Defining, Evaluating, and Designing Best-in-Class Network Security
White Paper

Prepared for WatchGuard® Technologies, Inc. by Washburn Communications
Published: June 2012
Introduction
Network security intrusions and data theft incidents grab headlines almost daily. These breaches paralyze highly visible companies, such as Sony and Citigroup, and put the personal information and identity of millions of people into criminal hands. Similarly, notoriety-seeking hacktivists release sensitive information that embarrasses governments and threatens international diplomacy.

Organizations that are serious about protecting data, intellectual property (IP), and their reputation are increasingly demanding best-in-class, multilayered solutions. These solutions centralize security controls in a single device, improving the IT organization’s control and simplifying management of network security.

WatchGuard and its security service partners continue to rack up industry awards and recognition as well as routinely earning top rankings from independent testing agencies across many different network security categories. That’s why organizations of all sizes rely on WatchGuard solutions for comprehensive network protection, peace of mind, and value. Industry-leading feature sets and capabilities combine to make WatchGuard Extensible Threat Management (XTM) a best-in-class, next-generation network security platform:

- **Layered and complete.** Layers of protection cooperatively and dynamically detect, block, and report on malicious traffic while passing benign traffic through.
- **Flexible.** A modular architecture in WatchGuard XTM helps organizations stay on top of the evolving threat landscape, including spyware, spam, viruses, Trojans, web exploits, and blended threats.
- **Industry-leading specialty security services.** Unlike competitors in the multilayered security space, WatchGuard XTM incorporates specialized security services from proven industry leaders. This approach provides WatchGuard customers with a best-in-class solution for each protection layer that meets their organizations’ complex and changing security needs.
- **Integrated.** Integrated management of the entire security platform provides administrators with confident, efficient control of all functions, including partner-provided threat management software, in a single, unified interface.

Read on to understand why WatchGuard is “best-in-class by design.”

Security Challenges and Trends
The growth in IP networks and proliferation of new applications, devices, and web technologies in the workplace creates more potential vulnerabilities for IT networks. As we trend toward additional applications running in the cloud, even more network traffic will pass beyond the trusted LAN and outside the firewall. Assault vectors shift, and new threats spring up hourly from spyware, spam, viruses, Trojans, web exploits, and blended threats.

**The Web Is a Key Battleground**
The web is the vector through which malware propagates in most networks. With the web providing such a broad attack surface, social networking is a growing risk as organizations rely on social media. A Robert Half Technology survey of 1,400 CIOs showed that 51 percent of them permitted employees to use social media sites like Twitter and Facebook on the job as long as it’s for business purposes.¹

Social media is built around a culture of trust, yet social media sites lack the technical means to validate that people really are whom they say they are. The same is true of apps; there is only nominal validation, and social media users can put their computers and the organization’s network at risk. On some social networking sites, apps have access to profile information and the browser, essentially the same access as a “friend.” Many of these sites have various technical vulnerabilities:

- HTTP has no built-in security
- The complexity of web 2.0 applications can lead to imperfect code, which can open up social networking sites to SQL injection and cross-site scripting attacks.

Criminals target high-traffic sites. Facebook is the most visited site on the web, followed by YouTube. Unfortunately, criminals exploit user trust and induce people to visit malware sites, download applications that contain malware, or otherwise compromise the client computer and infect the network.

**Employee Productivity and Organizational Reputation Are at Stake**

Public-sector and private-sector organizations find that they need to go beyond security protection and consider workforce productivity solutions. Public-sector organizations need to stay accountable to constituents for how employees use publicly funded computing resources and their time. Both types of organizations desire to avoid scandals and ensure employee productivity. Increasingly, they rely on security services that restrict Internet and application usage to what is appropriate for the workplace.

**Delivering Multilayered Protection**

As shown in Figure 1, Info-Tech Research Group, a global leader in providing IT research and analysis, positioned WatchGuard as a market “Champion” in its Vendor Landscape: Unified Threat Management report. This clearly demonstrates the superiority of WatchGuard’s approach to best-in-class, defense-in-depth protection, which we’ll describe in the sections that follow.

![Figure 1. Info-Tech Research Group positions WatchGuard in its “Champion” category for multilayered security.](image)

---


Founded in 1996 as a supplier of firewall and VPN appliances, WatchGuard has evolved into a leader in providing reliable, easy-to-manage security appliances to thousands of organizations worldwide. The company’s award-winning XTM network security solutions combine firewall, VPN, and security services in a simple-to-use appliance to meet complex security needs. By managing one unified solution rather than multiple point solutions, IT administrators can spend less time and money securing the network and applying updates.

**Defense-in-Depth for Physical and Virtual Environments**

Today’s briskly evolving multi-faceted threat landscape means having a simple packet-filtering firewall isn’t enough. Organizations are increasingly demanding a multilayered approach to security services—one in which various security layers and services work cooperatively to dynamically detect, block, and report on malicious traffic while passing benign traffic through as efficiently as possible.

As shown in Figure 2, one way WatchGuard accomplishes next-generation, defense-in-depth security is by offering a complete and industry-best set of threat management solutions including, gateway antivirus, content and URL filtering, antispam, intrusion prevention, and application control.

Because new threats appear constantly, WatchGuard XTM is designed to protect against previously unrecognized threats, providing what is known as “zero-day” protection.

We call this layered approach defense-in-depth because it covers an organization at every potential level of network attack.

![Layered security in WatchGuard XTM provides defense-in-depth.](image)

Through deployment of a virtual appliance, WatchGuard also addresses the unique requirements of the most demanding virtual environments. WatchGuard XTMv applies the same best-in-class defense-in-depth capabilities of the XTM physical appliance to virtual environments.

**Challengers for Multilayered Security Supremacy**

Other multilayered security vendors claim what, at a glance, appears to be a comparable checklist of features and services. However, these vendors are largely security generalists who primarily develop each security layer in-house.
While a few competitors enlist partners for services that they do not develop themselves, companies taking this approach struggle to match WatchGuard’s effectiveness at seamlessly integrating the partner security service into the user interface (UI). If there is one interface for managing the appliance and a different interface for one of the security services, an already overburdened IT manager must learn and monitor yet one more tool to secure the network. This can lead to administrative burden and risk of potential security configuration error.

**Best-in-Class Security Services from WatchGuard**

Rather than become another security generalist trying to develop each discrete security technology with overstretched resources, WatchGuard has pioneered a different approach—one of leveraging the expertise and innovations of industry-leading specialists. These security technology specialists, who may have hundreds of employees focusing on a particular technology, offer best-in-class products in their respective areas of expertise, and we’ve incorporated their highly validated, industry-leading technologies into WatchGuard XTM. These partners, which include, among others, AVG, Websense, Commtouch, BroadWeb, and Kaspersky offer the following:

- Specialize in a very focused area of security
- Have many years of experience
- Maintain dedicated resources to retain their leadership position
- Have received industry accolades and awards
- Have been vetted as leaders in their respective specialties through evaluations that WatchGuard and third-party testers have conducted separately

![Figure 3: WatchGuard leverages the expertise of leading industry specialists. Competitors largely attempt to develop each technology in-house.](image)

**Stacking Up Superior Security, Layer-By-Layer**

Similar to assembling an all-star sports team consisting of the best players from a variety of teams, WatchGuard’s strategy enables us to offer a truly best-in-class security solution that covers many different aspects of security. At each layer, this translates into:

- Larger databases
- Richer features
• Higher accuracy
• Faster scanning
• Stronger detection
• Better protection than competitor offerings

Ultimately, this approach of incorporating best-in-class security services has ranked WatchGuard in the “Champion” (see Figure 1) position ahead of other multilayered network security solution providers.

XTM security subscriptions complement the built-in protection of the WatchGuard XTM firewall, boosting security in critical attack areas, including assaults from spyware, spam, viruses, Trojans, web exploits, and blended threats. Organizations can purchase only the WatchGuard XTM security services subscriptions that they need or buy the offerings as part of a bundle, which includes:

• WatchGuard Gateway AntiVirus and WatchGuard Reputation Enabled Defense
• WatchGuard WebBlocker URL Filtering
• WatchGuard spamBlocker
• WatchGuard Intrusion Prevention Service
• WatchGuard Application Control

Let’s take a closer look at WatchGuard XTM’s all-star team of best-in-class threat management services.

**WatchGuard Gateway AntiVirus**

WatchGuard Gateway AntiVirus, powered by AVG, scans web traffic using continually updated signatures to detect and block all types of malware. AVG AntiVirus is consistently a top performer in third-party antivirus tests and relies on a combination of traditional virus signatures and behavioral and heuristic analysis to detect malware. This combination of detection methods helps WatchGuard Gateway AntiVirus successfully identify and block viruses, Trojans, scareware, malware, and spyware.

**Leading Signature Database for Better Threat Coverage**

When it comes to onboard signature databases, the larger the database, the wider the net of protection. As shown in Figure 4, WatchGuard Gateway AntiVirus, powered by AVG, boasts considerably more onboard signatures than competing in-house solutions.

![Figure 4. WatchGuard AV Standard has 50,000 more signatures than the closest competitor. *WatchGuard extended edition is used for larger appliances, including XTM 8 series, XTM 1050, and XTM 2050.](image)
**Validated Best-in-Class by Leading Third-Party Testing Agencies**

Three independent testing agencies, which includes Virus Bulletin, AV Comparatives, and AV-test.org, gave their approval of AVG’s AntiVirus (see Figure 5). Among alternative providers of layered network protection, only one offered an antivirus solution that passed reviews by one of the three testers; however, it didn’t perform as well as WatchGuard’s partner solutions. None of the other network security providers have antivirus solutions that these third-party testers even considered for testing.

![Third party antivirus testing organizations have validated WatchGuard’s best-in-class partners (AVG and Kaspersky). Most of our competitors don’t even merit consideration.](image)

**Award-Winning Antivirus for Greater Confidence**

WatchGuard has chosen to work with companies that are leaders in what they do. We believe that a best-in-class service provider tends to win awards, gain certifications, and garner accolades that recognize their effectiveness. Antivirus partner AVG is one of the largest, most widely recognized and highly validated global antivirus vendors, with more than 28,000 resellers, partners, and distributors. AVG consistently wins awards from industry associations, including AV Comparatives, AV Test, ICSA Labs, PC Pro, and SC Magazine. AVG is a publicly-traded company with annual revenue of $270 million.

![Antivirus Accolades](image)

Figure 6: Don’t take our word for it, see how independent organizations rank AV solutions.
Cloud-Based URL Filtering for Even More Assurance

To further bolster protection while retaining fast browsing, WatchGuard’s cloud-based cloud reputation lookup service, called WatchGuard Reputation Enabled Defense, helps prevent users from accessing sites infected with malware.

Hundreds of thousands of WatchGuard users around the world help feed the WatchGuard cloud reputation authority database, which is also supplemented with feeds from industry leading URL aggregators. WatchGuard Reputation Enabled Defense extends the capabilities of WatchGuard antivirus security service partners. Benefits include:

- Continuous updates keep current with dynamic web content and changing web conditions.
- Up to 50 percent of URL scanning can be skipped without compromising security, resulting in faster browsing times and greater throughput at the gateway.

WatchGuard WebBlocker

WatchGuard WebBlocker, an URL-filtering solution powered by Websense, prevents inappropriate and unsafe web surfing, controlling access to sites that host objectionable material or pose network threats.

Leading URL Master Database for Better Filtering

The Websense-powered WatchGuard WebBlocker tool has the industry’s most accurate, current, and comprehensive master database of URLs, developed by Websense over decades.4

Figure 7. Websense is solidly positioned in the “Leaders” quadrant among providers of secure web gateways.

4 http://www.websense.com/content/MasterDatabase.aspx
Market Leadership and Award-Winning URL Filtering

Industry analyst IDC states that Websense has market share close to 40 percent larger than the next-largest vendor.\(^5\) Websense has racked up accolades and awards from SC Magazine, Information Security Magazine, CRN, and Frost & Sullivan, and others (see Figure 8).

<table>
<thead>
<tr>
<th>URL Filtering Accolades</th>
</tr>
</thead>
<tbody>
<tr>
<td>Websense</td>
</tr>
<tr>
<td>Fortinet</td>
</tr>
<tr>
<td>Sonicwall</td>
</tr>
<tr>
<td>Palo Alto</td>
</tr>
</tbody>
</table>

Figure 8. An abbreviated list of recent awards garnered by WatchGuard partner WebSense. Competitor solutions remain largely unheralded.

Trusted by Familiar Names in Social Media

Facebook, the most visited site on the web, according to Google, chose WatchGuard partner Websense to provide URL scanning to protect Facebook users.\(^6\) The URL-filtering tool provides a warning if a website is potentially unsafe.

With threats increasingly emanating from websites, organizations may find it reassuring to have such a powerful, trustworthy URL filter as part of their WatchGuard XTM network security solution.

WatchGuard spamBlocker

Powered by Commtouch, WatchGuard spamBlocker stops unwanted email at the gateway, with a 99 percent detection rate and with almost no cases of false positives. Commtouch’s patented Recurrent Pattern Detection technology detects spam outbreaks as they emerge for immediate, continuous protection from unwanted and dangerous email.

WatchGuard spamBlocker offers:

- **Patented, effective prevention**—Recurrent Pattern Detection technology reviews more than 4 billion messages daily and is able to detect and prevent spam regardless of language, content, encoding, or other evasion techniques.
- **Easy to use**—spamBlocker is simple to configure and includes helpful reporting and quarantine functions.
- **Virus blockade**—spamBlocker uses Commtouch’s virus outbreak-detection technology to block email-borne viruses at the gateway.

---


• **Market leader**—Since 1991, well-known organizations, including Fortune 100 companies, have incorporated Commtouch email security and anti-spam solutions in their software.

<table>
<thead>
<tr>
<th>Company</th>
<th>Vendor</th>
<th>Anti-spam Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>WatchGuard</td>
<td>Commtouch</td>
<td>1991</td>
</tr>
<tr>
<td>SonicWall</td>
<td>In-house</td>
<td>2009 (CASS)</td>
</tr>
<tr>
<td>Fortinet</td>
<td>In-house</td>
<td>~2003</td>
</tr>
<tr>
<td>Palo Alto Networks</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Figure 9. WatchGuard spamBlocker is powered by Commtouch, a premier provider of email security, providing antispam solutions since 1991.

**WatchGuard Intrusion Prevention Service and WatchGuard Application Control**

WatchGuard Intrusion Prevention Service and WatchGuard Application Control are both powered by BroadWeb. WatchGuard Intrusion Prevention Service provides real-time protection against network threats, such as SQL injections, spyware, cross-site scripting, buffer overflows, and drive-by-download attacks. A list of blocked sites saves valuable processing time by dynamically blocking IP addresses that have been positively identified as the source of an attack. WatchGuard Application Control supplies fine-grained control and unparalleled visibility for more than 1,800 applications (see Figure 10) helping organizations optimize network usage and employee productivity and block unproductive and inappropriate applications. WatchGuard Application Control also lets organizations control their usage of applications by category, application, or application subfunctions. Moreover, with WatchGuard, all application policies are clearly applied along with all other firewall policies.

**Market Leader in IPS and Application Control**

BroadWeb is a leading provider of network intrusion prevention technology at the application-layer level. It pioneered solutions in application identification and control.

<table>
<thead>
<tr>
<th>Company</th>
<th># of Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>WatchGuard (powered by BroadWeb)</td>
<td>1,800+</td>
</tr>
<tr>
<td>Palo Alto Networks</td>
<td>1,433</td>
</tr>
<tr>
<td>Fortinet</td>
<td>1,200+</td>
</tr>
<tr>
<td>SonicWall</td>
<td>1,100+</td>
</tr>
</tbody>
</table>

Figure 10. BroadWeb is a leading provider of Application Control solutions.
WatchGuard Tested and Approved
WatchGuard testing shows BroadWeb solutions to be highly effective in protecting organizations. WatchGuard performs much of this testing by using an industry-standard, best-in-class testing mechanism from Spirent/MuDynamics.

Selecting a Best-in-Class Security Solution
With network growth showing no signs of abating, organizations need a network security device that has the capacity to drive security and inspection activities quickly and reliably. Many multilayer network security solutions share similar feature lists, but not all of them can be considered best-in-class. The following section provides four key questions an organization should ask as it evaluates any multilayer security solution, along with a description of how WatchGuard XTM answers the need.

How robust is each layer? Ask questions about the size of the database, the richness of features, accuracy and detection rates, and speed of scanning. Unlike competitors, WatchGuard XTM incorporates the top-performing specialized security services from proven industry leaders. Working together, these components dynamically detect, block, and report on malicious traffic while efficiently allowing benign traffic to pass through. In addition, the proxies in WatchGuard XTM appliances protect organizations from new, previously unrecognized, zero-day threats.

How much experience and independent recognition does the company have? Generally, the longer a security company has been in business and the more accolades it has received, the more robust and highly developed the security service. WatchGuard XTM relies on security services from a collection of industry-best providers that are prime movers in their respective fields of specialty; continually receive multiple industry accolades and awards; and have been proven to be best-in-class through tests that WatchGuard and independent, third-party testers have conducted.

How flexible is the solution? Does the solution require hardware replacement to add new security functionality? Some solutions require customers to periodically upgrade hardware or insert special cards to gain new capabilities. In contrast, WatchGuard XTM offers a modular architecture. As the threat landscape changes, if WatchGuard releases a new security service, customers can add it with just a license key upgrade and gain a whole new layer of security without having to replace the hardware.

How easy is the solution to manage? Ask for a demonstration of the user interface. A few competitors use partners for one or more security services, but do not extend the UI to the security services. The result is one interface for managing the appliance and a different interface for security services. WatchGuard has engineered its award-winning XTM line of products to fully integrate—all the way to the UI—with best-in-class security solutions from WatchGuard and industry-leading partners.

Administrators can manage security functionality in WatchGuard XTM, including all security services subscriptions, from a single intuitive console, web-based UI, or command-line interface. These management and monitoring tools are included with the purchase of WatchGuard XTM appliances. The outcome of unified management is simpler, more accurate, and confident control of security management, a lower learning curve, and greater efficiency—all of which contribute to lower security management costs.
For More Information
For more information, visit www.watchguard.com/products/xtm-main.asp, contact a WatchGuard reseller, or call 1 (800) 734-9905 in the United States and Canada.

ABOUT WATCHGUARD
Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard’s award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2012 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard Logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part.No. WGCE66776_061212