UPAS

ZERO TRUST ARCHITECTURE

COMPREHENSIVE ZERO TRUST CYBER SECURITY SOLUTIONS

ZERO TRUST · TRUST UPAS

— Product Catalog —

- APAC CIO Outlook -

TOP 5 / TOP 10
Cyber Security Solutions Provider
in Taiwan / APAC


ZERO TRUST
TRUST UPAS



UPAS

A Leading Brand of Intranet Security Control System

UPAS was founded in 1993 as a pioneer and leader in internal network security and control systems. Starting with the development of IP management and NAC (Network Access Control) system products, it has been deeply involved in the fields of cyber security and network management for many years, assisting customers in establishing comprehensive internal network security and control systems, improving internal network security and management efficiency, reducing management costs, and strengthening cyber resilience.

Professional and Dedicated Service for You

UPAS is committed to providing customers with best intranet security solutions; it is our mission to help customers in building solid boundary protection, ensuring security and compliance of terminal devices of intranet, and preventing ransomware intrusion and confidential data leakage. The team has accumulated fruitful achievements with government bodies, key infrastructure, science and technology industry, manufacturing industry, finance industry, medical care institutions, education research institutes and enterprises. We will keep learning to customers, optimizing products to respond to customer demands, and moving forward together with customers on the path of information security.

Leading the Way with Technology and Stepping onto the International Stage

UPAS has service bases in Taiwan, Mainland China, Japan and Southeast Asia; whether your are a large multinational, overseas brand or international brand, UPAS, by virtue of professional technologies, can provide you perfect solutions, zero trust security architecture and solid intranet security protection as per your requirements.

Your Intranet Environment May Be Exposed to the Following Risks



- Incomplete inventory of devices in the intranet environment provides opportunities for hackers.
- Illegal devices are unauthorized access, creating potential crisis.
- The number of IoT devices has increased dramatically and failed to use Agent management.



- Windows Patch hasn't been updated and vulnerabilities will appear on devices.
- Virus signature has not been updated, and the new virus will invade recklessly.
- Software vulnerabilities in endpoint devices cannot be repaired in a timely manner by administrators.
- GPO is incompliant.



- Important files have been leaked.
- Employees' personal devices enter the intranet to access data without permission.
- Employees use personal USB to access important information.



- Employees privately connect to hubs or share IP routers, affecting the company's internal network.
- External visitors use the internal network without verification.
- Terminal devices withdrawal a domain without permission.



- Personnel using mobile devices to take photos or screenshots to leak confidential information.
- Installing illegal applications on mobile devices without authorization.

Multiple Risk Defenses. Diverse Device Management. No Need for Multiple Software.

UPAS ZTA gives you the most solid intranet security solution.

UPAS 5S Key Advantages

ZERO TRUST ARCHITECTURE

Simple

- It adopts the NAP patented technology, has the simple deployment architecture, and is easy to install and set
- It has the function of flexible deployment, and is suitable for cloud and ground setting
- It has the modular architecture, can be applied freely and flexibly, and also boasts high CP values
- It is highly compatible with and supports various brands of switches, antivirus software and network architecture
- It enjoys exquisite UI design, user-friendly UX design, and realizes system installation and setting in one page, reducing page swapping, and is easier to use

Support

- The ZTA system has the sole platform and sole Agent, and accommodates NAC, ITAM, IAM, IPAM, MDM, etc.
- The Agent supports the management of operating systems of Windows, Linux, macOS, Android, iOS, etc.
- It supports Patch updating, antivirus software installation, application installation, and blocked software and USB management, software vulnerability update, GPO patching, etc., and realizes total automation
- It provides integral functions, and supports syslog, API, etc.
- It supports clear data chart analysis on the NOC homepage and highly visual device information
- It provides diverse and rich report functions and can automatically generate various kinds of reports

Smart

- The perfectness, maintenance rate, attribute identification, Agent deployment rate, terminal device compliance inspection rate, etc., are all up to over 98%, ensuring the system security
- The smart and automatic design, including automatic allowlist, automatic grouping, automatic Agent dispatching, automatic policy compliance inspection by group, automatic isolation patching, automatic connection recovery, etc., economizing on manpower and time saving

Safe

- It has high security mechanisms, such as fault ByPass, error-proof design, etc.

Stable

- It is well received and trusted by the excellent high stability efficiency

5 Cyber Security Solutions

20 Function Modules

All-round zero trust architecture never trust and keep verifying

NAC
Network Access Control

Main Module

ARP ARP Scanner Access Control
IP/MAC Management Module

DAM Device Authentication Management



ITAM
IT Asset Management



- **PM** Patch Management
- **DM** Device Management
- **ROM** Remote Operations Management
- **TIM** Trust Inference Management
- **GPO** GPO Management
- **VANS** Vulnerability Alert and Notification System



IAM
Identity and Access Management

- **AD** ADVantage

ZERO TRUST ARCHITECTURE

A professional management tool tailored for IT and MIS workers

IPAM
IP Address Management

ARP

Main Module

ARP Scanner IP Management

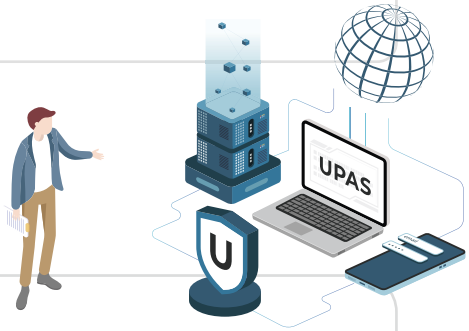
IP/MAC Management Module

MDM
Mobile Device Management

MDM

Mobile Device Management

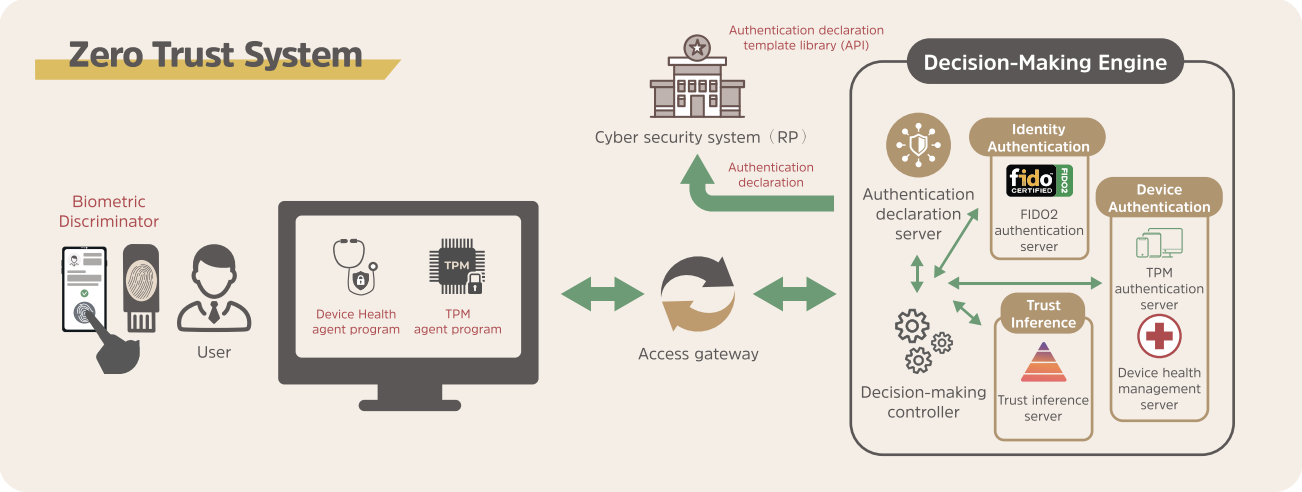
Other Value-Added Management Solutions



- **SIM** Security Integration Management
- **IPL** IP Locator
- **IPv6** IPv6 Management
- **IPAF** IP Application Form Functionality
- **DHCP** DHCP Server Integration Functionality
- **IPLI** IP Usage Log Integration Functionality
- **IDC** ID Checker
- **GAM** Guest Access Management
- **SCP** SCP Console
- **APP** UPAS Management App

UPAS ZTA All-Round Zero Trust Architecture

In 2020, National Institute of Standards and Technology (NIST) published NIST SP 800-207; as the zero-trust principles listed in NIST SP 800-207: “Enterprise should collect current information about assets, basic network architecture and communication as much as possible, and use such information to enhance the security status.” UPAS can help in asset and health inspection of intranet-access devices firstly, and then device authentication to prevent the possibility of intranet intrusion of counterfeit devices.



Phase I

Identity Authentication

FIDO password-less double-factor identity authentication.

Phase II

Device Authentication

Device authentication based on the device trust platform module (TPM), and device health management.

Phase III

Trust Inference

Dynamic decision on resource access results based on user scenarios and device health status.

Introduction of UPAS ZTA Modules

Built under the zero-trust architecture, UPAS’ five solutions are composed of 1 main module and 20 modules with different functions. You can freely select function modules to match the main module to create your exclusive best solutions.

UPAS independently developed technologies have been granted with domestic and overseas patents, can effectively block intranet access of illegal devices, and monitors intranet security from time to time. It has various alert mechanisms, user-friendly operation interfaces and various reports, and can help you effectively accomplish endpoint security protection and intranet security control.



Sole platform • Sole Agent

Free combinations of function modules

ARP ARP Scanner

Access control

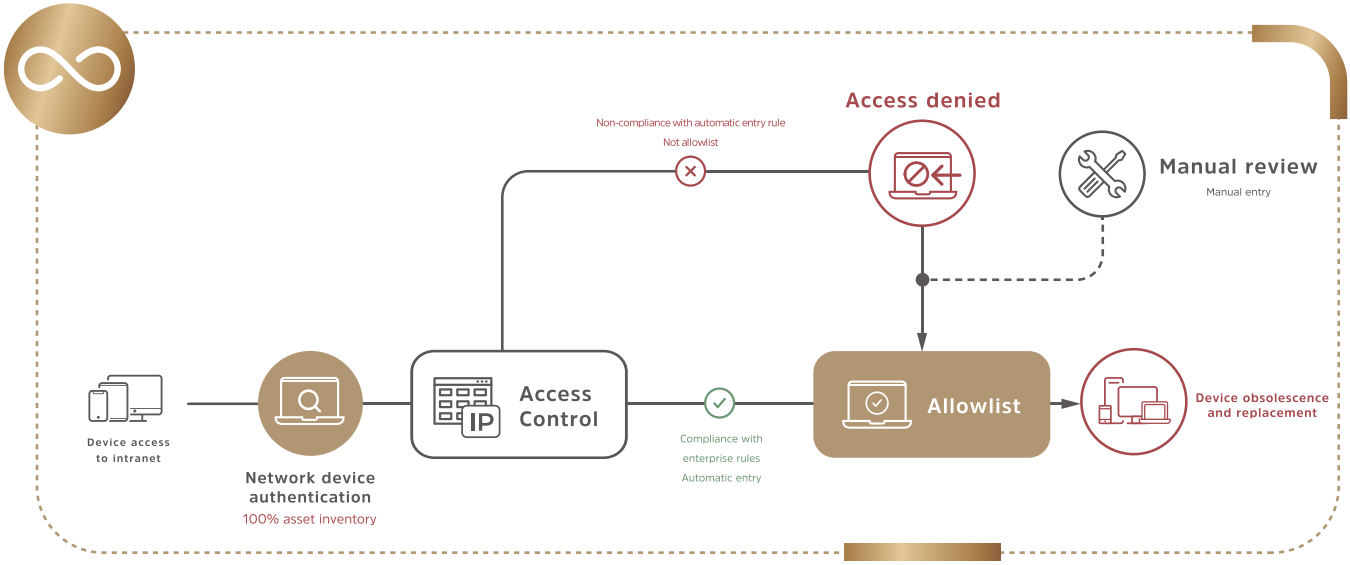
By virtue of the ARP patented packaging and resolution technology, it can realize data collection, device authentication and intensified access control without Agent installation. It can do 100% asset inventory to realize IP/MAC management, device access management (network access control) and network blocking.

An administrator can make access rules as demanded, and then the UPAS system can automatically establish a device allowlist; it only allows devices complying with security policies to have access to the intranet, and prohibits unauthorized external devices, and provides alert mechanisms of page redirection, Agent UI, MSG, etc., to ensure the intranet security fundamentally.

DAM Device Authentication Management

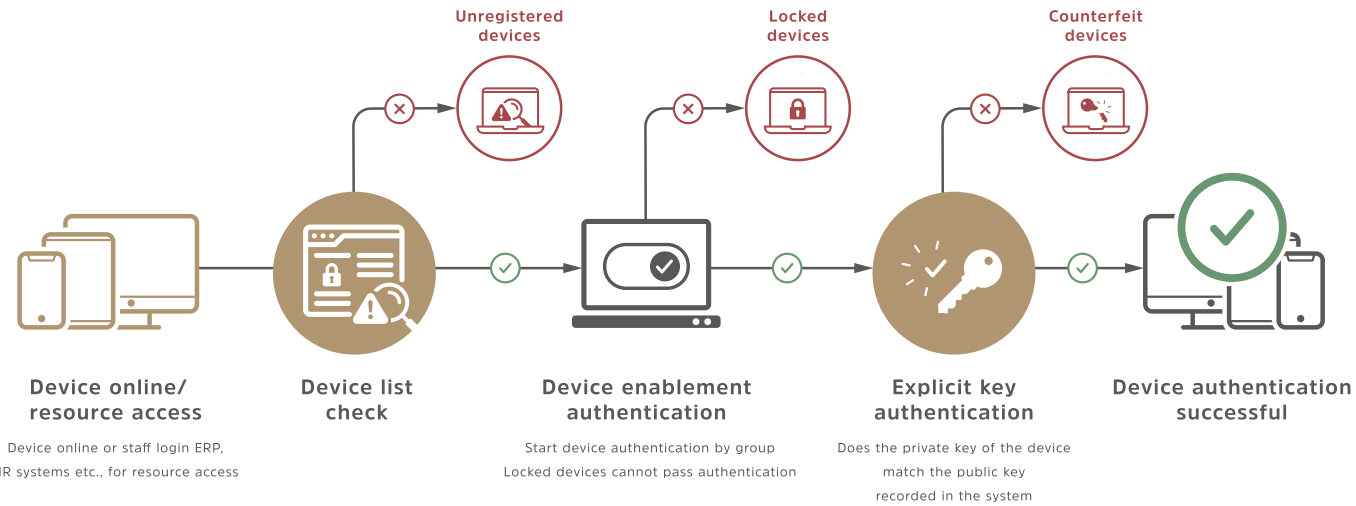
The module of DAM (device authentication management), through the Agent deployed at terminal devices, can inspect the hardware or software protection levels of the devices. It can verify whether the accessed devices are trusty when they go online, but also can be applied in resource access scenarios. Comprehensive security protection measures are available through integrating with identity authentication vendors.

The module provides device management functions, such as addition, locking and deletion, and has the functions of enquiring about device health information, panel statistics data and authentication histories, and notifies the administrator of authentication failure in the manner of event.



▲ Operation Process of ARP Scanner (access control)

▼ Operation Process of Device Authentication Module



PM Patch Management

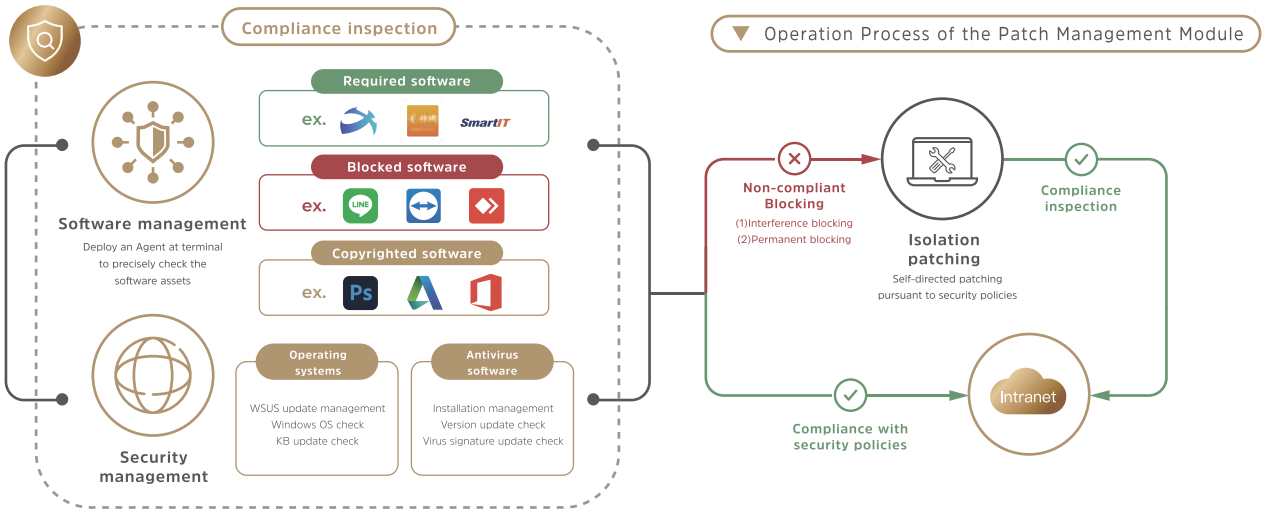
Through the Agent deployed in terminal devices, it can scan periodically and capture the software list of a intranet-access device, its Windows operating system version No./KB, and its antivirus software information and virus signature versions; based on the collected software list, it can also check: the quantity of required software, blocked software and copyrighted software, software versions, and feedback to WSUS Server, etc.

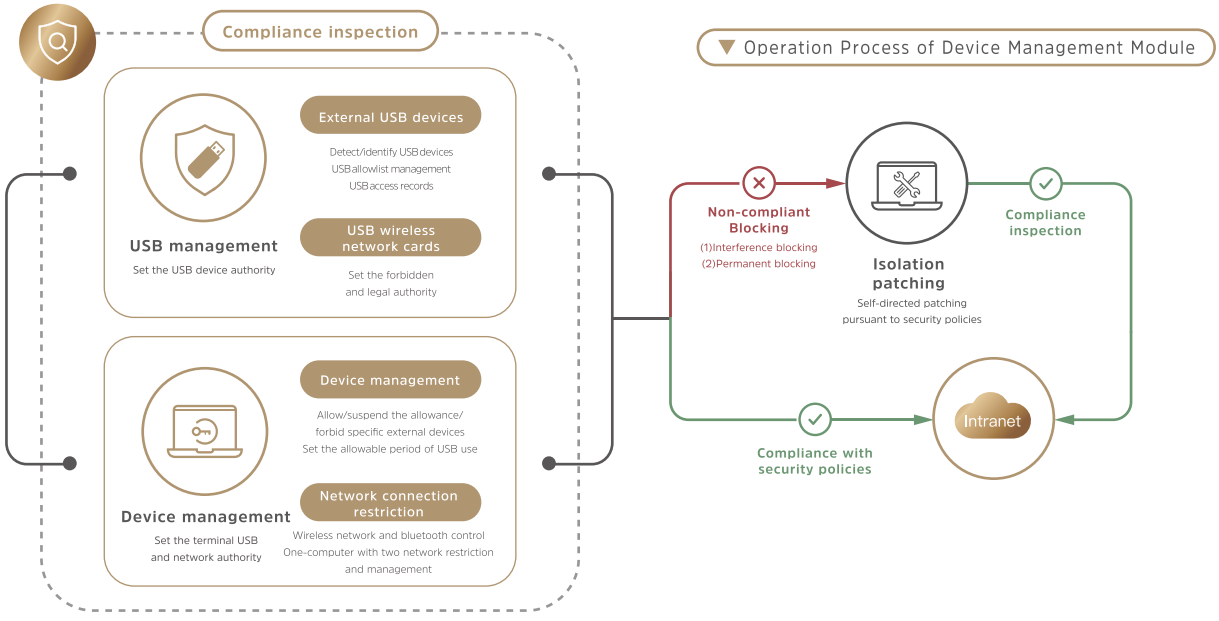
In case of non-compliance (required software is not installed, block software is installed, pirated software is used, software which should have been updated is not updated, no feedback to WSUS, etc.), it can disconnect the network and keep the reason for restriction informed on the redirection page, and set authority at different degrees to facilitate stable operation of devices and direct patching to comply with security policies. Besides, it can be connected with the ROM module which enables the administrator to assist devices in automatic software patching.

DM Device Management

Through the Agent deployed in terminal devices, it can identify and control external USB devices, such as USB storage devices, memory cards, action devices, USB network cards, optical drives, etc., and set the authority of computers for accessed devices, such as the authority of device access and revision, etc., to avoid confidential data leakage. It can also establish a USB storage device whitelist to prevent unauthorized unknown USB storage devices from data transmission and access.

Besides, it can detect and forbid the connection of devices to wireless network or bluetooth, to prevent confidential data transmission via personal network through bypassing the corporate network.





ROM Remote Operations Management

Through the Agent deployed in terminal devices, it collects various software and hardware models and specifications of devices, and performs remote operations management.

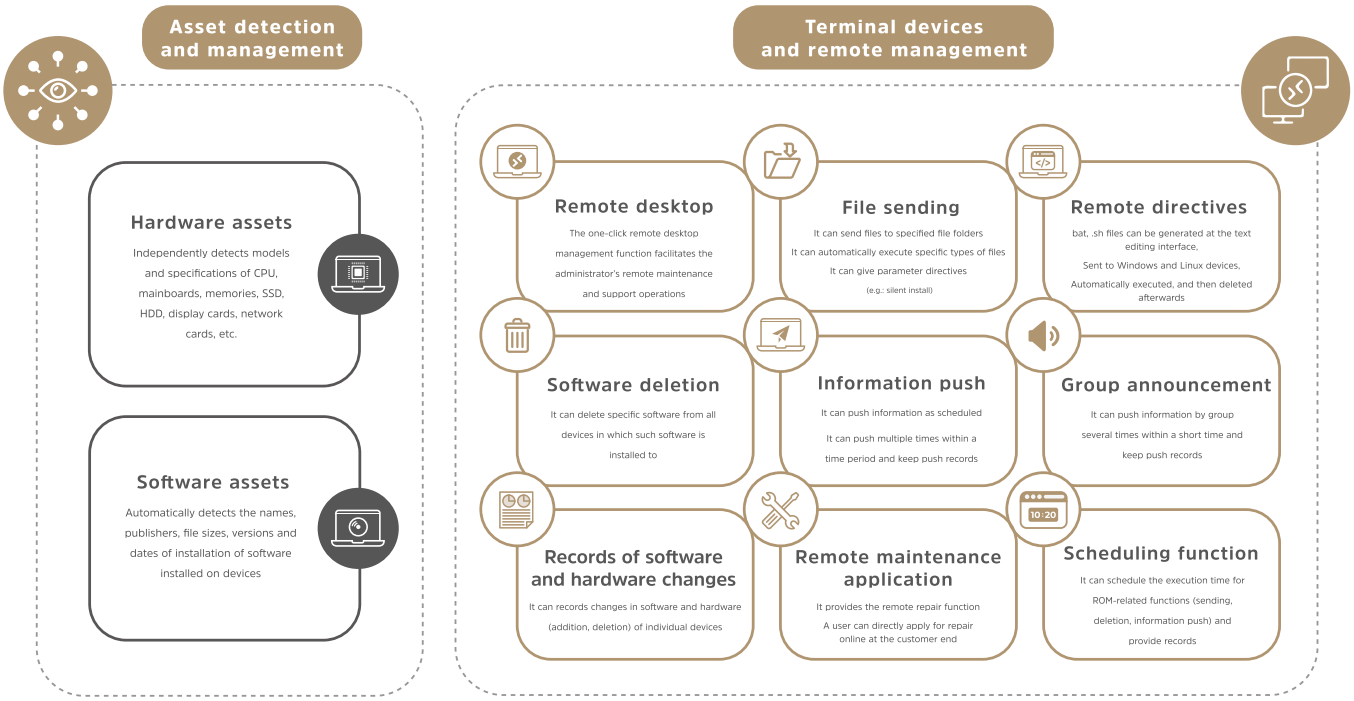
It has the functions of remote desktop management, file sending, and software deletion. It can realize silent install of files with the parameter directives. It can also provide functions of information push and group broadcasting to facilitate the administrator's management and maintenance of terminal devices. A user can also send a remote desktop request to the administrator, explains the problems through Agent UI, and asks the administrator to handle the problems in a timely manner.

TIM Trust Inference Management

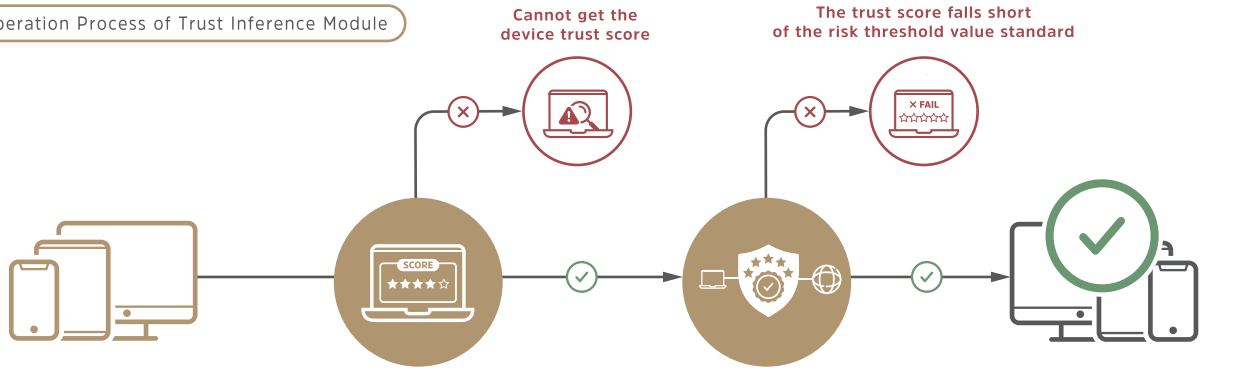
The TIM module checks device information (including OS, antivirus, software installed, and latent risk vulnerabilities) as reference for device security evaluation.

The security data collected, with identity authentication and device authentication, can be regarded as the evaluation standards of trust scores for resource access, and the decision-making controller determines the access results. The module includes functions of device security detection, trust score information, panel statistics data and historical records.

▼ Explanations on Functions of the Remote Operations Module



▼ Operation Process of Trust Inference Module



Device online/ resource access

Device online or staff login ERP, HR systems, etc., for resource access

Get the device trust score

Get the current device trust score by suing the trust inference algorithm

Reach the risk threshold value standard

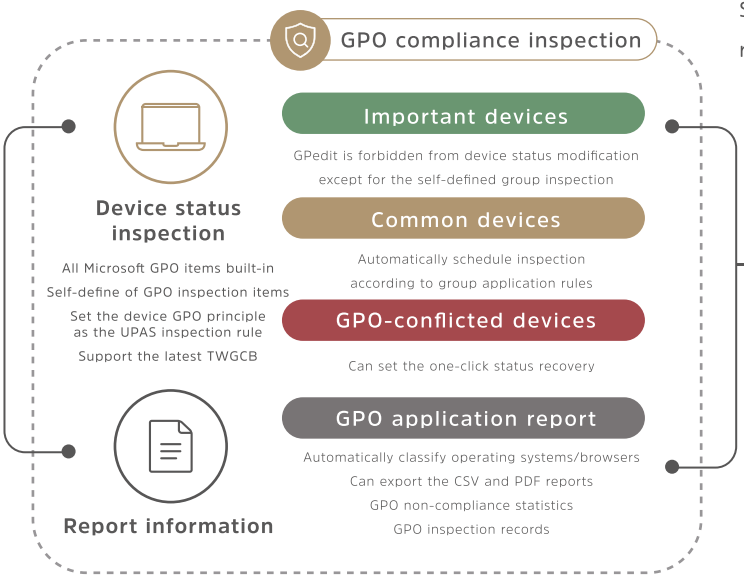
Compare the trust score with the risk threshold value; when the trust score doesn't meet the standard, the device cannot proceed with resource access

Complete the device trust inference process

GPO GPO Management

The GPO management module support the latest TWGCB, and can detect the device GPO application within the domain without having the highest WMI domain authority in the context of highly-complete asset inventory, and execute automatic or manual patching for GPO non-compliant devices, and automatically reports the application results and provides patching records.

It has the function of one-click status recovery, and can recover devices to the status before GPO application to avoid that devices cannot work well after GPO application.

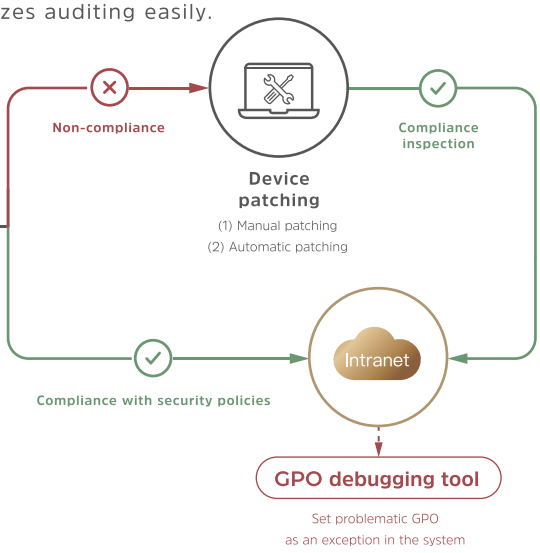


▲ Operation Process of GPO Management Module

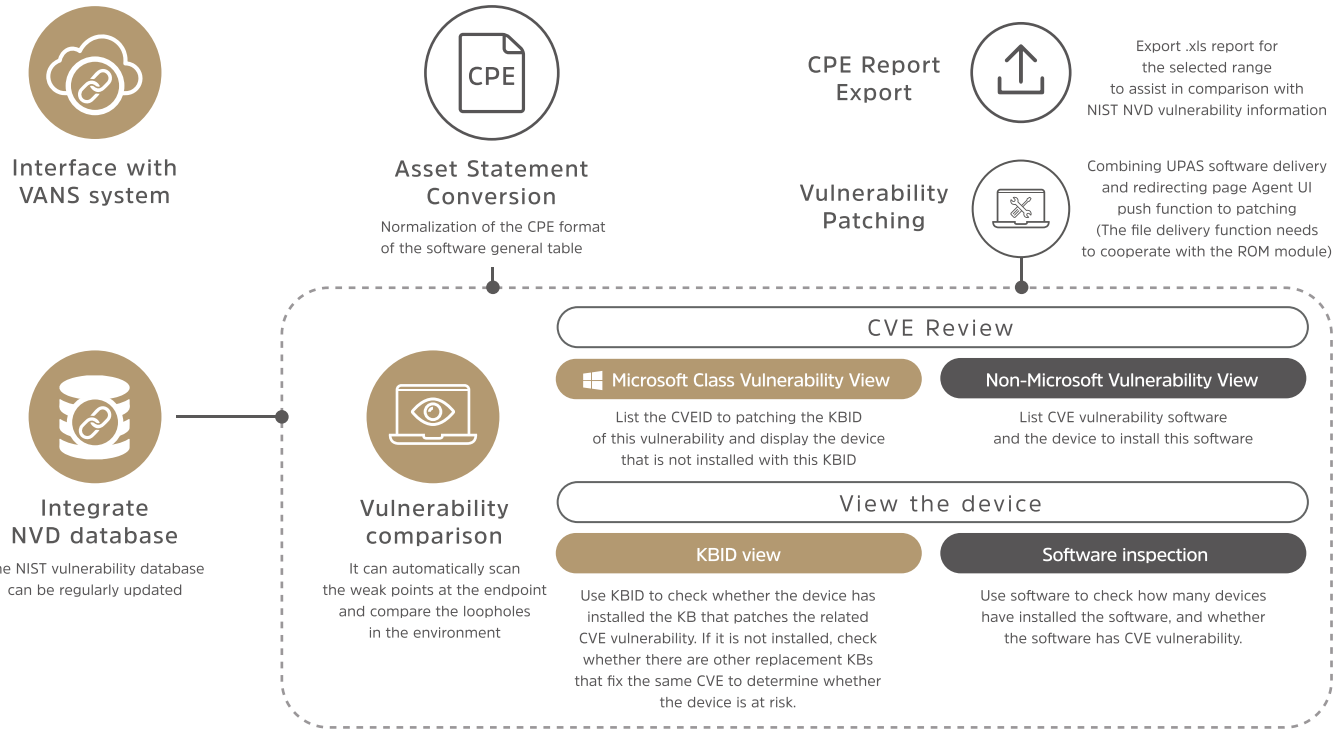
VANS Vulnerability Alert and Notification System

It can integrate the NVD vulnerability database, automatically compare the computer software asset vulnerabilities within the environment, and uniformly inquires that whether the computer software assets of enterprises have CVE vulnerabilities released by NVD.

CVE can be used to detect Microsoft and non-Microsoft vulnerabilities, device KBID can be used to detect the quantity of devices of installing software with CVE vulnerabilities, and vulnerabilities can be patched through software update check, software distribution, Agent UI, page redirection, etc. It also supports the exporting of CPE list and one-click upload to the VANS System of the Institute of Cyber Security, which realizes auditing easily.



▼ Operation Process of Vulnerability Alert and Notification System



AD ADVantage

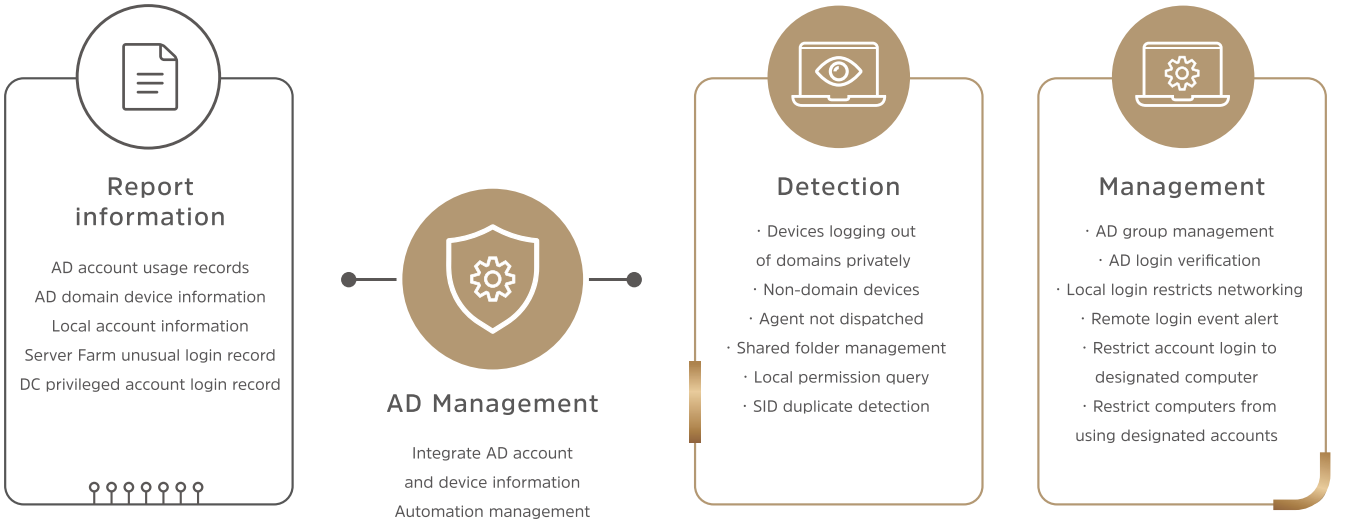
Through binding AD accounts and computers, forbidden local login, forbidden unauthorized domain exit, etc., it forces all computers to follow companies' security policies, use specific AD accounts for logging in specific PC, makes security policies and management cover all Windows devices, integrates over 20 AD information and device information, and provides account use records.

It can detect files and changes in shared file folders. It can detect SID repetition events, and generate privileged account login and logout records and local accounts, and other information, and assist the administrator in discovering abnormalities, and control all devices which should be accessed to the AD domain.

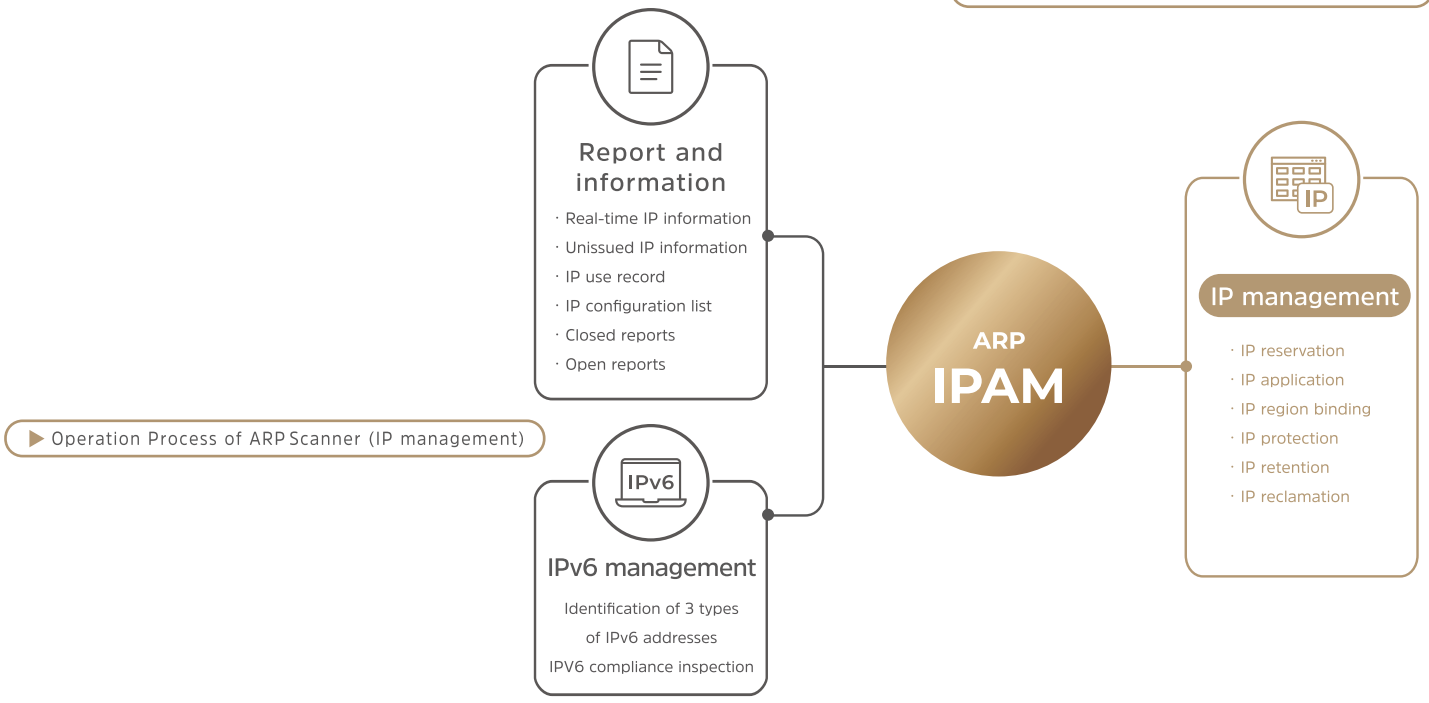
ARP ARP Scanner IP management

It can do multiple binding of IP/MAC/DHCP section/computer name/hardware fingerprint (UUID) to all accessed devices to realize the functions of IP protection, IP retention, IP reclamation, IP conflict prevention, MAC simulation prevention, etc.

UPAS can simultaneously generate: various intranet statistics lists, such as undistributed IP list, IP configuration list, IP use record, open reports, closed reports, etc., help the administrator completely master the intranet assets and IP use situations, and realize relevant setting in one page, facilitating the administrator's timely and easy management of intranet IP resources and devices.



▲ Operation Process of AD Management Module



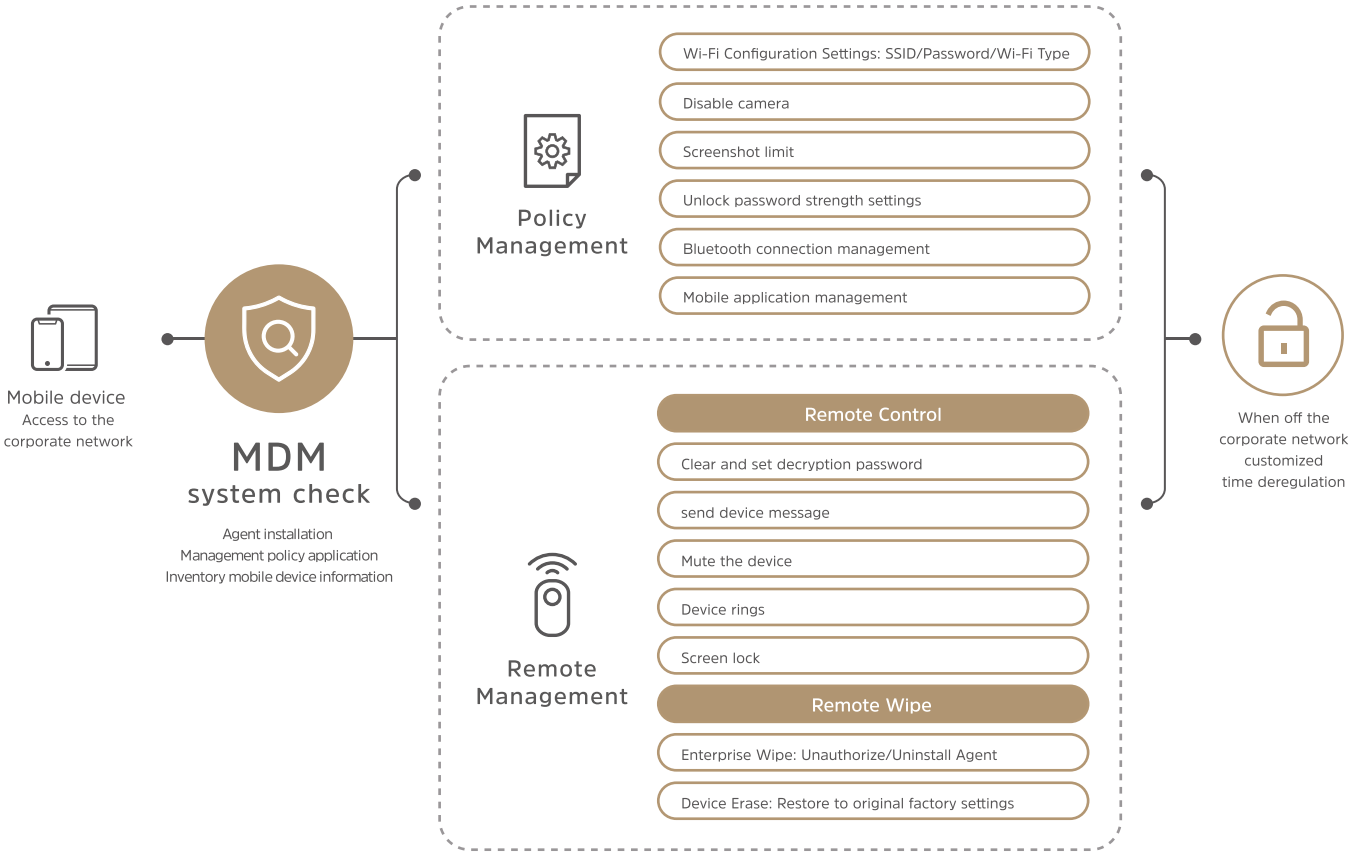
▶ Operation Process of ARP Scanner (IP management)

MDM Mobile Device Management

Through deploying an Agent in Android devices or establishing iOS MDM Server, it can collect information of IP/MAC/accounts/mobile phone models/detailed OS versions/manufacturers/roaming status/last connection time, and execute management of WiFi connection and bluetooth connection, setting password strength, restriction of photograph and screenshots, and application program management, and functions of remote screen locking, delocking,unlocking password resetting, etc.

It can set respective management systems in different plants/working areas, and automatically distribute the groups according to the OS versions/IP section used, and applies the specific group's security policies, reducing the administrator's workload.

It even adds remote functions of factory data resetting, silent mode, ringing, message sending, etc., for Android devices, and provides auxiliary offline positioning judgement to ensure that mobile devices are free of control after leaving the control areas, which can prevent employees for preventing to leave the control areas, then getting out of control and further stealing confidential data.



▲ Operation Process of Mobile Device Management Module

SIM Security Integration Management

Without Agent installation required in terminal devices, it can indirectly realize the integration management of the WSUS host, various antivirus software (Symantec/Trend Micro/McAfee/Kaspersky/Guardian 360) and assets management software (Shenwang/WinMartix/X-Fort/IP-guard/SmartIT/Ivanti/SCOM/SCCM), carries out various compliance inspections, and forces users to do patching till compliance by network disconnection and page redirection, and set different authority restriction for non-compliant devices.

By using the IP/MAC system, it can reach almost 100% WSUS allowance rate, antivirus software installation renewal rate and assets management software update rate, and make terminal devices comply with companies' security strategies.

IPL IP Locator

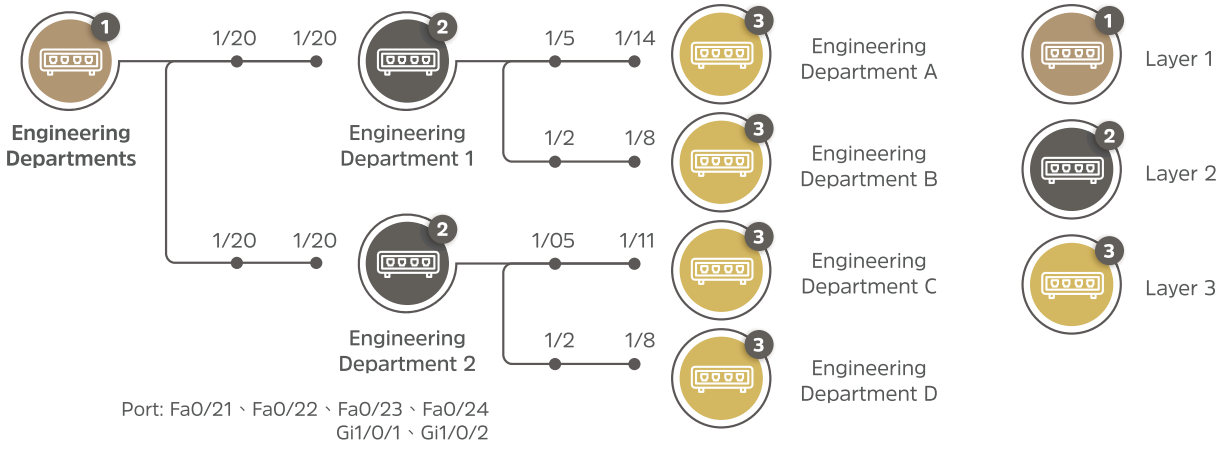
It uses SNMP to automatically establish the relevancy of up-down switch cascading, identifies physical IP addresses of devices, automatically generates the network topological graph, provides historical records of MAC/IP/Switch/Port/VLAN ID, supports the vast majority of brands of switches, and can obtain devices information from multiple platforms of Windows/Linux/MacOS/Android/iOS, etc.

It assists the administrator in personnel inventory and assets statistics, and can build a sole port and multiple MAC list or bind MAC/Port; in case of unauthorized device access, the system will give an alert automatically and has a revision hint prompted to ensure the intranet security and normal network operation.

▼ Explanation on Security Integration Management Module



▼ Architecture Diagram of IP Address Resolution Module



IPv6 IPv6 Management

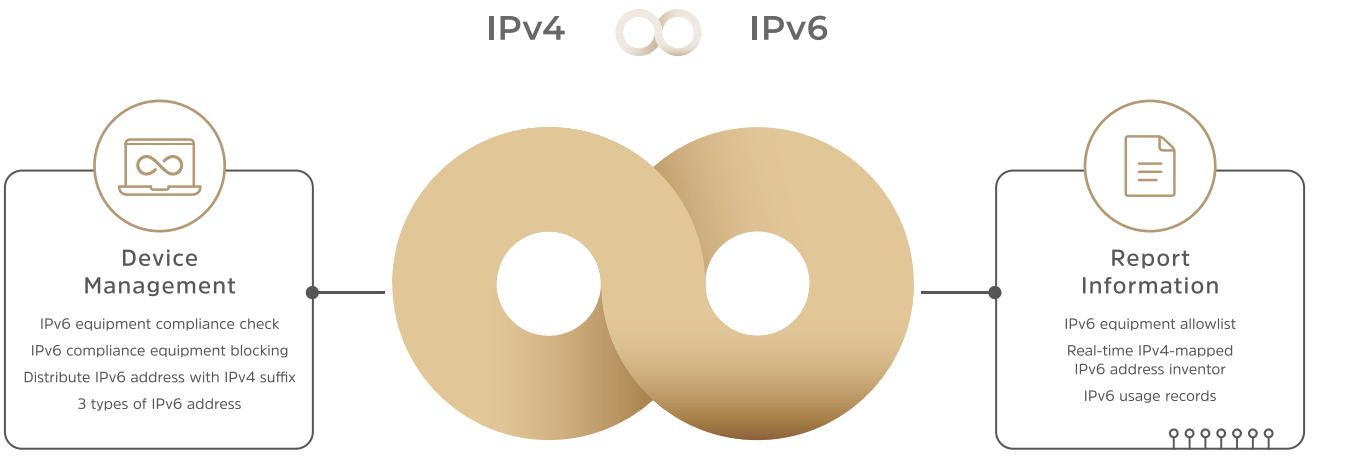
Without Agent installation requirement, it can support comprehensive IPv6 management, can detect three types of IPv6 addresses of single-point broadcast, multi-cast and any-one broadcast, and conduct compliance inspection to IPv6 devices and block external devices using IPv6.

It has the function of automatically set an IPv6 allowlist, can provide temporary and permanent IPv6 allowlists, and import or export IPv6 device lists. According to IPv6 management requirements, it can set allowlists for different management scenarios, and provide multiple IPv6 and MAC addresses for binding functions.

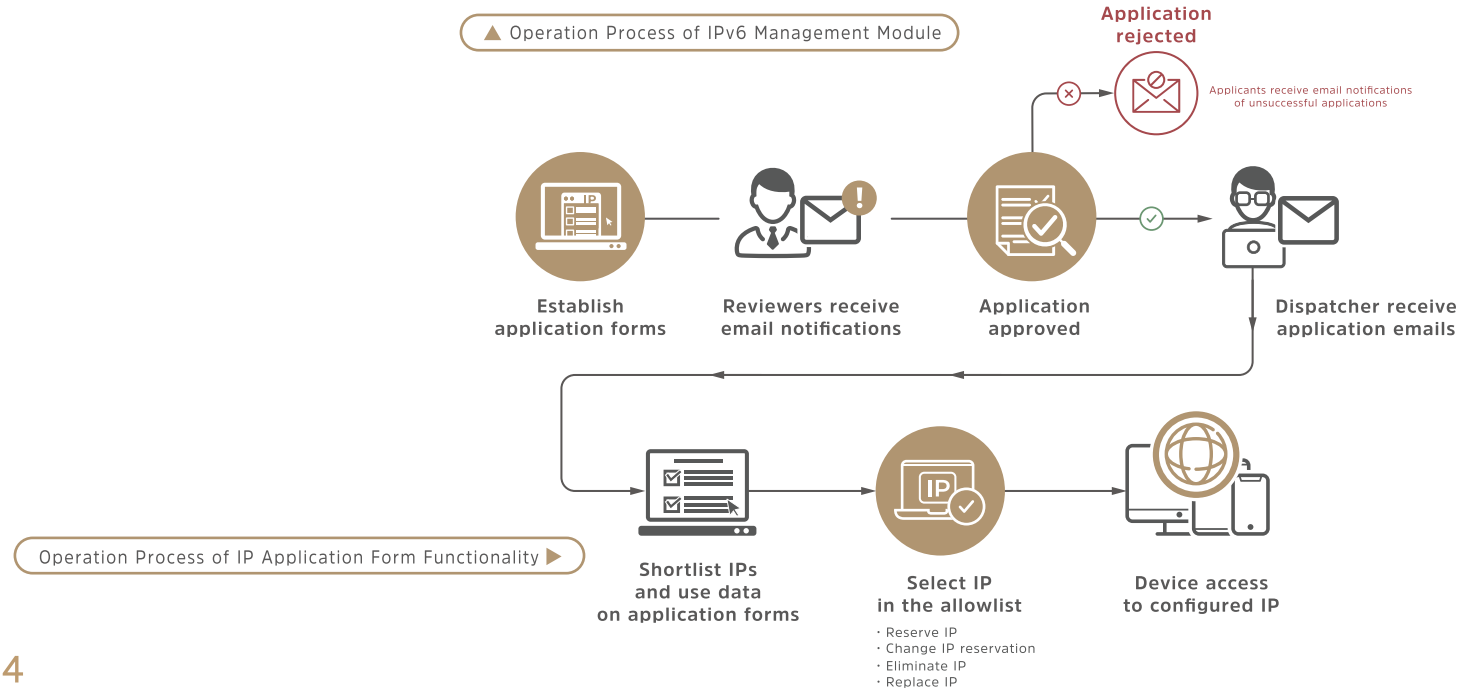
Besides, it provides real-time IPv6 information, historical records and corresponding lists of IPv4 addresses.

IPAF IP Application Form Functionality

The self-defined online IP application form make applicants can complete IP application easily, streamlines troublesome paper application review processes, and realizes comprehensive electronic operation. Besides, users can use the function of search in the IP interface and can search available IPs rapidly in the same page. Once a user has confirmed the IP he/she wants to use, the system brings relevant IP application form information and an applicant can trace the application progress easily and refer to all operation status wen necessary, and these records will be simultaneously recorded on the interface of application records. At the same time, it has the exporting function which allows applicants to export all relevant application information for backup and enquiry. This not only ensures data security, but also facilitate the future investigation and management more.



▲ Operation Process of IPv6 Management Module



Operation Process of IP Application Form Functionality ▶

DHCP DHCP Server Integration Functionality

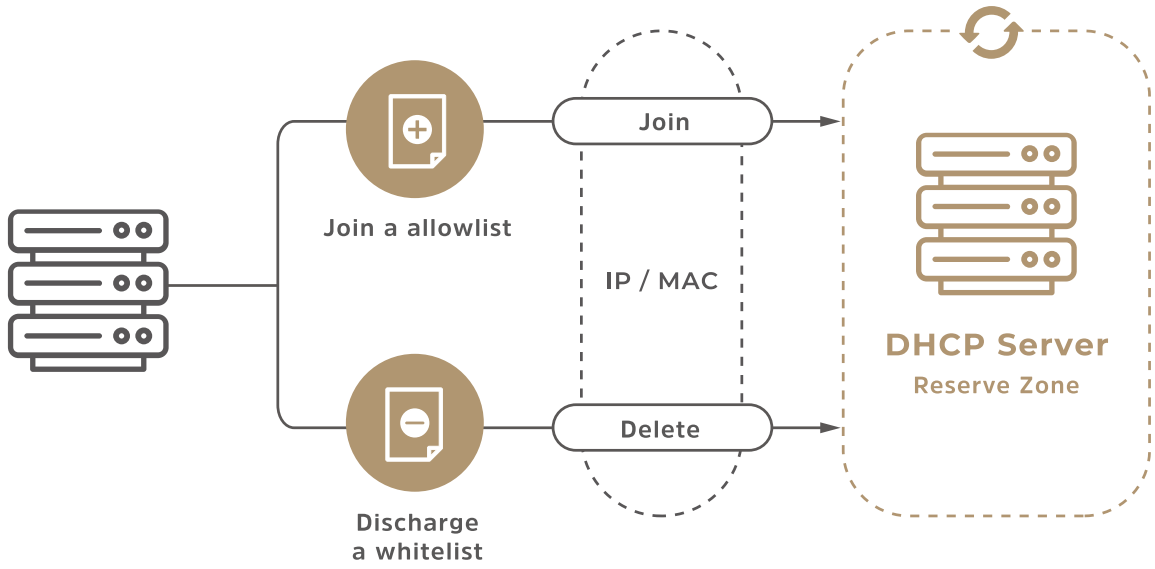
It can synchronize the dispatch of specified IP and MAC to DHCP reserve zones via the allowlist. After the allowlist is established, it automatically synchronize the IP and MAC combinations to the reserve zone of the DHCP server through the system. When an IP is deleted from the allowlist, the system automatically deletes corresponding IP and MAC from the reserve zone of the DHCP server.

Compare the IP and MAC in the allowlist periodically; in case the same IP but different MAC, the system automatically change the corresponding MAC for the IP in the reserve zone of the DHCP service into the MAC address in the allowlist to keep consistent. When an IP and MAC combination is in the reserve zone of the DHCP server but not on the allowlist, the system deletes it from the reserve zone to ensure that the reserve zone only reserves the corresponding IP and MAC addresses as set in the allowlist.

IPLI IP Usage Log Integration Functionality

UPAS can synchronize the online and offline IP usage information and records to a specified Syslog host, which means that it can trace and monitor the IP activities on the Internet in a real-time manner. The function will help ensure network security and provide more complete monitor and analysis tools to optimize network operation and management. It is convenient to store and retrieve historical data by synchronizing information to the Syslog host for risk evaluation, event investigation and compliance.

▼ Operation Process of DHCP Server Integration Functionality



Operation Process of IP Usage Log Integration Functionality ▼



IDC ID Checker

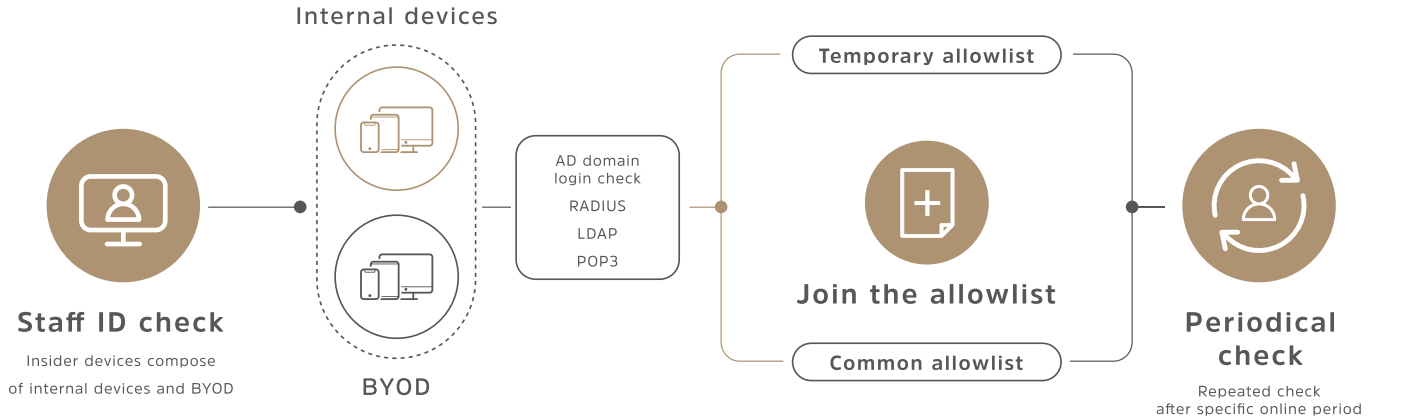
Check staff's BYOD identities through AD/LDAP/POP3/RADIUS servers, rapidly identify devices and manages access permits, and builds the zero-trust security in staff and devices.

When a staff member is accessed to a company or government intranet, the system directs the authentication from the redirection page, and automatically grants corresponding access authority (Internet/intranet/specific network segments) and valid period to the staff member after ID check according the the company's security policies, and also asks periodical device check at fixed time.

GAM Guest Access Management

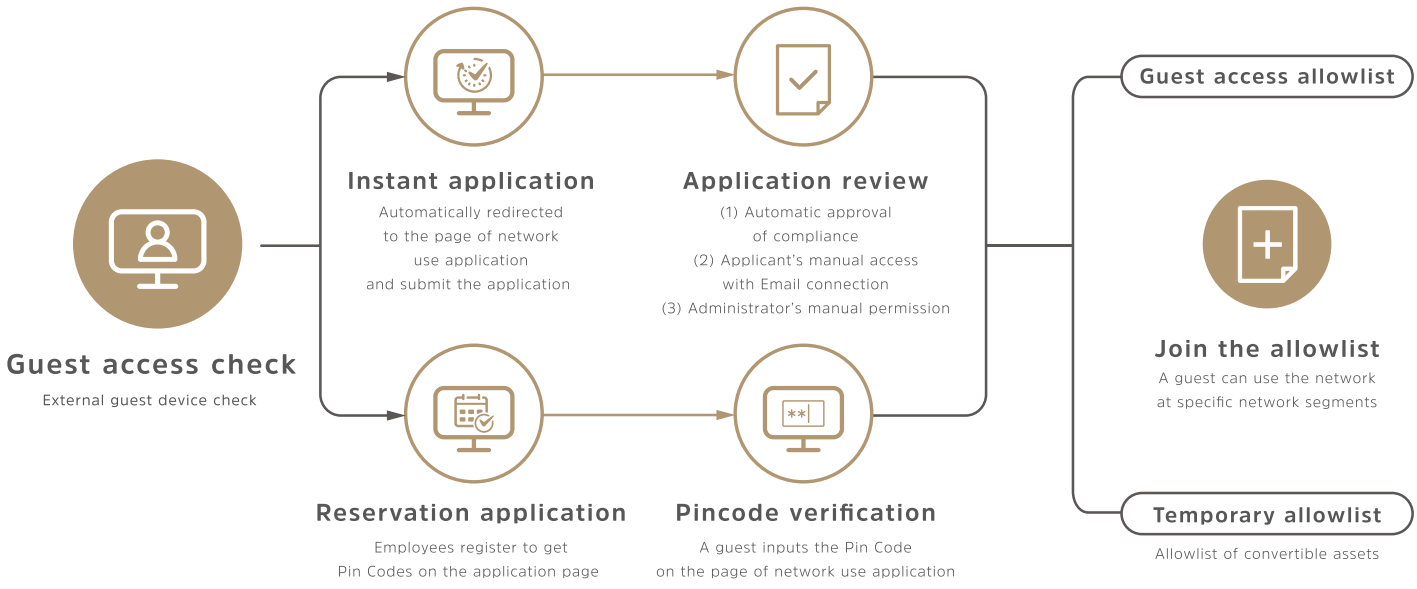
When a guest's external devices are connecting with the company network, the module of guest access management can provide automatic guest access reservation applications, and makes the network accessible through automatic permission, manual permission, and visitee permission.

A guest using reservation application gets a Pin Code in advance, and can have access to the network by inputting the Pin Code on the page of connection application after entering the company network; all guest can set the access authority and period from the intranet and Internet, and the system automatically reclaims the authority when the period expires. The automatic mechanism can easily identify and manage guests, and generate detailed record reports for check



▲ Operation Process of ID Checker Module

▼ Operation Process of Guest Access Management Module



SCP SCP Console

It can assist large enterprises with 5000 pairs of IP/MAC realize transnational and transregional management, and uniformly manage other regions by setting SCP Console/branch Console/Sensor in the headquarter to prevent abnormal Console connection in different regions, and can also check the intranet status of various regions in a real-time manner to integrate global internal data, assisting managers in analyzing event trends and security management policies.

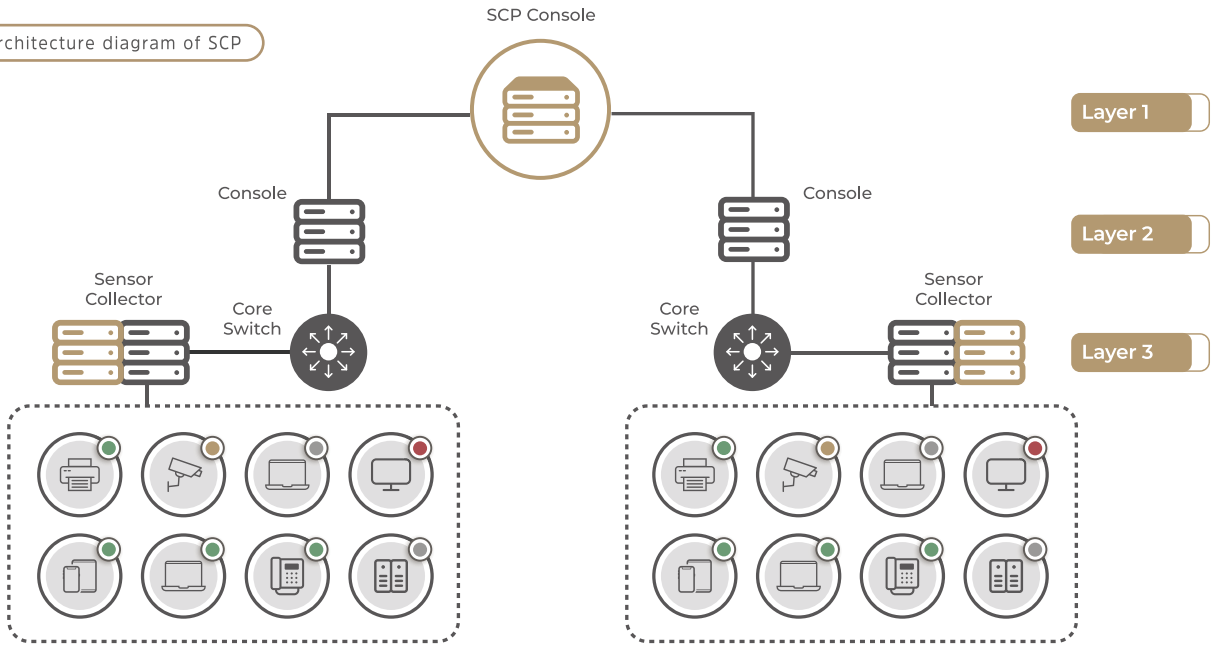
It can also timely synchronize the device information on the allowlist and business trip allowlist to Consoles in different regions in a real-time manner, simplify travelling employees' authority management to keep updated synchronically globally.

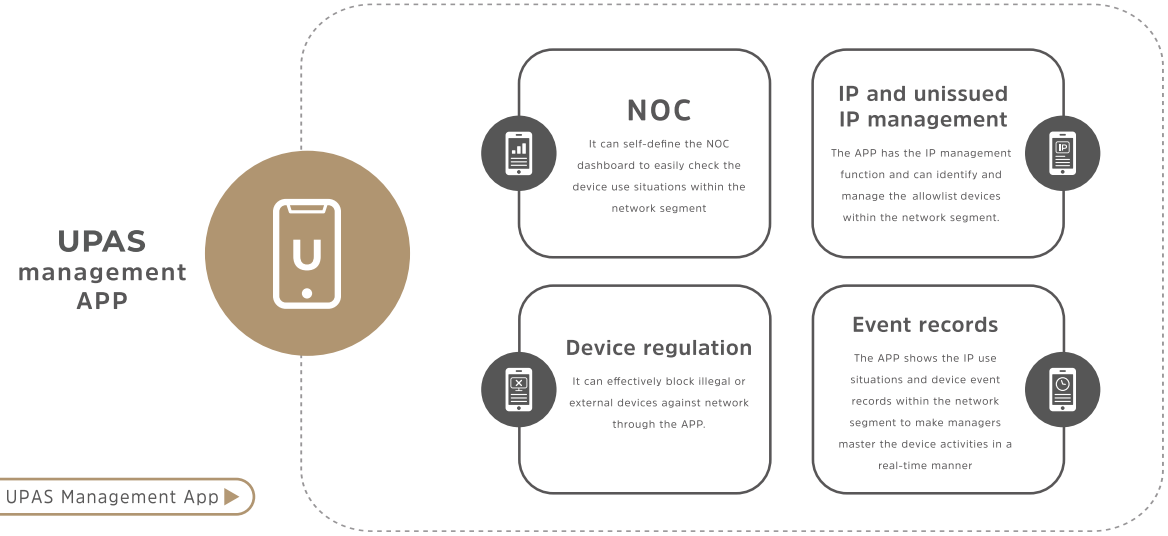
APP UPAS Management App

The action management APP integrates the practical functions of UPAS, and enable managers to keep informed of the company network segment and device use situations at any time anywhere. Managers can easily check the device use situations within a network segment via the self-defined NOC dashboard.

Besides, the APP provides the function of IP management, and can easily identify and manage whitelist devices within the network segment. Through the device regulation function, it can effectively block illegal or external devices against network. Meanwhile, the APP shows the IP use situations and device event records in the network segment to make managers thoroughly master the activity situations of each device and timely respond to latent issues.

▼ Architecture diagram of SCP



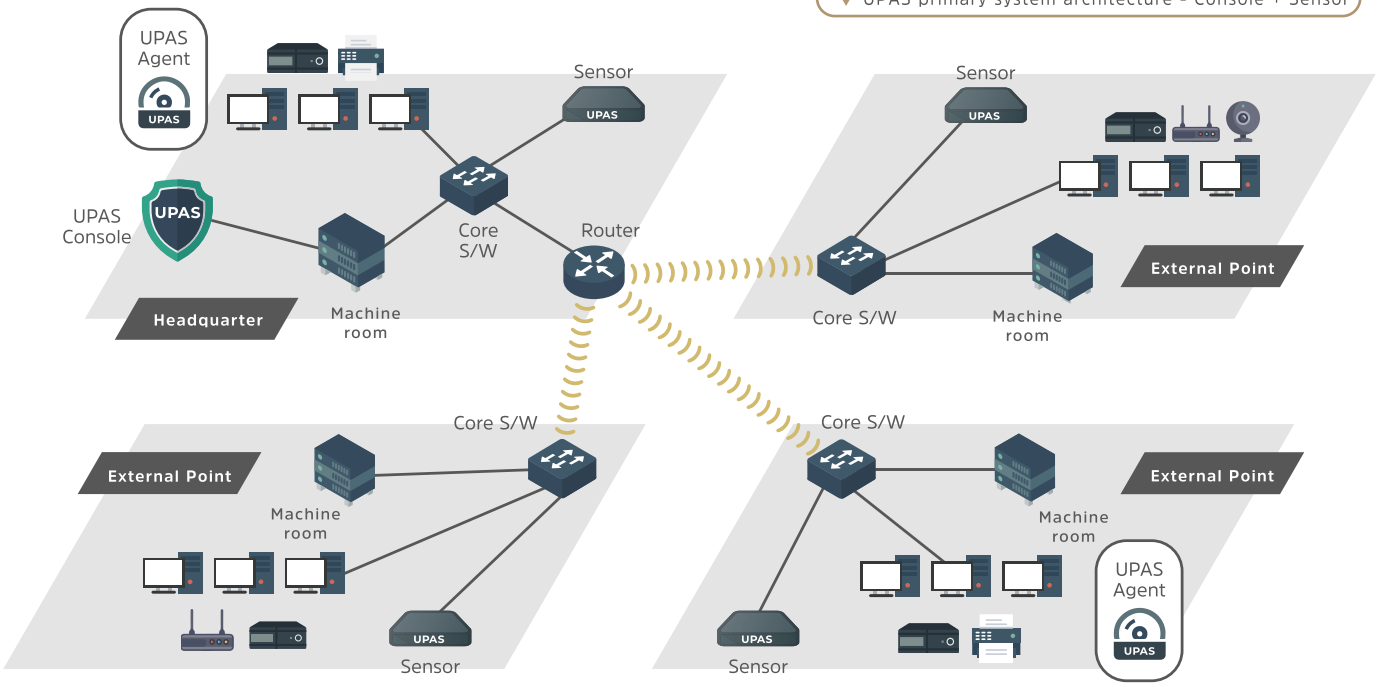


Function Diagram of UPAS Management App ▶

UPAS primary system architecture - Console + Sensor (+Agent)

It is in the sit-in deployment rather than changing the customer-end network architecture, and is applicable in wireless and wired network environments. As long as the Sensor is connected with the Core S/W of the customer environment, the network packet can be obtained through the Trunk Port, all the online devices are checked, and identity check and network access control is done through Console.

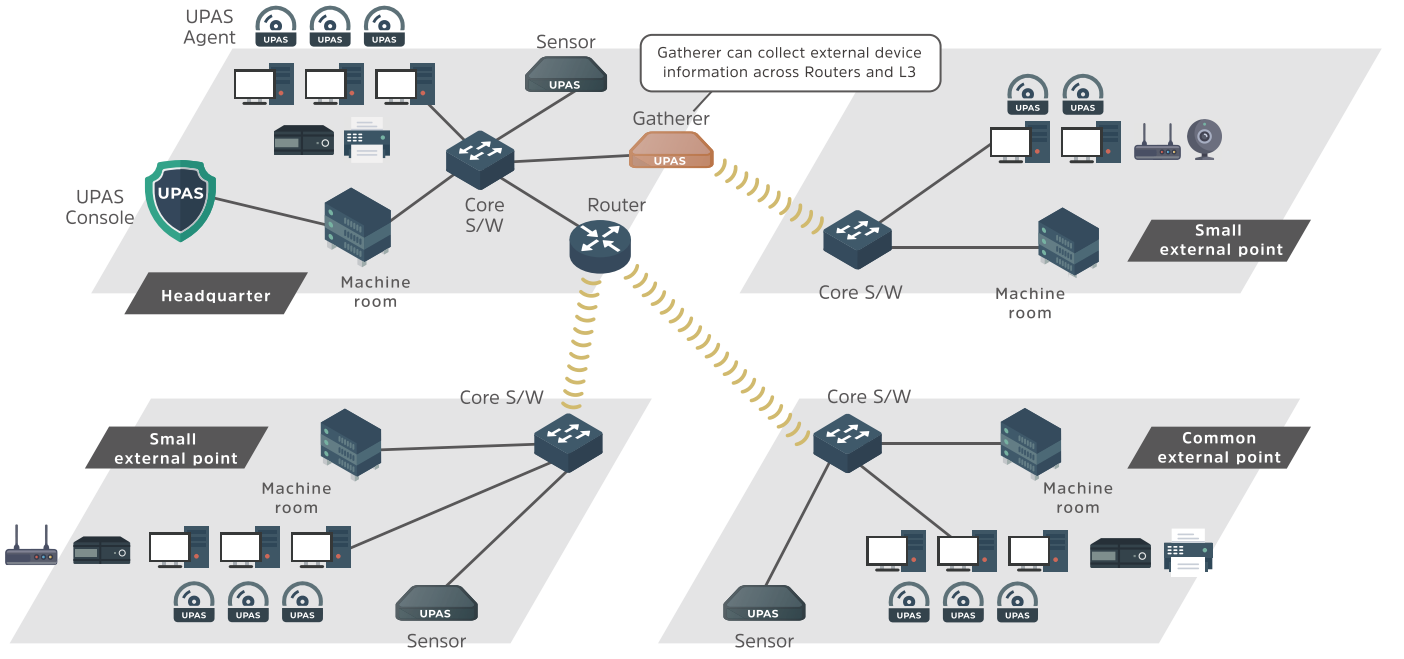
▼ UPAS primary system architecture - Console + Sensor



Gatherer architecture

The Sensor + Gatherer hybrid scheme can the requirements of access control and advanced assets management; especially in the environment with numerous external points, the setting of Gatherer in the headquarter can realize management across Router and Firewall, significantly lowering the system setting cost.

▼ Sensor+Gatherer architecture



UPAS ZTA supports various operating systems across platforms

Support the Windows system
Support the MacOS system
Support the Linux system

ZERO TRUST ARCHITECTURE

- Copyrighted software management
- List of installed software
- File/directive sending
- Blocked software and program inspection
- External USB device management
- Software deletion
- Required software and version inspection
- USB allowlist
- Remote desktop
- Device software change record
- Wireless network management
- User starts remote service request
- Automatic patching
- Software and hardware assets information
- Information push/ group broadcast

Recommended specifications of UPAS ZTA

	Console		Sensor	
CPU	< 1,000 U	4C8T	BOX: <500	J3160 (4C4T)
	1,000 ~ 3,000 U	8C16T	BOXi7: <1,000	i7-8550U (4C8T)
	3,000 ~ 5,000 U	12C24T	1U: 2,000	E3-12XX (4C8T)
RAM	< 1,000 U	8 GB	BOX: <500	4 GB
	1,000~3,000 U	16 GB	BOXi7: <1,000	8 GB
	3,000~5,000 U	32 GB	1U: 2,000	8 GB
HDD	< 1,000 U	250 GB SSD X4 Raid5	BOX: <500	250 GB SSD X1
	1,000~3,000 U	250 GB SSD X4 Raid5	BOXi7: <1,000	250 GB SSD X1
	3,000~5,000 U	250 GB SSD X5 Raid10	1U: 2,000	250 GB SSD X1
Notes	Please separately confirm the single network cards for over 5000U		2000 U/20 VLANs/ 20 network segment restriction	

UPAS ZTA 5 Major Solutions

Tailored to your management demands
Common application scenarios

Based on the main intranet cyber security and management issues enterprises face, UPAS provides five solutions by integrating functions of the 20 strong modules of UPAS ZTA.



NAC Network access control

To ensure no illegal device accessed to the intranet

ARP DAM

Application scenarios

With the significant growth of access network devices in type and quantity, enterprises and government bodies must consider security risks of these devices.

1. How does a company realize comprehensive device inventory and intranet access control and ensure network security without installing an Agent?
2. It is necessary to automatically establish device allowlists according to security policies, and forbid non-compliant devices to have access to intranet.
3. It is expected to do trusted device verification when devices go online and provide comprehensive device security protection.

Solutions

- The NAC system of UPAS uses the ARP patented package resolution technology to realize Agent-less data collection, device identification and highly-intensified access control, and realize 100% asset inventory, including IP/MAC management and network access control.
- The UPAS system can set access rules as demanded, automatically establish a device allowlist, and prohibit the access of unauthorized external devices. At the same time, it provides alert mechanisms of page redirection, Agent UI, MSG, etc., to ensure intranet security.
- The module of DAM device authentication performs hardware or software protection level check, including the functions of enquiring about device health information and authentication histories. The system notifies the administrator of authentication failure in the manner of event.



ITAM IT asset management

Comprehensive virus defence and vulnerability patching
Being compliant and worriless, ensure device health

PM DM ROM
TIM GPO VANS

Application scenarios

There are blind angles in terminal security schemes for installing agent software, and the number of devices without perfecting installation is constantly growing in most enterprises:

1. Versions of many online devices of enterprises are not updated regularly, and external intrusion nodes easily occur; how to ensure the accurate operation of antivirus software and application programs of enterprises?
2. Unknown external devices (e.g.: USB flash drives) are used for data access, resulting in great confidential data leakage and blackmail risks.
3. How to ensure the compliance with governmental regulations of internal devices of enterprises and units, and control their health?

Solutions

- UPAS offers asset management and security monitoring by automatically scanning endpoint devices, collecting software and system details, and integrating vulnerability databases for automated identification and patching of system vulnerabilities.
- Convenient remote management includes remote desktop control, file distribution, and message push/group broadcasting functions for efficient device management by administrators.
- Enhanced trust assessment and access control evaluate trust scores based on device security and identity authentication, determining access permissions. It also offers device security inspection, trust score details, and access history to aid administrators in making access decisions.

IAM Identity authentication management

To ensure that both device and staff identities pass verification

AD

Application scenarios

Intranet-accessed devices must be identified and managed, and be granted the minimal authority based on the identities, making digital identities visual for managers.

1. Enterprises hope to force all computers to comply with their security policies, including using specific AD accounts for logging in specific PC, controlling all Windows devices, etc.

2. Enterprises need to monitor changes in files in shared file folders, and detect latent security risks and abnormalities.

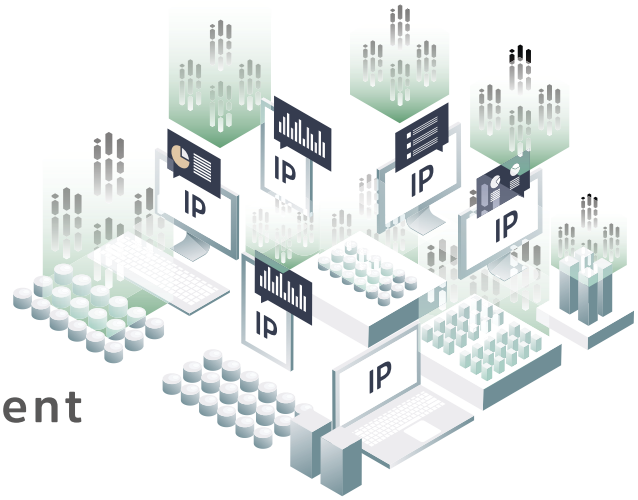


Solutions

- Through binding AD accounts and computers, forbidden local login, forbidden unauthorized domain exit, etc., UPAS forces all computers to follow companies' security policies and use specific AD accounts for logging in specific PC, integrates AD information and device information, and provides account use records.

- It can detect changes in files in shared file folders, including operations of addition, revision, deletion, etc., and detect latent security risk in a timely manner to protect company data security.

- Thorough detecting SID repetition events, and privileged account login and logout records and local accounts, and other information, it assists the administrator in discovering and responding to abnormalities, and control all devices which should be accessed to the AD domain.



IPAM IP address management

Make IP management easier

ARP

Application scenarios

As enterprises and governmental organizations get larger in scale, numerous and complicated network resources remain to be effectively managed and applied.

1. The trouble of management caused by chaotic IP addresses not only affects normal operation, but also dramatically make administrators spend more time in basic maintenance.

2. When an event occurs, it is time-consuming and strenuous in finding problems, missing the best rescue timing.

Solutions

- IPAM can automatically identify device attributes, show IP/MAC information, has the function of multiple binding of IP/MAC/DHCP section/computer name/hardware fingerprint (UUID) for all accessed devices to realize IP protection, IP retention, IP reclamation, and prevent IP conflict and MAC simulation, etc.

- The UPAS can realize management-related functions in one page and generate various intranet statistics list, help managers completely master the intranet assets and IP use situations, and assist the administrator in timely management of intranet IP resources and devices.

MDM Mobile device management

To ensure the security of your mobile devices and confidential data

MDM

Application scenarios

Smartphones, tablet PCs and other devices are popular, and the use authority of network environment should get more attention.

1. The system openness of mobile devices and the convenience of application development without meticulous regulations will alert cyber security risks and upgrade data leakage risks.

2. How to develop BYOD/COPE management regulations

Solutions

- MDM, by combining the network access control technology, sets application regulation policies by group after compliance inspection and identity authentication when mobile devices are connecting to an organization network to strictly protect organizational information security.

- Managers can set management policies by region, with regulatory items of WiFi connection setting, setting password strength, restriction of photograph and screenshots, etc.; and can realize remote (ROM) control of devices in the management interface for screen locking, agent program uninstalling, factory data resetting, unlocking password setting and clearing, ringing and silent mode, information push.

- It supports iOS/Android operating systems.



ZERO TRUST

TRUST UPAS

Benefits from installation of UPAS solutions



NAC – to establish intranet boundary protection

Effectively reduce risks. Prevent risks caused by privately connected devices, including data leakage and virus Trojan horse intrusion.



Asset Inventory – enhanced device visibility

Establish an IoT asset inventory to enhance device visibility and avoid idle devices. And identify device attributes, OS, location, user information and other intranet device data.



Compliance Check – to improve intranet compliance rate

AD management completion rate

Windows Patch update rate

Antivirus software installation rate and update rate

Application software installation rate and update rate



Improve software and hardware management policies

Prevent illegal copyrights from being claimed by the original factory by controlling and disabling software, checking illegal copyrights; asset management can control USB external devices, limit Wi-Fi usage, and prevent the behavior of one machine with two networks.



Improve IP management process

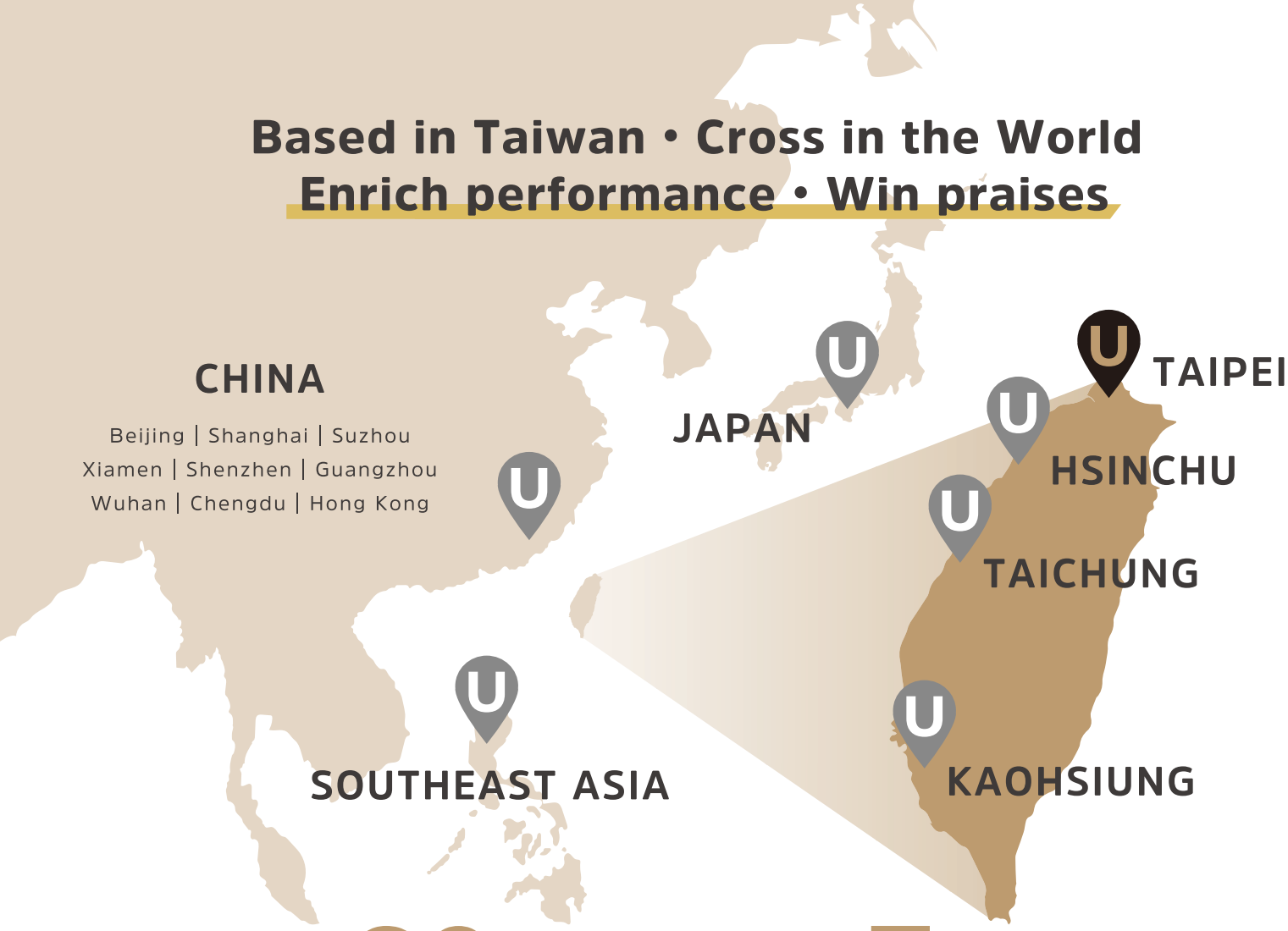
IP distribution, IP recycling, IP reservation, IP protection, IP usage records, IP configuration list, shutdown report, non-shutdown report.



Assist in passing regulations and cyber security audits

Comply with audit standards such as "ISO27001", "NIST CSF", "Cyber Security Management Act", supply chain security check and so on.

Based in Taiwan • Cross in the World
Enrich performance • Win praises



30 years

Original Software Vendor from Taiwan

Professional and independent research and development experience

7

Major Industrial Applications

Government | Technology | Manufacturing
Finance | Medical | Education
General Business | Critical Infrastructure

3800+

Customers Testimony and Trust

100+

Large Enterprises with over 10000 IP

Awarded the evaluation by *APAC CIO Outlook*,

an American Silicon Valley journal

2023 TOP5 Cyber Security Solutions Provider in Taiwan
2023 TOP10 Cyber Security Solutions Provider in APAC

UPAS

ZERO TRUST ARCHITECTURE

Know more about your exclusive best security management solutions

Website | Facebook | LINE | Medium | LinkedIn