

Enterprise Desktop Security

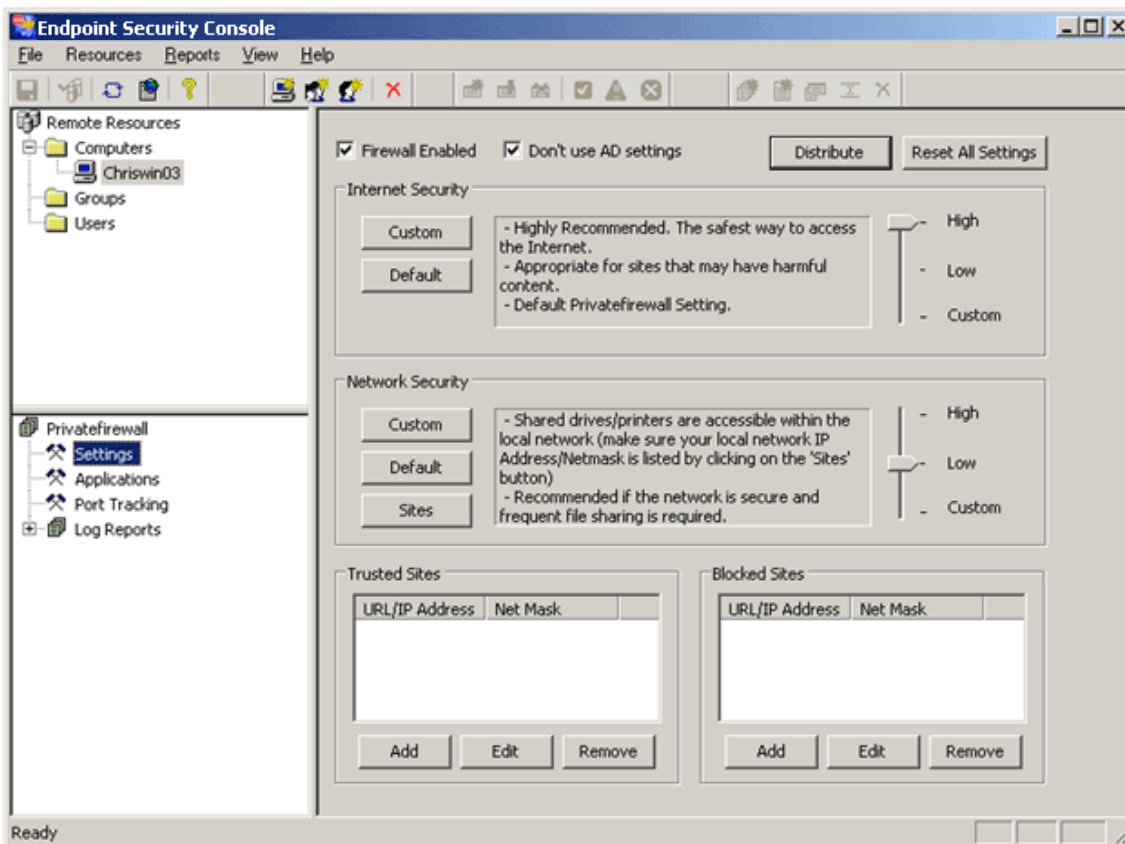
Any PC on your Enterprise Network can be a security risk if not properly managed and protected. Endpoint Security Console monitors and allows connections that it knows to be trusted or authorized, preventing spread of worm attacks or theft of data at the desktop level where most of the critical corporate information is created.

What is Endpoint Security Console?

Privacyware's Endpoint Security Console (ESC) provides a centralized administrative control capacity for assuring network endpoint protection on desktop and notebook computers utilizing Privacyware's popular Personal Firewall and Intrusion Protection Application, Privatefirewall. ESC enables system administrators to install, monitor, and configure Privatefirewall on any Windows workstation within a server domain. Settings can be customized for each endpoint or User Groups which are defined and configured within Active Directory.

The key capabilities of the ESC are the network configurable aspects of security policies and system use enforcement enabled by Privatefirewall on an enterprise endpoint. The ability to control this aspect of total enterprise security will help organizations to continuously defend and audit their networks not only for improved business operations, but also for regulatory compliance requirements.

Key Features and Benefits –



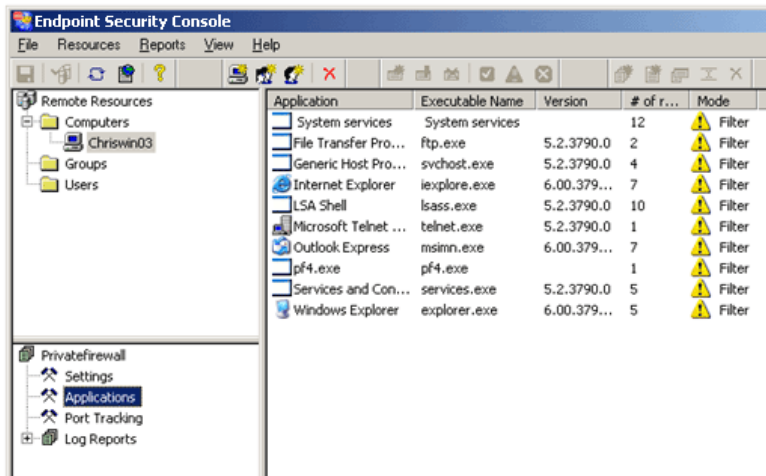
Endpoint Security Console provides an intuitive management interface that allows all installation, reporting, and configuration from one centralized location. This interface displays Internet and Network Security settings, Trusted and Blocked IPs/Websites, and Firewall Log Reports unique to each workstation, allowing the Administrator complete control over their network's desktop security.

General

- Workstation installation is completely automated, requiring no action from users.
- In addition to network workstations, Active Directory Users and Groups can also be configured from the Management Console.
- Advanced Firewall Log Reports can be sorted by Web, Mail, or System access attempts going back Hours, Days, Weeks, or a customized time period.
- ESC conveniently detects network connections and automatically sets rules allowing access within that network.
- Settings from one workstation can be distributed to the entire network instantaneously.

Application Detection and Firewall Policy Management

- Monitor all incoming/outgoing traffic and prevent trusted applications from being "Hi-Jacked" to steal network-accessible files. Endpoint Security Console automatically opens only the ports necessary for Internet access of a particular application.
- Control which applications can access the Internet by selecting Allow, Filter, or Deny traffic.
- Establish custom levels of security for specific "Trusted" and "Blocked" IP and Website Addresses — especially useful when different levels of security are required for specific websites compared to the default "Internet" security level.
- Define application specific or global packet filtering rules that can be applied to incoming, outgoing or bi-directional traffic.



Security & Reporting –

Internet Traffic (Packet) Filtering Security Level Control – Allows simple adjustment of security levels (i.e., High, Low, Custom) depending on the amount of protection required.

Port tracking and reporting – Tracks all ports to prohibit unauthorized port scanning or any other type of intrusion. Generates detailed reports on all port scan attempts and displays instantaneous on-screen alerts.

“Non-Standard” packet filtering – Endpoint Security Console blocks non-standard (non-winsock) outgoing packets that are commonly used by hackers to gain access to your system.

System Requirements

Management Console

Windows 2000, XP, Windows Server 2003
Intel processor (>700 MHz)
64 MB minimum RAM
10 MB of free disk space

Workstation

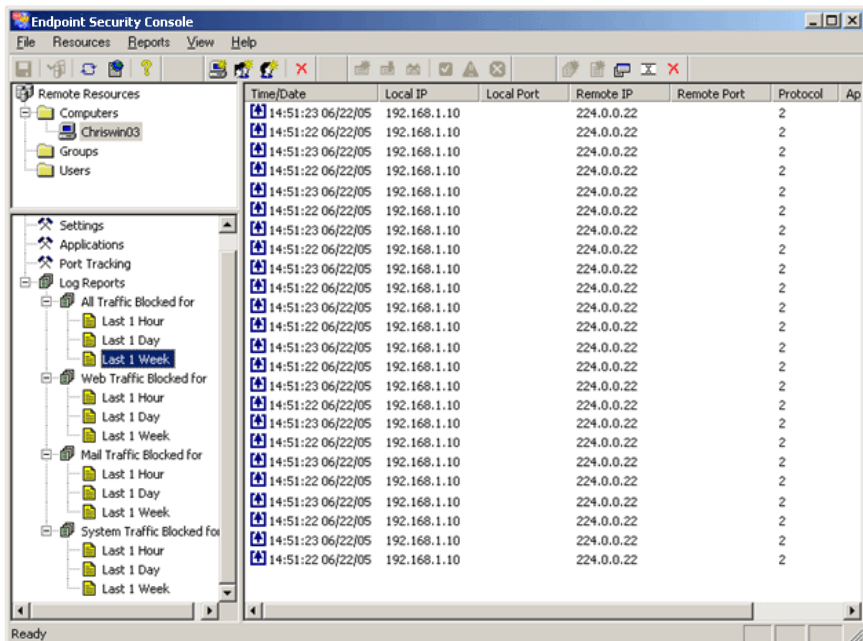
Windows 2000, XP, Windows Server 2003
Intel processor (>166 MHz)
16 MB minimum RAM
5 MB of free disk space

About Privacyware

Privacyware is an innovative provider of desktop and host defense and enterprise security data analysis solutions. Our unique competencies in non-linear mathematics, neural networks and self-learning systems, combined with proficiency in complex software and systems development allow us to create innovative security solutions that fuel better decision making and enable enterprises to remain a step ahead of hackers and others seeking to compromise critical systems.

Contact Information

Privacyware
130 Maple Avenue
Suite 7B
Red Bank, NJ 07701
732-212-8110 p
732-212-9210 f
info@privacyware.com
www.privacyware.com



Firewall Log – Contains a complete list and detailed information related to all incoming and outgoing packet activity. This is useful for tracking down incoming intrusion attempts to their source.