

Why Linux threats mean business

A Sophos positioning paper

March 2006

Linux is expanding rapidly beyond its traditional base of enthusiasts, finding rising popularity as a server platform for corporations. This paper highlights the threat to businesses caused by the interaction of unprotected Linux computers with Windows and other platforms. The paper also discusses the vulnerability of mixed IT environments to the range of increasingly complex threats. It concludes with an explanation of how Sophos Anti-Virus® meets the technical challenges of protecting Linux, drawing on Sophos's multi-platform expertise to offer uninterrupted, integrated threat management across the entire network.

An evolving tool for business

The Linux operating system has come a long way since Linus Torvalds released the first version of the Linux kernel, or "core" of the operating system in 1991. The open source rules under which all Linux kernels are released have led to constant and enthusiastic development, resulting in many useful applications for public use.

Linux is no longer the sole preserve of a community of dedicated users – it is being adopted with equal enthusiasm by major corporations. The management tools, support packages and service offered by mainstream Linux distributors such as Red Hat, SUSE and TurboLinux have made Linux far more accessible to businesses. Linux is proving to be a popular commercial tool, and is increasingly used on servers for mainstream applications such as email, web, file and print sharing.

Uptake of Linux on enterprise networks is widely anticipated to continue growing over the next few years. According to analysts IDC, the overall marketplace revenues for server and PC hardware and packaged software on Linux will reach \$35.7 billion by 2008.¹

Uptake of Linux on enterprise networks is widely anticipated to continue growing over the next few years.

Deployment, however, is likely to remain focused at the server level. Linux is now being used on desktops and even laptops, but most organizations prefer a multi-platform solution, using Linux and either Windows or Mac on clients. From a security perspective, Linux has historically been seen as a harder to

use, yet safer, platform than Windows and other systems. However, the growing use of commercially supported Linux in corporate, government and education networks carries significant security implications.

The threat to organizations

Windows viruses can hide on unprotected Linux computers and spread to the rest of the organization when the two systems interact, causing significant damage. Windows viruses on Linux servers can also be sent to networks in other enterprises. Infecting other companies with viruses not only damages the sender organization's reputation and credibility, but can also expose it to legal liability. Propagation of malicious code to and from Linux-based systems occurs through commonly used mail and web protocols, as well as network shares such as Samba and NFS.

Windows viruses can remain hidden on unprotected Linux computers and spread to the rest of the organization.

An area of intense debate is the question of how susceptible Linux computers themselves are to malware, since the overwhelming majority of viruses, worms, spyware and Trojans target Windows systems. This is primarily because of Microsoft's market dominance. As Linux continues its growth as a mainstream operating system, it will inevitably take a greater share of the attention of virus writers – particularly those motivated by financial gain – with access to the wealth of Linux code and information freely available on the web.

Finally, using multiple operating systems increases the complexity of the IT structure. This risks opening gaps in

network defenses at a time when threats are infiltrating businesses in increasingly complex ways – a recent example is Bofra, a threat with blended characteristics of worms, viruses and spam. As more networks migrate to Linux, it will be increasingly important that their anti-virus software forms part of an integrated solution that can provide a reliable umbrella of protection across all tiers and platforms.

Issues with protecting Linux

The complexity of the threat facing multi-platform environments is compounded by the engineering challenges of providing reliable protection for Linux computers. There are three main issues: on-access scanning, quantity of kernels, and customization.

On-access scanning

On-demand and scheduled virus scanning are no longer enough to provide security for Linux computers – today's threats can propagate across a network as soon as an infected file is accessed, either by user action or by low-level functions within the operating system. This makes on-access scanning of files vital. However, providing on-access scanning for Linux has historically been a complex and cumbersome task, since the anti-virus software must directly plug in to the kernel software in order to intercept file system operations.

Threats can propagate across a network from a Linux computer as soon as an infected file is accessed.

The solution is a tool known variously as a file intercepting module, extension, interface, or hooking mechanism. There are open source file intercepting modules available for Linux, which are often incorporated into anti-virus software. However, while these file intercepting modules are useful and flexible tools, they can have limitations in terms of reliability and performance – for example, an inability to scan multiple distributed file systems such as LSM, Syscall and VFS.

Quantity of kernels

There are many distributors of Linux, often offering more than one version of their product. For example, a distributor may release several home and professional distributions. These distributions are periodically updated with new features or to correct security and stability issues. Providing anti-virus software support for such a large number of updated kernel versions is a complex challenge. Many anti-virus vendors struggle to keep pace, choosing to ignore interim patches or updates and waiting for a major kernel update before investing the resources in supporting it – this is clearly unacceptably disruptive in the corporate environment.

Customization

One of the many benefits of the Linux operating system is the ease with which it can be adapted and modified to suit specific network environments. Some organizations, for example, customize kernels for use with their own in-house applications. However, this makes it impractical or even impossible for many anti-virus vendors to continue supporting them.

The Sophos solution

Sophos Anti-Virus for Linux is built on 20 years of experience in providing multi-platform protection – Sophos was the first security company to offer protection for UNIX users. Sophos Anti-Virus for Linux has been engineered to provide complex, multi-platform networks with reliable protection, addressing the engineering and security management challenges posed by Linux:

- Sophos Anti-Virus for Linux incorporates a uniquely designed file intercepting module which provides high-performance, low impact on-access scanning. Sophos Anti-Virus for Linux sets new standards for speed, reliability, stability, and scalability. It also systematically scans multiple distributed file systems, ensuring comprehensive protection for networks.
- On-access scanning in Sophos Anti-Virus for Linux is powered by Decision Caching™ technology that provides high-speed performance by scanning only those files that have changed since last accessed.
- Sophos supports a wide range of Linux distributions and kernel versions. Whenever a Sophos-supported distributor releases a new kernel version, Sophos Anti-Virus is updated to support it and this update is automatically downloaded to the network.
- Sophos Anti-Virus for Linux can recompile automatically to remain compatible with the kernel whenever the kernel is updated, providing uninterrupted protection even before the corresponding Sophos Anti-Virus update is available. Uniquely, this feature also enables Sophos Anti-Virus to adapt to customized kernels automatically.*

Sophos Anti-Virus for Linux also updates the network automatically with the latest virus identity files. This can be achieved in two ways:

- In pure Linux environments: through the use of cascading Linux servers and direct updates from Sophos – shown in figure 1a.
- In multi-platform environments: through a combination of Sophos's centralized updating tool, EM Library™, and central installation directories (CIDs) – shown in figure 1b.

* If you recompile Sophos Anti-Virus for Linux to support a Linux distribution unsupported by Sophos, or a customized Linux kernel, Sophos reserves the right not to provide support where any such recompilation or customization has taken place. Sophos will use reasonable endeavors to provide first-line support. Should issues arise that require second-line support, or any other escalation process, Sophos cannot guarantee that such issues will be resolved.

Administration and management are made easy through a choice of either a web GUI or by using a command line interface. Sophos Anti-Virus for Linux detects and disinfects malware on-access, on-demand, or automatically at scheduled times using the commands “at” or “cron”. The increased speed at which new threats emerge is also addressed with Genotype™ technology, which is part of the Sophos virus detection engine and protects against families of viruses even before specific detection is available.

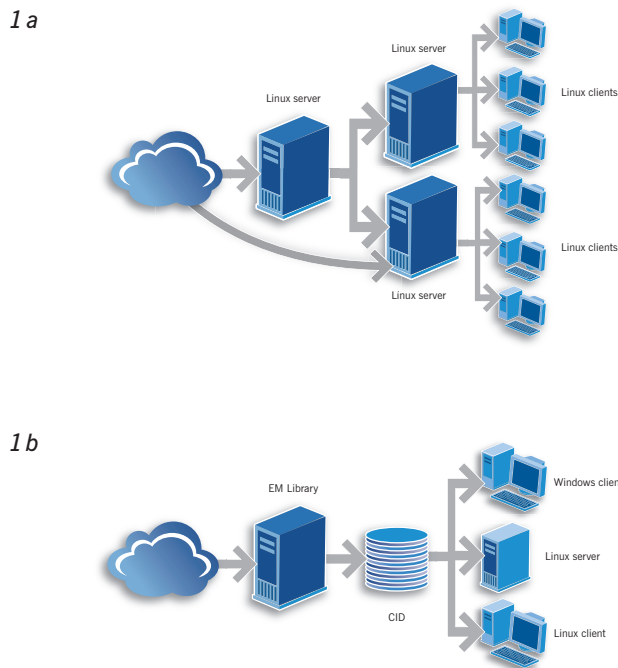


Figure 1: How automatic updating of Sophos Anti-Virus for Linux works in all-Linux networks (1a) and in multi-platform networks (1b).

About Sophos

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centers, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

Integrated threat management

Sophos solutions encompass the whole IT infrastructure. Our combined gateway and endpoint expertise enables Sophos to provide continuous, best-of-breed protection for Linux from viruses, worms, Trojans, spyware and spam, whether deployed on servers, desktops or laptops.

Because Sophos is focused exclusively on the needs of organizations, businesses using Sophos Anti-Virus for Linux are supported by a comprehensive enterprise service, which includes 24/7 engineer support. This support is backed up by SophosLabs™, a global network of threat analysis centers providing constant research and identification of emerging spam and virus threats.

Conclusion

The growing use of Linux in corporate networks means Linux-related security issues are forming an increasingly important threat to businesses. The chief danger lies in the increasing complexity of both the threat and the IT environment, with Windows viruses able to hide on “carrier” Linux computers. Sophos Anti-Virus for Linux addresses these issues with a solution that protects complex networks with vital on-access scanning capability, automatic updating and intuitive management functions. By drawing on our two decades of experience, skilled research capability, powerful technologies and cross-threat, multi-platform approach, Sophos offers the best, integrated solution to threat management for Linux in the corporate environment.

To find out more about Sophos and how our products can protect your organization, visit www.sophos.com.

Sources

- 1 The Linux Marketplace – Moving From Niche to Mainstream [prepared for OSDL], IDC Software Consulting 14 December 2004 (www.osdl.org/docs/linux_market_overview.pdf)