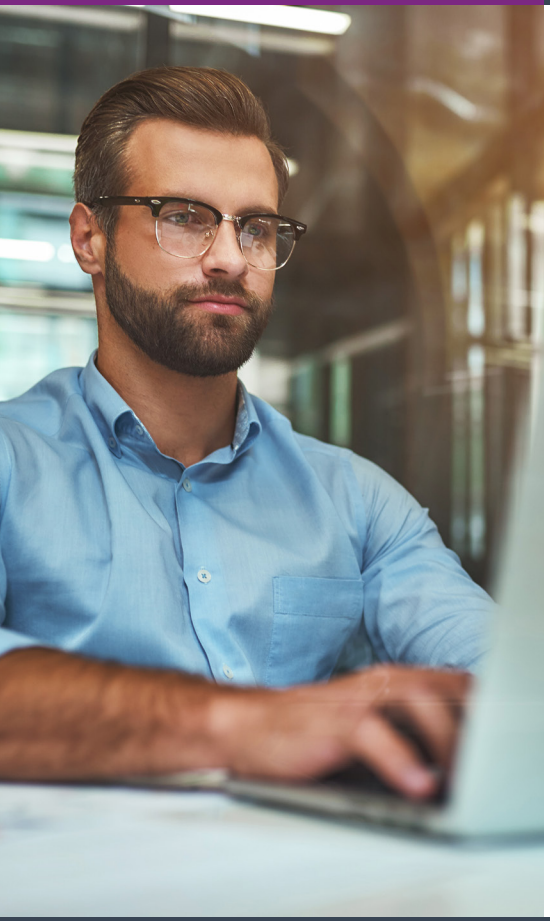
anm

SD-WAN FOR UTILITIES

THE BACKBONE OF SECURE SUBSTATION AUTOMATION

WHITE PAPER



OUR BIGGEST DIFFERENTIATOR IS UNDERSTANDING YOU

At ANM, we believe understanding your business is just as important as understanding technology. That's why we always keep your end goals in mind and work closely alongside you to achieve them. Our team takes pride in providing engineering excellence and quality customer service with a local focus. We specialize in the fastest-growing areas of IT, including risk mitigation, enterprise infrastructure and digital transformation.

DEEP ENGINEERING EXPERTISE

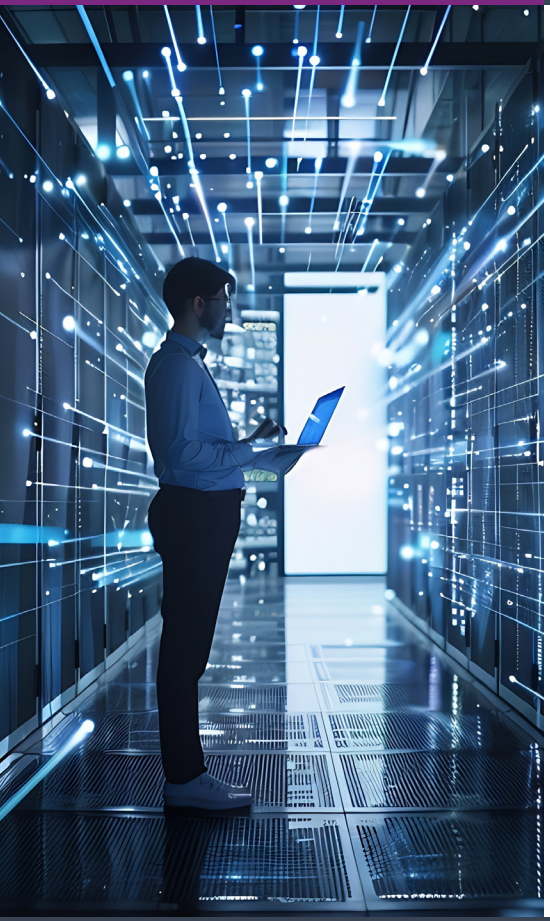
In addition to having six engineers per salesperson, with ANM you get a team of engineering expertise who are not only book smart on the technologies, but also street smart. This means we can help you best operationalize the technologies and avoid common pitfalls.

VENDOR INDEPENDENT RECOMMENDATIONS

The technology landscape is crowded and confusing. Our team of experts make tailored recommendations for your needs. We understand the best partners for your needs are the ones who have an opinion and can help you get technology selection right.

AN ACCELERANT, NOT A BOTTLENECK

We all know technology and business processes have enough bottlenecks. Our goal is to help you move faster so you can expect a sense of urgency when you work with our team.



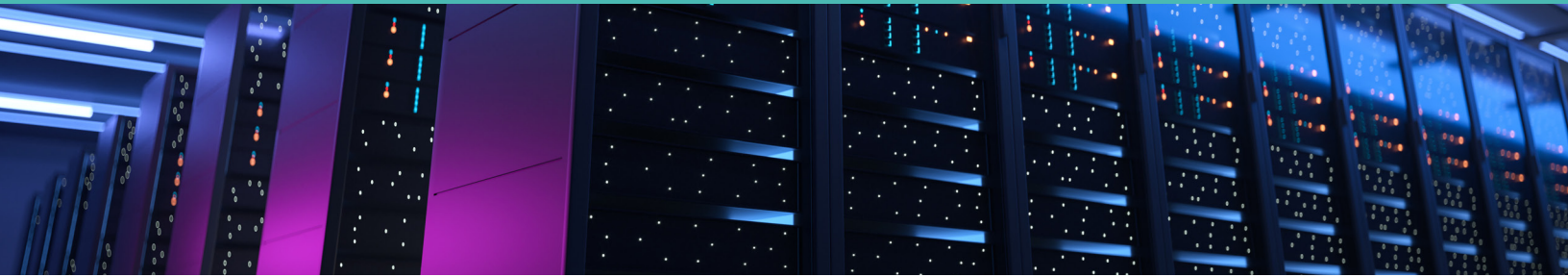
SD-WAN FOR UTILITIES: THE BACKBONE OF SECURE SUBSTATION AUTOMATION

EXECUTIVE SUMMARY

Over the past two decades, the utility sector has undergone a quiet but profound transformation. Networks that were once designed purely for stability and predictable workloads are now expected to support an explosion of distributed energy resources (DERs), advanced sensors, and real-time control systems.

Utilities have recognized this transition and are investing heavily in energy infrastructure. In 2024 alone, U.S. investor-owned utilities spent approximately $186.4 billion, 80% of which was allocated to infrastructure and grid modernization. Yet most field networks connecting substations and remote sites still rely on legacy WAN architectures built for a very different era.

Originally built to provide secure point-to-point connections, these legacy systems now stand in stark contrast to today's demands for flexibility, scalability, and heightened cybersecurity. As operational technology (OT) converges with IT to enable real-time visibility and data-driven operations, vulnerabilities have multiplied, leading to a sharp rise in cyber incidents.



A recent study reveals that 62% of water and electricity utility operators in the U.S. and the U.K. were affected by cyberattacks in the past year. Among them, 57% experienced operational disruptions, and 54% suffered permanent corruption or destruction of data or systems.

As demand surges and threats continue to rise, utilities can no longer afford to operate critical infrastructure on outdated network foundations. To keep pace with this rapid grid evolution, utilities need an agile, secure, and scalable network fabric. Software-defined WAN (SD-WAN) is fast becoming the connective tissue of modern utility infrastructure, linking field sites, substations, and cloud platforms through a single, adaptive network. Embracing this new model can help utilities protect critical assets today while building the flexible, intelligent networks they will need tomorrow.

> In the past year, 62% of water and electricity utility operators in the U.S. and the U.K. were hit by cyberattacks.

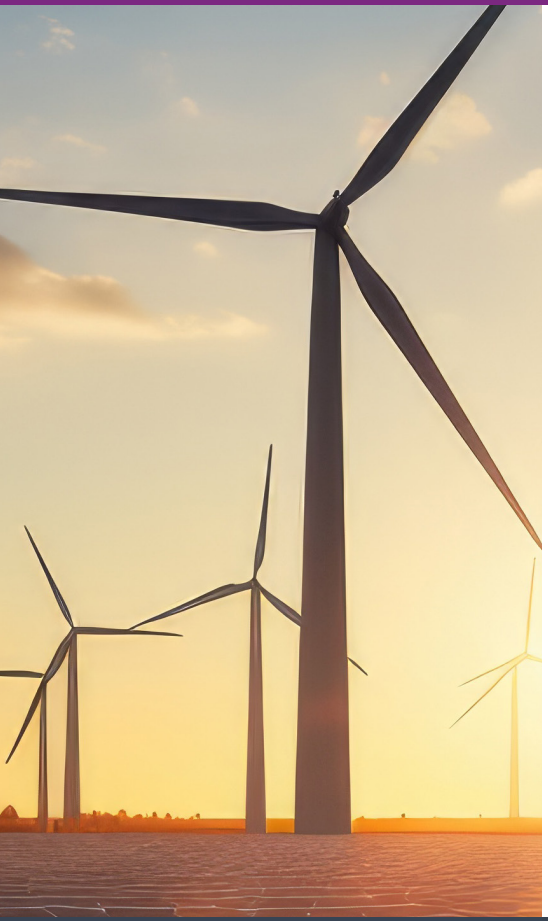
THE GROWING GAP BETWEEN GRID DEMANDS AND NETWORK CAPABILITIES

Utilities are navigating one of the most challenging operating environments in history. They're expected to deliver fast, affordable, always-on service while simultaneously modernizing for clean energy, defending against cyberattacks, and complying with increasingly unforgiving regulations. The result is a widening chasm between expectations and operational capability.

SHIFTING CONSUMER EXPECTATIONS

Today's consumers are digitally fluent, mobile-first, and sustainability-conscious. They expect real-time visibility into their energy use, intuitive digital tools, and responsive service. The utility experience is now measured against tech platforms, not just other energy providers.

But meeting these rising expectations is challenging. Utilities need real-time data, edge connectivity, and flexible infrastructure that can personalize experiences at scale while maintaining the physical grid that underpins it.



SURGE IN CLEAN ENERGY MANDATES

Clean energy mandates are rapidly accelerating. Over half of U.S. states have already implemented renewable portfolio standards (RPS) or clean energy standards (CES) requiring utilities to deliver a growing share of electricity from clean sources. Notably, California's SB 100 requires renewable energy and zero-carbon resources to supply 100% of electric retail sales by 2045. Virginia's Clean Economy Act (VCEA) aims for 100% clean electricity by 2050.

GROWING COMPLIANCE RISKS

At the same time, compliance with standards such as NERC and FERC reliability rules leaves little margin for error, with non-compliance penalties reaching up to $1 million per day. Staying in compliance now means more than routine maintenance. It requires predictive analytics, cross-functional coordination, and the ability to respond to failures quickly.

> Failure to comply with reliability rules can cost utilities $1 million per day in penalties.

ESCALATING CYBERSECURITY THREATS

Finally, as the backbone of critical infrastructure, utilities are top targets for cyberattacks. By August 2024, attacks on U.S. utilities had already jumped by 70% compared to the previous year. Nation-state actors and cybercriminals view utilities as high-value targets, as evidenced by the 2021 Colonial Pipeline attack, which resulted in a $4.4 million ransom payment and an additional $1 million in penalties.

Expanded Attack Surfaces and Remote Access Risks

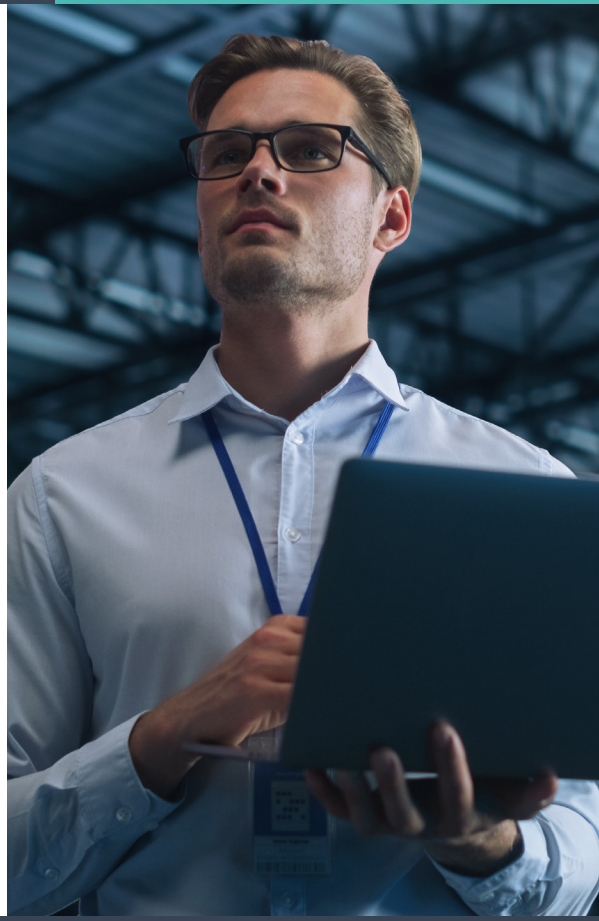
DOMAIN	RISK	WHY EMERGING TODAY
IT	Decentralized access from remote locations – Employees, contractors, and field crews connect from home networks or public Wi-Fi, increasing exposure.	> Growth of distributed workforce; > Reliance on BYOD (bring your own device); > Reduced effectiveness of traditional perimeter security.
	Weakened perimeter defenses – Traditional firewall-based models fail when endpoints are dispersed and often unmanaged.	> Shift from centralized office access to remote/hybrid work environments.
DOMAIN	RISK	WHY EMERGING TODAY
OT	Insecure remote access tools – Many lack MFA, session recording, auditing, or role-based access controls.	> Rapid adoption of remote substation; monitoring/ maintenance; > Need for faster vendor access without proper vetting.
	Unmonitored third-party connections – Vendors use their own tools with little visibility for utility operators.	> Increased outsourcing of OT functions; > Geographic expansion of assets; > Urgency to resolve issues remotely.
	Proliferation of remote endpoints – More sensors, PLCs, and edge devices accessible over networks.	> Digitization of substations; > Convergence of IT and OT networks; > Expanded automation footprint.

THE LIMITATIONS OF LEGACY WANS

Legacy architectures, typically MPLS circuits and point-to-point leased lines, were designed for a centralized, static grid. They offered stability, but little agility. Today, these rigid systems are struggling to keep up with the rapid growth of DERs, real-time analytics, cloud-native tools, and edge-connected assets.

The urgency to modernize is reinforced by the age of the physical grid itself: nearly 70% of U.S. power transformers are more than 25 years old, and much of the broader infrastructure dates back 50–75 years.

> Much of America's electric grid was built 50 to 75 years ago.



INFLEXIBILITY AND SLOW RECOVERY

Modern grid operations depend on real-time data exchange and rapid responsiveness. Legacy WANs, with failover times that can take minutes instead of milliseconds, leave utilities exposed to prolonged outages and delayed system recovery.

This lack of agility hampers the integration of new assets, such as microgrids and electric vehicle charging infrastructure, which slows down modernization efforts and leaves operators frustrated.

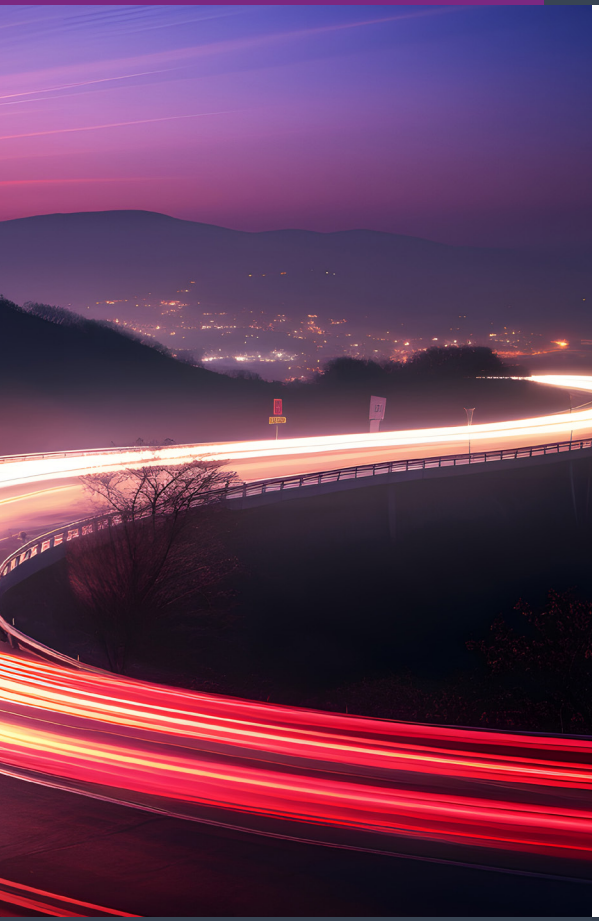
LIMITED VISIBILITY AND HEIGHTENED RISK

Older network designs also fall short in providing visibility into traffic and device behavior. Without centralized monitoring and application-level controls, operators are forced into reactive maintenance rather than proactive management.

Troy Baietto, a Senior Network Architect at ANM, explains:

> *"Troubleshooting takes a long time on legacy WANs. If you want to update an NTP server, you have to go touch every single router to do so."*

As networks become more complex and interconnected, the risk of undetected vulnerabilities and potential disruptions increases. In some substations, control networks are still built on T1s or other low-capacity circuits, as dictated by the original equipment vendor. These constraints slow response times and make it harder to maintain consistent security controls.



OVERCOMING THE CHALLENGES OF OT/IT CONVERGENCE

These limitations block the structural changes utilities need to modernize. As grids become more decentralized and data-driven, the lines between operational technology (OT), which runs the grid, and information technology (IT), which manages data, analytics, and customer interfaces, are rapidly blurring.

OT/IT convergence can enable faster outage response, predictive maintenance, real-time compliance tracking, and secure remote operations. However, without a unified, flexible network foundation, that convergence remains out of reach.

Bridging OT and IT touches every layer of utility operations. From protocols and governance to cybersecurity and real-time data sharing, convergence presents technical and organizational hurdles that many utilities are still grappling with.

ALIGNING PRIORITIES AND CULTURES

One of the major challenges of IT/OT convergence is the stark difference in priorities between the two. OT teams focus on reliability and safety, maintaining equipment expected to run for decades with minimal interruptions. Meanwhile, IT teams operate in a faster-paced environment that embraces rapid updates, continuous improvement, and agile innovation.

> *"IT people are used to delivering to an SLA. If your executive doesn't get an email, that's a pain. But, in OT, if you aren't delivering power, people can die of heat exhaustion. There's a massive gulf between how IT and OT approach their work."*
>
> ***Jason Sieroty**, a Utility Network Engineer, ANM*

Aligning these differing priorities requires careful change management and strong leadership to foster trust and collaboration across departments.

TECHNICAL INTEGRATION RISKS

As utilities connect OT to IT for visibility and control, they also import legacy weaknesses. Many field devices were built for closed networks without encryption or authentication. Once bridged into enterprise systems, they can easily become entry points for attacks.

The risk is even greater when substations maintain a parallel vendor link to controls providers such as Ericsson or GE, creating a second ingress that must be policed. Because standard OT protocols trust the wire, the vendor's posture becomes part of the utility's risk profile. Add real-time analytics, remote access, and cloud integrations, and the attack surface expands across domains.

The implications of this are clear: perimeter-only security will not suffice in this environment.

MEETING PERFORMANCE AND AVAILABILITY DEMANDS

Another challenge is the need for ultra-low latency, deterministic performance, and near-perfect uptime in both IT and OT. A converged environment must support a diverse mix of industrial protocols, high-volume data streams, and dynamic traffic patterns without compromising performance or security.

Without a modern, adaptive network infrastructure, utilities risk building fragile systems that buckle under operational pressures and remain vulnerable to evolving cybersecurity threats.

TACKLING MODERN CHALLENGES WITH A NEW NETWORK FOUNDATION

For years, organizations have relied on tools like VPNs, firewalls, and endpoint protection to secure their networks. But, in converged IT/OT environments they assume fixed perimeters and managed endpoints, and cannot enforce granular, identity-based controls across edge-to-cloud traffic.

In some cases, utilities are completely air-gapped from substation networks; in others, they share a WAN but rely on strict segmentation to prevent lateral movement. These architectural choices reflect a long-standing physical security mindset in OT, but applying the same rigor to logical network access is still a work in progress for many operators.

This is where SD-WAN stands apart, not as another bolt-on tool, but as a network foundation built for distributed, high-stakes environments. SD-WAN provides the agility, segmentation, and performance optimization needed to keep both IT and OT workloads running securely and predictably.

SD-WAN AS THE MODERN UTILITY BACKBONE

SD-WAN introduces a fundamentally different approach to building and managing utility networks. Instead of relying on rigid, hardware-bound connections, SD-WAN embeds security into the fabric of the network to enable:

- End-to-end encryption for data in motion;
- Micro-segmentation to contain threats and isolate incidents;
- Real-time visibility and control over every remote connection, regardless of location.

It also allows seamless integration of various transport types like fiber, LTE/5G, and satellite, with automatic failover to ensure uninterrupted service. This flexibility enables utilities to adopt a proactive security stance, safeguard critical assets, and meet both regulatory and consumer expectations.

Key Benefits

Encrypted Traffic	End-to-end AES-256 IPsec encryption across all paths
Threat Isolation	Micro-segmentation to limit lateral movement
Teal-Time Control	Centralized orchestration across field and control environments
Transport Agnostic	Supports fiber, LTE/5G, satellite with automated failover

EMBEDDED SECURITY BY DEFAULT

Unlike legacy WANs where security appliances are often bolted on at the perimeter, SD-WAN platforms integrate robust security measures from the ground up.

Security Built Into the Network Fabric

When a new substation router or field gateway comes online, it automatically establishes encrypted VPN tunnels with other nodes, securing all data in transit. This protects control traffic such as SCADA commands and relay signals from interception or tampering.

Advanced SD-WAN devices also offer built-in next-gen firewalls (NGFW), intrusion detection and prevention (IDS/IPS), malware filtering, and deep packet inspection — centrally managed and consistently enforced across all locations, including unmanned sites.

Micro-Segmentation for Attack Containment

Micro-segmentation further limits the blast radius of any breach. By isolating traffic by application or device type (e.g., relays vs. IT traffic), SD-WAN prevents lateral movement across the network. A compromised node can't access unrelated systems without passing through enforced policy checks.

Organizations that implement integrated Zero Trust and micro-segmentation report a 95.8% reduction in lateral movement during security incidents, underscoring the real-world effectiveness of this approach.

SIMPLIFYING COMPLIANCE AND GOVERNANCE

Given the highly regulated nature of the energy sector, utilities must continuously meet standards such as NERC CIP (Critical Infrastructure Protection) in North America, as well as international frameworks like IEC 62443 for industrial control systems. Achieving compliance traditionally meant bolting on numerous controls – firewalls, network zones, access logs – and managing them manually across dozens or hundreds of sites. SD-WAN significantly streamlines compliance efforts by building many of these controls into its normal operation.

Virtual Segmentation and Policy Consistency

NERC CIP mandates that critical assets be isolated within Electronic Security Perimeters and that all electronic access be controlled and monitored. SD-WAN's ability to create virtual network segments and secure tunnels for each category of traffic makes it straightforward to define and enforce these perimeters. With centralized policy management, a utility can define segmentation rules once (for example, separating SCADA control traffic from corporate data) and automatically push them to every site, ensuring consistent enforcement of access controls system-wide.

Centralized Logging and Monitoring

Another area of compliance simplification is logging and monitoring. Regulations require extensive monitoring of network connections and quick incident response (e.g. CIP-005 and CIP-008 demand tracking of remote access and reporting of security incidents). SD-WAN solutions typically provide centralized logging of all WAN traffic and user connections. This not only helps in detecting incidents early, it also creates an audit trail to demonstrate compliance during reviews.

GAINING DEEPER VISIBILITY AND CONTROL

Operational visibility is absolutely critical in preventing incidents and ensuring reliable grid performance. Legacy WAN setups often functioned as black boxes – utilities had limited insight into what traffic was flowing between remote sites or whether a rogue device had appeared in the network.

SD-WAN changes that by providing granular, real-time visibility into network behavior across all locations. Every SD-WAN node continuously reports metrics on link performance, application usage, and security events back to a central controller or dashboard. This means network engineers and security teams can see exactly what is happening on the grid's communication fabric at any moment, from a substation in a rural area to the control center's core network.

With this level of intelligence, utilities can:

- Detect anomalies early;
- Respond swiftly to potential threats;
- Make more informed decisions about maintenance and operational priorities.

PRIORITIZING CRITICAL APPLICATIONS

Not all network traffic is equal – especially in utilities, where certain data streams are truly mission-critical. SD-WAN's ability to identify and prioritize applications at a granular level is one of its most powerful features for grid operations. Utilities can define policies that automatically recognize and prioritize key traffic such as SCADA telemetry, protective relay (teleprotection) signals, synchrophasor data, and other control system communications.

By contrast, less critical traffic (corporate email, general internet browsing, even non-urgent IoT sensor data) can be given secondary priority. This intelligent QoS (Quality of Service) ensures that during periods of congestion or network strain, the important stuff always goes first.

Moreover, SD-WAN's application-aware routing goes beyond static priority queues. The system actively monitors each available WAN path for latency, packet loss, and congestion in real time. If the primary MPLS circuit, for instance, suddenly exhibits high latency or an outage, the SD-WAN can instantly switch a high-priority SCADA stream over to a secondary link (like fiber broadband or 5G) to maintain the performance needed.

This dynamic routing happens autonomously in milliseconds, often faster than a human operator could even detect the problem.

ACCELERATED SCALABILITY AND DEPLOYMENT

The transition to DERs and new grid assets demands rapid expansion and seamless connectivity. Traditional WAN architectures have struggled to keep up with this pace because deploying a new site often meant long lead times (for telecom circuits) and manual device configurations by specialized engineers.

SD-WAN flips this script, making network expansion faster, simpler, and more scalable. With SD-WAN, utilities can bring new sites online in a fraction of the time previously required, thanks to features like zero-touch provisioning and centralized orchestration.

Zero-touch deployment means that a field technician can install an SD-WAN router or appliance at a new site (e.g. a substation or a wind farm control cabin) and simply power it on, without any pre-configuring. The device automatically connects to the SD-WAN controller (often over an existing internet link or LTE) and downloads its configuration and security policies.

This is a huge advantage when scaling to dozens or hundreds of remote locations, where sending network engineers to each site would be cost-prohibitive.

CLOUD AND EDGE INTEGRATION

Beyond improving site-to-site connectivity, SD-WAN opens the door for utilities to more seamlessly integrate with cloud services and edge computing resources, capabilities that are increasingly essential in the modern grid.

Today utilities are leveraging cloud-based applications for everything from advanced grid analytics and AI-driven maintenance predictions to customer-facing applications and even cloud-hosted SCADA platforms.

At the same time, they are deploying edge computing devices (for example, substation automation servers or microgrid controllers) that need robust connectivity. SD-WAN is built to handle this hybrid environment by providing secure, high-performance links to anywhere: not just between physical sites, but also to cloud endpoints and edge nodes.

SD-WAN also simplifies multi-cloud and hybrid cloud connectivity. Utilities often use a mix of public cloud providers (Azure, AWS, Google Cloud) for different purposes. With SD-WAN, secure tunnels can be extended into each cloud environment, and the network can intelligently route traffic to the correct cloud based on application policies. All of this is managed centrally, so the complexity of dealing with multiple cloud on-ramps is abstracted away.

REAL-WORLD IMPACT

The benefits of SD-WAN translate directly into measurable, real-world improvements that utilities can observe across their operations.

IMPROVED RESILIENCY AND UPTIME

Utilities depend on continuous data exchange among control centers, substations, and field devices to maintain grid reliability. SD-WAN's dynamic routing and near-instant failover have led to an impressive 94% reduction in network downtime which helps reinforce confidence among regulators and consumers who depend on uninterrupted energy delivery.

COST AND EFFICIENCY GAINS

Shifting from rigid MPLS-based networks to SD-WAN can lower connectivity costs while offering greater flexibility. Utilities can leverage a mix of broadband, LTE/5G, and fiber connections to optimize both performance and budget.

A composite industry study by Forrester revealed how implementing secure SD-WAN delivered a staggering 300% ROI with a payback period of just eight months, while slashing network disruptions by 65%.

Centralized orchestration and automated management reduce the time and resources required for configuration and maintenance. These efficiency gains allow technical teams to focus on strategic initiatives rather than routine troubleshooting.

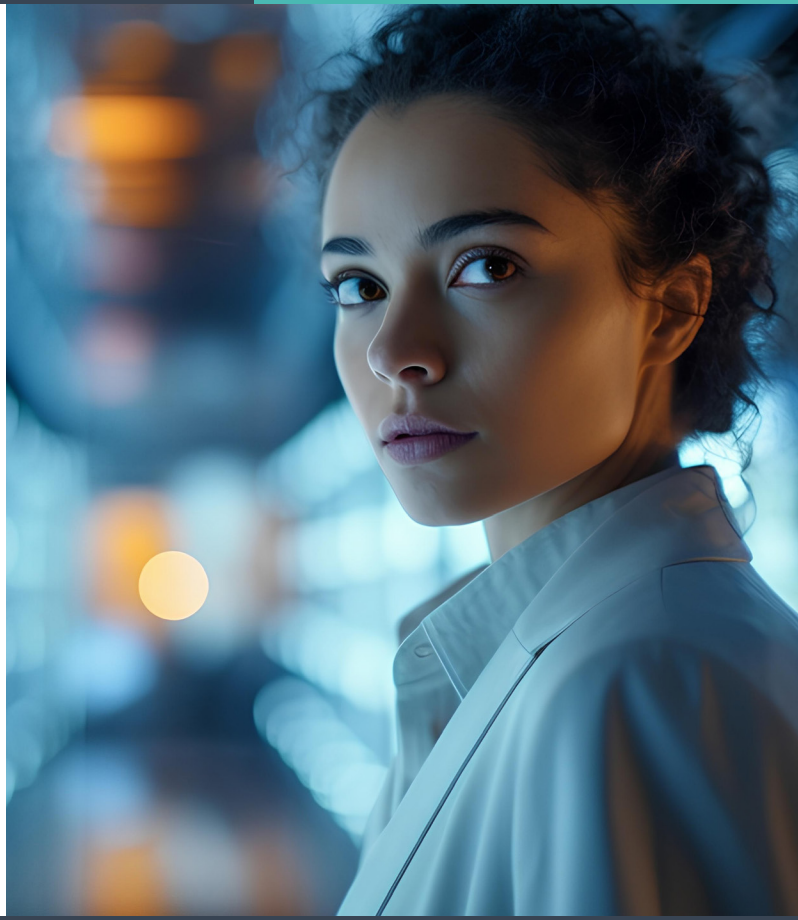
Over time, the financial savings can be reinvested into grid modernization projects and new energy programs.

> SD-WAN has delivered 300% ROI with a payback period of just eight months.

ACCELERATED DIGITAL TRANSFORMATION

SD-WAN's compatibility with cloud platforms and edge computing enables faster substation deployment, DER integrations, and the adoption of emerging technologies like electric vehicle charging and microgrids. It also helps utilities to shift toward predictive maintenance and automated fault detection.

This flexibility allows utilities to adapt more easily to regulatory requirements and market pressures while building the foundation for a smarter, more responsive energy ecosystem.



THE FUTURE
OF UTILITIES WITH SD-WAN

Utilities stand at a crossroads. Legacy WAN architectures, once sufficient for centralized and predictable operations, now hold organizations back from achieving the flexibility and security required by the modern energy environment.

With rising cyber threats, increasing integration of distributed resources, and the push toward real-time grid intelligence, the limitations of outdated systems become more apparent and more dangerous each day.

SD-WAN presents a clear alternative by offering a secure and adaptable foundation that empowers utilities to improve operational efficiency, strengthen cybersecurity, and accelerate grid innovation.

However, successfully realizing these benefits requires thoughtful planning and an experienced partner who understands both the technology and the unique needs of critical infrastructure environments.

ANM brings decades of experience helping utilities design, deploy, and manage advanced network solutions. From strategy and architecture to implementation and ongoing support, our team of experts works alongside utility leaders to navigate complexity and unlock the full potential of SD-WAN.

Now is the time to move forward.

Ready to make the switch? Contact ANM today to deploy a smarter, more secure network built for the modern grid.