Understanding Unified Threat Management (UTM) and Next-Generation Firewalls (NGFWs): Advancing Network Defenses both Now and in the Future for Mid-Size Organizations

A Frost & Sullivan Analysis

Chris Rodriguez
Senior Industry Analyst, Information and Network Security

Sponsored by WatchGuard
INTRODUCTION

Next-Generation Firewall (NGFW) is an exciting concept in the network security industry that promises integration and consolidation of essential network perimeter protection technologies. However, there remains a high level of market confusion about what NGFW offers and many customers are surprised to discover that NGFW does not include important security capabilities.

At a minimum, NGFW functionality will include stateful firewall, application control, user-based controls, and an intrusion prevention system (IPS). By comparison, Unified Threat Management (UTM) solutions offer a comprehensive array of network security technologies that go far beyond NGFW functionality. UTM solutions provide stateful firewall, an intrusion prevention system (IPS), gateway antivirus, Web content security, email security, and data leakage prevention (DLP). Most importantly, UTM vendors have successfully updated their products to include NGFW functionality, such as application-aware and user-aware controls.

STATE OF THE UTM AND NGFW MARKET

NGFW Solves Security Weaknesses Inherent in Stateful Firewalls

The stateful firewall has been available for over a decade and provides essential security and network management functionality. It is used in almost every IT organization around the world. The NGFW was developed primarily to solve a glaring weakness in stateful firewalls. Stateful firewalls operate by inspecting a limited set of information collected from data packet headers. The limited data collected from packet headers is incomplete and does not provide sufficient context to detect threats that propagate through legitimate network traffic.

To address this limitation, NGFWs were designed to perform a more thorough inspection and provide additional contextual information about network traffic to support more sophisticated, multi-threaded, and adaptive security policies.

NGFW Offers New and Advanced Features that Enhance Customer Value

Part of the excitement around NGFW is the enhanced contextual data about network traffic, such as user identity and application type, that these solutions provide. Businesses can use the granular data collected by NGFWs to create advanced policies. Additionally, vendors continue to expand the data that can be used to create and enforce access policies such as location, time, and device type.

NGFW functionality allows businesses to create granular and effective security policies. For example, NGFW policies can enable marketing teams to pursue innovative strategies leveraging Facebook and Twitter, while blocking access to these applications in more sensitive departments such as finance.

Vendors Build Upon and Extend the Capabilities of NGFW

NGFW has proven to be a very compelling solution for organizations of all sizes and is an important component in the security puzzle. However, the initial definition of NGFW provides a limited set of functionality that may not protect against future malware and threats.

Leading UTM vendors continue to add new functionality to their solutions to protect against new threats and to support rapidly changing network technology requirements. In recent years, vendors have added advanced

---

1. Please note that the insights and opinions expressed in this assessment are those of Frost & Sullivan and have been developed through the Frost & Sullivan research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.
functionality in their products, such as advanced threat protection, Web application firewall (WAF), and distributed denial-of-service (DDoS) mitigation.

The addition of new or advanced security features in NGFW and UTM solutions delivers tangible business value that helps to justify customers’ investments and assures customers that their investments will adapt to future needs.

**Advanced Threats Require New Network Security Technologies**

Advanced malware such as Flame and Stuxnet demonstrate the rapidly evolving skill sets and tactics employed by threat actors. For example, the advanced malware called Flame included features such as a modular design and the ability to propagate over multiple infection vectors. Flame can record audio, Skype conversations, Bluetooth data, key strokes, and screen captures, and can even hide evidence of its operations.

Threat actors continue to demonstrate a high level of adaptation and innovation in developing new and sophisticated attack techniques. As a result, the ability to implement a robust information security architecture requires network security solutions that are flexible and that can expand to add new protection features and security technologies over time.

**WATCHGUARD’S POSITION IN THE MARKET**

WatchGuard is an established competitor in the network infrastructure security industry with a legacy of providing flexible products at compelling price points. The WatchGuard product strategy focuses on visibility, performance, and integration of best-of-breed technologies. These principles guided the company’s decision to offer its network security solutions as a modular platform.

The WatchGuard platform integrates best-of-breed security technologies from pure-play vendor partners such as Websense, Kaspersky, AVG, TrendMicro, and Sophos. This partner-centric strategy allows WatchGuard to offer best-of-breed protection and value to its customers with the flexibility to change partners and add functionality as necessary.

WatchGuard network security solutions are designed to work as an integrated unit but can also be deployed as point solutions if necessary for certain business segments, network environments, or other use cases. For example, high-end WatchGuard appliances can be deployed as pure-play NGFWs. The WatchGuard strategy addresses the growing customer need to implement best-of-breed security technologies with budgetary restrictions, time constrictions, and expertise limitations.

WatchGuard released its Dimension visibility and reporting tool in 2013. Dimension is offered as a “zero-install” virtual machine that can be deployed in customers’ public or private cloud environments. Dimension presents important security data to customers based on proprietary WatchGuard correlation engines, which identify pertinent security and performance issues. Dimension provides “one-click” instant reports, pre-defined audit reports, visualization tools such as dashboards and threat heat maps, and is “cloud-ready” and cloud vendor-agnostic.

WatchGuard was recognized as leading in multiple competitive categories in the 2014 Global Analysis of the UTM and NGFW Market research study by Frost & Sullivan, available here. WatchGuard’s performance in these categories is highlighted in Figure 1.
Figure 1 – Competitive Factors and Assessment, (WatchGuard) 2014

<table>
<thead>
<tr>
<th>Competitive Factor</th>
<th>Requirements</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management/Usability</strong></td>
<td>User interfaces should be intuitive, informative, and centrally managed</td>
<td>WatchGuard Dimension provides highly granular data in a graphical representation that lets customers pinpoint security gaps, optimize policies and network traffic, and offers “one-click” reporting.</td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td>Options and service bundles that map to customer requirements</td>
<td>WatchGuard appliances can support any of the security services that customers need to deploy. Customers can deploy a NGFW now and easily upgrade to partial or full security capabilities when needed.</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>Product line breadth and high ratio of product performance compared to cost</td>
<td>The WatchGuard product integrates best-of-breed solutions. Consolidation of leading security technologies in a single network appliance presents a more affordable solution compared to the cost of several disparate point products.</td>
</tr>
<tr>
<td><strong>Performance/Scalability</strong></td>
<td>Network performance with security functions enabled</td>
<td>Use of commercial hardware such as Intel Xeon processors allows WatchGuard to improve the packet processing performance of its appliances by multiple factors by using Intel’s Data Plane Development Kit (DPDK).</td>
</tr>
<tr>
<td><strong>Roadmap</strong></td>
<td>Product development plans, partnership strategies, mergers and acquisitions</td>
<td>WatchGuard plans significant improvements for future versions of its Fireware operating system, including running the firewall as a hypervisor. This separates the software from underlying hardware and provides a number of performance and flexibility advantages.</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan

STRATEGIC RECOMMENDATIONS

Ease of use and meaningful reporting will be increasingly important competitive factors as customers seek to maximize value from their investments by eliminating inefficient practices and mitigating business risk. Businesses should shortlist vendors that have demonstrated a commitment to ongoing product development in order to ensure that their investments are “future-proofed” against ever-changing technologies and emerging threats. Frost & Sullivan recommends that businesses consider the value and flexibility offered by WatchGuard network security solutions when updating their network protection architecture.
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