Rockwell Automation

CASE STUDY:

How a Canadian Water Utility Improved Cybersecurity and Operational Resilience

Table of Contents

Responding to Rising Cybersecurity Risks

The Colonial Pipeline and Oldsmar attacks became a wake-up call to Critical Infrastructure providers, particularly those whose operations are tied to public safety. OT cybersecurity has quickly grown into a top priority and providers have begun to seriously evaluate their vulnerabilities and risks,

Yet, many Critical Infrastructure operators still don't have a holistic cybersecurity program in place. Some simply don't know where to begin. In fact, a recent survey by the Water Sector Coordinating Council found some of the most pressing cybersecurity needs are technical assistance, advice, or assessments – needs that indicate operators are in the early stages of their cybersecurity journey.

OT cybersecurity in water utilities, as in many Critical Infrastructure sectors, can be complex, with legacy equipment making it difficult to segment, monitor, and patch as efficiently as in IT. This was certainly true for one Canadian water and electricity distributor that provides fresh drinking water and electrical distribution to approximately 250,000 customers in Canada.

30%

By 2025, 30% of Critical Infrastructure organizations will experience a security breach.

Source: Gartner

Challenges

Business leaders understood the need to update infrastructure, lifecycle management and OT cybersecurity capabilities. The Oldsmar water plant attack highlighted the pressing need to deploy cybersecurity capabilities to better protect public safety. Specifically, the Canadian utility company sought to strengthen network perimeter security and implement secure remote access, along with threat monitoring and detection capabilities.

Given a lack of internal cybersecurity and infrastructure skills, the utility contacted Rockwell Automation for help with designing, implementing, and managing a turnkey cybersecurity solution that would help protect its overall environment, ensuring uptime and public safety.

What Was Deployed

Working with Rockwell Automation was the logical choice for the utility, thanks to a 20-year relationship built on the foundation of prior automation services. Over the years, Rockwell Automation has helped the facility build, standardize, and integrate its technological infrastructure. The utility was confident the Rockwell Automation team understood its business operations, infrastructure security, and OT system. They also knew, from previous engagements, that Rockwell Automation backs its security and architecture expertise with comprehensive end-to-end capabilities.

Step 1:

Asset Inventory

Rockwell Automation delivered a blend of lifecycle management and lifecycle refresh initiatives, with cybersecurity elements baked in from the start.

An initial step involved a comprehensive audit of the company's digital assets to assess risks and vulnerabilities. An audit is critical because every unidentified device represents a potential network on-ramp for cybercriminals. "If you can't see the assets on your plant floor, then you can't protect them," says Robert Matear, business development lead for Connected Services at Rockwell Automation in Canada.

So far, less than a third (30.5%) of water utilities have identified all OT-networked assets. That's not entirely surprising, as research shows only 30% of Critical Infrastructure providers have a cybersecurity plan in place. "So many Critical Infrastructure operations are not currently deploying or even considering cyber solutions, and most of them are reluctant to even talk about it," says Kevin Moran, Commercial & Water Projects at Rockwell Automation in Canada.

Real-time inventory capabilities can provide instant visibility into network assets to help keep systems up and running. Yet asset inventory is an arduous undertaking for many organizations.

Step 2:

Security by Network Segmentation

The Canadian water utility also wasn't taking advantage of a critical network security architecture: segmentation. This technique divides a network into multiple subnetworks that allow security teams to control traffic flow and access rights. The Rockwell Automation team helped implement network segmentation and add protection mechanisms, enabling privileged access security policies, optimized network use, and reduced network access during a cyberattack, which helps prevent malware from propagating laterally across wider network resources.

Network segmentation also helps future-proof the company's technology architecture. "We're prepping their environment from an infrastructure perspective to make full use of cybersecurity technologies such as real-time monitoring and threat detection," says Matear.

Step 3:

Virtualized Industrial Data Center

Rockwell Automation also worked closely with the utility to upgrade the compute infrastructure with dual Industrial Data Centers (IDCs), adding cross-backups and managed support services to the overall solution. The utility's older single-managed IDC was updated to a physically separated dual-IDC stack with cooperative backups. This step provided site-level redundancy for process operations and a more reliable compute infrastructure that Critical Infrastructure providers need to stay up and running, even if there is a downed server room.

Use of a pre-engineered IDC helped facilitate a rapid deployment, providing greater operational security and faster time-to-value. The utility also leveraged Rockwell Automation's comprehensive managed services, providing 24/7 remote monitoring and administration, to address management resourcing and skills gap. This resulted in simplifying day-to-day operations and provided peace of mind for the plant staff

Step 4:

Network perimeter security with an IDMZ (Industrial Demilitarized Zone)

The utility's security leads were concerned about strengthening network perimeter security to protect OT assets from unauthorized access.
In this situation, an Industrial Demilitarized Zone (IDMZ) was implemented. IDMZs are considered a foundational network design element for IT and OT convergence scenarios, residing at Purdue level 3.5 - between the IT network and the OT Network. This network perimeter is a secondary demilitarized zone boundary, to broker only secure communications between IT & OT, mitigating threats to mission-critical OT assets, often originating from the IT network.

In this utility's case, the stretched IDMZ architecture resides across both IDCs, which also helps the organization maintain secure remote operations - even in the event of a partial infrastructure outage.

"In this case, the dedicated OT virtualized compute infrastructure, hosts a stretched IDMZ across two IDCs, to permit a site redundant IDMZ. The utility's leaders were serious about maintaining uptime of their critical and remote operations, even in the event of a plant disaster," says Matear.

Outcomes

Toward a more secure future

Rockwell Automation helped the Canadian utility build a more modern and secure operational infrastructure to move confidently into the future, despite rising risks and evolving threats. With this project, the water utility has gained:

- A more secure, connected, and resilient OT operating environment
- 24/7 remote monitoring, administration, patching, and maintenance
- Lifecycle management of critical assets to mitigate obsolescence challenges
- A future-proofed plant network
- Better protection of all assets through real-time asset tracking and inventory
- Improved operational efficiency by minimizing unplanned downtime

How does a large transformation project like this get started? Rockwell Automation began by performing a comprehensive and professional cybersecurity assessment. The assessment reveals vulnerabilities that are then addressed in the design phase, later moving to implementation and ongoing management. The utility's networks and systems that comprise the security lifecycle are now updated, patched, and managed as a service, simplifying operations for the utility in an era of IT and cybersecurity staffing shortages.

The utility's confidence has grown since embarking on its cybersecurity journey. Rockwell Automation is helping the utility to improve threat detection, remote access, and access controls using OT security solutions from technology partner, Claroty. Claroty solutions quickly deliver value and boost security by detecting hack attempts and suspicious network activities. "It's not unusual for a customer to deploy Claroty Threat Detection and immediately detect several ghost assets and many unpatched devices across their network. We provide remediation solutions and services, to solve these challenges and help our customers optimize their environment, to improve cyber posture" Matear explained.

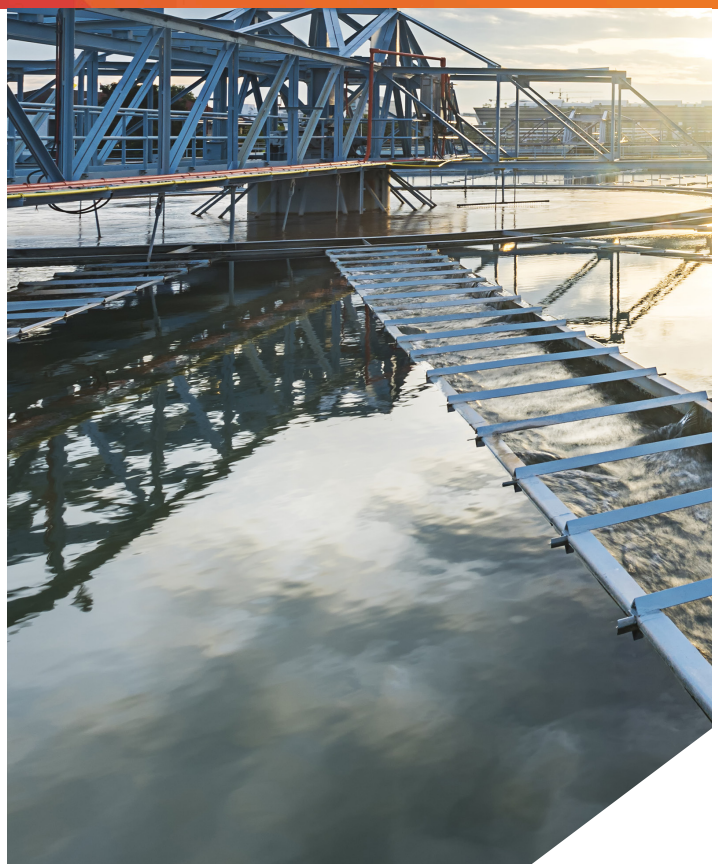
The planned deployment will include Claroty's Continuous Threat Detection (CTD) to monitor OT traffic and pinpoint threats and anomalies across the enterprise. Claroty Secure Remote Access (SRA) will also be deployed, facilitating Role-based Access Control (RBAC) and privileged access management (PAM) to lock down accounts with elevated access rights. These additional solutions also generate data that will guide Rockwell Automation's teams in optimizing performance.

Securing What the World Relies On

Cybersecurity is essential to keep Critical Infrastructure up and running 24/7. Yet our research shows that many utilities don't yet use basic cybersecurity controls, and this is where Rockwell Automation can help.

Whether you're a local water district needing a fast automated solution or serving millions of customers, we can meet you anywhere in your OT cybersecurity journey, starting from assessment of the environment to design, through implementation and ongoing management.

Visit our Critical Infrastructure resource center or talk to a Rockwell Automation expert today.



Multi-Solution Strategic Partnership

Connected Services

- Site-redundant IDCs with cross-backups and managed support
- Secure network infrastructure with managed support
- Redundant IDMZ architecture across two IDCs for network perimeter security
- Claroty Continuous Threat Detection (CTD) to monitor OT traffic and provide plant-wide threat and anomaly detection (future)
- Claroty Secure Remote Access (SRA) to permit secure remote access and facilitate RBAC (Role-Based Access Control) and Privileged Access Management (PAM) (future)

Rockwell Automation services

- TechConnect℠ support services
- Imbedded Rockwell Automation Engineer
- Customer Block of Time
- Connected Services

Rockwell Automation product

- 100% Rockwell Automation Allen-Bradley® controls environment

Ecosystem partners:

- Panduit
- Dell EMC
- Cisco
- VMware
- Microsoft

Rockwell Automation

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-AP002A-EN-P-June 2022