etisalat and

Case Study

Oil & Gas Industry

e&'s end-to-end unified solution enabled better network performance and security posture.

Customer Background

A leading oil production organisation in the United Arab Emirates (UAE) and among the world's largest oil companies. The enterprise operates across the entire hydrocarbon value chain and has more than 15 subsidiary companies in upstream, midstream and downstream stages of production. The organisation develops both onshore and offshore gas fields and operates two oil refineries. Recently all subsidiaries came under one common identity, which enhanced the organisation's visibility and positioning at a local, regional and international level.

Playing an extremely crucial role in the economic development of the UAE, the organisation has created a positive impact on the nation, community and people. The company has a visionary outlook of implementing innovative practices that maximise the value of its resources along with meeting the volatile demands of the energy market. By deploying the latest solutions and technologies the organisation wants to remain at the forefront of the global energy industry.

Challenges

The parent organisation managing the IT operations for their subsidiary companies was facing challenges to unify the IT operations, deploy uniform IT security policies, and reduce its operational costs.

The organisation had a multi-vendor environment, where the WAN connectivity was provided by e&, but LAN and security portfolio e.g., Hybrid DDoS Next Generation Firewall etc., were procured in silos and managed by multiple IT vendors with non-standardised IT policies.

Managing LAN, WAN and colocation services in the multi-vendor support environment with isolated help desks proved time-consuming and brought business inconsistencies.

Each subsidiary had dedicated IT resources in the office and disperse IT policies because of the lack of uniform IT expertise in certain subsidiaries. Since each operating company had their own internet breakout from e&, non-standardised web security policies resulted in IT complexities and higher operating costs.

- Inefficient application architecture with disperse network
- Non-standardised security portfolio
- Inconsistent support processes and isolated help desks
- High IT operation costs
- Lack of uniformity in IT policies and resources

24/7
Managed Service
For proactive monitoring

Solution Details

The reputed energy producing organisation recognised that by partnering with a Managed Service provider, their IT Group policies would be standardised and the IT department's operations and practices would be enhanced at a lesser cost than before.

The management was convinced that their IT network was more secure and scalable in the hands of e& as a Managed Service provider offering Managed Services for WAN, data centre hosting and deploying Hybrid DDoS & Next Generation Firewall for their 11 office locations in the UAE.

To facilitate immediate IT Network resolutions, a team of dedicated managed resources was provided in the customer's premise, along with dedicated Service Managers in the NOC for handling L1 & L2 issues, and subsequently, have a Managed Service on 24/7 for proactive monitoring of routers, firewall devices, encryption, DNS, core connectivity and data centre as part of the end-to-end solution. The overall solution was wrapped around with consolidated Service Desk as one bundle that will be managed by e& GSOC and CNOC.

Delivering immediate benefits, e& provided the following unified solutions in all their sites consisting of:

- Consolidated managed private network & DC with centralised internet connectivity
- Centralised and standardised web filtering policies
- Managed Service with SLA for the core network and colocation services
- Dedicated Managed Resources provided in customer locations
- Central monitoring of cybersecurity threats

TECHNICAL DETAILS

- Managed WAN
- Managed LAN
- Managed Data Centre & DR
- Managed Security

BUSINESS RESULTS & BENEFITS

- Control and monitoring of cybersecurity threats across OPCOs with uniform IT policies
- Reducing TCO through standardised infrastructure
- Business continuity, higher uptime with redundant connectivity for all links including DC and DR on 24/7 monitoring
- Network consolidation between the customer's DC and e&'s DC
- IT infrastructure replacement along with end of life routers and switches
- Improved collaboration between OPCOs with network consolidation
- Centralised unified security posture with better visibility at group level
- Simplified support process with unified help desk
- Reduced cost