

Power Sector Infrastructure Modernization at Enterprise Scale



Infrastructure modernization for critical power-sector operations

EXECUTIVE CONTEXT

COMnet delivered a multi-domain modernization program for one of India's largest power companies, integrating network management, automation, SD-WAN-ready firewall architecture, switching rollout, server deployment, and multi-OEM governance under one accountable delivery model.



Network Management

Management and automation suite for centralized visibility.



Secure SD-WAN

Firewall architecture across locations for secure transformation.



400+ Switches

Large-scale switching rollout across distributed locations.

IMPACT

- Established centralized network management and automation capabilities to improve visibility, change control, and operational consistency across distributed power-sector environments.
- Delivered firewall and SD-WAN-ready security architecture across multiple locations, strengthening segmentation, traffic control, and perimeter resilience.
- Rolled out 400+ network switches across locations to standardize access and aggregation connectivity for enterprise and site operations.
- Executed end-to-end server deployment across multiple locations, supporting compute readiness, infrastructure standardization, and operational continuity.
- Reduced multi-vendor complexity by positioning COMnet as the single point of accountability across network, security, infrastructure, and OEM stakeholders.

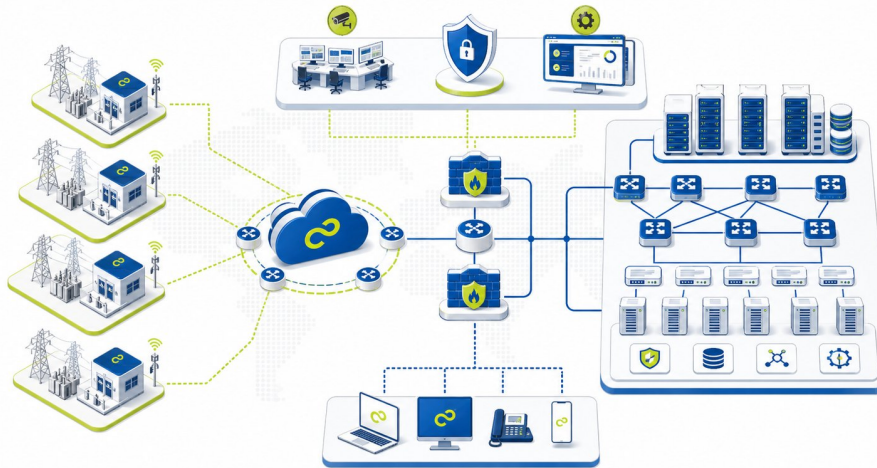
MAJOR ISSUES

- Distributed plants, offices, and operational sites required unified monitoring, device governance, and consistent network/security operating procedures.
- Fragmented network and firewall environments increased policy drift, support complexity, and risk during SD-WAN transformation.
- Large-scale switching and server rollout introduced deployment risk across sites, including configuration consistency, change-window control, and acceptance signoff.
- Critical power infrastructure demanded resilient architecture, minimal service disruption, and disciplined coordination across OEMs and implementation teams.
- The client required an accountable partner to integrate network management, security controls, endpoint/server deployment, and ongoing operational support.

Infrastructure modernization for critical power-sector operations

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE



Engagement Highlights

- Designed and deployed a network management and network automation suite for centralized control, visibility, and operational repeatability.
- Architected and delivered multiple network firewalls across locations in support of secure SD-WAN transformation.
- Delivered 400+ switches across locations with standardized deployment, configuration governance, and site-level execution.
- Managed the relationship across multiple OEMs through a single point of accountability and structured escalation governance.
- Completed end-to-end server deployment across multiple locations to support infrastructure modernization and workload readiness.

Technical Deployment Scope

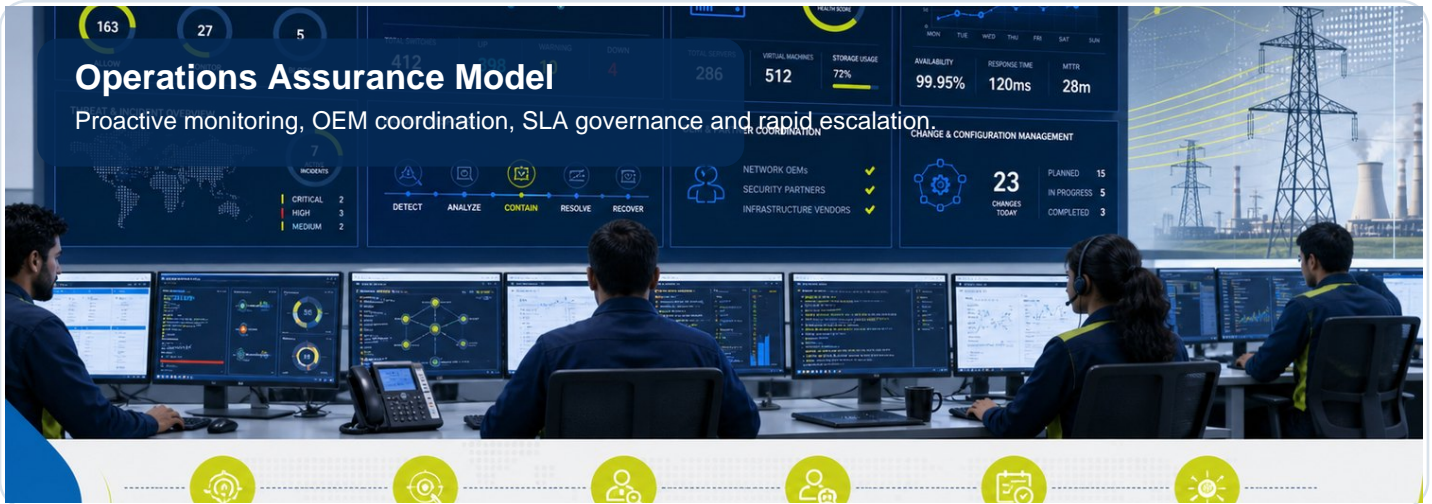
- Geographically Distributed Service Model: Deployment methodology supported multi-location power-sector environments, including plant, office, and operational connectivity patterns.
- Centralized Management Plane: Network management and automation layer provided inventory visibility, configuration governance, event visibility, and standardized administration.
- Security Enforcement Layer: Network firewalls were designed for SD-WAN traffic flows, segmentation, secure internet and inter-site communication, and policy consistency.
- Campus/Branch Switching Layer: 400+ switches were deployed across locations to strengthen endpoint, server, and operational network connectivity.
- Server and Compute Layer: Multi-location server deployment created a standardized compute baseline for infrastructure and application services.
- OEM and Support Integration: COMnet coordinated OEM partners, field engineers, remote teams, documentation, and escalation paths through one governance framework.

Power Sector Infrastructure Modernization at Enterprise Scale



Infrastructure modernization for critical power-sector operations

KEY STRATEGIES



- Reference Architecture First: Reusable design patterns were applied for firewall, switching, network management, and server deployment to reduce variance across sites.
- Security-by-Design: Firewall deployment was aligned with segmentation, least-privilege traffic control, SD-WAN readiness, and operational resilience requirements.
- Automation-Led Operations: Network automation was positioned to reduce manual administration, improve change accuracy, and support faster troubleshooting.
- Phased Rollout Governance: Site readiness, staging, deployment windows, validation, rollback planning, and acceptance criteria reduced implementation risk.
- Single Point Accountability: COMnet acted as the integration and accountability layer across OEMs, delivery teams, and client stakeholders.
- Operational Readiness: Documentation, runbooks, knowledge transfer, and support handover ensured the environment could be sustained after go-live.
- Executive Visibility: Delivery tracking, risk registers, escalation governance, and periodic reporting provided transparency to business and technology leadership.

Solution Model

- Network Management & Automation: Central platform for visibility, configuration tracking, operational alerts, and automation-led administration.
- Secure SD-WAN Foundation: Distributed firewall architecture for segmentation, route control, and standardized security policy.
- Switching and Server Modernization: Standardized switch rollout plus multi-location server implementation with testing and handover.
- Program Governance: OEM coordination, delivery tracking, risk management, documentation, and executive reporting under COMnet ownership.



EXECUTIVE OUTCOME

COMnet established a secure, scalable infrastructure foundation across network management, SD-WAN-ready firewalls, 400+ switches, server deployment and OEM governance.