avast business

GUIDE

6 Reasons Why Security Appliances Are Failing the SMB

avast business

Introduction

A decade ago it was much easier for MSPs to protect their SMB customers from cyber threats using UTMs and Security Appliances. With less advanced threats, most small and medium business (SMB) offices were protected with a combination of antivirus and office-based firewalls. In 2007, the Unified Threat Management (UTM) appliance was introduced as an advanced firewall with additional all-in-one security features. These UTM appliances were designed to help SMBs protect their business office perimeter at an affordable price. Over time, UTMs added web content filtering layers to protect endpoints as well as servers, and their data, against web-based threats. Shortly after UTMs came out, another new appliance called Secure Web Gateway (SWG) was born. SWGs were stand-alone appliances specifically designed to protect a business from web threats.

Over the years, the UTM and SWG appliance industries have grown into what is today a $4.9 billion dollar a year business servicing the millions of small to medium businesses that lack the security experts and larger budgets available in the enterprise space.

SMB security appliance salespeople have made millions in commission selling UTM and SWG appliances, hot spares, upgrades and multi-year maintenance contracts for appliances. These appliances filled a need 10 years ago, but they haven't kept up with changes in how people work and how data needs to be protected.

Unfortunately, most SMB owners are unaware that the on-premise SMB appliance model has inherent security holes that can result in a breach, which could mean a disaster for your business. This paper uncovers the most common reasons that UTMs and security appliances are failing MSPs, and their SMB customers.

Contents

Reason #1: Appliances only protect some of the people, some of the time.

The days when employees worked in an office from 9 to 5 are all but over. The widespread availability of Wi-Fi has enabled workers to be on the move outside the traditional office perimeter. More and more employees are working from home offices, airports, coffee shops, hotels – really anywhere they have a wireless connection. In addition to employees, vendors, IT technicians, contractors, and others have access, often on weekends and at odd hours of the day. Traditional appliances only protect the declining number of fixed servers and workstations that reside behind the office perimeter. Laptops, personal (BYOD) phones, other tablet devices that move freely back and forth between the home and corporate networks aren't protected and often carry threat payloads.

Another trend along with increased mobility is the move to gradually replace large central offices in favor of multiple, smaller regional or branch offices. To connect and secure these offices, IT often employs a mix of MPLS (Multiprotocol Label Switching) leased lines, VPN concentrators, or duplicate sets of security appliances for each location. In doing so, branch office security becomes inherently costly, inefficient, and complex. Amid the confusion and hassle, many workers connect directly to the internet, bypassing the office network security. When they do, most have ZERO protection beyond antivirus security.

As an IT Service Provider, how are you protecting employees outside the office walls?

Reason #2: Appliances only protect some of your data.

The old days when the central office contained all the company data are over. The last 10 years have seen a huge shift from on-premise server and central office data rooms to the cloud-based public and privately hosted virtual servers and virtual data centers. The last 10 years have also seen rapid adoption by SMBs of third-party cloud applications, like Office 365, Salesforce, Box, and hundreds of others.

This means that company data is now scattered across multiple servers and cloud data centers. New 5G technologies will continue to encourage and accelerate the already rapid shift to distributed, cloud-based data centers.

In most companies today, the on-premise appliance now only protects a fraction of the company data that used to reside within the office perimeter.

As an IT Service Provider, how are you protecting your clients' data outside the office walls?

Reason #3: SMB appliances do not provide enterprise-grade protection.

While nearly all UTMs and SWGs advertise an SSL / TLS decryption feature, they're most often turned off because they're frequently undersized to meet budget requirements. In fact, according to Gartner, 90% of UTMs have SSL web inspection feature turned off due to latency issues and/or SSL certificate error issues. This leaves a gaping security hole, leaving the network near totally exposed, since the vast majority of business traffic (including security threats) are now encrypted!

Without the SSL / TLS inspection features turned on, every other security feature on the appliance means absolutely nothing! With SSL and the many other configuration options, most appliances are incorrectly configured in the field. Even if correctly set up, they require security experts with rare skillsets for constant adjustment and certificate updates to stay current and work most effectively with other network devices.

Without the SSL / TLS inspection features turned on, every other security feature on the security appliance means absolutely nothing!

Reason #4: SMB appliances don't have the latest security lists.

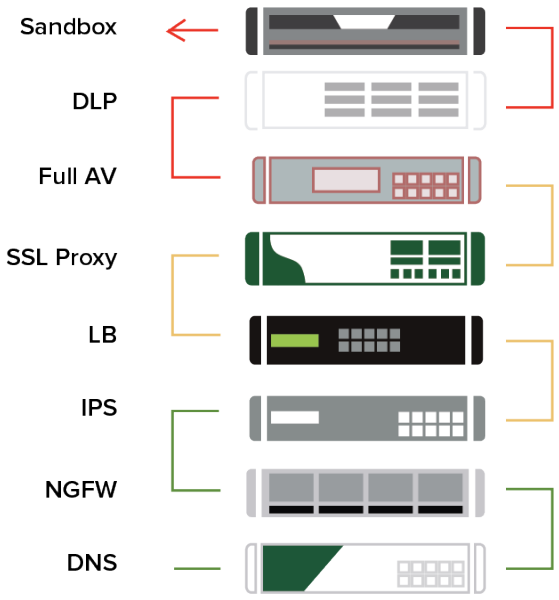
Defense against advanced threats should be as good for an SMB as it is for an enterprise, just on a smaller, more affordable scale. According to Small Business Trends, SMBs are increasingly targeted by hackers with **43% of cybersecurity attacks targeting small business.**

In addition, **new threat variants appear at an astonishing rate of 125,000 per day.** Unfortunately, most on-premise appliances have definition files downloaded infrequently and allow these new variants into the network before the definition lists are updated.

With thousands of new threats daily, IT Service Providers need cloud based gateways to provide assurance that all customers are protected by the latest lists.

Reason #5: “All in One” UTM appliances really aren't all you need.

“All in One” UTM appliances really aren't all you need. While UTMs are often marketed as “all-in-one” appliances, they don’t contain the layers of security required to protect small and medium-sized businesses. UTMs pack several layers of security into one box, but they often take shortcuts on features, functions, and sizes of definition files. Depending on the manufacturer, most UTMs will not offer integrated email security, antivirus endpoint security, patch management, and identity or password management – all of which are key components of a comprehensive layered security strategy for SMBs. By contrast, to eliminate security gaps, the typical enterprise business will have multiple, expensive boxes to protect each office location. Enterprise IT staff will normally install point solution appliances as opposed to an all-in-one UTM. In effect, these boxes are high-powered computers that specialize and excel in a particular layer of security.



Finally, legacy appliances UTMs and SWGs often can’t keep up with employee growth and additions of new bandwidth, restricting productivity and security. SMBs typically stick to a 3 to 5 year budget cycle and will risk their security and sacrifice productivity in order to wait for the next opportunity to purchase.

Did you know?

Defense in Depth, a term borrowed from the military, is a strategy using multiple security measures to protect the integrity of information. This way of thinking is used to cover all angles of business security - intentionally being redundant when necessary. If one line of defense is compromised, additional layers of defense are in place to ensure that threats don't slip through the cracks. This method addresses the security vulnerabilities that inevitably exist in technology, personnel, and operations within a network.

Today's cyberthreats are evolving and growing rapidly. Defense in depth is a solid, comprehensive approach to utilizing a combination of advanced security tools to protect critical data and block threats before they reach endpoints.

LEARN MORE ABOUT DEFENSE IN DEPTH AND LAYERED SECURITY

Reason #6: Appliances have several hidden costs.

There is a certain attractiveness to a plug-and-play appliance. However, the real truth is that SWG and UTM security appliances are only a small part of the total cost of ownership (TCO)

- Appliances normally have add-on support and maintenance contracts
- Appliance performance degrades and will most often need to be upgraded to a higher model when:
  - SSL inspection is turned on.
  - Increasingly cheaper bandwidth is added, only to find out that the UTM becomes the bottleneck.
  - More employees and/or locations are added.
- Appliances are single points of failure. If they break, businesses either need hot-spare backups or expensive "High Availability" contracts to reduce company downtime.
- Appliances require on-site IT experts to set up and perform firmware and software upgrades on a regular basis. A severe shortage of IT and security experts in SMB markets continue to drive the costs higher.
- Branch offices either need completely new sets of appliances or expensive MPLS leased lines to backhaul traffic through to the central office and back out to the internet.
- Appliances require secure computer rooms with HVAC, racks, battery backup and electricity.

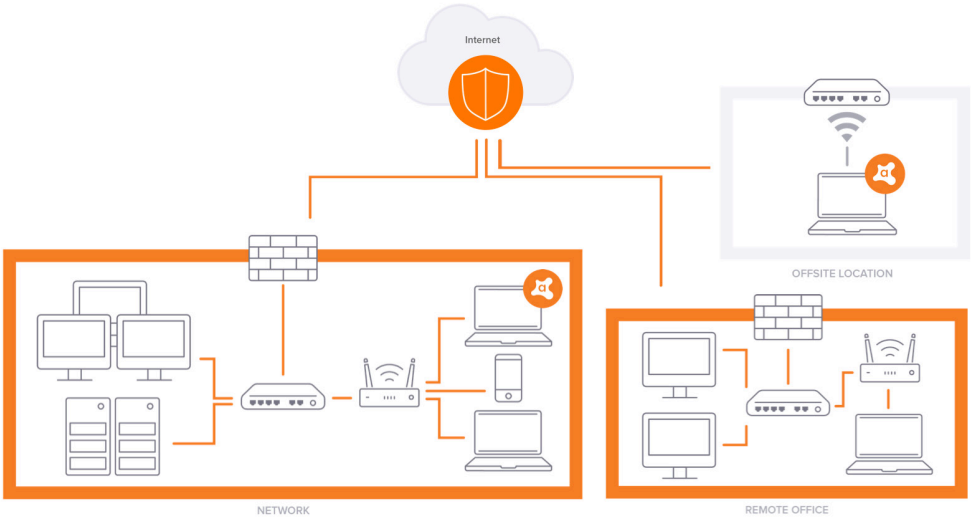
All these factors lead to increased operational costs for Managed Service Providers, without adding any extra benefits to SMBs.

All of these costs are minor compared to the ultimate cost: losing your business due to inadequate security!

Security Solutions for Today's SMBs

It is clear that the appliance-based security models of the past – including the traditional Castle and Moat and Hub and Spoke models – are dying out. Advanced, more frequent threats combined with the unstoppable shift toward worker mobility, cloud-based servers, and cloud applications, now require that modern-day security protect beyond the four walls of the office perimeter.

In the end, legacy appliance-based models are not as inexpensive as they seem – and can cost your business in the event of a serious breach.



Security experts agree that the Internet has become the new office perimeter and must be defended in a new, comprehensive way. Fortunately, there is an emerging software-defined security (SDSec) model that addresses the security gaps left by traditional methods in a more logical, efficient, and effective way.

At Avast Business, we know that cybersecurity must be quicker, smarter, and more reliable than ever. We provide powerful, affordable security solutions for SMBs to protect businesses from web threats.

Schedule time with a Business Security Expert to get answers to your specific questions along with a personalized walk-through of Avast's suite of SMB-centric security solutions.

REQUEST A DEMO

About Avast Business

Avast Business provides integrated, enterprise-grade endpoint and network security solutions for SMBs and IT service providers Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. The result is superior protection that businesses can count on. For more information about our managed services and cybersecurity solutions, visit **www.avast.com/business**.