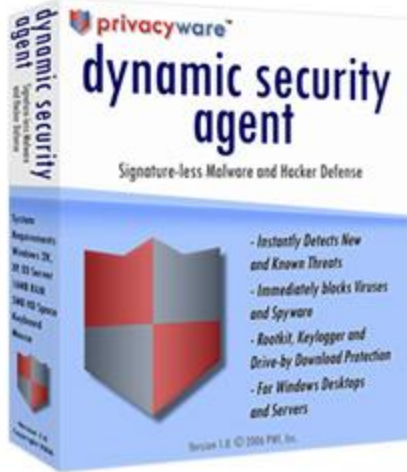


## Signature-less Malware and Hacker Defense

The web may be free, but we all know that to safely bank online, buy music, software, or books, or even simply surf the web, there is a price to pay. To combat online threats, firewall, anti-virus and anti-spyware software have become essential investments for any home or business computer. These programs monitor and control system access and scan and remove your system of malicious or spying software.

But the range and sophistication of malicious software and hacking techniques is rapidly expanding and traditional software solutions do not provide a proactive defense against it. Now, Privacyware meets this need with Dynamic Security Agent.



## What is Dynamic Security Agent?

Dynamic Security Agent (DSA) is a proactive, multi-layered defense solution for Windows desktops and servers that detects, blocks and quarantines activity characteristic of known malware, hacking, phishing and other threat types so that personal computer users and IT managers within small, medium or large organizations can more effectively and proactively protect the environments and private data for which they are responsible. An exceptionally simple user interface makes DSA a breeze to manage. You'll realize expanded protection and become educated about the nature of activity, trusted and un-trusted, that occurs on your system.

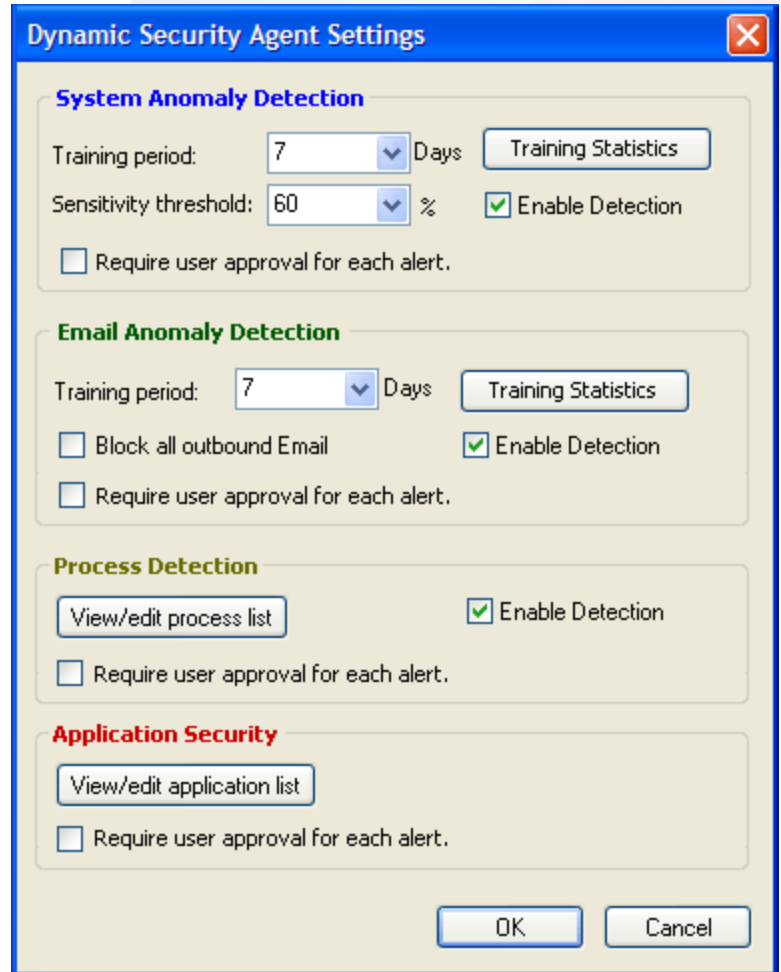
### Main Product Features

- Application Monitor/Manager
- Registry Monitor
- Process Monitor/Manager
- Email Anomaly Analyzer/Manager
- System Anomaly Analyzer

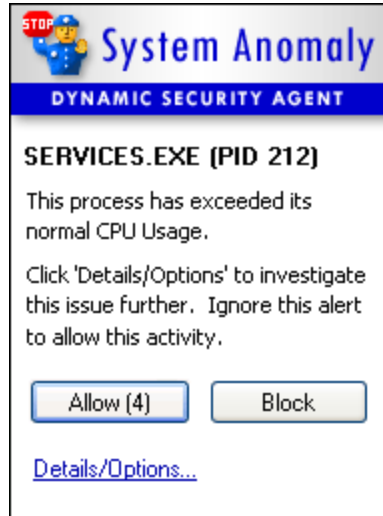
DSA also detects malware and intrusions based on behaviors characteristic of unauthorized system use.

Some of these include:

- Attempts to access a protected registry area
- Attempts to access a protected object
- Attempts to control Windows service
- Attempts to create a DNS request
- Attempts to initiate outgoing TCP traffic



The Dynamic Security Agent Main Menu provides management control over most of its features, including System Anomaly Detection, Email Anomaly Detection, Process Detection, and Application Security.



DSA features compact, user-friendly tray alerts that provides basic activity information. If more information is desired, the 'Details/Options...' link will provide larger, more detailed alerts.

## Proactive, Multi-Layered Defense

- **Application Security** – DSA monitors all traffic to and from your PC and prevents trusted applications from being “Hi-Jacked” to steal local or network-accessible files. The integrated Process Monitor adds an important layer of defense to conventional firewall protection by identifying process-level behavior characteristic of intrusion techniques and malware activity.
- **Stealth Mode** – DSA controls the openings to a user's computer. By “cloaking” the computer's IP address, the PC becomes invisible to the Internet and potential intruders thereby reducing the risk of intrusion or attack.
- **Process Detection** - DSA prevents various types of viruses and worms by tracking all trusted processes and providing alerts when any potentially malicious process attempts to run.
- **Advanced packet filtering** – DSA's layer 3 firewall uses a proprietary stateful packet inspection technology to detect and block unauthorized access to your system.
- **System Anomaly Detection** – DSA analyzes the normal use patterns of running applications and generates alerts as it detects unusual activity. The System Anomaly Detection Engine applies a sophisticated algorithm to establish a baseline of normal use based on several system variables such as CPU utilization, thread count, and others.
- **Email Anomaly Detection** – Privatefirewall mitigates the impact of attacks targeting email clients by tracking the volume and frequency of outbound emails and providing alerts when there is unusual activity.

DSA's layered approach to PC and enterprise endpoint defense protects your system from various Windows vulnerabilities and progressive techniques that hackers exploit to gain unauthorized system access and deliver malicious payloads. For example:

- **Windows OS Exploits** - Files that appear to be safe, but actually allow hackers to gain unauthorized access to your computer.
- **Malware: Virus, Spware, Trojan and Worms** Malware replicate, spread, steal personal information, and inflict damage to computers.
- **Rootkits** – Invisible to most types of system monitoring software, Rootkit can be installed by an intruder to execute whatever criminal activity they have in mind.
- **Hackers** - Criminals that leverage system vulnerabilities, social engineering, and other techniques to break into computer systems.

## System Requirements

### Hardware

- 166 MHz Pentium® or faster
- 8 MB RAM
- 5 MB of free disk space

### Software

One of the following operating systems:  
Windows® 2000 Professional  
Windows® 2000, 2003 Server  
Windows® XP Home, Professional

## About Privacyware

Privacyware is an innovative provider of multi-layered endpoint defense and enterprise security intelligence software. Our products increase the level of protection from new and known malware and intrusions on 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