# Petrobras Strengthens Critical Infrastructure Security with Xage Zero Trust Fabric

## Overview

Petrobras is one of the world's largest integrated energy companies, generating more than 162 billion dollars in net revenue and employing nearly 40,000 people across offshore platforms, refineries, terminals, and downstream operations in Brazil and abroad.

The company faced increasing cybersecurity risks caused by outdated remote access tools and limited visibility into user activity. More than 1,600 employees and contractors required secure connectivity to over 80 operational sites, many of which are located in remote or difficult to reach regions.

Petrobras relied on a diverse mix of legacy OT systems and modern IT environments, and traditional tools such as VPNs, jump servers, and basic segmentation were no longer sufficient. These tools created opportunities for broad, uncontrolled access and made it difficult for the organization to ensure consistent oversight across a highly distributed operational footprint.

As cyber threats in the energy sector intensified and operational demands grew more complex, Petrobras sought a more modern and secure approach that could protect both legacy industrial systems and new digital infrastructure without creating disruption or risk to critical operations.

## Challenges

Petrobras had limited visibility into detailed activity logs, which made it difficult to maintain accountability and meet growing compliance expectations. COVID era constraints increased reliance on improvised and legacy solutions, further exposing the organization to security gaps.

PETROBRAS

### Headquarters

Rio de Janeiro, Brazil

### Industry

Oil & Gas

### Key Takeaways

- Unified Zero Trust security across IT, OT, and cloud without disrupting operations.
- Agentless MFA, least-privilege, and just-in-time access for employees and contractors.
- Stronger protection for offshore platforms, refineries, pipelines, and remote sites.

The company also faced growing industrywide risks that prompted a proactive effort to strengthen cyber resilience. Third party access was another major concern because contractors needed frequent entry into sensitive environments, yet Petrobras lacked the ability to tightly control or supervise these sessions.

Weak or shared credentials were common and created unnecessary exposure. Across the OT landscape, many systems lacked native authentication capabilities, and remote access tools such as VPNs expanded the attack surface by granting broad network access without granular control. Offshore environments added another layer of complexity because inconsistent connectivity prevented centralized enforcement and made traditional authentication methods unreliable.

## Solution

Petrobras deployed the Xage Zero Trust Fabric to unify access control and modernize cybersecurity across its OT, IT, and cloud environments. The organization defined strict requirements for the new solution. It needed strong authentication for all remote access, the removal of shared credentials, clear auditability, and an easy way to retrieve access logs.

Petrobras required complete segregation between OT and IT, along with an approach that allowed secure access even in remote locations where connectivity is limited. Legacy system support was essential, and the solution had to be easy to deploy, maintain, and scale across all sites. Petrobras also needed consistent session recording capabilities, and a standardized workflow for both employees and third party vendors.

The Xage Zero Trust Fabric met these expectations by providing identity based access and distributed enforcement that works even when network connectivity is unavailable. The platform delivered a unified access layer where every user, device, and application is verified and granted only the minimum permissions necessary. Multifactor authentication, least privilege policies, and just in time access were applied consistently across all systems. The solution secured both modern and legacy systems without requiring operational changes or downtime.

## Outcomes

Petrobras significantly improved the security of its critical infrastructure by eliminating broad VPN access and adopting granular Zero Trust controls. Remote access became more secure and efficient and technicians and contractors were able to perform their work more easily while operating within strict identity-based boundaries. The organization gained complete visibility into user activity through detailed logs, audit trails, and session recordings. These capabilities improved compliance readiness and made it possible to supervise third party access in real time.

Xage's distributed enforcement allowed operations to continue smoothly at offshore sites even when connectivity was intermittent. The platform also enabled Petrobras to manage legacy assets such as Windows XP machines in a secure and controlled manner, which was not possible with previous solutions.

By isolating OT systems, reducing lateral movement, and enforcing least privilege access, Petrobras lowered its risk exposure to ransomware, supply chain threats, and credential misuse. The company also gained insight into the number of users and sites operating across its remote access environment, which had previously been unknown. With Xage, Petrobras established a scalable and future ready cybersecurity foundation that supports digital transformation, cloud expansion, and safer, more efficient energy operations across its global footprint.