ENDPOINT PROTECTION

GV : Thạc Sĩ - Nguyễn Duy

Email : duyn@uit.edu.vn

Nội dung

- Endpoint Protection là gì?
- Tại sao lại sử dụng Endpoint Protection?
- Cơ chế hoạt động của Endpoint Protection?
- Công nghệ Endpoint Protection của IP-Guard?
- Tính năng của IP-Guard
- Triển khai IP-Guard

Nội dung

- **Endpoint Protection là gì?**
- Tại sao lại sử dụng Endpoint Security?
- Cơ chế hoạt động của Endpoint Security?
- Công nghệ Endpoint Security của IP-Guard?
- Tính năng của IP-Guard
- Triển khai IP-Guard

Endpoint Security là gì

- Endpoint Protection là giải pháp quản lý/quản trị đầu cuối (User và Computer)
- Endpoint Protection cho phép:
  - Quản lý thông tin phần cứng máy tính
  - Quản lý ứng dụng trên máy tính người dùng
  - Quản lý việc truy cập internet của người dùng
  - Quản lý các device (USB, Bluetooth, CD-ROM,…)

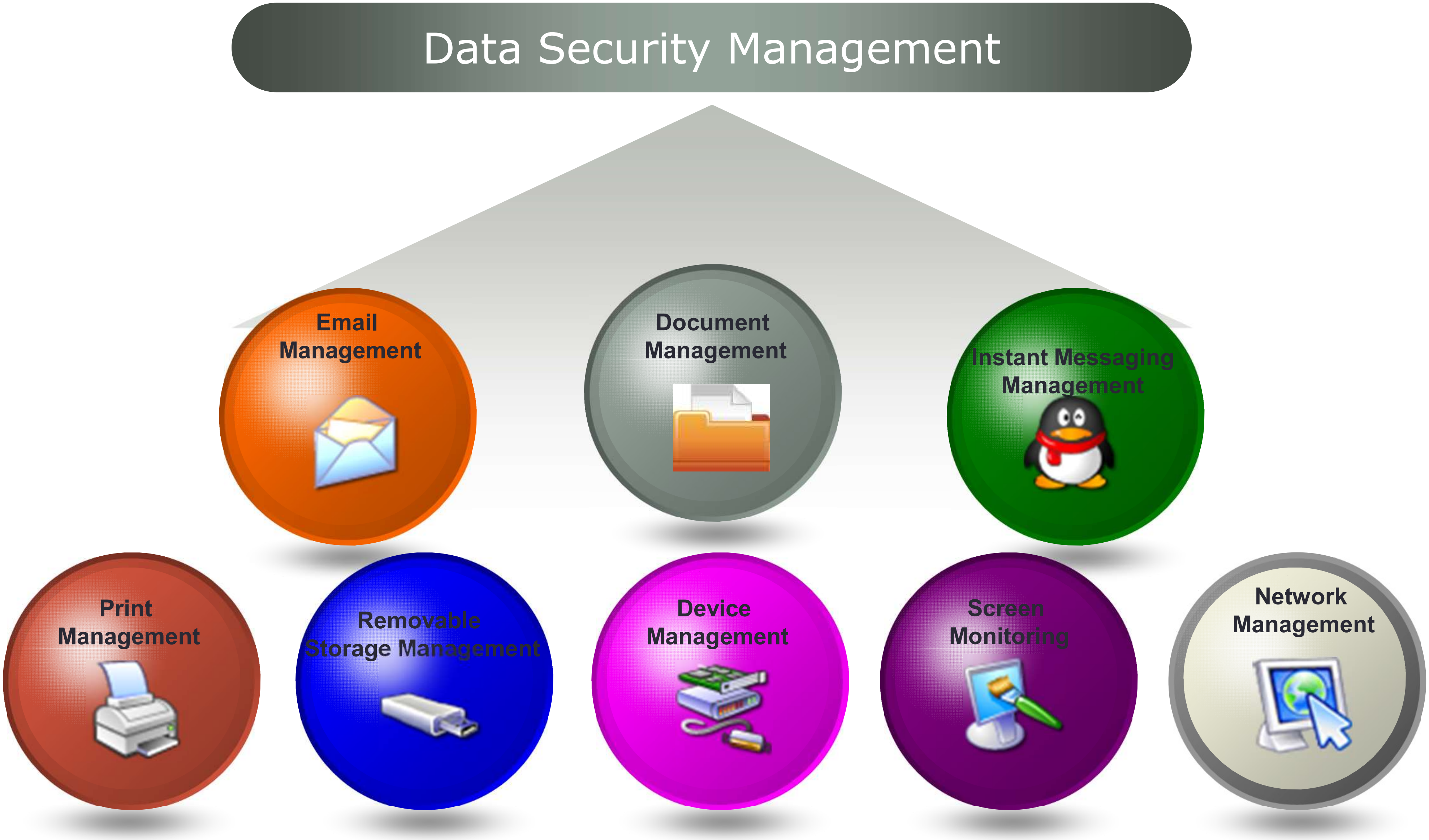
Nội dung

- Endpoint Security là gì?
- **Tại sao lại sử dụng Endpoint Security?**
- Cơ chế hoạt động của Endpoint Security?
- Công nghệ Endpoint Security của IP-Guard?
- Tính năng của IP-Guard
- Triển khai IP-Guard

Tại sao sử dụng Endpoint Security

- Quản lý bảo mật trực tiếp ở mức đầu cuối
  - Hardware
  - Device
  - Application
  - User
- Giảm lưu lượng gói tin không hợp lệ đi trong mạng
- Chi phí rẻ và linh động trong việc thay đổi công nghệ

Data Loss Prevention



Data Security Management

Email Management

Document Management

Instant Messaging Management

Print Management

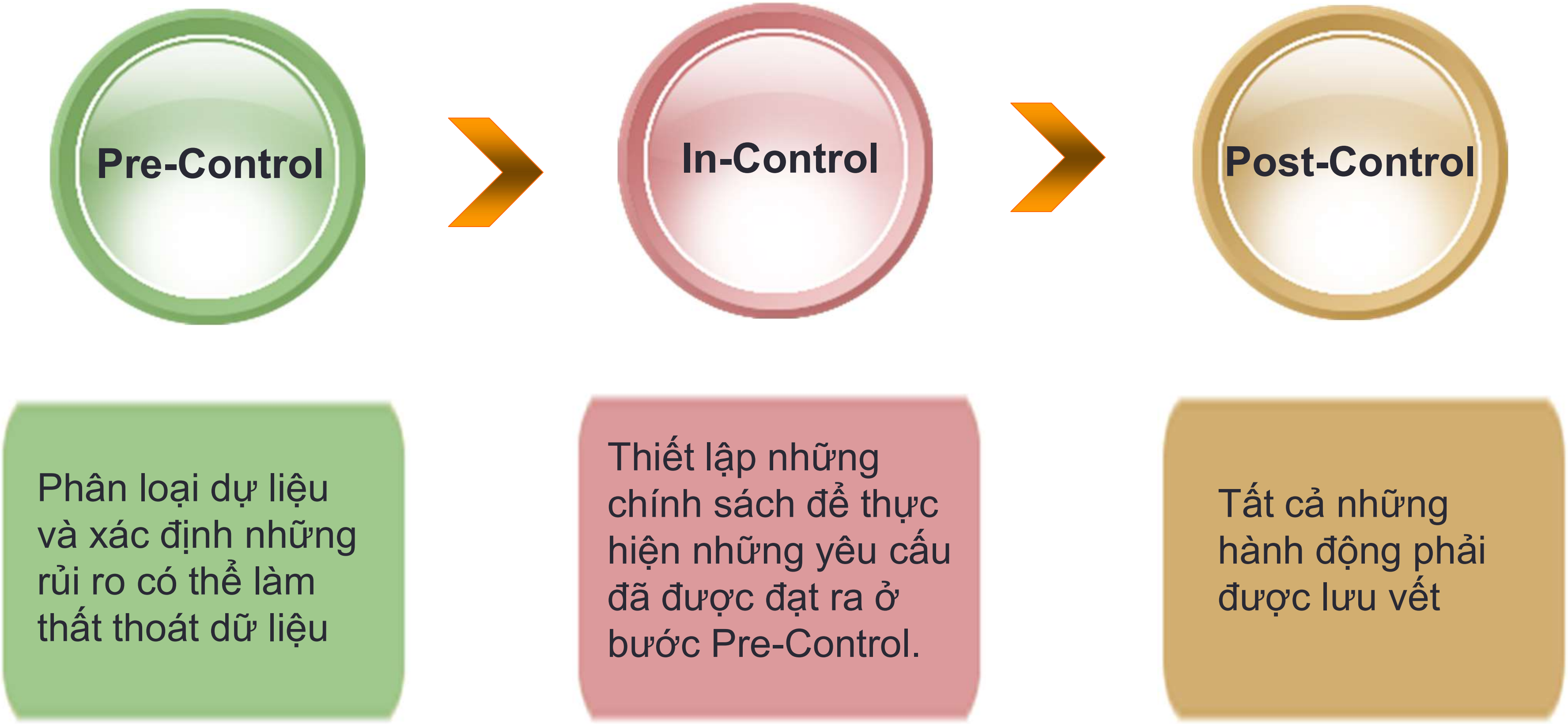
Removable Storage Management

Device Management

Screen Monitoring

Network Management

Data Loss Prevention



Pre-Control

In-Control

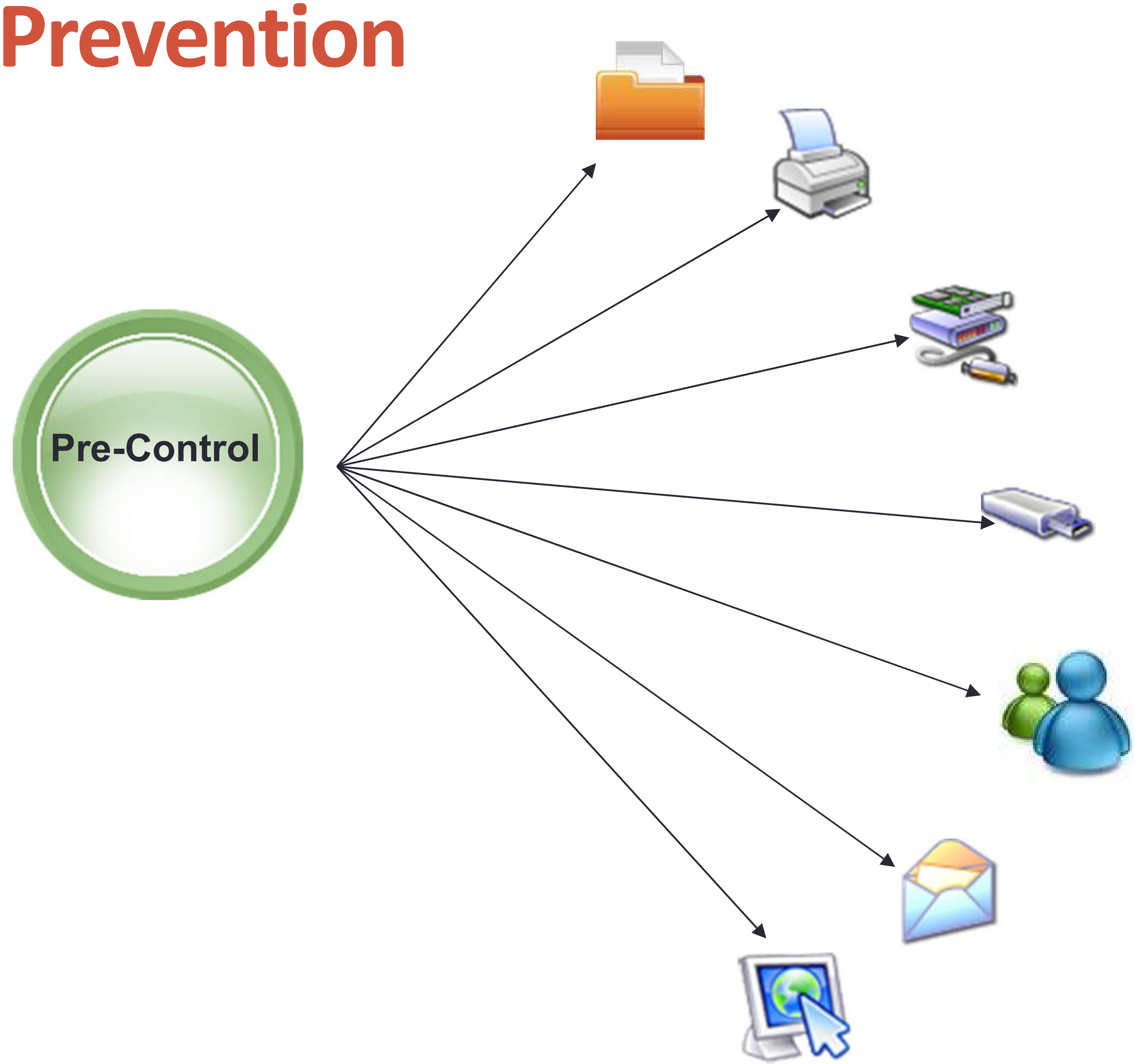
Post-Control

Phân loại dự liệu và xác định những rủi ro có thể làm thất thoát dữ liệu

Thiết lập những chính sách để thực hiện những yêu cầu đã được đạt ra ở bước Pre-Control.

Tất cả những hành động phải được lưu vết

Data Loss Prevention



Data Loss Prevention

In-Control

General Control

Document Management

Email Management

Device Management

Print Management

Instant Messaging Management

Offline Control

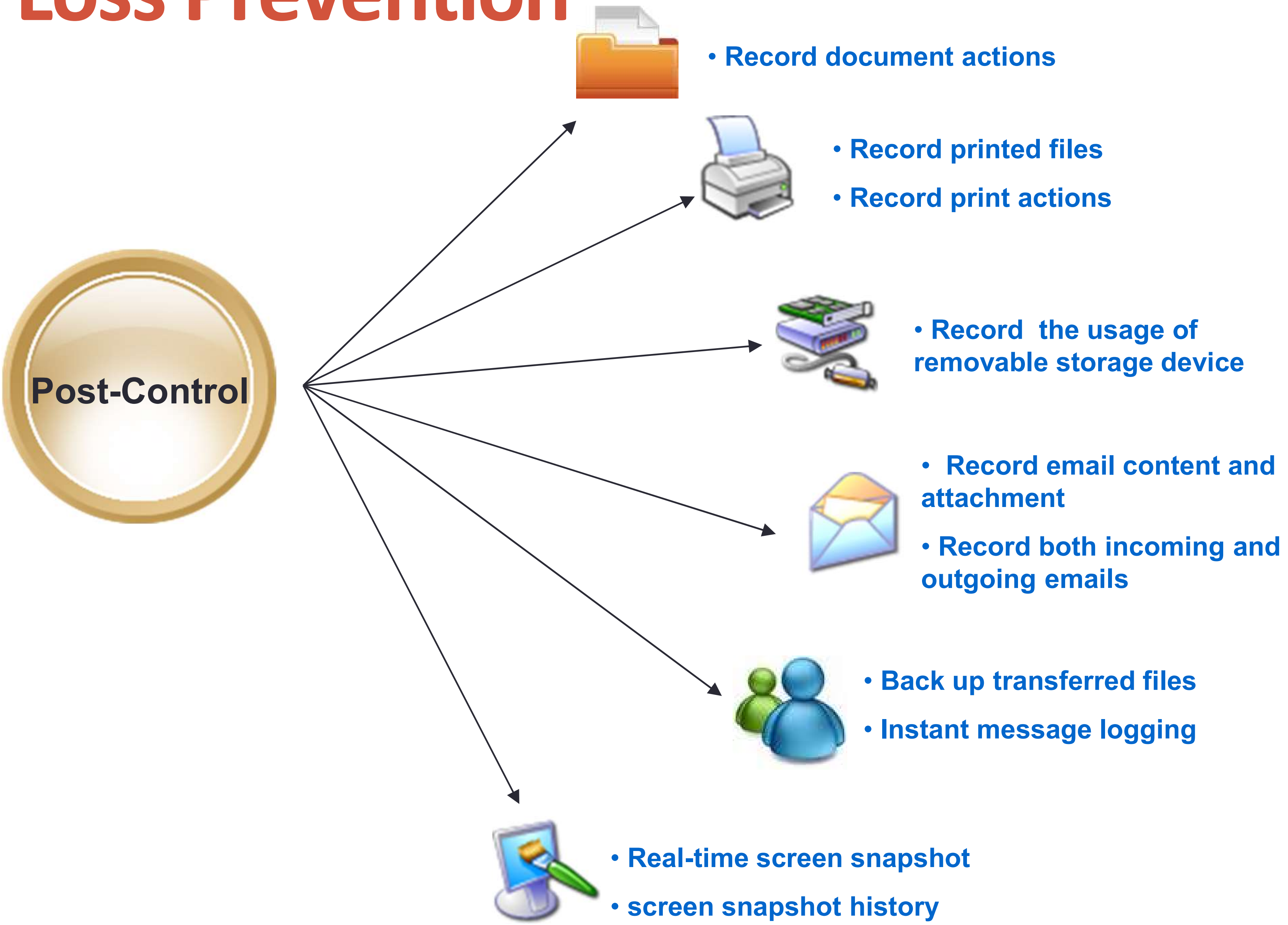
Những chính sách phải luôn luôn được thực thi ngay cả khi máy tính ở trang thái offline

Document Backup

* Sao lưu lại các tập tin trước khi được chỉnh sửa hoặc xóa

* Sao lưu lại các tập tin trước khi được gởi ra bên ngoài

Data Loss Prevention



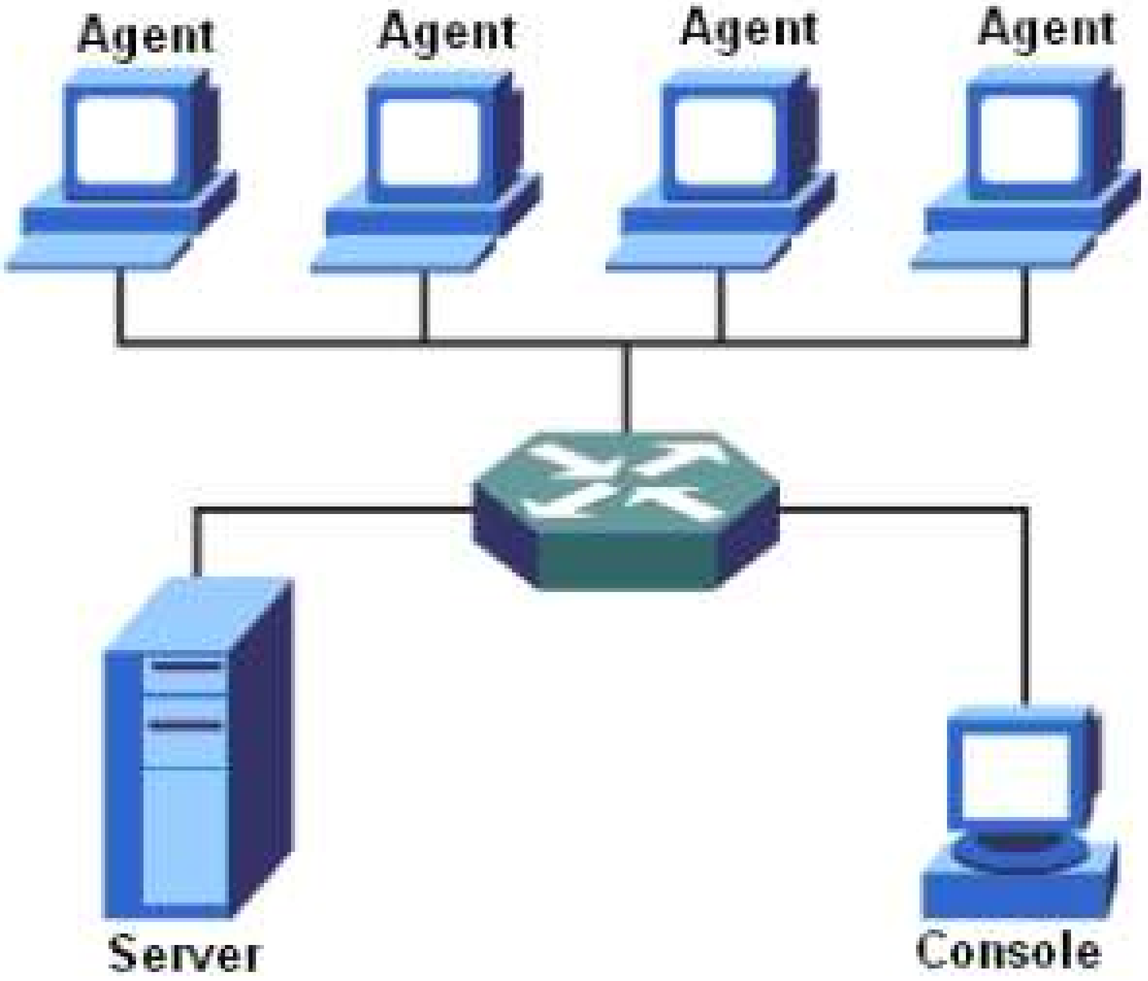
Post-Control

- Record document actions
- Record printed files
- Record print actions
- Record the usage of removable storage device
- Record email content and attachment
- Record both incoming and outgoing emails
- Back up transferred files
- Instant message logging
- Real-time screen snapshot
- screen snapshot history

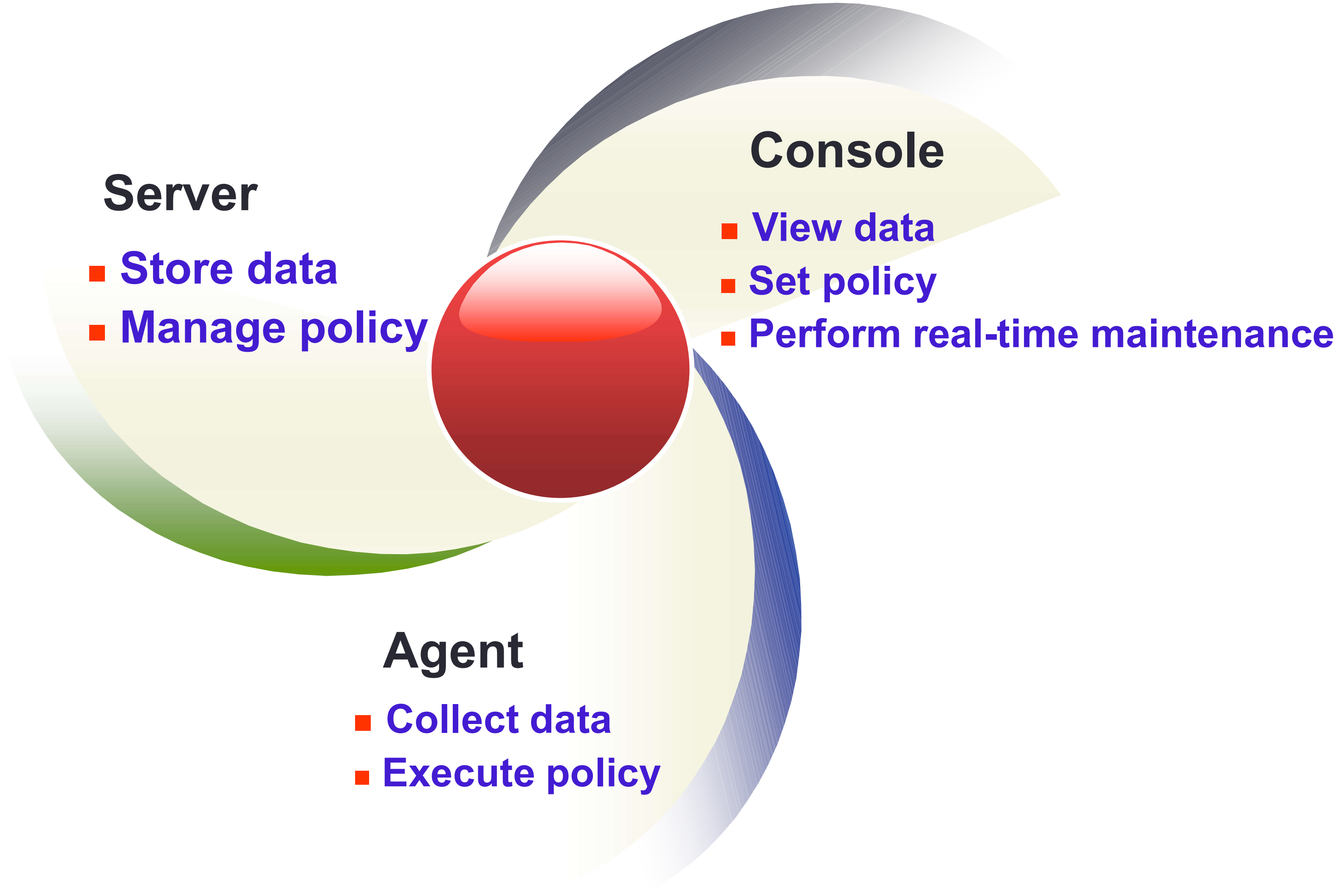
Nội dung

- Endpoint Protection là gì?
- Tại sao lại sử dụng Endpoint Protection?
- **Cơ chế hoạt động của Endpoint Protection?**
- Công nghệ Endpoint Security của IP-Guard?
- Tính năng của IP-Guard
- Triển khai IP-Guard

Mô hình hoạt động của Endpoint Security



Mô hình hoạt động của Endpoint Security



Console

- View data
- Set policy
- Perform real-time maintenance

Server

- Store data
- Manage policy

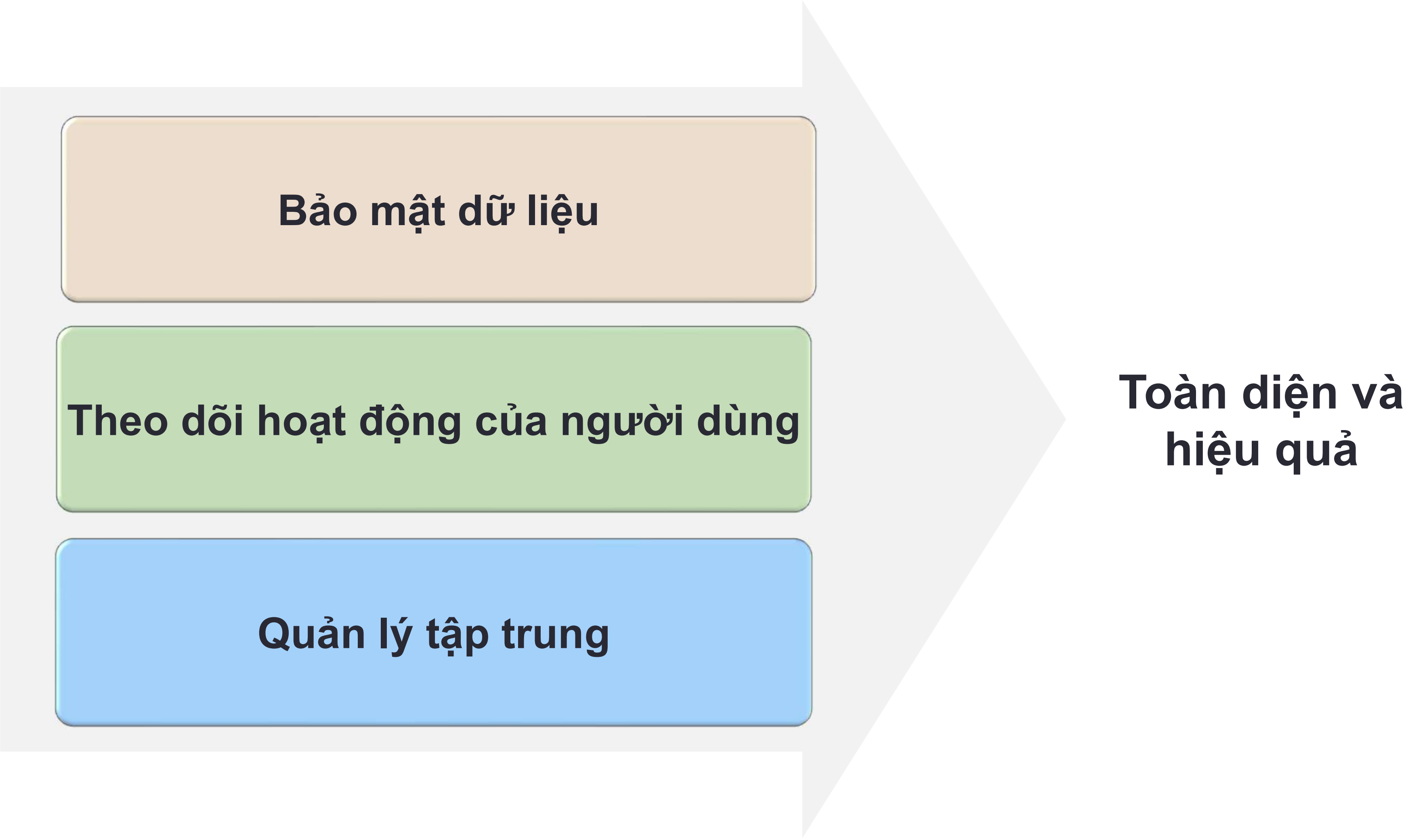
Agent

- Collect data
- Execute policy

Nội dung

- Endpoint Security là gì?
- Tại sao lại sử dụng Endpoint Security?
- Cơ chế hoạt động của Endpoint Security?
- **Công nghệ Endpoint Security của IP-Guard?**
- Tính năng của IP-Guard
- Triển khai IP-Guard

Công nghệ Endpoint Security – IP Guard



Bảo mật dữ liệu

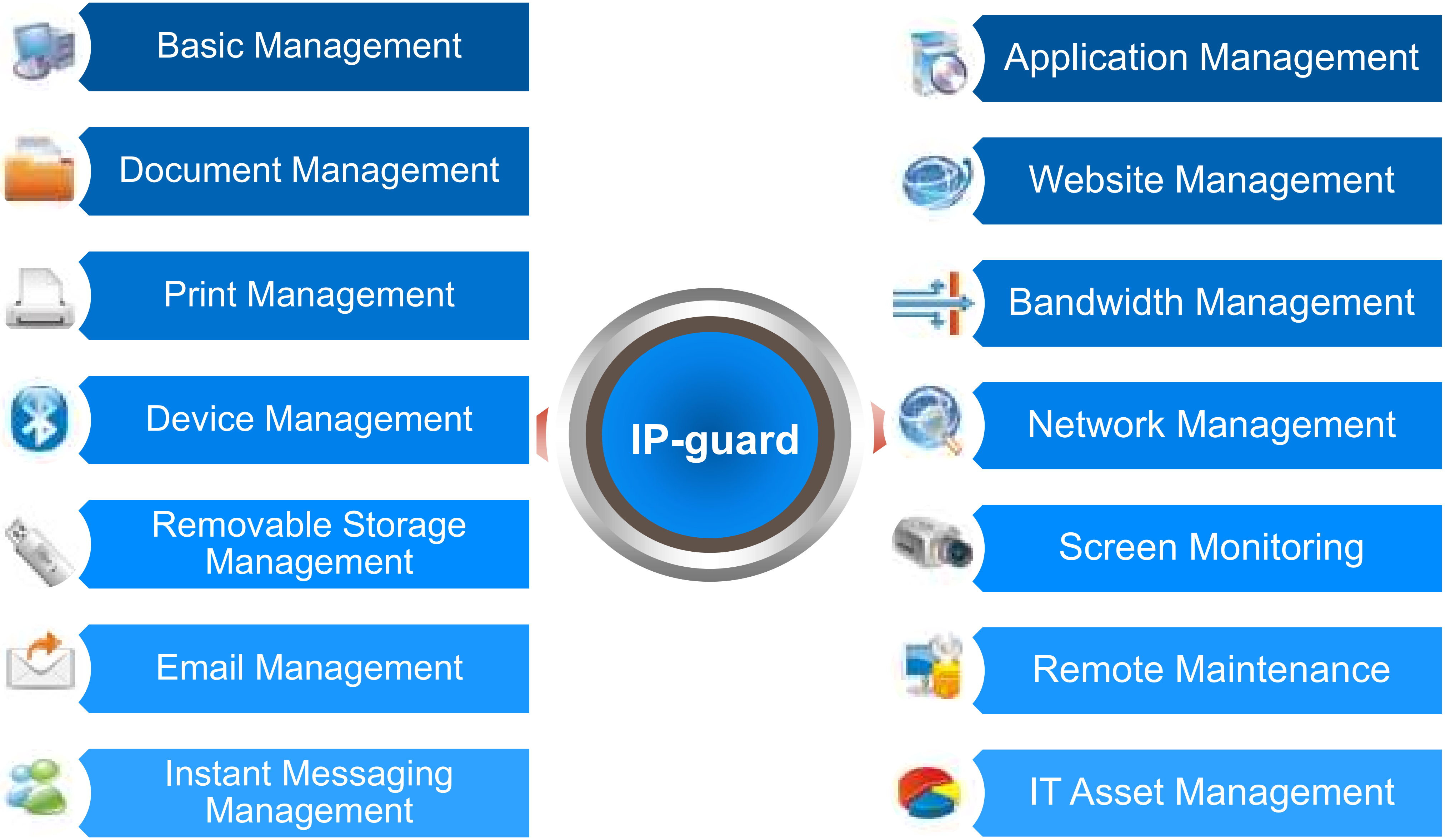
Theo dõi hoạt động của người dùng

Quản lý tập trung

Toàn diện và hiệu quả

Nội dung

- Endpoint Security là gì?
- Tại sao lại sử dụng Endpoint Security?
- Cơ chế hoạt động của Endpoint Security?
- Công nghệ Endpoint Security của IP-Guard?
- **Tính năng của IP-Guard**
- Triển khai IP-Guard



IP-guard

- Basic Management
- Document Management
- Print Management
- Device Management
- Removable Storage Management
- Email Management
- Instant Messaging Management
- Application Management
- Website Management
- Bandwidth Management
- Network Management
- Screen Monitoring
- Remote Maintenance
- IT Asset Management

Basic Management Module

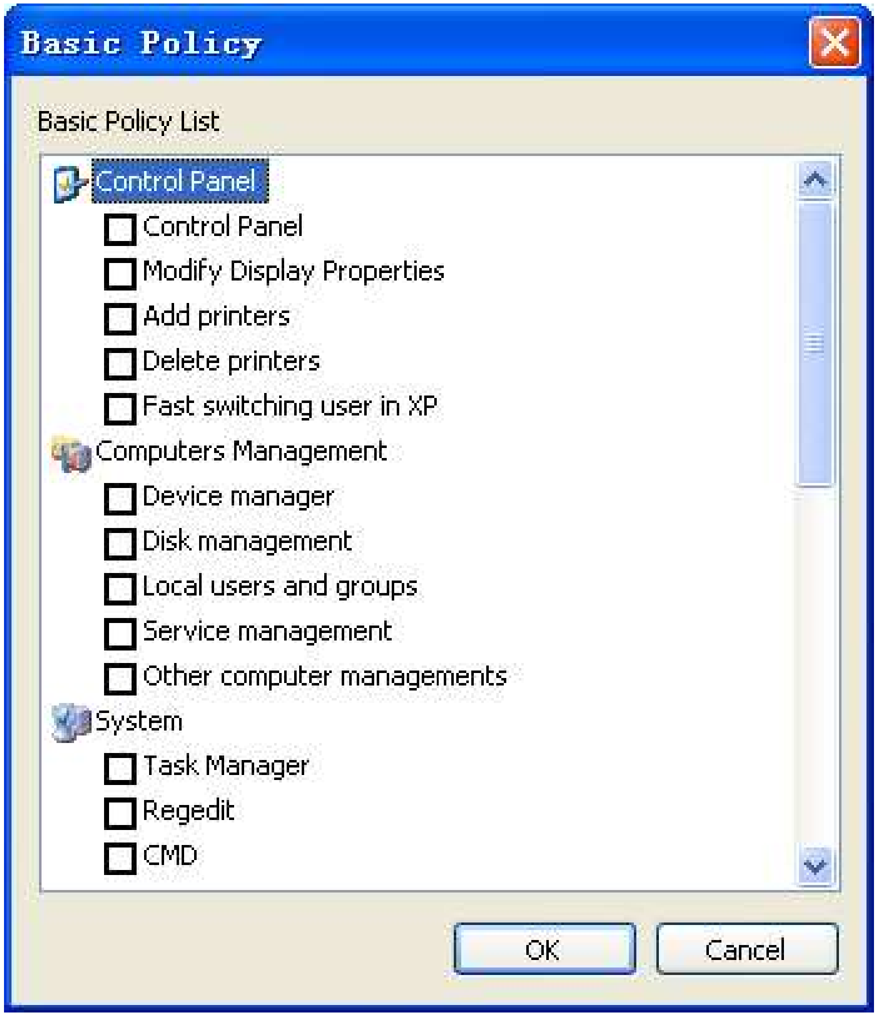
Basic and essential module of IP-guard. It’s a mandatory module.

- Basic Events Log
  - Record computer startup, logon, logoff, shutdown to check when do your employee start working and what time do they leave their workstations
- Basic Control
  - Remotely lock, log off, restart and turn off agent computers to manage computers or stop illegal operations
- Basic Policy
  - Block users from randomly modify system setting in order to prevent accidental and intentional destruction and improve system security.

Basic Management Module

Basic Policy

- Basic Policy
  - Control Panel
- Computers Management
  - System
  - Network
  - IP/Mac Binding
  - ActiveX
  - Others



Basic Policy

Basic Policy List

Control Panel
- □ Control Panel
- □ Modify Display Properties
- □ Add printers
- □ Delete printers
- □ Fast switching user in XP

Computers Management
- □ Device manager
- □ Disk management
- □ Local users and groups
- □ Service management
- □ Other computer managements

System
- □ Task Manager
- □ Regedit
- □ CMD

Document Management Module

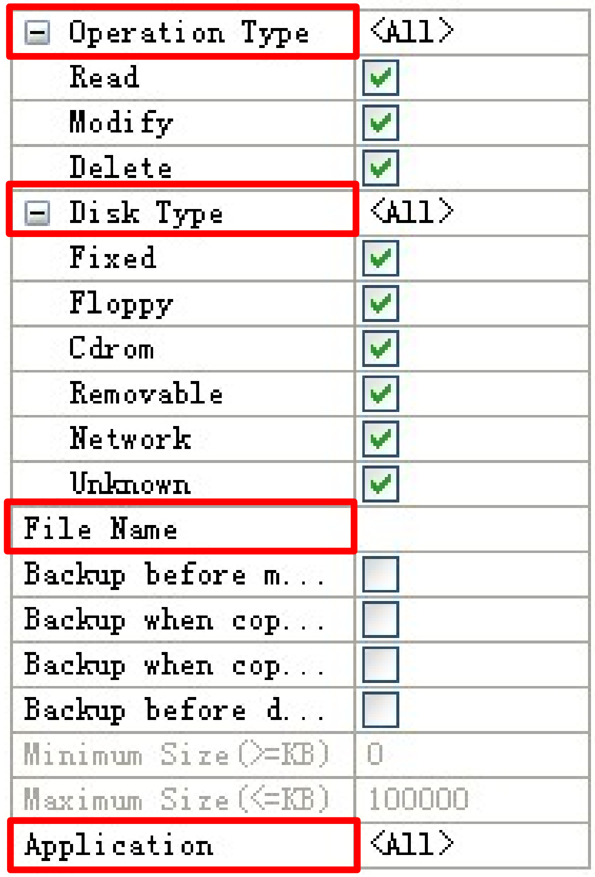
Control and monitor document actions to safeguard intellectual property

- Document Control
  - Effectively control document actions to prevent unauthorized actions, malicious modification and deletion.
- Document Backup
  - Back up documents before they are modified or deleted to make sure the security of important documents
- Document Logging
  - Record document actions in detail
  - Record document actions of any computer on shared documents

Document Management Module

Document Policy

- Document Control
  - By file name
  - By operation type
  - By disk type
  - By application



⊟ Operation Type	<All>
Read	☑
Modify	☑
Delete	☑
⊟ Disk Type	<All>
Fixed	☑
Floppy	☑
Cdrom	☑
Removable	☑
Network	☑
Unknown	☑
File Name	
Backup before m...	□
Backup when cop...	□
Backup when cop...	□
Backup before d...	□
Minimum Size(>=KB)	0
Maximum Size(<=KB)	100000
Application	<All>

Print Management

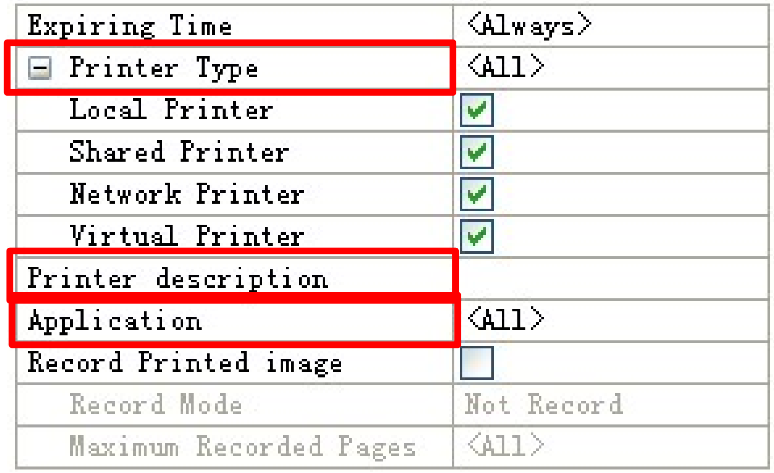
Monitor file printing to prevent data leakage

- Print Control
  - Control printing permission to prevent data leakage
  - Reasonably assign print resource to stop wasting print resource
- Print Logging
  - Record print actions in detail for administrator to evaluate the effective usage of print resource
- Print Backup
  - Back up the image of printed file

Print Management

Print Control

- Print Control
  - By printer type
  - By application
  - By Printer name



Expiring Time	<Always>
⊟ Printer Type	<All>
Local Printer	☑
Shared Printer	☑
Network Printer	☑
Virtual Printer	☑
Printer description	
Application	<All>
Record Printed image	□
Record Mode	Not Record
Maximum Recorded Pages	<All>

Device Management

Control and monitor the usage of various devices to prevent data leakage

- Device Control
  - Block external devices from connecting to the intranet to protect data security and stop data breaches
  - Detailed and specific control

List of Controlled Device

- Storage Devices
  - Floppy, CDROM, Burning Device, Tape, Removable Storage Device
- Communications Devices
  - COM, LTP, Bluetooth, Infrared, SCSI Controller, etc.
- Dialup
  - Dial-up Connection
- USB Devices
  - USB hard disk, USB CDROME、USB LAN Adapter, USB Image Device, etc.
- Network Devices
  - Wireless LAN Adapter, Virtual LAN Adapter, PnP Adapter (USB, PCAMCIA)
- Others
  - Audio device, Virtual LAN Adapter
- Any added new devices

Removable Storage Management

Authorize and encrypt removable storage device to protect your valuable data anywhere at anytime.

- Permission Control
  - Strictly control file in motion to protect data
- Automatic Encryption & Decryption
  - Automatically encrypt data when files are written to any removable storage device to enhance the security level of data in motion
- Whole Disk Encryption
  - Format corporate removable storage device as encrypted removable storage device.
  - Automatically encrypt and decrypt data stored on the encrypted removable storage device within the corporate environment.

* NOTE: Encrypted removable storage device only can be used within the corporate environment

Email Management

Control and monitor incoming and outgoing emails to prevent data leakage

- Email Control
  - Block sending specified POP3/SMTP emails or Exchanges emails out of the organization via email to prevent data leakage
- Email Logging
  - Fully record sender, recipient, subject, text and attachment
  - Support POP3/SMTP email, Exchange email, webmail, and Lotus email

Instant Messaging Management

Control and monitor instant messaging to safeguard data security and improve work efficiency

- IM Logging
  - Completely record instant messages, participants, time to prevent data leaking out via IM applications
- File Transfer Control
  - Block sending files out of the corporation over limited size or with limited file names
- File Backup
  - Back up transferred file

Application Management

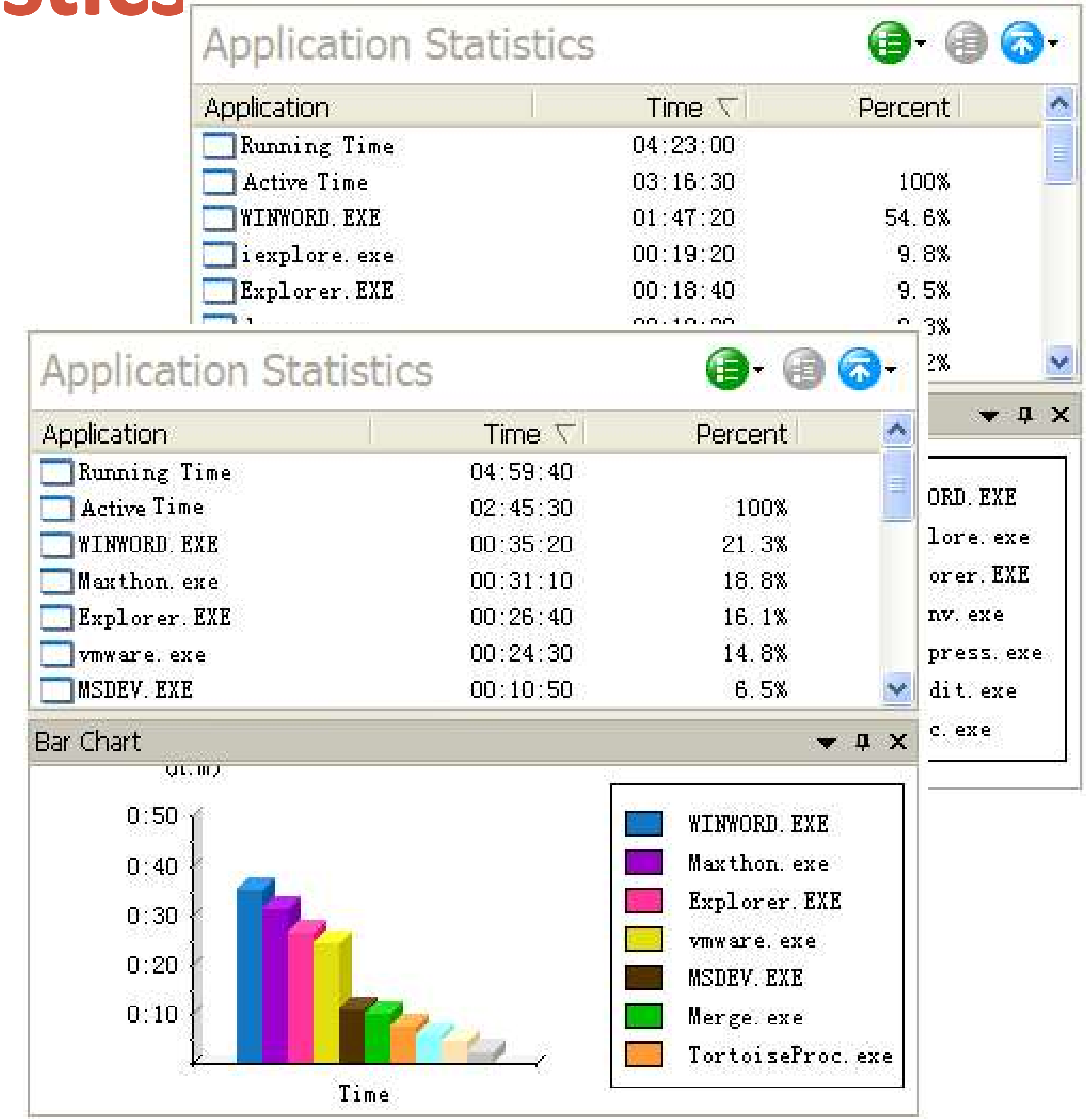
- Control and monitor application usage to improve work efficiency

- Application Statistics
  - Gather statistics by category, name, detail and group to let you know your employee’s work performance
- Application Control
  - Filter non-work related applications to make your employees concentrate on work business
  - Block malicious application to protect computer security
- Application Log
  - Record application start, stop, window switch to track the application activity of staff

Application Management

Application Statistics

- Application Statistics
  - Gather statistics by category
  - Gather statistics by name
  - Gather statistics by detail
  - Gather statistics by group



Application Statistics

Application	Time	Percent
Running Time	04:23:00	
Active Time	03:16:30	100%
WINWORD.EXE	01:47:20	54.6%
iexplore.exe	00:19:20	9.8%
Explorer.EXE	00:18:40	9.5%

Application Statistics

Application	Time	Percent
Running Time	04:59:40	
Active Time	02:45:30	100%
WINWORD.EXE	00:35:20	21.3%
Maxthon.exe	00:31:10	18.8%
Explorer.EXE	00:26:40	16.1%
vmware.exe	00:24:30	14.8%
MSDEV.EXE	00:10:50	6.5%

Website Management

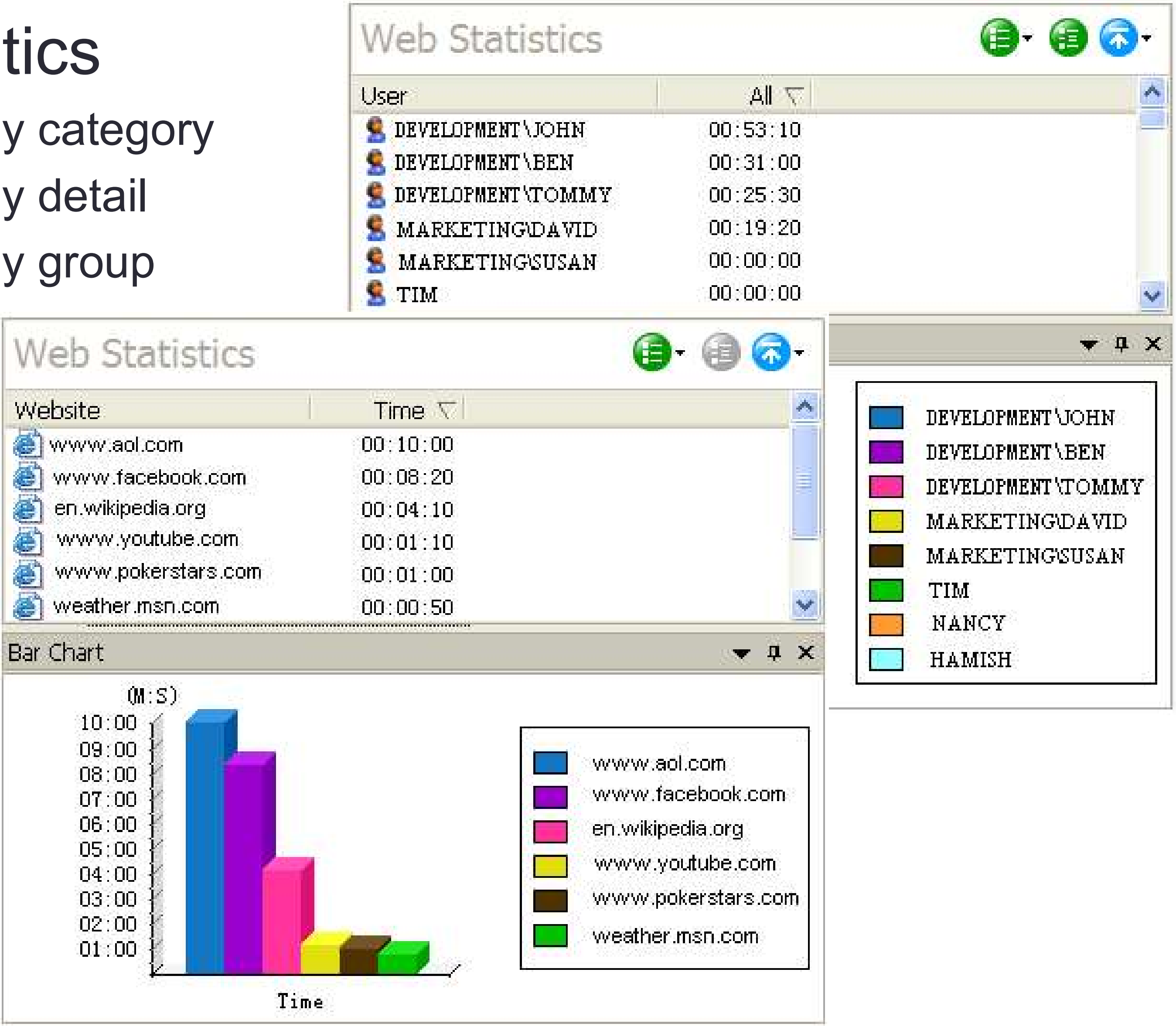
Record staff’s web browsing activities; limit web site access right to regulate staff’s online activity

- Website Statistics
  - Gather statistics by different ways to let you know your staff’s web browsing activity
- Website Management
  - Filter non-work related websites during a specified time period
  - Block malicious and inappropriate websites
- Website Log
  - Record the URL, caption, and time of the visited websites to track what your staff were browsing during office hours

Website Management

Website Statistics

- Website Statistics
  - Gather statistics by category
  - Gather statistics by detail
  - Gather statistics by group



Web Statistics

User	All
DEVELOPMENT\JOHN	00:53:10
DEVELOPMENT\BEN	00:31:00
DEVELOPMENT\TOMMY	00:25:30
MARKETING\DAVID	00:19:20
MARKETING\SUSAN	00:00:00
TIM	00:00:00

- 🟦 DEVELOPMENT\JOHN
- 🟪 DEVELOPMENT\BEN
- 🟥 DEVELOPMENT\TOMMY
- 🟨 MARKETING\DAVID
- 🟫 MARKETING\SUSAN
- 🟩 TIM
- 🟧 NANCY
- 🟦 HAMISH

Web Statistics

Website	Time
www.aol.com	00:10:00
www.facebook.com	00:08:20
en.wikipedia.org	00:04:10
www.youtube.com	00:01:10
www.pokerstars.com	00:01:00
weather.msn.com	00:00:50

Bar Chart

- 🟦 www.aol.com
- 🟪 www.facebook.com
- 🟥 en.wikipedia.org
- 🟨 www.youtube.com
- 🟫 www.pokerstars.com
- 🟩 weather.msn.com

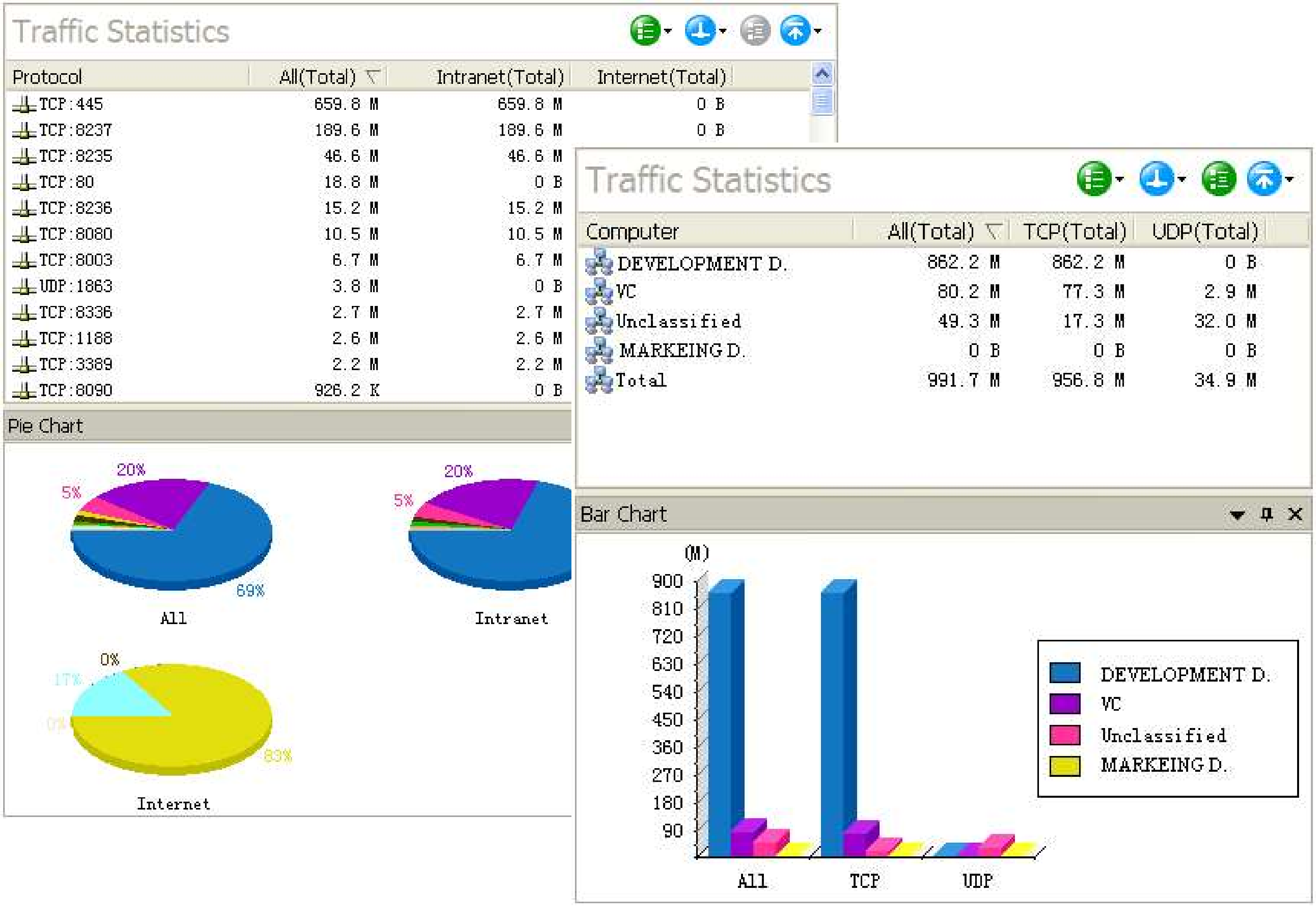
Bandwidth Management

- Limit and control bandwidth to avoid any bandwidth abuse

- Traffic Statistics
  - Gather statistics by different ways to assist administrator to analyze traffic consumption
- Bandwidth Control
  - Limit bandwidth by IP address or port to help administrator reasonably assign various bandwidth to different users
  - Limit BT download, online video watching to make sure that you have sufficient bandwidth for business use

Bandwidth Management

Traffic Statistics



Traffic Statistics

Protocol	All(Total)	Intranet(Total)	Internet(Total)
TCP:445	659.8 M	659.8 M	0 B
TCP:8237	189.6 M	189.6 M	0 B
TCP:8235	46.6 M	46.6 M	
TCP:80	18.8 M	0 B	
TCP:8236	15.2 M	15.2 M	
TCP:8080	10.5 M	10.5 M	
TCP:8003	6.7 M	6.7 M	
UDP:1863	3.8 M	0 B	
TCP:8336	2.7 M	2.7 M	
TCP:1188	2.6 M	2.6 M	
TCP:3389	2.2 M	2.2 M	
TCP:8090	926.2 K	0 B	

Pie Chart

Traffic Statistics

Computer	All(Total)	TCP(Total)	UDP(Total)
DEVELOPMENT D.	862.2 M	862.2 M	0 B
VC	80.2 M	77.3 M	2.9 M
Unclassified	49.3 M	17.3 M	32.0 M
MARKEING D.	0 B	0 B	0 B
Total	991.7 M	956.8 M	34.9 M

Bar Chart

Network Management

- Prevent unauthorized external computers from accessing internal network

- Network Control
  - Offer firewall function and block unauthorized computer from communication with internal computers in order to protect intranet security
- Network Intrusion Detection
  - Scan the whole network to immediately stop unauthorized computers from connecting to the internal network so as to safeguard information security

Screen Monitoring

Record and replay screen snapshot to let you know what your employees do step by step

- Screen Monitoring
  - View the real-time desktop screen of any computer
  - Monitor computers with multi displays
  - Centrally monitor multi computers at one time

- Screen Record
  - Completely record screen history for your latter review
  - Set different intervals to capture screen snapshot when different application are being used so as to pay attention to risky applications
  - Can save a lot of screen snapshots due to effective compression
  - Screen history can be exported to wmv format.

Remote Maintenance

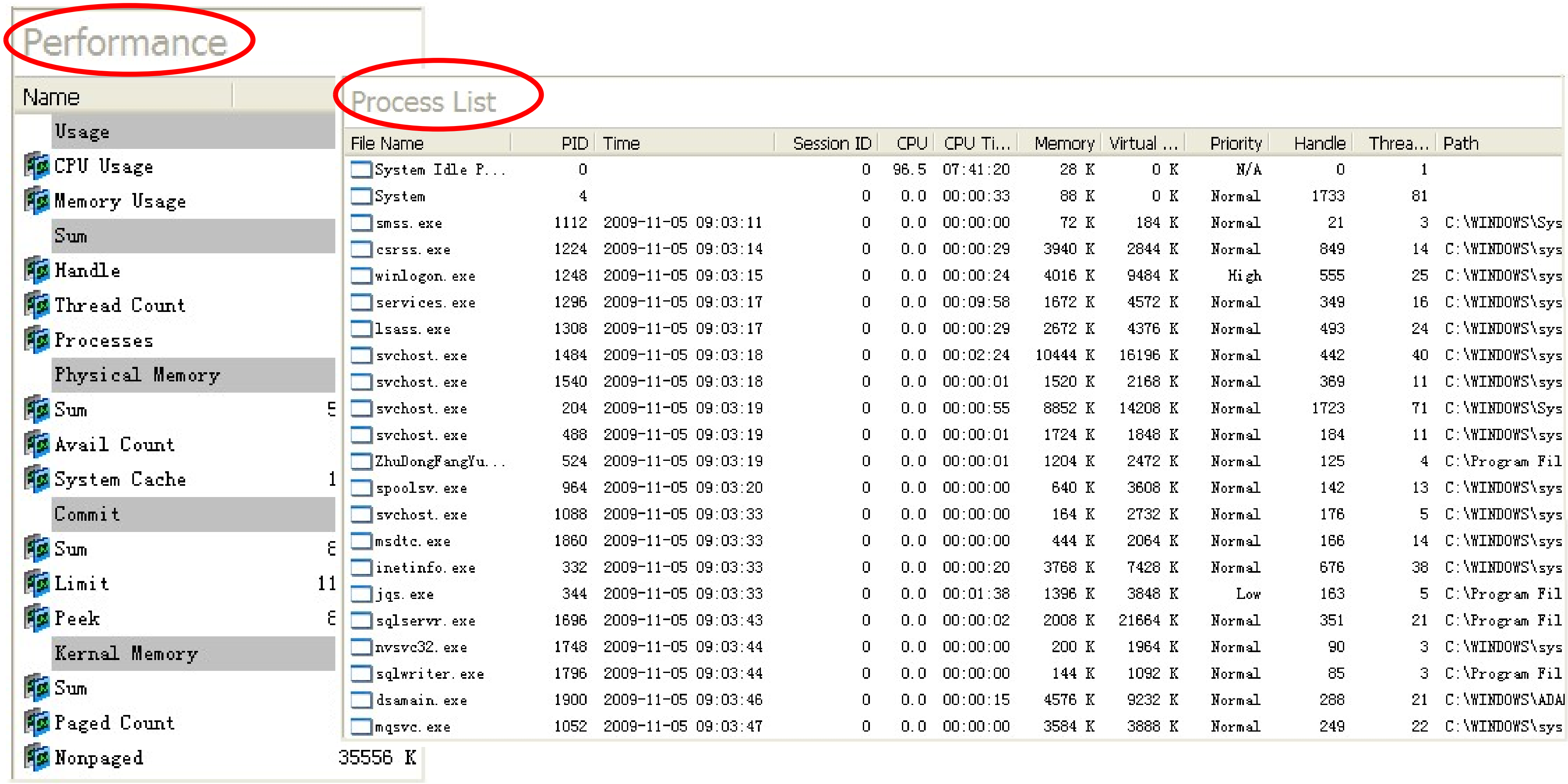
- Support remote maintenance so as to let you shorten the downtime and quickly solve the system problem

- Remote Troubleshooting
  - Check the real-time running processes of client computers
  - Remotely analyze the running status, system fault and device status of client computers
- Remote Control
  - Perform remote assistance or demonstrate operational instruction
- Remote File Transfer
  - Remotely transfer files from remote computers to local computer, and from local computer to remote computers in order to quickly gather fault samples to diagnose the problem and update files

Remote Maintenance

Maintenance

- Centrally view the running status of any remote computer through IP-guard console



Performance

Name	
Usage	
CPU Usage	
Memory Usage	
Sum	
Handle	
Thread Count	
Processes	
Physical Memory	
Sum	5
Avail Count	
System Cache	1
Commit	
Sum	8
Limit	11
Peek	8
Kernal Memory	
Sum	
Paged Count	
Nonpaged	35556 K

Process List

File Name	PID	Time	Session ID	CPU	CPU Ti...	Memory	Virtual ...	Priority	Handle	Threa...	Path
System Idle P...	0		0	96.5	07:41:20	28 K	0 K	N/A	0	1	
System	4		0	0.0	00:00:33	88 K	0 K	Normal	1733	81	
smss.exe	1112	2009-11-05 09:03:11	0	0.0	00:00:00	72 K	184 K	Normal	21	3	C:\WINDOWS\Sys
csrss.exe	1224	2009-11-05 09:03:14	0	0.0	00:00:29	3940 K	2844 K	Normal	849	14	C:\WINDOWS\sys
winlogon.exe	1248	2009-11-05 09:03:15	0	0.0	00:00:24	4016 K	9484 K	High	555	25	C:\WINDOWS\sys
services.exe	1296	2009-11-05 09:03:17	0	0.0	00:09:58	1672 K	4572 K	Normal	349	16	C:\WINDOWS\sys
lsass.exe	1308	2009-11-05 09:03:17	0	0.0	00:00:29	2672 K	4376 K	Normal	493	24	C:\WINDOWS\sys
svchost.exe	1484	2009-11-05 09:03:18	0	0.0	00:02:24	10444 K	16196 K	Normal	442	40	C:\WINDOWS\sys
svchost.exe	1540	2009-11-05 09:03:18	0	0.0	00:00:01	1520 K	2168 K	Normal	369	11	C:\WINDOWS\sys
svchost.exe	204	2009-11-05 09:03:19	0	0.0	00:00:55	8852 K	14208 K	Normal	1723	71	C:\WINDOWS\Sys
svchost.exe	488	2009-11-05 09:03:19	0	0.0	00:00:01	1724 K	1848 K	Normal	184	11	C:\WINDOWS\sys
ZhuDongFangYu...	524	2009-11-05 09:03:19	0	0.0	00:00:01	1204 K	2472 K	Normal	125	4	C:\Program Fil
spoolsv.exe	964	2009-11-05 09:03:20	0	0.0	00:00:00	640 K	3608 K	Normal	142	13	C:\WINDOWS\sys
svchost.exe	1088	2009-11-05 09:03:33	0	0.0	00:00:00	164 K	2732 K	Normal	176	5	C:\WINDOWS\sys
msdtc.exe	1860	2009-11-05 09:03:33	0	0.0	00:00:00	444 K	2064 K	Normal	166	14	C:\WINDOWS\sys
inetinfo.exe	332	2009-11-05 09:03:33	0	0.0	00:00:20	3768 K	7428 K	Normal	676	38	C:\WINDOWS\sys
jqs.exe	344	2009-11-05 09:03:33	0	0.0	00:01:38	1396 K	3848 K	Low	163	5	C:\Program Fil
sqlservr.exe	1696	2009-11-05 09:03:43	0	0.0	00:00:02	2008 K	21664 K	Normal	351	21	C:\Program Fil
nvsvc32.exe	1748	2009-11-05 09:03:44	0	0.0	00:00:00	200 K	1964 K	Normal	90	3	C:\WINDOWS\sys
sqlwriter.exe	1796	2009-11-05 09:03:44	0	0.0	00:00:00	144 K	1092 K	Normal	85	3	C:\Program Fil
dsamain.exe	1900	2009-11-05 09:03:46	0	0.0	00:00:15	4576 K	9232 K	Normal	288	21	C:\WINDOWS\ADAI
mqsvc.exe	1052	2009-11-05 09:03:47	0	0.0	00:00:00	3584 K	3888 K	Normal	249	22	C:\WINDOWS\sys

IT Asset Management

Easily manage IT asset to reduce management cost

- Asset Information
  - Automatically collect software and hardware information and provide asset inventory to facilitate administrator’s management
  - Offer non-IT asset management function
- Asset Change
  - Record software and hardware changes in detail
  - Instant alert on asset changes

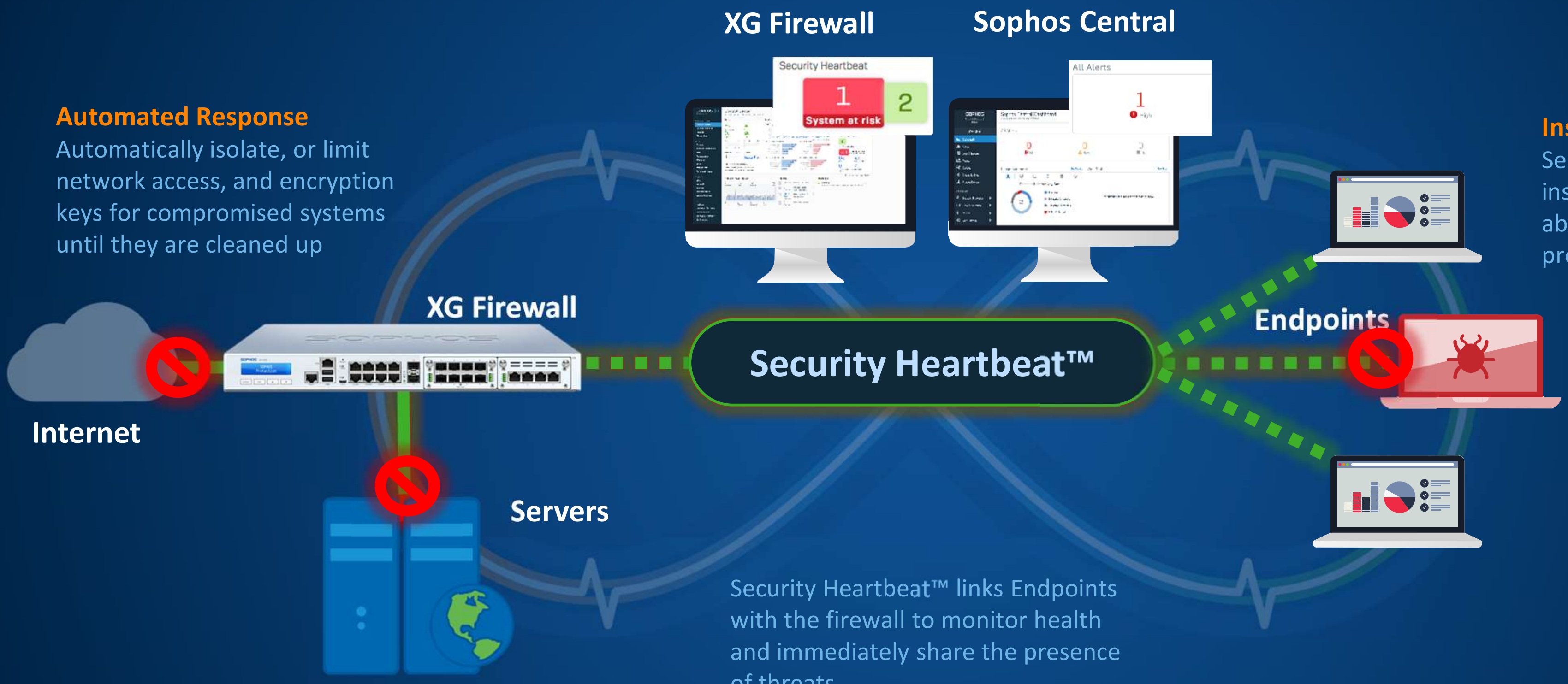
IT Asset Management

- Vulnerability Management
  - Automatically scan system vulnerability of agent computer and provide easy-to-read report and solutions
- Patch Management
  - Check Microsoft for new patches at regular intervals
  - Automatically download and deploy new patches to agent computers
- Software Deployment
  - Deploy files and programs with ease
  - Support breakpoint transmission to facilitate background installation and interactive installation

Nội dung

- Endpoint Security là gì?
- Tại sao lại sử dụng Endpoint Security?
- Cơ chế hoạt động của Endpoint Security?
- Công nghệ Endpoint Security của IP-Guard?
- Tính năng của IP-Guard
- **Triển khai IP-Guard**

Synchronized Security - Automatically Responding



Automated Response

Automatically isolate, or limit network access, and encryption keys for compromised systems until they are cleaned up

Instant Identification

Security Heartbeat can instantly share telemetry about the user, systems and process responsible

Security Heartbeat™ links Endpoints with the firewall to monitor health and immediately share the presence of threats.

XG Firewall is the only firewall using endpoint health in firewall rules!

THE END