PROTEGENT

Enterprise Security

Technical Whitepapers

Protegent Enterprise Security has been designed to provide security solution to Enterprise Networks. It is a Multi Tier Security suite that includes Data Leakage Prevention, Activity Reporter and Asset Tracking.

PROTEGENT ENTERPRISE SECURITY includes following software components:

Protegent Management Console:

A single administration screen to deploy, manage and control the features, settings and access user reports and alerts on any unauthorized usage for Protegent Enterprise Security. It reduces the administrative workload by centralizing all management activities for "Data Leakage Prevention", "Activity Reporter" & "Asset Tracking".

Manageability:

- Remotely deploy, manage and uninstall Protegent on clients.
- Identification of non-compliant systems.
- Backup option for settings, reporting, network structure and license to restore for later use.
- Optimized for Business Environments.
- Centralized Updates.

Settings:

- Arrange clients in groups as per usage, department or policy based structure
- Create settings specific to user or group.
- Overwrite or append settings as per requirements.

Reports:

- Detailed reports of each client
- Email Notification to the administrator at any desired time interval.
- Send reports to FTP
- Extensive queries & search reports
- Centralized asset management
- Centralized activity reports
- Centralized reports for all port, specific ports, all clients or specific client
- Alert as soon as any unauthorized action performed at client system.

Data Leakage Prevention (PORT LOCKER)

Data leakage prevention allows user to safeguard data/ file from unauthorized access. It prevents vital and important data to be transferred from one pc to another using Flash drive, CD/DVD writers, PCMCIA port, Ethernet ports, Printer ports, infrared ports and Bluetooth port. It provides the Options to lock/unlock single or multiple ports with authorized password. It allows user to lock ports with different lock type options for e.g. permanent, specific time duration (scheduled block) and when the computer remains idle. It displays the alert as soon as an unauthorized action is performed against the locked ports. It provides complete log related to Permanent Blocked, Schedule Blocked or Un-Blocked Ports with actions performed including changes in setting, locking and unlocking the ports.

Feature list of Data Leakage Prevention

- Proactive protection against data theft.
- Sets restrictions against all communication ports by blocking and unblocking them.
- Unique feature of Whitelisting the authorized USB by using unique hardware ID of the device.
- Option of assigning **USB Readonly** setting to whitelisted and non-whitelisted USB mass storage device.
- Prevent data theft as well as unauthorized access of critical data Locks USB, CD/DVD, IEEE, Network Adaptor, Printer, Infrared port and Bluetooth port.
- Options to open single or multiple ports with authorized password when it is Permanent locked/Idle locked/scheduled locked.
- Option to save software settings so that it can be restored when needed. Option to reset software settings to default.
- Option of reporting system activities through e-mail or by FTP.
- Option of reporting system activities through mail as scheduled (i.e. Daily, Weekly, and Monthly etc.) by user.
- Option of sending Incremental Report or Complete Report as selected by user.
- Unique feature of White listing the authorized USB by using unique hardware ID of the device.
- Special feature of Print Screen Locking
- Setting of report log size (Min 1 MB to Max 5 MB).
- File Transfer Log will show the reports of file transferred to and from a USB mass storage device & it will also show the detail reports of files added, removed and rename to and from a USB mass storage device.
- E-mail filtering log shows the complete log of the outgoing emails filtered and blocked on the client's system. Detail includes date and time when the mail was blocked, receiver's email address (To, Cc, Bcc), attachment name and size, subject of the email and content of body.

Activity Reporter

Activity Reporter would be a very important tool for companies to monitor the activities of all computer users. This would act as an ideal spy without the knowledge of the user that their every key stroke/ every activity on the computer or internet is being monitored and screen shot / report is generated on a regular basis.
The unique feature of **Activity Reporter** to whitelist and blacklist applications would enable you to monitor more effectively. The various options of reporting along with the different formats of reporting would ensure monitoring is effective and keep the network more secured. The features of **Activity Reporter** would definitely act as a foil for anyone to do any fraudulent activities in the organization.

Feature list of Activity Reporter

- Captures Application activity, Internet activity, Clipboard, Keystrokes, Screenshots, Working log of clients.
- With the help of application monitor time log can be maintained for specific applications.
- Unique feature of blacklist and whitelist application
    - Blacklist: Applications and websites that are added will get captured and be visible in alert.
    - Whitelist: No alert will be generated of the application and website added in the whitelist list.
- Option to select the level of tracking.
- Send the reports to a specific email address or upload to an FTP location.
- Password protected so only authorized person can access the reports. Runs in Absolutely invisible mode.
- Remote Installation/Update/Uninstall.
- Records contents of password protected web pages, including Web Mail messages.
- Monitors all users on a PC, even if you don't know their passwords.
- Monitors Windows Clipboard activities like copy and cut.
- Monitors computer activity only when user goes online (optional).
- Setting of report log size (Min 1 MB to Max 5 MB).
- Captures ICQ, Miranda, Skype, Google Talk, MSN, AIM, AOL, Yahoo, QIP chats.
- Detection and notification of the custom keywords (alerts).
- Reports of Application activity, Clipboard activity, working log, Internet activity, Keystrokes, Screenshots all in HTML format.
- Intercepts DOS-box and Java-chat keystrokes
- Invisible in the Windows startup list.

Asset Tracking

Asset Tracking tool tags and tracks the condition of **Software Assets** (i.e. Windows Info., Installed Software's & reports) & **Hardware Assets** of computers (i.e. Memory, Storage, Printer, Mouse, Keyboard, Hard Disk, Network, Processor, Sound etc.) if any changes occur on the system. Asset Tracking with Early Warning Systems for pending hard disk problems. It does this by continuously monitoring various hard disk parameters (such as Hard disk Temperature, S.M.A.R.T and details). Asset tracking provides the feature of Disk Cloning (i.e. it can paste the contents of a potentially fatal disk on to a healthy disk) and Disk Scanning (i.e. display bad sectors on hard disks).

Feature list of Asset Tagging & Tracking

- **Tags & Track Hardware Assets** i.e. Motherboard, Memory, Printer, Mouse, Keyboard, Hard Disk, Network, Processor, Sound etc. If any changes in hardware occur then auto message sending feature on server.
- **Tags & Track Software Assets** i.e. operating system Info, Installed Programs. Auto message sending on server with respect to software changes
- Real time hard drive status monitoring.
- Avoid losing your important data due to hard drives overheating.
- Hard drive health status information.
- Amount of bad blocks or physical bad sectors on the hard drives.
- S.M.A.R.T. attributes.
- Disks scan option to check physical bad sectors.
- Disk Cloning option to take the back up of the hard disk.
- Prompts emergency system shutdown in case of hard drive overheating.
- Previewing raw values of S.M.A.R.T.
- Setting of report log size (Min 1 MB to Max 5 MB).
- Alert if changes encountered in Hardware Assets & Software Assets.
- Hard disk real time temperature with respect to time graph.
- Email alert for S.M.A.R.T & Asset Tracking.
- Schedule feature.

System Requirements:

Hardware & Software Required at Server

For Windows 2000

- 1.66 MHz or higher processor
- 512 MB of RAM Memory (1 GB recommended)
- 2.5 GB available hard disk space (1 GB recommended)
- Windows 2000 (SP 4 Update Rollup 1)
- Internet Explorer 6.0 (or higher)
- Microsoft Data Access Components 2.8 (MDAC)

For Windows XP/2003/Vista/Windows 2008/Windows 7

- 1.66 MHz or higher processor
- 512 MB of RAM Memory (1 GB recommended)
- 2.5 GB available hard disk space (1 GB recommended)

Hardware & Software Required at Client

For Windows 2000

- 1.66 MHz or higher processor
- 512 MB of RAM Memory (1 GB recommended)
- 60 MB available hard disk space (64 MB recommended)
- Win 2000 (SP 4)

For XP/Windows 2003/Vista/Windows 2008/Windows 7

- 1.66 MHz or higher processor
- 512 MB of RAM Memory (1 GB recommended)
- 60 MB available hard disk space (64 MB recommended)

Protegent Enterprise Security Packs Availability

Unistal's **Protegent Enterprise Security** is available with all three components:

- Protegent Enterprise Security for 1 server + 5 clients.
- Protegent Enterprise Security for 1 server + 10 clients
- Protegent Enterprise Security for 1 server + 25 clients

Enterprises with a larger user base may choose the components to suit their requirements

- ✓ Data Leakage Prevention
- ✓ Activity Reporter
- ✓ Asset Tracking
- ✓ All of them

Note: One pack will provide only one management server for Protegent Enterprise Security.