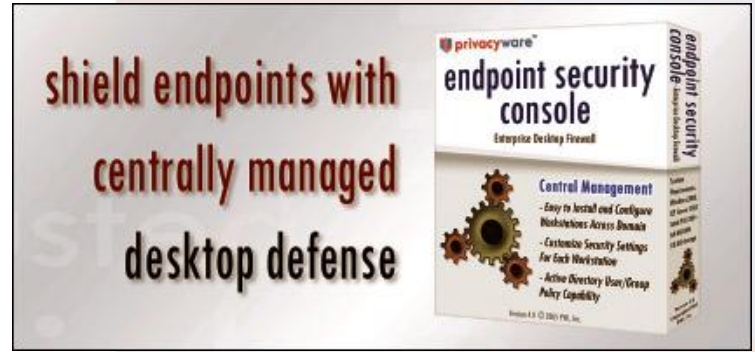


## Endpoint Security Console - Centrally Managed Desktop Defense

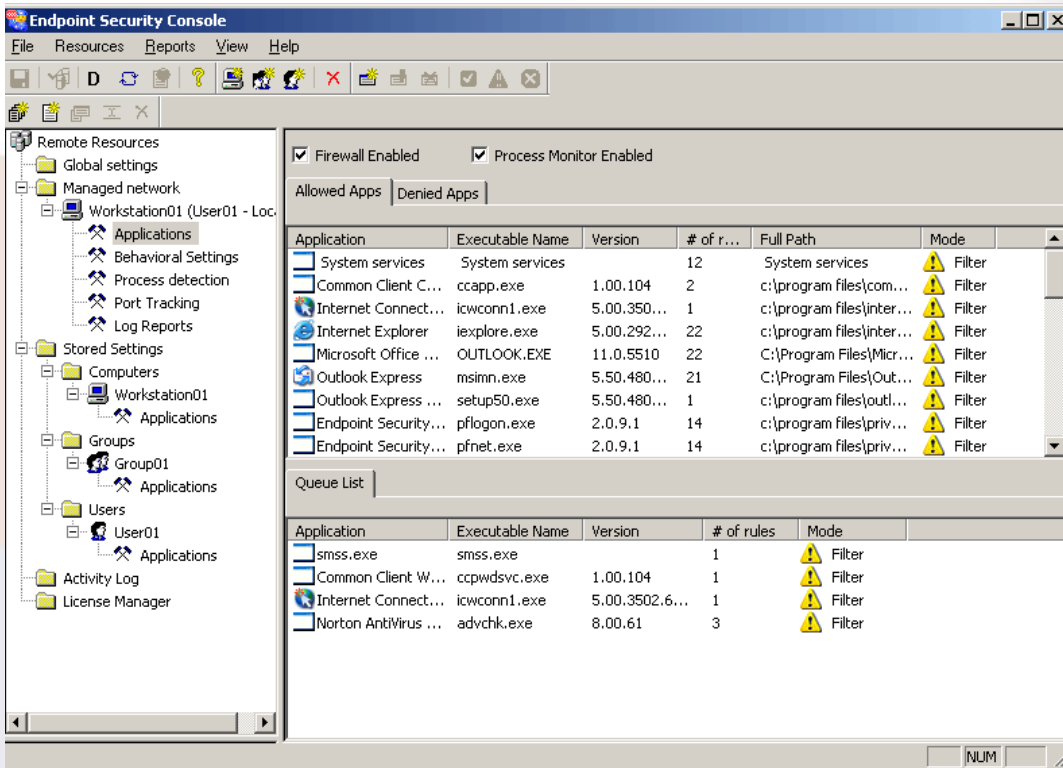
PCs on enterprise networks can be a security risk if not properly managed and protected. Endpoint Security Console uses conventional and behavioral technologies to prevent unauthorized system access, block known and new virus, worm, Trojan, rootkit and other malware injection, and deter theft of data at the desktop level where most critical corporate information is created.



## What is Endpoint Security Console?

Endpoint Security Console (ESC) is the central installation and administrative console for Privatefirewall, Privacyware's Personal Firewall and Host Intrusion Prevention Software. Endpoint Security Console enables administrators to install, monitor, and configure Privatefirewall on any workstation within a server domain. Settings can be customized for individual computers or for Users/Groups defined and configured within Active Directory. Key ESC features include: Inbound/Outbound Packet Filtering, Port Scanning, IP/Website Protection, Process Detection, and System and Application Anomaly Detection.

## Key Features

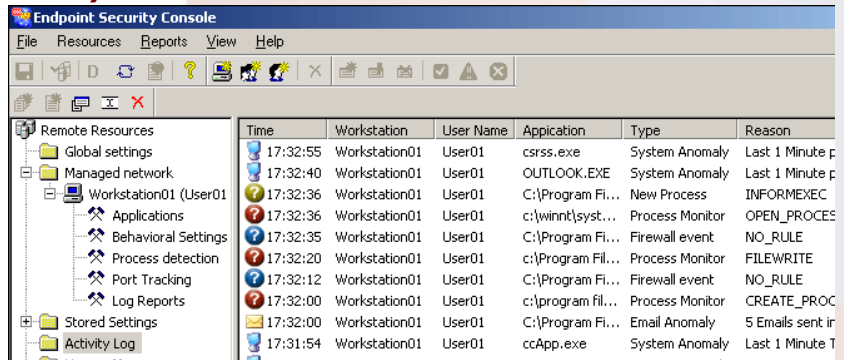


- System and Application level behavioral analysis baselines typical use patterns and detects and blocks unacceptable deviations.
- Centralized alert management enables network access and application rules to be defined based on specific alerts and distributed to Users and Groups.
- Workstation installation is completely automated, requiring no action from users.
- Stealth Mode: "Cloaks" computer's IP address, making PC invisible to the Internet and potential intruders.
- Application and Process Queue Lists contain recent activity from endpoints that require administrator approval.
- Settings from one workstation can be distributed to the entire network instantaneously.
- Detailed reports for Internet, System, and Email traffic.

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

## Application Detection and Behavior-Based Security

- Monitor all incoming/outgoing traffic and prevent trusted applications from being “Hi-Jacked” by cyber-criminals. Endpoint Security Console automatically opens only the ports necessary for Internet access of a particular application.
- Control which applications and processes can access the Internet by selecting Allow, Filter or Deny traffic.
- ESC evaluates WinAPI calls and analyzes a comprehensive list of system variables and security-sensitive registry keys to prevent possible malware, attack, or policy violations.
- ESC models and monitors system and application level behavior to identify and block activity characteristic of known malware, hacking, phishing and other threats.



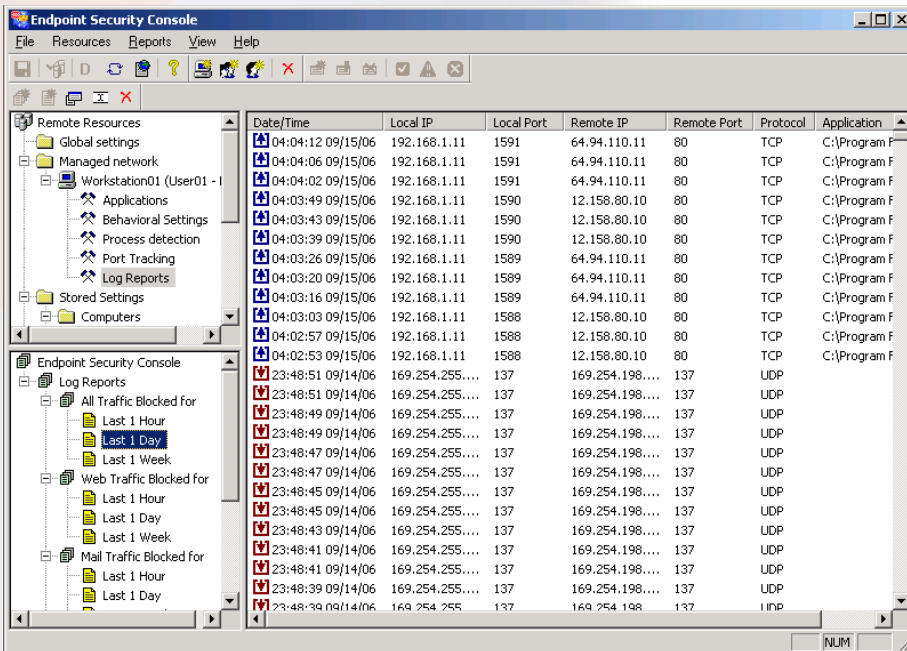
**Activity Log** – Lists all types of events generated from any workstation. This includes Application or ‘Firewall’ events, Process Monitor, New Processes, System Email Behavior. The administrator can Allow or Deny any event listed.

## Security & Reporting –

**Trusted and Blocked IPs and Website Addresses** – Block potentially malicious IP addresses and/or websites across the network.

**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.

**Advanced Packet Filtering** – Layer-3 firewall uses proprietary stateful packet inspection technology to detect and block unauthorized access to your system. Provides simple adjustment of security levels (High/Low/Custom) to establish different degrees of security for Internet and Local Network access.



**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.

## System Requirements

### Hardware

- 700 MHz Pentium® III or faster
- 128 MB RAM
- CD-ROM drive (for installation from CD)
- 10 MB of free disk space

### Software

One of the following operating systems:  
 Windows® 2000 Server  
 Windows® 2003 Server  
 Windows® 2000 Advanced Server  
 Windows® XP Home Professional  
 \*Active Directory is required for some features.

## About Privacyware

Privacyware is an innovative provider of host and desktop threat prevention and enterprise security analytics software. Our products increase the level of protection from new and known malware and intrusions in individual, small business and large enterprise computing environments and enable IT managers, security analysts, and security and compliance officers to more thoroughly understand the environments for which they are responsible and to more effectively identify and comprehend malicious and/or deviant activity.

## Contact Information

Privacyware  
 68 White Street, 2<sup>nd</sup> Floor  
 Red Bank, NJ 07701  
 732-212-8110 x235 p  
 732-212-9210 f  
[info@privacyware.com](mailto:info@privacyware.com)  
[www.privacyware.com](http://www.privacyware.com)



ISV/Software Solutions  
 Data Management Solutions