netsweeper

SECURITY FEATURES OF NETSWEEPER

"The next layer of security"

Netsweeper Anti-virus

Using Netsweeper's Web filtering technology, malware of all forms will be identified in real-time as new threats are found. Filter and block these threats before they infect a computer or network.

Netsweeper Anti-spyware

Protect your personal information using solutions from Netsweeper to identify and prohibit spyware from even entering your network or computer.

Netsweeper Anti-phishing

Protect personal information such as usernames, passwords, credit card details and banking information by blocking access to phony phishing sites.

Netsweeper: "The next layer of security"

When most organisations implement an Internet Content Filtering solution, their main driver is typically one of the following:

- Improve the productivity of students or employees and keep them on task by restricting access to distracting websites.
- Ensure bandwidth resources are not being abused for personal reasons like gambling, streaming video or gaming.
- Mitigate legal liability and harassment matters resulting from the viewing, distributing or storing of illegal, copyrighted or trademarked content.
- Enforce or comply with internal Acceptable Use Policies or external regulatory laws, such as CIPA, by monitoring, auditing and filtering access to websites deemed unacceptable.

A fifth but less apparent driver, is the need for a solution to protect computers and/or networks from viruses, malware, spyware or phishing scams.

Though many organisations install an assortment of applications to counter these attacks, Netsweeper has proven through its core categorisation technology that these threats can be identified and blocked before they infect a computer or network. Netsweeper acts as another layer of security by protecting sensitive data and preserving IT resources for more value added projects.

Netsweeper Testimonial

"With the Netsweeper product we do not even need to have an anti-virus or anti-spyware program loaded on our computers. It just doesn't make sense to slow down the performance of our computers with unnecessary programs."

Scott Kluess
BBQ Management

About Netsweeper

Netsweeper Inc. empowers organisations to guard against Internet abuse and to offer their end users a secure, productive Internet experience, protected from harmful, malicious and inappropriate content. Netsweeper provides intelligent, network and workstation based web filtering technology to corporations, Internet service providers, educational institutions, government organisations and OEM partners around the world. Since its inception in 1999, Netsweeper has grown dramatically with offices and distribution channels in Canada, The United Kingdom, India, Middle East, The United States, South America, and South Africa.

How Netsweeper prevents system intrusion

Anti-virus and anti-spyware tools can stop many known attacks but typically are only as effective as their last update. In some cases, these updates are done days, weeks or months apart. Further, some malware attacks are so inconspicuous that many users are not aware they have been infected until it's too late.

Netsweeper's proprietary Internet Content Filtering solution is often regarded as 'another layer of security'. As requests are made to the Internet, the system simply blocks out URLs previously identified as a virus, spyware, phishing or other malicious application. As new URLs are identified, Netsweeper's real-time categorisation engine will learn of new threats long before most other security programs are aware they exist.

This constantly updated list of infectious URLs is developed using 2 techniques.

1. Netsweeper subscribes to a number of highly reputable commercial feeds that regularly provide updated lists of URLs for Phishing and illegal sites.
2. As Netsweeper's global user base make URL requests to sites not seen before by Netsweeper, and therefore not listed in our central URL database, these new URLs are scanned and categorised by our core scanning technology. Using commercial anti-virus technologies, the categorisation engine is also trained to scan for all forms of malware. As new URLs are identified infectious, they are added to the master database, which is then synchronised with Netsweeper's global network of Content Naming Servers. This real-time process ensures that all Netsweeper users are protected from new malicious and damaging URLs.

Benefits using Netsweeper solutions from a security perspective:

- Management will rest assured that sensitive data is safe from malicious attacks and possible theft through spyware and phishing.
- Productivity will remain positive as 'computer crashes' resulting from viral attacks on the network or computer stations will be drastically minimized.
- IT managers will spend less time 'cleaning' networks and individual computers (and laptops) and spend more time focused on critical, value added tasks like reporting and system maintenance.
- Individual users, either students or employees, will be able to function as expected or needed and not be subjected to forced downtime with computers not operating properly.