QuantLayer

Critical Infrastructure Whitepaper

CRITICAL INFRASTRUCTURE · WATER SECTOR

Securing Canada's Water Infrastructure

AI-Orchestrated Zero Trust for Modern Water Treatment Systems

Protecting drinking water, wastewater, pumping stations and critical infrastructure through immutable identity, continuous authentication and autonomous threat response.

DOCUMENT
Sector Whitepaper
v1.0 · July 25, 2026

AUDIENCE
Utilities · Municipalities
CISO · OT Security · Ops

CLASSIFICATION
Public — Advisory
Powered by BDATA

CONTACT
info@bdata.ca
bdata.ca

Table of Contents

ABOUT THIS DOCUMENT

This whitepaper describes how AI-orchestrated Zero Trust — delivered through the QuantLayer™ platform — can protect Canada's drinking water, wastewater, and distribution infrastructure against modern cyber threats. It is written for utility executives, municipal CISOs, operational technology leads, and government policy teams responsible for sector resilience. The technical narrative draws on Canadian government threat assessments and consulting-sector Zero Trust reference architectures.

Sector-specific
Water treatment, wastewater, distribution, remote stations

Standards-aligned
IEC 62443, NIST 800-207, CSF 2.0, GoC readiness goals

AI-orchestrated
Continuous verification, adaptive policy, autonomous response

01 Executive Summary

Water is Canada's most essential public utility. The systems that treat, monitor, and distribute it — from remote pumping stations to municipal SCADA networks — have quietly transformed into digital, interconnected environments. That transformation delivers efficiency, but it also exposes drinking water, wastewater, and distribution operations to the same adversaries targeting energy, healthcare, and government.

WHY THIS MATTERS NOW

- State-sponsored intrusion campaigns (Volt Typhoon and Iranian-affiliated actors) have been observed pre-positioning in North American water utilities.
- Ransomware operators increasingly target utilities of every size, exploiting flat networks, remote access, and shared credentials.
- Supply-chain compromises (SolarWinds, MOVEit) show that trusted software is now a common attack path into OT.
- Legacy PLCs, RTUs, HMIs and vendor VPNs were never designed for adversarial network conditions.

≈4,000	70%+	3×	<1s
Water systems across Canada	Utilities using remote engineering access	Growth in OT-targeted intrusions since 2022	Required response window for ICS attacks

THE QUANTLAYER APPROACH

QuantLayer™ replaces perimeter and password-based trust with an identity-first, AI-orchestrated Zero Trust fabric. Every user, engineer, OEM technician, PLC, RTU, HMI, and cloud service is cryptographically attested and continuously verified. Policies adapt in real time based on behavior, posture, and risk — and autonomous response contains threats before they reach chemical dosing, pump control, or distribution logic.

> **EXECUTIVE INSIGHT**
>
> Perimeter defense assumed the plant network could be trusted. In modern water operations — with cloud historians, remote maintenance, and vendor access — that assumption no longer holds. Continuous verification is the new perimeter.

02 Canada's Water Infrastructure Landscape

Canadian water infrastructure spans thousands of municipal utilities and regional authorities, each operating a mix of legacy and modernized control systems. Treatment plants, reservoirs, distribution networks, and remote pumping stations increasingly rely on digital telemetry, cloud monitoring, and third-party maintenance.

Treatment Plants
Filtration, disinfection, chemical dosing, quality monitoring

Wastewater
Lift stations, aeration, sludge processing, effluent monitoring

Reservoirs & Storage
Level control, tank sensors, pressure management

Distribution
Pressure zones, valve stations, smart meters, leak detection

Remote Pumping
Cellular / radio backhaul, unmanned RTUs, DNP3 telemetry

Cloud & Remote Ops
Historians, dashboards, mobile SCADA, OEM vendor access

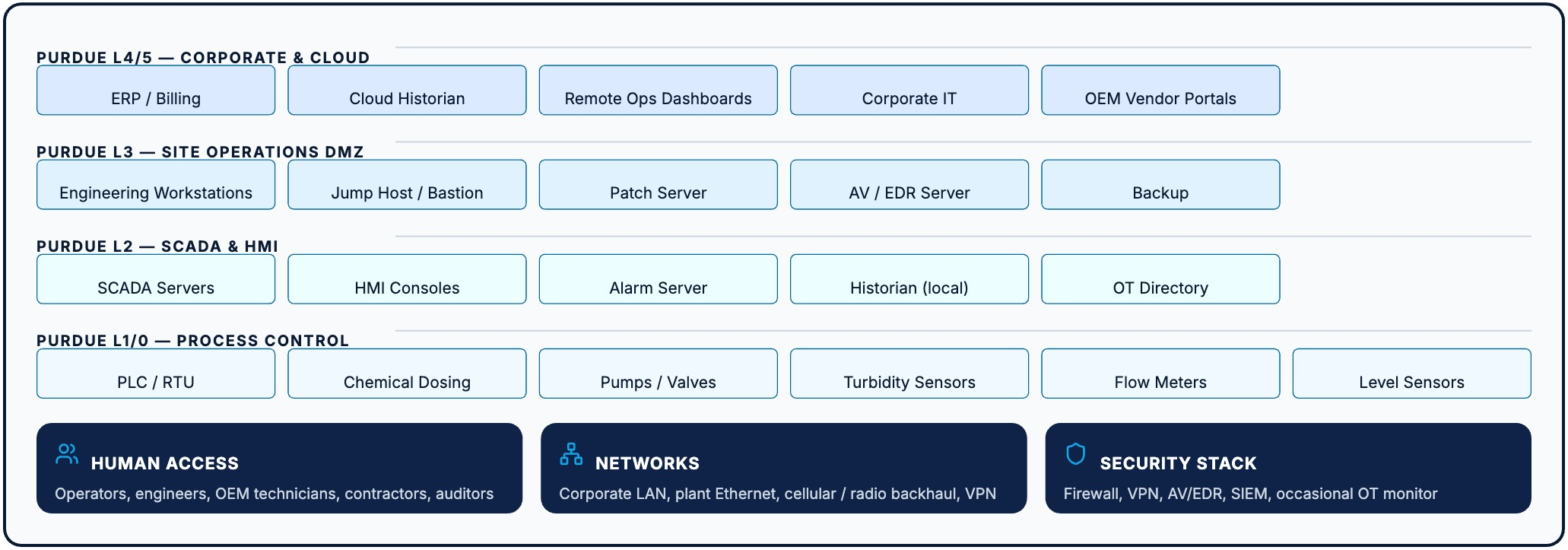
DIGITAL TRANSFORMATION DRIVERS

- Aging workforce and reduced on-site staffing drive adoption of remote SCADA and cloud dashboards.
- Regulatory requirements demand more granular monitoring, reporting, and continuous evidence.
- OEM support models rely on always-on vendor VPN access to PLCs, HMIs, and analyzers.
- Smart-meter and IIoT rollouts push network reach beyond traditional plant boundaries.

> **OPERATIONAL REALITY**
> A typical mid-size Canadian water utility runs 20–200 PLCs, 5–15 SCADA workstations, several OEM vendor connections, and a public-cloud historian — all interdependent, and most protected by little more than a shared VPN and perimeter firewall.

03 Reference Water Utility Architecture

A generalized, technology-neutral view of a modern Canadian water utility environment.



WHY THIS MATTERS

Each Purdue layer historically implied a trust boundary. In modern operations these boundaries are routinely bypassed — vendor VPNs terminate at L2, cloud historians reach into L3, and remote operators connect from anywhere. Trust must move from the network to identity.

04 Threat Landscape — State, Criminal, Hacktivist

The Canadian Centre for Cyber Security has consistently assessed critical infrastructure — including water — as a strategic target for state-sponsored and criminal actors. The threat is no longer theoretical; adversaries are actively pre-positioning, extorting, and probing utility environments across North America.

Actor Class	Examples	Objective	Method
State-sponsored	Volt Typhoon, Iranian IRGC-linked groups	Pre-position, disruption capability	LOTL, valid credentials, exposed PLCs
Ransomware crews	LockBit, BlackCat, Cl0p affiliates	Extortion, service disruption	Phishing, RDP, VPN exploits
Hacktivists	CyberAv3ngers, pro-nation groups	Symbolic disruption, propaganda	Default passwords, exposed Unitronics/Modbus
Supply-chain	SolarWinds, MOVEit, 3CX	Indirect access via trusted software	Trusted-update compromise
Insiders	Disgruntled ops or contractors	Sabotage or theft	Legitimate access, few controls

WHY WATER IS A RISING TARGET

- High public-health and political impact from even minor disruptions.
- Small utilities often lack dedicated OT security staff and 24/7 monitoring.
- Exposed PLC brands (Unitronics, Modicon, Siemens) are trivially discoverable on Shodan.
- Remote vendor access rarely follows least-privilege or session recording principles.

CYBER CENTRE ASSESSMENT

The Government of Canada assesses that state-sponsored cyber actors are almost certainly capable of disrupting Canadian critical infrastructure, and that water is among the sectors with meaningful residual risk due to legacy control systems and limited monitoring.

05 Notable Attacks & Attack Timeline

A representative — not exhaustive — chronology of publicly reported water-sector cyber incidents.

2000 Maroochy Water (AU)
Insider used stolen radio equipment to release 800,000 L of sewage — first widely documented OT attack.

2016 Kemuri Water (US)
Attackers altered treatment chemical levels via an internet-exposed SCADA web portal.

2021 Oldsmar, Florida
Remote intrusion via TeamViewer changed sodium hydroxide setpoint by 100×.

2023 Aliquippa, Pennsylvania
CyberAv3ngers compromised Unitronics PLC at a water booster station using default credentials.

2024 Multiple US utilities
EPA and CISA warn of ongoing Iranian and Russian-linked intrusions across small utilities.

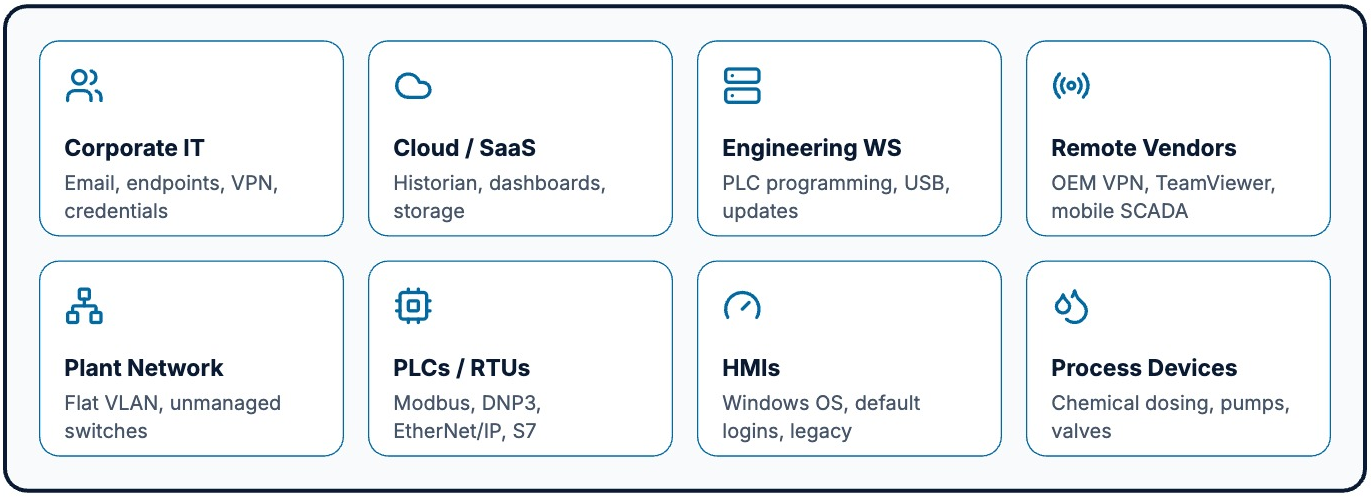
2025 Volt Typhoon pre-positioning
Five Eyes agencies confirm long-dwell access in US critical infrastructure — including water.

PATTERN RECOGNITION

Nearly every publicly known water incident traces back to three root causes: exposed remote access, default or shared credentials, and flat networks with no segmentation between IT and process control. Each of these is directly addressable with Zero Trust.

06 Current Water Plant Attack Surface

The modern water utility exposes multiple attack surfaces that adversaries chain together.



COMMON ATTACK VECTORS OBSERVED

- Phishing → corporate credential theft → VPN to plant DMZ.
- OEM technician laptop compromise → vendor VPN → engineering workstation → PLC.
- Internet-exposed HMI or PLC with default credentials, directly discoverable.
- Cloud historian API key exfiltration → tampering of operational baselines.
- USB or removable-media used for legitimate updates but weaponized for malware.

07 Attack Path Analysis — Contractor to PLC

A realistic multi-stage intrusion chain against a mid-size water utility.

STAGE 1

Stage 1 — Initial Access
Contractor laptop compromised via phishing malware. Credentials cached for utility VPN.

STAGE 2

Stage 2 — Reconnaissance
Attacker enumerates internal DNS, discovers SCADA subnet, historian, engineering workstation.

STAGE 3

Stage 3 — Lateral Movement
Reuses cached admin credentials to pivot from IT to plant DMZ. RDP into engineering workstation.

STAGE 4

Stage 4 — OT Access
Uses vendor engineering tool to connect to PLC over Modbus/TCP. Reads ladder logic.

STAGE 5

Stage 5 — Impact
Modifies chemical dosing setpoint or pump control logic. Suppresses HMI alarms.

IMPACT

A single compromised contractor laptop — with no additional zero-day required — can traverse from IT to process control in under an hour. Every stage exploits a trust boundary that Zero Trust is designed to eliminate.

08 Challenges of Traditional Security

Perimeter security worked when plant networks were physically isolated. That model no longer reflects how utilities actually operate.

Control	Historical Assumption	Modern Reality
VPN	Only trusted users on the inside	Credential theft → full lateral access
Perimeter firewall	Attacks come from the internet	Attacks arrive via vendor VPN, cloud, USB
Passwords / shared logins	Users protect their credentials	Reused, shared, phished, cached everywhere
Flat plant network	Physical isolation is enough	OEM & cloud traffic routinely cross boundaries
Legacy OT devices	Not internet-connected	Reachable via jump hosts, VPN, or Shodan
Manual IR	SOC has time to respond	OT attacks execute in seconds, not hours
Signature-based detection	Known malware dominates	Living-off-the-land, valid credentials

CONSULTING INSIGHT

Layering more perimeter tools on legacy assumptions does not close the gap. The architectural shift required is from network-based trust to identity-based, continuously evaluated trust — for every user, device, and machine identity.

09 Why Zero Trust is Now Required

Zero Trust — codified in NIST SP 800-207 and echoed in the Government of Canada cyber security readiness goals — replaces implicit network trust with continuous, explicit verification of every access request.

Never Trust
No user, device, or workload is trusted by default — including OT.

Always Verify
Every session cryptographically attested and re-verified continuously.

Least Privilege
Access scoped to exactly what the identity requires, and no more.

Micro-segmentation
Cell / zone / conduit segmentation aligned to IEC 62443.

Continuous Auth
Trust score recomputed as posture and behavior change.

Adaptive Policy
Policy engine adjusts privilege based on real-time risk.

Every access request — human or machine — is evaluated in real time.

10 Introducing QuantLayer

QuantLayer™ is an AI-orchestrated Zero Trust platform purpose-built for converged IT and OT environments. It combines immutable device identity, continuous authentication, adaptive policy, and autonomous response into a single control fabric that operates across a utility's entire estate.

Immutable Device Identity

Hardware-rooted machine fingerprints for every PLC, HMI, RTU, workstation and cloud workload.

Continuous Authentication

Passwordless, cryptographic re-verification of every session — human and machine.

AI Orchestration

Continuous trust scoring, behavior analytics, and adaptive policy — under human governance.

Autonomous Response

Sub-second containment: isolate, quarantine, revoke tokens, block sessions.

Secure Remote Access

Identity-bound, agentless access for OEMs and contractors — no shared VPN.

Micro-segmentation

IEC 62443-aligned cell / zone / conduit segmentation across the plant.

Asset Visibility

Passive discovery, digital twin, and continuous inventory of every asset.

Post-Quantum Ready

PQC-aligned cryptographic identity — future-proofed by design.

STANDARDS ALIGNMENT

QuantLayer maps natively to NIST 800-207 (Zero Trust), IEC 62443 (industrial security), NIST CSF 2.0, MITRE ATT&CK for ICS, CIS Controls, and the Government of Canada Cyber Security Readiness Goals.

11 The Continuous Trust Lifecycle

QuantLayer replaces one-time enrolment with a closed-loop lifecycle. Trust is not granted — it is continuously earned and re-earned through observable evidence.

1 Discover
Passive network discovery of every asset — no agents, no downtime.

2 Fingerprint
Cryptographic identity derived from hardware + firmware + configuration.

3 Verify
Enroll and attest device against golden baseline.

4 Authenticate
Passwordless, mutual authentication for every session.

5 Authorize
Policy engine grants least-privilege access.

6 Monitor
Continuous behavior and posture telemetry.

7 Detect
AI anomaly detection across protocols and users.

8 Isolate
Autonomous containment on trust-score decay.

9 Recover
Restore trust after posture is re-attested.

10 Audit
Immutable evidence trail for compliance.

EXECUTIVE INSIGHT

A device with a valid certificate but degraded posture — outdated firmware, anomalous protocol behavior, or unusual peer communication — has its trust score decayed automatically. Access is contracted before an alert reaches a human analyst.

12 Attack Chain Interruption — Before vs After

The same contractor-to-PLC intrusion, evaluated with and without QuantLayer.

Without QuantLayer

- Contractor VPN trusted implicitly
- Cached credentials reused across zones
- Flat plant network — lateral movement unimpeded
- PLC accepts Modbus writes from any host
- HMI alarms suppressed — operator unaware
- Impact reached before SOC investigates

With QuantLayer

- Contractor identity re-verified per session
- Passwordless — no cached credentials to steal
- Micro-segmented cells block lateral movement
- PLC only accepts writes from attested engineering identities
- Trust score decays on anomalous protocol behavior
- Autonomous isolation before impact reaches process

OUTCOME

QuantLayer breaks the attack chain at every stage — initial access, lateral movement, OT access, and impact — without requiring the operator to detect the incident manually.

13 AI-Orchestrated Continuous Trust

QuantLayer's AI orchestration layer continuously evaluates six trust dimensions and composes them into a single adaptive policy decision.

Human Trust
Identity provider, behavior baseline, session posture

Device Trust
Fingerprint, firmware, patch state, configuration drift

Application Trust
Binary integrity, allowed processes, memory posture

OT Protocol Trust
Modbus / DNP3 / S7 baselining and anomaly detection

Session Trust
Geo, network, time-of-day, peer graph

Machine / AI Trust
Agent identity, prompt integrity, tool-use scope

Adaptive orchestration under human governance and full auditability.

14 Alignment with Industry Standards

Every QuantLayer capability is mapped to a recognized industry or government framework.

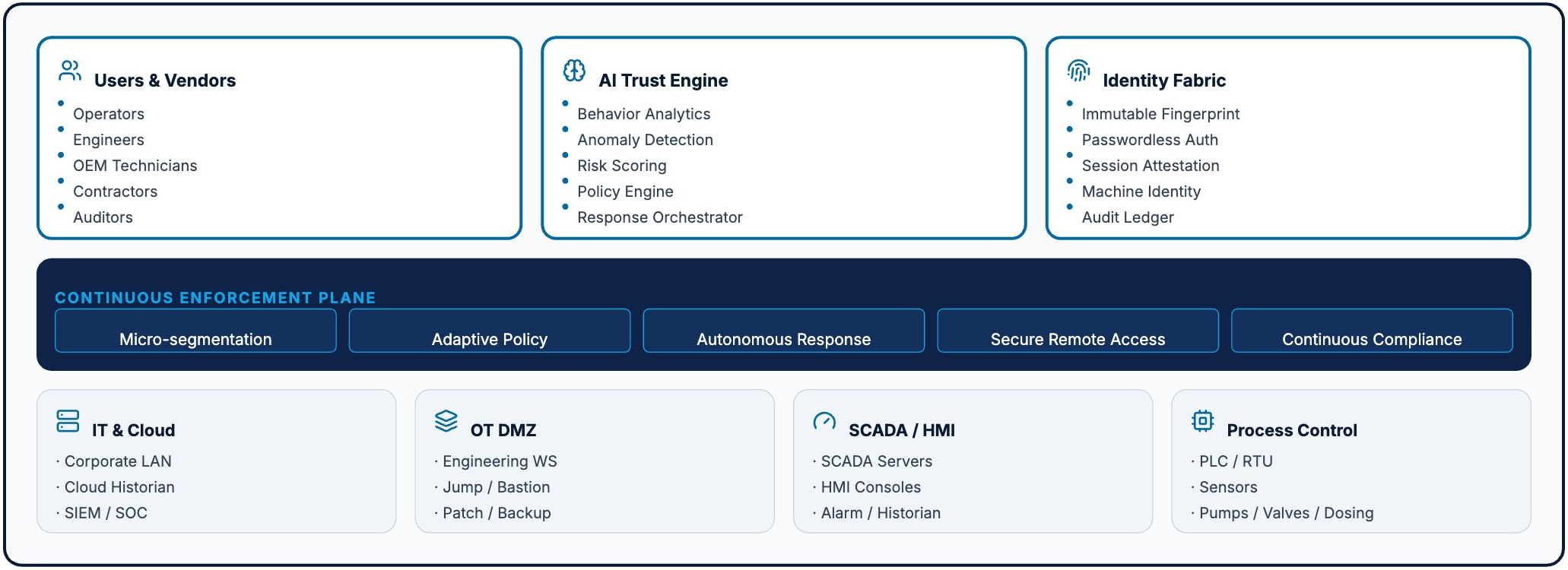
Framework	Scope	QuantLayer Alignment
NIST SP 800-207	Zero Trust Architecture	Full — PE/PA model, continuous authentication
NIST CSF 2.0	Cyber security framework	Govern · Identify · Protect · Detect · Respond · Recover
IEC 62443	Industrial automation & control	Zones, conduits, security levels, identity-based access
ISA / IEC 62443-3-3	System security requirements	SR1–SR7 mapped to native capabilities
MITRE ATT&CK for ICS	Adversary techniques	Detection and mitigation coverage matrix
CIS Controls v8	Security controls baseline	Asset inventory, access, protection, monitoring
GoC Cyber Readiness Goals	Canadian critical infrastructure	Directly aligned with sector-specific priorities
NERC CIP (adjacent)	Bulk-electric system	Applicable patterns for water utility operators

REGULATORY OUTLOOK

Canadian federal and provincial regulators are moving toward mandatory cyber baselines for critical infrastructure. Utilities that adopt continuous, evidence-based controls are positioned to satisfy future requirements without re-architecting.

15 QuantLayer Reference Architecture

End-to-end reference deployment for a Canadian water utility.



Every asset in every layer is enrolled, attested, and continuously scored by the AI Trust Engine.

16 Business Benefits & Outcomes

The operational and financial impact of adopting AI-orchestrated Zero Trust.

Operational Continuity

Reduce process disruption risk by breaking the attack chain before it reaches control logic.

Ransomware Risk Reduction

Passwordless, micro-segmented environments eliminate the most common ransomware entry paths.

Vendor Access Security

OEM technicians access only the specific device, for the specific time window, under session recording.

Insider Threat Mitigation

Anomalous behavior — from any identity — drives real-time policy adjustment.

Continuous Compliance

Live evidence for IEC 62443, NIST, CSF 2.0 and GoC baselines — no audit sprint.

Reduced Downtime

Autonomous response contains incidents in seconds instead of hours.

Improved Resilience

Multi-site, federated deployment survives regional or upstream failure.

Cyber Insurance Readiness

Documented Zero Trust posture supports lower premiums and broader coverage.

≤1s	≥90%	0	100%
Mean containment time	Attack-chain stages interrupted	Shared passwords in scope	Asset visibility across IT + OT

17 Conclusion & Next Steps

Cybersecurity is no longer an IT problem. For Canada's water utilities, it is an operational resilience requirement — inseparable from public health, environmental stewardship, and municipal trust. The perimeter model that protected earlier generations of infrastructure does not scale to the connected, vendor-integrated, cloud-augmented operations of today. QuantLayer™ enables utilities to modernize OT security without disrupting operations. By continuously verifying every identity, evaluating every session, and autonomously enforcing Zero Trust policies across the entire water ecosystem, it moves the sector from reactive perimeter defense to proactive, evidence-based resilience.

RECOMMENDED PATH FORWARD

1. Baseline current OT asset inventory, remote access surface, and identity hygiene.
2. Prioritize highest-risk vectors — vendor VPN, engineering workstations, exposed PLCs.
3. Deploy QuantLayer in observation mode to establish behavioral baselines.
4. Transition to enforcement in a phased, cell-by-cell rollout aligned to IEC 62443.
5. Integrate continuous compliance evidence into audit and reporting workflows.

ENGAGE BDATA

Design a Zero Trust roadmap for your utility.

info@bdata.ca · bdata.ca · Powered by BDATA Solutions Inc.

Sources referenced during preparation include the Canadian Centre for Cyber Security's assessments on threats to Canadian critical infrastructure, CISA / EPA advisories on water-sector intrusions, and public reporting on the incidents referenced in Section 05.