FROST & SULLIVAN

Avoiding the Acronym Red Herring:
Navigating Market Complexity to Fulfill Security Requirements

A Frost & Sullivan White Paper

Chris Rodriguez, Senior Industry Analyst, Information & Network Security

INTRODUCTION

The network security industry is in a constant state of evolution, perpetually responding to new technologies and emerging threats. For every newly discovered cyber threat attack vector, yet another security product is developed to address the shortcomings of existing tools. The process is iterative, and the need for these security technologies is cumulative. Each new product developed is added to the security lexicon but rarely, if ever, are existing tools retired. This evolutionary process has been accelerated in recent years, as new products have emerged to address challenges such as mobile devices, cloud services, and advanced malware.

The result is a crowded marketplace, characterized by a multitude of security tools and their concomitant marketing messages, terminology, and acronyms. The security industry is now bursting with the complexity created by a multitude of individual products, from intrusion prevention systems (IPS) and Web application firewalls (WAF) to newer technologies such as sandbox analysis and Endpoint Detection and Response (EDR) solutions.

For most enterprise organizations, navigating this complex and confusing market landscape is a challenge that inhibits security. Yet enterprises are able to invest time researching new threats, assessing their own unique organizational risk, evaluating available products, and developing an expert understanding of each new product. Small and medium-sized businesses (SMBs) do not have this luxury. SMBs are particularly challenged given more extreme time and resource constraints. Distributed enterprises face similar challenges, as they are often organized as a collection of small storefronts and branch offices or as a central office tasked with managing a large number of offices. Either option requires the individual locations to operate with a degree of autonomy.

Security vendors contribute to the confusion further, developing and promoting eye-catching product names and acronyms. For example, as functionality has been consolidated into stateful firewall platforms such as intrusion prevention, application control, and Web content security, product names and acronyms such as Next-generation Firewall (NGFW) or Unified Threat Management (UTM) have been introduced to the security lexicon, which added confusion rather than clarity. But, ultimately, whether the platform that these tools are deployed on is a NGFW or a UTM is a red herring.

A refocused, strategic approach to security is required to meet the specific needs of small businesses, as well as businesses that are structured similarly or face similar challenges, such as small enterprises and distributed enterprises. This approach should be pragmatic and streamlined, and focused on achieving broad security goals without significant sacrifices in security efficacy. Frost & Sullivan provides the following recommendations as a roadmap for small businesses to achieve effective security.

MODERNIZING NETWORK SECURITY IN A SMALL BUSINESS CONTEXT

The enterprise and SMB are similar in the threats that they face, yet SMBs face additional constraints that enterprises may not. For example, simplicity, usability and manageability may be luxuries for many enterprises, while such attributes are necessities to SMBs. SMBs require many of the same security technologies, but tailored for their unique needs. SMBs must begin the security process by first identifying these requirements.

Security Goals in Small Businesses are Defined in Context of Real-world Constraints

Small businesses are unique; they are NOT small enterprises. The small business is characterized by limited resources, time, and expertise. Small businesses rarely have dedicated security staff and likely have only a handful of people (or one person) on the IT team. SMB customers cannot afford to be distracted by the ceaseless cycle of security product development, constantly researching, deploying, integrating, and tuning the latest security tools.

Distributed enterprises face similar issues as small businesses. A distributed enterprise is comprised of many different remote offices, branch offices, or storefronts—each of which may need localized security tools or may operate independently from main offices. Often, distributed organizations cannot afford dedicated IT or security teams for each branch office or storefront.

SMBs Require a Focus on Problem Solving

The security industry is overcrowded. SMBs simply cannot maintain an in-depth knowledge of every available solution in each individual category of security tools. Confusing market terminology and conflicting marketing messages further hinder market adoption. Each new product introduced to the market requires an accompanying "catchy" name that may or may not communicate the benefits of the solution and is often reduced to an even less helpful acronym. Furthermore, vendors may use specialized or modified terminology to promote their own product or vision for the market. Small businesses can no longer allow market complexities to derail their security strategies.

> *The small business must focus first and foremost on its specialty—the business that pays its bills.*

The small business must focus first and foremost on its specialty—the business that pays its bills. Security is, and will be, a distant secondary concern. Small businesses require all-in-one solutions that are easily deployed and affordable. The next generation of SMB security solutions should deliver effective, comprehensive security, instead of a mash-up of popular enterprise products. These solutions will prove beneficial for distributed enterprises and small enterprises as well.

ADVANCING FROM PRODUCTS TO SOLUTIONS

The security model is reactive: a new threat vector is discovered and new security tools are developed to address the issue. Then the process repeats. The new technologies are able to solve the specific security weaknesses that they were designed for, but are delivered as disparate point products that leave gaps in the overall security architecture for attackers to exploit. This model places too great a burden upon the customers, and is unsustainable for SMBs and distributed enterprises. Small businesses, and ultimately businesses of all sizes, must update their approach to security by seeking out complete solutions rather than point products.

Understanding Tools within a Complete Security Lifecycle Process Context

The current security model, though untenable, thrives because of the hope for a "magic pill"—the idea that the next product will solve every security issue. Yet, the reality is that each security technology is just one tool to aid in the greater effort to defend networks and data. Security products must be understood and evaluated in this limited but realistic context. An adjusted understanding of security products reveals that each new technology performs a vital but limited aspect of the overall security process.

Focus on the Objectives of Security and not Products

Security is an important goal that will require the use of specific products, but security products should not be conflated with a complete security strategy, which is outcome focused. True security requires a complete, virtuous cycle of prevention, detection, correlation, and response. These objectives are broken down as follows:

- **Prevention:** Prevent threats where possible; the goal of many traditional security technologies.
- **Detection:** Detect threats and breaches; the goal is to accept that breaches happen and to be prepared to minimize time from infection to detection.
- **Correlation:** Validate effects of different security tools so that no one tool can be fooled (trust but verify); the goal is to see the "bigger picture" and provide complete security. Correlation can not only illuminate breaches, but also reduce false alerts that may result from the detection of anomalous yet not malicious activity.
- **Response:** Remediate and "close the loop"; the goal is to take action based on the other three steps. Ideally, this will be automated where possible.

Ultimately, organizations of all types and sizes are best served by focusing on the outcome of improving cyber security through complete solutions that meet the key security objectives listed above. Security solutions should do more than generate alerts (prevent or detect). They should help to complete the security cycle by closing gaps and prioritizing security risks (correlate), and aiding customers in necessary remedial efforts (respond).

Solutions Provide Reduced Complexity

Many vendors bundle disparate security tools and services that aren't truly integrated. Benefits such as "one vendor, one bill" and pricing discounts are always welcome. However, this approach doesn't solve any security problems if it pushes the burden of making the security and network products work together back on the customer. In order to provide effective and complete security, SMBs and distributed enterprises should seek out solutions that seamlessly integrate new security technologies into existing processes.

FROST & SULLIVAN: THE LAST WORD

Whether the tool is an IPS, NGFW, UTM, Web filter, or malware sandbox, it is just one tool of many needed to secure businesses from the wide range of modern threats. SMBs cannot afford to waste time on confusing marketing messages and product names and concepts. Businesses, especially small businesses and distributed enterprises, must invest their limited time and resources into solutions that protect their networks completely and thoroughly, and with minimal disruption and effort—solutions that deliver enterprise-grade security without the accompanying costly sprawl of appliances. The focus is solutions, not products—outcomes, not technology.

Chris Rodriguez
Senior Industry Analyst – Information & Network Security
Frost & Sullivan
Chris.Rodriguez@frost.com

FROST & SULLIVAN

NEXT STEPS

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

- Visit our **Digital Transformation** web page.

- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY

331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

SAN ANTONIO

7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON

4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041