



Customer Story

Burger King Scales SD-WAN for Hundreds of Restaurants

Burger King scaled its existing WAN infrastructure with Forcepoint Next-Gen Firewall and SD-WAN, enabling the deployment and management of policies for hundreds of its restaurants centrally, remotely and efficiently.

Coming up on End of Life for its existing WAN appliances, Burger King chose to explore other options. Forcepoint Next-Generation Firewall (NGFW) and Software-Defined Wide Area Networking (SD-WAN), combined with URL Filtering and Advanced Malware Detection (AMD) stood out as the superior option. As a result, Burger King enjoyed immediate cost savings and reliable connectivity.



CUSTOMER PROFILE:

Burger King is the leading Quick Service Restaurant brand in Turkey. Operating over 650 restaurants since 1995, its focus on its consumers and its vertically integrated business has enabled the company to win numerous awards across the EMEA region.

INDUSTRY:

Retail

HQ COUNTRY:

Turkey

PRODUCT(S):

- › Forcepoint Next-Gen Firewall
- › Forcepoint Secure SD-WAN
- › Forcepoint Advanced Malware Detection

Transitioning from End of Life to Next-Generation

Burger King, the leading QSR brand in Turkey operating over 650 restaurants since 1995, has experienced rapid growth and development as a result of its focus on its consumers and its vertically integrated business.

As its Wide Area Network (WAN) approached the end of its life-cycle, Burger King sought a new approach of managing its sprawling network. Burger King worked closely with its partner, ATP, to identify the best fit.

“Combining the franchise and local networks to create one integrated network was a top priority,” Bülent Cengiz, Senior Manager at ATP, said. “We also wanted all connections on one landline so that we could provide greater resiliency for each restaurant.”

A comprehensive list of features and capabilities of nearly every Software-Defined Wide Area Network (SD-WAN) vendor on the market were evaluated. The list included.

- Granular analysis and visibility of network activity.
- Zero-touch deployment via cloud.
- Centralized management of policies.
- IPSec termination for massive networks and traffic prioritization.
- BGP dynamic routing protocols with extensive networks with over 1,000 network points.
- Automatic failover.
- Load shedding, balancing and redundancy.
- Ease of use for administrative interface.
- Built-in firewall and cloud security capabilities.
- Minimum packet loss.
- Accommodate multiple connection types.

Making the Smart Decision

Burger King and ATP underwent a rigorous comparison process that included a PoC (Proof of Concept) and feature comparisons for every top vendor in the marketplace.

“We awarded points for both the criticality and the level of importance the feature or capability held for us,” Cengiz said. “Each line item received a score out of five for all vendors, giving us the opportunity to grade them equally.”

Forcepoint Next-Generation Firewall (NGFW) with SD-WAN came out ahead of all other vendors with a 91% rating, and an average score of 4.5 out of 5 for all categories. The results demonstrated that Forcepoint was the smart decision for Cengiz and the team.

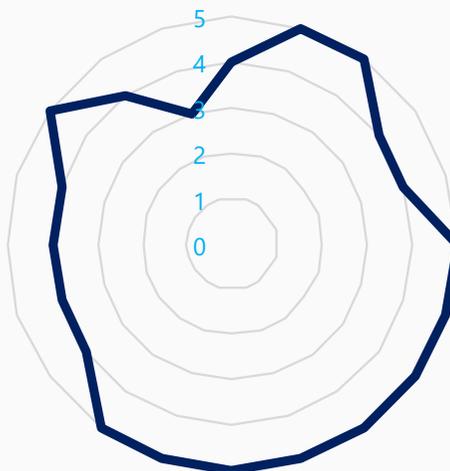


FIGURE 1: FORCEPOINT NEXT-GENERATION FIREWALL (NGFW) EVALUATION GRAPH



Challenge

- › Replacing existing WAN appliances of a rapidly developing customer.
- › Centralizing the IT management of over 1,000 network points with on NGFW SD-WAN policy.
- › Combining existing LTE and xDSL lines to manage business critical applications on branch sites.
- › Reducing downtime to prevent lost opportunity costs.

On top of requesting improvement in its network security, Burger King was in urgent need of an enterprise level antivirus or malware solution. Integrated Advanced Malware Detection (AMD) provided the company the protection it required to better prevent cyberattacks.

Burger King and ATP subsequently worked together to deploy over 1,300 N51LTE at each individual site. Once delivered to the restaurants, plugging in the device was the only installation requirement which needed to be performed by the on-site staff – all achieved without any technical assistance. Following the simple installation, Cengiz and his team remotely configured the device using the cloud to deliver pre-defined policies.

Burger King also deployed four 3301 NGFW appliances and one 2105 NGFW appliance at Data Center's as a Hub site during the process.

Gaining Immediate Benefits

Burger King was able to gain immediate benefits with its Forcepoint investment. It integrated its 800+ restaurant networks and 100+ franchise networks, allowing ATP to manage all network policies centrally.

With automatic failover and load sharing, Burger King was able to privatize the network and prevent unwanted traffic from interfering with connection speeds. Furthermore, greater resiliency provided more reliable network access for payment systems.

“Reliable communication from one restaurant to all related systems ensured that the network didn't impact operations and meant downtime and loss of revenue was far less likely,” Cengiz said.

Even a single outage in the Quick Service Restaurant industry has serious financial implications.

A failed credit card machine, an interruption in the mobile order system, or the loss of takeaway and delivery services can cost a restaurant direct income due to lost opportunities. This loss increases incrementally during rush hours. Moreover, these problems affect customer experience and loyalty, which may have negative consequences on the brand on the long-term.

Burger King not only managed to reduce missed opportunities but also gained better protection from cybersecurity vulnerabilities in restaurants. AMD safeguarded restaurants from crippling ransomware attacks and URL filtering blocked connections to known bad websites.

Ultimately, the project increased operational productivity, showcasing the true benefits of next-generation network security capabilities. With the solutions in place, Burger King continues to scale its deployment to well over 1,000 locations in Turkey.

Approach

- › Initially deploy 867 N51LTE appliances and scale to over 1,000.
- › Deploy four 3301 NGFW appliances, one 2105 NGFW appliance.
- › Combine franchise and local networks into one network.
- › URL Filtering to block connections to bad websites.
- › AMD to prevent unknown attacks.

Results

- › Zero-touch cloud deployment of firewalls.
- › Centralized management of firewalls for all locations.
- › Secure connectivity from restaurants to HQs.
- › Direct tangible savings on OPEX and CAPEX.
- › Reduction of downtime to prevent lost opportunity costs.