

An In-depth Analysis of SMB vs. Enterprise Security

Introduction

One of the most commonly used acronyms in business today is “SMB”. Yet, most vendors who service both Small and Mid-sized Businesses and Enterprises differentiate the two based either on the company’s annual revenue or by its number of employees. However, when it comes to IT security, neither of these measurements is very appropriate. Rather than attempting to label them, these vendors should spend their time and energy assessing the security needs and the availability of resources for each, so they can provide each of them with the security solution that best fits their specific needs.

When it comes to securing the company’s network assets, SMBs and Enterprises require the same security coverage – but the SMB’s level of expertise, availability of personnel, and available budget are typically in sharp contrast to those of the enterprise. Security vendors like to highlight “enterprise-class” as a selling feature for their SMB customers, yet what they actually provide, lacks in coverage, performance, and feature set compared to their enterprise offerings.

Same Security Needs

Because network threats are indiscriminately propagated via the Internet, they do not differentiate between SMBs and enterprises. Therefore, regardless of its size, any Internet-connected company is going to be faced with the same threats. Businesses of all sizes will face threats carried via inbound and outbound HTTP traffic. Similarly, nearly all businesses today employ email for daily communications, both inside and outside the company. Therefore, they will be challenged by the range and ever-growing number of email-borne threats. If they host their own email or Web site, additional security measures must be in place to protect the email and Web servers.

The same can be said for the company’s application servers, databases, or any other components of the network infrastructure. Regardless of size, all businesses – SMBs and enterprises, alike – are confronted by threats to these vital assets. The only significant difference between them is their scale of operations.

Fundamentally Different Resources

The main point of differentiation between an SMB and an enterprise has to do with the company’s human and financial resources. While SMBs have most of the same overarching security needs as their enterprise counterparts, they possess significantly fewer resources – with far less bandwidth – to effectively deal with those needs.

An Enterprise will have a full-blown IT Security department to manage the firm’s on-going security needs. This means deploying complex systems to effectively secure all of the firm’s network assets at each of its locations. It also means keeping current with the rapidly changing threat landscape and modifying the company’s security policies, as necessary, in response to new threats. Most importantly, it means keeping their finger on the pulse of the company’s network traffic, including analyzing log files to determine if there are any unusual traffic patterns. An Enterprise will have the financial wherewithal to purchase these systems, and the personnel to effectively run them.

Conversely, an SMB may or may not have a full-time IT department – and almost certainly will not have a single full-time dedicated security expert. Instead, many will have a single employee dedicated for all the business IT needs including security. Others simply outsource all their IT needs.

SMBs normally lack the time and financial resources required to implement a complex enterprise-level security solution. While a considerable price tag and a six-month deployment may seem normal to a large enterprise, most SMBs are unwilling or unable to commit to such a high level of expenditure, and they require virtually immediate results.

Different Security Decisions

Faced with these resource challenges, SMBs will naturally make some difficult security decisions. Whereas their enterprise counterparts have the capability to spend exorbitant amounts of time and money deploying a multi-layered, proactive, detailed security system to achieve maximum efficacy, SMBs must assess what they can afford, as well as what they will have the ability to maintain.

The most technically exquisite system in the world is useless to an SMB if it requires significant amounts of manual intervention on a regular basis. With only a portion of one or more IT staffers’ time dedicated to security, a complex system that provides a plethora of information such as SMTP and HTTP traffic anomalies in log files is relatively useless, since the IT staff lacks the time to review those logs. Similarly, a complex system that requires months to fully implement does no good to an SMB that needs the security solution up and running in days – with limited IT staff.

Between these seemingly insurmountable challenges, coupled with their notably lower level of security awareness, many SMBs will pick and choose their security solutions based on cost, simplicity, and automation, rather than on robustness and efficacy.

Current Security Offerings for SMB

Most security vendors that have traditionally served the enterprise market still fail to properly address the IT security needs of the SMB market. SMB offerings from these security vendors possess fewer and less powerful hardware components than their enterprise counterparts, and will therefore suffer from slower performance. Most of these vendors simply strip features and capabilities from their enterprise products, in an attempt to create an offering for the SMB market at a reduced price. For example, an enterprise URL filtering product containing a black list with 50 million addresses may be cut down to only 5 million addresses for the SMB version. Similarly, an enterprise anti-malware engine containing 500,000 malware signatures may only contain 3,000 signatures in the SMB version – just enough to cover the “wildlist”, the official list used by the security industry of viruses spreading in the real world. Or, an enterprise-level email filtering product with the capability to catch spam and other malware based on their content or appearance may be reduced to a dynamic black list of known spam domains for the SMB version.

Some security vendors even dramatically reduce the power and functionality of their product. While the enterprise version of a security system may be comprised of best-of-breed software and technology, the SMB product may utilize open source security software. Features may also be stripped out of the SMB version, making the product less robust or less user friendly. Most importantly, all of these reductions create a significant security exposure for SMBs, making their networks inherently less safe than those of their enterprise counterparts.

Small and Mid-sized Businesses Needs

Email and Web access together represent the majority of business-critical applications used by SMBs. Organizations must look for several attributes when choosing a security system that encompasses email.

Comprehensive protection for businesses of all sizes

Small and mid-sized businesses face the same threats and challenges from Internet base threats as large enterprises. Businesses should look for security companies that have a worldwide presence and that scan Web and email content day and night to identify new threats. Once, organizations used to look for “day zero” protection; or protection from email threats on the first day they were identified. Now, organizations of all sizes demand “zero hour” protection.

High-performance solution

In order to be effective, Web and email security scanning must be fast. Many Internet gateway protection solutions take a long time to process incoming and outgoing communications, bogging down network communication response times and frustrating users.

Business continuity

An effective Internet gateway security solution must not only guard against identified threats, it must also protect against threats that have yet to be identified by malware and spam laboratories.

Intuitive administration

Small and mid-sized businesses do not have the IT resources to spend on complicated installation, maintaining several security software packages, cumbersome upgrades, or user licensing issues. The solution must be user friendly for both deployment and maintenance. The solution must also include intuitive web GUI for configuration and graphical statistical summaries .

Conclusion

When it comes to securing the company’s network assets, SMBs and Enterprises have the same security needs, but they possess vastly different levels of expertise, as well as human and financial resources. As such, “Enterprise-class” is a wonderful thing, so long as it refers to the power and comprehensive nature of the protection. However, this term should not mean that the product is a watered-down version of an Enterprise product. Instead, SMB security solutions should be built from the ground up, specifically to meet the unique needs of the SMB. Most importantly, the SMB product must provide the same level of security protection that is available in the Enterprise version.

NETGEAR® ProSecure™ STM Web and Email Threat Management Appliance Solution

The ProSecure STM Appliance uses a unique technology that detects and blocks outbreaks based on their rapid and wide distribution behavior. This approach can detect spam and malware outbreaks as soon as they emerge, and block all associated messages in real time.

The ProSecure STM Appliance features patent pending Stream Scanning Technology that is designed to scan data streams as they enter the network. With Stream Scanning Technology, the NETGEAR STM is able to process large amounts of data in real-time, using a single scan to identify spam, malware, security breaches, or unnecessary applications. This ensures that users on the network receive their email and Web content clean and without delay.

The ProSecure STM Appliance uses a proactive behavioral defense system that eliminates the gap between a vulnerability being exploited and the fix. The NETGEAR solution uses forensic analysis to identify suspicious characteristics of incoming and outgoing network traffic, and neutralizes them until they can be examined more closely.

NETGEAR, the NETGEAR logo, Connect with Innovation and ProSecure are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2009 NETGEAR, Inc. All rights reserved.