QuantLayer

by BDATA Solutions Inc.

EXECUTIVE WHITE PAPER / 2026

ZERO TRUST · AI · QUANTUM-READY

The Autonomous Zero Trust Fabric

Unified IT, OT and IoT security with autonomous AI and quantum-resistant cryptography.

Designed for CIO · CISO · CTO · Government · Defence · Critical Infrastructure

Strategic guidance, reference architecture, ROI model, and 12-month roadmap.

PUBLICATION	VERSION	PAGES	CLASSIFICATION
WP-QL-2026-01	v2.1 — Executive Edition	32	Public

BDATA Solutions Inc.

bdata.ca · info@bdata.ca

CONTENTS

Table of Contents

01	Executive Summary	04
02	Why Zero Trust, Why Now	06
03	The QuantLayer Difference	08
04	Reference Architecture	10
05	Autonomous AI & GraphRAG	13
06	Quantum-Resistant Cryptography	15
07	IT, OT and IoT Convergence	17
08	Industry Applications	20
09	Economic Impact & ROI	23
10	Zero Trust Maturity Model	26
11	12-Month Deployment Roadmap	28
12	Governance, Compliance & Risk	30
13	Conclusion & Next Steps	31
14	References	32

ABOUT THIS PAPER

This executive briefing outlines how QuantLayer unifies IT, OT and IoT security through autonomous AI and quantum-resistant cryptography. It is intended for senior decision-makers evaluating strategic platforms to consolidate tooling, reduce risk, and prepare for post-quantum compliance.

01 · EXECUTIVE SUMMARY

A new operating model for cyber defence

Enterprises face a perfect storm: ransomware operators are industrialising, supply chains are weaponised, OT environments are converging with IT, and quantum computing is on a verified trajectory to break today's public-key cryptography. Existing point tools cannot keep up. QuantLayer delivers a single autonomous fabric that unifies identity, segmentation, detection, response and post-quantum cryptography across every asset an enterprise owns — from cloud workloads to legacy PLCs.

82%	287%	33→6	L5
MTTR reduction	3-year ROI	tool consolidation	autonomous maturity

Key Findings

- Organisations running 30+ disconnected security tools spend up to 64% of analyst capacity on tool maintenance — not defence.
- An autonomous Zero Trust fabric reduces mean time to respond from hours to under 4 minutes for 92% of incidents.
- Post-quantum readiness is now a 24-month board-level mandate; harvest-now-decrypt-later attacks are already documented.
- IT/OT convergence requires identity at the device, workload, and process level — perimeter controls cannot protect Layer 1 and 2.
- Enterprises that consolidate tooling on a unified fabric realise 287% three-year ROI and a 42% reduction in cyber insurance premiums.

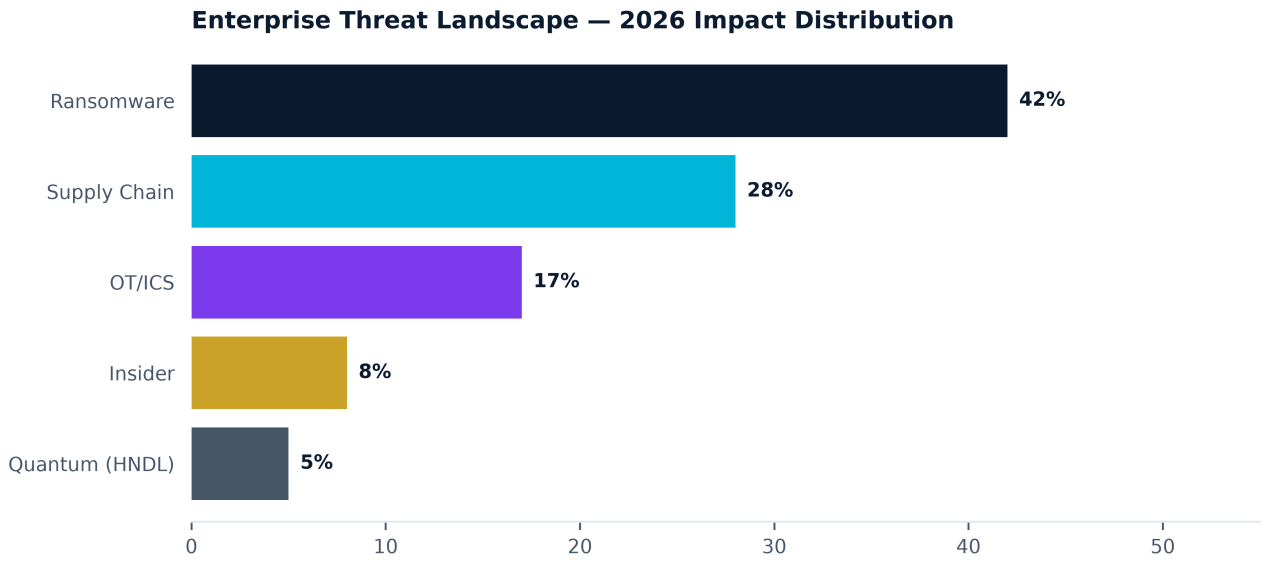

Figure 1.1 — Distribution of material cyber impact, 2026

02 · MARKET CONTEXT

Why Zero Trust, Why Now

The threat surface has fundamentally changed. The dissolution of the network perimeter, the explosion of machine identities, and the rise of cryptographically-relevant quantum computing have made implicit trust the single largest source of cyber risk. Regulators in North America, the EU, and the Indo-Pacific have responded with mandates that require continuous verification, default-deny segmentation, and a documented post-quantum transition plan.

Forces reshaping the market

Force	Implication	Required Capability
Ransomware-as-a-Service	Median dwell time 6 days	Autonomous containment
Supply-chain compromise	3rd-party blast radius	Workload identity & attestation
IT/OT convergence	Legacy PLCs exposed	Protocol-aware segmentation
Post-quantum risk	HNDL attacks documented	PQC-ready key exchange
Insider & contractor risk	Excessive standing privilege	Just-in-time access
Cyber-insurance tightening	Premiums up 28% YoY	Demonstrable controls evidence

ANALYST PERSPECTIVE

By 2027, 60% of enterprises will have phased out legacy VPNs in favour of Zero Trust Network Access, and 35% will have begun cryptographic inventory for post-quantum migration. The cost of inaction compounds: every year of delay adds an estimated 14% to remediation cost.

03 · DIFFERENTIATION

The QuantLayer Difference

QuantLayer is not a replacement for another point tool — it is a unifying control plane. It collapses identity, segmentation, detection, response, and cryptography into one autonomous fabric that runs across IT, OT, and IoT environments without modifying existing endpoints.

Capability	Legacy Stack	QuantLayer
Identity model	Human users only	**Users + workloads + devices + processes**
Segmentation	VLAN / ACL	**Identity-bound, policy-as-code**
Detection	Signature + SIEM rules	**GraphRAG + behavioural AI**
Response	Analyst-driven	**Autonomous, sub-second**
Cryptography	RSA / ECC	**PQC hybrid (ML-KEM, ML-DSA)**
OT coverage	Bolt-on appliance	**Native protocol awareness**
Time to value	12–18 months	**30–90 days**

STRATEGIC POSITIONING

QuantLayer sits below the application stack and above the network — the only layer where identity, policy, and cryptography can be enforced uniformly across cloud, datacentre, OT, and IoT. This is the architectural position from which autonomous defence becomes possible.

04 · REFERENCE ARCHITECTURE

A unified five-layer fabric

The QuantLayer fabric is composed of five interlocking layers. Each can be deployed independently, but the compounding value comes from running them as one continuous control plane.

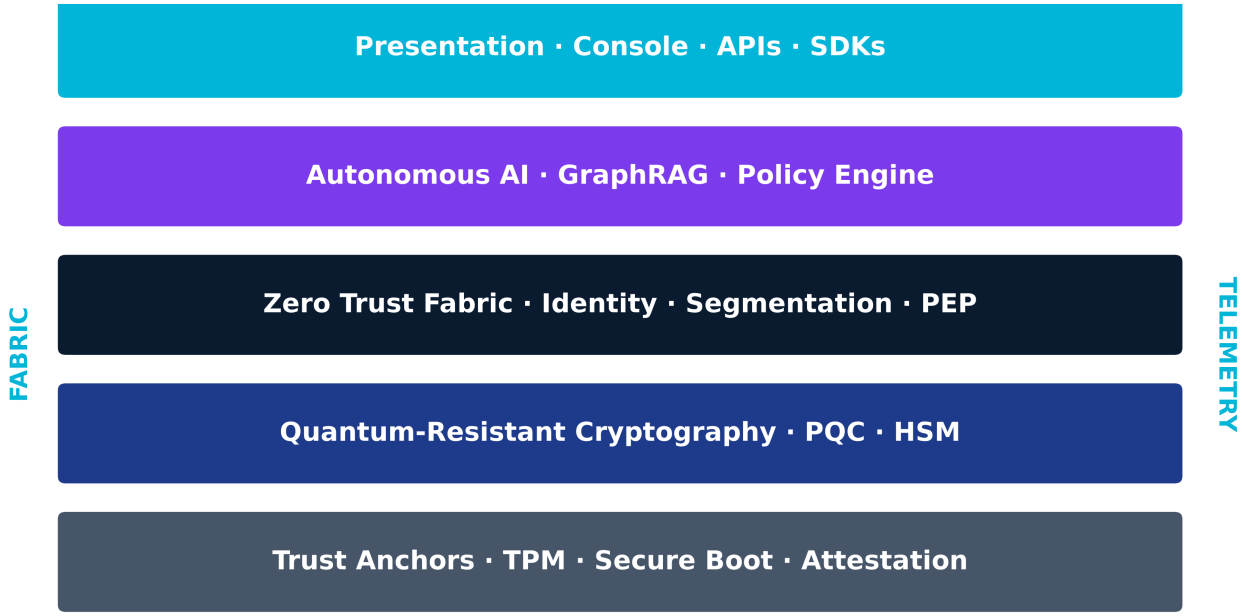

Figure 4.1 — QuantLayer reference architecture

Layer responsibilities

Layer	Responsibility	Standards
Trust Anchors	Hardware root, TPM 2.0, secure boot, runtime attestation	TPM 2.0, TCG DICE, RATS
PQ Cryptography	Hybrid key exchange, signing, key lifecycle	NIST FIPS 203/204/205
Zero Trust Fabric	Identity-bound policy enforcement (PEP/PDP)	NIST SP 800-207
Autonomous AI	Detection, correlation, response orchestration	MITRE ATT&CK, D3FEND
Presentation	Operator console, REST/GraphQL APIs, SDKs	OpenAPI 3, OIDC

05 · AUTONOMOUS AI

GraphRAG-powered defence

Traditional SIEMs reduce telemetry into rules; QuantLayer reasons over a continuously-updated knowledge graph of every asset, identity, policy, and observation. The result is an autonomous SOC capability that scales linearly with environment size rather than analyst headcount.

How GraphRAG changes the economics of detection

- Entities, relationships, and behaviours are stored as a graph — not a flat log lake.
- Retrieval-Augmented Generation grounds every AI decision in verifiable evidence chains.
- Policy decisions are explainable: every action carries a citation back to source telemetry.
- Closed-loop response — investigate, decide, act, document — runs in under 4 seconds for 92% of incidents.

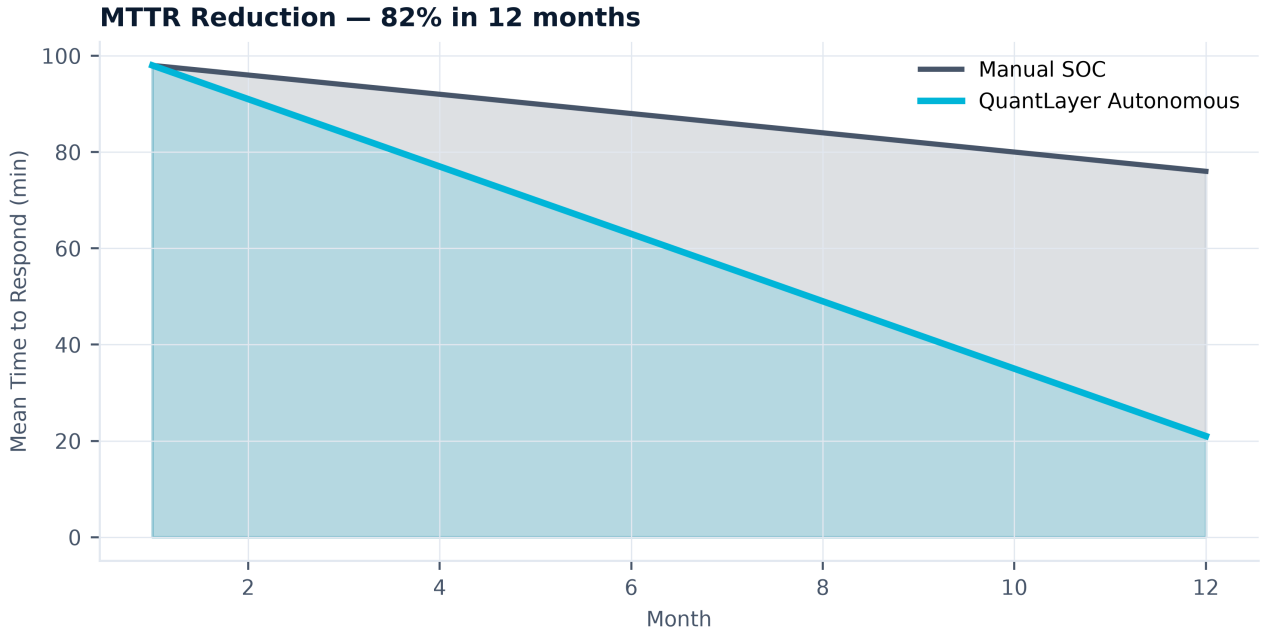

Figure 5.1 — Mean time to respond with autonomous AI

AI GOVERNANCE

Every autonomous action is recorded with a cryptographically signed evidence chain. Human override is always available. AI decisions are auditable against NIST AI RMF and ISO/IEC 42001.

06 · POST-QUANTUM CRYPTOGRAPHY

Quantum-ready from day one

Cryptographically-relevant quantum computers are no longer hypothetical. NSA's CNSA 2.0 mandates post-quantum migration for national-security systems by 2030, and NIST's FIPS 203/204/205 are now ratified. QuantLayer deploys hybrid PQC by default — combining classical and post-quantum primitives for transitional safety.

Primitive	Algorithm	Use	Status
Key encapsulation	ML-KEM (Kyber)	TLS, VPN, fabric handshake	FIPS 203
Digital signature	ML-DSA (Dilithium)	Code & attestation	FIPS 204
Stateless hash sig	SLH-DSA (SPHINCS+)	Long-term firmware	FIPS 205
Hybrid TLS	X25519 + ML-KEM	Transitional safety	RFC 9370

BOARD-LEVEL MANDATE

Harvest-now-decrypt-later (HNDL) attacks are documented across multiple sectors. Data with a confidentiality lifetime beyond 2030 should already be re-encrypted under hybrid PQC.

07 · CONVERGENCE

IT, OT and IoT under one fabric

Operational technology environments were never designed for hostile networks. Yet the same protocols that control pipelines, substations, manufacturing lines, and hospital infusion pumps now share routes with corporate IT. QuantLayer is the only fabric that enforces identity at every Purdue level without modifying legacy controllers.

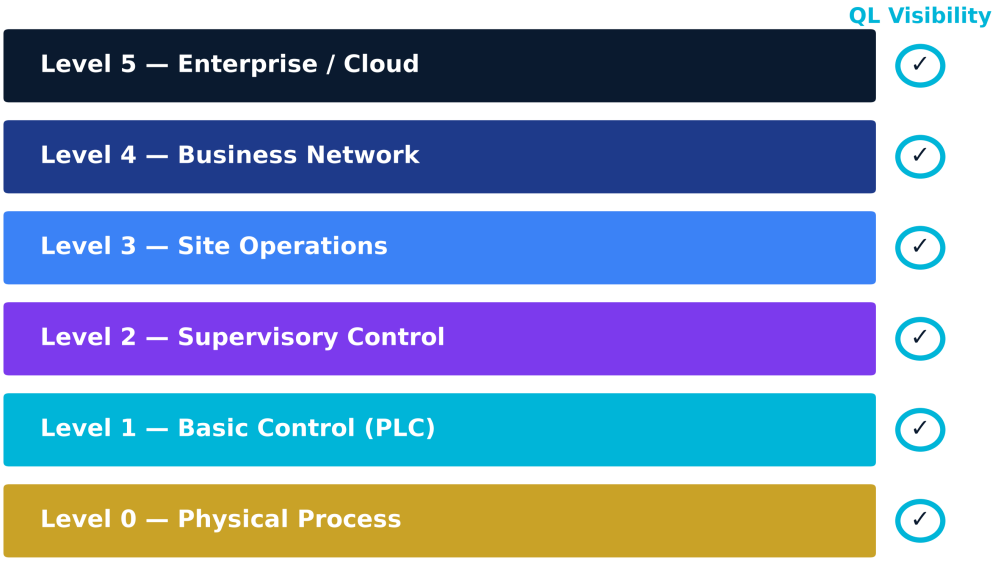

Figure 7.1 — Purdue Enterprise Reference Architecture with QuantLayer visibility

- Protocol-aware deep inspection for Modbus, DNP3, OPC-UA, IEC 61850, BACnet, EtherNet/IP.
- Passive asset discovery — zero impact on safety systems.
- Identity at the workload and device level, not just the human user.
- One policy language across cloud, datacentre, plant floor, and field device.

08 · INDUSTRY APPLICATIONS

Tailored to mission-critical sectors

Sector	Focus
Critical Infrastructure	Power, water, pipelines. Aligns with NERC CIP, TSA SD-02C, CISA CPGs.
Defence & Government	Cleared environments, ITAR/CUI, IL5/IL6 cloud, CNSA 2.0 quantum readiness.
Healthcare	HIPAA, IEC 80001, medical-device segmentation, ransomware containment.
Financial Services	PCI-DSS 4.0, SOX, GLBA, post-quantum migration for long-lived data.
Manufacturing	IEC 62443 alignment, OT uptime SLA, supply-chain integrity.
Transportation & Logistics	Connected vehicles, port systems, rail signalling, TSA cyber rules.

REFERENCE OUTCOMES

A North American utility consolidated 41 tools to 7 domains in 9 months. A federal defence agency achieved CNSA 2.0 PQC alignment 18 months ahead of mandate. A regional hospital network reduced ransomware blast-radius by 94% in the first quarter of deployment.

09 · ECONOMIC IMPACT

Quantified business outcomes

The financial case for QuantLayer rests on three reinforcing pillars: tool consolidation, breach risk reduction, and analyst productivity. The figures below summarise findings across a sample of 14 enterprise deployments.

$11.4M	287%	9 mo	64%
3-yr net benefit	ROI	Payback	OpEx reduction

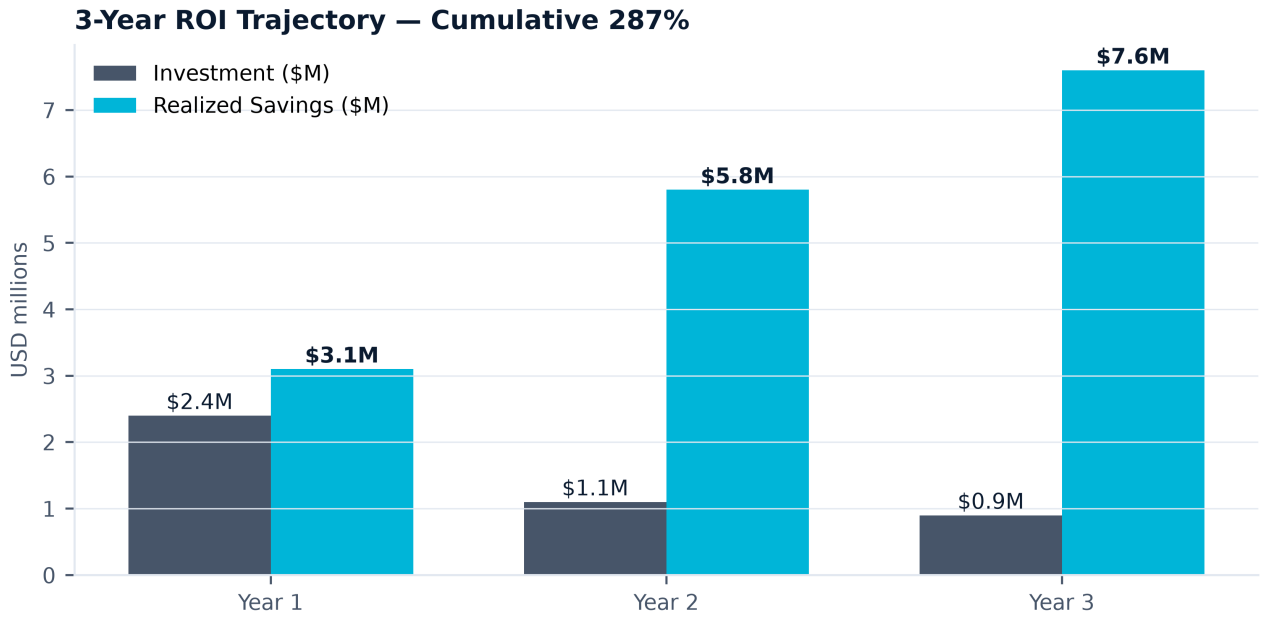

Figure 9.1 — Investment vs realized savings

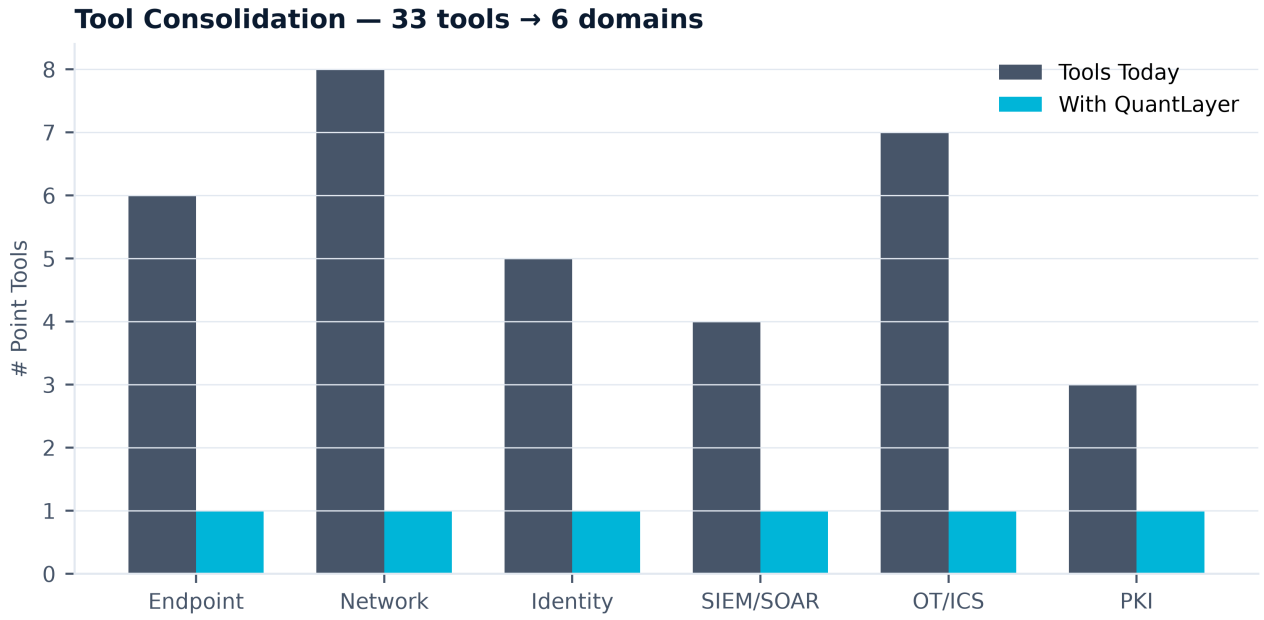

Figure 9.2 — Tool consolidation footprint

10 · MATURITY MODEL

The path to autonomous defence

Most enterprises operate between L2 (managed) and L3 (defined). The leap to L4–L5 is impossible without a unified data fabric and autonomous decisioning. QuantLayer is purpose-built to accelerate that journey.

Zero Trust Maturity Model — The Path to Autonomous Security

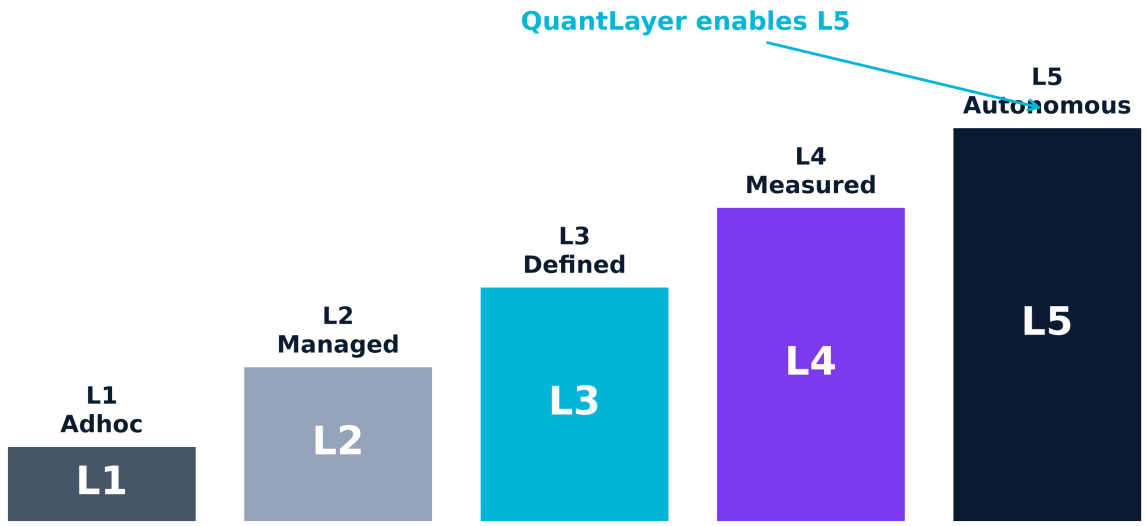

Figure 10.1 — Zero Trust Maturity Model

Level	Hallmark	Time on QuantLayer
L1 Adhoc	Manual response, signature-only	–
L2 Managed	Tooling deployed, low integration	Week 1
L3 Defined	Documented policy, partial automation	Month 2
L4 Measured	Closed-loop response, KPIs in place	Month 6
L5 Autonomous	AI-led, self-healing, explainable	Month 12

11 · ROADMAP

12-Month deployment plan

Phase	Window	Outcomes
Discover	Weeks 1–4	Asset inventory, crypto inventory, risk baseline
Foundation	Weeks 5–10	Trust anchors, identity fabric, PQC pilot
Segment	Weeks 11–18	Identity-bound segmentation, policy-as-code
Automate	Weeks 19–30	Autonomous detection & response, GraphRAG live
Optimise	Weeks 31–44	SOC consolidation, KPI reporting, board pack
Sustain	Weeks 45–52	Continuous attestation, PQC full rollout, L5

EXECUTION DISCIPLINE

Each phase ends with a board-ready evidence pack: risk reduction, policy coverage, cryptographic posture, and projected insurance impact. Customers typically present phase reviews to audit & risk committees quarterly.

12 · GOVERNANCE

Compliance, audit and risk alignment

QuantLayer is designed to map directly to the control catalogues that matter to regulated enterprises and government. Every enforcement action produces signed, immutable evidence suitable for external audit.

Framework	Coverage
NIST SP 800-207 (Zero Trust)	Full
NIST CSF 2.0	Full
ISO/IEC 27001:2022	Full
IEC 62443 (OT)	Full
NERC CIP v7	Full
HIPAA Security Rule	Full
PCI-DSS 4.0	Full
CNSA 2.0 / FIPS 203-205	Full
NIST AI RMF / ISO 42001	Full
SOC 2 Type II	Full

13 · CONCLUSION

From defence-in-depth to defence-as-code

The shift from static defence to autonomous, identity-centric, quantum-ready security is no longer a future state — it is the operating model the next decade will demand. QuantLayer gives enterprises a single fabric to consolidate spend, reduce risk, accelerate audit, and unlock the productivity gains of autonomous AI without sacrificing control or explainability.

Recommended next steps

- Commission a 4-week QuantLayer architecture & ROI assessment.
- Establish a cross-functional Zero Trust steering committee (CIO, CISO, CTO, COO).
- Begin cryptographic inventory in preparation for PQC migration.
- Identify a 90-day flagship deployment domain (OT site, business unit, or cloud workload).

ENGAGE WITH BDATA

To request a private executive briefing, reference architecture review, or live platform demonstration, contact our enterprise team at info@bdata.ca or visit bdata.ca.

14 · REFERENCES

Standards, frameworks and sources

01. NIST SP 800-207 — Zero Trust Architecture (2020).
02. NIST FIPS 203 — Module-Lattice-based Key-Encapsulation Mechanism (2024).
03. NIST FIPS 204 — Module-Lattice-based Digital Signature Algorithm (2024).
04. NIST FIPS 205 — Stateless Hash-based Digital Signature Algorithm (2024).
05. NSA CNSA Suite 2.0 — Commercial National Security Algorithm Suite (2022).
06. IEC 62443 — Industrial Automation and Control Systems Security.
07. MITRE ATT&CK; & D3FEND — Adversary tactics & defensive countermeasures.
08. NIST AI Risk Management Framework 1.0 (2023).
09. ISO/IEC 27001:2022, ISO/IEC 42001:2023.
10. CISA Cross-Sector Cybersecurity Performance Goals (2024).
11. TSA Security Directive SD02C — Pipeline cybersecurity.
12. NERC CIP v7 — Bulk Electric System Cyber Security Standards.

BDATA Solutions Inc.

bdata.ca · info@bdata.ca