Managed Perimeter Security

Help reduce cyber threats, enhance customer service, and boost productivity with customizable layers of security that integrate 24/7 SOC monitoring, next-generation firewall, scalable Unified Threat Management (UTM), wireless failover, and more with Managed Perimeter Security.

Challenge

Security breaches that impact major corporations make the headlines. But the consequences for medium businesses can be equally serious and just as costly, especially since the average cost of a ransomware attack on an organization is $133,000.

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. Mid-size enterprises in particular often lack resources and expertise. And because they believe they're not large enough 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 mid-size 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 ransomware attack on an organization is $133,000.

The 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 US- and nearshore-based cyber analysts, Perimeter Security by CES 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 visibility 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

Managed Perimeter Security by CES is a cost-effective way for 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, Managed 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 and identity theft as a result of intrusions and cyberattacks 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.**

info@usclaro.com

Managed Perimeter Security

833-992-5276

Claro
Enterprise Solutions