FROM BLIND SPOTS TO RESILIENCE

How Real-Time Asset and Relationship Mapping Protects the Modern Energy System

By: Jeff Collins

Key Takeaways

- **Blind spots in energy aren't small IT issues.** They've triggered billion-dollar outages and even national crises, proving that what you can't see can destabilize the grid.
- **Failures don't spread from one asset alone.** They spread through hidden connections between IT, OT, and cloud systems, links most teams never see in real time.
- **Static lists and siloed tools can't keep pace.** Spreadsheets and point solutions weren't built for today's distributed, digital energy environment, leaving leaders a step behind.
- **Real-time asset and relationship mapping is the foundation of resilience.** It exposes hidden pathways of failure before they cascade, giving operators the chance to act before small problems become system-wide crises.

The State of Energy Infrastructure: Distributed, Digital, and Fragile

The way energy is generated and delivered is changing faster than at any point in the past century. Wind farms now cover regions once dominated by coal plants. Solar arrays line rooftops and deserts. Large-scale batteries store power for when the sun sets or the wind slows. Gas and hydro plants still provide a backbone, but the future of energy is increasingly distributed, renewable, and digital.

To keep this system running, operators depend on a complex web of assets: plant controllers, inverters, turbines, storage systems, SCADA platforms, cloud dashboards, and vendor portals.

Some assets are physical, some virtual, many hidden in places teams rarely visit.

This interconnected environment promises resilience and cleaner power. But it also creates fragility. Unlike the centralized grids of the past, today's distributed generation is only as strong as the weakest unseen link.

Most energy operators believe they know their infrastructure. In reality, they often have only spreadsheets, quarterly scans, or outdated CMDBs that can't keep pace with constant change. The result is blind spots: invisible assets and relationships that only become apparent when something goes wrong.

And in the energy sector, when something goes wrong, it rarely stays local. It cascades.

The Three Blind Spots Holding Energy Back

Blind Spot #1: You Don't Know What You Have

Modern energy systems include turbines, controllers, gateways, cloud dashboards, and vendor-managed accounts. Some are tracked. Many are not. Static inventories and manual updates fall out of sync quickly, leaving critical gaps.

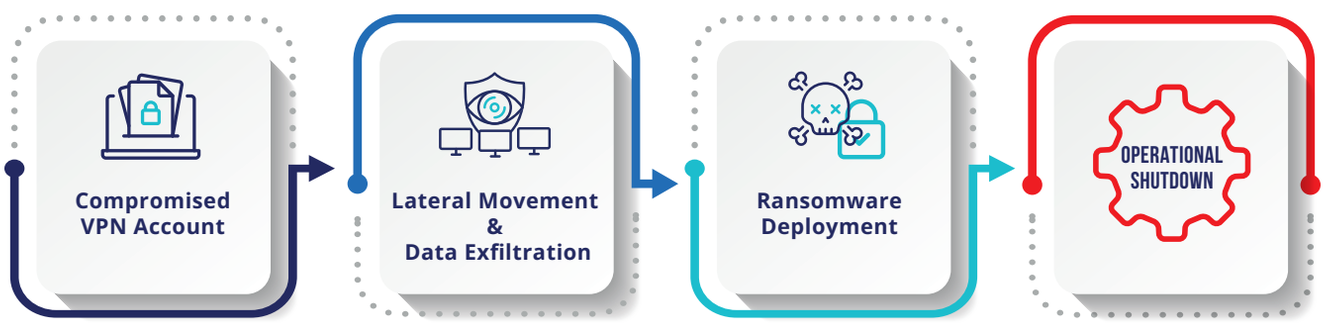
That gap was on full display in 2021, when Colonial Pipeline was forced to shut down 5,500 miles of pipeline carrying nearly half the East Coast's fuel.[1] The entry point wasn't a storm or a direct hit on control systems. It was a forgotten VPN account — inactive, but still live — that attackers used to access Colonial's IT network.[1]

Once inside, they encrypted business systems, including billing, creating risk severe enough that operations had to be halted.[1] Colonial paid $4.4 million in ransom before recovery began.[2]

The root problem wasn't sophisticated hacking. It was a blind spot, a single asset no one realized was still active.

This is the kind of blind spot that slips past static inventories and manual updates, until it's too late.

The Attack Pathway for Colonial Pipeline (2021)



One shadow asset exposed a pathway from IT into OT — and triggered a national fuel shortage.

Blind Spot #2: You Don't Know How It's Connected

An inventory list can show what assets exist, but it cannot show how those systems are connected. In energy environments, unseen relationships create pathways for small intrusions to escalate into large-scale outages.

This was evident in Ukraine in 2015, when attackers disrupted three regional power distribution companies, cutting electricity to more than 225,000 customers.[3]

The attackers didn't use sophisticated zero-day exploits — brand-new software flaws that no one knows about yet. They relied on stolen usernames and passwords, which gave them access to SCADA systems and allowed them to remotely switch substations on and off.[3] To delay recovery, they deployed KillDisk malware to wipe systems.[3]

The breach wasn't just about stolen passwords. The deeper problem was the unseen relationship between IT and OT networks, a bridge system managers did not realize was open until attackers had crossed it.

No list of assets can reveal these hidden bridges; only a live map of relationships can.

Blind Spot #3: You Don't Know How to Contain Failure

Even when teams detect a fault, they often lack visibility into how it will ripple across interconnected systems. What looks like a localized issue may trigger widespread outages if asset connections (i.e., the dependencies between systems) are not understood.

This was the case during the Northeast Blackout of 2003. On August 14, a software bug in an Ohio utility's alarm system prevented operators from seeing that power lines were overloaded.[4] With no clear view of dependencies — how one overloaded line would push stress onto others — they missed the chance to reroute power or shed load where it would matter most.

The failure wasn't caused by a single bug. It was the result of cascading stress across relationships no one could see. That lack of visibility into dependencies, and the inability to pinpoint where to intervene, turned a local fault into an international crisis.

What Needs to Change

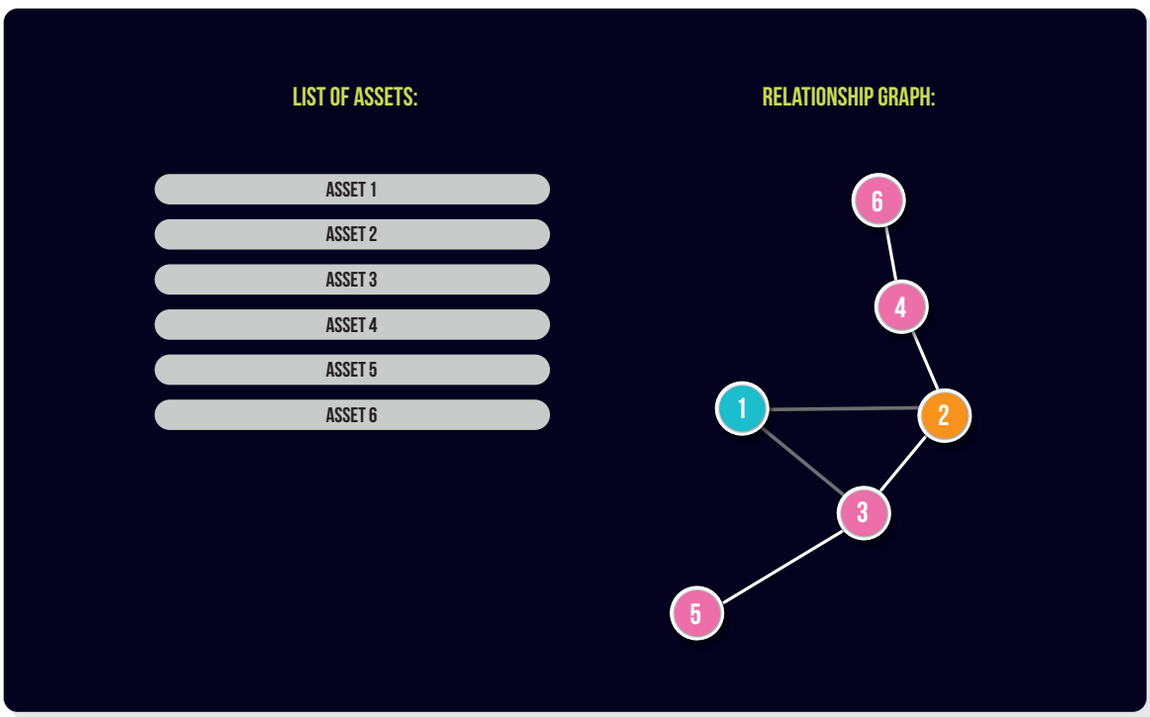
Solving these challenges requires more than asset tracking or traditional monitoring. Energy systems have grown too interconnected, and failures no longer occur in isolation. A single weak point can ripple across IT, OT, and cloud in minutes.

Operators need a new approach:

- **From static inventories to dynamic asset discovery.** Spreadsheets and periodic scans cannot keep up with constantly changing infrastructure.
- **From isolated monitoring to unified observability.** Viewing performance, availability, or security in silos creates blind spots. Teams need one map that shows how these signals intersect.
- **From asset lists to relationship maps.** Knowing what you own is not enough. Resilience depends on seeing how assets connect, where dependencies exist, and how failures spread.

Without visibility into how failures ripple, operators are left guessing where to intervene.

Asset List vs. Relationship Graph



A list shows what you have. A relationship graph shows how it all connects — and how failures cascade.

How WanAware Helps

See and stop risks before they cause outages.

Traditional monitoring tools only raise alerts once something is already broken. WanAware gives energy providers a proactive edge—mapping assets and dependencies in real time so operators can spot weaknesses early and act before they disrupt generation, transmission, or distribution.

Discover and Understand Assets (AIM)

- Get a complete, real-time inventory of IT, OT, IoT, and grid assets without deploying agents.
- Integrate easily with legacy control systems and vendor data exports—no customization required.
- **Outcome:** A trustworthy asset record that eliminates unknowns, reduces blind spots, and strengthens grid reliability.

Understand Relationships and Dependencies (KDE)

- Map a live dependency graph across plants, substations, control systems, and customer services.
- See how stress in one area—like a failed transformer or misconfigured SCADA node—ripples across the grid.
- **Outcome:** Clear visibility into interdependencies and weak points so teams

can contain failures before they cascade into regional outages.

Model and Resolve with Confidence (Digital Twin)

- Safely test firmware updates, policy changes, and configuration adjustments in a virtual model before rolling out to critical infrastructure.
- **Outcome:** Fewer self-inflicted outages, smoother upgrades, and greater operator confidence in system resilience.

Enable Automated Remediation (Remediation Module)

- Run automated actions to isolate compromised devices, reconfigure systems, or alert the right control team.
- **Outcome:** Faster mean time to resolution (MTTR) during incidents and less strain on already limited field and operations staff.

The Payoff: From Blind Spots to Resilience

With WanAware, energy teams gain:

- **A continuously updated asset inventory** across generation, storage, transmission, and distribution.
- **Relationship mapping** that reveals dependencies between IT, OT, and cloud.
- **Context-aware prioritization** that separates minor issues from risks with system-wide impact.
- **Predictive modeling** to identify cascade risks before they spread.
- **Automated remediation** to accelerate containment and reduce manual workload.

The result: a shift from reactive recovery to proactive resilience. Instead of discovering blind spots during an outage, teams can surface them in advance, act with confidence, and reduce the risk of high-impact failures.

Conclusion: Resilience Comes From Seeing the Whole System

The Colonial Pipeline shutdown, the Ukraine cyberattack, and the Northeast blackout all had different triggers. But they shared the same weakness: teams lacked a real-time view of their assets and the relationships between them.

Resilience in the modern energy sector does not come from tracking assets alone. It comes from understanding how those assets connect, where dependencies create risk, and how failures spread.

WanAware enables this shift by unifying discovery, relationship mapping, and observability into a single platform. For energy operators, that means blind spots can be identified and addressed before they become national crises.

- Download the *Energy Asset Blind Spot Checklist* — a practical guide for uncovering risks in your environment.

Uncover Risks in Your Environment

- Activate your *free 30-day trial of WanAware AIM* — Start your trial today and within minutes you'll see a live asset inventory organized by business units, locations, and workloads. No credit card required.

See Your Live Asset Inventory Today

References:

1.U.S. House of Representatives, Committee on Homeland Security. (2021, June 9). Cyber threats in the pipeline: Using lessons from the Colonial ransomware attack to defend critical infrastructure: Testimony of Joseph Blount, President and CEO, Colonial Pipeline Company.

2. U.S. Department of Justice. (2021, June 7). Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside.

3. U.S. Department of Homeland Security, ICS-CERT. (2016). Cyber-Attack Against Ukrainian Critical Infrastructure. Alert (IR-ALERT-H-16-056-01).

4. U.S.–Canada Power System Outage Task Force. (2004, April). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations.

www.wanaware.com