

The Adaptive Business

Ensuring the responsiveness to meet today's challenges

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[®]

Table of Contents

Introduction	1
Adapting to tighter budgets	2
Adapting to tighter regulations	3
Adapting to a flexible workforce	4
Adapting to broader collaboration	5
Adapting to greater mobility	6
Adapting to new applications	7
Adapting to emerging threats	8
Adapting to potential disaster	13
Conclusion	14

Introduction

To persevere and succeed in today's economy, companies need to adapt to rapidly-changing business realities. In these challenging economic times, companies are suddenly faced with the need to be more competitive and productive using fewer resources, and under increasingly-stringent regulations. Businesses must be flexible in bringing the talent and resources they need from a wider range of distributed employees, part-time workers, contractors, partners and consultants. IT departments must adapt to a torrent of new software and hardware technologies that are no longer always under their complete control. And, more than ever, companies must be prepared to adapt and respond to emerging threats from malware and disasters.



Adapting to tighter budgets

The new economic climate has tightened corporate budgets across-the-board. Funding for staff, facilities and operations is now at a premium. Expenditures for new equipment or enhanced applications now undergo heightened scrutiny.

*To adapt, businesses need to
insist on greater value.*



For IT, this means demanding solutions that deliver full functionality at the most affordable price-point, to clearly demonstrate the greatest return on investment. At the same time, businesses need to choose solutions that streamline and automate management overhead, to reduce total cost of ownership.

Adapting to tighter regulations

The growing demand for government assistance and bailout funding carries with it an increasing insistence on corporate accountability. Companies across every business sector face more stringent regulatory compliance demands. Even if your company is not directly affected, you likely transact with regulated lenders, underwriters, suppliers and other business partners that are affected.



To adapt, businesses need

proactive strategy, not merely reactive compliance.

IT departments have been adapting to regulatory compliance since the emergence of e-business, whether it be PCI, HIPAA or Sarbanes-Oxley. However, point solutions are not the most cost-effective approach. IT needs to strategically incorporate best practices for monitoring, auditing and reporting into their standard operations, and evaluate security solutions by their ability to comprehensively meet compliance demands across multiple and evolving regulatory requirements.

Adapting to a flexible workforce



Companies are undergoing restructuring. Businesses are cutting staff and closing physical plants and facilities. And yet, they still need to remain productive and competitive in a global market. A great number of businesses will fill gaps in needed resources by contracting with former employees as part-time staff working from their homes.

To adapt, businesses need to embrace telework initiatives.

IT has a number of mature technologies, such as SSL VPN and VoIP, at its disposal with which to provide teleworkers secure remote access to the same mission-critical applications and resources they received as full-time employees. Telework initiatives can also reduce facilities overhead, leverage “green business” tax incentives, and open up more-affordable staffing pools.

Adapting to broader collaboration

With cuts in staff, businesses are working leaner, and depending more upon outsourcing to third-party partners as a cost-effective means of providing talent and services on an as-needed basis. However, not every vendor or solutions provider is able or qualified to fill the needs.

To adapt, businesses will need to develop shared-responsibility partnerships.

Reduced IT departments need more assistance with emerging security technologies, while still retaining staff and budget flexibility. IT is increasingly developing relationships with integrated managed service providers (MSPs) that can share more responsibility for network security, and deliver greater economies of scale with easy-to-deploy, centrally-managed solutions.



Adapting to greater mobility



Like it or not, more teleworking and third-party collaboration means there are more employees, partners and consultants accessing company resources remotely, using 3G wireless laptops, PDAs and smartphones. These mobile devices are outside the traditional network perimeter—and therefore outside of direct IT control. Subsequently, these devices are prone to theft, hacking, outdated anti-virus signatures, unsafe downloads and malware infection.

To adapt, businesses must incorporate mobility into their security strategy.

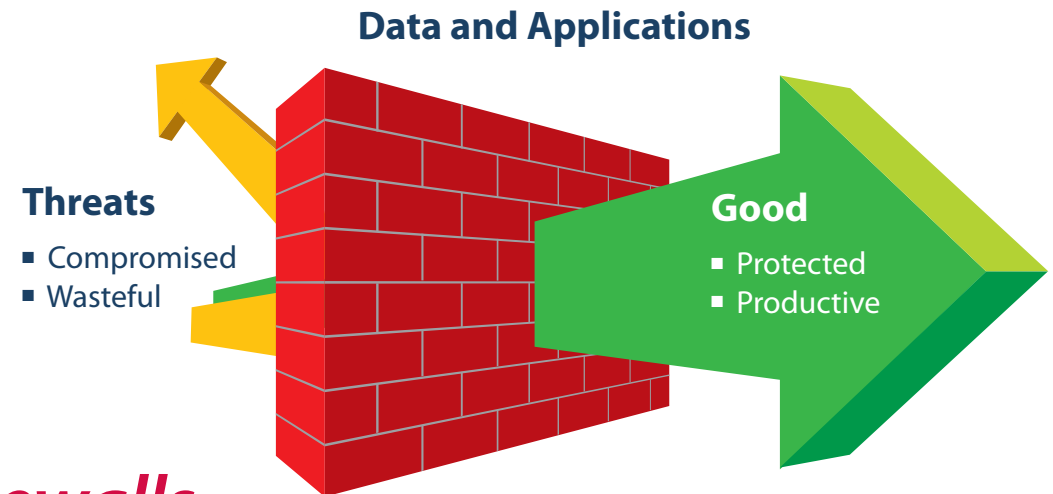
IT must define comprehensive policy for business-related usage of mobile devices, and select security solutions that are able to enforce that policy with granular mobile endpoint control. Best practices include “Clean VPN” solutions that integrate SSL VPN secure remote access technology with Unified Threat Management (UTM) firewalls which decontaminates vulnerabilities and malicious code from remote mobile users and branch offices traffic before it enters the corporate network, and without user intervention. CleanVPN ensures both inbound protection from malware and outbound protection from the loss of data.

Adapting to new applications

As much as 25% of application traffic passing through corporate firewalls is personal, and not business-related. Applications like instant messaging, social networking, online trading, peer-to-peer (P2P) file sharing, streaming media and personal e-mail consume network throughput, and expose companies to potential malware infection and data loss.

To adapt, businesses need to deploy application-centric firewalls.

Today, security management is seen less in terms of devices, ports and subnets, and than in terms of who is allowed access to what data using what applications from what locations. IT needs to define policy on what kind of information can traverse the enterprise perimeter, and enforce it using application firewalls that can effectively filter Web-based applications, streaming media, peer-to-peer applications (P2P) and e-mail attachments.



Adapting to emerging threats

The development of malicious software has become a global-scale, profit-driven criminal activity. Malware developers and hackers are highly-paid and highly skilled professionals who are working around the clock to generate new threats to business systems. Countermeasures, such as anti-virus, anti-phishing and anti-spam technologies, are only fully effective when they disseminate updated malware signatures to business systems before an emerging threat can attack.

*To adapt, businesses need
real-time protection as threats emerge.*



IT needs continuous real-time threat protection solutions that can ensure the strongest defense posture with minimal IT intervention. Best practice suggests solutions that dynamically and continually update threat signatures in real-time as they emerge, based upon extensive feedback networks of global business environments.

Adapting to potential disaster

In a global marketplace, extreme weather, terrorist attacks, fires, earthquakes or power-grid blackouts are not a matter of if but of when. Any event that can disrupt workflow or destroy mission-critical information has the potential to put a company out of business.



*To adapt, business must have
flexible, reliable recovery mechanisms in place.*

IT not only needs clearly-established disaster recovery plans in place, but it needs to activate and test these plans on a regular basis to ensure they are reliable. Best practices for disaster recovery include highly-available systems redundancy; automated backups to secondary sites; bare metal imaging of key server operating systems, settings, programs and databases; and secure Web-based access to mission-critical business applications to ensure ongoing business operations from remote locations.

Conclusion

Today's businesses must adapt to extraordinary challenges to survive. It is the role of IT to enhance business adaptability by defining policy and selecting solutions that are the most flexible, responsive, comprehensive and cost-effective.



How Can I Learn More? Read other SonicWALL Whitepapers:

- Missing Link: A Security Strategy for Web 2.0 and Social Networking
- Missing Link: Taking Secure Access to the Next Level – Achieving Granular Control that Really Works
- Security Incite: Unified Threat Management and Next-Generation Network Security Platforms

Click here to opt-in to receive SonicWALL Newsletters

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an e-mail to feedback@sonicwall.com.

Forward to a Friend

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.