

Infrastructure that Defends against Quantum and AI- Powered Threats

Resilient Infrastructure

Semih Kavala
Solutions Engineer, sekavala@cisco.com



AI + Quantum = Attacks at machine speed



AI
accelerates
discovery



Quantum
undermines
encryption



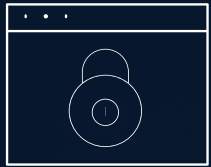
Small cracks
expose full
attack paths

Zero-minute attacks break your Zero-Trust architecture



How do we build
resilient infrastructure?

Enhancing baseline security posture out-of-the-box



Secure use, simplified

Out-of-the-box
secure settings and
proactive risk alerts

*Deprecates then removes
insecure protocols*



Real-time threat response

Immediate shielding
from vulnerabilities without
disrupting operations

*Live Protect “shields” to zero-day
vulnerabilities*

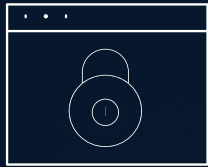


Future-ready resilience

Transparent risk visibility
and post-quantum
cryptography readiness

*Prompts secure data collection with
most secure protocols and methods*

Enhancing baseline security posture out-of-the-box



Secure use, simplified

Out-of-the-box
secure settings and
proactive risk alerts

*Deprecates then removes
insecure protocols*



Real-time threat response

Immediate shielding
from vulnerabilities without
disrupting operations

*Live Protect "shields" to zero-day
vulnerabilities*



Future-ready resilience

Transparent risk visibility
and post-quantum
cryptography readiness

*Prompts secure data collection with
most secure protocols and methods*



Resilient Infrastructure

Secure use, simplified

Secure Use, Simplified

Driving several small but significant improvements for big impact



Simplify Use Cases

Shift the dynamics in our portfolio by increasing default protections



Insecure Features

Removing legacy insecure features with clear migration paths



New Capabilities

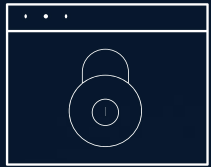
Implement new and modern security capabilities that enrich our product security



Detect & Respond

Ensure platforms provide for higher level protections and monitoring

Enhancing baseline security posture out-of-the-box



Secure use, simplified

Out-of-the-box
secure settings and
proactive risk alerts

*Deprecates then removes
insecure protocols*



Real-time threat response

Immediate shielding
from vulnerabilities without
disrupting operations

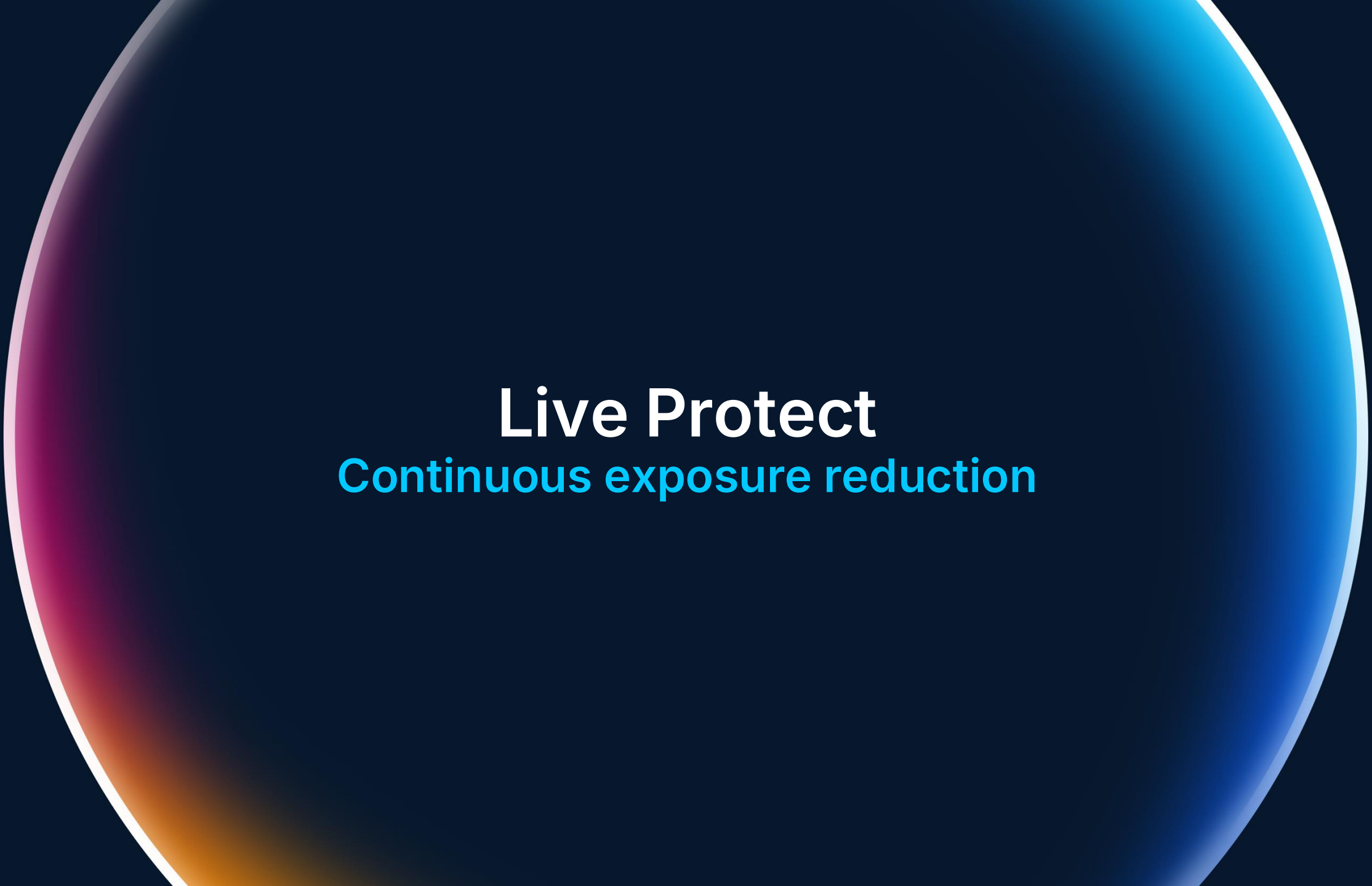
*Live Protect “shields” to zero-day
vulnerabilities*



Future-ready resilience

Transparent risk visibility
and post-quantum
cryptography readiness

*Prompts secure data collection with
most secure protocols and methods*

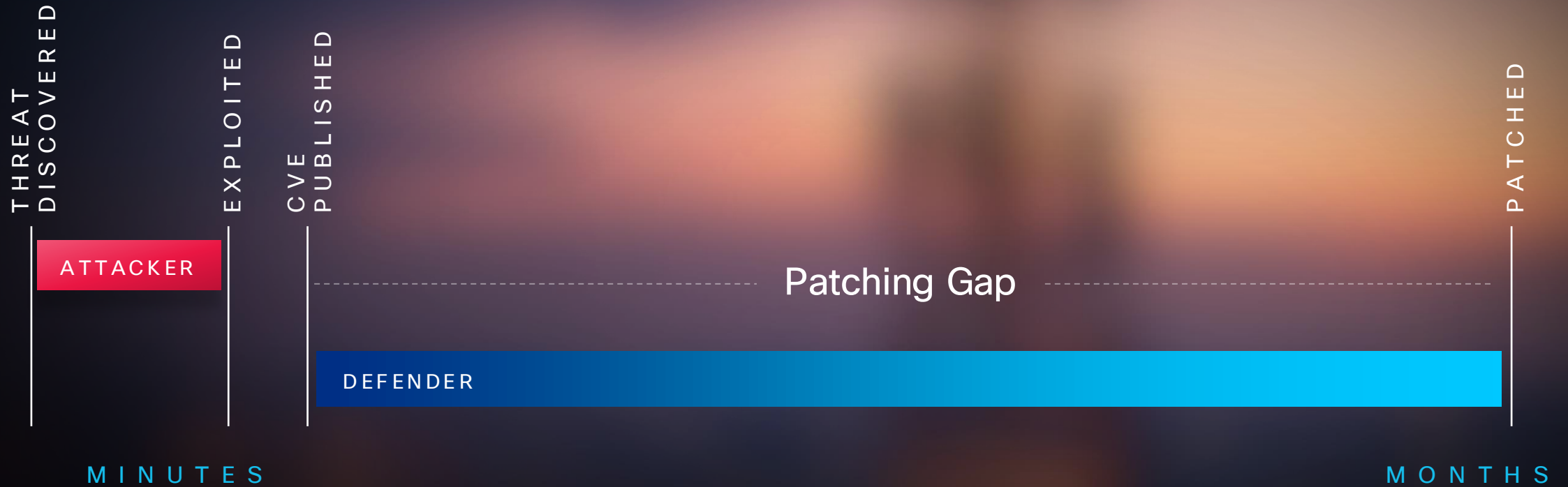


Live Protect

Continuous exposure reduction

AI-speed attacks compress the patching window

Minutes to exploit. Months to patch.



Live Protect



EXTENDING ACROSS CISCO NETWORKING AND SECURITY

Apply policy to
live system

No PSIRT patching
or upgrade

No downtime or
switch reboot

Continuous
re-validation

Live Protect helps teams act before patching is complete

01 Identify affected assets

Critical & High CVEs requiring shield deployment

CVE ▾

CVE-2025-20241: IS-IS Denial of Service Protection	Nexus 3000 Switch Nexus 9000 Series Switch	Aug 27, 2025 12:34:00 PM (PST)
CVE-2024-20400	OmniSwitch6450 S	July 1, 2028 06:00:00 AM (PST)

Devices with vulnerable CVEs

127 ↗ +23% from this week

02 Deploy Vulnerability Shields

Deploy Live Protect ^

Protect mode

Monitor mode

Undeployed critical shields

Firewall

3 shields affecting 354 devices (34%)

Campus switch

All critical shields deployed

Nexus Switching

2 shields affecting 1243 devices (34%)

Campus Gateway

1 shield affecting 18 devices (34%)

03 Monitor Shield activity

Devices with high hitcounts			
Device ID	Device type	Total hitcount	Shield status
sw-bldg-a-floor2-01	Nexus switch 9000	24	28 1 14 2
sw-bldg-a-floor2-01	Nexus switch 9000	24	28 1 14 2
sw-bldg-a-floor2-01	Nexus switch 9000	24	28 1 14 2
sw-bldg-a-floor2-01	Nexus switch 9000	24	28 1 14 2

04 Patch software and auto-retire Shields

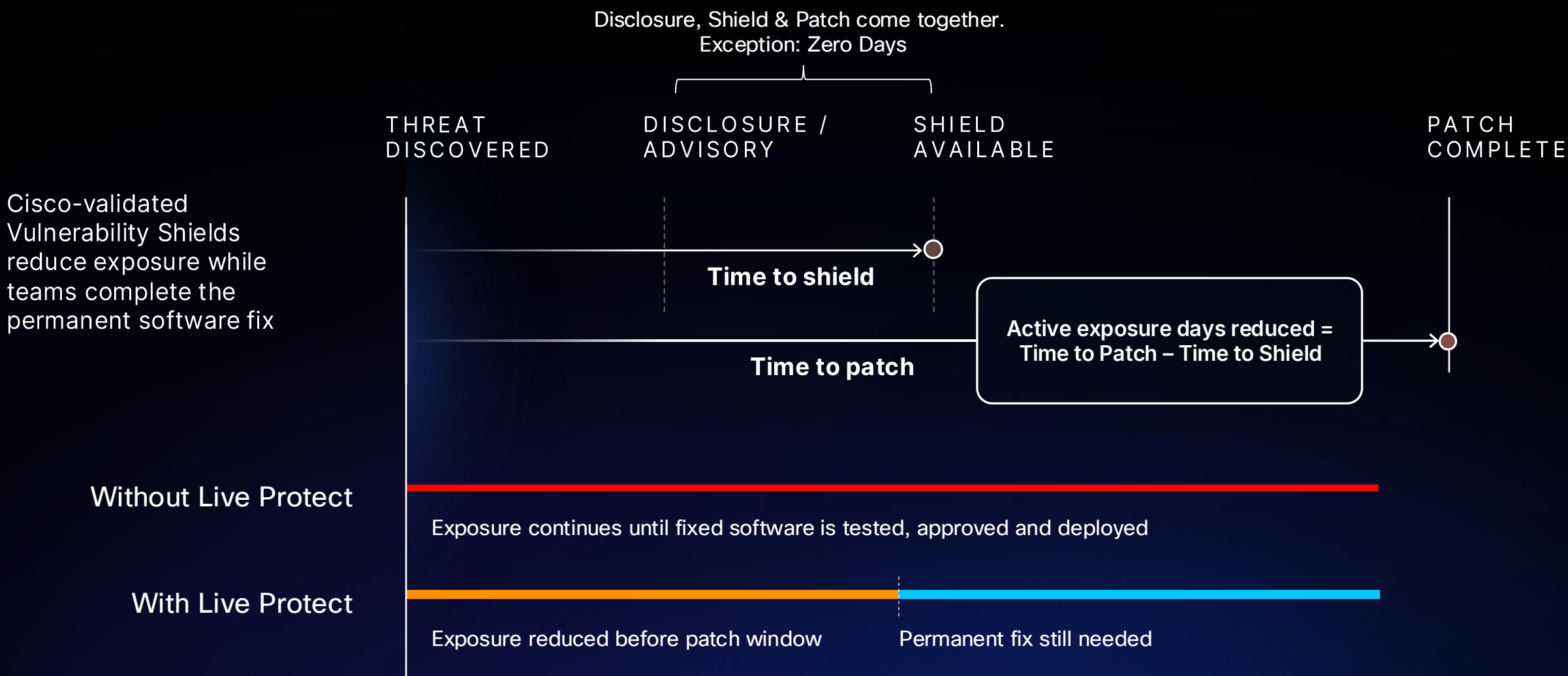
✓

34 devices are no longer vulnerable to CVE-2025-20241.

The distributed exploit shield that blocked exploit attempts related to this vulnerability was tested and is now removed to optimize system performance. The Live Protect vulnerability

✕

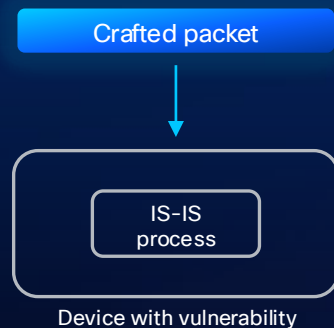
Live Protect closes the exposure gap, not the patching process



Blocking an IS-IS denial-of-service attack with a Live Protect Shield

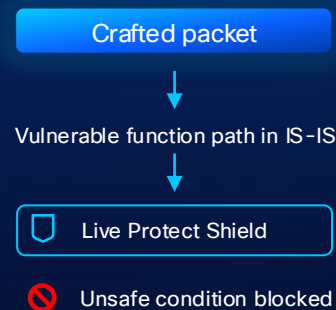
Example: CVE-2025-20241

The Attack



- Crafted packets reach vulnerable IS-IS parser
- IS-IS process may restart
- Device reload creates DoS condition

Live Protect



- Shield at vulnerable IS-IS function path
- Exploit condition blocked
- Normal IS-IS routing preserved

Operator benefit



- Avoid unplanned reloads / upgrades
- Preserve routing stability
- Patch through planned change control

Cisco validates each shield before operators deploy it

Live Protect is not a DIY runtime rule. Vulnerability Shields are initiated and validated through Cisco's security and product process.

1

PSIRT advisory intake

2

Talos exploit analysis & shield design

3

Shield testing (Cisco & 3rd party)

4

Shield release guidance

5

Operators stage & deploy

What Cisco validates

- Shield feasibility & Exploit-relevant targeting
- Normal behavior preserved
- Supported platforms, releases, modes, and limits
- Retirement path after fixed software

Operators get

- Cisco-provided, Cisco-validated protection
- Less customer burden for custom control design, testing, support, and retirement

Live Protect in action...

- CVE detect/mitigate workflows in Nexus Dashboard
- No software upgrade
- No downtime or reboots
- Export events to Splunk and other SIEMs
- API and CI/ CD support

The screenshot displays the Cisco Nexus Dashboard interface. The top navigation bar includes a search bar, user profile (John Business Corp, Inc), and a refresh button. The left sidebar shows navigation options: ND-SYS-1, Home, Manage, Analyze, and Admin. The main content area is titled 'Device Security' and shows the 'Overview' tab selected. A specific CVE is highlighted: 'cisco-sa-n39k-isis-dos-JhJA8Rfx', which is a 'Cisco Nexus 3000 and 9000 Series Switches Intermediate System-to-Intermediate System Denial of Service Vulnerability'. The 'What's wrong?' section provides details about the vulnerability and its impact. The 'What's the impact?' section shows a table of affected devices, all of which are protected by Live Protect.

Live Protect successfully deployed
Live Protect is now protecting 5 devices.

What's wrong?
A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload.

Advisory level Critical
CVSS 10.0

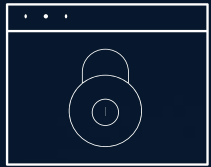
Status Protected
Last scan time Nov 4, 2025, 12:34:00 PM (PST)

Detection time: August 27, 2025, 8:35:00 PM (PST) | Related CVEs: CVE-2025-20241

What's the impact? 5 devices

Name	Fabric	Device role	Software version	Live Protect	Compensating control	Hits
Spine-1	ShopGlobalAI	Spine	10.6(2)F	Enabled	Protected	3
Spine-2	ShopGlobalAI	Spine	10.6(2)F	Enabled	Protected	1
Smart-Leaf-1	ShopGlobalAI	Leaf	10.6(2)F	Enabled	Protected	—
Smart-Leaf-2	ShopGlobalAI	Leaf	10.6(2)F	Enabled	Protected	2
Border-Leaf-3	ShopGlobalAI	Border leaf	10.6(2)F	Enabled	Protected	1

Enhancing baseline security posture out-of-the-box



Secure use, simplified

Out-of-the-box
secure settings and
proactive risk alerts

*Deprecates then removes
insecure protocols in IOS-XE*



Real-time threat response

Immediate shielding
from vulnerabilities without
disrupting operations

*Live Protect "shields" to zero-day
vulnerabilities*



Future-ready resilience

Transparent risk visibility
and post-quantum
cryptography readiness

*Prompts secure data collection with
most secure protocols and methods*

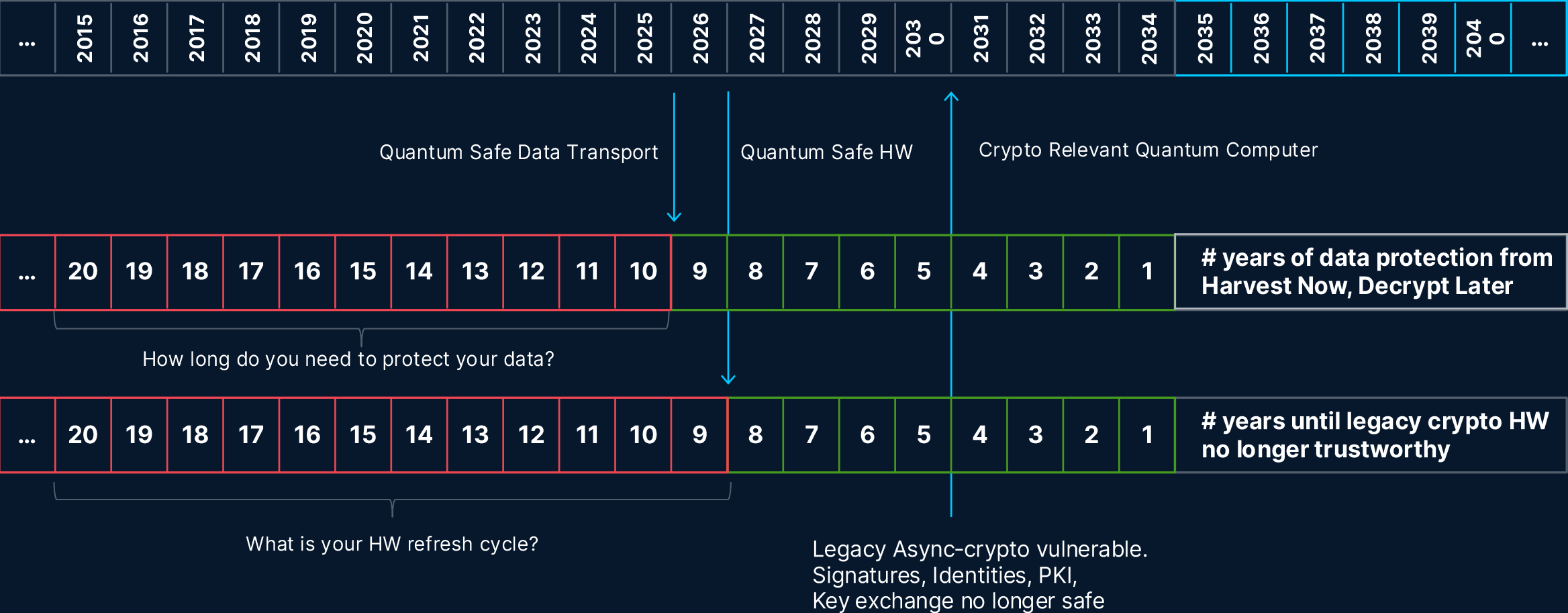


Quantum Resilient Products & Communication

Future-ready resilience

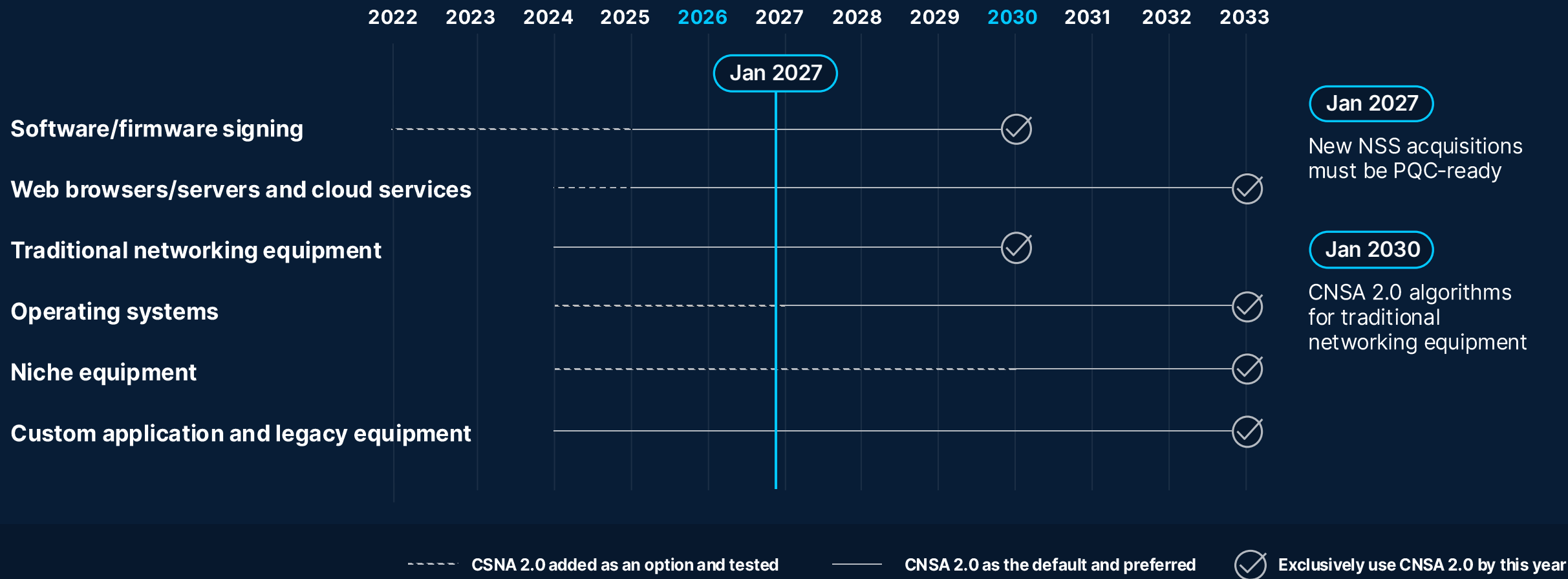
Why worry today, when QC is not yet available?

It has to be about the refresh cycle and the data that you already have now...



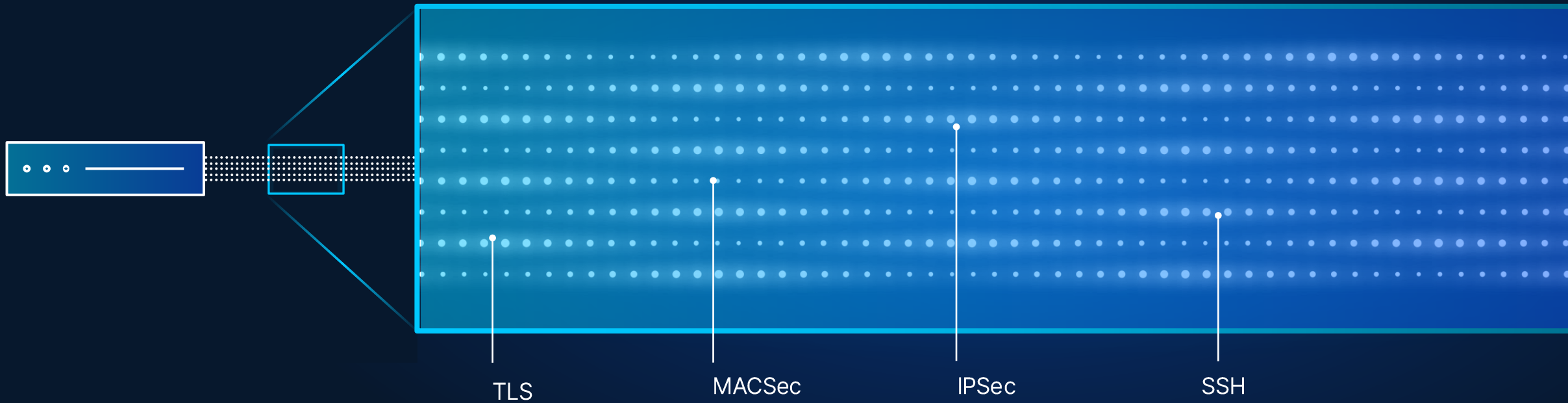
The mandate: CNSA 2.0 accelerates timeline

Transition cannot wait for next hardware refresh cycle, new infrastructure acquired today must be PQC-compliant



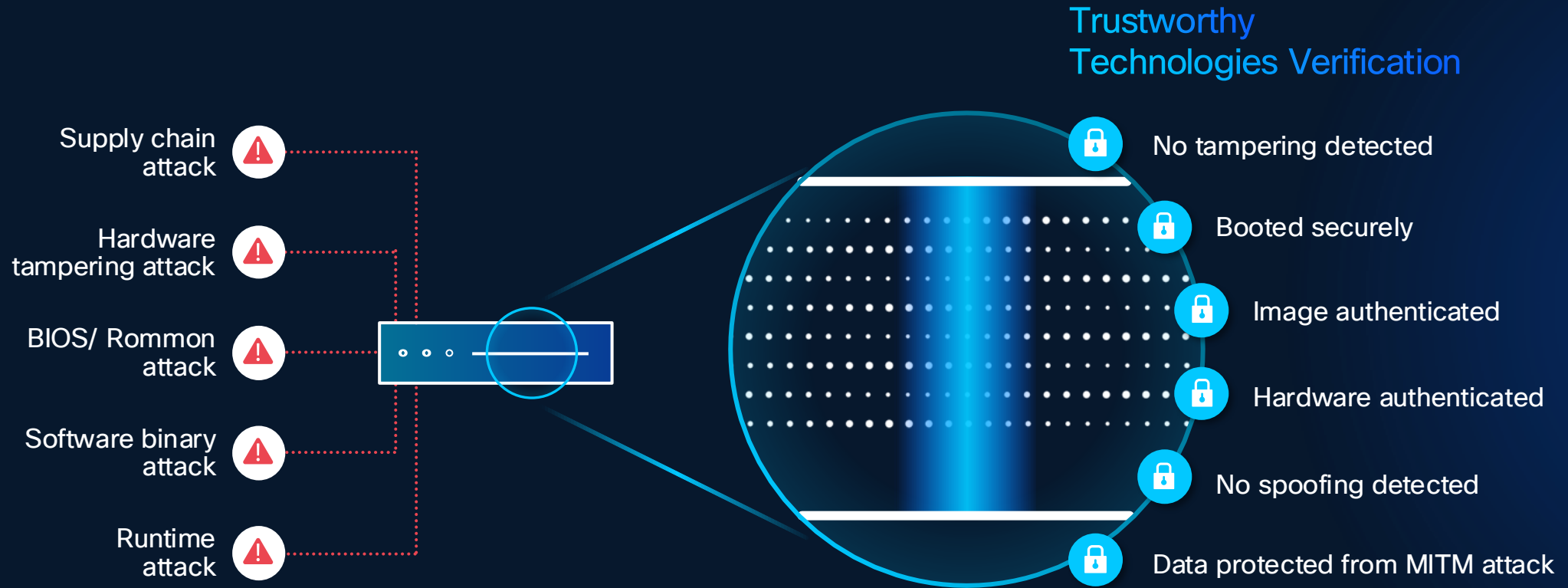
Protect what flows

Quantum-safe communication



Device Quantum Resilience

Quantum safe products



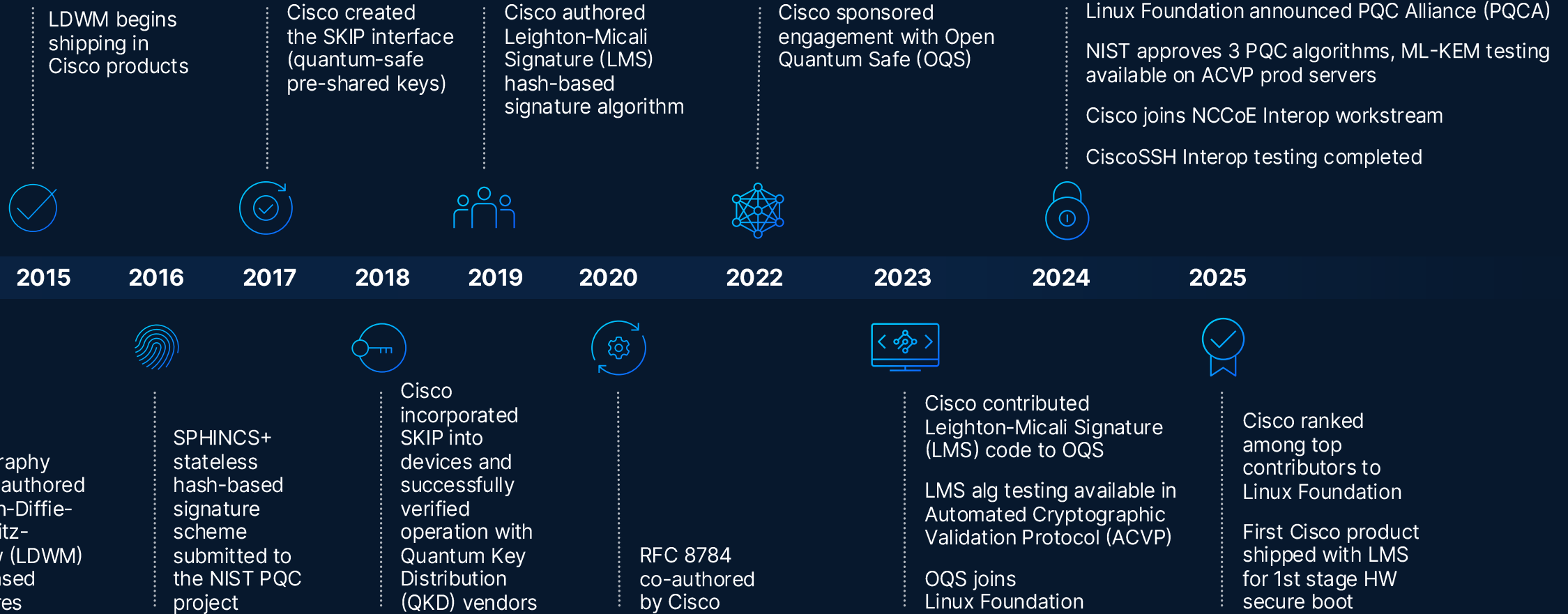
Cisco will deliver *Core* Quantum Resilience

Quantum Resilience	Quantum Safe Communication	Quantum Safe Products	
Level 1 <i>Partial</i>	3 rd -Party Key Management ¹	Secure Boot (older gen)	
Level 2 <i>Core</i>	Confidentiality ²	Secure Boot (next gen) Firmware Integrity	Aligned to CNSA 2.0
Level 3 <i>Extended</i>	Confidentiality ² Authentication ³	Secure Boot (next gen) Software/ Firmware Integrity Hardware Identity ⁴	

1. Post-quantum pre-shared keys (manual and dynamic) enabling crypto agility as well as quantum key distribution (QKD)
2. Relevant protocols vary by product but may include implementation of PQC algorithms across TLS, dTLS, IKEv2/IPsec, OpenPGP, MLS, X509, SSH, S/MIME
3. PQC standards remain undefined for much of public key infrastructure and authentication
4. E.g., SUDI (Single Unique Device Identifier)
Note: Levels 2 & 3 leverage NIST algorithms and align to CNSA 2.0 requirements

Cisco's commitment to quantum-safe standards

Cisco is actively shaping PQC for over a decade now—not just adopting it.



Cisco's end-to-end quantum-safe architecture



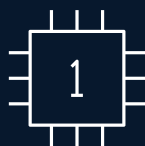
Applications/comms

PQC-based IPsec, MACsec, and TLS protect data in transit across L2-L4+



OS/Firmware

PQC Secure Boot utilizes LMS/XMSS and ML-DSA to verify platform integrity before execution



Silicon

Trust Anchor Module (TAM) establish a hardware root of trust



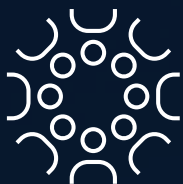
Get your free assessment with Cisco IQ CX Rep



- Talk to your Cisco IQ CX Rep
- Get a free assessment to build your roadmap
- Get started with your Quantum-safe journey today

Takeaway

Get started on your multi-year journey today!



See

Visit our demo of Live Protect and PQC solution on YouTube and our website



Learn

Visit our website:
Trust.Cisco.com



Try

Talk your Cisco rep and get started with a trial

Thank you



