



INDUSTRY

Food service

CHALLENGES

- Frequent downtime, high latency, flapping and packet loss
- Maintaining dual MPLS link at each store is costly.
- Unsatisfactory detection, automatic failover and recovery from link issues.
- Security vulnerabilities and loopholes at store locations.

RESULTS

- Significant cost savings.
- Increased availability and connectivity flexibility.
- increased business by reducing failed and missed orders, as well as increasing general availability of their store locations.
- Reduce TCO by enabling cheaper link connectivity options
- Improving throughput over the existing links.
- Consolidating WAN and security features into a single software stack.

Large Food Retailer Secure SD-WAN Case Study

*Increased Business Availability;
Better TCO; Integrated WAN and Security*

Company Profile

A primary quick-serve food retailer based in India and surrounding countries holds franchise rights to multiple leading international brands, as well as having recently launched their own brand to enter a new food market segment. The company employs tens of thousands of people and its network contains over a thousand restaurant locations, regional locations and warehouses.

Challenges

Several hundred of the company's current network locations consist of Fortinet appliances with no SD-WAN features enabled. Other sites use Cisco routers managed by an MSP with connectivity from various ISPs.

The company experienced several challenges with their existing infrastructure, including:

- **Link instability:** Frequent downtime, high latency, flapping and packet loss, impacting business with many dropped orders and stores being offline.
- **Cost:** Maintaining dual MPLS link connectivity to ensure backup availability at each store is costly.
- **Hybrid connectivity:** Unsatisfactory detection, automatic failover and recovery from link issues.
- **Security:** Security vulnerabilities and loopholes at store locations using DIA.

The company evaluated several proposed solutions from Fortinet, Cisco, Citrix, Silverpeak and VMware.

Solution Highlights: Versa Secure SD-WAN

Versa delivered a Secure SD-WAN solution to the company in partnership with Tata Communications as the ISP to refresh the majority of their sites, including stores, the data center, some warehouses and regional offices. To limit their risk, the company opted for a dual solution approach with 2 SD-WAN vendors and 2 ISPs.

Key company pain points addressed by the Versa Secure SD-WAN features and capabilities include:

- **Link instability:** The SD-WAN POC at multiple store locations with dual bad quality/lossy links (MPLS and broadband; dual LTE) significantly and consistently improved throughput, traffic stability and uptime. The Versa traffic conditioning features addressed issues related to packet loss and flappy links. Deploying these features curtailed business losses by reducing the order failure rate from 10-15 per day to 1-3, and simultaneously increased overall store availability.
- **Cost:** The Versa Secure SD-WAN provided savings by using MPLS as primary connectivity and broadband as secondary, instead of dual MPLS.
- **Hybrid connectivity:** The Versa Secure SD-WAN provided seamless link failover and bandwidth aggregation, significantly improving site reliability, availability and throughput.
- **Security:** Consolidating SD-WAN and branch security into a single device enabled JFL to deploy full-fledged NGFW and UTM features for store locations using DIA.

Results

The Versa Secure SD-WAN solution delivered significant cost savings, increased availability and connectivity flexibility to the company. The Versa SD-WAN increased the company's business by reducing failed and missed orders, as well as increasing general availability of their store locations. It also helped reduce TCO by enabling cheaper link connectivity options, improving throughput over the existing links and consolidating WAN and security features into a single software stack.