xage SECURITY

WHITEPAPER

Xage Zero Trust Access for Power Generation Environments

Secure access to plant systems, control centers, vendors, and critical operational assets

Power generation environments are different from traditional enterprise networks. They are distributed, operationally sensitive, and built around systems that directly support plant availability, safety, environmental compliance, and grid reliability.

A generation utility may operate gas plants, hydro powerhouses, pumped-storage facilities, renewable sites, control centers, plant historians, DCS platforms, PLC systems, turbine controls, engineering workstations, relay systems, SCADA applications, and vendor-supported operational systems. These environments are often spread across many facilities, each with its own network design, identity source, control system architecture, and operational procedures.

At the same time, many different users need access. Plant personnel need access to local applications. Engineers need access to workstations and configuration tools. OEM vendors need access during outages, troubleshooting, and maintenance windows. Contractors need temporary access for projects. Cybersecurity and operations teams need visibility into who accessed what, when, and why.

The challenge is not simply remote access. The real challenge is **controlled access.**

Utilities need a way to give the right person access to the right system for the right reason, without opening unnecessary paths into the plant network. This is where traditional VPN-based models begin to fall short.

Xage provides a Zero Trust Access model designed for operational technology environments. Instead of extending network access, Xage brokers access to specific applications, workstations, servers, and OT assets based on identity, policy, approval, protocol, and time. Access can be limited, monitored, recorded, and automatically removed when no longer needed.

For generation utilities, this creates a practical way to support secure operations without weakening plant segmentation or adding more complexity to already sensitive environments.

The access problem in power generation

Generation plants have many systems that require controlled access, but not every user should have the same level of reach.

A turbine vendor may need access to one support workstation. A controls engineer may need access to a DCS engineering station. A relay technician may need access to a specific relay tool. A plant operator may need access to monitoring applications. A cybersecurity analyst may need access to logs and session evidence, but not direct access to control systems.

These access paths are often handled today through a mix of VPNs, jump servers, shared local accounts, firewall rules, spreadsheets, email approvals, and manual coordination with plant teams. That model works only up to a point. As the number of plants, users, vendors, and systems grows, it becomes harder to manage and harder to defend.

The risks are well understood:

Current challenge	Why it matters
Broad VPN access	Users may receive more network reachability than they actually need
Long-lived vendor accounts	Access may remain active after the work is complete
Shared or local credentials	Activity is harder to tie back to an individual user
Jump server sprawl	Access paths become inconsistent across plants
Manual approvals	Plant owners may not have clean control over who gets access
Limited session visibility	It may be difficult to reconstruct what happened during a remote session
Fragmented logs	Evidence may be spread across VPN, firewall, endpoint, and jump host logs
Plant-by-plant exceptions	Access models become inconsistent and difficult to audit

In generation environments, this is more than an IT issue. Poorly governed access can increase operational risk, complicate outage support, weaken vendor accountability, and create audit gaps.

What Xage changes

Xage shifts the access model from **network-level connectivity to policy-driven, granular access to specific operational resources.**

In a traditional VPN model, once a user authenticates, they are typically connected into a defined network segment. From that point forward, the utility must rely on firewall rules, routing controls, jump servers, endpoint security, and operating procedures to restrict what the user can reach. This creates additional operational complexity and can increase risk if access paths are broader than the user's actual need.

With Xage, users do not require broad network access into the plant or operational environment. After authentication, users are presented only with the applications, workstations, servers, or assets they are explicitly authorized to access. Xage brokers the session directly to the approved target and applies the required controls around that session, including policy enforcement, just-in-time access, approval workflows, session recording, and audit logging.

This approach allows the utility to reduce unnecessary network exposure while still giving plant personnel, engineers, vendors, and support teams the access they need to perform approved work.

Xage helps utilities answer the questions that matter before access is granted:

Question	Xage control
Who is the user?	Identity integration with approved directories and identity providers
Are they strongly authenticated?	MFA and SAML integration
What are they allowed to access?	Policy-based access to specific systems and applications
Do they need approval?	Workflow-based approvals from the right owner
How long should access last?	Just-in-time, time-bound access
What can they do?	Protocol and target-based access control
Should the session be recorded?	Session recording and audit trail
Can evidence be produced later?	Centralized logs, session history, and reporting

This is the access model power generation environments need because it gives operations, cybersecurity, and plant teams control without forcing the user onto the broader plant network.

Where Xage fits in a generation environment

Xage can be deployed across central operations environments, control centers, plant networks, and remote facilities. The architecture supports central governance while allowing enforcement to sit close to the operational systems being protected.

In a generation utility, Xage can help secure access to:

Area	Example systems
Plant control environment	DCS workstations, HMIs, local SCADA, PLC systems, turbine controls
Engineering systems	Engineering workstations, programming tools, relay tools, configuration systems
Operational applications	Historians, dashboards, reporting tools, asset monitoring systems
Remote facilities	Hydro powerhouses, renewable sites, smaller generation facilities

Vendor-supported systems	Turbine OEM systems, emissions systems, controls, relays, instrumentation
Control centers	Operations center applications, dispatch-support tools, fleet monitoring systems
Administrative systems	Windows/Linux servers, directory services, backup systems, application servers

Xage Nodes can be placed in the right operational zones so access can be brokered without flattening the network. This is important because most generation utilities do not want to redesign every plant network just to improve remote access. They need a solution that works with existing segmentation, plant ownership, and operational boundaries.

Xage can also work with multiple identity sources. That matters because a generation utility may have corporate directory services, operations-specific directories, plant-local Active Directory, vendor identities, and emergency accounts. Xage does not require every plant and user group to be forced into one identity model before access can be governed.

Important use cases for generation utilities

Use Case	Generation Environment Challenge	How Xage Helps
OEM and vendor access	Turbine vendors, DCS vendors, relay vendors, emissions system providers, instrumentation vendors, and controls integrators often need remote access during maintenance, troubleshooting, outages, and upgrades. This is one of the highest-risk access paths because vendors may need access to sensitive plant systems, but they should not receive broad network reachability.	Xage limits vendor access to the specific system or application they are approved to support. Access can require approval, be active only during the approved work window, and be recorded for accountability. This gives plant owners and cybersecurity teams better control without slowing down legitimate support work.
Engineering workstation access	Engineering workstations are among the most sensitive assets in a plant. They may be used to configure PLCs, modify DCS logic, manage relay settings, support historian interfaces, or administer plant applications. Standing or overly broad access to these systems creates significant operational and cyber risk.	Xage restricts access to engineering workstations by user, role, protocol, site, approval status, and time window. Sessions can be recorded where required. This reduces standing privileged access and gives the utility clear evidence of who accessed critical engineering systems.

Control center to plant access	Control centers and operations teams often need access to plant dashboards, historian views, support applications, and selected plant systems. The access must be practical for operations, but it should not create broad network paths into each plant.	Xage allows control center users to access only approved systems without being placed directly onto the plant network. This preserves separation between central operations and local plant control environments.
Hydro and remote site access	Hydro fleets and remote generation sites are often geographically dispersed, lightly staffed, and dependent on variable connectivity. Traditional access models can create broad remote network exposure or require inconsistent site-by-site exceptions.	Xage's distributed model allows access enforcement to be placed near the remote facility. Users can be limited to approved systems rather than being given broad access across the remote network.
Historian and operational data access	Historians and operational data platforms are used by plant teams, engineering, analytics, operations, compliance, and business users. They are valuable, but they can also become an access bridge between operational systems and enterprise users.	Xage helps govern access to historian servers, dashboards, administrative tools, and supporting applications. This is especially useful where many users need operational data access, but only a small group should have privileged access.
Contractor and outage support	During outages, upgrades, testing, commissioning, and maintenance projects, contractors may need temporary access to plant systems. That access should not remain active after the work is complete.	Xage provides time-bound access for the approved work window and can automatically remove access when the window expires. This reduces the risk of stale contractor access.
Emergency access	Generation environments need emergency or break-glass access procedures for urgent operational events. These workflows must be fast, but still controlled and reviewable after the event.	Xage can support break-glass access with strong authentication, limited scope, session recording, automatic expiration, and post-event review.

Why Xage is stronger than traditional VPN access

VPN still has a place in some network architectures, but VPN by itself is not a complete access control model for generation OT.

The fundamental difference is simple: **VPN connects users to networks. Xage connects authorized users to approved resources.**

That difference matters in a plant environment.

Area	VPN-based access	Xage Zero Trust Access
Access model	Network-level connectivity	Application and asset-level access
User reach	Depends on routing and firewall rules	Limited to approved targets
Vendor access	Often requires VPN profile, account, jump host, and firewall path	Time-bound access to specific systems
Least privilege	Difficult to maintain across many plants	Enforced by user, role, asset, protocol, and time
Session visibility	Usually requires separate tools	Built into the access workflow
Access duration	Often persistent until manually removed	Automatically expires
Audit evidence	Fragmented across several systems	Centralized access and session evidence
Plant segmentation	Can create pressure to open network paths	Works with segmented plant environments
Multi-site scale	Becomes complex as sites and vendors grow	Designed for distributed environments
Operational control	Often owned by IT/network teams	Can include plant and asset-owner approvals

Security and operational value

Xage helps generation utilities strengthen access governance while keeping access practical for plant operations, engineering teams, vendors, and support personnel.

Outcome	Operational Value
Reduced attack surface	Users and vendors are not granted broad plant network access. Access is limited to the specific systems and applications they are authorized to use.
Stronger vendor accountability	Vendor activity can be tied to named users, approved access windows, specific target systems, and recorded sessions.
Improved segmentation	Access is brokered to approved resources instead of opening wide network paths into plant environments.
Reduced standing privileges	Temporary, just-in-time access can replace always-on access for vendors, contractors, and privileged users.

Cleaner audit evidence	Approvals, access logs, target systems, session duration, and session recordings are available for review and reporting.
Better plant ownership	Access to sensitive plant systems can be approved by the appropriate plant, operations, or asset owner.
Consistent multi-site governance	Common access controls can be applied across different plants, facility types, vendors, and user groups.
Less reliance on legacy access tools	Utilities can reduce dependence on VPN sprawl, jump servers, shared accounts, manual firewall exceptions, and ad hoc access procedures.

For plant teams, Xage makes access easier to control. For cybersecurity teams, it makes access easier to verify and audit. For vendors and engineers, it provides a clearer and more controlled path to the systems they need. For the utility, it creates a safer and more scalable access model across the generation fleet.

ABOUT XAGE SECURITY

Xage Security is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.

xage SECURITY