

# Mind the gap: the integrated multi-tier solution to malicious content

A Sophos white paper

July 2005

There is a widespread belief that the most effective way for an organization to secure its network is to protect it with software from more than one vendor. However, the increasingly complex nature of today's fast-moving threats radically changes the criteria for defense and demands an integrated, multi-tier approach to threat management. This paper demonstrates how the cross-threat expertise in SophosLabs™ and its agility in responding to new malware and spam campaigns makes Sophos uniquely able to integrate the management of all threats, no matter what their provenance or method of spreading.

## The challenge of the accelerating threat

Since the arrival in 1986 of the first PC virus, Brain, which infected a PC's boot sector, the threat landscape has changed enormously and at an ever-accelerating rate. Boot sector viruses were followed by other types of virus, like those that targeted executable files and mutating polymorphic viruses. Then macro viruses that infected Microsoft Office files put things on a whole new footing, in terms of both number and spread. Things sped up even more with the emergence of the first email-aware viruses – Melissa in 1999 and the Lovebug in 2000 – which caused meltdown of unprotected networks as email systems collapsed under the sheer weight of traffic. And then spam entered the scene, bringing all kinds of other new threats in its wake.

The number of new threats has continued to grow at rates originally believed to be unsustainable. In fact today, the rate at which new threats are appearing is increasing and Sophos Anti-Virus now identifies over 100,000 different viruses, as shown in figure 1.

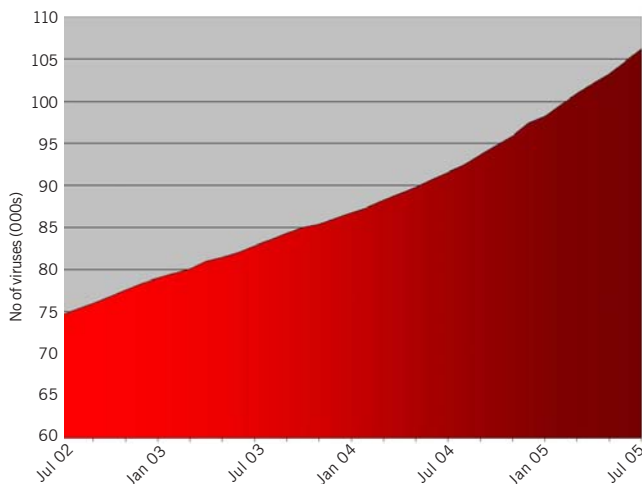


Figure 1: Increase in viruses July 2002–July 2005

A major challenge for those charged with protecting corporate networks is that both the threats against which they are defending and the networks that they are protecting change at ever increasing rates. Until now it has been common practice to address different parts of the problem with products from different vendors. However, this approach is becoming inadequate and holes in defense strategies are emerging.

---

*"Organizations that have tried to build best of breed security strategies have often found their heterogeneous environment less than helpful. For some, it has been an IT fiasco managing multiple vendor products."*

Chris Christiansen, IDC VP of Security Products,  
June 2005

---

## New and evolving dangers

Today the term "virus" is applied to an increasingly broad range of threats, evolving from its original meaning to cover worms and Trojan horses. New terms have also emerged, such as "spyware", "dialer", "keylogger" – most of which would previously have come under the umbrella term of "Trojan".

Spam, once simply an irritant, a form of unwanted advertising that cluttered up email systems, has at the same time evolved into an ever more sophisticated threat to security. Phishing attacks were originally a subset of spam, using scare tactics to trick victims into handing over sensitive information. Now, as well as their psychological techniques, they make use of Trojans, worms and viruses to install keyloggers and other

forms of spyware, silently gathering users' access codes and passwords, and scanning hard drives and networks for sensitive information. This data is then transmitted to third parties over the internet, granting them easy access to the identities and finances of their unsuspecting victims. Similarly "dialers", which surreptitiously connect to premium-rate phone numbers and add huge costs to the infected users' phone bills, are generally delivered in the form of a Trojan masquerading as something desirable to trick users into running it on their systems.

The emergence of these financially motivated attacks escalates the issue of computer security considerably, with yesterday's cyber vandals becoming today's cyber criminals. Where before viruses were mostly the work of hobbyists, the lure of money has brought increasing organization and sophistication to the business of infiltrating other people's computers and networks and the convergence of the virus and spam threat makes the need for integrated protection imperative.

---

*The convergence of the virus and spam threat makes the need for integrated protection imperative.*

---

## Going global in seconds

Not only are the quantity and variety of threats on the rise, the speed with which new attacks spread has also greatly increased. Exploits, taking advantage of software flaws, can spread without human intervention, allowing internet worms like Blaster and Slammer, which made use of vulnerabilities in Windows operating systems or Windows applications, to infect hundreds of thousands of machines worldwide in under an hour.

Insufficiently protected computers are coming under attack in shorter timescales than ever before. Sophos research shows that connecting an unprotected, unpatched machine to the internet leads to a 50% risk of infection within about 10 minutes, rising to a 90% chance after 45 minutes (see figure 2). There is not even time to download and install patches or firewalls.

This instant infection problem does not apply directly to corporate users, where network firewalls are in place. However, the internet is awash with scanners searching for vulnerable systems to infect, and the "always-on" broadband-using computers of home users are a ready target. They are increasingly hijacked – without their owners' knowledge – and used to launch a range of attacks against corporate users. These are the "zombie networks" used (and sold) to evade the anti-spam filters that rely on identifying suspicious source addresses or high-volume email campaigns.

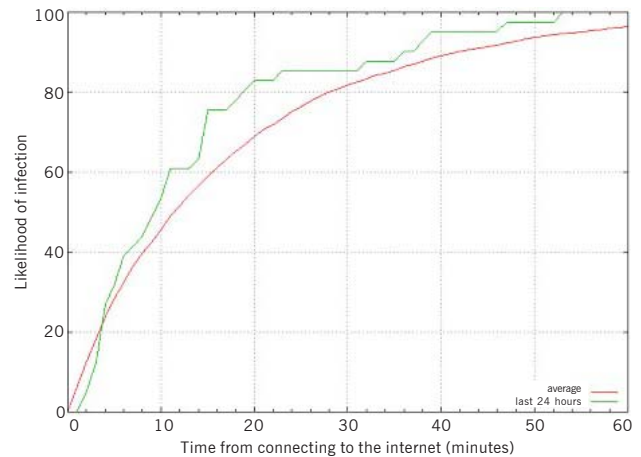


Figure 2: Distribution of infection times

## Communication out of control

As well as the growing diversity and sophistication of threats, there is explosive growth in the variety of communication routes they use, as shown in figure 3. This results from the increasing complexity of demands being placed on IT systems, demands for mobility, flexibility, and interoperability between different hardware and software.

Traditionally, email has been the principal means of infiltrating malicious content onto target systems. This has led those concerned with security to concentrate heavily on email gateway-based protection. While this remains a key part of any protection system, it offers no protection against other communication routes.

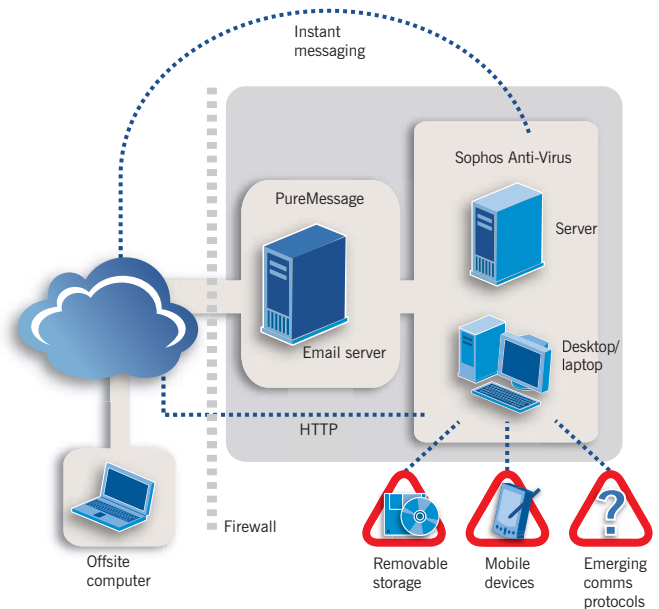


Figure 3: The diversity of threat entry points

Today malicious content is just as likely to enter an organization through web downloads, or instant messaging (IM) applications like AIM and Skype – whether authorized or not. Indeed IM applications are often designed to circumvent corporate security systems, and are extremely difficult to monitor or regulate. Most organizations that believe they have no instant messaging on their network, simply have not checked. Today's IM applications allow the transfer of files in and out of organizations, and where an organization has imposed strict security restrictions on its email, it is often senior executives who are switching to IM for convenience.

On top of the changing communications networks, an ever-expanding number of devices are capable of transferring files across many different protocols, without client software or even physical connection. Controlling every CD, USB storage device, memory card, smartphone and MP3 player that comes near corporate computers, wherever they are, is almost impossible, yet these are all potential entry points for malicious content. Neither is it feasible to filter traffic at each and every route through the perimeter. Desktop, or endpoint, protection has never been more important than it is today. For truly effective protection the endpoint and gateway protection must work together.

---

*New hybrid threats exploit the fragmented responsibility for protection and leave the business network open to gaps in its defense*

---

## The multi-tier arsenal

The need for multiple layers of defense to protect against malicious content is broadly accepted. The danger, however, is that there can be gaps in the defense structure, not as a result of individual product limitations, but due to the common practice of addressing malicious content as a series of distinct problems. Attackers do not categorize their attacks into neat buckets; consequently defenders do not have that luxury either.

### *Bofra's exploitation of security gaps*

Today's hybrid threats do not always lend themselves to easy categorization in terms of "virus" or "spam". Bofra, for example, which arrived in November 2004, illustrates the difficulty and danger of organizing defense along categorizations that are no longer valid. Bofra is a mass-mailing virus with a difference. Rather than simply emailing copies of itself to harvested addresses, it sends an email that contains a link to a web server which is running on the sender's computer and which contains malicious code. The

sequence of its actions can be summarized as follows:

- 1 Create a web server on a newly infected computer
- 2 Harvest email addresses from the infected computer
- 3 Send the harvested addresses an email with a link to the web server
- 4 Recipient opens email on uninfected computer and clicks on link (purporting to contain adult content)
- 5 Link exploits Internet Explorer IFrame vulnerability to infect the computer and create a web server...

... and so the process of infection continues.

Technically Bofra is a worm, but what matters is that it is stopped, not how it is labeled. Email gateway anti-virus solutions are ineffective against Bofra, because the virus is not in the email. The email just contains a link. However, the email sent by Bofra exhibits a number of spam characteristics – indeed Sophos provided early protection through Sophos PureMessage's spam filters.

So whose responsibility is it to protect an organization against Bofra? The anti-virus team? The email team? The web team? Patch management?...

## Exploding the myth

Most organizations structure their defense along these artificial boundaries, complicating responsibilities and leaving themselves dangerously exposed to threats which exploit this fragmented approach. The commonly held myth that the best way to protect these boundaries with different vendors' products is outmoded. Not only is this multi-vendor approach costly in terms of both money and administrative overhead, but more importantly it provides weaker protection.

A much surer defense comes from viewing the problem as a whole. By drawing on the comprehensive anti-virus and anti-spam detection capabilities from Sophos, which has a high degree of visibility into the full range of new and emerging threats, an organization greatly increases its protection. Point applications that target only parts of the problem cannot provide this level of protection.

---

*The pooled expertise and interconnected technology within SophosLabs enable its highly skilled experts to respond rapidly and effectively to emerging threats, no matter what combination of techniques is used to help them spread.*

---

As the malicious content problem evolves along several dimensions at once, it is essential that an integrated, multi-

dimensional approach is taken to protection. It is time to move from the disjointed protection shown in figure 4a to the integrated threat management of figure 4b. Only in this way can the unpredictability of the spam:virus dilemma be nailed.

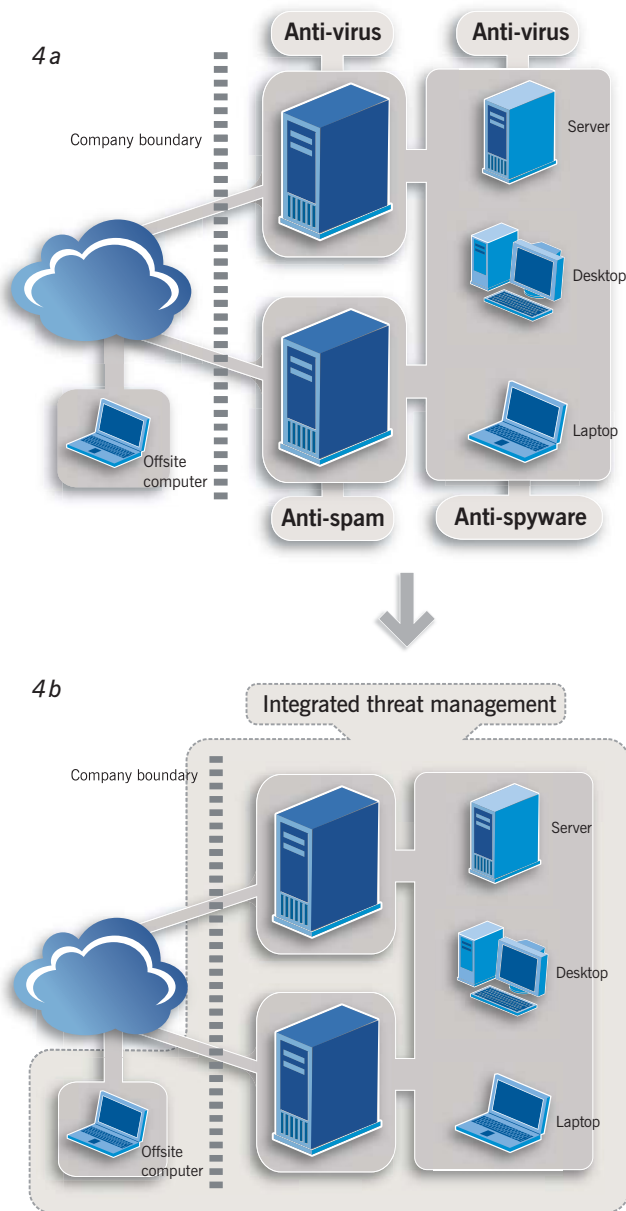


Figure 4: The all-embracing protection of integrated threat management

## Sophos's integrated threat management

With 20 years' experience in defending against threats, Sophos has intimate knowledge and expertise in protecting organizations against all types of malicious content. Our

products have been designed and developed in-house to provide consolidated protection at potential threat entry points. Bofra, for example, is stopped in its tracks by spam filters at the gateway and by anti-virus detection at the desktop/laptop before the web download can be executed.

## SophosLabs

SophosLabs™ – a network of threat analysis centers, strategically placed around the world – combines expertise in both malware and email analysis to ensure that the full range of detection capabilities can be applied to any new threat. Innovative techniques build on Sophos's established early detection and high-quality protection. Genotype™ technology in both the Sophos virus detection engine and anti-spam engine provides preemptive protection against new threats even before they emerge, closing the window of vulnerability that exists between a new threat emerging and signature-based detection being available.

Through its global visibility and a unique combination of cross-threat expertise and powerful integrated technologies, SophosLabs provides the 24/7 research and rapid response that organizations need to protect them from increasingly complex threats. (For more information, see the Sophos white paper, *Sophos Labs: integrated day zero protection in a rapidly changing threatscape* at [www.sophos.com/virusinfo/whitepapers](http://www.sophos.com/virusinfo/whitepapers))

---

*"Sophos is providing a unified solution that consolidates robust protection across all the vulnerable tiers so users can avoid the expense and uncertainty of integrating a range of solutions from different vendors."*

Chris Christiansen, IDC VP of Security Products,  
June 2005

---

## Gateway/email protection – Sophos PureMessage

Sophos PureMessage™ provides comprehensive, flexible email management at the gateway. It blocks up to 98% of spam in multiple language streams and scans all mail, detecting and disinfecting viruses, Trojans, worms and spyware. Threat reduction technology blocks new threats, such as email-aware worms, even before specific detection is available. In addition to malicious content detection and elimination, PureMessage offers the capability to implement sophisticated email routing policies, to match virtually any requirements and ensure compliance with the growing complexity of government regulations. The software is automatically updated over the internet with the latest virus detection files and spam rules.

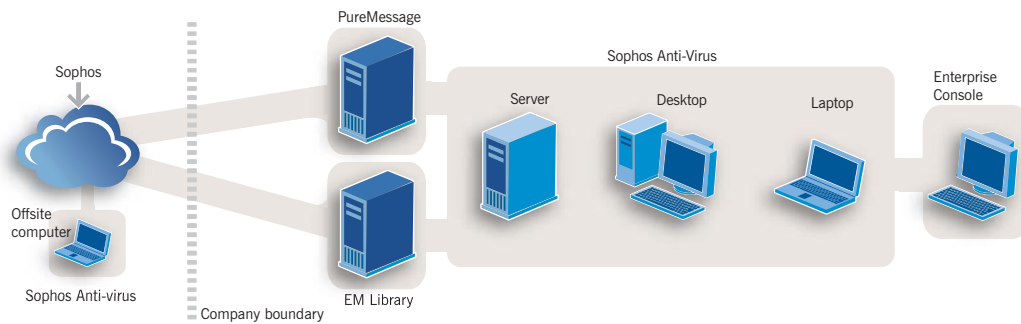


Figure 5: Integrated threat management from Sophos

### Managed endpoint security – Sophos Anti-Virus

Sophos Anti-Virus™ detects and disinfects viruses, Trojans, worms and spyware on file servers, desktops and laptops on a wide range of platforms. Along with powerful technologies within the Sophos virus detection engine, it incorporates sophisticated management tools including EM Library™ and Enterprise Console™. EM Library automatically installs and updates Sophos Anti-Virus across the network. Enterprise Console gives the administrator complete control, enabling the centralized setting of configuration and updating policies for Sophos Anti-Virus across the whole network (including remote computers), displaying the status of the software on all computers, and producing reports on all virus activity.

### Support infrastructure

Underpinning every Sophos license is Sophos's automated update system to ensure that updates are delivered to both desktop and gateway as quickly as possible.

All licenses also include 24/7 customer telephone support and are built on Sophos's core values of meeting corporate needs for reliable, robust solutions to real-world problems.

### Summary

The distinction between different types of threat is no longer always clear and handling the threats and the threat entry points as separate problems will leave gaps in network security. The cost and administrative overhead of having different vendors' products at the gateway and endpoint is very real and Sophos's cross-threat expertise makes this approach unnecessary. Two decades' experience, skilled research capability, and powerful technologies allow Sophos to respond rapidly and reliably to emerging threats and give it a unique ability to provide an integrated solution to the growing problems organizations face from malicious content.

*To find out more about Sophos and how our products can protect your organization, visit [www.sophos.com](http://www.sophos.com).*