Pacific Canbriam Secures OT Infrastructure with Xage Zero Trust Architecture

How Pacific Canbriam Eliminated VPNs, Implemented Segmentation, and Meet Regulatory Mandates with Xage Security

Overview

Pacific Canbriam, a Canadian energy producer, sought to enhance the security of its operational technology (OT) environment to address increasing cyber threats, comply with evolving cybersecurity regulations, and ensure business continuity. To achieve this, the company partnered with Xage Security to implement a modern Zero Trust architecture that would provide secure remote access and fine-grained, role-based access controls.

Challenge

Prior to engaging with Xage, Pacific Canbriam's OT network was broadly accessible via VPN, granting unrestricted access once connected. This lack of segmentation posed a significant security risk—leaving the network vulnerable to malware propagation and unauthorized activity.
The company also faced mounting regulatory pressure from cybersecurity mandates in British Columbia and Alberta, where noncompliance could lead to operational shutdowns. Pacific Canbriam recognized the urgent need to mitigate risk, replace its legacy VPN system, and comply with industry regulations—without creating complexity for internal teams or external contractors.

PACIFIC CANBRIAM ENERGY

The partnership enabled Pacific Canbriam to successfully transition from an exposed OT environment to a modern, compliant security infrastructure.

- **Risk Mitigation**
- **Improved User Experience**
- **Regulatory Compliance & Insurance Eligibility**
- **Operational Confidence**
- **Trusted Partnership**

Solution

Xage delivered a comprehensive Zero Trust solution built around defense-in-depth principles and asset-level access control. Through a single, unified deployment, Pacific Canbriam was able to meet multiple security objectives:

- **Network Segmentation:** Limited access strictly to necessary resources, reducing lateral movement and minimizing potential impact from breaches.
- **Secure Remote Access:** Eliminated the need for traditional VPNs, providing browser-based access for contractors via the Zero Trust Data Exchange.
- **Privileged Access Management (PAM):** Introduced built-in PAM capabilities and a password vault to safeguard privileged credentials.
- **Secure File Transfer:** Provided the ability to securely upload and download files.
- **Authentication Enhancements:** Enabled multi-factor authentication (MFA) for third parties and single sign-on (SSO) for employees—streamlining access while strengthening security.

Xage was selected over two competitors due to its robust asset-level controls, flexible deployment options, and intuitive user experience for both administrators and end users.

Outcomes

The partnership enabled Pacific Canbriam to successfully transition from an exposed OT environment to a modern, compliant security infrastructure:

- **Risk Mitigation:** The implementation of segmentation and granular controls drastically reduced the potential blast radius of security incidents.
- **Improved User Experience:** Contractors and administrators reported a more seamless and accountable access process.
- **Regulatory Compliance & Insurance Eligibility:** Achieved full compliance with provincial cybersecurity mandates and, for the first time, qualified for cyber insurance coverage.
- **Operational Confidence:** Leadership expressed renewed confidence, noting the ability to "sleep at night" with the enhanced protection of the production environment.
- **Trusted Partnership:** Pacific Canbriam continues to highlight Xage's exemplary support, calling the relationship a true strategic partnership.

xage SECURITY