Proactive security – IT body armor against business attacks

WHITE PAPER

Why you should read this white paper

Defending against today's diverse array of security risks can be an enormous drain on corporate resources; especially for emerging and growing businesses which need to protect themselves against exactly the same threats as large scale enterprises, but with only a fraction of the IT resources.

This white paper will examine current risk landscape and explain how leveraging an integrated security solution can provide businesses with more complete protection than a collection of point solutions, and at only a fraction of the cost.

The evolution of malware

Securing the corporate network has never been more challenging than now. The malware industry has been commercialized and the writers of malicious code are no longer mischievous youths intent on simple random cyber-vandalism, but rather organized criminals intent on stealing money, personal and confidential information, or both. This for-profit motivation has served to drive an increase in both the sophistication and frequency of attacks and resulted in forms of malware that are far more difficult to defend against than the "script kiddie"-authored viruses of the past. In addition to dealing with more complex forms of attack, businesses must also contend with both perennial problems, such as spam, and newer risks, such as employee misuse of the Internet or non-compliance with corporate policy.

While the risk environment is constantly evolving, so too are IT requirements. Road warriors armed with the latest in mobile computing weaponry and laptop-packing executives and sales staff all demand anywhere-access 24/7, but providing that access creates new access points to the network – access points which bypass many traditional perimeter security solutions. Furthermore, mobile devices which are either unprotected or not effectively protected can carry threats into the corporate network, threatening both data integrity and business continuity. Accordingly, endpoint security has become as vital as perimeter security – but ensuring that mobile and frequently disconnected endpoints are secured can be extremely problematic.

Today's risk landscape

Today, businesses need to protect themselves against an increasingly diverse, progressively more sophisticated and rapidly evolving array of threats from both external and internal sources.

- **Ubiquity of the World Wide Web.** The Web has become the attack vector of choice and leads the SANS Institute's list of the "Top Ten Cyber Security Menaces for 2008"1. The vulnerabilities present in many Web browsers and Web browser plug-ins provide attackers with an extremely soft target. Web site attacks have also become more complex than previously and now attempt to exploit multiple vulnerabilities simultaneously while deploying sophisticated mechanisms to hide their malicious payload from security products. Furthermore, it is not only Web sites on the dark side of the Internet that pose a risk; legitimate Web sites are frequently hacked and configured to deliver hostile code. This is especially problematic as users often apply different security settings to trusted Web sites or are simply less cautious when visiting such sites.
- **Proliferation of Malware.** Malware has reached epidemic levels with more than 5 million new or variant strains being identified during 20072 – that is 4 million more than were discovered during 2006. Additionally, destructive viruses have been unseated as the number one threat by other stealthier, non-destructive forms of malware that support the criminals' objectives of stealing money and data.
- **Rise of Phishing.** Phishing attacks are becoming increasingly commonplace. According to Gartner, 3.6 million people lost a total of $3 billion to phishing scams during the 12 months up to August 20073. Consumers are not the only targets of phishing attacks, organizations are being attacked with increasing frequency too. In specifically targeted ("spear phishing") attacks, publicly available information is used to create emails that appear highly credible but which carry a malicious payload. In 2006, the US State Department's network was compromised by malicious

code contained in an attachment to a spear phishing email4. While attacks on large enterprises and government departments attract the most publicity, smaller businesses are equally at risk as they are often perceived as softer targets by criminals.

- **Lost productivity and network resources.** Spam has become a global pandemic that cost businesses $100 billion in 20075. In the past, spam was used as a marketing tool by small-time rogues; now, it is used by organized criminals to perpetrate complex pump-and-dump scams6 that can net them millions of dollars.
- **The breakdown of the network perimter.** Laptops and mobile computing devices have become a real headache for the IT department and were listed as the leading security concern by attendees of the 2007 InfoSecurity Europe conference7. Enforcing security policy on mobile devices can be difficult and, consequently, such devices may not be effectively secured – which can enable them to act as vectors that carry malware inside the corporate network in a manner that completely bypasses traditional perimeter security solutions.
- **The threat within.** Employee abuse of the Internet has become a major problem for many businesses. In the UK, it has been estimated that the productivity lost as a result of employees using social networking sites, such as Facebook, during working hours costs businesses £6.5 billion8 – or just under $13 billion US – and that visits to such sites consume about 20% of their bandwidth. Add to that the time spent on sites such as eBay and general surfing, and the costs become even more substantial. Compounding the problem is the fact that social networking sites do have valid business uses and so a blanket ban simply may not be an option.

While attacks are becoming increasingly frequent and sophisticated, they are also becoming increasingly interconnected. Information posted to social networking sites is harvested for use in spear phishing campaigns > the malicious code delivered by spear phishing emails co-opts computers into botnets9 (networks of compromised computers that are remotely controlled and used for criminal purposes without the knowledge or consent of the owners of those computers) > the botnets are used to send out spam that carries a malicious payload or links to malicious Web sites > other computers are infected, co-opted into botnets and used to send pump-and-dump spam, launch denial-of-service attacks10, send out phishing emails and distribute yet more malware.

The real problem facing businesses today is not so much how to defend against this diverse array of threats – there are products available that address each security concern - but how to defend against them in a cost-effective manner.

The problem with point solutions

Products that address a single aspect of IT security (“point solutions”) such as intrusion detection and prevention systems (IDSs and IPSs), antivirus products, web and spam filters and plethora of other similar products that perform essential functions – but can also lead to a security infrastructure that has an extremely high support overhead. Each point solution represents another application that must be installed, configured, updated and maintained; each represents another vendor relationship that must be managed; each adds an additional tier of complexity that makes troubleshooting more challenging; and each represents another application which IT staff may need to be trained to use. Furthermore, because point solutions result in a complex architecture, the chances of human error increase – and that can lead to security holes being unintentionally introduced.

In short, while point solutions can certainly be effective, they are also likely to have an extremely high total cost of ownership (TCO).

BitDefender Business: enhancing security and lowering the TCO

BitDefender Business has been designed from the ground up to put comprehensive, world-class security at the lowest possible TCO.

- **Low TCO driven by improved productivity.** The acquisition costs of a security product account for much less of its TCO than the ongoing management and support costs. BitDefender Business has been architected to make management as easy and streamlined as possible and, accordingly, has an extremely low TCO.

  - ✓ **Security policies.** BitDefender Management Server includes a series of security policies that can be easily and speedily implemented using the built-in customizable templates. The policies can be used to control every aspect of BitDefender's behaviour including the setting of update schedules, antimalware scam schedules, firewall settings, antispam settings and to specify the response to any security or compliance event. BitDefender's offline policies enable administrators to ensure that computers continue to comply with policy even when disconnected from the network and not communicating with the Management Server. BitDefender can also be configured to automatically enforce policy on any computer connecting to the network by, for example, automatically installing BitDefender's client-side module on the computer, and to block the computer until it reaches a state of compliance.
  - ✓ **Integration with Active Directory (AD).** Groups created in AD can be replicated in the BitDefender Management Server and customized policies applied to each Group enabling a business to fully leverage its investment in the existing network architecture.
  - ✓ **Centralized management.** BitDefender's centralized management console save administrators time by enabling each BitDefender module to be controlled from a single location.

  BitDefender's streamlined management enables it to offer an extremely low TCO driven by improved administrator productivity.

- **Comprehensive integrated protection.** BitDefender removes the cost and complexity associated with maintaining multiple point products by integrating protection from viruses, Trojans, rootkits, spyware, spam, phishing scams, zero-day attacks and other threats into a single, easily managed solution.

  Additionally, BitDefender also enables businesses to guard against employee Internet abuse by setting rules to limit or block access to applications or Web sites that are known to be a security or productivity risk (instant messenger applications and social networking sites, for example). BitDefender is highly configurable and enables a business to choose whether to block an application or site completely or to restrict its use to certain hours or to certain Groups.

- **Scalability.** While some solutions become impractical when a large number of computers are managed due to delays in client-server communication, the one-way HTTP-based communication used by BitDefender requires only minimal network resources. BitDefender can, therefore, continue to meet the needs of a growing business and allow existing expertise to be leveraged.

- **World-class security.** BitDefender offers rock solid, industry-leading security. BitDefender products are ICSA and Checkmark certified and have received numerous VB100 awards. Additionally, BitDefender has one of the fastest response times to new threats in the industry.

Summary

Faced with a constantly shifting and rapidly evolving risk landscape, many organizations are finding that their security infrastructures are becoming increasingly difficult and increasingly expensive to manage.

BitDefender Business helps organizations simplify their security infrastructures by consolidating virus, malware, spam, phishing and firewall protection to a single, centrally managed point. By streamlining management in this manner, BitDefender Business can save an organization both time and money. Furthermore, by enabling organizations to enforce policy on frequently disconnected mobile devices, BitDefender Business helps organizations overcome one of today's most challenging security problems: securing their end points.

Most importantly, an organization deploying BitDefender Business can enjoy the peace of mind of knowing that their network is comprehensively protected by one of BitDefender's industry-leading security solutions.

About BitDefender

BitDefender is the creator of one of the industry's fastest and most effective lines of internationally certified security software. Since our inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe—giving them the peace of mind of knowing that their digital experiences will be secure. BitDefender solutions are distributed by a global network of value-added distribution and reseller partners in more than 100 countries worldwide.

More information is available at www.bitdefender.com.

References

[1]Top Ten Cyber Security Menaces for 2008
http://www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10__Cyber_Security_Menaces_-_2008&ref=22218

[2]Quantity of malware booms
http://www.heise-security.co.uk/news/101764/from/atom10

[3]Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks
http://www.gartner.com/it/page.jsp?id=565125

[4]House Committee on Homeland Security Subcommittee on Emerging Threats, Cyber Security, and Science and Technology (statement of Donald R. Reid, Bureau of Diplomatic Security)
http://homeland.house.gov/SiteDocuments/20070419153111-10569.pdf

[5]Industry Statistics (Ferris Research)
http://www.ferris.com/research-library/industry-statistics/

[6]Microcap stock fraud
http://en.wikipedia.org/wiki/Microcap_stock_fraud

[7]Security's Top Five Priorities
http://www.darkreading.com/document.asp?doc_id=123294

[8]UK takes £6.5bn hit from Facebook & company
http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2008/01/22/bcnface122.xml

[9]Botnet
http://en.wikipedia.org/wiki/Botnet

[10]Denial-of-service attack
http://en.wikipedia.org/wiki/Denial-of-service_attack