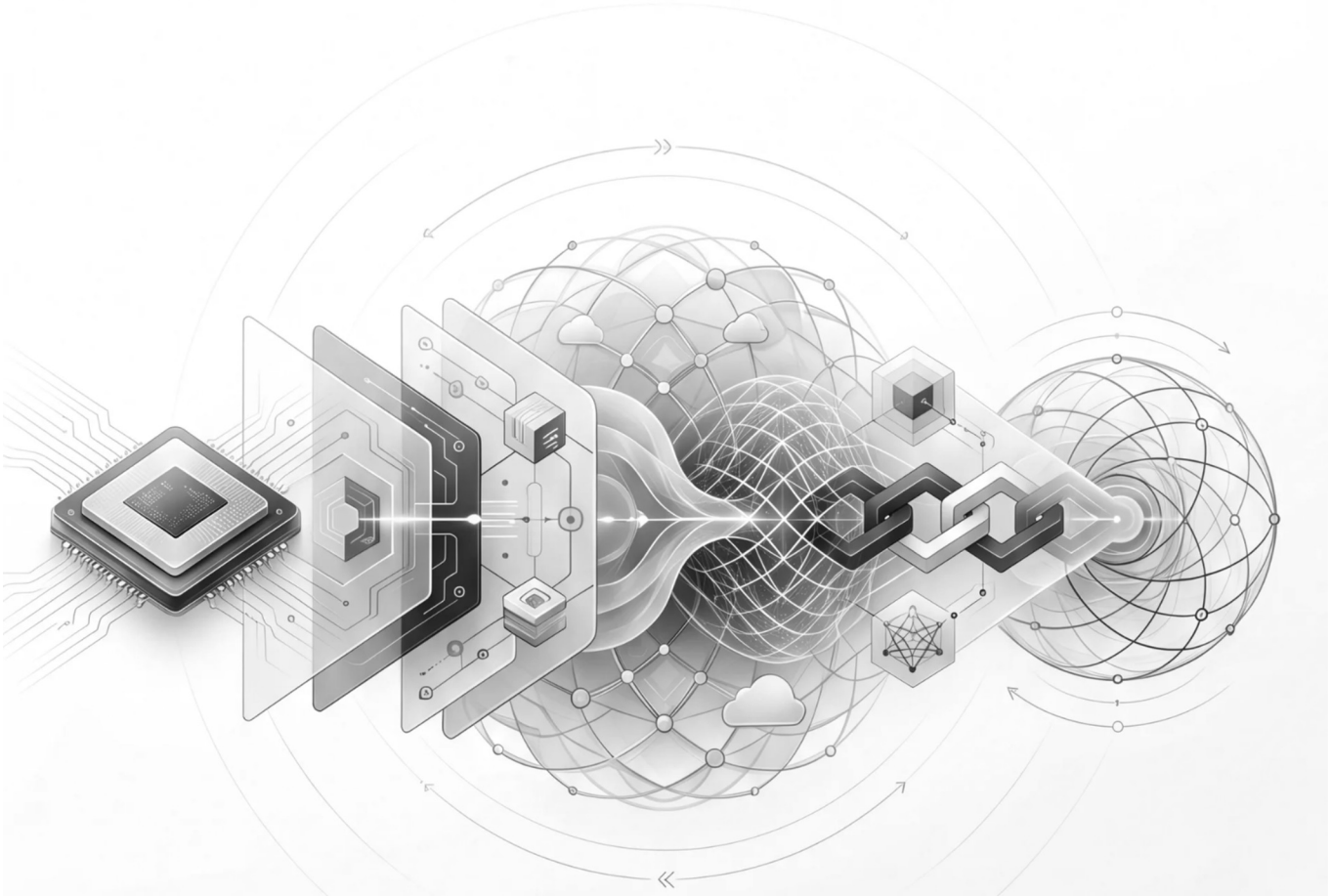
OmniTrust

Quantum Readiness Has Entered the Operational Era

Why Trust Must Be Governed Continuously from Silicon to Autonomous AI

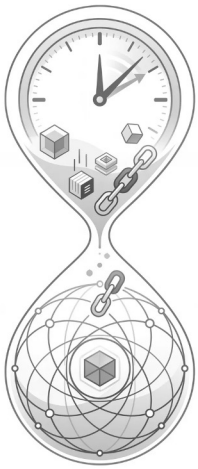


www.omnitrust.com

A Strategic Playbook for Operationalizing Trust in the Post-Quantum Era

Quantum Readiness Has Entered the Operational Era

Why Trust Must Be Governed Continuously from Silicon to Autonomous AI



Contents:

Preface – The Threshold Has Been Crossed

The conversation around post-quantum cryptography has fundamentally changed. For years, quantum computing was treated as a future risk - something to monitor, research, and eventually prepare for. Organizations viewed post-quantum cryptography (PQC) as a long-term migration project that could wait until quantum computers became commercially disruptive.

That assumption no longer reflects reality.

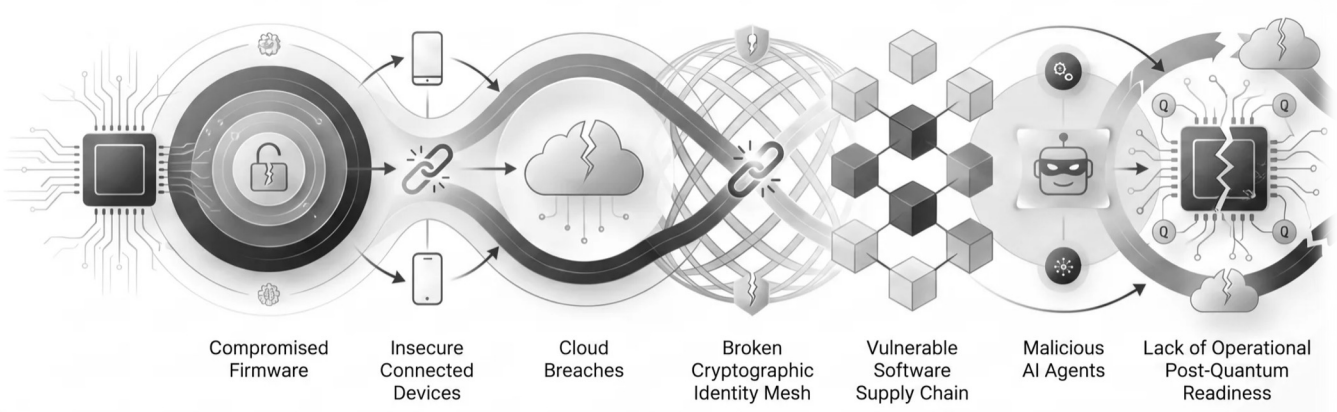
Throughout 2026, a series of developments that once appeared unrelated converged into a single operational inflection point. Hyperscale cloud providers accelerated quantum-safe infrastructure roadmaps. Semiconductor manufacturers invested heavily in hardware-rooted cryptographic agility. Enterprise software vendors began redesigning identity, signing, and trust architectures for hybrid cryptographic futures.

Meanwhile, AI introduced billions of new machine identities, autonomous software agents, APIs, and machine-to-machine trust relationships that traditional PKI and certificate management systems were never designed to govern.

Then came the clearest signal yet.

In June 2026, the United States issued two complementary Executive Orders - one advancing national quantum leadership and another accelerating the operational migration to post-quantum cryptography across federal systems. Together, they transformed PQC from a strategic recommendation into an operational mandate.

The Executive Orders introduced measurable milestones for cryptographic inventory, migration planning, validation, procurement, and cryptographic bills of materials (CBOMs). They also reinforced an uncomfortable reality that extends well beyond government.



Cryptography is no longer simply a security control. It has become operational infrastructure.

The implications extend far beyond replacing algorithms.
Organizations must now discover, inventory, govern, migrate, validate, and continuously maintain trust across an expanding ecosystem that spans:

- Silicon and secure hardware roots of trust
- Manufacturing and device provisioning
- Connected products and IoT devices
- Software supply chains and digital signing
- PKI, certificates, keys, and cryptographic assets
- Cloud infrastructure and Kubernetes workloads
- APIs and machine-to-machine communications
- Operational technology and critical infrastructure
- AI models, autonomous agents, and machine identities

Each of these systems has its own lifecycle. Each depends on cryptographic trust. Each must remain secure as algorithms, regulations, products, vulnerabilities, and threats continue to evolve.

Quantum computing did not create this challenge. It exposed a much larger one.

Most organizations have built trust infrastructure as a collection of independent technologies - PKI, certificate lifecycle management, HSMs, code signing, secrets management, device provisioning, identity systems, and compliance programs.

Few have built an operating model capable of governing trust continuously across the entire lifecycle of modern digital systems.

The organizations that succeed in the post-quantum era will not simply deploy new algorithms. They will embrace **cryptographic agility** and operate trust as a continuous lifecycle - from silicon to devices, software, cloud, and increasingly autonomous AI systems.

This paper argues that post-quantum cryptography is not merely a cryptographic migration project. It is the catalyst forcing organizations to rethink how trust itself is operationalized.
Because the real challenge is no longer selecting the next cryptographic algorithm.

It is continuously governing trust across every machine identity, every product, every workload, and every autonomous system that depends on it.

PREFACE (CONTD.)

Most enterprise trust architectures were built for a world of relatively static infrastructure, human users, and isolated security technologies. They were never designed to continuously govern trust across connected products, software supply chains, cloud-native infrastructure, operational technology, machine identities, or autonomous AI systems.

This is why post-quantum migration is really an operational trust transformation.

For years, organizations managed trust through disconnected operational silos:

- PKI & certificates
- Cryptographic keys & secrets
- Code signing & software integrity
- Device & machine identities
- Cloud & workload identity
- Software supply chain trust
- Hardware roots of trust
- AI identities & autonomous agents

> ” Quantum pressure is not creating the trust crisis - it is exposing one that already exists.

Most evolved as independent operational silos.

Few organizations built a unified operating model for trust. Instead, identities, certificates, code signing, devices, cryptographic assets, and compliance evolved as separate systems. That fragmentation was manageable when change was slow. It becomes a strategic risk when cryptography, software, regulations, and AI all evolve simultaneously.

Silicon
↓
Manufacturing
↓
Firmware & Software
↓
Connected Devices
↓
Cloud & Infrastructure
↓
Machine Identities
↓
AI Agents & Autonomous Systems

Unlike previous technology transitions, this shift is happening while software velocity accelerates, AI autonomy expands, machine identities proliferate, cryptographic complexity compounds and operational lifecycles extend across decades.

This is why the organizations moving fastest today are no longer treating post-quantum readiness as merely a cryptographic modernization initiative.

They are treating it as an operational trust transformation - and increasingly, they are realizing something else.

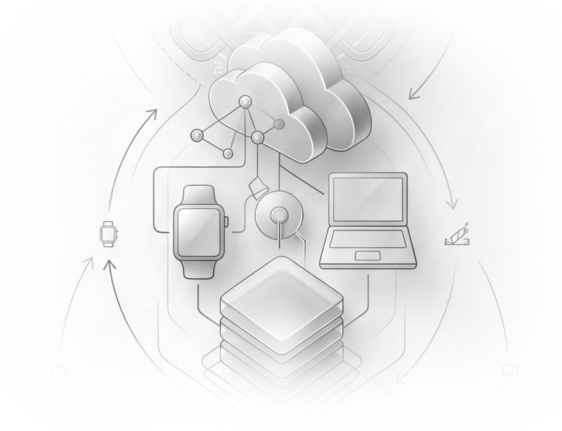
The organizations best prepared for the next decade will not simply migrate algorithms faster. They will operationalize lifecycle trust more effectively than everyone else.

Executive Summary

The cybersecurity industry is entering a structural transition.

Post-quantum readiness is no longer confined to:

- Cryptographic standards
- PKI modernization
- Certificate replacement initiatives



It is becoming an operational mandate across:

- Semiconductor ecosystems
- Connected devices
- Software supply chains
- Cloud infrastructure
- AI systems
- Autonomous execution environments

This shift is exposing a fundamental weakness in modern security architectures - trust remains fragmented.

Most organizations govern trust independently across certificates, secrets, software signing, devices, cloud identity, and AI systems. As AI autonomy accelerates and cryptographic complexity increases, fragmented trust architectures become operational risk.

The defining challenge of the next decade is no longer:

“How do we replace algorithms?”

It is:

“How do we operationalize trust continuously across the full lifecycle of connected and autonomous systems?”

Organizations that move first will establish, stronger operational resilience, faster cryptographic agility, safer AI deployment, improved regulatory readiness, greater software integrity, and long-term infrastructure continuity.

This paper presents a strategic framework for:

- post-quantum operational readiness
- practical recommendations for different sectors of the trust continuum
- a maturity model for organizational readiness
- an operational roadmap toward lifecycle trust governance

The Operational Trust Crisis

Over the last decade, the cybersecurity industry largely optimized around the dominant architectural shifts of the cloud era - accelerating cloud migration, SaaS adoption, identity-centric security models, Zero Trust networking, and DevOps-driven software velocity.

These transformations were both necessary and strategically important, enabling organizations to scale infrastructure, modernize operations, and increase agility across increasingly distributed environments. But while each initiative improved a specific domain of security and operational efficiency, they also evolved largely in parallel, creating fragmented trust ecosystems in which certificates, identities, software signing, secrets, devices, supply chains, and now AI systems are often governed independently rather than as part of a unified operational trust lifecycle.

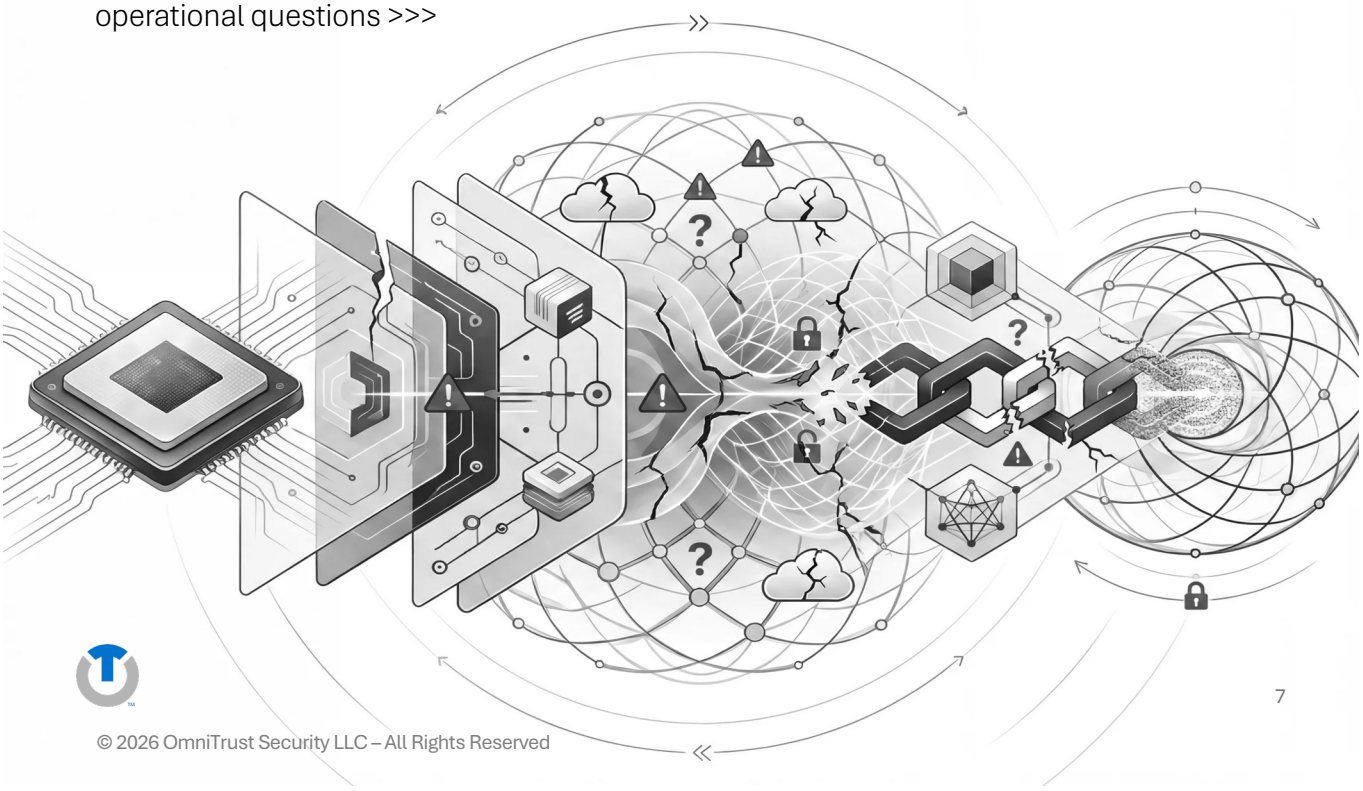
Modern organizations now operate across cloud workloads, edge systems, embedded devices, AI systems, and autonomous infrastructure. All of which rely on extensive software supply chains.

Yet trust governance remains distributed across disconnected teams and technologies.

The result: organizations often cannot answer foundational operational questions >>>

- Which systems control signing authority?
- Which devices rely on static cryptographic assumptions?
- Which AI systems possess delegated authority?
- Which workloads depend on vulnerable trust chains?
- Which OTA systems can enforce future cryptographic transitions?
- Which suppliers participate in operational trust paths?

This visibility gap is becoming strategic risk.

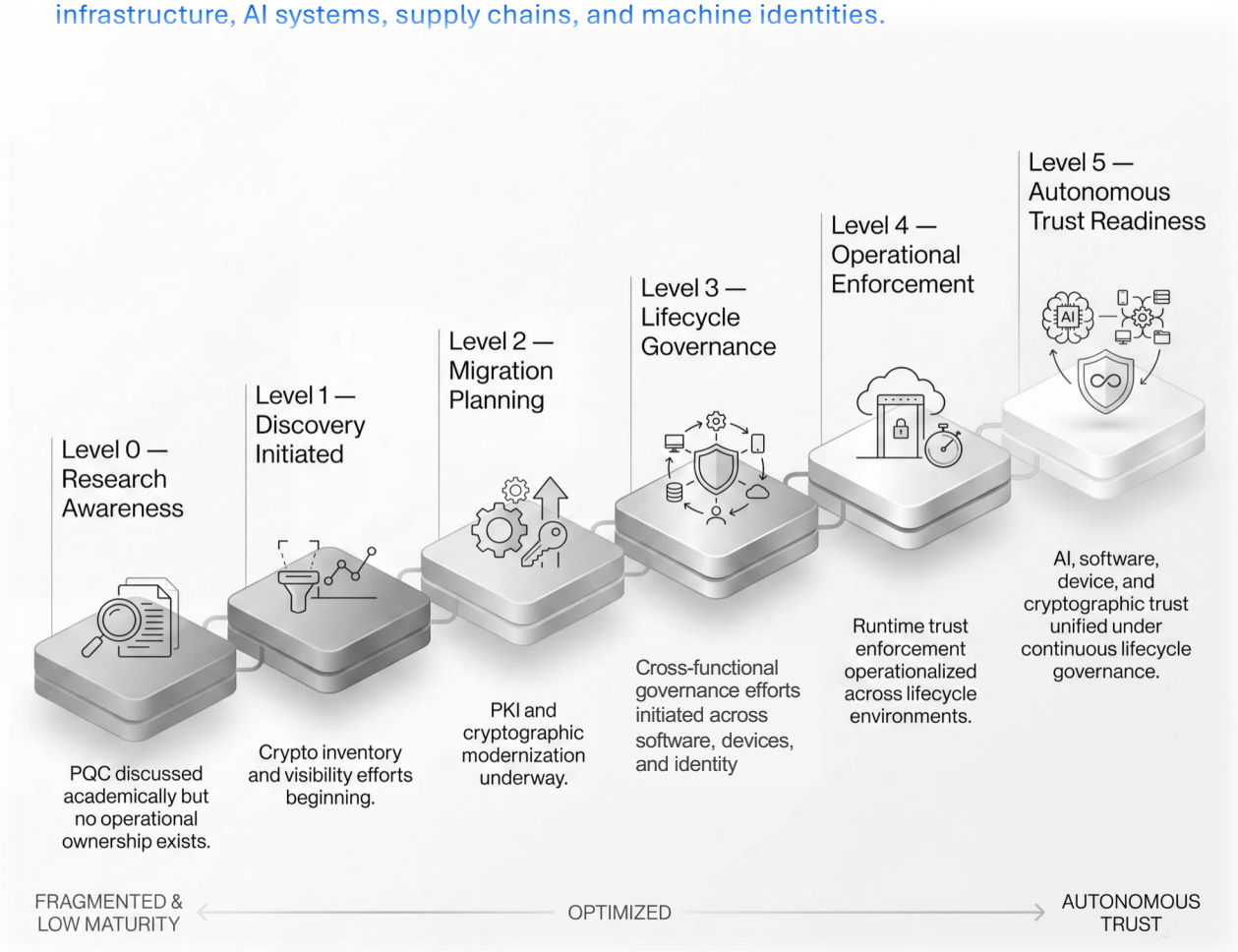


The Quantum Operational Readiness Index (QORI)

Where Is Your Organization on the Operational Trust Scale?

Level	Status	Organizational Reality
Level 0	Research Awareness	PQC discussed academically but no operational ownership exists
Level 1	Discovery Initiated	Crypto inventory and visibility efforts beginning
Level 2	Migration Planning	PKI and cryptographic modernization underway
Level 3	Lifecycle Governance	Cross-functional governance efforts initiated across software, devices, and identity
Level 4	Operational Enforcement	Runtime trust enforcement operationalized across lifecycle environments
Level 5	Autonomous Trust Readiness	AI, software, device, and cryptographic trust unified under continuous lifecycle governance

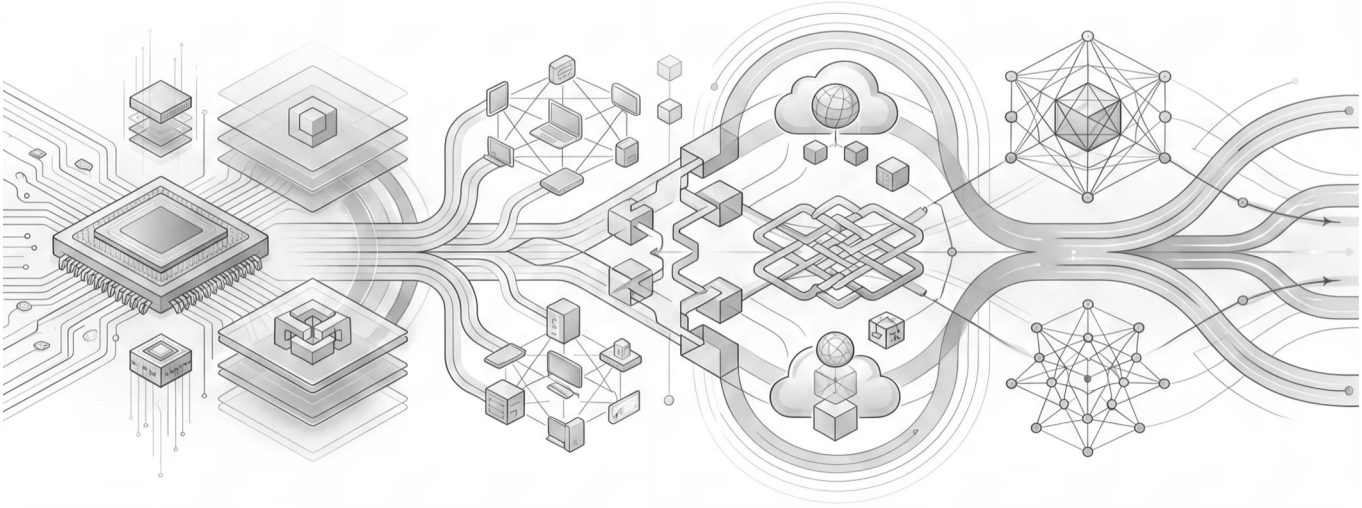
Most organizations today remain stuck between discovery and migration planning, focused primarily on cryptographic inventory and isolated modernization efforts. Very few have operationalized trust continuously across devices, software, cloud infrastructure, AI systems, supply chains, and machine identities.



The New Trust Continuum

The future trust architecture extends continuously across operational infrastructure.

The key insight is that trust failures no longer remain isolated within a single system or security domain - they propagate across the full operational continuum. A compromised signing authority, for example, can cascade simultaneously into software integrity, firmware integrity, connected devices, cloud workloads, AI systems, and even autonomous execution environments. This is why fragmented trust architectures increasingly fail under post-quantum pressure. Organizations may modernize individual components of trust, but without continuous lifecycle governance across the entire chain, operational risk compounds systemically rather than locally.



Layer	Trust Requirement
Silicon	Hardware root of trust
Firmware	Secure boot & integrity
Devices	Provisioning & lifecycle identity
OTA Systems	Trusted update orchestration
Software Supply Chain	Signing & provenance
Cloud Infrastructure	Workload identity governance
PKI & Cryptography	Key and certificate lifecycle
AI Systems	Runtime execution control
Autonomous Agents	Authority & behavioral governance

Part I

Silicon & Semiconductor Systems

The Post-Quantum Transition Starts Before the Enterprise

Who This Section Is For

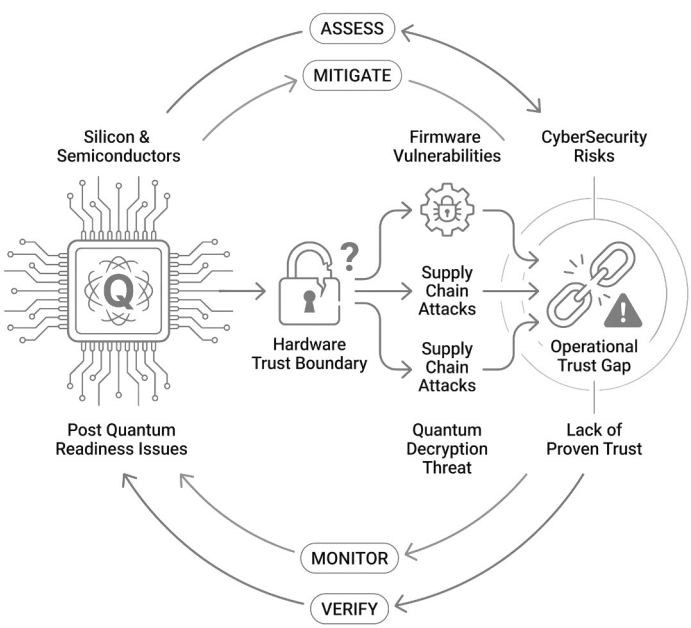
- Semiconductor manufacturers
- Chipset providers
- Embedded system architects
- Hardware security teams
- Secure provisioning organizations
- Firmware security leaders

The Longest-Lifecycle Trust Problem

Semiconductor and embedded ecosystems face some of the longest operational timelines in technology. Systems deployed today may remain operational for 10 years, 20 years, or even 30+ years. That fundamentally changes post-quantum planning. The issue is not simply future algorithm migration; the issue is maintaining cryptographic continuity across decades-long operational lifecycles.

This impacts:

- Secure provisioning
- Firmware signing
- Secure boot
- Manufacturing trust
- Root-of-trust continuity
- Field updates
- Embedded OTA systems



Most enterprise-only cybersecurity vendors cannot operationalize trust at this layer because their architectures begin inside the enterprise perimeter. The post-quantum era begins before the enterprise. At silicon.

Immediate Operational Priorities

1. Inventory Hardware-Rooted Cryptographic Dependencies

Most organizations lack visibility into:

- embedded cryptographic libraries
- hardware-bound algorithms
- signing dependencies
- manufacturing trust anchors

This creates migration blind spots.

2. Modernize Firmware Signing Governance

Firmware signing authority is becoming strategic infrastructure. Organizations must establish:

- signing authority governance
- revocation workflows
- lifecycle auditability
- hybrid cryptographic support

3. Build Long-Term Cryptographic Agility

The systems being deployed today may require multiple cryptographic transitions during operational lifespan. Static architectures will fail.

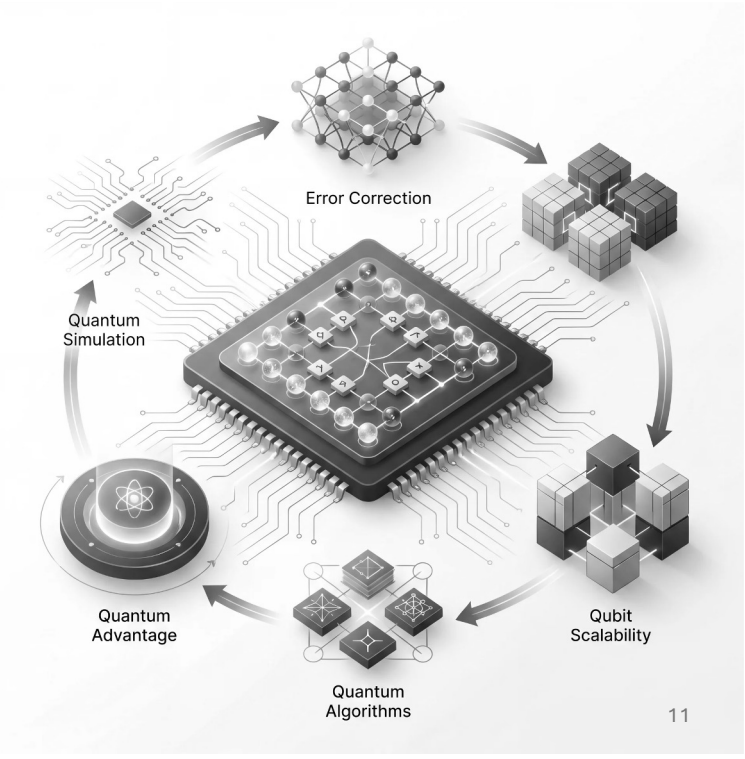
4. Align Manufacturing Trust Policy

Unify provisioning and lifecycle enforcement across:

- suppliers
- regions
- manufacturing ecosystems

Operational Recommendation

Organizations operating at the silicon and firmware layer should immediately establish cross-functional lifecycle governance around provisioning, signing, firmware trust, hardware-root continuity, and embedded cryptographic agility.



OmniTrust operationalizes trust across provisioning, signing, OTA infrastructure, and cryptographic lifecycle governance - uniquely governing trust continuously from silicon root through operational lifecycle enforcement.

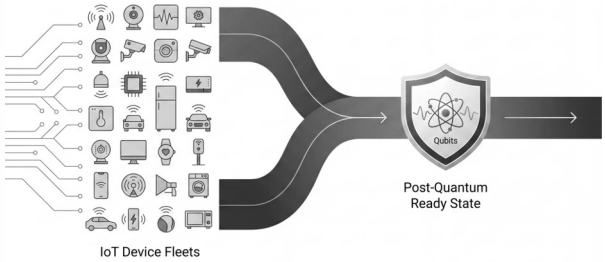
Part II

Connected Devices & IoT Ecosystems

Why the Fleet and OT Is Becoming the Front Line

Primary Stakeholders

- Automotive platforms
- Medical devices
- Industrial systems
- IoT manufacturers
- Connected infrastructure providers



The Fleet Migration Challenge

Enterprise environments can often modernize trust incrementally - reissuing certificates, rotating keys, and upgrading workloads as infrastructure evolves. Connected fleets are fundamentally different. Billions of deployed devices now depend on long-lived identities, embedded firmware, OTA infrastructure, and continuous software signing integrity, creating a far more complex operational challenge: how to govern trust continuously across massively distributed ecosystems that may remain in the field for decades.

Strategic Risks - OTA Infrastructure Becomes Critical

OTA infrastructure is no longer simply a software delivery mechanism - it has become operational trust infrastructure. Modern connected ecosystems now rely on OTA systems to maintain software continuity, enforce device integrity, govern cryptographic trust, and sustain operational resilience across billions of deployed systems. As post-quantum transition accelerates, the ability to securely orchestrate updates at scale becomes foundational to long-term operational continuity.

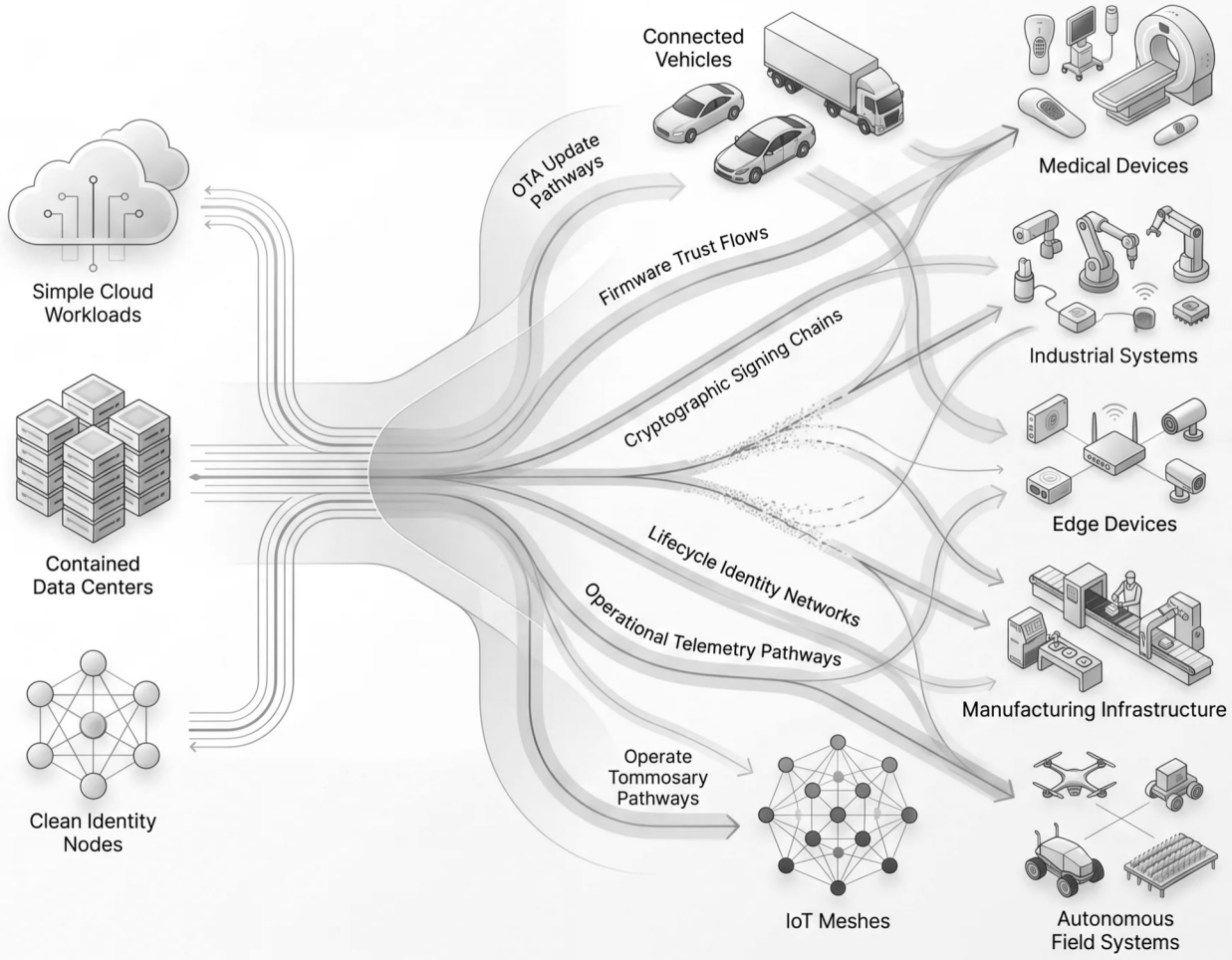
Revocation at Scale

Most organizations remain operationally unprepared for large-scale trust revocation across distributed device ecosystems. Compromised signing chains, hybrid cryptographic coexistence, and long-lived embedded identities create cascading operational challenges that traditional enterprise PKI models were never designed to handle. In massively connected environments, revocation is no longer just a technical event - it becomes a business continuity challenge.

Supply Chain Trust Expansion

Connected ecosystems increasingly depend on complex external trust relationships spanning third-party components, external firmware, software dependencies, and supplier signing systems. As these ecosystems expand, operational trust extends far beyond organizational boundaries, creating systemic dependencies across manufacturing, software delivery, and infrastructure operations. Under post-quantum pressure, supply chain trust fragmentation becomes operational risk.

Connected infrastructure has become the operational front line of trust.



Practical Recommendations

1. Inventory OTA & Signing Dependencies
2. Operationalize Fleet-Wide Cryptographic Agility
3. Establish Device Lifecycle Governance
4. Build Revocation Readiness
5. Govern Supply Chain Trust Continuously

OmniTrust

Where OmniTrust Helps - OmniTrust operationalizes:

- Secure provisioning
- OTA trust
- Firmware signing
- Revocation workflows
- Device lifecycle governance
- Supply chain trust validation

Across billions of connected systems globally.

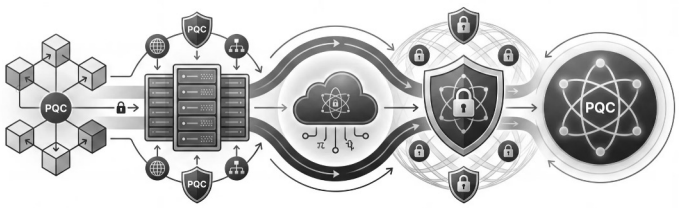
Part III

Software, Cloud & Enterprise Infrastructure

Why Trust Velocity Is Falling Behind Software Velocity

Primary Stakeholders

- DevOps organizations
- cloud security teams
- platform engineering
- CI/CD infrastructure owners
- enterprise PKI leaders



The Trust Velocity Gap

Software ecosystems now evolve continuously. AI-assisted engineering, ephemeral infrastructure, and machine-driven deployment pipelines have accelerated software velocity dramatically.

But trust governance has not scaled proportionally. This creates:

- signing sprawl
- secrets sprawl
- inconsistent policy enforcement
- fragmented workload identity
- audit gaps
- supply chain uncertainty

Software velocity is now exceeding trust governance velocity.

Strategic Risks - Software Signing as Hidden Infrastructure

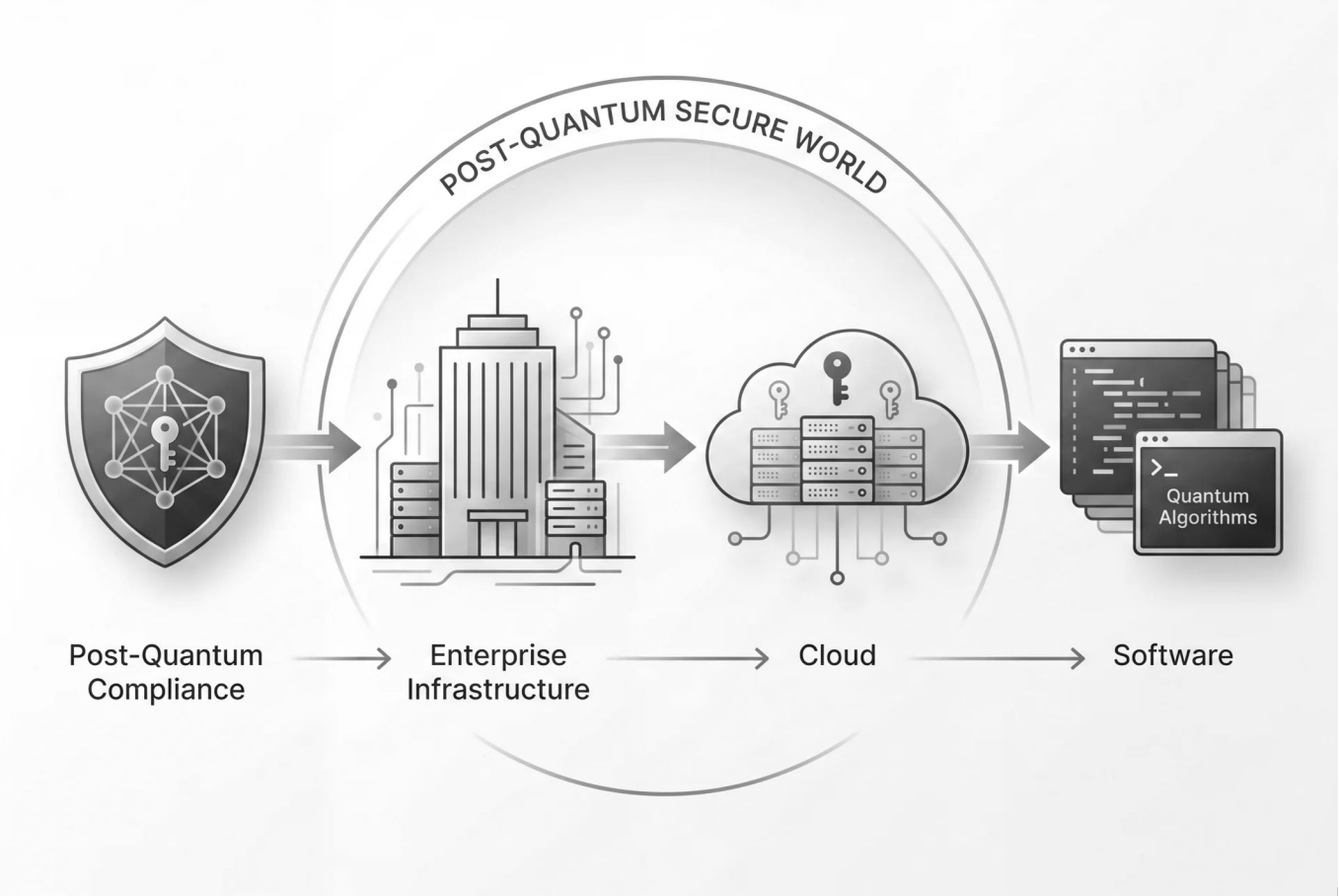
Software signing now governs software provenance, deployment trust, release integrity, and supply chain assurance across modern software ecosystems. Yet many organizations still manage signing reactively through fragmented workflows and inconsistent ownership. As software velocity accelerates, signing infrastructure becomes a strategic operational trust control point.

Secrets & Workload Identity Fragmentation Accelerates

Cloud-native environments introduce ephemeral identities, short-lived workloads, API-driven trust relationships, and increasingly decentralized infrastructure. Without continuous lifecycle governance, machine identity sprawl compounds rapidly across cloud ecosystems. The result: trust is harder to govern, enforce, audit, and operationalize consistently at enterprise scale.

AI-Generated Software Changes the Trust Equation

AI-assisted development is accelerating code generation, autonomous dependency inclusion, and machine-driven software creation at unprecedented speed. At the same time, software provenance becomes increasingly opaque, making trust verification dramatically harder. Organizations must now govern not only software integrity, but the systems generating the software itself.



Practical Recommendations

1. Discover Cryptographic Dependencies Across CI/CD
2. Govern Software Signing Centrally
3. Operationalize Supply Chain Provenance
4. Align Secrets Governance with Lifecycle Policies
5. Prepare Software Pipelines for Hybrid Crypto Futures

OmniTrust

Where OmniTrust Helps - OmniTrust operationalizes:

- Cryptographic lifecycle management
- Software signing governance
- Workload identity
- secrets orchestration
- supply chain integrity
- lifecycle auditability

OmniTrust Supports these capabilities across hybrid cloud and enterprise infrastructure.

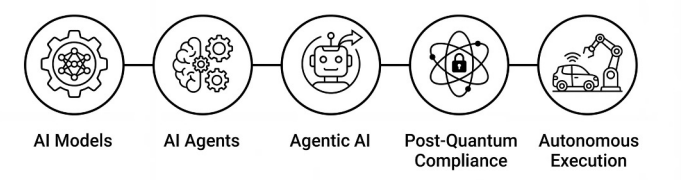
Part IV

AI & Autonomous Systems

Why AI Is Transforming Operational Trust

Primary Stakeholders

- Enterprise AI leaders
- AI platform teams
- CISO organizations
- Autonomous system developers
- Runtime governance teams



AI Is Expanding the Trust Surface Faster Than Governance

AI is expanding the trust surface at dramatically increased pace. Every new agent, model, integration, and data connection creates risk, visibility gaps, and attack vectors.

AI systems increasingly execute workflows autonomously, invoke APIs dynamically, generate software, interact machine-to-machine, and operate continuously across enterprise environments. This dramatically expands non-human identities, delegated authority, runtime trust relationships, and operational complexity - creating an attack surface that is increasingly autonomous rather than human-driven.

Uncontrolled Agent Permissions Create Operational Risk

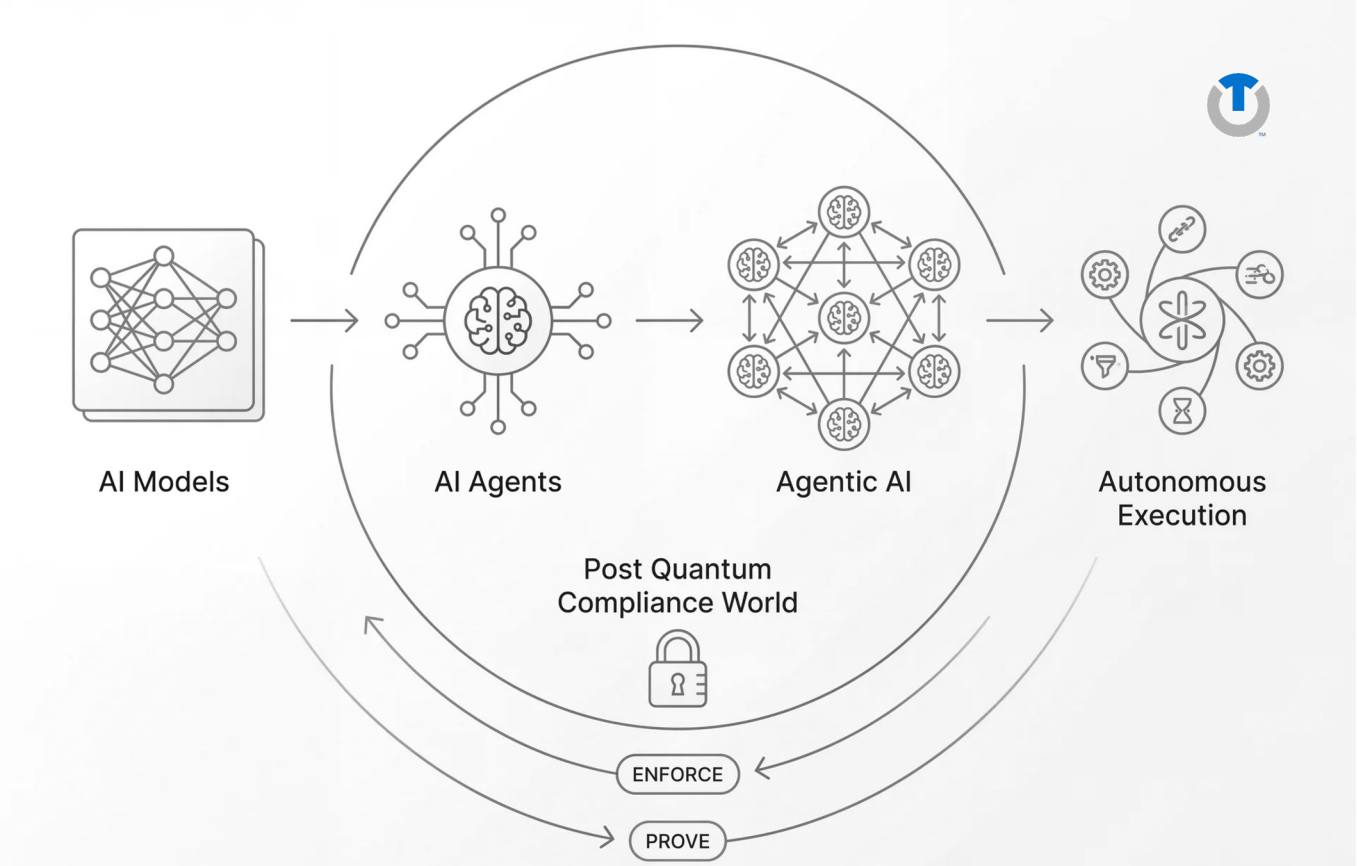
Most organizations still lack operational governance around AI authority boundaries, runtime permissions, and autonomous execution policies. As AI systems gain access to tools, workflows, and enterprise infrastructure, unmanaged agent permissions introduce escalating operational and security risks across increasingly interconnected environments.

Shadow AI Expansion Is Outpacing Organizational Control

AI adoption is accelerating faster than enterprise governance models can adapt. This creates opaque data movement, uncontrolled tool access, ungoverned model usage, and fragmented operational visibility across organizations. In many environments, AI systems are already operating beyond the visibility and policy boundaries of traditional security architectures.

Runtime Trust Enforcement Becomes Essential

Traditional cybersecurity architectures were designed around static policy enforcement and relatively predictable systems. Autonomous environments fundamentally change that model. AI systems require continuous runtime trust enforcement capable of governing dynamic execution, real-time decision-making, delegated authority, and machine-to-machine operational behavior.



Practical Recommendations

1. Discover AI Systems and Agent Activity
2. Treat Agents as Operational Identities
3. Operationalize Runtime Control
4. Govern Data & Tool Access Continuously
5. Build AI Lifecycle Auditability

OmniTrust

Where OmniTrust Helps - OmniTrust Halo Operationalizes

- AI systems
- Agentic environments
- Runtime execution
- Autonomous workflows
- Non-human identities

Discover → Control → Enable

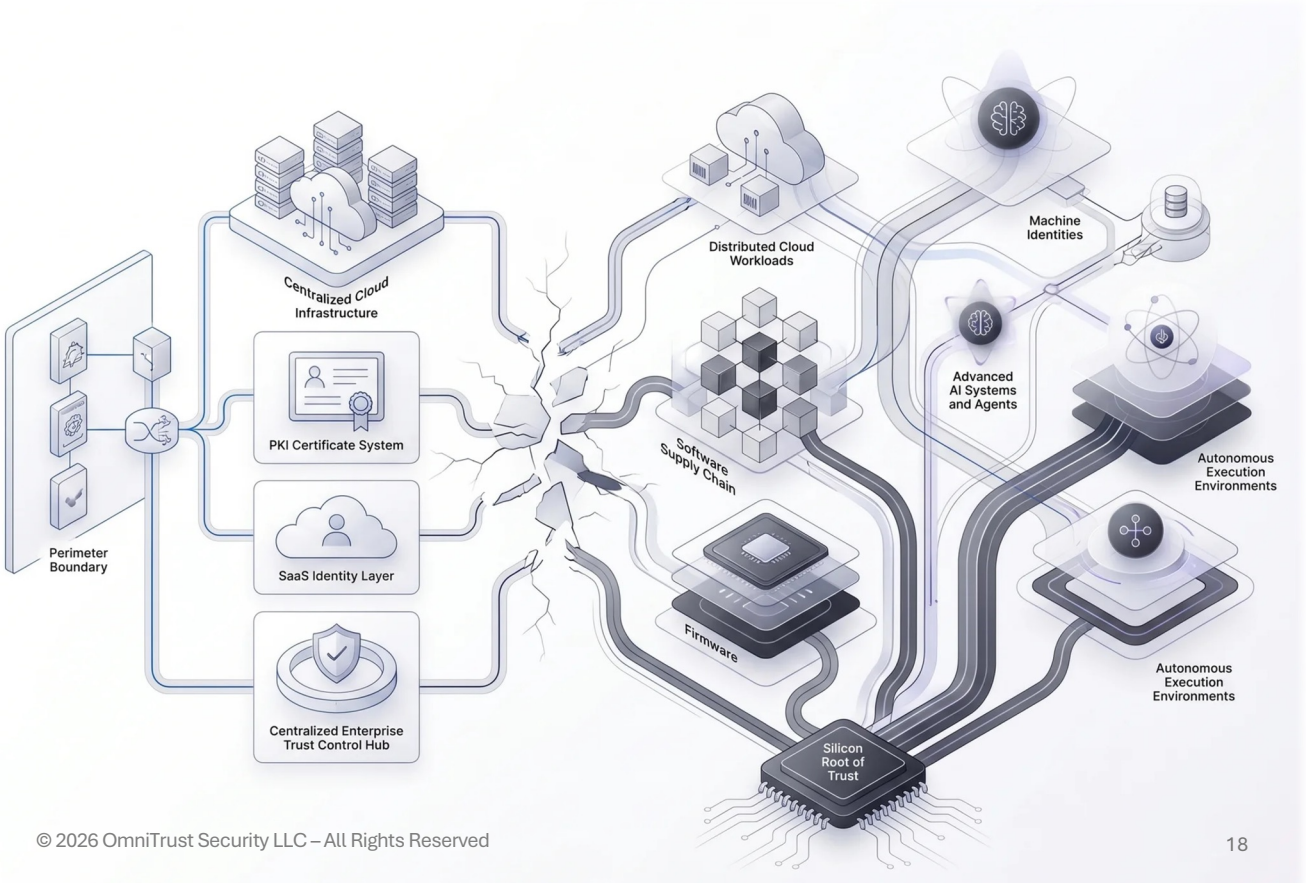
Providing continuous operational trust enforcement.

Why Enterprise-Only Security Is No Longer Sufficient

Most modern cybersecurity architectures were built for the enterprise IT era and optimized around cloud identity, perimeter governance, SaaS infrastructure, and PKI modernization. These capabilities remain critically important, but they were never designed to govern trust continuously across embedded systems, OTA ecosystems, software-defined infrastructure, AI-driven execution, and long-lifecycle operational environments.

The post-quantum era is exposing this limitation directly. Trust no longer begins or ends inside the enterprise perimeter. It now extends continuously across silicon, firmware, connected devices, software supply chains, cloud workloads, machine identities, AI systems, and autonomous operational environments. As these systems become increasingly interconnected, fragmented enterprise-centric trust models struggle to maintain operational continuity, enforce cryptographic governance, or govern trust across the full lifecycle.

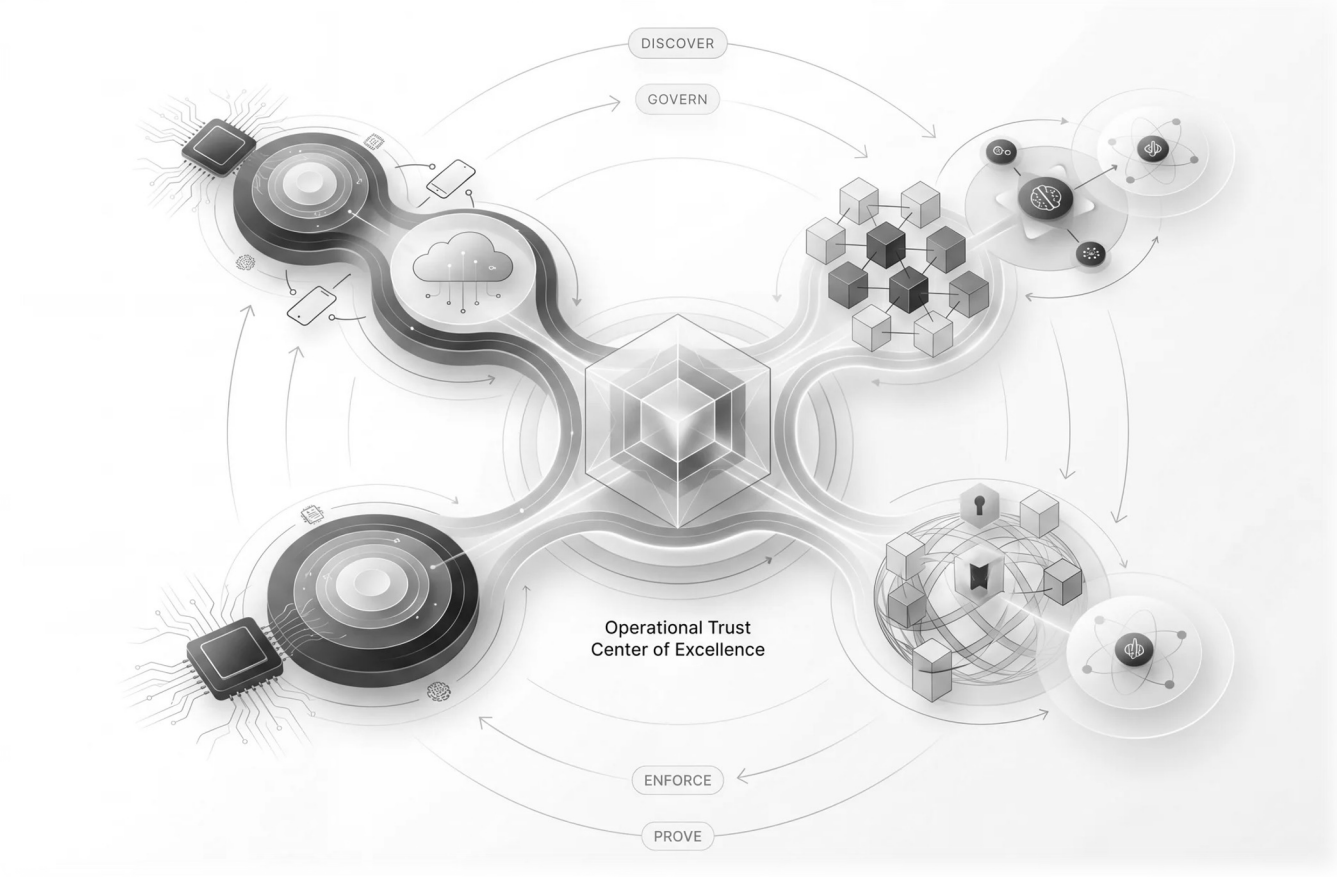
Enterprise-only providers still govern important portions of the trust chain. But the organizations best positioned for the next decade will require something broader: continuous lifecycle trust governance across the entire operational continuum - from silicon root of trust through autonomous execution.



Building the Operational Trust Center of Excellence

As operational complexity accelerates across connected systems, software-defined infrastructure, AI environments, and long-lifecycle ecosystems, organizations are increasingly discovering that fragmented trust ownership is becoming unsustainable.

Cryptographic governance, software integrity, device trust, AI oversight, runtime enforcement, and operational resilience are often managed independently across disconnected teams. This creates visibility gaps, inconsistent policy enforcement, and growing lifecycle risk. In response, leading organizations are beginning to establish Operational Trust Centers of Excellence (CoEs) designed to unify trust governance operationally across the enterprise lifecycle.



Core Functions of the Operational Trust CoE

- Cryptographic governance
- Software integrity and signing governance
- Device and OTA trust management
- AI governance and runtime control
- Lifecycle auditability and compliance traceability
- Runtime enforcement and operational policy orchestration
- Cross-functional operational resilience planning

Strategic Shift

The objective is no longer simply managing isolated trust technologies independently across infrastructure domains. The objective is operationalizing trust continuously across the full lifecycle - from silicon root of trust and software supply chains through AI systems and autonomous execution environments.

Strategic Recommendations for CEOs & CISOs

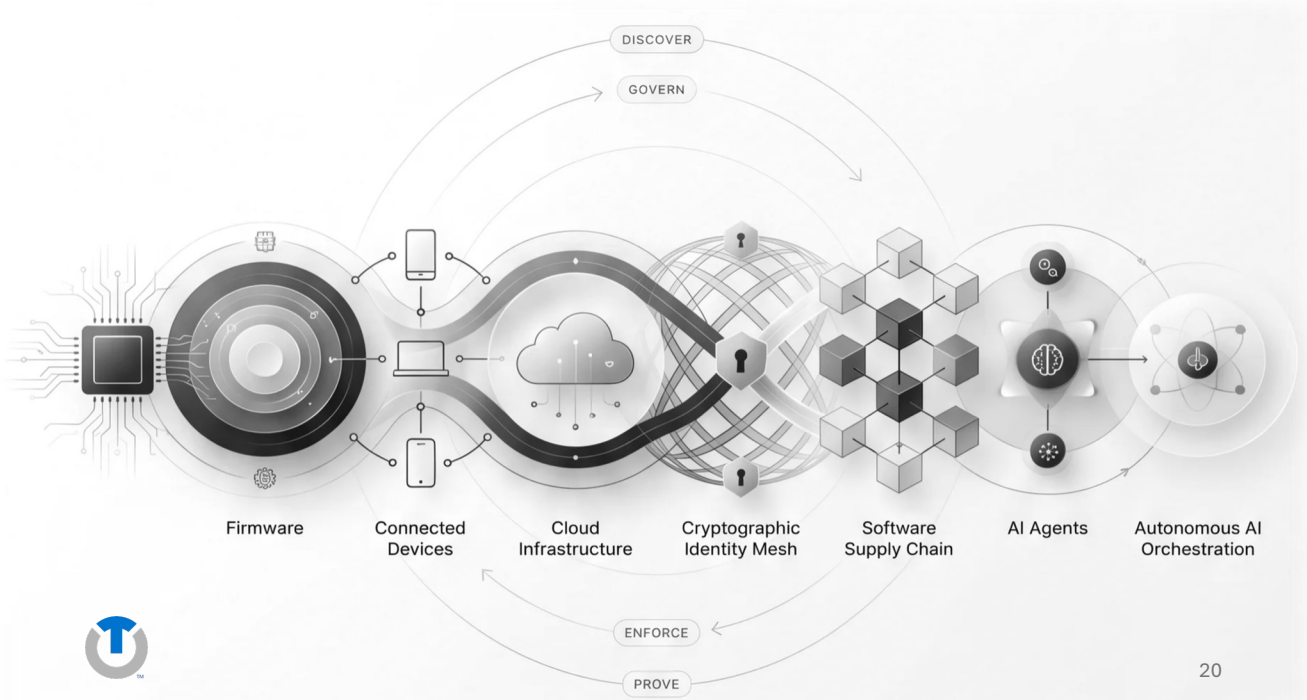
The post-quantum transition is increasingly becoming an operational leadership challenge rather than a purely technical modernization effort. As trust expands across software supply chains, connected devices, cloud infrastructure, AI systems, and autonomous execution environments, fragmented ownership models are creating growing systemic risk. Leading organizations are beginning to recognize that lifecycle trust must be governed as a continuous operational discipline spanning technology, security, software, infrastructure, and AI governance functions.

Strategic Priorities for Leadership Teams

- Treat post-quantum readiness as an operational transformation initiative - not simply a certificate replacement project
- Establish executive ownership for lifecycle trust governance across the enterprise
- Build cross-functional governance unifying PKI, software integrity, device security, AI governance, and runtime enforcement
- Prioritize lifecycle visibility across cryptographic inventory, trust dependencies, software provenance, and runtime awareness
- Prepare operationally for autonomous infrastructure and AI-driven execution environments

Strategic Implication

Organizations that operationalize trust earliest will gain structural advantage in resilience, software integrity, cryptographic agility, AI governance, and long-term operational continuity.



Conclusion

Trust Must Become Operational

The post-quantum transition is exposing a larger structural reality: modern trust architectures were not designed for the autonomous era. Most existing security models evolved around enterprise IT, cloud infrastructure, and relatively static operational environments. They were never intended to govern trust continuously across silicon, firmware, connected devices, software supply chains, cloud workloads, AI systems, and autonomous execution environments operating at global scale.

The organizations best prepared for the next decade will not simply modernize cryptographic algorithms faster than competitors. They will operationalize lifecycle trust more effectively across the full operational continuum.

The Next Era of Trust Requires

- Continuous lifecycle governance
- Operational cryptographic agility
- Runtime enforcement
- Software and firmware integrity
- AI governance and autonomous control
- Cross-functional operational resilience

The Defining Strategic Question

The challenge is no longer whether post-quantum transition will occur. The challenge is whether organizations can operationalize lifecycle trust before operational complexity outpaces governance.

OmniTrust helps organizations operationalize trust continuously across the full continuum - from silicon root through autonomous AI execution.

www.omnitrust.com

The OmniTrust Lifecycle Trust Model

Most cybersecurity platforms evolved from enterprise IT. Their architectures were designed primarily around cloud identity, perimeter governance, PKI modernization, and SaaS-era infrastructure security. While those capabilities remain important, they were not built to operationalize trust continuously across long-lifecycle, safety-critical, and increasingly autonomous environments.

OmniTrust was built differently. Its trust architecture originated in industries where trust failure creates operational, regulatory, and mission-critical consequences - including aerospace, defense, industrial systems, automotive, medical infrastructure, and safety-critical embedded environments. These sectors required continuous lifecycle assurance long before “post-quantum readiness” became an industry priority. As a result, OmniTrust evolved around a fundamentally broader operational trust model: governing trust continuously across devices, software, cryptographic infrastructure, supply chains, and increasingly autonomous systems.

Core OmniTrust Lifecycle Trust Domains

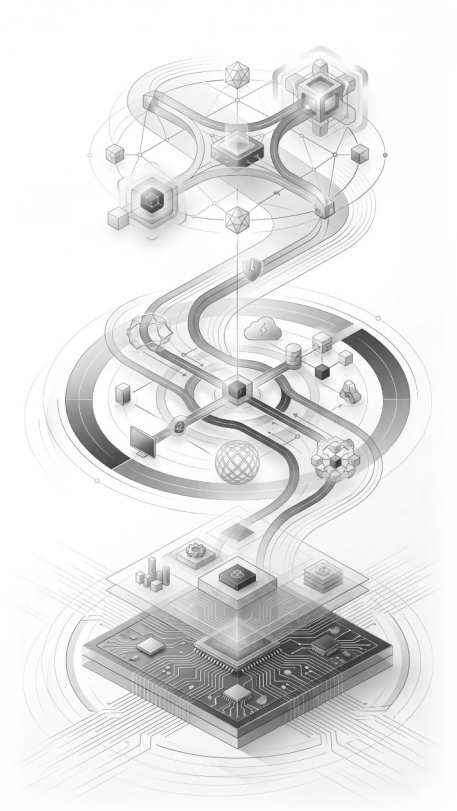
- Device Lifecycle Management (DLM)
- Identity Lifecycle Management (ILM)
- Certify lifecycle cyber risk governance
- AI Lifecycle Management (ALM) + the trust-native Halo AI runtime control and enforcement platform

Operational Outcomes Enabled by OmniTrust

- Assess trust continuously
- Govern trust across the lifecycle
- Enforce operational trust policies
- Prove integrity, compliance, and resilience

Operational Scope

- Connected devices and embedded systems
- Software and firmware ecosystems
- Cloud and cryptographic infrastructure
- AI systems and machine identities
- Autonomous operational environments



Strategic Implication

The post-quantum era requires more than enterprise-centric security modernization.
It requires continuous lifecycle trust governance spanning the full operational continuum - from silicon root of trust through autonomous execution.

www.omnitrust.com