Claro
Enterprise Solutions

Evolve Together

Use Case

Perimeter Security for Small and Medium Businesses

Cost-effective network protection to enable business focus. Perimeter **Security** is a justified and affordable investment that allows business owners and IT teams to **protect sensitive data**.

Challenge

Security breaches that impact major corporations make the headlines. But the consequences for small and medium businesses can be equally serious and, relatively speaking, just as costly. Kaspersky Labs estimates that, *in the first quarter of 2018, the average cost of a single cyber incident for a small and medium business was approximately $120K*.

Moreover, a cyber-security breach almost always damages a business' reputation – one of its most valuable and fragile assets – and frequently results in lost customers, partners and employees, as well as tainted relationships with stakeholders.

Despite the high stakes, many businesses fail to take the measures necessary to reduce security risk. Smaller enterprises in particular often lack resources and expertise. And because they believe they're too small to be a target, they tend to be less vigilant. As a result, they are slower to identify and respond to attacks. But the fact is that smaller organizations can have complex network environments requiring multiple firewalls and security appliances, as well as an active Security Operations Center to monitor for potential threats.

> **"THE AVERAGE COST OF A SINGLE CYBER INCIDENT FOR A SMALL AND MEDIUM BUSINESS WAS APPROXIMATELY $120K."**

Solution

Our Perimeter Security solution allows businesses to focus on strategic activities while maintaining an enterprise-grade security posture. Two tiers of service are available: Firewall + VPN comprises on-premise firewall and Virtual Private Network (VPN), while Full Unified Threat Management (UTM) adds Application Control, Web Filtering and Intrusion Prevention System (IPS).

Supported 24x7 by experienced U.S. - and LatAm-based cyber analysts, Perimeter Security is a cost-effective way for small and medium businesses to protect their networks.

Other features include:

- 24/7 proactive monitoring for network and security-related incidents
- Basic to comprehensive security features
- A web portal that provides full visibility and management of your environment
- Dashboards and on-demand report generation
- Ability to integrate with enterprise-wide solutions that comply with federal cyber security requirements, as well as state regulations such as the *California Notice of Security Breach Act*

> **"PERIMETER SECURITY BY CES IS A COST-EFFECTIVE WAY FOR SMALL AND MEDIUM BUSINESSES TO PROTECT THEIR NETWORKS."**

Benefits

An effective Perimeter Security solution can improve a business' security posture by providing access to state-of-the-art Security Operation Centers, as well as enable migration from Capex to Opex without a hefty investment in infrastructure. Additional benefits include full control over branch connections and devices, along with agility and a pay-as-you-grow adaptability to integrate new users and functionalities.

Relative to the cost and risk of compromised security, Perimeter Security is a justified and affordable investment that allows business owners and IT teams to protect sensitive data, as well as avoid criminal investigations or identity theft prevention services down the road.

To stay competitive, you need to focus on your core business operations. At the same time, you need to stay on top of the ever-evolving world of cyber threats and proactively address cyber security issues before they damage your business.

"BENEFITS INCLUDE FULL CONTROL OVER BRANCH CONNECTIONS AND DEVICES, ALONG WITH AGILITY AND A PAY-AS-YOU-GROW ADAPTABILITY TO INTEGRATE NEW USERS AND FUNCTIONALITIES."