Control • Record • Audit
Comprehensive endpoint security

Audit
Real-time audit

Record
Complete record of users activities

Control
Full control over user's activities

IP-guard consist of 14 major function modules, Virtually covers a corporate's endpoint management needs, helps you effectively to resolve all type of endpoint security concerns

Facing the existence of continuous security threats, constant evolving facts of methods, you will require an effective tool to build a secure, efficient network environment, through precise control, recording and audit tool, improving information security mechanism to reduce operational risk.

IP-guard focuses on confidential data leakages, the aspects of such leak. Targeting endpoint users, carrying out asset management, daily activity logging and endpoint behaviour management, providing management staff a high stability, high performance, automated and user friendly management tool, regardless of employees unintentional loss or malicious theft, resulting to the loss of important data or when improper behaviour effecting work performance, all may be grasped immediately with effective control.

Automated logging on endpoint, accuracy on asset inventory
With IP-guard agent installed, IP-guard will automatically log the computer activities, hardware and software information across the network, capabilities to include other non-IT asset information, providing accurate control over IT Assets.

Convenient remote control, reduce human resource cost
Managing your network from your desktop, providing maintenance, support or troubleshoot to the client machine or via a secure remote connection, take control or send files to the client machine.

14 modules, accomplish comprehensive data protection
Targeting on all kinds of file operations, applications and website usage, printing, hardware plug-ins, etc... policy settings on user rights and backup important documents before file operation, prevent confidential data leakage, loss or deletion.

Detailed logging, assist to understand user behaviour
Detailed logs on the information of the clients machine, user behaviour will be recorded by IP-guard, these immutable logs may be used for future audit or as forceful data.

Implement IP-guard
Strengthen Endpoint Security

Strengthen monitoring with screen recording
IP-guard's unique screen monitoring, allows admin to immediately capture the user's present screen, and may also set policy in time intervals to record.

Simplicity, User friendly interface
Centralized management console with easy to use interface, providing administrators with a quick start to the solution, through the one centralized management console to easily achieve the business requirements, implementing policies, monitor and audit.

Background monitoring and management
All the functions of the IP-guard Agent runs in the background, the users will not be affected with daily operations and will not know the existence of the Agent running

Modular design providing more flexibility, effective use of IT budgets
Modular design, prioritising the current IT requirements, maximize the functionality and benefits with the IT Budget.

Main features of IP-guard

Comprehensive management
Monitors endpoint behavior and confidential data through a comprehensive management console, remote management features for remote maintenance and control.

Active recording
Records endpoint activities and behaviors in conjunction with screen recording, supports screen snapshot history for queries, and information on your software and hardware IT assets.

Completely automated
Auto generate statistics on endpoint computer usage, providing various view of reports, analyze systems updates and vulnerabilities

System Requirements of IP-guard

Modules	Software Requirements	Hardware Requirements
Database	SQL Server 2000 SP4 / SQL Server 2005 SP1 / SQL Server 2008 / SQL Server 2008 R2	**Minimum Requirement:** Pentium 4 1.8G / 2GB RAM / AVAILABLE DISK 50GB and ABOVE
Server	Windows 2000 SP4 / 2003 SP1 / 2008 / 2008 R2	**Recommended Requirement:** Xeon 7020 / 4GB RAM / AVAILABLE DISK 120GB and ABOVE (Actual hardware spec to be advise after assessing the client's requirements)
Console	Windows 2000 / XP / 2003 / Vista / 2008 / 2008 R2 / 7	**Minimum Requirement:** Pentium 3 500 / 512MB RAM / AVAILABLE DISK 1GB and ABOVE
Agent	Windows 2000 / XP / 2003 / Vista / 2008 / 2008 R2 / 7	**Recommended Requirement:** Pentium 4 1.3G / 1GB RAM / AVAILABLE DISK 2GB and ABOVE

ABOUT US - VPR Solutions

VPR Solutions, a software service provider in the enterprise endpoint security and management field, providing business users with high stability, high performance, automated and easy to operate management system is our goal. Joint with local partners to operate in the local market to provide customers with more complete and efficient services, to help enterprises protect and manage important information, to cope with the worsening security threats, and thus effectively reduce the operational risk. VPR Solutions, through the advanced technology, with the characteristics of control, record, analyze and adopting a flexible modular design (IP-guard Enpoint security and management solution) of which, screen monitoring, application usage statistics, web page visited, web browser statistics and many other features. VPR Solutions, the first to introduce such enterprise applications in the local South Africa Market. This independent research and development system is well received by the majority of praise, many listed companies in South Africa and the well-known global companies are customer's of VPR Solutions. Furthermore, proofs the high reliability, high level of standards on service qualities with VPR Solutions.

VPR Solutions

www.vprsolutions.co.za

Address	: Palazzo Tower West, Montecasino, William Nicole Drive Fourways, Johannesburg
Postal	: PO Box 59, Fourways North, 2098
Tel	: 0861 747 472
	: +27 11 510 0210 (International)
Fax	: 0866 907 442

sales@vprsolutions.co.za
support@vprsolutions.co.za

VPR Solutions

IP-guard V3 COMPREHENSIVE ENDPOINT SECURITY AND MANAGEMENT SOLUTION

IP-guard V3

COMPREHENSIVE ENDPOINT SECURITY AND MANAGEMENT SOLUTION

Complete Control   Auto Record   Full Audit

Enterprise Endpoint Security Issues **IP-guard** A Complete Solution !

Misconduct on endpoint computer may reduce employees productivity, affecting the stability of enterprise IT systems and, more importantly, may endanger the security of the file data, which may led the companies to be caught in a high degree of risk. Facing various endpoint security issues and threats, with 14 functional modules, IP-guard is the optimal solution, manages almost all endpoint issues that may occur in an enterprises, satisfying the requirements and considerations on management burden and cost of implementation

Application Management
- Limit or Block IM, BT and other malice applications
- Limit or Block Melware or Freeware
- Prevent user from Window Title, Registry, Path, Document Name change to escape from Management

Screen Snapshot
- Real-time Screen monitoring, understand user's behavior, attend to suspicious or inappropriate activities immediately
- Screen recording, view snapshot history to trace user's behavior

Document Management
- Limit Read and Write Authority to important data
- Logging of document activities, convenient to trace file flow
- Backup important data before modift/edit or maliciously deleted. Ensure data security

Website Management
- Control users browsing activities, prevent users from uploading confidentil data
- Monitor browsing usage, manage productivity

Instant Message Management
- Supports upto 16 types of IM application, prevents user from sending out important data through IM applications
- Monitor users chat session, prevent important infomation leakage

Email Management
- Restrict outgoing email through varies conditions, prevent confidential data leakage
- Manage user Email activity, prevent data lose

Printing Management
- Prevent important data leakage from user printing to hard copy
- Monitor printing usage and content
- Manage random printing behaviour, reduce resource wastage

Bandwidth Management
- Manage network traffic, prevent network congestion from excessive download and upload

Basic Management
- Prevent users from altering system settings, IP/MAC address randomly, to escape from system management

Removable Storage Management
- Control removable storage usage, prevent data copy to unauthorised devices
- Auto Encryption function, ensure data secured even when device lost

Asset Management
- Record software / hardware devices information, effectively use of resource to reduce wastage
- Software deployment, support resume breakpoint transfering, reduce human resource and IT workload

Network Management
- Prevent Trojan / Virus from transmitting large volume of packets through specific communication protocol
- Isolate specific groups on the network, protect network communication security

Remote Maintenance
- Remote control and maintenance, real-time diagnose and control, assist IT staff to improve efficency on users IT problems

Device Management
- Effective control on usage authorities over all type of hardware device, such as Floppy Drive, CD-Rom, CD-Writer, MO, ZIP, Serial Port, Parallel Port, USB Hub, SCSI, 1394 Controller, Infrared devices, PCMCIA cards, Bluetooth devices, modems, USB keyboard / mouse, USB image devices, USB CDROM, USB storage, USB HDD, USB network cards, wireless network card, PnP network card, virtual network card, sound equipment, the virtual CD-ROM drive, etc...
- Prohibit user from adding any new hardware devices

IP-guard Features

Basic Management (Core)	Basic info, basic control, basic logs, basic policy, policy alerts, policy logs	Printing Management	Print operation logs, record printed contents, print control	Email Management	E-mail logs, e-mail control
Application Management	Application logs, applications statistics, application control	Screen Snapshot Management	Real-time multi-screen monitoring, screen snapshots, screen recording	Instant Message Management	Instant messaging logs, instant communication file transfer control
Website Management	Website browsing logs, website browsing statistics, website browsing control	Remote Maintenance	Remote maintenance, remote control, remote file transfer	Asset Management	Asset, copyright & patch management, system security vulnerabilities, software deployment
Bandwidth Management	Network traffic statistics, network traffic control	Device Management	Device Control	Removable Storage Management	Authorise removable storage, removable storage encryption
Document Management	Logging of file operations, file operation control, file backups	Network Management	Network communication control, intrusion detection	**Features** : Support Terminal Service, Thin-Client, VM-ware, muliti-screen setup, safe mode	

Server
High performance and large storage space computer, Used to store system information and policies.

NAC Server
In line with network infrastructure switching equipment, conduct access rights management on non-client devices and equipments to corporate network, usually installed on the computer closer to the network core location, may also be installed on the IP-guard server or administrator's computer.

Console
Used to view system information, implementing management polices and real-time maintenance. Usually installed on management's computer of a corporate environment, may also be installed on the same computer as the IP-guard server.

Wireless Area | **IT Department**

Sales Office — Console — Client — Console — Router — Internet — Wireless AP

Link — Console — Router — VPN — Client

Branch office

Client — Unauthorized computer — Certification — Client — Console — Switch — Network Printer

R&D Department

HEAD OFFICE

Switch — Certification — Client — Unauthorized computer — Client

Server Room
Terminal Server — **IP-guard** NAC Server — **IP-guard** Server

NAC authentication
Remote maintenance