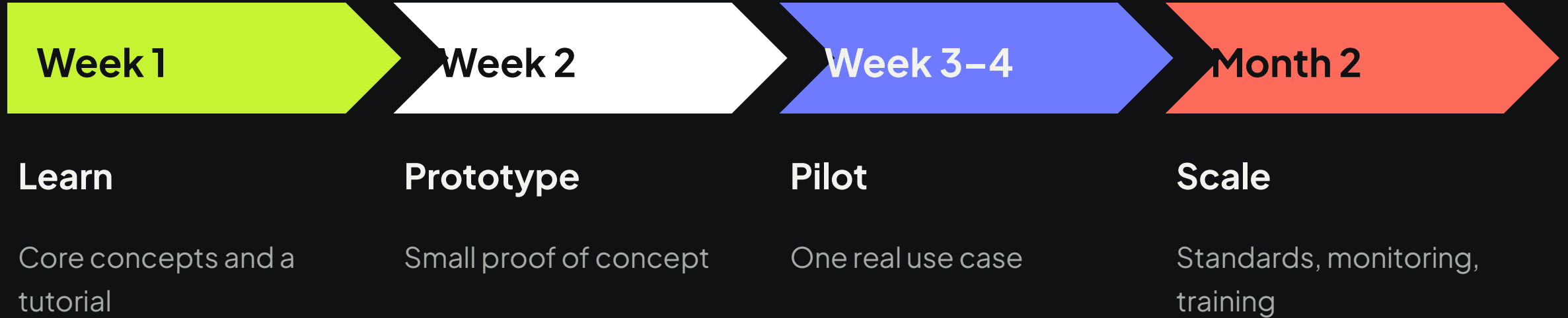
03

Start pilots

Test hybrid modes.



Getting started roadmap



Questions?

Thanks for your time.

Presenter Name

hello@yourdomain.in