

Anti-Spyware Evaluation Checklist for Corporate Computing

Spyware and adware can have a significant impact on corporate computing environments ranging from decreased system and network performance to the outright theft of sensitive information. Successful defense requires established management policies and procedures and an automated anti-spyware solution that offers *flexibility, low maintenance, and centralized controls*. This checklist outlines elements important to consider when choosing a corporate anti-spyware solution. PestPatrol™ provides the ability to do all of the following:

Make Sure You Are Totally Protected From Spyware

- Spyware
- Adware
- Trojans
- Keyloggers
- P2P Threats (Threats that open up backdoors in a network/sharing of confidential information)
- Hacker Tools (Sniffers, password crackers, identification of inappropriate use of remote control tools)
- DDOS Attack Agents
- Browser Helper Objects (Hi-jack web browsers)
- Commercial Administration Tools (VNC, RADMIN, PCANYWHERE etc.)

Preferred Deployment Methodology

- Centralized Management Console with no client-side installation
- Launched through command line or a batch file with no client installation
- Deploy anti-spyware application as an image by a command line launcher
- Installed as a stand-alone full client

Centralized Management Requirements

- Centralized deployment with no manual client installation
- Centralized reporting
- Interactive scan on demand
- Consolidated logging and reporting
- View "Network Neighborhood" and auto-discover trusted domains from a central management console

Scanning Capabilities

- Interactive on demand scans
- Scheduled scans
- Real-time scanning
- All of the above
- Scan configuration by user, preset or customized configurations
- Scan fixed and removable media at the client
- Scan from the desktop according to preset or customized configurations

Pest Management

- Auto-quarantine or auto-delete pests without end-user interaction
- Log only to see what is on the network first before taking action
- Auto-delete spyware cookies while quarantining pests of a higher level of threat
- Restore a pest from quarantine from the management console

Remote User Support

Remote users pose a major security threat to corporate networks and to themselves. You need to provide protection and have the ability to update and report on remote users.

- Verification and enforcement of updates for remote users
- Real time scanning protection for remote users upon boot up

Anti-Spyware Evaluation Checklist for Corporate Computing

Reporting

Reporting helps justify the ROI of a solution and informs management of the threats attempting to penetrate the corporate network. Minimum reporting capabilities for effective management reports are listed below:

- Centralized reporting capabilities
- Consolidate corporate pest detections into a single log on a designated server or
- Aggregation of reports into a centralized report
- Ability to save reports in an ASCII format for easy export to other applications
- Report by Workstation
- Report by Date and Time
- Report by pest in security risk priority order
- Report by pest category
- Report on specific pests

Updates

Updating pest definitions is an ongoing process that should be straightforward and automated. Updates should be provided on a regular basis and have a means for reporting new threats for inclusion in its signature updates.

- Automated updates
- Pest definitions updated at minimum on a weekly basis
- Verification of and enforcement of updates for domain users
- Provider must have a pest research team that provides a quick and efficient process to report new pests

Maintenance of Anti-spyware solution

- Automated
- Manually updated

Exclusion Management

- Exclusion by Path
- Exclusion by Pest Category
- Exclusion by Pest Name

Transparency to Users

- No user interaction
- No user interface

Real-time Active Protection

- Real-time memory protection
- Process termination / file removal of pests in active memory
- Ability to activate or deactivate real time scanning components

Alerting Capabilities

- Automated alerting of pests detected
- SMTP email alerts

Pest Detection Research

- Fast turnaround in adding newly discovered pest detection
- Ease of adding new scanning strings
- Detailed spyware research information and statistics available on website