

Free yourself to do more, while securing your business simply and cost-effectively

Jonathan Tait, Product Marketing Manager

In tough economic times, with tightened budgets and heightened competition, it's vital for businesses to secure their systems and data against a growing field of threats. However, implementing and maintaining full-spectrum protection can be a heavy drain on financial and human resources if not done right.

A more efficient approach to security means that resources – both human and physical – are freed up to improve and expand other areas. The end result is your business becomes more efficient, flexible and profitable.

Free yourself to do more, while securing your business simply and cost-effectively

Overview

As a result of the economic downturn, hard pressed IT departments must face up to their various pressing security needs with ever tighter budgets. And if those numbers aren't frightening enough, IT faces other numbers that are equally as stark.

A new infected webpage crops up every 4.5 seconds. 2008 saw malicious email attachment increase five-fold. New spam-related webpages arise every 15 seconds. And, to top it off, 97 percent of business email is spam.

Yes, malware is back.

Once a pest likely to cause high-profile damage but manageable with sensible desktop protection and safe backup policies, malware has become increasingly sophisticated, devious and stealthy while growing from a pattern of sporadic spikes to a constant deluge of new and unusual attacks (see the chart at right).

Yet workers need access to email and the internet to carry out their business efficiently. They need to move data around fast on USB sticks and other writeable media and as mobility increases they also need remote access to corporate networks from laptops and smart phones. These requirements all present serious threats of accidental leakage or deliberate siphoning off by malicious cybercriminals.

Legislation and regulation of corporate IT use, including rules on accountability, disclosure and secure data handling, are designed to ensure a safer environment, but compliance adds an extra weight to already strained security teams.

Malware becomes a more sophisticated and growing threat

- » Sophos uncovers a new infected webpage every 4.5 seconds
- » There were five-times more malicious email attachments at the end of 2008 than at the beginning
- » Sophos discovers one new spam-related webpage every 15 seconds
- » Ninety-seven percent of business email is spam

Source: Sophos Security Threat Report: 2009

There are as many ways of securing a business as there are security vendors showing off approaches to protecting data, systems and networks. It may be tempting to invest in a multi-layered, multi-provider, multi-product approach, attempt to protect against each separate danger with a specific and targeted solution.

However, that approach comes with unanticipated costs to the implementer, with greatly increased requirements in terms of expertise, training, support, maintenance time and effort. Worst of all, disconnected thinking can also leave unexpected gaps in protection.

IT managers cannot afford to soak up the extra costs in equipment, licensing and manpower imposed by an ill-fitting, disparate array of protection solutions. A streamlined, unified approach may well provide excellent savings as well as greatly improved security.

The growing demands of security

In the last five years, the traditional image of the virus writer as a lonely geek aiming for fame by infecting as widely as possible, or causing maximum damage, has become a thing of the past.

The modern malware creator is a highly driven, often highly skilled programmer, whose work is commissioned and put to use by organised criminal gangs. The goal of malware is money, not recognition, and stealth is highly prized. The methods and techniques for making malware pay expand and evolve at a rapid pace, with the more general risks of infected systems being absorbed into botnets for use in spam campaigns and DDoS attacks, draining bandwidth and resources, supplemented by the more personal dangers of data theft.



The web is under constant bombardment from hackers probing for vulnerabilities in software



Phishing techniques have evolved along similar lines, from simple and generally easily-spotted requests for online banking passwords to subtler, more insidious methods, sometimes personally crafted to penetrate a specific organization and gain access to systems and data. The web is under constant bombardment from hackers probing for vulnerabilities in software or website coding that will allow them to insert their own malcode or extract information from databases supposed to be kept private. At the same time, the black market in credit card and bank login information is booming.

The worldwide recession has only increased the output and sophistication of the attackers. Decreasing salaries and increasing unemployment in high-tech industries has made a move to the criminal underworld ever more appealing for talented programmers.

Meanwhile, the increasing mobility of workers and their data has led to a string of public failures to maintain data security, with tales of sensitive information contained on USB sticks or laptops being lost in the post, left on public transport or sold on eBay seeming to crop up almost every day. The need for encryption and data protection cannot be overstated—the damage to a business when customers learn their credit card data has been exposed on their website or left on a train is irreversible. With a public increasingly aware of the value of their personal data, and made more than usually money-conscious by the economic downturn, trust and reputation are critical to acquiring and retaining customers, and nothing dents a reputation like a public and embarrassing security leak. Sensitive corporate data also has a high value in the wrong hands, and is becoming an ever more highly prized target for today's data thieves.

Governments, themselves not unfamiliar with the embarrassment of data leaks, are increasingly tightening regulations regarding data management, and most businesses will be affected in some way by rules on handling customer information, particularly when it comes to financial details. Compliance with regulations requires securing of all vectors for the introduction of malware and the leakage of information, including all operating systems regardless of the perceived malware risk. Maintaining and proving compliance on diverse systems can add a considerable burden to the workload of IT departments and security administrators, even before any incident has occurred.

When a corporate network has been penetrated by malware, there is even more to do. In the wake of an attack, a company must do several things: pin down and isolate the infection vector, remove the malcode and its activities. Then it must assess the potential impact the infection may have had. And it must do all of this in excruciating detail.

The specific flaw in policy or protection that gave the infection access must be identified and fixed, which in a diverse environment running a range of security software can be no easy task. In the case of data loss, similar investigations must find the loss vector and the associated risk, find out what data may have been exposed and, if encryption is employed, whether encryption remains secure.

Once the failing layer has been spotted, the appropriate people must be contacted to provide support and fix any problems. Many of these tasks will be beyond the skills and resources of all but the biggest and most highly-trained of security teams. Often, it's best delegated to security providers, but when running a range of solutions for different vectors it is not always easy to know which of the range of providers to hand it off to.

The growing costs of security enforcement

IT managers are presented with a bewildering spectrum of requirements in the security arena. Gateways, servers and desktops must be protected from malware infestation and hacker penetration while maintaining required levels of performance. Mail streams must be filtered to remove time-wasting spam, dangerous attachments and social engineering con tricks, but the flow of business-critical communication must not be impeded. Remote devices must be allowed access to networks, but not if they belong to untrusted users. Users need access to online information and resources, but must be shielded from malicious sites. Corporate and customer information must be encrypted and stored safely, with access easily available to those who need it but with the risk of leakage or exfiltration tightly controlled. All these areas need monitoring and managing, ensuring continuous and universal implementation and operation, as well as the application of updates and patches.

Alongside all these balancing acts is another challenging two-edged sword, weighing the investment in acquiring security solutions against the additional, often unforeseen costs. When selecting a security solution, it is tempting to fixate on two clear, but generally contradictory, criteria: performance and purchase price. Considering only which solution will cover a threat vector most effectively, or which will patch it for the lowest initial outlay, ignores a wide swathe of other, equally vital criteria.

The market for security products grows in parallel with the expansion of cyber threats. New start-ups with bright ideas push forward revolutionary new products, while the incumbent giants of the security world roll out new improved versions of their desktop suites, more modules for their corporate UTMs, more complex catch-all appliances. Specialists pronounce themselves "best of breed" in every arena; anti-spyware product makers belittle the abilities of traditional anti-virus vendors to cope with a slightly different breed of desktop danger. Firewall makers produce ever more complicated and bewildering sets of options to block, mangle or filter incoming and outgoing connections, while NAC vendors promise absolute exclusion of unwanted or untrusted systems from corporate networks. Data leak prevention firms promise to parse the most complex encryption to ensure data cannot be extracted from a protected network, while encryption firms boast of unbreakable, "military grade" data protection. From amidst this seething sea of offerings, IT managers must pick the arsenal with which they will keep their companies safe and secure.

Security solutions can get a bad reputation with users, interrupting their workflow, slowing down machines, blocking vital access to information. Slowing down the workforce of course raises running costs, as less gets done in more time. Emails lost in spam filters can mean lost business, and can have even more serious legal consequences. Users need to be trained to interact properly with their security software—to check email quarantines, to allow anti-malware updates on their remote devices, to ensure sensitive data is not stored or transferred without proper encryption, not to try to bypass web protection, and to learn divergent methods for interoperating with diverse protection layers can hit training budgets hard. Security policies and solutions require company-wide user acceptance, with users taking responsibility for their part in the security effort, but persuading people to make do with awkward requirements, navigate ill-fitting product combinations or put up with resource-hogging filters can add an extra burden of pain to IT departments, over and above the loss to the company in worker productivity.



The security of an organization, the safety of its systems, users and data, must be treated holistically as a single goal.



Multiple layers of protection covering the multitude of infection and data loss vectors can also, of course, have a heavy impact on IT teams themselves. Simply sourcing a selection of appropriate products can take up time and money, while training admins to properly install, configure and maintain a wide range of solutions can be hugely expensive. Dealing with different interface designs, updating, patching and reporting systems, maintaining support contracts and keeping track of support handlers, ensuring policies are implemented coherently without unnecessary overlaps or dangerous gaps, each task multiplies in

complexity with each additional solution provider in a mixed, multi-layered security approach. With IT budgets frozen or even shrinking as competition for business grows and revenues decline, all this additional time and effort takes an ever heavier toll on dwindling resources, while demands increase and the potential cost of a security incident becomes ever more serious. For enterprises to thrive in difficult times, IT teams need to be dedicating their time to projects and initiatives that will add value to the business - they cannot afford to waste money and effort fighting security fires with expensive and inefficient techniques.

The simple solution

For a business to achieve optimum performance, it cannot be shackled by complex and awkward security processes, but similarly cannot leave itself exposed to danger. For IT managers to ensure all potential security risks are mitigated, they cannot afford simply to opt for the solution with the lowest purchase price to cover each separate need, yet likewise cannot afford an expensive, inflexible and unwieldy modular approach lacking in joined-up thinking. The security of an organization, the safety of its systems, users and data, must be treated holistically as a single goal. To achieve this goal, a single provider who can cover all security requirements in a simple and unified manner, and can deliver the expertise to get it implemented and set up with minimum burden to the IT department, provides the ideal solution.

The essential areas required for a complete and robust protection policy at the desktop level are anti-malware protection with strong proactive elements, on all platforms, along with firewalling, intrusion prevention, network access control, data leak prevention and comprehensive data encryption, all supported by central management and reporting. To have these all handled from a unified system, and supplemented by gateway-

level mail and web filtering, minimises rollout and administration time and energy, and also, thanks to sharing of resources between functions, reduces performance impact perceived by end users and across networks.

By choosing a single security provider to cover every vector, efficiencies can be made across the board. Acquisition, licensing and support arrangements can be made in a single swoop, freeing up time and budget for strategic requirements. Deployment and monitoring of protection for all environments and platforms, enforcement of policies across sites and networks, and incident reporting from all layers of protection can be managed in a joined up way, allowing compliance with internal and external requirements to be easily measured and proven.

Streamlined and uniform design and implementation provide ease of use and reduce the need for multiple, expensively trained in-house experts in a range of products. Access to training and quality, expert support for all protective layers from a single point of contact minimises costs and avoids expensive organisational and logistical requirements imposed by multiple providers, while expertise in multiple threats and threat vectors provides access to informed handling of potential issues in whatever form they arise without the need to analyse the issue internally, with all the associated costs. Multi-skilled expert teams who can look at the needs of a business holistically can provide proactive protection against new threats, and even entirely new threat vectors, relieving IT departments of the burden of keeping ahead of the latest dangers, as well as the hassle and potentially more serious side-effects of a security breach.

A provider that can fit all these requirements can fulfil the need for a complete and comprehensive security policy, and can guarantee to reduce costs into the bargain.

Boston, USA | Oxford, UK
© Copyright 2009. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any
form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM