



SonicWALL 2010 Security Trends

Contents

Predictions for 2010	2
New Wave of Teleworkers Prompts Tighter Remote-Access Security	2
First Post-Recession Hires Will Be Temporary Workers and Contractors	2
Workers Access Core Systems from New Platforms	2
Social Media Becomes Integral to Business Communications	3
Converged Communications Complicate Security	4
Application Security Gets Murky in the Cloud	4
Gartner Highlights Seven Cloud-Computing Security Risks	4
Virtualized Applications are Vulnerable to Real Security Threats	5
Data Center Consolidation Raises New Security Concerns	5
New Infrastructure Deployments	5
Data Leakage is Everywhere	5
How to Ensure a Secure Future	6
Conclusion	6

Predictions for 2010

The year 2009 brought about major shifts in network and computer security. While social networking, virtualization, consolidation, downsizing and outsourcing drove the agenda for nearly every organization, those with malicious intent tapped into these trends to achieve their goals in novel ways. The year's most significant security challenges revolved around hackers' use of increasingly sophisticated botnets, and their exploitation of social networking activities to target unsuspecting companies and individuals.

Drawing upon our detailed knowledge of security issues and our unique perspective of global security threats SonicWALL® developed this paper to provide an overview of anticipated trends in 2010. Our goal is to assist organizations of all sizes strengthen their understanding of the threat landscape and best prepare their defenses for the coming year.

New Wave of Teleworkers Prompts Tighter Remote-Access Security

Teleworking has been around for years, but the H1N1 outbreak in 2009 spurred companies to enable employee access from remote locations.¹ Though organizations may have seen this remote-access initiative as a temporary measure, their employees took a different view. After all, once employees receive permission to work remotely, they are averse to surrendering it.



While this shift will force organizations to grapple with a number of challenges, security is likely the most pressing one. Mainly focused on enabling access as part of H1N1 contingency plans, many companies underestimated the security issues related to this move. Continued increases in teleworkers, both temporary and permanent, will introduce many novices – and unknowns – into the

remote access process. Adding to the challenge in 2010 will be that companies are expanding their workforce with contractors and they take a “wait and see” approach to stability of the economy. In both cases companies will need to review their remote access policies to utilize a remote user's credentials, system attributes and even their needs, to determine the corporate information they can access.

First Post-Recession Hires Will Be Temporary Workers and Contractors

As the economy recovers, temporary workers and contractors are often the first employees that organizations bring on board.² Temporary workers and contractors often use their own systems to access the company's network and its resources. Because these workers often contract with multiple companies simultaneously, an organization may be limited in its ability to install software – or in some way control or manage – these outside systems. At the very least, businesses can avoid administrative nightmares when blending permanent and temporary employees. The key is to develop a tightly integrated policy based on the employee's role, the system the employee uses and/or is trying to access, and the employee's physical location. Nevertheless, policy alone is never enough. Organizations must be able to bring a new temporary worker or consultant on board rapidly and terminate their access just as quickly.

Workers Access Core Systems from New Platforms

As consumer applications increasingly form the roots of a growing number of enterprise tools, organizations are unwillingly relinquishing control over the IT environment. The fact is businesses can no longer assume that everyone is using a corporate BlackBerry that is covered by a strong security policy. Instead, employees are accessing information and applications from consumer devices including the Apple iPhone and Motorola Droid, to name a few. In a Goldman Sachs Smartphone Survey, 52% of the iPhone owners who responded say they use their smartphones for business.³ Moreover, all reports point to these devices making their way into the corporate environment in even greater numbers. For one, Gartner projects mobile phones will be the primary Web access device by 2013.⁴



Sales of smartphones, such as the iPhone and Nokia Corp.'s N97 touch-screen phone, increased 12.8% to surpass 41 million units in the third quarter of 2009.

Source: The NASDAQ Stock Market Inc., Global Handset Sales Rebound, Seen Rising In 4Q – Gartner

¹ Network World, *H1N1 drives demand for secure remote access*, November 12, 2009 <http://www.networkworld.com/news/2009/111209-h1n1-drives-demand-for-secure.html>

² Scripps News, *Post-recession, temporary workers becoming norm*, December 3, 2009 <http://www.scrippsnews.com/node/49522>

³ ZDNet, *Goldman Sachs: BlackBerry, iPhone own smartphones, but if Apple ever gets an enterprise subsidy...*, August 3, 2009 <http://blogs.zdnet.com/BTL/?p=22066>

⁴ MediaPost Communications, *Gartner: Mobile To Outpace Desktop Web By 2013*, January 13, 2010 http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=120590

⁵ The NASDAQ Stock Market Inc., *Global Handset Sales Rebound, Seen Rising In 4Q – Gartner*, November 12, 2009 <http://www.nasdaq.com/asp/company-news-story.aspx?storyid=200911120153dowjonesdjonline000343>

⁶ Telecom News, *AOTMP Report: Lax Wireless Device Security Protocols Exposes Nearly 2 in 5 Enterprises*, January 8, 2010 <http://vartips.com/mobility/aotmp-report-lax-wireless-device-security-protocols-exposes-nearly-2-in-5-enterprises-992.html>

⁷ CIO Magazine, *BlackBerry Security Exec Warns of Smartphone DDoS Attacks*, November 18, 2009 http://www.cio.com/article/508076/BlackBerry_Security_Exec_Warns_of_Smartphone_DDoS_Attacks

Though most organizations are fully aware of the burgeoning use of unsanctioned smartphones to access corporate assets, they appear slow in making the necessary policy and procedure updates – perhaps ignoring these devices altogether. According to the AOTMP report, “Securing Your Mobile Environment,” issued in December 2009, nearly two of every five enterprises are at risk of exposing sensitive data on wireless devices, and ineffective wireless policies and protocols could be to blame.⁶



With millions of employees accessing corporate data via third-party applications not managed or secured by the IT group, IT departments everywhere are forced to redefine their security approach and policies. Like it or not, the “customization of IT” is taking hold, as organizations attempt to rein in some of the freewheeling devices and applications in their midst—and the move could not come at a better time. Even Research in Motion’s vice president

of BlackBerry security sounded an alarm when he expressed concerns about compromised or “rogue” smartphones being used to bring down wireless carrier’s cellular networks via distributed-denial-of-service (DDoS) attacks.⁷

Without question, companies need to define a security policy for smartphones. As organizations evaluate their approach to smartphone-endpoint control, they should determine how they will detect and filter viruses and worms that may be tuned for Android and iPhone platforms. Otherwise, companies would need to trust telecommunications providers to offer the requisite level of security, which would be an unrealistic scenario for any serious business.

Social Media Becomes Integral to Business Communications

According to an IDC report dated April 2009, “24% of enterprise employees use social networking tools to collaborate, 14% of Fortune 100 employees have a profile on LinkedIn, and 2% of enterprise employees use microblogging to collaborate. It is no longer a question of if or when enterprise employees will use Web 2.0 tools – the genie is out of the bottle.”⁸ While many organizations tested the social-media waters in 2009, 2010 will see even more companies embracing social media and networks as critical communications

channels. For example, here at SonicWALL, we use BrightTalk as the “YouTube for business communications.” We also leverage Twitter to rapidly gather and disseminate customer, channel, and product information. In addition, we find Facebook valuable to establish our reputation and extend our reach.

As companies increasingly jump onto the Web 2.0 bandwagon, a growing number of employees are using social-media tools and applications in the business environment. This is yet one more extension of the “consumerization of IT.”⁹

Increased use adds increased vulnerabilities. Just as mobile devices expose the corporate network to potential threats, so do social-media tools and applications. In fact, social-media and networking widgets and applications can carry the same kind of spyware, keyloggers, and bots that infest the shadier regions of the Web. It is only logical that greater use of social media will lead to increasingly sophisticated attacks on social networks.

Going forward, attackers will launch automated, context-sensitive, and targeted attacks that prove highly effective. Tapping into basic human nature (and the concept of social engineering¹⁰), attackers send communication that the recipient is likely to open and read. For example, if an organization posts a job opening on Facebook, an attacker will send a malicious virus disguised as a résumé.

Alternatively, if someone on a forum asks group members for pictures from an event, an attacker will send a message purportedly from one of the members, with a virus disguised as photos. As the number of Web 2.0 hacking incidents steadily increases¹¹, businesses need to adjust their security practices accordingly.



⁶IDC, *Preparing for the 2.0 World: How Enterprises Need to Think About Emergent Social Technologies*, April 2009 https://www.sun.com/offers/details/IDC_2.0_World.xml

⁹Gartner, *Gartner Says Consumerization Will Be Most Significant Trend Affecting IT During Next 10 Years*, October 20, 2005 http://www.gartner.com/press_releases/asset_138285_11.html

¹⁰Wikipedia, *Social engineering (security)*, http://en.wikipedia.org/wiki/Social_engineering_%28security%29

¹¹Telegraph Media Group Limited, *Business Club - does Web 2.0 need Security Web 2.0?*, September 3, 2009 <http://www.telegraph.co.uk/finance/businessclub/6133659/Business-Club---does-Web-2.0-need-Security-Web-2.0.html>

¹²IDC, *Preparing for the 2.0 World: How Enterprises Need to Think About Emergent Social Technologies*, April 2009 https://www.sun.com/offers/details/IDC_2.0_World.xml

As IDC articulated in its report: *Preparing for the 2.0 World: How Enterprises Need to Think About Emergent Social Technologies*, "In order to ensure visibility, management, security, and compliance of enterprise information, IT must provide the tools that employees want to use or risk having enterprise information distributed and managed by services over which they have no control."¹² However, IT must do this while keeping in mind the timeless adage of the need to balance security and productivity. It is simply not practical to implement draconian rules such as "block all social media applications during business hours to eliminate unproductive time." A more realistic approach is for businesses to understand who is using which social media applications. Then they can establish simple IT policies to ensure guaranteed access, bandwidth, and communications for people who need it, and restricted access for those using applications in unproductive ways.

Converged Communications Complicate Security

Much as social-networking tools have become entrenched in the corporate culture, converged communications infrastructure to support voice, video, and data is taking hold. In fact, 22% of CIOs surveyed by Goldman intend to increase spending in this area. The drivers for this increased uptake are the fact that organizations can access technologies



such as HD Telepresence; less-expensive, higher bandwidth connections like Verizon FiOS; and services like hosted Voice or Video over IP (VoIP).

As more and more enterprises merge their voice, video and data networks, new concerns arise. For example, how do companies prevent YouTube access from interfering with VoIP usage? If every employee is able

to video conference from their desktops, how does the organization guarantee bandwidth for all? If cybercriminals can take down the company Web site with a DDoS attack, what havoc can they wreak on the VoIP system?

To protect converged communications, organizations need to focus on quality of service and bandwidth management, while continuing to provide secure communications, be it data, voice or video. At the network perimeter, a firewall must ruthlessly inspect traffic across all ports and protocols to ensure security. However, with converged communications, the firewall must also address quality of service requirements, through wire-speed

throughput (low latency) and bandwidth control and prioritization on a per-application and per-user basis.

Application Security Gets Murky in the Cloud

Savvy organizations define security rules that keep pace with the changing computing environment. For instance, there was a time when companies mapped a firewall rule all the way from an IP address to a server on a certain LAN segment. Then as employees became increasingly mobile, companies defined rules based on users and applications, instead of on ports and IP addresses.

New computing trends are forcing yet another shift in corporate security stances. With cloud computing on the rise, enterprise applications – such as Salesforce.com and SharePoint – are increasingly mobile. In these scenarios, corporate information migrates between an organization's data center and the cloud data center, between cloud data centers, and across servers within cloud data centers. It is no wonder Gartner recommends that organizations consider seven major cloud-computing security risks before contracting with a cloud vendor.¹³

Even with full awareness of the security risks associated with cloud computing, organizations running applications in the cloud are still challenged to implement a security policy that defines who should access the application and from where. To resolve this issue, businesses need to call upon past experience. While cloud computing introduces a new method of implementing, maintaining, and accessing corporate applications, it requires a security approach similar to the one employed to secure the corporate environment.

Gartner Highlights Seven Cloud-Computing Security Risks

1. Sensitive data may be exposed to unauthorized vendor personnel.
2. Regulatory compliance could become an issue if the cloud-computing provider refuses to participate in external audits and security certifications.
3. Data can be stored virtually anywhere around the world, potentially leading to violations of local privacy requirements.
4. Data security measures may be insufficient, make data unusable, or complicate availability.
5. Unless the provider is able to completely restore data, such as in the event of a disaster, valuable information could be lost forever.
6. Investigating inappropriate or illegal activity may be difficult – and even impossible.
7. Mergers and acquisitions could threaten the availability of a customer's data.

Source: Gartner, *Assessing the Security Risks of Cloud Computing*, June 2008¹⁴

¹³ InfoWorld, *Gartner: Seven cloud-computing security risks*, July 2, 2008 <http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853>

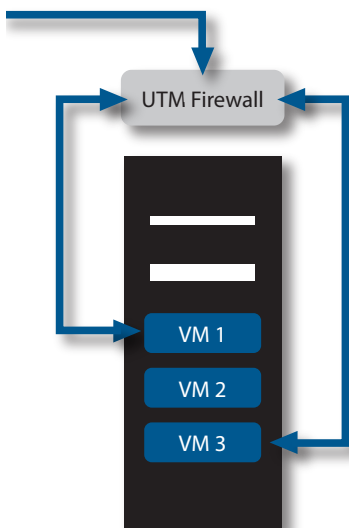
¹⁴ Ibid

¹⁵ Network World, *Virtualization security remains a work in progress*, December 22, 2009 <http://www.networkworld.com/news/2009/122209-outlook-virtualization-security.html>

¹⁶ Gartner, *Gartner CEO and Business-Executive Survey Shows 62 Percent of CEOs See IT Having a Key Role in Post-Recession Strategy*, December 14, 2009 <http://www.gartner.com/it/page.jsp?id=1254414>

Much as they have done to date, IT groups need to define a security policy that addresses users, applications, and the content being accessed. The new twist is to reserve cloud computing for applications that are suitable in that type of environment.

Virtualized Applications are Vulnerable to Real Security Threats



Along with cloud computing, virtualization is making its mark in a range of business environments. According to Gartner, roughly 18% of server workloads have been virtualized, and that number should climb to 28% in 2010 and almost 50% by 2012.¹⁵ While many companies have embraced virtualization for obvious reasons, they may not realize the new challenges associated with protecting applications and information in this environment.

Before virtualization, when organizations ran multiple applications in different data centers, they set up firewalls between servers and applications. In a virtualized environment, no implicit security barriers exist between applications. As a result, it is challenging to make sure that someone with access to application A does not automatically inherit access to application B.

Data Center Consolidation Raises New Security Concerns

As much as companies are tapping into virtualization to consolidate multiple servers into a single physical device, they are consolidating independent enterprise data centers into larger, more efficient data centers. The benefits are clear: cost savings and improved inter-application performance. However, the downside might not be as apparent. Any inter-data center security measures currently in place will be lost with the move. In addition, organizations will need to examine access controls – which may now be in the hands of a third party.

To protect applications in the data center adequately, organizations should consider the following technologies. First is an SSL VPN to provide scalable access to applications with fine-grained control. Next is a Deep Packet Inspection firewall to provide highly redundant secure network access into the data center to mitigate connectivity risk. This Deep Packet Inspection firewall can also sit between server groups to preserve legacy security separation while maintaining performance benefits.

New Infrastructure Deployments

As the recovering economy causes purse strings to loosen, many organizations will accelerate the deployment of infrastructure projects they put on hold due to economic conditions. In fact, 62% of CEOs recognize that IT-enabled changes will be a key element in their post-recession strategy, according to Gartner.¹⁶

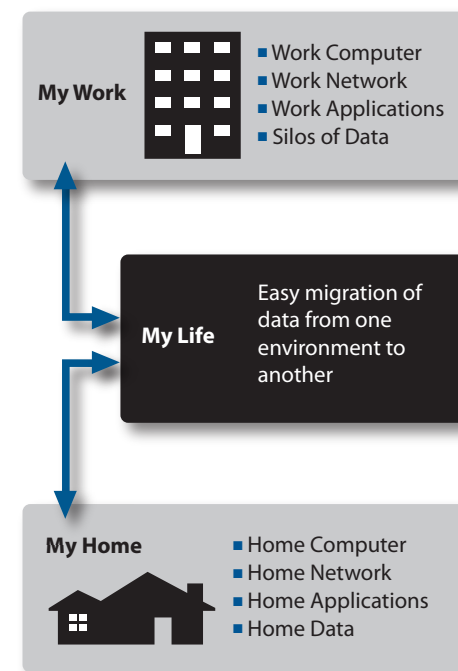
Companies will be tempted to purchase point solutions to satisfy immediate needs, but this strategy will only increase costs down the road. After all, the use of multiple diverse systems drives up maintenance and training costs.

Rather than let an automatic reaction dictate the course, it may be time for organizations to consider consolidated security. For example, businesses can swap out an existing, single-function firewall for a unified threat management firewall that also happens to be VoIP-ready. This decreases maintenance and training requirements while streamlining management and reporting. Just as important, it accommodates the company's changing needs when it comes to enabling cost-effective communications.

Data Leakage is Everywhere

Regardless of industry, data leakage is an issue that every business faces today. Part of the reason is that there is less and less separation between the computing and networks used for personal and work lives.

People can access personal data from work – for example, related to banking, shopping, and travel – and work data from home. Moreover, they can do so on their smartphones and laptops, which they can take into and out of the corporate environment. In addition, employees can easily migrate data from the Microsoft Exchange Server at work to their Gmail account. When one considers how simple it is to accidentally send an email to the wrong addressee, it is not a stretch to see how easy it is to share data intentionally with unauthorized recipients.



¹ Network World, *H1N1 drives demand for secure remote access*, November 12, 2009 <http://www.networkworld.com/news/2009/111209-h1n1-drives-demand-for-secure.html>

² Scripps News, *Post-recession, temporary workers becoming norm*, December 3, 2009 <http://www.scrippsnews.com/node/49522>

³ ZDNet, *Goldman Sachs: BlackBerry, iPhone own smartphones, but if Apple ever gets an enterprise subsidy...*, August 3, 2009 <http://blogs.zdnet.com/BTL/?p=22066>

While data leakage is complicated to deal with, good business sense – along with regulatory requirements such as Payment Card Initiative level 4 and Electronic Health Records – should compel organizations to address this problem in 2010. A solid approach is to leverage email security to spot data leaving the network. By layering a Deep Packet Inspection firewall on top of that, organizations can block malware and limit common data leakage paths. Finally, application intelligence uses custom signatures can prevent data from leaving the network.

How to Ensure a Secure Future

While new technologies and ways of working and collaborating bring great benefits, they are also contributing to the perforation of the network perimeter – and redefining every organization's infrastructure. The challenge is to secure this new infrastructure. To do this, businesses must protect their users at every endpoint from viruses, Trojans, and phishing and DDOS attacks that originate from a variety of social-networking channels and data centers around the world connected by all types of networks.

A comprehensive defense incorporates advanced technology with policies focused on users, content, and applications. SonicWALL provides unique protection against spam – and other email threats like phishing attacks – by actively gathering vital learning from an expansive network called the SonicWALL Global Response Intelligent Defense (GRID) Network. With more than four million sensors, the GRID Network provides collaborative intelligence, enabling SonicWALL to deliver a fast and accurate response to the latest security threats.

Conclusion

In 2009, organizations learned how to run their businesses close to the bone. They extracted as much as possible from every asset to maximize their return on investments while ensuring sustainable operations. In 2010, companies can apply this same philosophy to grow their business. For example, they can harness technologies such a social networking, teleworking, and converged communications, to benefit their business in numerous ways. That said, as always, organizations need to guard against the latest threats. By balancing new technologies with vigilance, companies can move forward with confidence.

About SonicWALL

SonicWALL® is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high-performance business network. For more information, visit the company Web site at www.sonicwall.com.

SonicWALL's line-up of comprehensive protection



NETWORK
SECURITY



SECURE
REMOTE ACCESS



WEB AND E-MAIL
SECURITY



BACKUP
AND RECOVERY



POLICY AND
MANAGEMENT

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™