

Five Important Security Trends in 2009

The network security landscape is ever-changing, so the threat to business networks never looks the same year to year. As we move into 2009, WatchGuard anticipates a few shifts in how attackers try to intrude on networks, and some changes in the context in which these networks operate. Here are five of the changes we expect.

1. The Web Is the Battleground

It's important for every network administrator to understand that the main battleground will be on the web. Attackers follow people and people are on the web, with almost every Internet service "web-ized" – from phone calls on Vonage and Skype to entertainment and training on YouTube and Hulu.com. Attackers also know that many businesses have custom-written web applications that often include vulnerable code. Add to that the fact that the cost of attacking is next to nothing. In fact, it's so low that attackers reap immense margins even if their attacks only succeed one or two percent of the time.

Our recommendation is for IT administrators to redouble defenses on web servers and browsers.

2. More Attacks via SSL / HTTPS

Every quality e-commerce site uses HTTPS to encrypt transactions. As a result, virtually all network administrators have to allow SSL to pass through their firewall, simply to support their organization's business mission. Because SSL is encrypted, administrators can't actually see what is being carried in that SSL traffic and attackers like to take advantage of the camouflage. Formerly, doing so was technically too difficult for most hackers, but now that organized crime is driving malware, malware is getting increasingly sophisticated.

We advise administrators to pay particular attention to endpoint integrity. Look for strong authentication capabilities in security products and robust SSL VPN capabilities.

3. Social Networking Threats Will Get Worse

In a world where a "friend" is an online stranger you arbitrarily decide to trust, security is almost nonexistent. Security analysts have long known that social networking sites such as MySpace, Facebook, Friendster, and others are, from a security viewpoint, rough neighborhoods. In 2009, we expect to see more uses of social networking sites as attack platforms, and more tricks and scams pulled against the participants.

We recommend that network administrators block all access to these sites unless there is a compelling business reason to use them.

4. Botnets with More Stealth

Botnet technology actually made some of its most breathtaking innovations in 2007, and those innovations paid off in 2008 with noisy, high-traffic infiltrations that got lots of press. We believe that in 2009, bots will be just as big and more effective than ever, but botmasters will put increased emphasis on discreet segments operating quietly under the radar. They have figured out how to make bots extremely lucrative, and now their focus will shift to keeping bots active for longer and longer periods without being detected.

The best defense against botnets is a fully integrated, multi-layered, interlocking security solution for wide-ranging protection in all attack vectors.

5. The Year of Cyber-Law

Questionable activities involving the Internet, from harassment to malicious impersonation, grew so rapidly these last few years that the law has not been able to keep up. These glaring holes are causing legislatures to scramble. Many laws will be proposed – and some of them perhaps not well considered.

We can't predict how many will pass, but whatever the results, we advise you to be on the alert for a wave of legislation in 2009. You and your customers will be obligated to comply, and in some cases, to prove your compliance.

WatchGuard® Network Security Solutions

At the heart of every WatchGuard XTM or UTM solution is a powerful “Layer 7” deep application inspection firewall and VPN to provide strong security out of the box. Our suite of security subscriptions boosts protection in critical attack areas to block spam, spyware, viruses, bots, trojans, web exploits, and blended threats for even greater levels of security. Customers rely on our WatchGuard SSL appliances for secure anywhere, anytime network access, and for remote cellular connectivity they add our easy-to-deploy 3G Extend accessory.



WatchGuard® XTM 1050

Headquarter/Data Centers—up to 10,000 users
The XTM 1050 is a high-speed network security appliance that delivers enterprise-grade performance and protection at an affordable price. 10 Gbps firewall throughput and 12 Gigabit Ethernet ports combine with advanced networking features including clustering and high availability (active/active) to handle high-volume network traffic securely.



Firebox® X Peak™

Main Office/Headquarters—up to 1000 users
Firebox X Peak is the high performer of our Firebox X family of appliances, with up to 2 Gbps firewall throughput and 8 Gigabit Ethernet ports to support LAN backbone infrastructures and gigabit WAN connections. All Peak models are powered by an advanced OS, and deliver a superior overall solution that meets the security and reliability needs of SMEs with demanding network environments.



Firebox® X Core™

Small & Mid-Size Regional Offices—up to 300 users
Firebox X Core is our best-selling line of UTM appliances for SMEs, delivering robust security that can scale to meet growing demands. Customers can easily upgrade to a higher model in the line for more capacity and performance, move up to an advanced OS, and add powerful security subscriptions by purchasing simple license keys



Firebox® X Edge

Small Offices, Wireless Hotspots—up to 55 users
Firebox X Edge is a stand-alone firewall and VPN endpoint solution for small businesses, remote offices, and telecommuters. Available in both wired and wireless versions, it's the ideal endpoint solution for connecting a secure VPN tunnel back to a WatchGuard XTM or Firebox X Core or Peak appliance.



WatchGuard® SSL

Anytime, Anywhere Access Appliances
WatchGuard® SSL connects end users to more network resources and applications, with support for more platforms and mobile devices than any other remote access appliance in its class. Multiple authentication options make it easy for IT to tightly manage access, while for end users, access is a breeze.



3G Extend

Cellular Connectivity for WatchGuard Appliances
It's easy to add 3G wireless connectivity to a WatchGuard security solution to maximize equipment uptime and ROI. This handy accessory provides cellular connectivity that can be used for either primary or backup Internet services. It offers ultimate flexibility to meet specific needs, supporting more than 50 modem cards and ISP providers

For more information on WatchGuard products, visit www.watchguard.com or call 206-521-8365.