



## The Target on Your Network is Growing Securing Your Network During an Economic Downturn

### Introduction

With the economy in its current state, the following scenario may be all too familiar: You've just left your Manager or Controller's office with the tune of "cost containment initiatives," "budget cuts," and "more with less" still ringing in your ears. On the long walk back to your office, you're trying to assess how this is going to affect, or possibly devastate your IT organization. Capital purchases will need to be delayed, you'll need to stay on older software platforms longer – headcount may be reduced. Reeling from these painful realizations, it's all too possible to lose sight of your overall goals, and default to a plan that only addresses the current budget reality without coming close to delivering the same IT value to the organization. In this white paper, we present opportunities that will allow you to maintain IT value as it relates to network security and prepare for a rapid cycle of future IT investment, even while in the midst of a difficult economic downturn.

### Defining Your Network Security Posture

In order to get your network security game plan together during an economic downturn, it's important to have a good handle on what your primary network threats were prior to the change in the environment, and how that change is likely to affect the current threat landscape.

You've most likely built a network security posture focused on protecting against malicious attacks and using defense-in-depth, while trying to implement a culture of security. You've learned that desktop AV is not a suitable stand-alone security solution, even for the smallest company, and that a router and a firewall are very different pieces of network equipment. You are aware of industry compliance requirements like PCI-DSS, HIPAA, and CIPA. Knowing what you know, you've crafted

---

a security solution for your organization that balances known risks with effective protective measures. One question remains: How is that security going to stack up against new “recession-driven” threats?

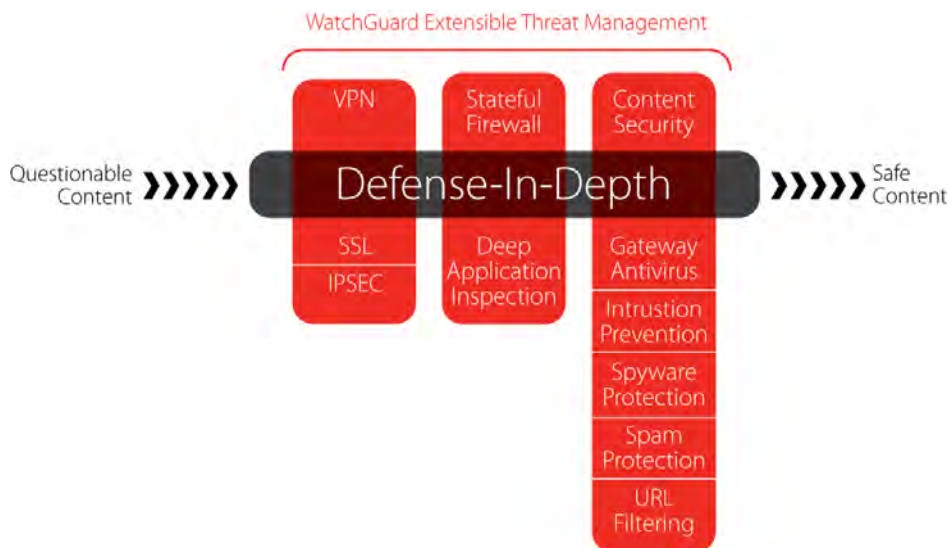


Figure 1: Defense-In-Depth

To answer that, we need to consider what we think the bad guys are planning.

## The Bull's Eye Gets Bigger

If you still believe that today's hackers are bored teenage kids trying to hack into networks to play pranks, impress their friends, or get their hands on the newest computer game - you're in for a rude awakening.

Hackers are career criminals that have learned how to steal vital information through illegal network access, turning large profits via an incredibly organized criminal enterprise. Hackers specialize. Some focus their attacks on exploiting easy targets and vulnerabilities. Some focus on developing tools, such as viruses or phishing exploits, and sell them to other hackers who have targets in mind. Some build extensive botnets and “lease” out the computing power to be used in large-scale automated attacks against known vulnerabilities, or as a diversion so that other hackers can carry out their malicious attacks undetected. Others are hangers-on to the hacker community, taking ill-gotten information and turning an illicit profit. Many of these specialists market their nefarious skills on IRC chats or in sophisticated forums where reputation ranking is encouraged. So, don't fool yourself, hacking is big business – and all businesses become attractive marks when defenses are scaled back. If payment card information and personal client information are part of your business – you become particularly attractive to hackers. But don't forget, even a small business with extra computing bandwidth to siphon makes a great target if it's an easy hack.

Specialization makes cyber-crime a fairly easy game to break into. Add to that, an economic downturn, rising unemployment, tight credit, home foreclosures, and countless other financial pitfalls. When faced with financial ruin, what is a computer-savvy person to do? Normally, a turn to the dark side is not an option – but when backed against a wall, typically honest people end up weighing the pros and cons: it is easy to break into, causes no risk of personal injury, allows for work from home during normal hours... for fear of talking you into this line of work, I'll stop here. But you get the point. Crime is on the rise during tough financial times, and cyber-crime is going to be a very

attractive path for many disenchanted and disenfranchised workers. Overall, the number of attacks on business networks will increase as will the innovation behind attacks. In fact, we expect vast growth in the number of socially-engineered network attacks with help from inside accomplices.

How are you expected to defend against the sudden surge of cyber-crime carried out by a hacker army bolstered by a bevy of new recruits? Well, now is the time to stay the course, maintain all existing defenses, and consider new ones.

## Rethinking Your Network Defenses

Perform a network security audit to find out what your network security strengths and weaknesses are before you finalize any plans. It's important to know how well you're prepared to stand up against the throng of malicious attacks that plague businesses. Keep any industry related compliance issues in mind.

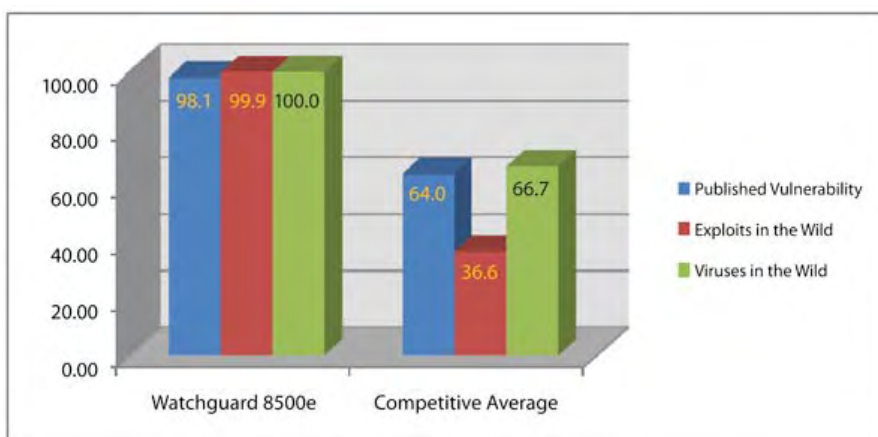


Figure 2: shows how WatchGuard Technologies' Firebox X Peak 8500e UTM blocked almost every attack launched against it by the Miercom Vulnerability Test Suite.

As you begin to investigate ways to improve your network security posture, you may run into some surprises – the first being the variety of security products available in the marketplace. You may have thought that you had excellent coverage with a couple products, but now find that some key components are missing. Second, you'll find that depth of packet scanning makes a colossal difference in your threat coverage. While some vendors are using investment dollars on marketing campaigns instead of proxy development, the reality is that by scanning more of the network packet, more threats will be deflected – proxy-based security provides the most effective packet scan available. Lastly, you should notice how easy it is to add additional layers of perimeter security with an Extensible Threat Management (XTM) product in place. UTM products are designed to deliver protection against blended threats in one, easy-to-manage device.

You've taken a long, hard look at your current security posture; now ask yourself some basic questions:

- Is your most sensitive information protected by multiple layers of security?
- Can you reasonably expect to stop blended threats at the perimeter?
- Do you have gaps in your coverage?
- How can you bolster security as your company grows?

Once you determine what you have in place, you'll have a much better idea of what is needed to protect against a growing and ever more potent threat landscape. First, fill all dangerous gaps, next add additional

---

layers of security around the most sensitive information in your network, and make sure that all industry regulations that apply to your business are met. With your network security solution list in hand, it's time to take on the question of that shrinking budget.

## **Making the Budget Fit**

As with every challenge you strive to meet, you'll have greater success if you keep the goals in mind, and then look for the right path to get you there. You've got your mind on the game, you've mapped out a security posture that is right for your company and speaks to the current threat environment - so the only question is, how can you make it a reality given the economic downturn and your new budget reality?

Now is the time to consider all the usual alternatives, as well as new options that you might not have considered before:

- **In-house or outsourced solutions**

As network security becomes more complex, many IT services companies now offer it as an option in their services portfolio. Managed Services Providers can tailor a plan that meets your specific needs – most will include perimeter and/or client security, management, reports and network uptime service-level agreements in the range of 4 to 5 9's (99.999% uptime). For some companies, it may be easier to obtain higher levels of security with managed services by paying a monthly charge rather than financing a new IT installation. WatchGuard can certainly help identify a MSP that specializes in WatchGuard security solutions.

- **New vendors**

When it comes to network security, there are specialized vendors and those who provide it as a niche within a broad portfolio of network equipment. If you are using the latter, operating under the assumption that there is a cost associated value in sticking with one vendor, you might be surprised when you start seeking outside bids. WatchGuard partners work with clients who labor under this assumption. When clients can no longer afford costly solutions, they're happy to find that they can cost-effectively replace their old equipment and support their layered security services with a single UTM appliance.

- **Make your needs known to your valued partner**

Whether you've been working with an online or local reseller, you haven't fully utilized a valuable resource if their role has been strictly defined as order-taker. For greatest efficiency, you need to take full advantage of expertise that exists outside your company. Explain your budget and your goals – let your partner do the leg work to develop an alternative that meets your business needs. You might be pleasantly surprised by what they deliver.

- **Calculate TCO**

Don't forget to consider all the costs associated with your network security needs. Security subscription renewals, per-user VPN licenses, management licenses, advanced feature purchases – vendors do not necessarily treat these in the same manner. You need to look at the initial purchase as well as continuing expenses for an accurate evaluation. This is another good reason to engage your partner in the effort – they are likely familiar with vendor practices and can find one that best matches your needs.

---

- **Consider all costs and balance the end game** (network efficiency losses are costs, network security prevents these losses)  
IT managers have likely been deploying this strategy already, but it has a place in evaluating network security as well. Inadequate network security can lead to a vast number of unrecoverable costs. Ponemon Institute estimates that the expense associated with a customer data breach is \$202/customer record. That's the real cost of contacting the customer, paying retribution, legal fees, etc., but doesn't even touch the cost a damaged reputation has on current and future revenue. Network downtime translates into business costs, reduced bandwidth and CPU from botnets translate to efficiency losses and costs, and so on and so on. The Department of Labor reports that 93%<sup>1</sup> of businesses that suffer a data breach are no longer in business five years later. Some catastrophes are so incredibly detrimental that businesses take out insurance against them. Network and data breaches fall into that category. So, in order to justify the expense, you need to fully expose the risks.

Although we can't provide a specific plan for every budget affected by the economic downturn, we have provided suggestions that enable you to find different ways to meet your needs, as well as plenty of evidence to justify network security management. Now that you've addressed your current situation it's important to consider how your current network security strategy will change as we come out of the economic downturn and move into a more prosperous time.

## Preparing for the Next Period of Economic Growth

To borrow a phrase that we're all familiar with, "this too shall pass." So, even though special strategies may need to be deployed during these difficult economic times, plans still need to be made to bolster network security as we emerge from the downturn and continue to face ever-evolving network threats.

Use this time to train and prepare the network constituents for the next wave of exploits. The future growth of your business depends on a network that is unhindered and uninterrupted by network attacks. Training and awareness are part of a larger campaign that fosters the growth of a Culture of Security within your organization.

Increasingly, hackers are looking to exploit unaware, uninformed, and unprepared network users. Most users require external internet access to perform their jobs, and often times operate company-owned computers in under-secured networks. Vulnerabilities could be exploited to gain access to local files as well as the entire network infrastructure. Users need to be taught that exploits exist, how to avoid them, how to recognize a compromised system, how to report it, etc. With proper education you can breed a healthy "Culture of Security." The ultimate goal being users who act in a consistently secure manner at all times. To implement a Culture of Security is no small effort, and to maintain it requires a constant and consistent program that builds over the course of years.

## Conclusion

We hope the information provided here will make the "more for less" directive seem more achievable – at least in terms of network security. We've shared guidance and suggestions to ensure that network security health is at the forefront of your concerns and given you the necessary tools to approach others with an appropriate security posture in mind. We've talked about the importance of planning for future business growth and the threat landscape you may face. Lastly, we've talked about how you can cope during this difficult time without taking steps in the wrong direction. No matter what...stay safe!

---

<sup>1</sup> ["Economic Downturn Underscores Need for Proactive Measures to Safeguard Data and Minimize Risk,"](#) Nov. 19, 2008



advanced  
network  
systems

For More Information,  
Contact Us:

800.639.6757  
[sales@getadvanced.net](mailto:sales@getadvanced.net)

[www.getadvanced.net](http://www.getadvanced.net)

---

#### **ABOUT WATCHGUARD**

Since 1996, WatchGuard has been building award-winning unified threat management (UTM) network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. We recently launched the next generation: extensible threat management (XTM) solutions featuring reliable, all-in-one security, scaled and priced to meet the unique security needs of every enterprise. Our products are backed by 15000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including retail, education, and healthcare. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

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. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox are either trademarks or registered 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. WGCE66628\_050109

---