Cybersecurity Fabric: Pervasive and Zero-Trust approach for cyber protection and mitigation

Xage Security, Inc
445 Sherman Ave
Suite 200
Palo Alto, CA 94306

Author: Roman Arutyunov, Co-Founder and VP Products
roman@xage.com

In response to:
Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure
Agency: Office of Electricity, Department of Energy (DOE)

Table of Contents

Executive Summary

Following the Colonial Pipeline ransomware hack, costing $4.4 million in ransom and millions more in lost profits, reputational damage and governmental scrutiny, the volume and severity of cyberattacks are forcing federal agencies to incentivise cybersecurity overhauls. But behind the government's calls for change are the struggles of energy industries to embrace the digital revolution.

Modernization of our energy industries requires digital analytics, data-driven automation, collaboration with partners, suppliers, and customers involving both digital and physical assets. The vision for a smart power grid, for instance, looks something like this: Electric substations are managed by Industrial IoT devices that can communicate with administrators, partners and customers in real-time; various energy assets – wind, water, solar, nuclear, and fossil fuels — are all automatically blended to optimize generation and distribution; energy-intensive spaces, like data centers or large office buildings, as well as residential homes, all have smart thermostats that leverage machine learning to optimize heating and cooling, driving down costs and energy consumption.

Fixing the security problems inherited from joining new and legacy equipment together (a common and often necessary approach in the industrial world) requires more than a new security solution off the rack; it requires a whole new mindset. Current approaches largely dependent on **network isolation** are no longer offering adequate cyber protection, are complex to manage, and are limiting the growth of digital transformation. Security can no longer be thought of as merely a defensive tactic. Instead, it needs to be understood as the foundation for transitioning to "smart" infrastructure—a vision that has grown more popular in theory than it has in practice.

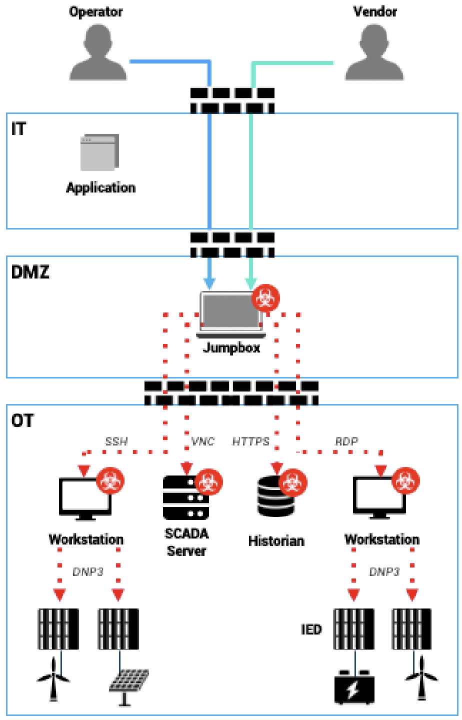
To unlock the benefits of digital transformation in energy industries must adopt a zero-trust pervasive approach to security that controls all interactions between people, machines, applications, and data across OT and IT systems at any location. This pervasive cybersecurity fabric would protect every asset, legacy or new, and all interactions, giving energy industries the controls they need to protect and mitigate cyber attacks. The lack of a granular zero-trust security strategy is precisely why incidents like the Colonial Pipeline ransomware hack can easily escalate to a point where the operation is forced to shut down, and it's why nearly each week we see a new large-scale cyberattack cripple yet another critical operation.

With a zero trust strategy implemented to protect everything from 20-year old systems with no passwords and no encryption, to present-day controllers with unmanaged credentials to future IoT devices with built-in digital identities, operators will begin to feel the benefits of digital transformation. They'll experience easy remote access, efficient data sharing and convenient collaboration across the ecosystem of partners, supplies, and customers.

Common Security Practices and Their Shortcomings

The majority of industrial operators use an isolation approach to secure their machines, utilizing firewalls, VPNs, DMZs, and Jump Boxes to create multi-layered networks—with threadbare machine protections. These approaches were invented two or even four decades ago and do not match the needs of modern industrial operations, as they:

- Isolate, rather than support the connectivity needed for smart energy applications and integration of distributed renewable energy resources.
- Define a wide network-based perimeter, so anyone on the network can gain access, rather than identity and resource based, so only authorized parties have access to authorized resources and per the security policy.
- Set static, coarse grain, complex rules, rather than provide the dynamic, fine-tuned control operators need. Should a vendor get the same level of access as an employee?
- VPNs put users (and malware on their machines) directly into the networks making it hard to control which systems they interact with and what they do
- Jump boxes designed to separate different network segments are windows machines which are vulnerable and often the target of attacks
- Cumbersome rules in firewalls that are hard to configure and maintain. Thousands of static accounts used by multiple people, leveraged by malware, and difficult to audit
- Deploying new applications is often a big hurdle; it’s difficult to control application to device and data interactions



VPNs place user inside the network
Many open firewall ports into the DMZ

Vulnerable machines shared accounts & shared passwords

Multiple IP ports open
Little/no security against IP address spoofing

Vulnerable protocols, vulnerable machines, shared account & shared passwords

Implicit trust zones (Network segment access = general access)

Diagram 1: Common attacks vector in industrial operations

Zero Trust Access (ZTA) and It’s Benefits

Traditional isolation security approaches use the enterprise or the operation as the perimeter, separating assets into trust zones, and automatically trusting and granting permissions to the machines, apps, and users within those trust zones. A zero trust security model extends this approach to improve security while also reducing complexity.

A zero trust access (ZTA) model uses identity as the perimeter, and rather than automatically assuming trust for any entity that can gain network-segment access, sets a standard that no trust should be assumed for machines, apps, or users until their identity is authenticated and their access authorized per the security policy. This approach utilizes identities and credentials to create a secure environment, and even so, grants authorization to only a limited set of interactions, and only for the required duration.

The modern operation has field, control center, datacenter, and recently cloud deployments, with interactions between people, machines, apps, and data across those deployments and external parties. Current approaches need to be extended, such that, when a user or application needs access to a resource, it can be allowed without opening a “hole” for attackers. The outdated tools in use today simply do not provide this level of granularity.

Rather than overfitting systems with isolation approaches like firewalls and VPNs, today’s distributed, multi-party, scaling IT/OT operations need security that is identity-based and enforces ZTA. A ZTA approach is applicable not just for humans and machines, but between all humans, machines, apps, and data comprising the operation. This means operators no longer need to accept security trade- offs in their businesses, which are a byproduct of a legacy design unadaptable for modern networks.

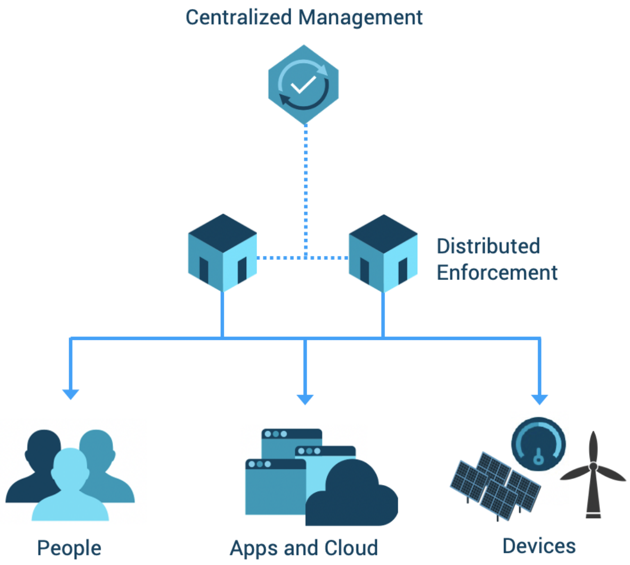


Diagram 2: Centralized management and distributed enforcement: all interactions any location

The National Institute of Standards and Technology (NIST) has been advocating for a zero-trust approach for securing operations with their special publication (NIST SP 800-207) describing the relevance and applicability of the zero-trust architecture is safeguarding our industries. Additionally Xage is working with NIST on a revision to the NIST 800-82 v3 guidelines for securing industrial control systems (ICS) to include zero-trust technologies and methods for cyber attack protection and mitigation.

> *"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location"*
> NIST SP 800-207 Aug 2020

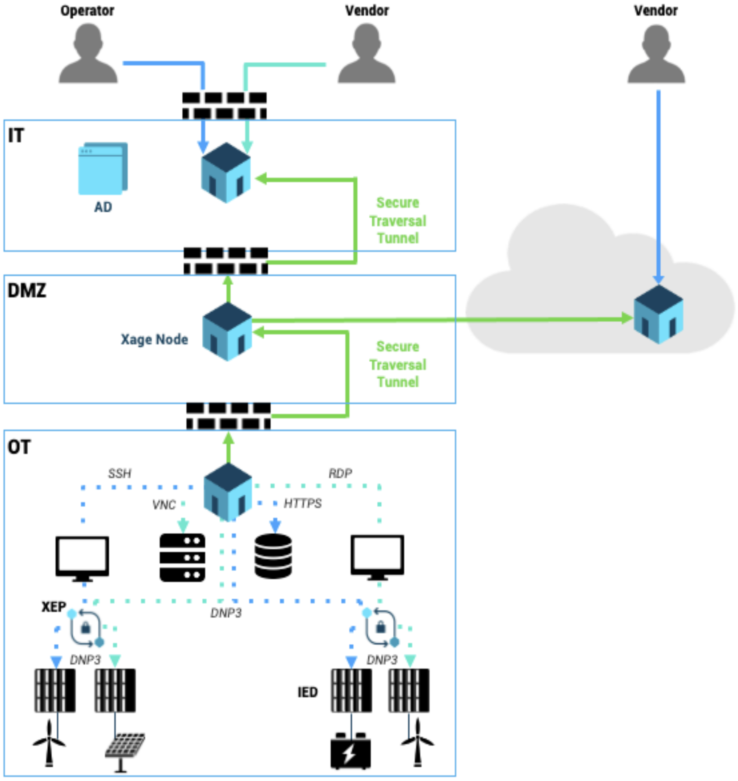


Diagram 2: Zero-trust architecture protects operations and mitigates cyber attacks

The Zero-Trust Access (ZTA) approach would have the following benefits:

- No reliance on implicit trust zones, static accounts & firewall rules
- Each identity (user, machine, app, data) forms its own "perimeter" protection
- Access permissions controlled based on identity, role, and policy
- All interactions have "just-enough-access" enabled "just-in-time"

- Unsecured protocols such as RDP, VNC, Modbus and their vulnerabilities are never exposed outside of the organization, instead proxied over TLS sessions
- Unlike VPNs that put remote user devices (and potential malware on them) into networks, ZTA remote user devices are never inside the network (not even corporate)
- Controls user-to-machine, machine-to-machine, app-to-machine, and app-to-data interactions and secures file/data transfer within and across OT, IT, and Cloud
- Vertical (corporate/remote to control network) and horizontal (ICS site to site) access management
- Driven by central policy management and enforced using distributed nodes (any asset, any location) - The cybersecurity mesh with distributed identity based enforcement is a top strategic trend for 2021 according to Gartner.
- Overlays into existing OT/IT architectures with no network changes or systems changes (compatible with existing deployed base of workstations, HMIs, IEDs, etc..)

Energy Industry Incentives through Rate Recovery

Electric utilities are highly regulated by state and federal regulatory bodies such as the California Public Utilities Commissions (California PUC) and Federal Energy Regulatory Commision (FERC). Investor-owned utilities which serve over 72% of all electrical customers in the United States are currently incentivized to make infrastructure improvements (capital expenses) in order to adjust rates they are able to charge consumers leading to growth in revenue.

Today, infrastructure improvements are defined as mainly capital purchases for hardware power electronics and systems and communication infrastructure to improve grid stability and resiliency. Many network and communication solutions provide built-in network-based security mechanisms which as we discussed in this paper do not go far enough. Stand-alone cybersecurity products which often come in the form of software or software-as-a-service (SaaS) are largely viewed as operational expenses, rather than capital expenses, and therefore purchasing cybersecurity products does not have the same level of incentive for utilities.

Given the scale and reach of the recent cyber attacks it is clear that cybersecurity is in fact an infrastructure improvement that results in better grid stability and resiliency and utilities should be able to recover their investments in cyber security through current capital expense rate recovery mechanisms. This has recently been proposed by FERC in the Cybersecurity Incentive Policy White Paper dates June 18. 2020 (Docket No. AD120-19-000).

This policy adjustment, if adopted by FERC and state PUCs, will create a step change in our nation's ability to protect our electrical energy infrastructure. Similar incentive considerations could be extended to other industries such as oil & gas through surcharges collected to fund cybersecurity regulation.