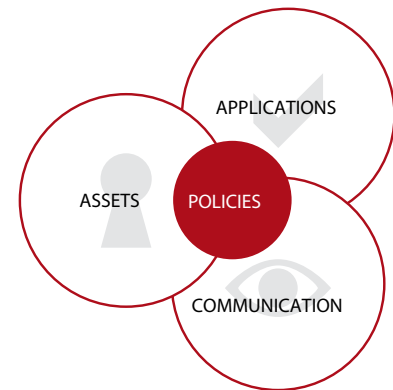




Add real zero day protection to your network by monitoring and controlling all programs and services running on every single PC – even when they move outside the network.



The challenge for businesses

A secure business environment is a requirement to running a successful business. Interference on the network can impact the company revenue and reputation. Today, companies have invested many resources on anti virus and perimeter firewalls. This is good but it does not offer the required protection.

Signature based anti virus products only react to a threat if it is known by the product and a solution is available. Up to 7.000 new malware programs are released every day, and vendors experience delays in product updates. In addition to the known malware, there are dedicated malware products that have been created with the goal to attack just one single company. Those malware products will very seldom be detected by the anti-virus labs, since the attacks are not spread world wide and knowledge of the malware is non-existent.

The perimeter firewall has no function against threats coming from the inside. Such inside attacks can be caused when laptops bypass the perimeter firewall. So when they connect to the company network, they spread the malware. Furthermore, laptops outside the network are not protected by the perimeter firewall, so data on the laptops is at risk of being attacked.

An additional and often overlooked threat occurs when malware and other potential dangerous software are brought onto the network via different devices such as CD/DVDs, MP3 players and USB sticks. Those devices may have transported data between home, friends, and customers and any dangerous software may initiate an attack and impact the network.

The NetOp solution

With NetOp Process Control, you complete your existing IT security solution with a real zero day protection.

With the “white list” approach you decide which programs and processes that are allowed to run and communicate on the end-points. Unwanted as well as unknown and potentially dangerous programs and processes will not be able to execute and, therefore they can't harm your network.

At a Glance

- Real zero day protection as malicious code can not execute
- Process control with “white list” for protection against unknown and unwanted programs and processes
- Integrated client driver-based firewall for reliable monitoring of the data communication
- Configurable security profiles and zones for PC inside and outside the company
- “Follow me” security where profiles switch automatically based on location rules
- Driver based solution – can not be knocked out, and starts when a network is available
- Great flexibility to set rights for the user and groups to fit your organization
- Timesaving central configuration and administration with the NetOp Policy Server
- Minimum consumption of resources – can be used even on older computers

NetOp® Process Control

Functions & Benefits in detail

Process Control: Manage the processes running on your system by defining rules that apply for any application. This gives you the ability to deny applications to run at all, to allow communication, to only allow communication of a trusted network or to prevent any communication.

Deny unknown processes from executing: NetOp Process Control protects the system against unknown threats by configuring the Process Control to prevent unknown processes from executing and communicating.

Bi-directional blocking of ports and protocols: Only opens the required ports and protocols in either the inbound or outbound direction, or both, to tighten firewall security.

Flexible administration of user rights: It is easy to define the rights for users and groups through the integration of Active Directory and Organizational Units. The tool adapts to the organization, and not the other way round.

Profile system with automatic network detection rules: This automatically switches the way your Process Control is configured when you are working on a different network - even if two or more networks are using the same IP address range. Profiles can be configured for 1 or a range of IP-addresses, for 1 or a range of MAC-addresses, and for 1 or more Domains.

Always on due to driver based process control and firewall: All filter algorithms are implemented at the driver level (as an NDIS Driver). The process control and firewall are therefore always on, providing maximum protection to the user even if the Process Control application itself is not running.

Protection from internet attacks: Unused ports are closed and only packets that have left the network are allowed to return if the packet ID has not been altered. This protects the endpoint against specific attacks and port scanning.

Secure Component Checking and protection against Process Hijacking: By verifying the calculated checksum, the Process Control checks the integrity of the application that is trying to communicate. If this has been modified, you are notified. By tracing an application's parent process, the computer Process Control knows if another application is trying to spawn an already trusted application and thus denies access to the network, even for the trusted application.

Encrypted communication: Encrypted communication to the NetOp Policy Server and local system databases provide security against malicious code trying to attack the Process Control software configuration.

Security Policy Management: The NetOp Policy Server Console controls the configuration of Programs, Ports, Protocols, Trusted Nets and Banned Nets. The console also controls the Profiles and Profile Rules for each Security Policy. New programs that users have tried to launch can be approved or denied for a certain Security Policy. This can be activated at the NetOp Process Control within seconds. The security profile system allows among other settings a range of IP-addresses, a range of MAC-addresses and multiple Domains.

Replica Servers: These are arranged in a cluster to ensure maximum system availability, to allow for redundancy, load distribution, and to interact with NetOp Process Control and record these interactions. Replica Servers regularly interact with their Master Server to receive security policy updates and return their NetOp Process Control interaction recordings for storage on the Master Server. Each Replica Server can service several thousands Process Controls.

Modules

NetOp Policy Server	Central administration, management and monitoring of the IT policies
NetOp Process Control client	Program that shall be installed at all client PC's

System Requirements

- Server supports Windows 2000/XP/Vista, Windows Server 2000/2003 all server editions
- Client supports Windows 9X/ME/2000/XP/Vista

Licensing

License model	Perpetual licensing per user. Support and NetOp Upgrade Insurance for 1 year.
---------------	---

Flexible purchasing options available.

Supplementary solution

NetOp Netfilter	Dynamic web content filtering product for the professional administrator.
-----------------	---



Try now. Test the full version free for 30 days
www.netop.com/freetrial

