5. An Effective Solution for SMB Security

Eager for security solutions without complexity and without the need to invest large amounts of resources in both time and money, many small businesses are turning to service providers for their cybersecurity needs. Service providers are in a unique position in the market because they can touch all network traffic in and out of increasingly complex SMB environments, on fixed and mobile, ensuring that workers' devices stay safe, whether at the office, home or on the road.

Such security services can include:

- Threat protection against phishing, malware, and viruses
- Content filtering of inappropriate internet content
- Network Firewall functionality to prevent unwanted connections and communication

Threat Protection:

Viruses, ransomware, phishing, crypto-jacking, and spyware are among the many threats businesses face every day. Network-based threat protection can keep the small business safe against all kinds of malware and online threats. These threats can cause major disruption to business operations, financial loss, compromise customer data, and damage the company's reputation. The security protection services would:

- Protect all on-premises PCs and devices instantly against malicious sites
- Check every website request for threats
- Offer Zero-touch deployment delivers protection via the network
- Not require IT expertise or management
- Provide reports of security level and threats blocked
- Automatically learn and protect against new attacks

Content Filtering:

Internet connectivity is vital to any business, but it can also seriously damage productivity. Employees can be easily distracted and waste time and network bandwidth. Employees and the business itself can be protected by having access to inappropriate and offensive content automatically limited or blocked. Content filtering services that can be defined by the business owner would:

- Restrict content access by blocking employees from visiting offensive or inappropriate websites that damage productivity and put the company at risk. It would filter requests from all PCs and devices according to the categories selected (i.e. gambling, pornography, ecommerce, social media)
- Increase productivity and reduce risk of inappropriate behavior
- Block or allow specific sites, listing websites that the business wants to always block or allow, that override the category definitions. For example, allow specific ecommerce sites used for business procurements.
- Provide notifications when an employee attempts to access restricted content

Network Firewall:

A Network Firewall service gives small businesses additional visibility and control over their Internet traffic, complementing the threat protection and content filtering services. These services should include:

- Rules based on source, destination, service, and action.
- Pre-configured rules for typical use cases
- A GUI suitable for small businesses without firewall expertise, including wizard-driven rule creation

6. Conclusion

SMBs do not have the resources to adequately secure their networks from the increasing wave of cybercrime. To be effective, there should be 24/7 protection, and this is beyond the reach of all but the largest companies. Cybercriminals understand this concept, which is why they target the SMBs on a constant basis with phishing, malware, and ransomware. The most effective way for these smaller businesses to protect their data assets is through the connection to the internet as provided by their communications service provider. CSPs around the world have started offering Security as a Service to small and medium-sized businesses, as a flexible and affordable solution that does not require cybersecurity expertise. This is the least expensive, most comprehensive and expeditious way for SMBs to get protection against the increased cybercriminal activities and continue to focus on their core business.