Transforming a Distributed Legacy Network into a Secure, Integrated System

Industry: Manufacturing & Mechanics

Project: Cybersecurity

Customer Description

The customer is a global leader in manufacturing and mechanical solutions, operating across multiple continents. They optimize supply chains for clients at local, regional, and global levels. Through acquiring several manufacturing firms, they inherited legacy IT systems, leading to challenges in managing a unified and secure network.

Background

The customer's acquisitions resulted in a fragmented network infrastructure. IT management was outsourced to local vendors who implemented temporary security solutions, leaving the customer with several issues:

- **Inconsistent network infrastructure,** complicating centralized management.
- **Lack of visibility and control,** affecting decision-making.
- **Multiple transport mechanisms (MPLS,** Internet, VPN), causing inefficiencies.
- **Outdated equipment,** posing security and performance risks.
- **High operational costs** due to multiple licenses and contracts.

Customer Business Objectives

The primary goals were to:

- **Centralize network management** for better visibility and efficiency.
- **Standardize security policies** across all global offices.
- **Reduce costs** through license consolidation under a single Enterprise Agreement.
- **Upgrade infrastructure** for better performance and scalability.

Axelliant's Approach

Axelliant was selected to lead the project, employing a phased approach to stabilize and secure the network while providing a scalable solution.

Discovery and Assessment

During discovery, Axelliant identified critical issues:

- **Inconsistent network architecture** and outdated hardware.
- **Lack of network segmentation** and open access vulnerabilities.
- **Decentralized IT management,** with no standard user authentication.
- **Unmanaged traffic** and poor network performance.
- **Multiple transport methods** with no unified strategy.

Solution Implementation

Axelliant implemented a comprehensive solution that included:

Network Restructuring:

Outdated hardware was replaced with Meraki Network Switching and Access Points, offering a scalable, cloud-managed solution.

Security Enhancements:

NextGen Firewalls, Cisco Umbrella for DNS-layer security, and Cisco DUO for multifactor authentication secured both perimeter and internal networks.

Network Segmentation:

Critical systems were isolated from internet-based ones, reducing risks. Cisco ISE provided centralized **dot1x authentication**, ensuring only authorized users and devices accessed the network.

Traffic Management and Transport Optimization:

Axelliant unified transport methods and introduced Trusted Network Detection for remote users, improving security and enforcing policies. QoS ensured better network performance.

License Consolidation:

Axelliant streamlined licensing under a **Cisco Enterprise Agreement**, reducing redundancies and costs.

Communication Enhancements:

Cisco Webex Calling and Meeting Solutions improved global collaboration and communication.

Conclusion

Axelliant successfully transformed the customer's fragmented and outdated network into a modern, secure, and centrally managed system. This not only enhanced security but also improved efficiency and reduced costs. The scalable solutions provided by Axelliant positioned the customer for future growth, ensuring their network is resilient and adaptable to evolving business needs.