paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

A COLLABORATIVE PERSPECTIVE FROM ANTERIX, GE VERNOVA, AND PALO ALTO NETWORKS

Anterix | GE VERNOVA

How Secure AI-Enabled Private Mobile Networks Transform Utility Operations

Avoiding Common Risks to Achieve Resilience

1 Introduction

As digital transformation accelerates, the number of utility-sensing devices and controllable assets is rapidly expanding across the grid. Intelligent electronic devices (IEDs) increasingly monitor, protect, control, and automate equipment in substations and beyond. Traditional centralized grid architectures lack the speed, flexibility, and scalability to keep up with the modern operational demands of these multiplying and complex devices.

Utilities need to shift to a distributed network, with multiple control nodes in communication and coordination with one another. Now, artificial intelligence (AI) technologies, including small language models (SLMs), enable intelligence directly at the edge.

Secure AI-enabled private networks are vital to support the orchestration of the distributed grid architecture. They also provide the necessary tools to protect critical infrastructure, enabling integrity, confidentiality, and availability of communications.

As grid transformation rapidly evolves, utilities that are slow to adapt and embrace AI might struggle to meet the challenges happening around them. Private mobile networks (PMNs), along with purpose-built, AI-aware security solutions, are foundational for these assets to communicate in a safe, secure, coordinated, and efficient manner so utilities can improve grid orchestration.

2 Emerging AI: Utility Applications and the Need for Private Networks

The emergence of AI is transforming the electrical grid into an intelligent, highly coordinated, and adaptive system. It's also shifting operations to be more predictive, prescriptive, and autonomous.

Traditional scheduled or reactive maintenance approaches can stress operations and maintenance (O&M) budgets. With AI-powered intelligent analytics systems, however, utilities can move to predictive health monitoring systems that are asset-specific, data-driven, and condition-based, signaling for maintenance only when needed.

Based on historical operations and near-real-time data feeds, these models empower utilities to avoid truck rolls based on usage or calendar cycles. These monitoring systems also incorporate AI-driven prescriptive elements that provide O&M action recommendations to optimize maintenance, provide decision makers with actionable intelligence, and give a holistic view of asset health.

Small Language Models

SLMs have recently emerged as more efficient, domain-specific, and concise than their large language model (LLM) counterparts. They enable deployment on edge devices that are resource constrained (compute, storage, and networking) and were previously off-limits. Utilities no longer have to run rigid, centralized models of grid operation and control on the public cloud. They can now place the power of AI at the edge, shifting their focus to more distributed and flexible models, to meet the needs of a rapidly transforming and more dynamic grid.

Autonomous Agents

Autonomous agents can manage localized grid functions independently, by managing distributed energy resources (DERs), reconfiguring network topology, and improving performance under changing load conditions. This distributed architecture with multiple control nodes enables utilities to divide their networks into autonomous zones so, when a disruption occurs, it can protect itself to avoid cascading failures.

Multiagent Systems

Multiagent systems expand on this idea to allow for collaborative operations where information is shared, and agents collectively manage grid performance with visibility into neighboring zones and the larger network. The grid transforms into a dynamic, self-organizing system that can adapt in real time to internal and external forces.

Additional AI Applications

Table 1 provides an expansive list of AI-led applications that are transforming the grid.

Table 1. AI-Enabled Utility Private Network Applications

AI Role	Benefits
Classify, locate, and isolate line faults.	Faster restoration, fewer outages, higher reliability, and faster RCA.
Optimize load balancing and voltage regulation.	Reduces energy losses, enhances power quality, and improves efficiency.
Analyze consumption, theft, and demand surges.	Accurate billing, theft detection, and better demand forecasting.
Forecast renewable generation and optimize dispatch.	Provides higher renewable penetration and improved grid stability.
Predict EV demand and manage charging schedules.	Avoids overloads, supports electrification, and balances demand.
Use embedded and external sensor data to monitor health and predict failures.	Reduces unplanned outages, extends asset life, and reduces O&M costs.
Analyze drone imagery and sensor data in real time.	Safer inspections, faster condition assessments, and reduced costs.
Detect anomalies in OT/IT network traffic.	Protects grid backbone and ensures resilience against espionage.
Augment protection schemes with predictive decisioning.	Faster fault clearing, greater selectivity, and improved stability.
Evaluate asset telemetry data from various sensors.	Predicts failures, reduces downtime, and optimizes maintenance cycles.

Hardened Private Mobile Networks Minimize AI Challenges

While AI can bring added value, it also creates new challenges as more devices, assets, models, and data now populate and communicate across every level of the network. They can expose a vast new landscape of attack vectors, resulting in spoofed data, poisoned models, and fake asset statuses.

A strong cybersecurity foundation and posture are essential to protect against emerging threats in this type of decentralized model. Data communications that involve control commands, sensor data, and asset status must be secure. To strengthen their cybersecurity posture, utilities must use AI in cybersecurity solutions to help defend against malicious AI, especially amid growing threats from nation-state actors, cybercriminals, terrorist groups, insider risks, and hacktivists. They must minimize exposure and safeguard their critical infrastructure by establishing hardened, private networks.

As utilities integrate more AI-powered solutions into their systems, they must protect their infrastructure, data, and command communications. They must build a security framework on the foundation of PMNs to maintain grid reliability and resiliency.

3 Private Mobile Networks: The Key to Reducing the Threat Landscape

Private mobile networks are critical AI enablers for OT and enterprise environments primarily due to the traffic profile of AI workloads. These workloads often require a high-capacity uplink to stream large volumes of sensor, video, and telemetry data to AI models, with comparatively smaller amounts of feedback or inference results coming back.

Public mobile networks are typically optimized for download-heavy traffic (e.g., consumer video, browsing, and apps). Private mobile networks, however, suit AI-driven use cases far better in industrial and mission-critical environments because utilities can customize and tune them to prioritize uplink capacity, latency, and reliability.

Private Network Advantages

PMNs offer enhanced security because private networks are separate from public networks and use a dedicated licensed spectrum, giving utilities the essential control and security for mission-critical applications. Private networks include a broad set of security capabilities and built-in features—as defined by the 3GPP (3rd Generation Partnership Project), a global wireless standards body—to enable delivery of advanced cybersecurity protections.

Capabilities

Private networks have many fundamental security capabilities built in, including:

- **Strong network and device authentication** to verify that devices belong on a network.
- **Subscriber identity protection** to help protect network information from being compromised.
- **Robust authentication** management and encryption capabilities.

Utilities own and manage SIM provisioning, device onboarding, and access policies. Every endpoint is uniquely identified, trusted, and continuously verified. Operating on a dedicated licensed spectrum and built with 3GPP security standards, private networks deliver robust protection through network authentication, identity shielding, and encryption.

Isolation from the public infrastructure helps ensure secure, traceable, and reliable data flows, by preventing data poisoning and safeguarding the integrity of AI-driven operations that are critical to mission-focused utilities. Utility companies benefit from the rigorous access controls and advanced authentication methods, which prevent unauthorized access and improve network performance and reliability. These capabilities enable a level of control that public networks cannot achieve.

Benefits

Many utilities are concerned about physical security attacks on substations and other grid assets. A PMN offers many benefits for physical security applications, including low latency, quality of service, and analytics capabilities. These networks can also support a range of enhanced physical security applications like video monitoring with analytics, gunshot detection, and the ability to deliver alerts and dispatch field personnel.

Private networks provide the necessary tools to protect the critical infrastructure, enabling communications integrity, confidentiality, and availability. Utilities can incorporate multiple layers of customizable security to align with established cyber frameworks such as NIST or the International Organization for Standardization (ISO). The security features can provide full visibility into connected assets and their behavior, including traffic monitoring and establishing device and traffic policies for

effective segmentation. Private networks support additional security layers, including device threat monitoring and prevention, device URL filtering, traffic monitoring, identification, authentication, and implementation of customized network access policies.

Public Network Attacks

Recently, sophisticated state-sponsored actors have escalated their targeting of foundational connectivity, exposing the systemic vulnerabilities inherent in public networks. The Salt Typhoon and Volt Typhoon campaigns exemplify this shift toward deeply embedded, strategic compromises of critical infrastructure.

Salt Typhoon

The Salt Typhoon attack is a cyberespionage campaign operated by an instrument of the Chinese government that has penetrated US telecommunications systems. It serves as a stark reminder of the dangers organizations face when relying too heavily on public telecommunications networks for critical operations.

This attack demonstrates how highly organized threat actors can exploit the interconnected nature of modern communications to surveil, disrupt, or even manipulate information flows. Once attackers establish persistence within telecom systems, they can potentially track movements, intercept calls, and harvest metadata at scale—all without directly breaching a company's internal systems.

Salt Typhoon underscores the need to understand the exposure presented when using public telecom networks as fundamentally untrusted. Encryption, segmentation, and redundancy are now baseline requirements for resilience. Without these countermeasures, enterprises risk leaving their most valuable asset—information—vulnerable to persistent and large-scale espionage campaigns.

Volt Typhoon

The Volt Typhoon attack illustrates the sophistication of state-backed adversaries and the strategic risks that arise when attackers successfully bridge the gap between IT and OT environments. Adversaries use techniques to avoid detection and seek to position themselves for long-term disruption of critical infrastructure.

When attackers establish a foothold in IT networks, they can move laterally into OT systems, threatening the operational stability of utilities and other essential services. This attack underscores the urgency of securing the entire spectrum of digital infrastructure where IT and OT converge.

Stronger Defense with Private Mobile Networks and Zero Trust

Private mobile networks have become a powerful tool for resilience. Unlike a public telecom infrastructure, PMNs offer organizations a dedicated, controlled environment for their communications and data flows. When utility companies reduce their reliance on shared carrier infrastructure, they gain stronger control over authentication, traffic segmentation, and endpoint validation. This isolation makes it significantly harder for adversaries to exploit the same systemic vulnerabilities used in attacks like Volt Typhoon. Moreover, private networks enable deterministic performance, which is critical for utilities' latency and reliability.

In addition to the inherent security capabilities of PMNs, utilities must deploy with zero trust and continuous visibility, as well as operate under the assumption that no device, user, or application is inherently trustworthy. They must continuously verify every interaction, tightly segment access, and ensure that anomalous behavior triggers immediate investigation. Visibility into traffic protocols, applications, and potential threats, as well as into the mobile identifiers that belong to the devices within the private network, prevent lateral movement between IT and OT domains.

By combining a private network with zero trust principles and advanced monitoring, utility enterprises can build both stronger walls and smarter defenses. Even if adversaries gain access, utilities can ensure that their ability to persist or cause disruption is severely constrained.

4 | Building an AI-Ready Private Mobile Network Security Architecture

Forward-thinking utilities are boosting efficiency and speed by deploying AI-capable devices at the network edge to process sensor data locally for real-time applications like grid management and predictive maintenance. The effectiveness of these systems hinges on trusted, accurate sensor data. But, they are vulnerable to serious security threats like data tampering, spoofing, meddler-in-the-middle attacks, and AI model poisoning, which could lead to catastrophic failures.

A Multilayered Security Approach

To secure these critical systems, utilities must adopt a multilayered security approach, including a zero trust framework. Together, they enable utilities to continuously authenticate all devices, use encryption for data in motion, implement network segmentation to contain breaches, and use continuous monitoring for anomalies.

As utilities integrate AI into grid automation systems, the supporting communication and security architecture must evolve in parallel. An AI-enabled infrastructure creates new dependencies. For example, models rely on trusted sensor inputs, edge devices process sensitive operational data, and command outputs demand secure execution in real time. Protecting this end-to-end flow requires isolated technical controls and a cohesive, multilayered, AI-aware security framework that's built on the foundation of PMNs.

Private Mobile Network Security Framework

Figure 1 shows this framework as a layered stack with the following levels from the bottom level to the top level:

- **Core security:** At the base lies the secure core, which provides encrypted and resilient transport.
- **Edge security:** The edge becomes a security enforcement zone for data-generating devices and local AI workloads.
- **AI ecosystem security:** Safeguards around models, agents, and training data must be integrated directly into operational workflows.
- **Governance and compliance:** To bind all these layers together, governance and compliance ensure alignment with regulatory requirements, industry standards, and organizational accountability.

Together, these layers create a defense-in-depth strategy for an AI-powered grid so that, if one layer is breached or degraded, the others continue to enforce trust and resilience.

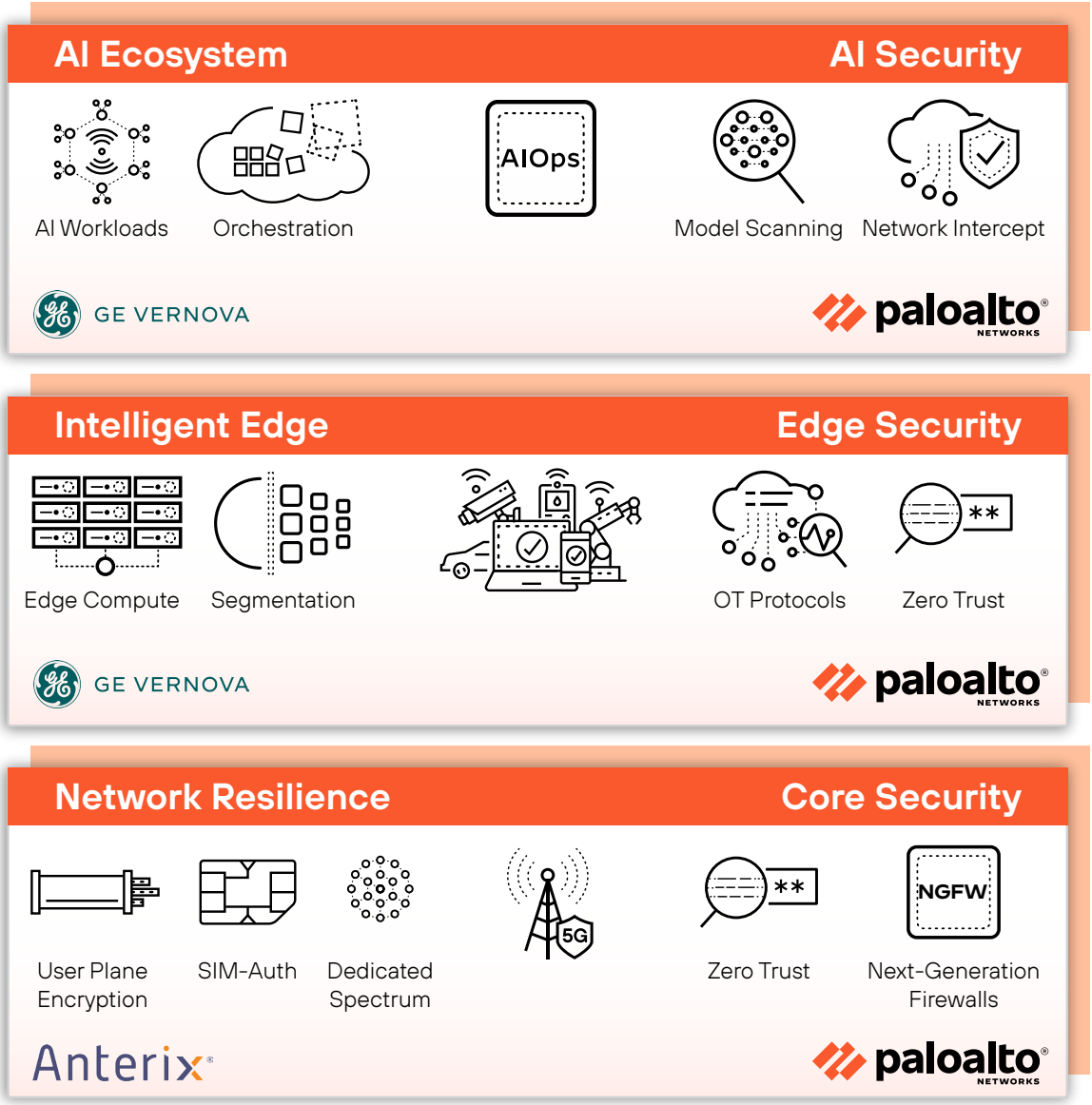

Figure 1. Private mobile network solution framework

Secure the Core

Private mobile networks' secure core ties together substations, renewable energy assets, and industrial metering into a resilient operational fabric. In a hybrid communications architecture (figure 2), this core integrates multiple transport domains—licensed narrowband, LTE, broadband over powerline, and Wi-Fi—with multiprotocol label switching transport profile (MPLS-TP) and optical transport systems, to provide encrypted, failover-ready, deterministic performance. By unifying these technologies under a single private network, utilities achieve both flexibility and control, helping ensure that no single point of failure can disrupt critical operations.

At the same time, the control plane must be tightly secured. Identity-based security posture and access policies prevent unauthorized traffic from traversing between domains, while embedded encryption and redundancy mechanisms ensure continuity of service. This level of security is particularly critical in the utility environment, where adversaries increasingly seek to exploit routing vulnerabilities so they can move laterally across IT and OT systems. By combining a ruggedized transport infrastructure with AI/ML-driven anomaly and exploit detection at the core, utilities can transform what was once a passive backbone into an intelligent defense layer.

Secure the Edge

The edge is where the grid meets utility customers. Substations, distributed energy resources (DER) sites, area medium income (AMI) neighborhoods, and the field workforce all interact with the network here. In a hybrid communications architecture (figure 2), these diverse access points rely on cellular, narrowband, broadband power line communication (BPLC), and Wi-Fi to connect securely back to the core. Without segmentation, strong identity controls, and AI-powered advanced threat prevention, a vulnerability in one domain could compromise the other domains.

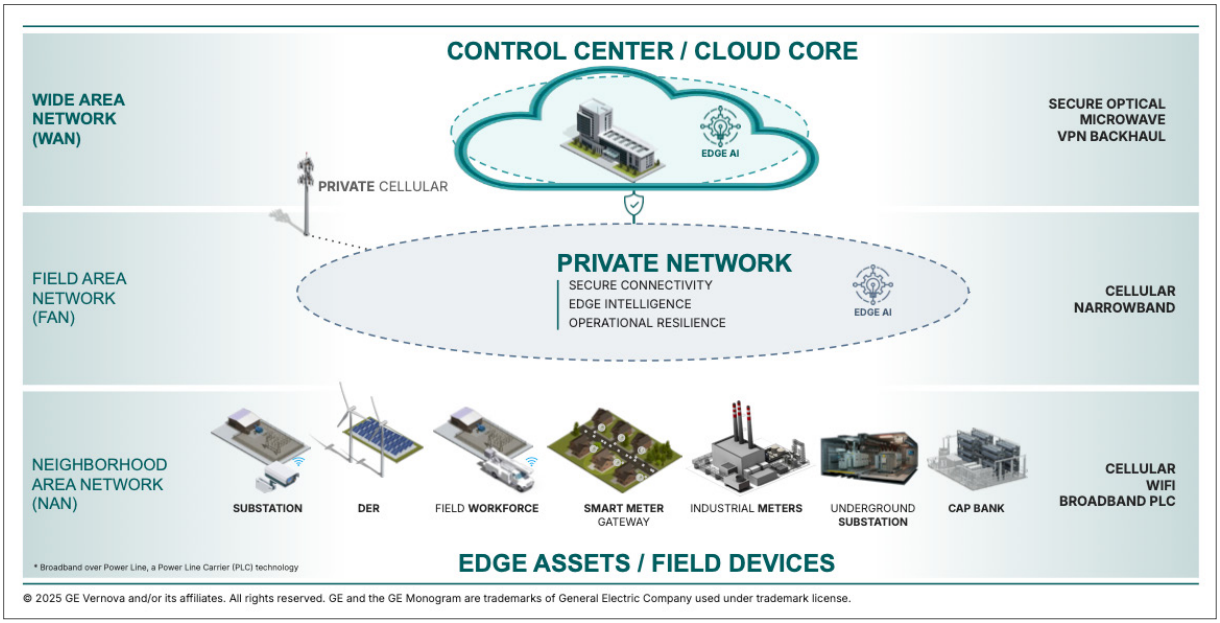

Figure 2. Utility communications architecture

Utilities, therefore, must treat edge security as an enforcement zone, where policies are consistently applied regardless of the access medium. SIM-based authentication ensures that only authorized devices can connect, while segmentation policies isolate telemetry, control, and fault data streams.

Hardened edge routers, such as those deployed in substations and renewable energy sites, now serve a dual role: routing traffic while hosting local security functions and, increasingly, lightweight AI applications. These edge AI workloads filter noisy telemetry, detect anomalies close to the source, and reduce traffic backhaul to the control center. In doing so, they expand both the intelligence and resilience of the PMN.

Visibility and Monitoring

A hybrid communications environment offers utilities immense connectivity, but it also multiplies potential blind spots. Cellular, narrowband, BPLC, and Wi-Fi each introduce their own telemetry, interference patterns, and attack surfaces. To operate securely, utilities must achieve end-to-end visibility across this entire landscape. Monitoring overlays represent how anomaly detection and continuous threat assessment can be embedded at multiple layers of the network—from substations and renewable energy gateways to the field workforce and control center.

AI and ML are particularly effective in this context. By correlating events across access technologies and transport domains, they can detect patterns that human operators might miss. Examples include radio frequency interference, which suggests a jamming attack, an unauthorized device joining over Wi-Fi, or an unexpected topology shift in the LTE domain.

Real-world campaigns, like Volt Typhoon, highlight the stakes. That is, state-sponsored adversaries can "live off the land," blending malicious activity with normal traffic to avoid detection. They can also use AI to analyze network traffic inline and instantly stop known, unknown, and highly evasive threats to prevent patient zero. Utilities can hope to identify such threats before they cascade into operational disruption only by embedding continuous, AI-driven monitoring into the PMN.

Secure the AI Ecosystem

AI systems—including models, agents, orchestration layers, and training data—represent new attack surfaces. Edge-deployed AI applications should undergo runtime integrity checks and be sandboxed to isolate compromised modules.

Utilities must continuously perform red teaming exercises to simulate adversarial attacks and model scanning to automatically analyze AI models for vulnerabilities and misconfigurations. More secure update mechanisms, including model signing and audit logging, help maintain trust in distributed AI systems over time. To prevent risks, such as poisoned training data, prompt injection, and sensitive data leakage, utilities must use security solutions that can discover, assess, and protect AI applications, agents, models, and datasets across their lifecycle. Given the rapid evolution of AI, they must assume that even trusted components can fail eventually or be exploited, making layered defenses and continuous verification essential.

Figure 3 shows the relationship between field devices, edge compute, PMNs, and AI platforms. Field devices, such as sensors and other intelligent electronic devices, generate operational data, which is often processed locally at substations or edge routers.

The PMN acts as the secure conduit in this flow, helping ensure that only authenticated, encrypted, and validated traffic moves toward central or cloud-based AI systems. By positioning PMNs as the trust layer in this pipeline, utilities can reduce the attack surface and help ensure that AI decisions are based on accurate and uncompromised data. This architecture demonstrates why PMNs are both communication tools and foundational security assets for an AI-ready grid.

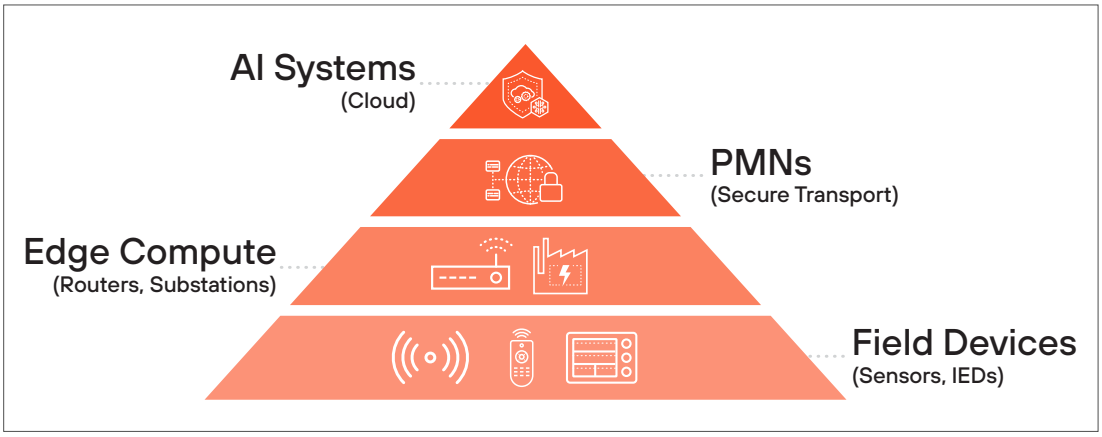

Figure 3. Private Mobile Network Framework

Governance and Compliance

Utilities face growing regulatory pressure to account for AI-driven operations. Effective governance is a critical success factor for AI adoption in utilities. Oversight must extend to AI models, data protection, and third-party risks, while aligning with regulatory frameworks, such as NERC CIP, IEC 62443, and IEC 61850. Utilities should establish clear governance frameworks that balance innovation with accountability and compliance.

5 Conclusion

AI is an increasingly powerful tool that is essential for utility companies to innovate and help transform their operations. The Volt Typhoon attack is a warning. It indicates that attackers are becoming more sophisticated and adept at living off the land, posing direct threats to the nexus of AI and private networks.

Securing AI requires protecting algorithms, but it demands safeguarding the data, devices, and networks that underpin intelligent operations. Utilities that deploy AI-ready private networks and adapt unified zero trust strategies across IT, OT, and AI systems will build the resilient, intelligent grid required for the future.

About Anterix

Anterix is transforming how critical infrastructure stays connected. As the nation's leading connectivity partner for utilities, Anterix delivers more secure, private 900 MHz licensed spectrum and advanced intelligent infrastructure solutions that enhance efficiency, strengthen resilience, and accelerate digital transformation. Backed by a growing ecosystem of industry-leading partners, Anterix provides the connectivity foundation that powers a more resourceful and resilient future. Learn more at www.anterix.com.

About GE Vernova

GE Vernova Inc. (NYSE: GEV) is a purpose-built global energy company that includes Power, Wind, and Electrification segments and is supported by its accelerator businesses. Building on over 130 years of experience tackling the world's challenges, GE Vernova is uniquely positioned to help lead the energy transition by continuing to electrify the world while simultaneously working to decarbonize it. GE Vernova helps customers power economies and deliver electricity that is vital to health, safety, security, and improved quality of life. GE Vernova is headquartered in Cambridge, Massachusetts, U.S., with approximately 75,000 employees across 100+ countries around the world. Supported by the Company's purpose, The Energy of Change, GE Vernova technology helps deliver a more affordable, reliable, sustainable, and secure energy future. Visit www.gevernova.com.

About Palo Alto Networks

As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_wp_how-secure-ai-enabled_010626