India-based Retailer Centralizes Network Security by Utilizing Enterprise Threat Protector

The Situation

A prominent furniture and home goods retailer headquartered in India has multiple offices, storefronts, and warehouses located throughout the country. The company partners with both local businesses and large manufacturers to offer a wide range of products to their customers. They sell products through their online retail site, app, and stores, and also host live events like henna workshops and cooking classes at their stores. Along with growing the business, the company also prioritizes corporate social responsibility, employee satisfaction, and sustaining a culture of innovation.

The Challenge and Goals

With so many different initiatives both on and offline, the company's CTO wanted to bolster the company's network security posture. In particular, he was intent on increasing Internet traffic protection, and creating and managing a company-wide and in-store acceptable use policy (AUP). The AUP needed to transparently outline what is allowable, taking into consideration the type of business they are, the diversity of users they have in the offices and warehouses, and the type of patrons they serve at their family-friendly retail locations. It was also essential to provide differing degrees of access dependent on the users (e.g., whether a user is accessing the corporate or guest network, which content types are being utilized, and the length of session time required for connectivity). Therefore, they required a policy that acts as a calibrated and adjustable filter versus a blunt, across-the-board censor. This policy, and the service that supports it, needed to be dynamic, agile, and easily updated in real time to react to Internet trends, emerging threats, and evolving user needs. Finally, it needed to be an easy-to-install, simple-to-manage, cloud-based solution with no hardware or software installation necessary. Since there are so many different locations between the retail stores, warehouses, and corporate offices, simplicity and centralization of policy management were key.

COMPANY
Retailer based in India

INDUSTRY
Retail

SOLUTIONS
Enterprise Threat Protector

KEY IMPACTS
- Protect and defend all locations with a centrally managed policy

- Proactively mitigate evolving Internet threats

- Implement a company-wide acceptable use policy across all corporate and retail locations

Why Enterprise Threat Protector

The CTO met with Akamai after hearing about Enterprise Threat Protector. Akamai immediately enrolled the company in a trial, and the CTO was able to turn on the service same-day. While immediately interested by the ease of configuration, he was even more impressed when the service detected and mitigated targeted threats on the network, including both malware and CnC traffic.

All configuration and ongoing management of Enterprise Threat Protector is done through Akamai's cloud-based Luna portal, so management can be handled from any location at any time, which was a key requirement for the CTO. Additionally, policy management is quick and easy; changes can be pushed out in minutes to ensure all locations and employees are protected.

Most exciting to the CTO was the real-time dashboard that comes standard with Enterprise Threat Protector and provides an overview of DNS traffic, threat events, and AUP activities. If he requires detailed information on any activity, it can be viewed through individual dashboard elements.