TECH mahindra

Whitepaper

QuantumTrust Fabric:

Architecting Digital Trust for the Post-Quantum Enterprise

A Strategic Blueprint for CSPs and Regulated Industries in the Quantum Era

Table of Contents

Executive Summary

As modern enterprises evolve, traditional security models are no longer sufficient to meet their growing requirements. Tech Mahindra's QuantumTrust Fabric enables businesses to build digital trust in a world shaped by quantum computing, AI, and evolving regulations. QuantumTrust Fabric distinguishes itself from outdated security solutions by employing a flexible, layered approach to build trust into every aspect of your digital environment—spanning identity, data, infrastructure, and governance.

This whitepaper explains the importance of trust in today's era, how QuantumTrust Fabric works, and the value it delivers across various industries. It also highlights Tech Mahindra's unique approach to building scalable, future-ready trust systems.

Introduction

Context and Background

The digital economy is undergoing a fundamental transformation. As organizations adopt cloud-native applications, expand across distributed partner ecosystems, and integrate AI into critical systems, perimeter-based security and rigid policies quickly fall short, making trust a business imperative. Traditional cybersecurity models were never built for today's dynamic, API-driven, quantum-exposed environments.

Cybercrime is estimated to cost the global economy over $10.5 trillion annually by 2028 (Cybersecurity Ventures). Meanwhile, advancements in quantum computing pose a threat to existing encryption protocols within the next decade. As a result, regional regulators are now enforcing operational resilience, data transparency, and identity assurance.

Relevance Today

For large enterprises, digital trust is a critical boardroom discussion. It affects customer trust, investor decisions, and the ability to grow geographically. The convergence of Zero Trust Architecture (ZTA; Microsoft), post-quantum cryptography (PQC), AI-based governance, and regulatory compliance necessitates a comprehensive reassessment of trust design, monitoring, and enforcement strategies.

Overview of QuantumTrust Fabric

QuantumTrust Fabric is a digital trust framework that incorporates quantum-resilient encryption, GenAI-powered observability, and compliance automation across your digital environment. Built on seven trust layers, it integrates via a plug-and-play platform layer, is modular by design, and adapts to an enterprise's maturity and industry context.

Quantum Trust Fabric Uses:

- Agentic AI for autonomous policy governance
- Zero Trust and PQC as default enforcement paradigms
- Trust Telemetry Index (TTI) for measurable trust performance
- Composable integrations with hyperscaler, on-perm, and SaaS ecosystems

Market Indicators

Recent industry data highlights significant gaps in encryption methodology, visibility, and regulatory readiness, underscoring the urgency of a structured transition to quantum-safe cryptography (IBM Security). Key examples include:

Seventy-one percent of organizations lack a coherent strategy for quantum-safe encryption (Deloitte).

Sixty percent of CISOs report a lack of visibility across multi-cloud trust zones (Gartner).

By 2030, national security systems and regulated industries must implement NIST-approved post-quantum cryptographic (PQC) algorithms (National Institute of Standards and Technology).

The Need for a Trust-Centric Architecture

Why Traditional Security Falls Short

Legacy cybersecurity models defend fixed perimeters using isolated tools like firewalls, antivirus, and intrusion prevention systems, which are no longer sufficient. Organizations currently operate in dynamic ecosystems that span across multiple clouds, edge computing nodes, hybrid infrastructures, and third-party SaaS providers.

In such distributed digital systems:

- Data flows continuously across borders and trust zones
- Identity is no longer tied to a device or network segment
- Cyber threats use AI to bypass legacy detection systems
- Regulations require real-time transparency and verifiable compliance

As a result, modern security practices shift from merely blocking threats to continuously assessing trust and enforcing policies that adapt in real time to evolving risks.

What a Trust-Centric Architecture Enables

A trust-centric architecture is not limited to perimeter security. It ensures that:

- Every digital interaction is vetted for trustworthiness, whether it involves a user login, API request, or data flow.
- Trust rating, combined with telemetry, is continuously generated, monitored, and addressed as needed.
- Smart automation ensures that policies align with how your systems operate, eliminating the need for manual intervention.
- Quantum-safe protection is embedded by design, not retrofitted as an afterthought.
- Compliance updates can be easily adapted to regulatory requirements without affecting core systems or workflows.

This architecture is designed for composability, interoperability, and observability, enabling seamless integration with existing environments while easily accommodating new requirements.

The QuantumTrust Fabric Framework

Overview of the Framework

QuantumTrust Fabric employs a modular, multi-layered design that incorporates trust as the foundation for enterprise IT. This framework employs AI, quantum-safe encryption, and built-in compliance to protect enterprise systems.

For QuantumTrust Fabric, trust is a never-ending process that follows these core principles:

- **Zero Assumptions**: The system does not automatically trust any user, application, or infrastructure; it verifies everything.
- **Always Verifiable**: Signing, validation, and visibility are built into every interaction, ensuring no lapses in transparency and accountability.
- **Self-Optimizing**: AI and ML constantly adapt policies based on the context and anticipated potential threats.
- **Composable and Pluggable**: The architecture is agnostic of the different environments and integrates easily, ensuring flexibility and scalability.

Architectural Design and Trust Layers

Architectural Philosophy

QuantumTrust Fabric is modular and layered by design, with each layer focusing on specific areas, such as identity, data, applications, or infrastructure. Organizations can decide whether to implement these layers individually or in combination, depending on their digital development stage and regulatory compliance requirements.

Each layer handles tasks autonomously, while adjacent layers share trust telemetry. The platform maintains an enterprise trust graph for real-time advanced correlation, policy enforcement, and compliance scoring.

QuantumTrust differs from monolithic security architectures by being non-intrusive. It can be incrementally introduced and is compatible with all cloud types. Besides, it works with CSP-native services, on-premises systems, and multi-tenant SaaS environments.

Design Benefits

QuantumTrust Fabric architecture offers certain design features that aim to provide users with flexibility, reliability, and future adaptability:

- **Horizontal scalability**: The design for all layers uses stateless microservices to scale independently.
- **Composable deployment**: Depending on the use cases, each layer can be selectively deployed (e.g., identity first, then data).
- **Observability built-in**: Systems can read all telemetry generated for every interaction and come with semantic context.
- **Autonomous remediation**: If trust violations occur, the system triggers AI-led policy adjustments without requiring human intervention.

The Seven Layers of QuantumTrust Fabric

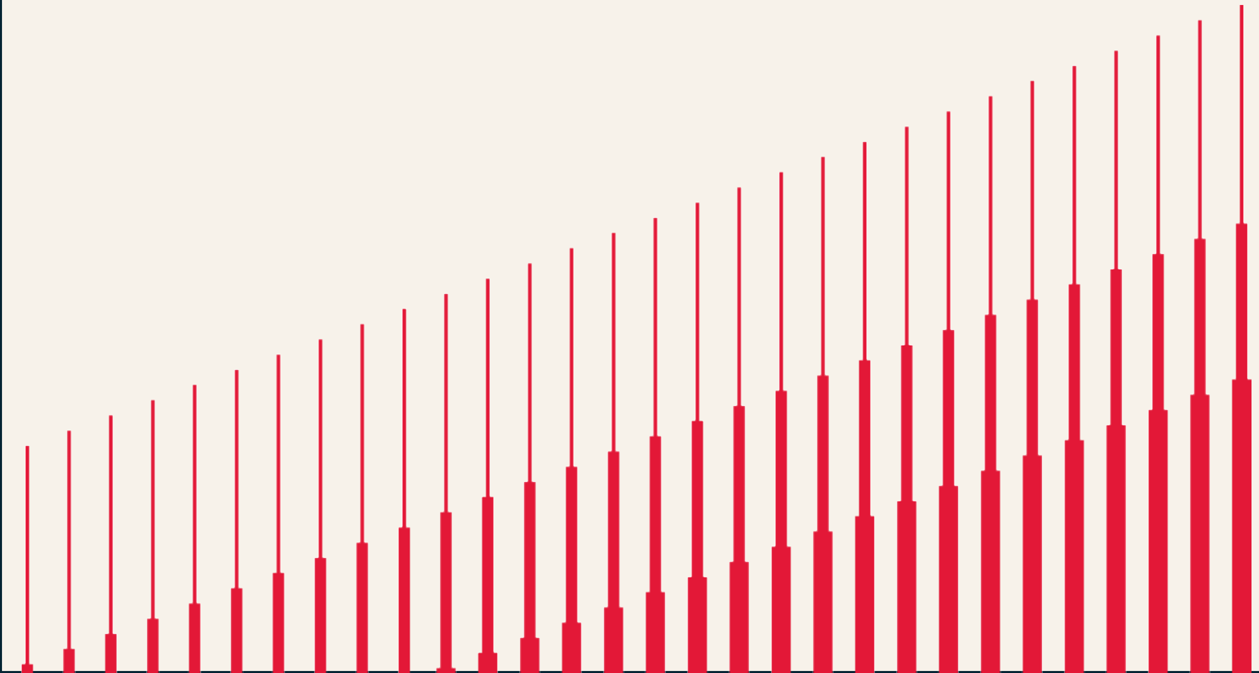
Each of these seven layers focuses on a specific area of trust. They also help securely manage workflows, enforce policies, and meet compliance requirements across layers.

Secure Identity and Entitlement	Data Trust and Privacy	Application and API Trust	Infrastructure Trust	Operations and Observability	Compliance and Governance Overlay	Platform and Integration Layer
Implements post-quantum cryptographic (PQC) protocols for identity assurance; integrates with existing IAM systems	Encrypts and masks data; integrates with data fabric, DLP, and cloud storage	Embeds runtime protection mechanisms for APIs and app components; performs analysis of microservices traffic	Validates device integrity with attestation from TPM or secure enclaves; logs infrastructure state changes with cryptographic audits	Generates the Trust Telemetry Index (TTI); integrates with SIEM, EDR, and observability platforms	Maps internal controls to regulatory requirements using AI; automates audit artifacts and impact assessments	Facilitates integration with DevSecOps, container runtimes, and policy engines; offers SDKs and APIs for rapid onboarding of partners; offers design benefits
A telco CSP provides time-bound access to 5G edge nodes using decentralized tokens for a partner IoT vendor	healthcare CSP converts patient records into tokens for AI model training while preserving data utility and meeting HIPAA compliance	A fintech CSP detects insider threats using GenAI to monitor API behavior	A smart factory provider uses secure enclaves to validate firmware updates on OT devices	A global CSP identifies lateral movement by linking IAM drift with unusual CPU spikes	A banking CSP uses this layer to auto-validate PCI-DSS controls across geographies	A cloud-native SaaS company integrates trust scoring into its B2B onboarding process

Agentic AI and Autonomous Trust Operations

What is Agentic AI?

Agentic AI refers to autonomous systems that operate within set ethical, regulatory, or operational limits. In QuantumTrust Fabric, Agentic AI helps manage trust, predict threats, and automatically correct policy errors, reducing the need for human intervention.



The Role of Agentic AI in QuantumTrust Fabric:

Autonomous Policy Enforcement

QuantumTrust uses Agentic AI to enforce trust policies in real-time based on:

- Context (user role, location, risk profile)
- System behaviour (latency, anomalous access, payload anomalies)
- Historical baselines and emerging risks

For instance, if a workload shows unusual internal traffic between cloud zones during off-hours, the agent automatically restricts access, notifies administrators, and starts capturing detailed telemetry.

GenAI-Powered Root Cause Analysis (RCA)

The operations and observability layer includes GenAI that performs analysis of:

- Infrastructure events
- API calls
- Identity logs
- SIEM alerts

It identifies the root causes of incidents and suggests remedial actions. Over time, it learns from the resolution feedback loops and gets better at predicting likely future violations.

Continuous Trust Optimization

The Agentic AI layer gathers trust signals from all system layers to constantly monitor the **TTI**. When the index drops below acceptable levels, the system automatically:

- Restricts access
- Alerts administrators
- Triggers deeper diagnostics and policy recalibration
- Initiates incident containment
- Recommends governance adjustments (e.g., access reviews or cryptographic key rotation)

Cross-Tower Correlation

For enterprises, QuantumTrust agents examine telemetry across application, infrastructure, and network towers. This allows:

- Cross-tower correlation of threat signatures
- Enforcement of access and encryption policies uniformly

Unified policy optimization across clients and tenants

Industry Applications and Use Cases

QuantumTrust Fabric is not a one-size-fits-all solution. It is designed to be context-aware and easily adaptable across various industries. Its layered architecture, modular deployment model, and ready-to-use integration connectors make it suitable for regulated and high-trust sectors.

Telecommunications (CSPs)

Use Cases:

5G Slice Security: Assigns specific trust policies to 5G network slices to support mission-critical workloads securely and reliably.

Edge Identity Assurance: Ensures edge nodes and central orchestration platforms communicate securely and reliably across locations, maintaining smooth operations and data safety.

Subscriber Behavioral Trust Scoring: Utilizes real-time, risk-based authentication based on subscriber behavior to verify identity and prevent unauthorized access.

GenAI-Driven NOC: Integrates trust signals directly into Network Operations Center (NOC) workflows to enable autonomous anomaly detection and response, improving operational resilience and reducing manual work.

Example:
A European CSP integrated QuantumTrust into its subscriber onboarding journey, utilizing TTI scores to assign identity verification levels and fraud detection policies in real-time.

Banking and Financial Services (BFSI)

Use Cases:

Perpetual KYC: Updates customer profiles in real time by merging internal and partner data, providing a more accurate view of customer behavior and preferences.

Open Banking API Security: Confirms external third-party requests using cryptographically signed trust assertions to ensure authenticity and reduce unauthorized access risks.

Tokenized Data Vaults: Creates encrypted personal data reserves to comply with GDPR and DPDPA, ensuring secure storage, controlled access, and privacy by design.

Example:
A Tier-1 bank used the compliance and governance overlay of QuantumTrust to automate impact assessments and internal audit trails under the EU's Digital Operational Resilience Act (DORA).

Manufacturing and Industry 4.0

Use Cases:

- **IIoT Trust Zones**: Secures interactions between factory sensors and cloud analytics systems to maintain data integrity, prevent unauthorized access, and provide reliable insights for industrial operations.
- **Digital Twin Integrity**: Validates the accuracy of digital replicas by tracing data through traceability chains, ensuring transparency, reliability, and trust in simulation results.
- **AI Co-Pilot Governance**: Applies policy-based restrictions to AI models that control robotic or predictive systems, ensuring performance remains within defined safety, compliance, and operational limits.

Example:

An automotive manufacturer implemented infrastructure-level verification to ensure that only approved firmware updates are applied across its global plant control systems.

Healthcare and Life Sciences

Use Cases:

- **Consent Traceability**: Maps the accessing and processing of personal health information (PHI) with patient consent logs, ensuring transparency and regulatory compliance.
- **Data Minimization Enforcement**: Ensures AI diagnostic systems access only the fields required for analysis, thereby protecting sensitive data and ensuring compliance with privacy regulations.
- **HIPAA Audit Automation**: Generates real-time snapshots of policy compliance for both internal audits and external reviews, enabling teams to stay up-to-date with regulatory standards and operational best practices.

Example:

A health-tech CSP offers "Trust-as-a-Service" to its clinical trial partners by integrating QuantumTrust with its data access workflows and audit platforms.

Business Value Metrics

QuantumTrust Fabric helps businesses become more resilient. It provides measurable results across operational efficiency, regulatory readiness, partner trust, and cost optimization. These benefits are essential for companies that operate in multi-cloud, regulated, and high-risk environments.

	Description	Benefits
Reduction in Compliance Preparation Time	Traditional compliance processes are labor-intensive and reactive. QuantumTrust automates control mapping and evidence generation by embedding Compliance and Governance Overlay across systems.	• 40 to 60% reduction • Before QuantumTrust: Average audit prep time ~4-6 weeks • After QuantumTrust: Reduced to 1-2 weeks with auto-generated compliance telemetry
Improved Mean Time to Resolution (MTTR)	Using GenAI for Root Cause Analysis (RCA) and policy drift detection, QuantumTrust helps Security Operations Centers (SOCs) to resolve incidents faster by identifying precise trust issues rather than just surface-level anomalies.	• 35 to 50% improvement in MTTR • Impact: 50% reduction in time to resolve high-severity incidents
Faster Partner Onboarding	With plug-and-play APIs and set trust policies, QuantumTrust simplifies and accelerates onboarding of new B2B clients, partners, or developers.	• Reduces onboarding cycle from 30 days to 12 days (up to 60%) • Accelerates time-to-market for new services and integrations • Ensures secure and policy-aligned access from day one • Improves partner satisfaction and scalability
Enhanced Trust Transparency	Through continuous measurement via the Trust Telemetry Index (TTI), enterprises gain visibility into their trust posture. This metric is reported to regulators, clients, and internal stakeholders.	• Increases brand reputation, improves audit readiness, and reinforces customer loyalty • 3x improvement in Trust transparency • Enables real-time trust scoring and anomaly detection • Supports pro-active governance and risk management
Operational Cost Savings	By merging tools, automating processes, and eliminating manual audits, QuantumTrust drives direct and indirect cost savings.	• Reduced tooling overlap and licensing costs • Fewer compliance breaches and penalties • Minimized time-to-market delays due to partner readiness gaps • Cuts manual labor and audit overhead • Overall operational costs savings of 20 to 25%

Future Vision and Strategic Evolution

As digital ecosystems evolve, the fabric shifts trust from a static requirement focused on compliance to a dynamic capability that continuously generates revenue and adapts to changes.

1. Trust as a Strategic Asset

In the future, trust metrics will have a direct impact on shareholder value, brand strength, and digital growth. Enterprises that demonstrate their trustworthiness through the use of telemetry, attestation, and automated policy controls will gain a competitive advantage in regulated and data-sensitive markets.

Example:
CSPs offering "Trust-as-a-Service" APIs will enable fintech and healthcare clients to evaluate infrastructure security before engaging in high-value digital transactions.

2. Integration with Future Paradigms

Post-Quantum Computing Readiness

By 2030, national security systems and regulated industries must implement NIST-approved post-quantum cryptographic (PQC) algorithms. **QuantumTrust Fabric** bridges the gap by supporting both current and PQC stacks, while managing the transition seamlessly.

Agentic AI Governance

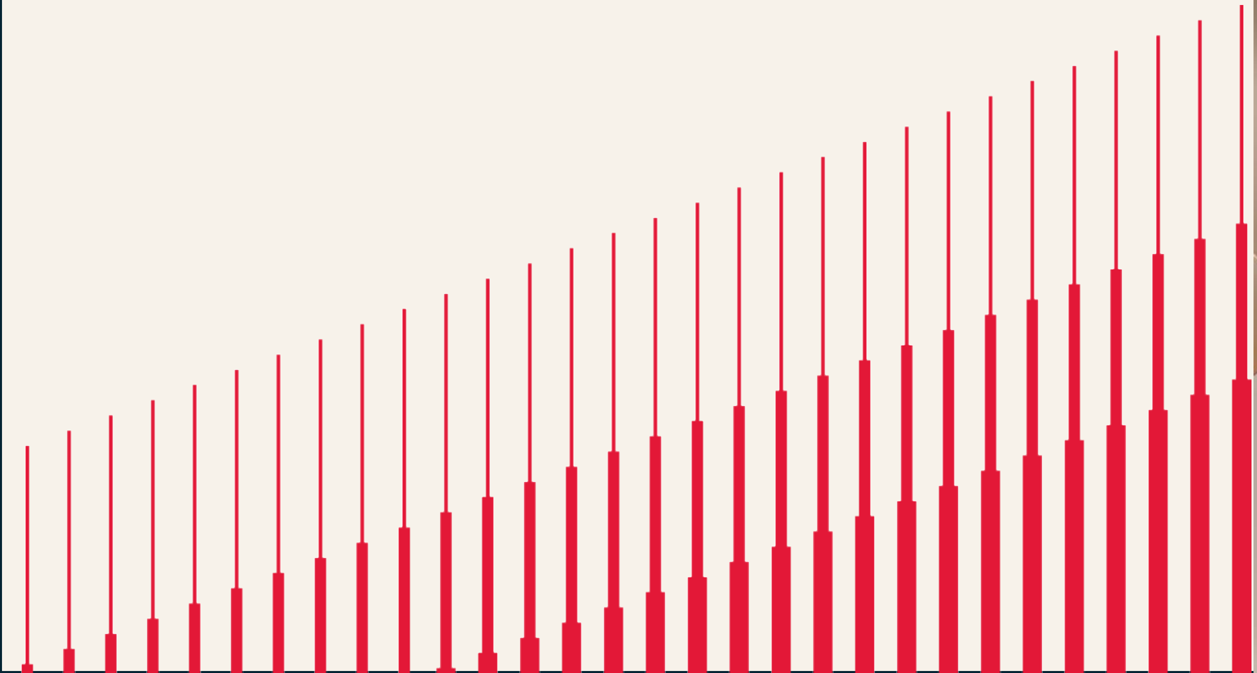
Enterprises will shift from human-in-the-loop control to machine-driven policy creation and enforcement. QuantumTrust's AI agents will evolve to:

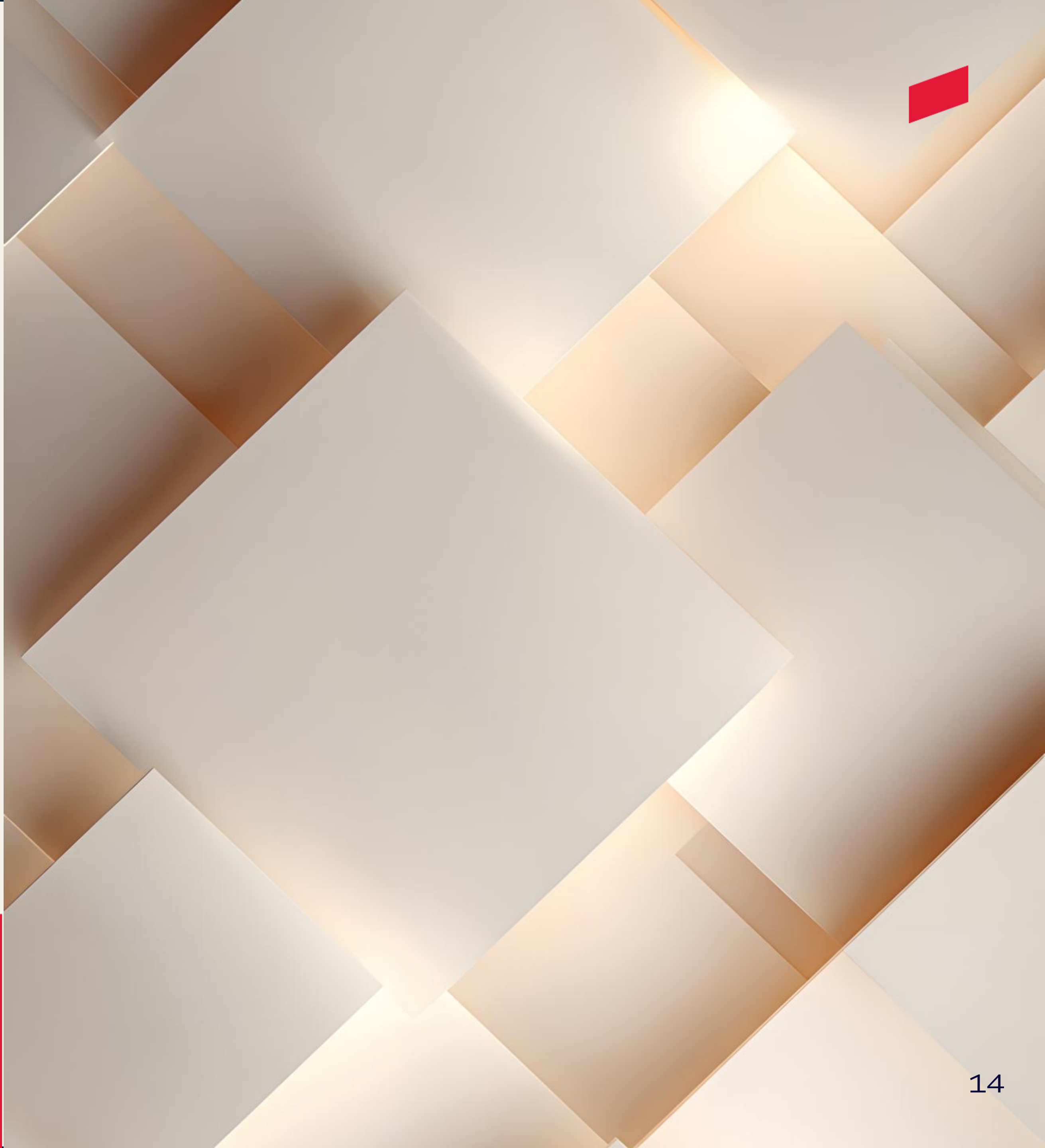
- Self-manage trust rules
- Justify decisions using explainable AI (XAI)
- Comply dynamically with future AI regulations (e.g., EU AI Act)

3. Ecosystem Monetization

Future versions of QuantumTrust will include:

- **Decentralized trust marketplaces**: Enterprises sharing verified trust artifacts using blockchain or zero-knowledge proofs
- **Trust-broker models**: CSPs serving as trust certifiers for smaller SaaS or edge providers
- **Revenue-sharing mechanisms**: Linked to verified trust levels and SLA compliance





4. Long-Term Evolution (10-Year Outlook)

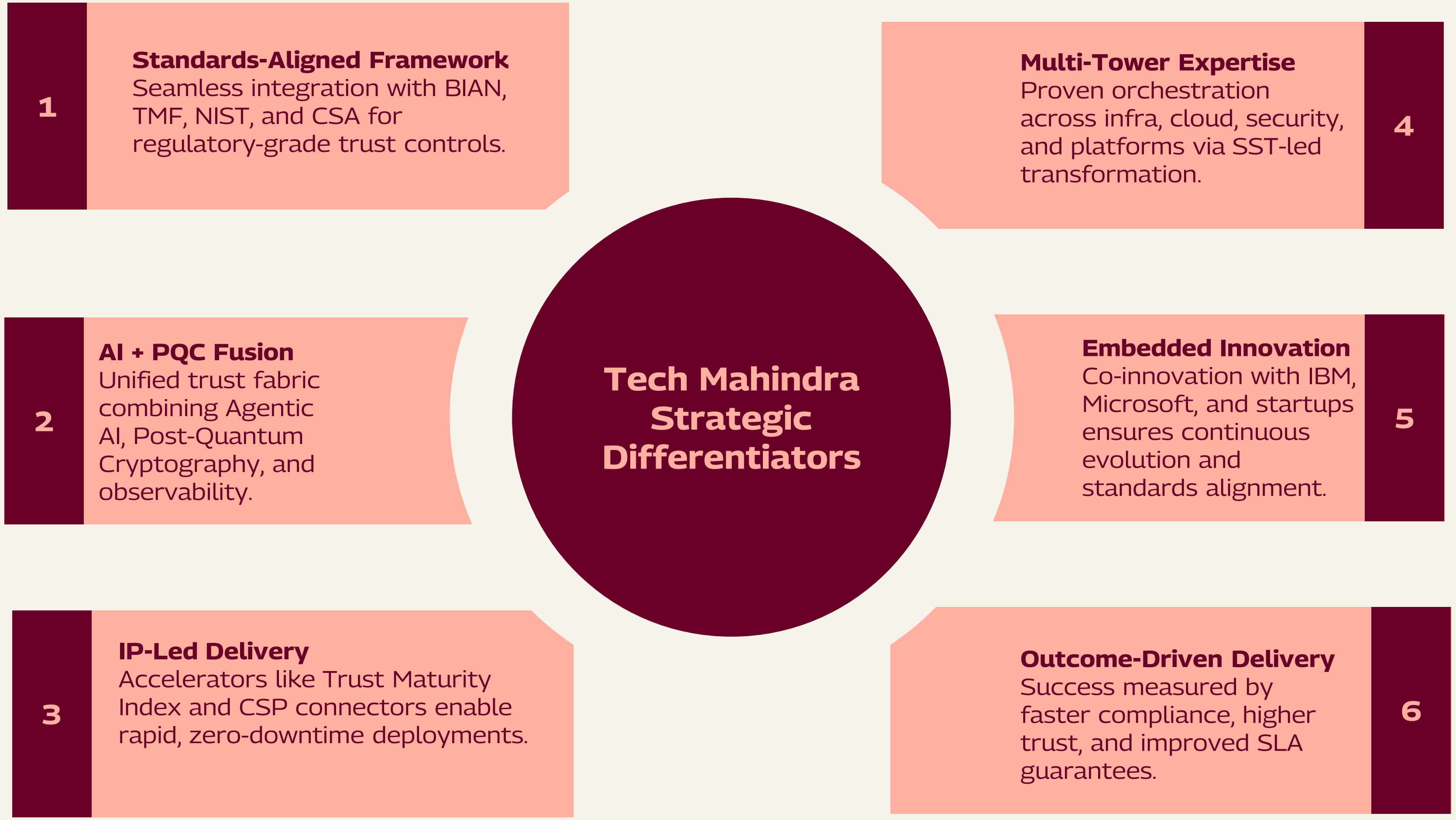
Horizon	2025-2026	2027-2028	2029-2030	2031+
Capabilities	Modular trust layers, PQC support, GenAI in SOCs	Trust telemetry SLAs, Trust-as-a-Service APIs	Autonomous trust ecosystems, AI-governed compliance	Self-sovereign enterprise trust identities, zero-breach architectures
Strategic Shift	Shift from siloed security to orchestrated trust zones	CSPs monetize trust transparency	Trust becomes part of brand equity and valuation	Fully composable, quantum-immune trust grids

Vision Statement

QuantumTrust Fabric will evolve beyond a security framework to become a global digital trust infrastructure. It will function across borders, clouds, and vendors, helping businesses grow securely in a world influenced by Agentic AI, decentralized ecosystems, and post-quantum threats.

Why Tech Mahindra?

What sets us apart is our ability to deliver **business-aligned, technically robust, and ecosystem-ready trust architectures** at scale.



Tech Mahindra Strategic Differentiators

1 **Standards-Aligned Framework**
Seamless integration with BIAN, TMF, NIST, and CSA for regulatory-grade trust controls.

2 **AI + PQC Fusion**
Unified trust fabric combining Agentic AI, Post-Quantum Cryptography, and observability.

3 **IP-Led Delivery**
Accelerators like Trust Maturity Index and CSP connectors enable rapid, zero-downtime deployments.

4 **Multi-Tower Expertise**
Proven orchestration across infra, cloud, security, and platforms via SST-led transformation.

5 **Embedded Innovation**
Co-innovation with IBM, Microsoft, and startups ensures continuous evolution and standards alignment.

6 **Outcome-Driven Delivery**
Success measured by faster compliance, higher trust, and improved SLA guarantees.

Client Quote

“Tech Mahindra’s QuantumTrust platform didn’t just secure our data; it redefined how we onboard partners, audit services, and build brand credibility.”
— CIO, Tier-1 APAC CSP

Conclusion

Digital trust is no longer optional. It is now a fundamental requirement. As cybersecurity becomes complex and quantum computing approaches mainstream adoption, CSPs and enterprises are required to shift from fragmented, reactive security models toward **orchestrated**, **proactive**, and **verifiable trust frameworks.**

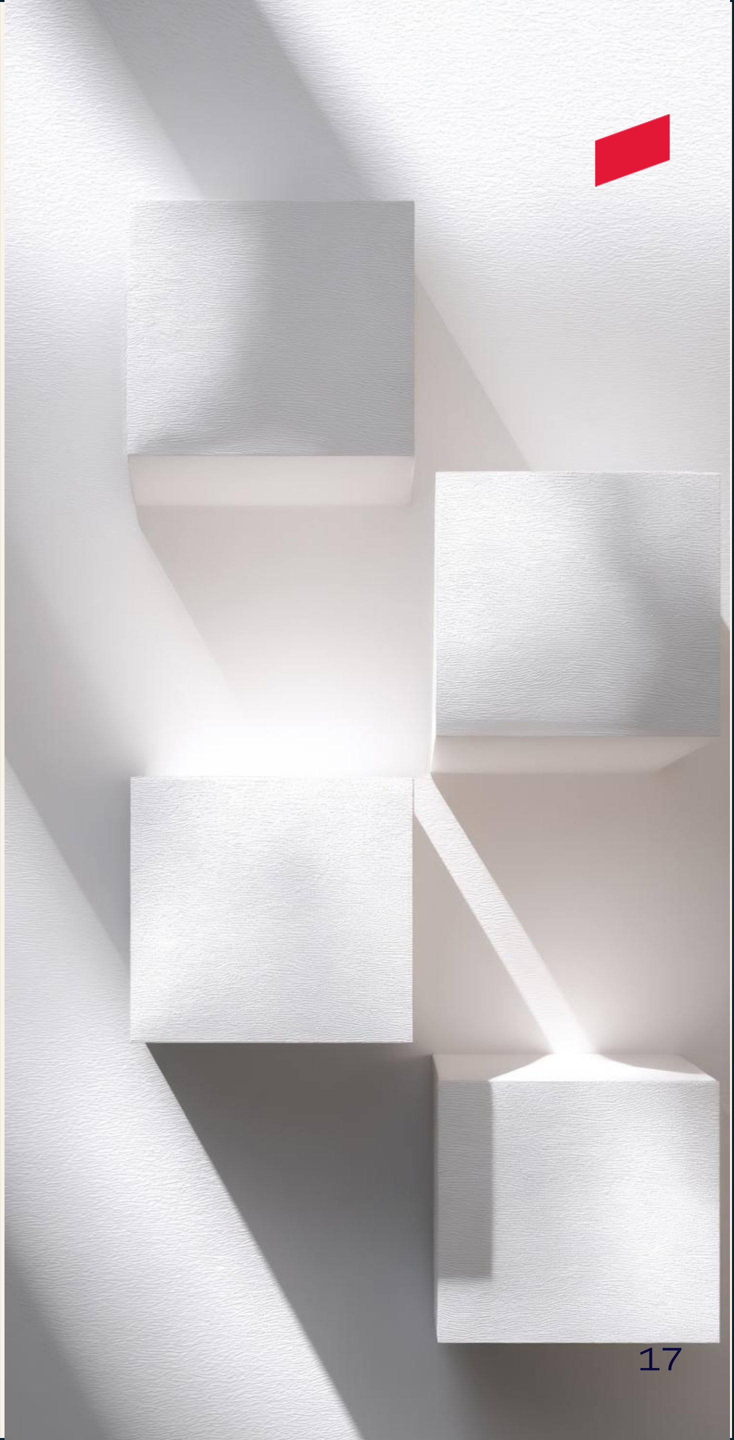
Tech Mahindra's QuantumTrust Fabric is leading this change. It redefines cybersecurity by making trust a **layered**, **measurable**, and **monetizable capability**. More than just a framework, it's a future-ready platform that integrates PQC, Agentic AI, and cross-domain telemetry to support resilient and secure digital ecosystems.

From Tier-1 telcos to emerging edge providers, the framework adapts to various needs by delivering outcomes like:

- Faster compliance alignment
- Measurable trust transparency
- Accelerated partner onboarding
- SLA-backed monetization of trust

QuantumTrust Fabric is designed to address both current and future risks, where trust is the primary objective, not merely a byproduct of security.

In a post-quantum world, trust becomes the true currency, not just data. Enterprises that can prove, measure, and monetize it will lead the next decade.



Author Details

Mukund Harale
Principal Solution Architect- Large Deals,
Strategic Solutions & Transformation,
Tech Mahindra

Vipul Rattan
Head-Offering Development & Strategic
Growth for Large Deals, Strategic
Solutions and Transformation,
Tech Mahindra

Mahesh Wandkar
Head, EA & Deal Origination-
Large Deals, Strategic Solutions
& Transformation,
Tech Mahindra

Ramesh Singh
Head Enterprise Architecture &
Solutions, Strategic Solutions and
Transformation Group (Large Deals),
Tech Mahindra

References

Cybersecurity Ventures: Global cybercrime cost projection

Microsoft: Microsoft's zero-trust security model.
https://www.microsoft.com/en-us/security/business/zero-trust

Deloitte: Post-quantum compliance and readiness survey [Insights].
Deloitte - Quantum Cyber Readiness Services

Gartner, Inc: Cybersecurity Mesh Architecture (CSMA).
Gartner - Cybersecurity Strategy

National Institute of Standards and Technology: NIST Post-Quantum Cryptography Standardization Project.
https://csrc.nist.gov/Projects/post-quantum-cryptography

IBM Security: IBM quantum safe readiness guide.
https://www.ibm.com/security/resources/quantum-safe-readiness-guide

Forrester Research: The future of security operations [Report].
https://www.forrester.com/report/the-future-of-security-operations/RES161462

About Tech Mahindra

Tech Mahindra (NSE: TECHM) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 152,000+ professionals across 90+ countries helping 1100+ clients, Tech Mahindra provides a full spectrum of services including consult-ing, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognises global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

TECH
mahindra

www.techmahindra.com
www.twitter.com/tech_mahindra
www.linkedin.com/company/tech-mahindra

Disclaimer: Brand names, logos, taglines, service marks, tradenames and trademarks used herein remain the property of their respective owners. Any unauthorized use or distribution of this content is strictly prohibited. The information in this document is provided on "as is" basis and Tech Mahindra Ltd. makes no representations or warranties, express or implied, as to the accuracy, completeness or reliability of the information provided in this document. This document is for general informational purposes only and is not intended to be a substitute for detailed research or professional advice and does not constitute an offer, solicitation, or recommendation to buy or sell any product, service or solution. Tech Mahindra Ltd. shall not be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. Information in this document is subject to change without notice.