

## CASE STUDY

# Robust WAN and Physical Security Assessment and Design for a National Telecommunications Provider

Network Assessment and Security Enhancement for a National Telecommunications Provider with In Balance IT



## Executive Summary

In Balance IT was approached by a national telecommunications provider to perform a Network Assessment and provide recommendations for their Wide Area Network (WAN) and physical network security. The engagement focused on enhancing "Tier 0 - Core Connectivity Services," which are foundational infrastructure services required for critical applications to function. The objective was to simplify and optimize the network while leveraging existing investments.

## Introduction

In Balance IT collaborated with a large national telecommunications provider to secure their Wide Area Network and rearchitect their environment to accommodate future growth and ensure customer satisfaction. The scope included core network infrastructure, global interconnectivity, regional facilities, and enabling resiliency in the core network. In Balance utilized the EDGAR methodology (Engage-Discover-Gap-Analyze-Recommend) for conducting assessments. This gap analysis methodology guided the assessment process, tailoring activities to the unique characteristics of the engagement.

## Challenge

The client operated two core networks that utilized services from prominent public cloud providers while integrating with on-premises data centers. However, there were vulnerabilities identified in the network topology, such as a lack of internet redundancy between data centers. The risk of downtime existed due to critical production workloads distributed across Azure and AWS.

Additionally, core network devices required reconfiguration to address routing and spanning-tree protection issues, leading to intermittent disruptions in both data centers.

## Summary

### Company

National Telecommunications Provider

### Type

Telecommunications

### Challenge

There were vulnerabilities identified in the network topology, such as a lack of internet redundancy between data centers.

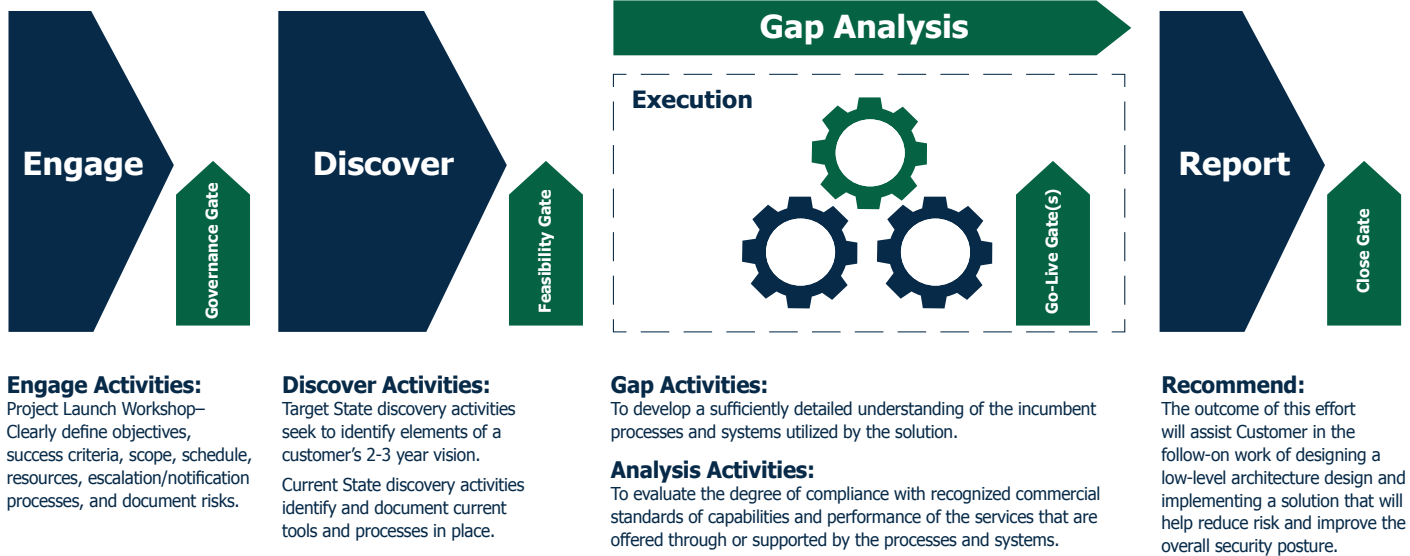
### Solution

In Balance recommended a methodical approach that achieved scalability, reliability, multi-datacenter capabilities, datacenter separation, security enhancements, and zero-trust architecture.

### Results

Connectivity upgrades were recommended to remove bandwidth constraints, improve scalability, and enhance overall network performance and reliability.

**EDGAR methodology**



**Solution**

The recommended approach involved choosing Azure as the primary cloud provider and designing the architecture based on Microsoft’s recommended landing zone concept. This approach created a scalable, resilient, and secure cloud environment in Azure.

For the network portion of the Azure environment, a centralized connectivity subscription was proposed, aligning with best practices and providing consistency throughout the cloud environment.

In Balance recommended a methodical approach that achieved scalability, reliability, multi-datacenter capabilities, datacenter separation, security enhancements, and zero-trust architecture. These outcomes aimed to simplify network expansion, implement redundancy, enable deployment in multiple regions, ensure datacenter isolation based on security requirements, inspect and secure North-South traffic, and implement a Zero Trust approach for east-west traffic.

**Results**

Both data centers required extensive improvements to leverage high availability architecture and resolve configuration issues. The current design provided centralized control over internet access but lacked sufficient east-west security controls. To address this, functions such as north-south connectivity, business partner connectivity, and VPN connectivity were

suggested to be consolidated into firewall pairs, utilizing features like SSL decryption for east-west traffic control. Connectivity upgrades were recommended to remove bandwidth constraints, improve scalability, and enhance overall network performance and reliability. Additionally, In Balance suggested leveraging licensed features that were underutilized to maximize technology investments.

To achieve the ideal future state, In Balance proposed three simultaneous workstreams:

- 1** Tactical business-as-usual recommendations: Implement tactical measures to document the network infrastructure, speeding up troubleshooting and knowledge transfer.
- 2** Tactical Break/Fix recommendations: Address issues such as cloud selection, CPU spiking, firewall configurations, and routing flapping.
- 3** Strategic recommendations: Develop solution designs and architecture oversight for a resilient and scalable future state. By executing these workstreams in parallel, the client could achieve a secure, up-to-date network infrastructure capable of supporting their growth and scalability requirements.

By executing these workstreams in parallel, the client could achieve a secure, up-to-date network infrastructure capable of supporting their growth and scalability requirements.

