Record
Active recording and comprehensive logs

Control
Total control of end user behavior

IP-guards 16 modules are a comprehensive management solution to counter all problems endpoint computers may encounter, and are also a cost effective way to gain control over endpoint computers within an enterprise.

Audit
View statistics and report

Control · Record · Audit
The Complete Solution to Endpoint Security

When facing the ever evolving threat to secure information security, organizations need an effective tool to build a secure and efficient network environment. IP-guards total control, comprehensive logs and efficient auditing will minimize corporate operational risks and create a safer network environment.

IP-guard focuses on endpoint information security by monitoring and controlling endpoint computer asset information, event logs and behavior. IP-guard provides a high performance, reliable, automated and easy to use system that captures and controls employee information leakage under any circumstances which allows administrators to secure and control the corporate environment.

Provide searchable Skype, WeChat, Line conversation log
Files and images transferred in the instant messaging application such as Skype, Google Talk, Line, WeChat etc. can be restricted. Text chat made in the instant messaging application can be searched via our console.

Screen watermark eliminate cellphone threats
Nothing prevents people from using a cellphone to take an image of sensitive information. Screen watermark displays information such as user name, computer name, IP/MAC address and customized content on the computer screen to provide the trail of information leak.

Secure protocols are supported
For the past few year websites adopt the HTTPS, IP-guard provides provide a complete solution to accommodate HTTPS protocol.

Building a secure environment with IP-guard

Refine network control to the application level
Regular firewalls restrict network access by IP and Ports. IP-guard's advanced network management block network access by IP, Port, and application to minimize interference between applications.

Operate in VDI environment
IP-guard's functions in the OS level uses minimal computer resource which allows us to in virtual machine environment such as VMWare Horizon, Citrix Xen Desktop environment.

Provide automated customize report
Analysis collected data and provide a trend, potential risk and various type of other reports to each department managers.

Controls portable devices
Total control of all devices connected to the computer include mobile phone, USB storage devices it's much more than controlling USB Ports

Request for temporary access
From time to time end users may require to use devices or software that had been prohibited by the company policy. We provide a mechanism to allow temporary access which ensures smooth business operation.

IP-guard Main Feature

Total Control: Manage endpoint workstation operation activities, software and hardware assets, remote control and maintenance via one single console

Active Recording: Record various types of endpoint workstation operation and activities according to the defined policies. Endpoint workstation's hardware and software asset changes and screen history are also included

Complete Auditing: Automatically analyse endpoint workstation's usage and provide various types of statistics and reports. Reports also include Windows update information, Windows vulnerability and software license information

System Requirements

Components	Software Requirements	Hardware Requirements
Database	MS SQL Server 2005 SP1 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019	• Processor : Pentium 4 Dual-Core • Memory : 4GB • Free Disk Space : 120GB
Server	Windows Server 2003 SP1 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019	
Console	Windows XP / Vista / 7 / 8.x / 10 Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019	• Processor : Pentium 4 • Memory : 512MB • Free Disk Space : 1GB
Agent	Windows XP / Vista / 7 / 8.x / 10 Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 Mac OS、Linux OS (Please contact with us)	• Processor : Pentium 4 • Memory : 512MB • Free Disk Space : 1GB

About Us

TEC Solutions Limited, a leader in enterprise endpoint security and management solutions. Been dedicated to research and develop an automated and easy-to-use solution for enterprises with high stability and performance.

TEC Solution Limited has representatives in Japan, Taiwan, Hong Kong, and China. With regional partners in Asia-Pacific, South Africa and Europe regions.

"IP-guard: Comprehensive Information Security Management System" protects important information from growing security threats. It eases the burden of IT management in corporations. By considering our customers' needs, TEC Solutions Limited adopted and develops with progressive technologies to allow users to log, manage, and analyze data. IP-guard's revolutionary design was the first endpoint security product provides enterprise level Screen Monitoring, Application Management, and Website Management. Our proprietary system offers a flexible module-based design in the purchase scheme, and it has received positive feedback from our customers. Many globalized corporations adapted IP-guard's as part of their solution, it further proves that IP-guard's high reliability and the excellent quality of services.

COMPUTEX Taipei 2010 Best Choice Award

IP-guard 3.11.1219
CNET Editors' Rating 4.5 stars

IP-guard V4
Information Security Audit

Total Control   Active Recording   Complete Audit

TEC Solutions Limited

Application Management

- Screen watermark feature displays end-user computer information on the computer's screen
- Restrict or limited usage of "green" software or any non-work related applications
- The application remains restricted or limited even when Windows registry, application name or path been altered.
- Software Installation Management controls software installation/uninstall rights at endpoint computer
- Restrict windows services to optimize computer efficiency
- Ability to restrict execute applications installed on USB or CD/DVD

Website Management

- Ability to use keyword and wildcards (*mail*) to restrict website browsing
- Control browsing behavior and prevent end users from uploading sensitive information via HTTP(S), FTP, TCP Protocols
- Provide glandular browsing report to improve end-user productivity
- Provide comprehensive website browsing logs include URL, Website title etc.

Email Management

- Ability to set multiple policies to prevent information leak via mail
- Ability to backup mail content and attachments
- Support General/Microsoft Exchange/Lotus Note system

Basic Management

- Ability to import AD/LDAP network structure to our system
- Control's more than 30 different types of Windows setting to prevent end-user adjustments
- Ability to schedule shutdown/sleep/reboot end-user computers
- Built-in backup feature to follow up with a data retention policy

Insight Report

- Ability to generate various type of periodic report
- Automatically generate and sending reports responsible personnel
- Built-in template for various types of reports allow supervisors to generate a related report in the shortest time
- Potential risk report to detect security breaches ahead of time

Asset Management

- Effectively manage hardware/software information within the organization
- License management collect software usage to prevent copyright infringement
- Uninstall software within the organization from our console
- Automatically perform windows update and vulnerability check
- Remotely installation software to reduce overhead

Screen Monitoring

- Monitor up to 16 screens at once
- Immediate response to unexpected matters
- Adjust recording frequency by applications
- Recorded screen history can be retrieved via event logs
- Support Windows, Linux, MAC OS

Device Management

- Ability to prohibit cell phone's MTP/PTP connection, mass storage device connected to endpoint computer and file transfer via Bluetooth protocol
- Effectively control various types of external devices include CD/DVD ROM drives, Non-system disks, USB Hubs, USB Mouse/keyboard/image device/storage device, Network cards, sound device, virtual CD/DVD ROM, movable device etc.
- Ability to restrict device by keyword
- Ability to restrict any new device
- Ability to endpoint computer to access unauthorized WIFI hotspot

Removable Device Management

- Ability set un-authorized USB device as a read-only device
- IP-guard Secure USB device has the ability to record offsite document operations on the device.
- Restrict USB Access authorities by users; the unauthorized user is prohibited to copy files to USB.
- Automatically encrypt document when its copy to IP-guard Encrypted USB device
- Provide details document operation logs on the USB device

Document Management

- Restrict document access right by computers, user name, disk type, path, application name or time
- Record document operations when add/modify/delete/move/upload/download and many other operations performed
- Backup document before delete/copy/modify operation
- Record shared folder operation activities, including copy from and copy to activities

Instant Messaging Management

- Supports various type of instant messaging applications such as Skype, Line, WeChat etc.
- Prevent document, image or file been sent via instant messaging application to prevent possible information breach
- Automatically backup files, images transfer via the instant messaging application
- Record content of instant messaging conversations

Print Management

- Prevent data leak by blocking unauthorized printing
- Detail printed log includes printed name, print time, document title, number of pages printed etc.
- Printed content stored in a un-changeable format which allows for future auditing
- Various types of watermarks can be applied to the printed page for security purposes

File Cloud Backup

- Scan files on the endpoint computers and centralize backup to cloud drive
- Built-in data deduplication algorithm to minimize required storage space
- Allow administrators to define backup file type and scheduled time

Remote Maintenance

- Ability to provide remote control to end user computer
- Remotely troubleshoot end-user computer issues in order to reduce system downtime
- Software uninstallation feature allows administrators to remove suspicious software

Bandwidth Management

- Monitor and control WAN and LAN Traffic
- Throttle network traffic by IP/Ports to reduce network traffic congestion
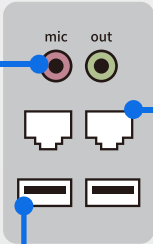
Network Management

- Manage network access by application, IP/Ports
- Manage and control network packages to prevent Trojan/Virus inflections
- Isolate a specific group of server/PC to enforce network security
- Provide software compliance feature to ensure all software on the endpoint computer meet the regulation of the company standard. Computer failed the test will be blocked from accessing the company network.

IP-guard The enterprise endpoint security solution

IP-guards 16 modules are a comprehensive management solution to counter all problems endpoint computers may encounter. It's also a cost-effective way to gain control over endpoint computers within an enterprise.

IP-guard Functionality Description

Basic Management	Basic Information, Basic Control, Event Alerts, Basic Policy, Policy Logs, Event Logs, Desktop Security Management
Application Management	Application Logs, Application Statistics, Application Usage Control, Software Installation Management, Screen Watermark
Website Management	Web Logs, Website Statistics, Website Control, Upload Control
Bandwidth Management	Traffic Statistics, Bandwidth Control
Document Management (**)	Document Operation Logs, Document Operation Control, Document Backup, Share Folder Operation Logs
Print Management (*)	Print Logs; Printed Content Recording; Print Control; Print Watermarks; Embedded QR code in print page
Screen Monitoring (**)	Instant Screen Snapshot, Multi-screen Monitoring, Screen History Playback
Remote Maintenance	Remote Maintenance, Remote Control, Remote File Transfer, Software Uninstall
Device Management (*)	Device Control, Block By Keyword, Block WIFI
Network Management (**)	Network Communication Control, Intrusion Detection
Email Management	Email & Attachment Logs, Email Control
Instant Messaging Management	Instant Messaging Conversation Logs, Instant message Document Transfer Control
Asset Management	Asset / Software License / Windows Patch/Vulnerability Management and Software Deployment, Software Uninstall
Removable Device Management (*)	Authorize Removable Device, Encrypt Removable Device, Device Operation Logs
Insight Report	Report Template, Schedule Email Report, Potential Risk Report
File Cloud Backup	Automatic backup, Data Deduplication

Note：Support Terminal Server, Thin Client, Multi-screen Computer and Safe Mode

(*) Included in Desktop Security Management
(**) Module Support Windows / Mac / Linux OS

IP-guard System Structure

IP-guard Server
Used to stored collected data and policies recommended to install IP-guard server on a computer/server equipt with high-performance CPU and mass storage space.

Console
Used to view collected data, define computer policies and perform real-time maintenance. It often installed on the administrator's computer or install together with IP-guard server.

IP-guard NAC
To restrict the unauthorized device to access the corporate network.