



This white paper  
outlines Virus  
Solutions and  
Benefits.

# Virus Solutions & Benefits

<b>Viruses</b>	<b>2</b>
<b>What are Viruses?</b>	<b>2</b>
<b>Solutions</b>	<b>3</b>
<b>Benefits</b>	<b>3</b>

## Virus Solutions & Benefits

### What are Viruses?

A computer virus is a piece of programming code intended to cause some unexpected and usually undesirable event, such as lost or damaged files. Virus code is usually buried within the code of another program. Once the program is executed the virus is activated and attaches copies of itself to other programs in the system. The effects of a virus can range from harmless messages that appear on screen to destruction of data. It can happen right away or on a set date. More than 20,000 have been identified, and 250 new ones are created every month, according to the International Computer Security Association.

A worm is a computer program that replicates itself and is self-propagating. While viruses are designed to cause problems on a local system and are passed through boot sectors of disks and through files, worms are designed to thrive in network environments. The most famous (or infamous) worm was the Internet Worm of November 1988. It successfully propagated itself on over 6,000 systems across the Internet.

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming code or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. Technically, Trojans are not viruses since they do not replicate, however, it can be considered a virus if it is widely redistributed.

Prior to the explosion of Internet usage and email traffic in the late 1990s, the vast majority of viruses were spread by infected floppy disks or other relatively slow moving methods of transmission. Virus protection was more easily managed with desktop solutions. However, with email becoming ubiquitous in corporate environments and elsewhere, viruses and other harmful files have the ability to spread at lightning speed. Some estimate that today viruses, worms, and Trojan horses can spread and propagate at a rate of tens of thousands of copies per hour. At this rate, there is precious little time to update desktop and gateway anti-virus systems to ensure corporate networks and systems are protected.

## Solutions

While many companies install and run anti-virus software on users' desktops and gateway servers, the fast-moving nature of virus transmission today requires a more rapid response than desktop and gateway solutions can deliver. Also, relying on one anti-virus software package alone is not enough.

We prefer a layered approach to virus scanning. Sophos, Symantec, and Trend Micro used in conjunction can provide worldwide coverage and the ability to react much more quickly to virus outbreaks. Because stopping viruses is especially time critical, we maintain a very close developer relationship with our anti-virus partners and they will often work with us at every stage in the development of virus remedies. This allows us to deploy protection in many cases hours before new signatures are even publicly released. Additionally, we are able to provide immediate protection prior to the release of any anti-virus engine update by using its powerful policy and attribute blocking capability to block specific kinds of attachments or filter email based on specific characteristics of a message.

A company's reputation is important, and being the source of a damaging virus, worm, or Trojan horse that infects the systems of customers, partners, and suppliers can do harm to that reputation. Therefore, in addition to securing inbound email and ensuring viruses do not enter the corporate network; we also scan outbound email for viruses to protect the companies with whom your organization communicates.

## Benefits

- **Buffer zone** – Email is scanned for viruses before messages reach the corporate network, ensuring that viruses and malicious code never touch your infrastructure.
- **Multi-engine scanning** – Leverage the power of multiple virus scanning engines for more effective protection.
- **Rapid updates** – Ensures anti-virus updates occur every ten minutes; our operations staff can make changes to the network to block malicious content within minutes.