xage SECURITY

SECURING DISTRIBUTED ENERGY RESOURCES

MULTI-PARTY ACCESS SECURITY WITH ZERO TRUST

The Distributed Nature of Renewable Energy Sites

Societal concerns regarding climate change, together with the economic opportunities of green energy, are driving the adoption of renewable distributed energy resources (DERs). Yet, due to their distributed nature and multiple involved parties, DER sites can present a large cyber attack surface amid a fast-evolving threat landscape, creating major access management security challenges.

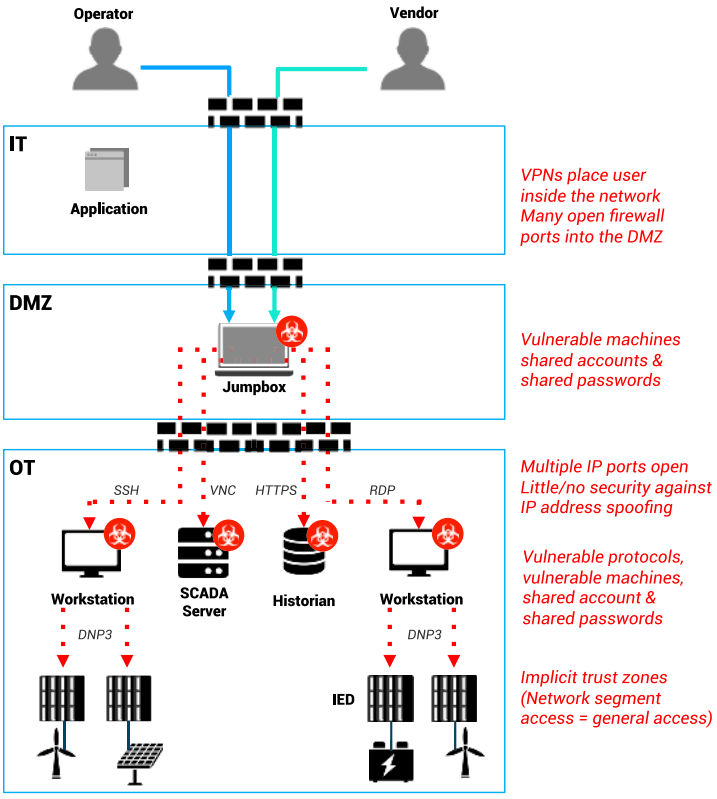
Today, too many DER sites rely on security models that slow innovation and are vulnerable to compromise. As energy companies become a top target for ransomware and other cyberattacks, change is needed.

Traditionally, power producers use perimeter-based and zone/layer-based models to design a security architecture for asset protection. Meanwhile, NERC CIP regulations significantly restrict the number of technicians allowed to access these assets, as all participants are required to meet standards with specific training and background checks in order to operate and maintain sites. To comply with these regulations using perimeter-based models, many enterprise and operational networks are separated by a demilitarized zone (DMZ). Existing approaches seek to control access to OT systems using a complex network architecture that includes firewalls, jump servers, SCADA software, password vaults, authentication software, VPN connections and a host of portals and scripts for managing user access.

This approach can prove vulnerable and costly especially as the number of DER sites and participants continues to grow. IT and operational organizations spend a significant amount of time and money on not only network and security design and implementation, but also ongoing maintenance to keep security controls updated and patched for protection and compliance needs. And of course, unguarded open firewall ports, stale or shared accounts on jump boxes and workstations, VPN-enabled network access, and poorly terminated access-protocols like RDP and VNC all provide entry-points for hackers.

Using this traditional approach, secure remote access for DERs is both expensive and inefficient; and more importantly, it becomes ever more vulnerable to cyber attacks over time.

Diagram 1: Remote access today: vulnerable, hard to use, complex, too trusting



xage

The Multi-Party Dilemma

The frequency of DER workforce changes across multiple parties only exacerbates these issues. Owners, operators, asset managers, vendors and manufacturers all require differing levels of on-site and remote access during normal operations over the generation asset's lifetime. The responsibilities of the various parties requiring access to DERs over their lifetime are captured in Diagram 2. Owners and operators of the assets will need to ensure security compliance requirements. Asset management and industrial manufacturers or vendors must ensure all financial and contractual requirements are met, which often include service level agreements or requirements directly attributed to regulatory compliance needs of owners and operators.

With traditional security strategies, operators responsible for controlling remote access must grant wider access than required to a wide range of parties and simply trust that users will only access specific sites or specific onsite devices—essentially creating an honor system to avoid enacting complex, overlapping network policies that complicate access altogether.

Using today's typical tools, operations would be required to set up a number of different products and configurations to provide multi-party remote access to a single site. Listed below are just some of the typical products to license, configure and maintain for remote access:

- VPN software for network authentication and access
- Identity access management software for authentication and optional features, i.e. MFA, Single Sign-On
- Privileged access control and password vault
- Scripts as necessary for device password rotation
- Firewalls, associated network and port configurations, i.e modem IP whitelisting, local (site) active directory, and domain controller set up and management
- A physical server, windows accounts to host ICS and device engineering software

These efforts are not trivial for a single site, and the nature of distributed generation is to have many sites under management that require the same level of protection. This makes today's tools and techniques unscalable for the power industry transformation.

Diagram 2: Access Requirements Matrix for a Typical DER

Entity	Responsibility	Access Needs
Asset Owner	If NERC registered facility, must comply with all applicable NERC Generation Owner requirements.	Will vary, may want remote access for reporting verification, asset management, etc.
Vendors	Numerous supply equipment and service providers needed to support the facility. Common providers will include inverter, HV substation, data management, SCADA integrator, and compliance program providers.	Will require full remote and at times local access for maintenance and troubleshooting of equipment. Service providers will need access to operational data for compliance reporting. Access may be scheduled, ad hoc, or conditional.
Asset Manager	Responsible for all financial and contractual requirements for the various sites. Represents the asset owner ensuring all parties and operators meet all contractual obligations and may include the Generation Operator is compliant.	Requires limited remote access and depends on the contractual involvement with the scope of supply with the asset owner.
Operators	Responsible for the operation of the site, and must meet all NERC Generation Operator compliance regulations.	Requires full remote and local access throughout the commissioning and operation of the site.

The Solution - Zero-Trust Multi-Party Remote Access

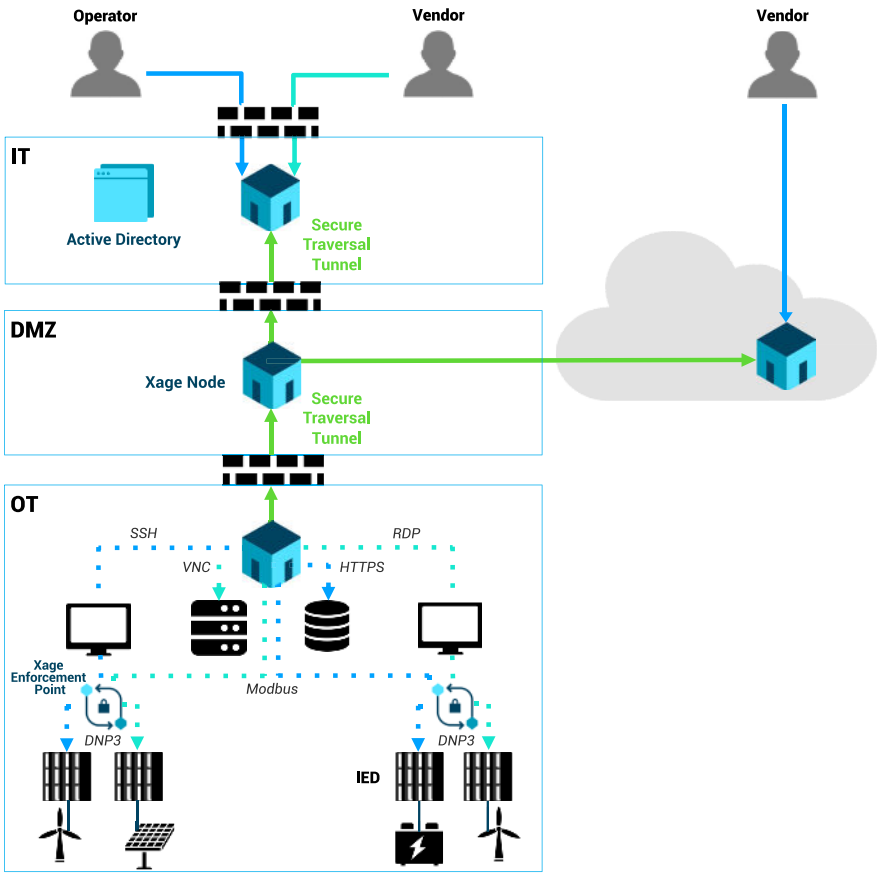
By embracing zero trust principles and end to end orchestration along with centralized policy management and distributed policy enforcement, remote or onsite DER operations can minimize traditional attack surfaces and mitigate threats while enabling multi-party access that is simple to use, administer, and audit.

A major tenant of zero trust is for an identity to be used for creating and enforcing security policies. For DERs, identity serves as a badge to traverse from the enterprise to the DMZ to the operational site networks, and ultimately even a device. To reduce the overhead for this granular access management, DERs need an access control solution that embodies the zero-trust principles set forth in NIST SP 800-207, including:

- Individual access perimeter based on an identity of each user and an asset, not just party, site, or network segment
- Distributed enforcement of access policies with the ability to automate and orchestrate across typical IT, DMZ and OT network boundaries
- Centralized policy management built around identities of people, applications, workstations accounts, and devices that also supports multi-party access
- End-to-end access control based on authenticated user identities
- Ability to orchestrate necessary protocol breaks between zones for compliance

The Xage Fabric offers each of these critical features to ensure operators can effectively secure, manage and automate their operations with ease and consistency.

Diagram 3: Xage Zero Trust Policy-driven Remote Access



The Xage Security Fabric - A Single Application for End to End Access Management:

- Manages identities and access policies in a multi-party environment; utilizes zero-trust principles of "just-in-time" and "just-enough-access" to individual assets
- Establishes encrypted end-to-end tunnels from outside entities to the DER site to enable security policies that traverse network layers
- Orchestrates security controls such as firewalls to enable identity-based access only when it's needed
  - Controls access to SCADA systems, operational devices, workstations, and applications, once authenticated
  - Blocks lateral movement to devices when access isn't authorized
- Facilitates multi-factor authentication
- Tracks comprehensive audit trails tied to individual user and asset identities
- Single scalable access management solution for vendors to multiple operators and operators to multiple sites.

The Benefits

Xage customers will see:

- Reduced set-up time for secure third party access. What typically takes days or weeks can be done in minutes.
- Reduced IT, operational, and capital costs through removal of dependence on technologies such as VPNs and Jumpboxes and significant reduction in administrative costs.
- Reduced hours maintaining firewall rules, workstation accounts, jump servers, various authentication applications.
- Increased security through elimination of attack vectors of shared accounts, VPN connections, open firewall rules, malware-infected laptops and lateral movement.
- Extended lifetime of installed assets
- Full auditability and adherence to security policies established with utilities, customers and partners.

Diagram 4: Distributed Access Control at Scale