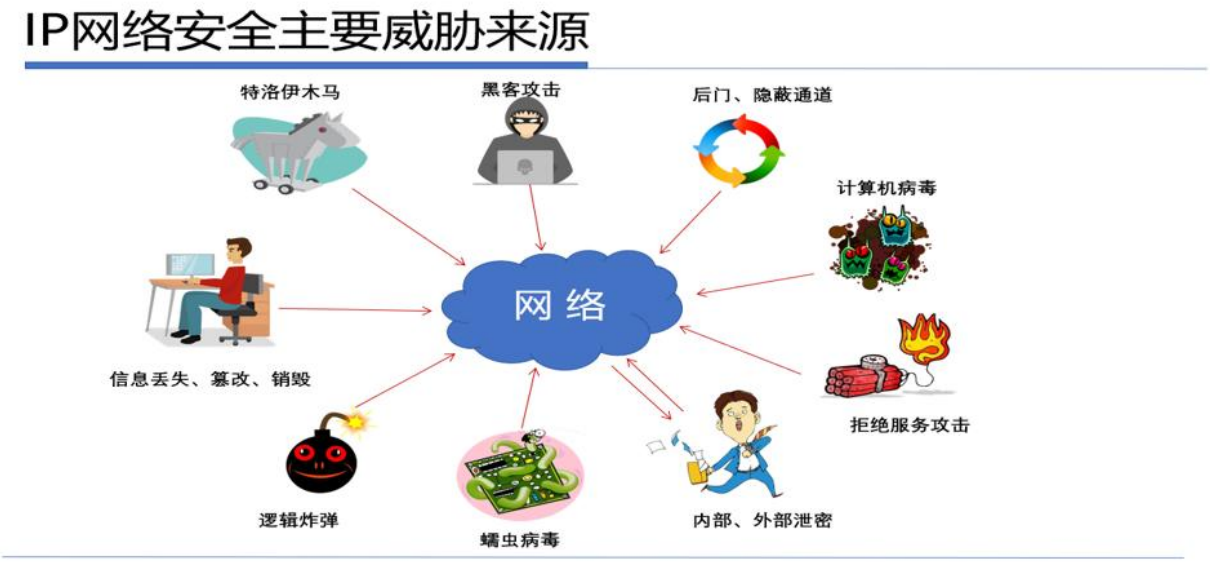
Document Ferry System

Product Overview

The Inventsoft Document Ferry System establishes a secure channel for file and information transfer between internal and external networks. It ensures that the secure channel is unified, and files and information are transmitted between the internal and external networks through this channel. The system comes with an instant messaging software system. Based on legal and compliant principles, it adopts an integrated software and hardware design, enabling a single device to handle file and message transfer between multiple networks. It provides a secure, efficient, and reliable file information management and transfer solution for enterprises and institutions with high security requirements, such as hospitals. This significantly improves the organization's office efficiency and data security and is an essential intelligent tool for modern organizations.

Product Features and Advantages

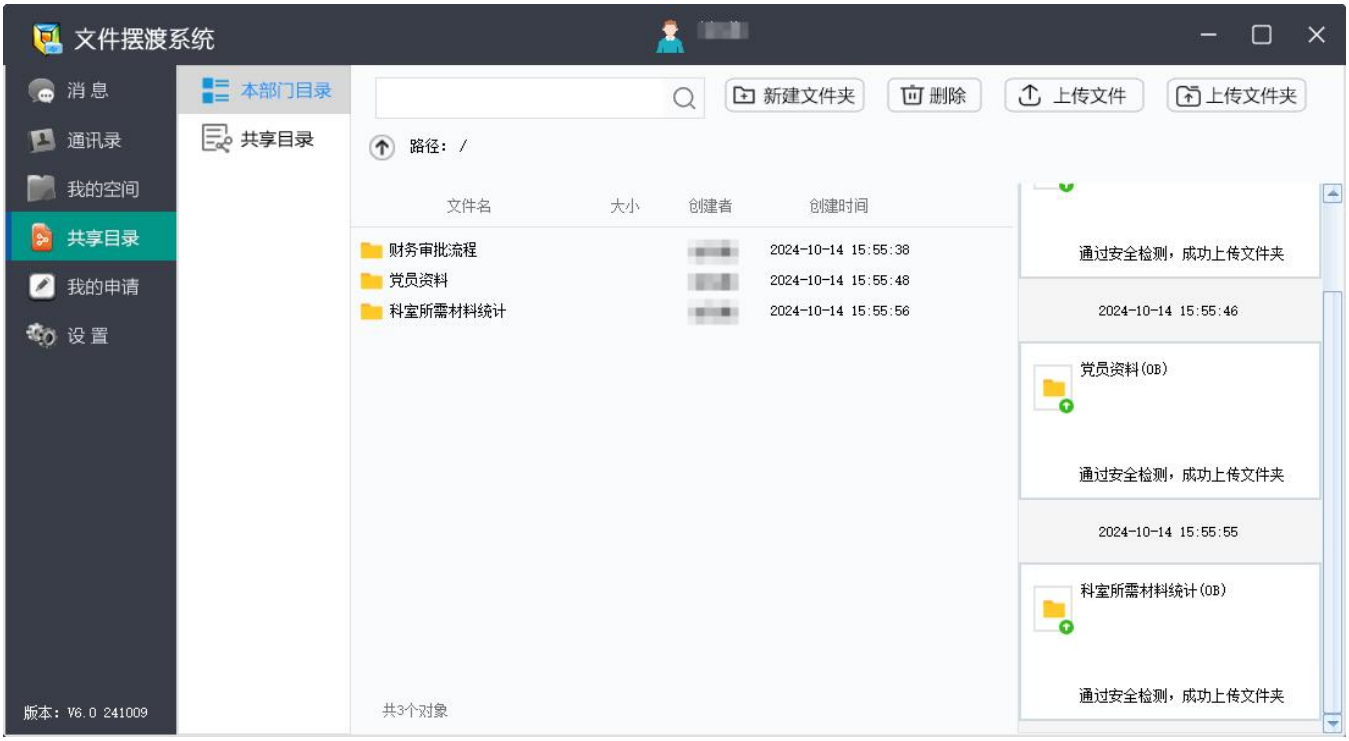
1. Does not change the original network isolation properties.
2. Integrated software and hardware design for simple and convenient deployment.
3. Non-IP communication to prevent external attacks.

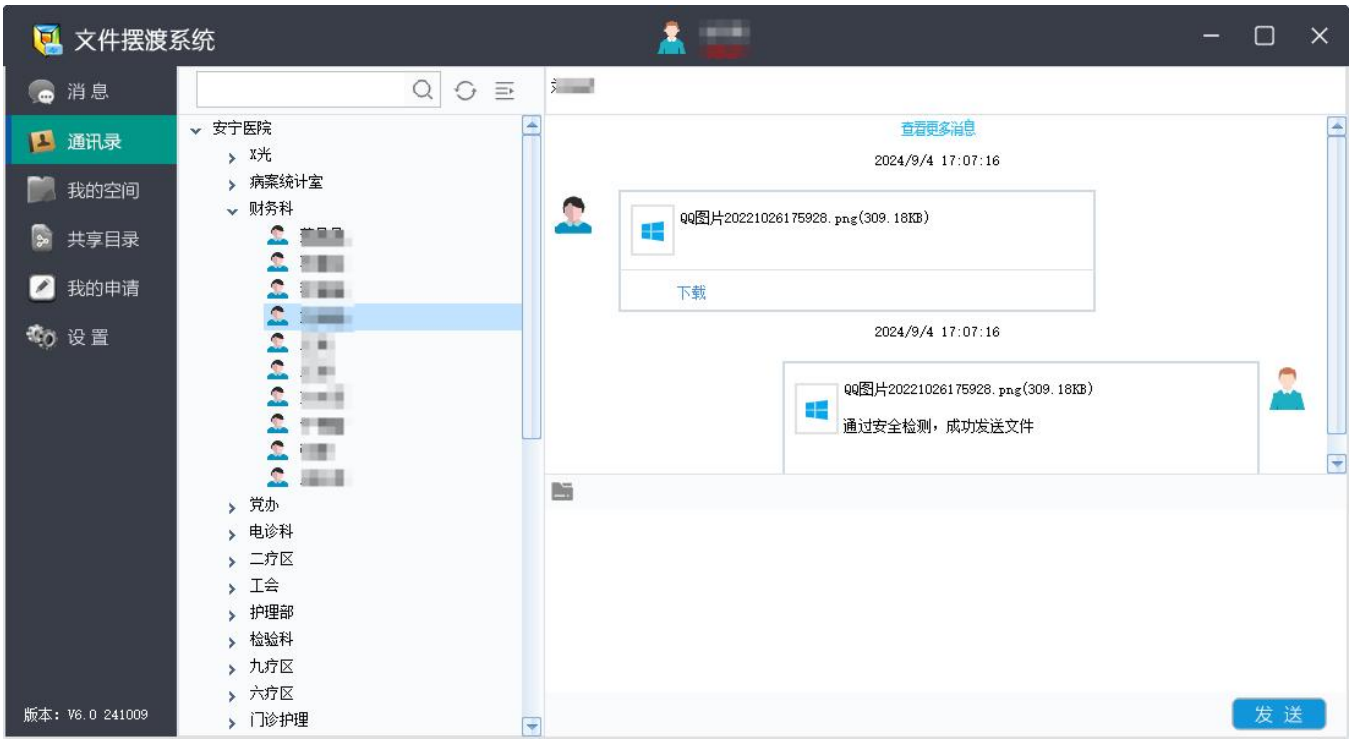


➢ Core Product Functions

1. Instantaneity： An instant messaging ferry software specifically designed is used to transfer files and information between networks (in conjunction with the file ferry device).
2. Content Security Inspection：The ferry device conducts strict security checks on data, including virus scanning, content filtering (sensitive words), file encryption, and approval of the file sending process.
3. Data Encryption:Files are encrypted before transmission, and only authorized recipients can decrypt and read the file content.
4. File Verification:Digital signature verification is performed on files to ensure that they have not been tampered with during transmission and to verify the identity of the sender.
5. Shared Directory:Supports departmental shared directories, facilitating file sharing and collaborative office work within the organization.
6. Log Record:Detailed log records are kept for all file and message transfer operations, including transfer time, sender, recipient, and file content.
7. Support for Large Files:Supports the transfer of large files between isolated networks.
8. Integrated Software and Hardware Design
(Supports Xinchuang Systems)

Product screenshot





Inventsoft | Fengyin

New Generation Network Security Active Defense System

➢ Product Overview

It constructs a highly sensitive and accurate network security reconnaissance network based on behavior, quickly and accurately detects internal network security threats (such as 0-day, APT attacks, hacker attacks, and extortion attacks), and stops security threats at the first step.

It has zero false alarms and a 100% early warning accuracy rate, providing high-quality network security data and solving the problem of unprocessed massive alarm data in current security operations.

It does not rely on security rules and can accurately and quickly detect various security threats of lateral movement attacks, including attacks from known and unknown threats.

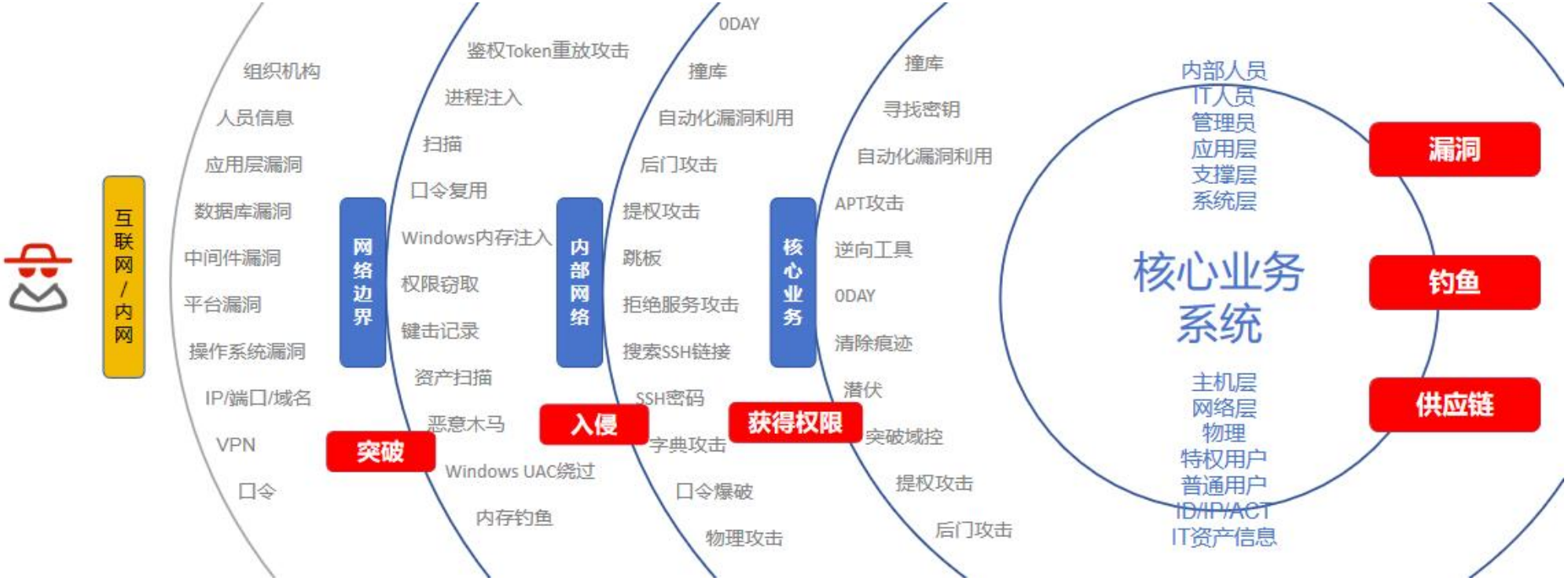
Based on high-quality and high-accuracy alarm data, it reduces the daily workload of security operation personnel, shortens the residence time of security threats in the internal network, and thus reduces network security risks.

The Inventsoft Fengyinl Active Defense System is an adaptive, active, and dynamic network security protection system based on behavior analysis methods. It is a beneficial supplement and enhancement to the existing network security system. It can help enterprises quickly establish automated, practical, and regular security protection capabilities against security threats without relying on personnel and skills, effectively responding to various network security threat attacks, HW, heavy protection, inspections, and other network security activities.

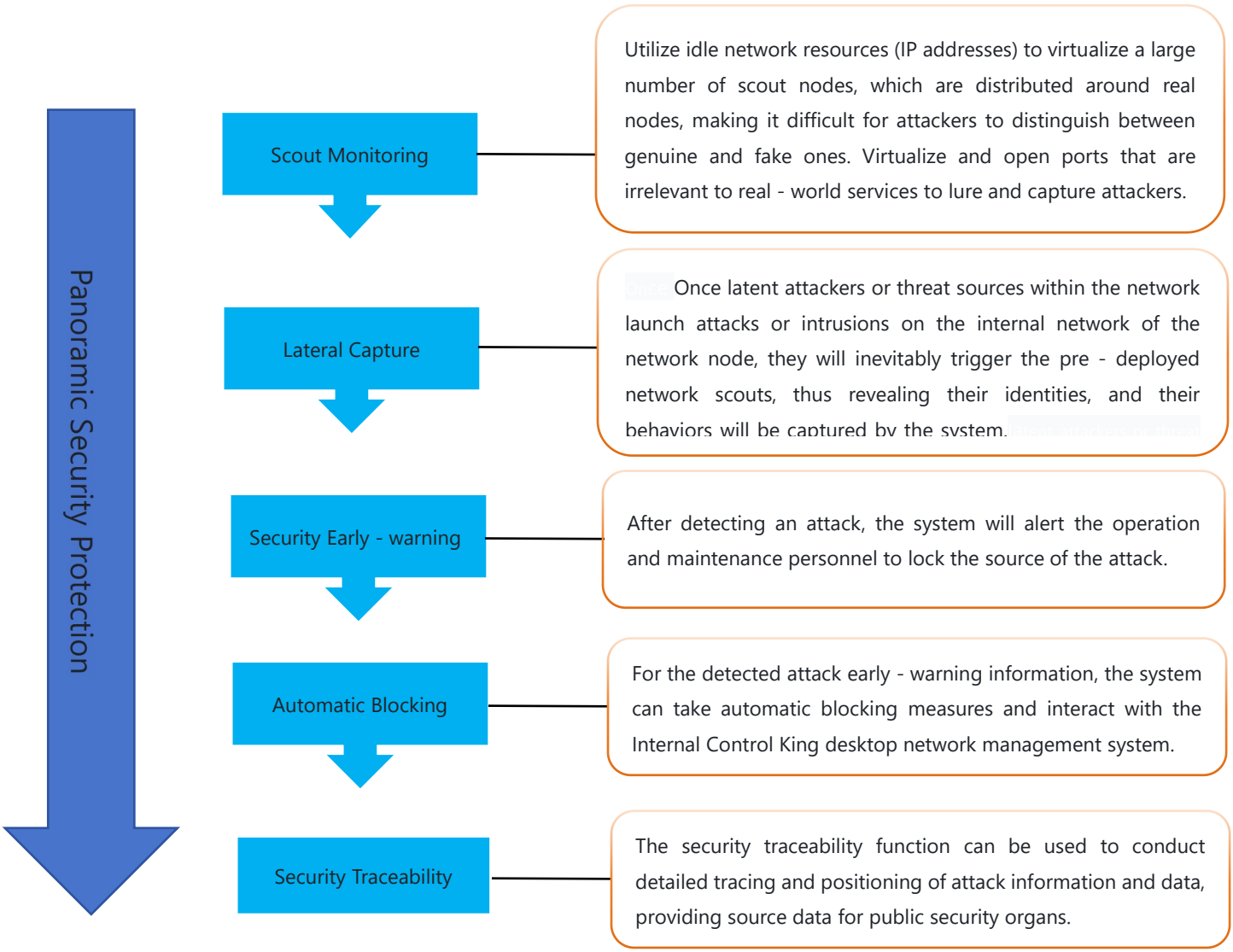
It can deploy network scouts (idle IP addresses of users) through mimic defense technology. The network scouts form a security monitoring and security trapping network. Combined with the actual internal network environment of the enterprise, high-interaction trapping and security simulation systems are deployed to build a network security reconnaissance system.

Once a network attack occurs, the system will issue a quick and accurate early warning and adopt automated isolation and blocking strategies, building an adaptive security protection system for the entire process of security threats for the enterprise and stopping security attack threats at the first step.

- Typical Attack Tactics Panorama

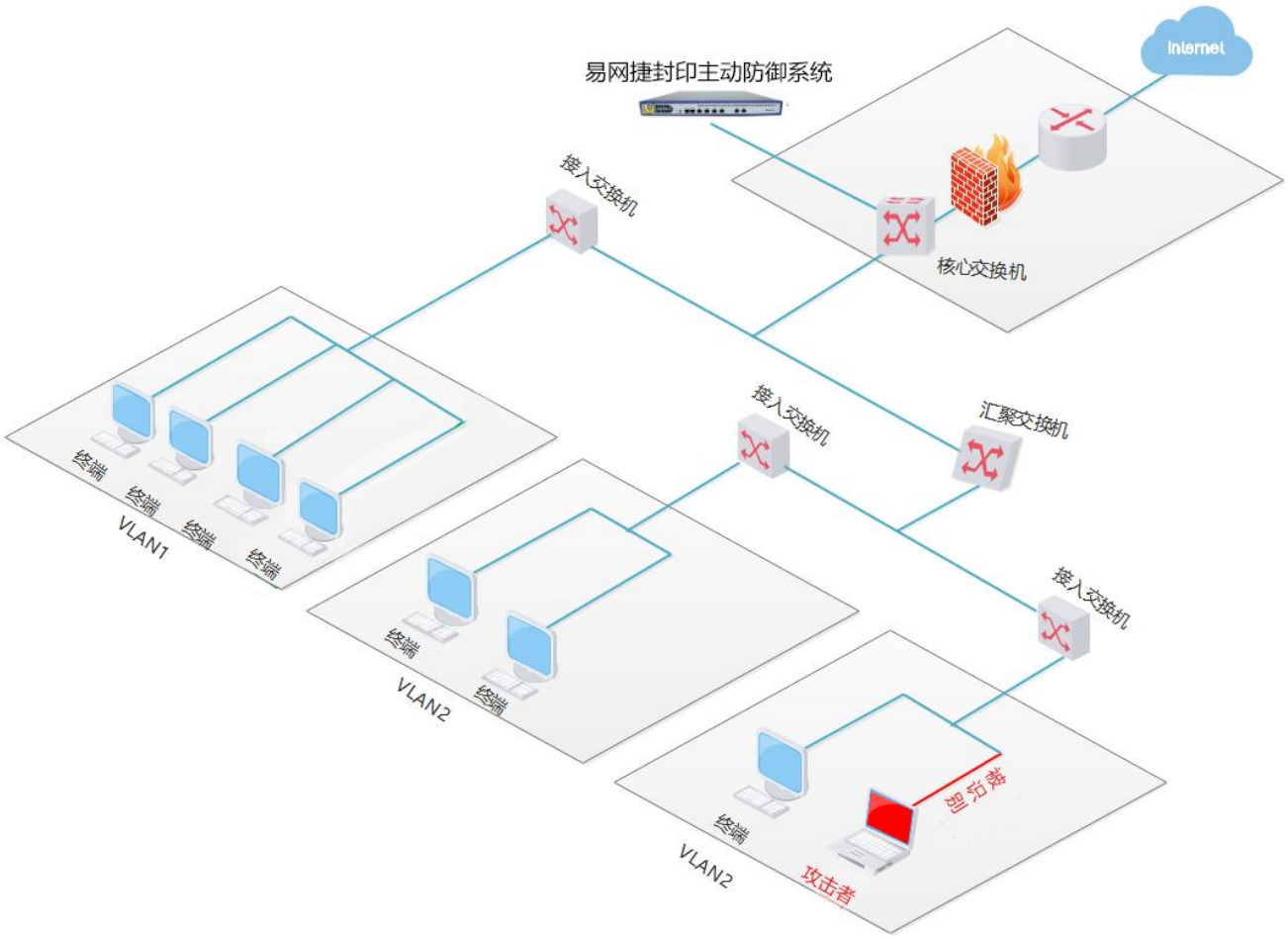


❖ Whole Process Security Protection



◆ Integrated Software and Hardware Design (Supports Xinchuang Systems)

■ Deployment Diagram



Terminal Desktop Management System

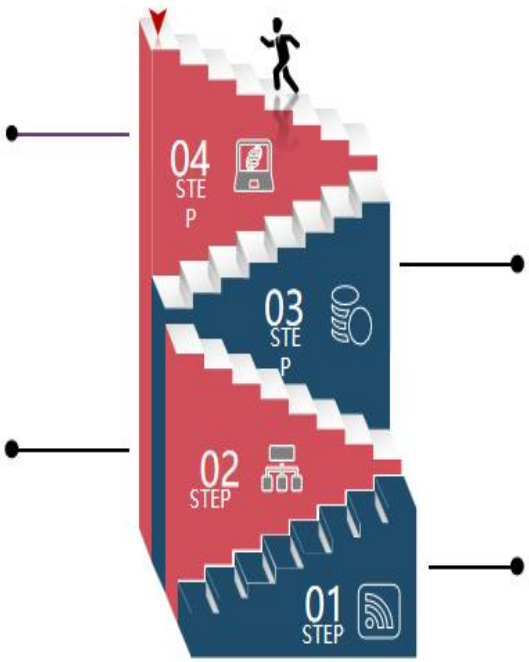
Product Overview

The Internal Control King Terminal Desktop Management System is an integrated security management and protection system that combines terminal security management, terminal behavior management, terminal operation and maintenance, and active defense. It covers network management, operation and maintenance management, and audit management. It records, tracks, and audits the computer usage behaviors within the organization, comprehensively standardizes employees' computer usage and Internet access behaviors, creates the most complete system security environment for users, avoids legal risks, reduces operation and maintenance costs, and improves work efficiency.

Product Features and Advantages

B/S Architecture: Fully compatible with all mainstream browsers: IE, Chrome, Firefox, 360, and others. Manageable from any terminal within the network, with simple, flexible, and convenient deployment and easy maintenance.

Multi-Level Cascading: Manages distributed branch networks.



High-Speed Cache Database: Supports 8,000 concurrent clients with low network demands.

Complex Network Support: Compatible with multi-VLAN and multi-subnet environments.

OS Compatibility: Windows XP/7/8/10, Linux, UOS, Kylin (32/64-bit).

➢ Core Functions

Five IT management principles, one system, four layers of protection, and 20 major applications comprehensively cover organizational management systems, formulate standardized strategies, and provide users with an overall solution for terminal desktop management.

Product screenshot

USB Removable Storage Medium Management System

● Product Overview

Through the authorized use and access control of USB storage media, it ensures that non-authorized USB storage media cannot be used when connected to internal network computers, and authorized dedicated USB storage media for the internal network cannot be used when connected to external network computers. At the same time, unauthorized users cannot decrypt USB drives, preventing document leakage. It is a data security management system that scientifically and reasonably controls the use scope, usage method, and data security storage of mobile storage media.

● Product Features and Advantages

✓ Wide Range of USB Control

1. USB devices include: USB flash drives, Bluetooth devices, WIFI devices, USB CD burners, mobile hard drives, mobile phones, digital cameras, camcorders, iPods, MP3/MP4 players, PDAs, and various CF/MD/SD/Flash Disk mobile storage devices.

2. USB storage media include: USB flash drives, mobile hard drives, mobile phones, digital cameras, camcorders, iPods, MP3/MP4 players, PDAs, and various CF/MD/SD/Flash Disk mobile storage devices.

3. USB communication peripherals include: Bluetooth devices, WIFI devices, and smartphones with Android and IOS systems.

✓ Low Cost

Existing ordinary USB mobile storage media can be converted into internal network - specific media.

✓ Flexible Authorization and Registration Methods

Including administrator authorization registration and user - side application for authorization.

✓ Secure Control and Compliant Use

Multi - layer authentication protection technology. It can automatically identify storage devices, non - storage devices, authorized devices, and non - authorized devices, as well as hardware information, etc., preventing non - compliant and unauthorized use of USB mobile storage media.

✓ **Detailed Device Records and Audits**

Fully records the attribute information and operation records of USB mobile storage devices, controlling potential threats.

❖ Core Functions

1. Internal Use for Internal - Disk, External Use for External - Disk

Ordinary USB storage media can be converted into "internal network - specific storage media" after authorization. Registered USB storage devices can only be used on internal computers with corresponding permissions. All external USB devices are prohibited from being used internally.

2. Fine - grained Control of Mobile Storage Device Usage Permissions

① Temporary Policy Application: When employees need to use a USB drive, they can apply on the client to temporarily enable the read/write permission of the USB drive. Managers review and set the usage permissions and time. Only after authorization can employees obtain the device usage permission.

② Managers can also directly set security policies to quickly complete the security control of USB storage media.

③ Unauthorized USB devices and USB devices that have exceeded the usage period cannot be used in the internal network.

3. Powerful USB Storage Medium Usage Audit

Accurately identifies all mobile storage devices connected to the network, monitors the usage behavior of USB drives in real - time, and detailedly records the plug - in and unplug - in records of USB media on terminal computers, file copy records, and authorization records, etc., forming audit logs for traceability.

4. Intelligent Identification and Differential Treatment of Different USB Devices

Automatically identifies storage devices and hardware information. Non - storage USB devices (including USB mice, USB keyboards, USB printers, etc.) do not affect normal use.

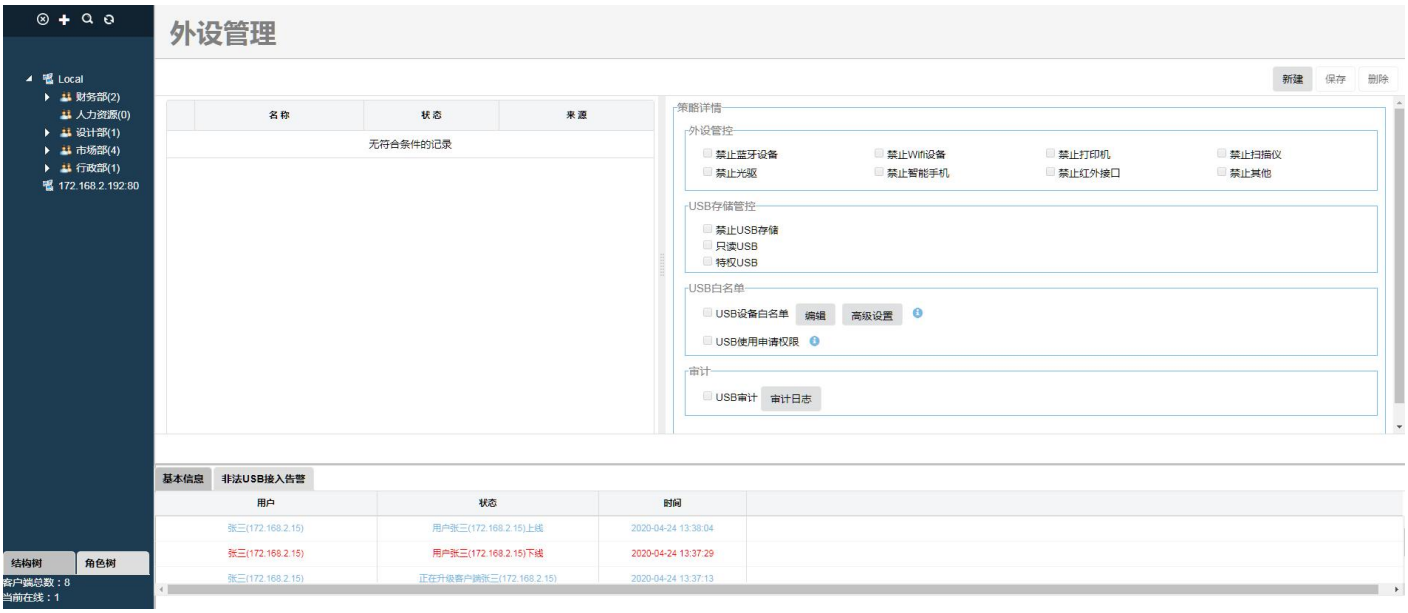
5. Complete Security Mechanism

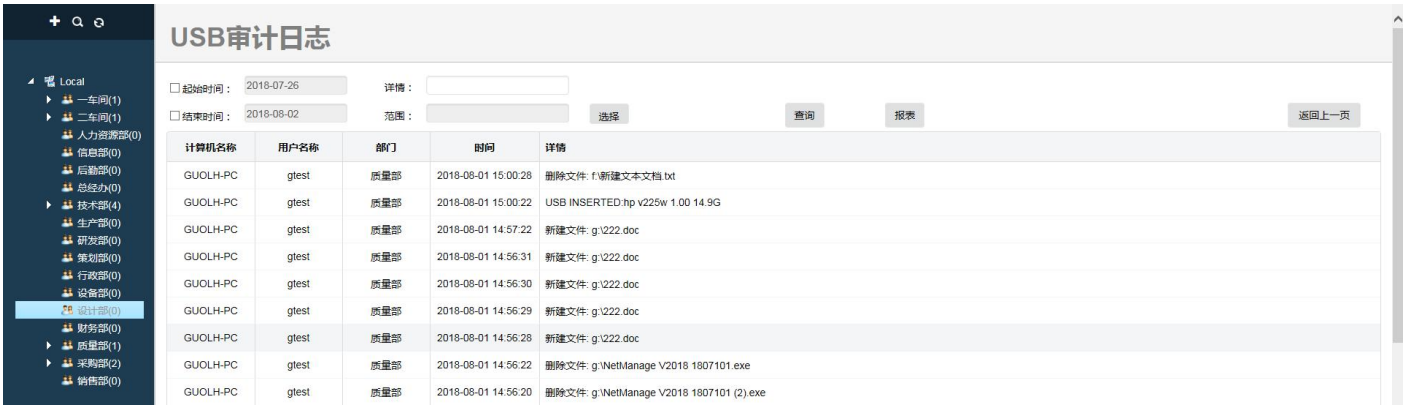
One - way copy function can be set for computers within the organization that contain important information. Whether it is an external USB drive or an authorized USB drive, only single - way copying in is allowed, which is convenient for external visitors and also prevents information leakage, enabling flexible combined control.

6. Off - line Policy to Effectively Limit the Spread of Confidential Information

Computers that are disconnected from the internal network are still subject to the USB mobile storage media control policy.

Product screenshot





Terminal Server Access Control System

- Product Overview

- It closely complies with relevant regulations proposed by national authoritative institutions, such as the "Information Security Classification Protection GB/T 22239 - 2008 Standard" and the "ISO27001 Information Security Management System", and realizes unified standardized management of people, terminals, IPs, and devices in the internal network.
- It effectively solves a series of thorny problems commonly existing in user units, such as inability to ensure network boundary integrity, boundary security, centralized management and control, real - name system for internal network terminals, precise positioning of dangerous devices, and network problem positioning.
- It also solves the problem of ensuring network boundary integrity while being compatible with old devices and systems. Users can smoothly achieve network real - name access control and network security status analysis without updating network devices, changing the network structure, or installing clients.

- Product Features and Advantages

Monitoring mode：
Side - by - side deployment without changing the user's network structure, minimizing the impact of the device on the network.

No - client design：
Realizes client - less access control, eliminating the cumbersome process of installing clients and providing a high - quality user experience. (Supports the management and control of various types of devices, including mobile phones, pads, cameras, smart TVs, and other intelligent terminals)

Hardware fingerprint technology：
The system automatically scans, collects, and binds device IP addresses, MAC addresses, access locations, and operating system identification information, generating a unique identifier for each device.

Visual and precise positioning：
Visual network topology for quick identification of loop ports.

High compatibility：
Good compatibility, and can be deployed in network environments with old and non - manageable network devices.

High stability：
Runs in the network 24/7 without the need to install monitoring agents in each subnet.

- Core Functions

✓ **Management and Control of Unauthorized Network - connected Devices**

Can immediately detect, locate, and alarm when wireless APs, switches, intelligent terminals, or wireless routers are connected to the network.

✓ **Full - network Terminal Authentication Access**

Realizes mandatory identity authentication for internal network terminals in a client - less form without changing the existing network architecture.

✓ **Access Blocking**

Uses protocols such as SNMP, ARP, and ICMP. By monitoring illegal network - connected devices and comparing with authentication information, it distinguishes illegal devices. Once an illegal device is discovered, it sends an alarm message according to the alarm settings and blocks the illegal access to ensure network security.

✓ **Temporary Access with Flexible Settings**

Fixed legal devices in the internal network are added to the access list. External visitors or temporary workers can access from any port regardless of their physical location, but their access rights are strictly controlled. Access time can be set, and once the time expires, the access will be immediately blocked to prevent illegal devices from taking advantage.

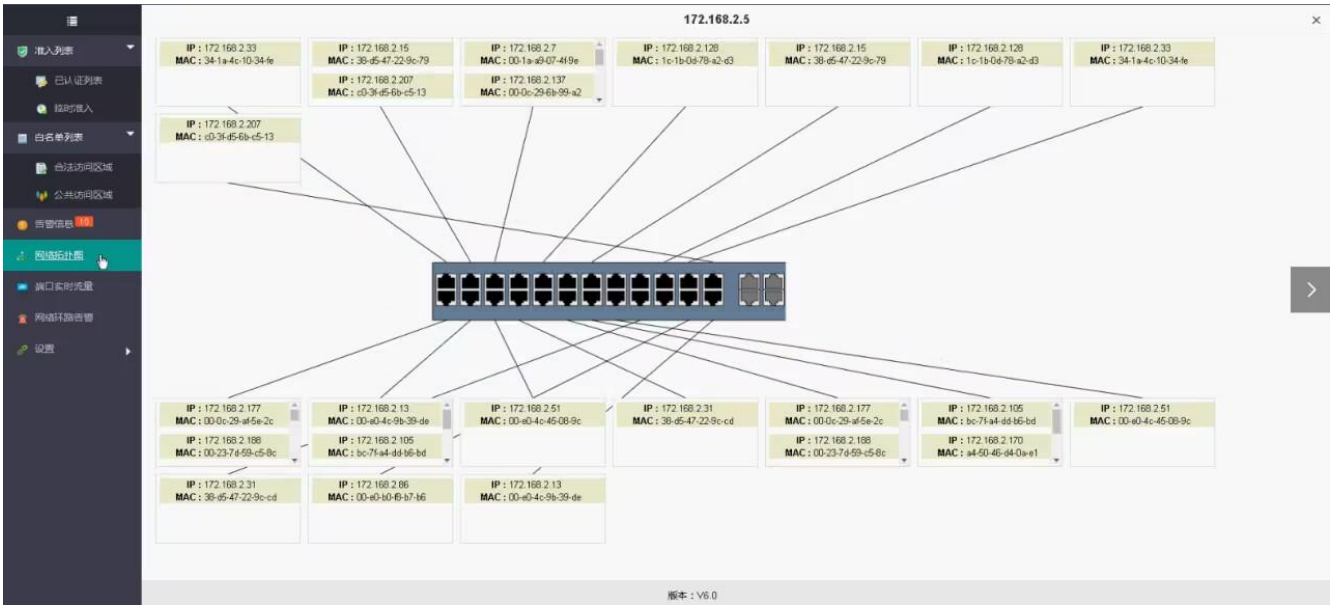
✓ **Uncertified List for a Clear View of Illegal Access Devices**

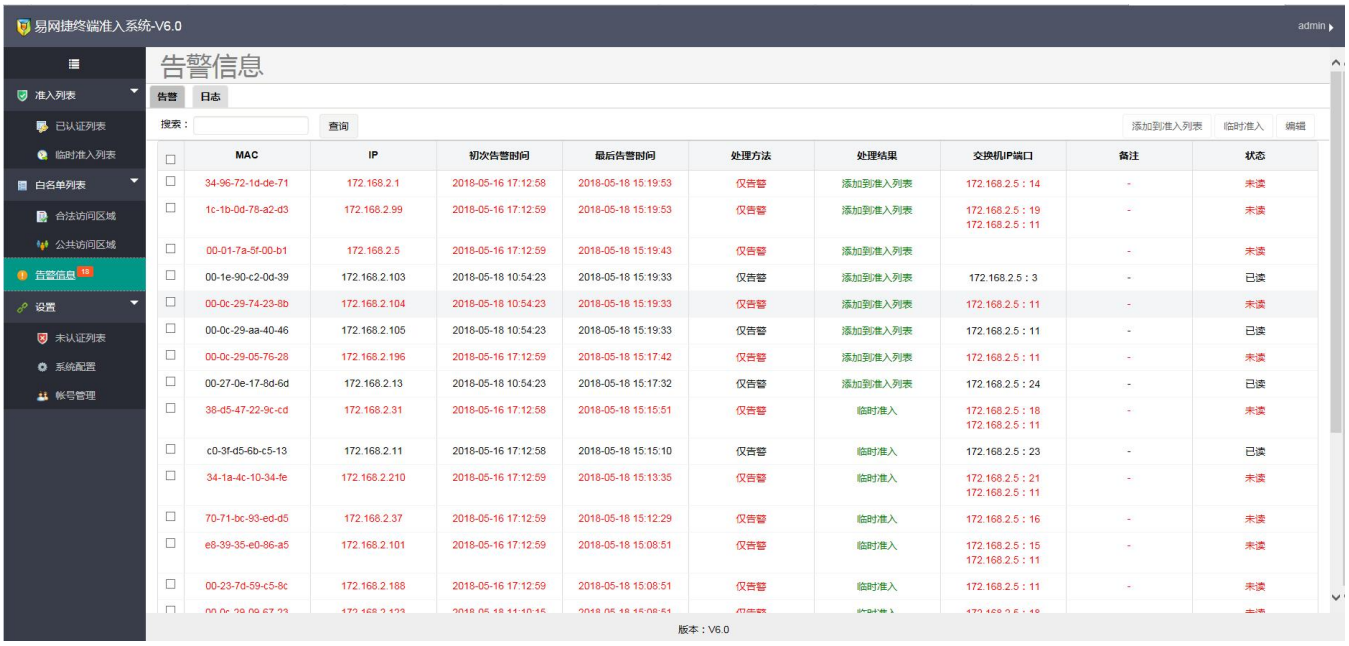
The uncertified list collects all unauthenticated terminal devices in the internal network. Legitimate unauthenticated terminal devices can be added to the certified list to complete the initialization of legal devices.

✓ **IP/MAC Address Management**

Monitors the usage status of all fixed and dynamically assigned IP addresses in real - time, preventing unauthorized IP address changes. Automatically collects network information such as IP - MAC addresses within the network.

■ Product screenshot





File Encryption System

Product Overview

The Internal Control King File Encryption System is an electronic document data information protection system. It provides real - time and comprehensive encryption protection for various formats of electronic files through high - strength encryption algorithms, ensuring that all confidential data within the organization is always in an encrypted state. Regardless of how files are stored or transferred, there is no need to worry about the leakage of important information. Through three main functions, namely internal rights management, file external distribution management, and offline authorization management, it achieves meticulous and comprehensive protection and control of important information within the organization, providing a secure and convenient data security solution.

Product Features and Advantages

1. Provides three different encryption modes: active encryption, mandatory encryption, and intelligent encryption, allowing users to choose flexibly according to actual needs.

2. Adopts various file external distribution and communication schemes, such as dividing security zones and setting file permissions, ensuring information security without hindering business operations, and achieving a perfect balance of security, cost, and efficiency.

3. Users are unaware during the use process, which does not affect employees' daily work habits. There is no need to train employees on operations, simplifying the work of system administrators. As long as they are in the encrypted environment within the company, files can be automatically decrypted without entering passwords, facilitating internal information communication.

4. Based on the Windows operating system kernel - level encryption technology, it supports super - large - scale data applications with low performance loss. No temporary plain - text files are generated during the encryption process.

5. Disaster recovery mechanism to calmly deal with unexpected situations.

◆ Core Functions

✓ Automatic Intelligent Encryption of Important Documents

Can automatically identify files according to their types, determine whether they are encrypted data types defined within the organization, and automatically encrypt the files.

✓ Lifecycle Management of Encrypted File External Distribution

For files that need to be distributed externally from within the organization to legitimate readers, the Internal Control King encryption system can strictly control the usage rights of externally distributed files, including the expiration time of opening, the number of opening times, and whether copying, editing, printing, and screen - capturing are allowed. When the number of opening times or the opening time of the externally distributed file reaches the limit, the file can no longer be used.

✓ Internal Rights Management to Effectively Reduce the Risk of Internal Information Leakage

① File Rights: User rights can be flexibly associated with sensitive document information of different security levels. Personnel with different rights can view corresponding confidential documents.

② Inter - departmental Rights: Different departments can be divided into different security zones, and encrypted files cannot be viewed across departments. Different departments can also be divided into the same security zone, allowing encrypted files to be viewed mutually.

✓ Workflow Approval Management: An Effective Combination of Systems and Technology

When employees need to perform operations such as file decryption and external distribution, they need to upload the application file for workflow approval. Only after the approval of superiors can they continue with the operation, effectively preventing file leakage.

✓ Offline Authorization Management to Prevent Arbitrary Document Diffusion

Can perform offline authorization for laptops used by employees on business trips or those working from home temporarily. Encrypted files can be logged in and used with a security password within the specified period.

✓ Email External Distribution Control

When sending files via E - mail, the specified trusted recipients need to be added to the email whitelist before allowing external distribution to the whitelisted addresses.

✓ Audit and Supervision of Rights

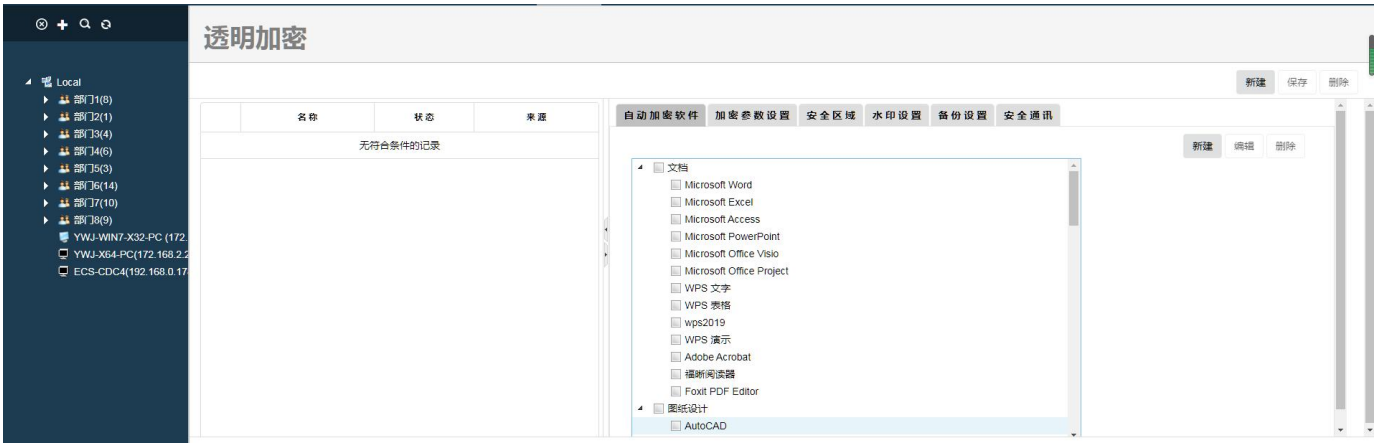
Can audit and track the settings of the software by the admin administrator. Multiple

levels of supervision ensure that the system operates in a secure and stable environment.

✓ Disaster Prevention and Backup Mechanism

Can perform regular or real - time backups of modified encrypted documents. Edited and newly created files will be automatically backed up to the server, ensuring that the original encrypted files are intact and available even in case of unexpected situations.

■ Product screenshot



Open Network Marginal Security Management System

● Product Overview

The Internal Control King Open Network Marginal Security Management System is designed for open networks (such as service halls and video networks). It builds a security barrier within the internal network, effectively solving a series of thorny problems, including network boundary integrity, boundary security, management of terminal cameras in public places, management of intelligent devices (such as all - in - one machines) in service halls, precise positioning and blocking of dangerous devices in open areas. The system can achieve multiple security functions, such as automatic discovery of all network devices, automatic identification of connected devices, comprehensive monitoring of the transmission process, automatic analysis of network access behaviors, automatic positioning and blocking of illegal devices, quick identification of network loops, and auditing of network - wide information events. From the outside to the inside, it forms a three - dimensional in - depth security defense system. The network marginal security management method is simple, with good expandability and compatibility. It supports multi - VLAN and dynamic DHCP network environments and can achieve large - scale network management with a small number of administrators. It is a low - cost, easy - to - implement, easy - to - manage, and highly reliable security solution that comprehensively addresses the security issues of open network margins.

✧ Product Features and Advantages

1. Access terminals in open areas can achieve access control functions without installing any clients or browser plugins.

2. Simple deployment and implementation, without the need to configure switches.

3. The "Network Marginal Security Control System" uses the monitoring mode to immediately block illegal access terminals without waiting.

4. Good compatibility, supporting common switches

5. Fixed IP address or DHCP dynamic acquisition of IP address management mode are applicable.
6. Support multi-VLAN deployment, and the "network marginal security control system" is deployed in the core switch TRUNK port.
7. 7 * 24 hours guarantee to run in the network, without the need to install monitoring agents on each subnet.

8. Integrated design of software and hardware (support Xinchuang system)

Kirin server operating system
domestic CPU
TiDB domestic database

◆ core function

First, accurately locate illegal devices
maliciously access smart devices to the intranet through the network port exposed in the public area of the unit, which is illegal for the unit to invade the internal network, resulting in illegal outreach. The internal control Wang Open Network Marginal Security Management System can instantly and accurately locate illegal intrusion devices. Illegal device information includes IP and MAC addresses.

Second, the illegal intrusion device is found to alarm and block

The SNMP, ARP, ICMP and other protocols adopted by the Internal Control King Open Network Marginal Security Management System, monitor network illegal access devices, compare authentication, and distinguish illegal devices. Once illegal devices are found, they send alarm information according to alarm settings and block illegal access to ensure cyber security.

Third, improve the alarm mechanism

When the illegal device is connected to the intranet, the end point access alarm client side will immediately pop up the alarm information, through the end point access alarm client side can check the alarm information in time, WEB control end has detailed alarm records, and can be safe equipment timely added to the access list or temporary access list.

■ Product screenshot