INTRANET SECURITY

NAC / IPAM / IAM / ITAM / MDM

NETWORK OPERATION CENTER • ZERO TRUST SECURITY

UPAS NOC

ZERO TRUST / RANSOMWARE PROTECTION

2022 BEST SOLUTION


NOW
RENTING

UPAS NOC

ZERO TRUST SECURITY

Pioneer of Intranet Security Control System

UPAS is a pioneer and leader of Intranet Security, offering a holistic solution that enables enterprises to continuously identify, monitor and enforce compliance of IP-connected devices and endpoints across diverse networks. UPAS NOC, an intelligent and scalable system, is flexible enough to be quickly deployed on the existing framework without 802.1X authentication.

More Than a Product

Our mission is to evolve your intranet security infrastructure with a comprehensive and frictionless strategy. Offering high-end and professional service, UPAS helps you establish security frameworks, protect confidential data and meet the regulations.

Why should we build up intranet security?

With the rapid development of network technology, everything will be clouded and mobile. According to a survey conducted by authoritative consulting company Gartner, IoT devices will exceed 26 billion in 2020. Both users and connected devices will show explosive growth. Applications, servers, and databases will also be linked to each other, breaking the old network boundary. Facing increasingly severe cyber threats, the Zero Trust information security management architecture is indispensable. Only by strengthening verification and access control can we effectively eliminate and promptly discover potential internal information security weaknesses.

Nowadays, enterprises pay high attention to external threats. By strengthening the firewalls and installing antivirus software, enterprises prevent malicious attacks from invading intranet. However, when the above threats are internal, it is often difficult to detect. Inside threats have the following advantages,

- In the daily operations of the enterprise, insider attackers have obtained legal access rights.
- Inside attackers know where the important data is stored and are also familiar with the internal protection mechanism.

The damage will be hard to control if the corporate lacks detection or prevention mechanisms when facing inside threats. Only through the joint defense of the intranet and internet can companies quickly establish the Zero Trust information security management architecture. Treat the intranet as internet, and continuously verify the identity of personnel, device security and network traffic, so as to strengthen the intranet security policy and improve the corporate network environment.

Why should we improve the visibility and controllability of the devices?

1.

The base of information security is to build up Zero Trust architecture. Therefore, how to let every connected devices to be accurately and effectively inventoried, identified, classified, checked ,and controlled is the primary mission to protect information security.

2.

By grasping the real-time information and security status of virtual and physical terminal devices in each network segment, and implementing automatic repair and access control mechanisms based on system policies, it can effectively help the system and data to ensure its security, and respond to information security events quickly and accurately at the same time.

3.

Before hackers invade the intranet, they will search the weaknesses of the uncontrolled devices as an entrance. If the devices are not fully managed and monitored, they will be found and used by hackers eventually.

4.

Traditional methods often use agent programs (hereinafter referred to as Agent) to achieve device visibility and controllability. However, according to research, in the future, more than 90% of the IoT devices will not be able to install Agent, making it difficult for traditional device identification and control technologies to be used.

Through the patented ARP packet analysis technology, UPAS NOC can implement asset inventory, compliance check, and access control with Agentless. UPAS NOC has played a key role in various intranet issues and greatly reduce the information security challenges.

Making Zero Trust
Real for Your Enterprise.

- Effortless and passive deployment **without requiring agents and 802.1X**
- **Bypass system** ensures no business interruption
- **Cross-platform** software runs on Windows/Linux /macOS/Android/iOS

UPAS NOC FEATURES

Eliminate non-compliant device access

UPAS NOC can block macOS, Windows 10 installed with 360 firewall or static IP, Huawei, Xiaomi mobile devices, and other endpoints.

Data integrity and device identification

UPAS NOC can fully identify the IP/MAC, device name and attributes, network card brand, workgroup, operating system, Switch Port, and AD account of nearly 30 types of devices, and complete reports for the most efficient management.

Automated identification and management

Compliant devices are automatically added to the allowlist, and applied with the group security policies; non-compliance devices are denied to access the corporate network and receive the guide message to remediate. Switch updates are automatically relocated; combined with the DHCP assignment function.

Data integrity and device identification

UPAS NOC ensures that the AD account enforcement rate, WSUS synchronicity rate, OS update rate, antivirus installation rate, virus signature update rate, and permit software installation rate reach 98% or more.

Access control

According to management requirements, the non-compliant devices' connections are granted minimal authority. These devices are configured to only connect to a specific host, and the guest access management, including on-site and appointment applications, limits the guest network segment.

High stability and low maintenance cost

The most modern solutions, simply import and flexibility of installing agent, help you embrace zero trust security without changing the existing network architecture. It deploys a bypass system to prevent service interruption while a human error occurs in the system. This ensures the stability of the corporate network.

Visual analysis

The network operation center and asset statistics dashboard integrate all intranet data and transform raw data into visualization, which is more data-driven with comprehensive real-time intranet dynamics to improve management and analysis.

What is **UPAS NOC**

UPAS NOC is a comprehensive intranet security platform, composed of 14 functional modules. Choose integration modules to create an effective solution that is unique to you.

Since our foundation, we've continuously invested in the research and development of unicast blocking issues against the requirement of IP management. Our research result obtained international patents effectively reduces the load on the network environment caused by packet transmission and detection. We offer an integrated, intranet security platform with patented technology for anyone to easily use. Everything we do is driven by our mission to helps people achieve the goal of protecting the endpoint security and efficiency control of the intranet.

14

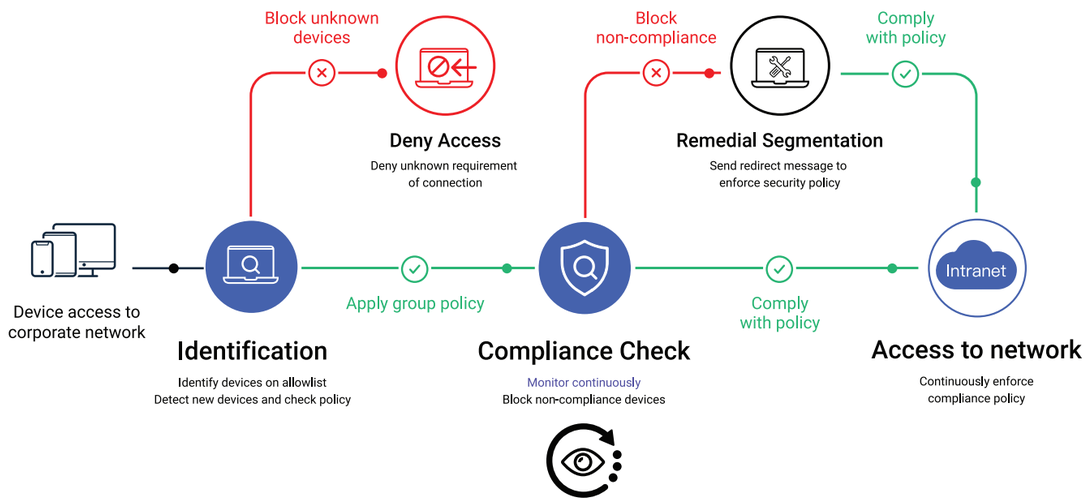
Customize your solution with 14 modules to boost your security more efficiently.

UPAS NOC MODULES

IP

ARPSCANNER

The UPAS NOC main module uses the patented ARP packet analysis technology, which can perform data collection, device identification and high-strength access control without installing Agent. The key functions are IP/MAC management, assets inventory, device access management (NAC, Network Access Control), and network blocking. Multiple bindings between IP / MAC / DHCP segment / computer name / hardware fingerprint (UUID) can be performed on all connected devices to achieve IP protection, IP reservation, IP invalidate, IP conflict prevention, and MAC impersonating. With the built-in reports, managers can manage intranet IP resources and devices in real-time.

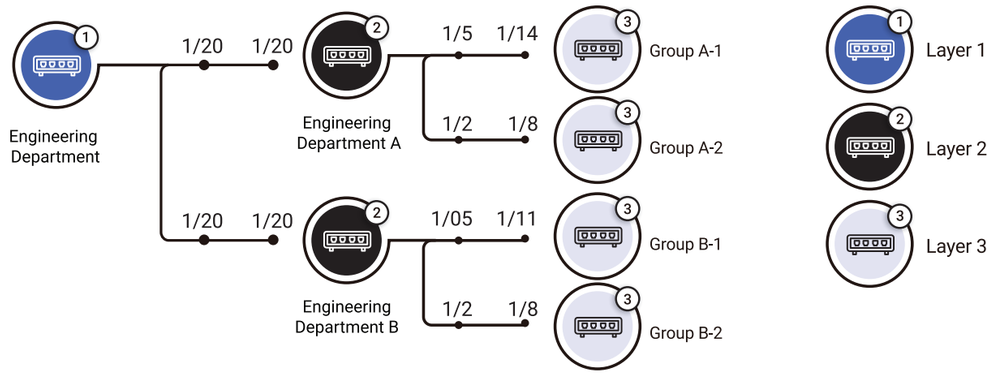


▲ ARPSCANNER System workflow diagram

IPL

IPLOCATOR

IPL uses the SNMP protocol to automatically establish the correlation between the upper and lower switches, identify the physical location of the IP address, generate the network topology, and provide the records of MAC/IP/Switch/Port/VLAN ID. It supports most of the switch brands in the market and can gather device information from different operating systems such as Windows, Linux, macOS, Android, and iOS, to assist managers in inventory assets. A single Port multi-MAC list can be established or MAC/Port binding can be set. If any unauthorized access event occurs, the system will automatically alert and pop up a correction prompt to ensure the intranet security.



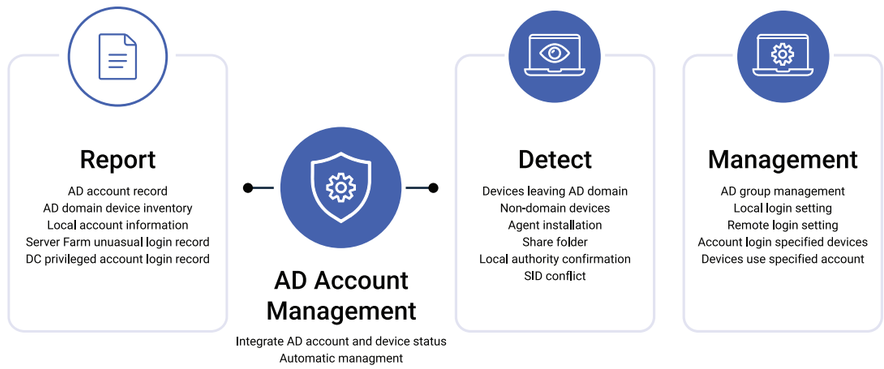
▲ IPLOCATOR Module network architecture diagram
Port: Fa0/21、Fa0/22、Fa0/23、Fa0/24、Gi1/0/1、Gi1/0/2

AD

ADVANTAGE

You can force all computers to follow corporate security policies by binding computers with AD accounts, prohibiting local login, prohibiting privately exit the domain, and using specific AD accounts to log in to specific PCs. The AD security policy and management cover all Windows devices, integrate more than 20 AD and device information. It also provides account usage records.

AD module can detect files and changes of shared folders, and SID conflict events, generate the privileged account login/logout records and local account information to assist managers in finding abnormal behavior, and manage all the devices which should join the AD domain.



▲ ADVANTAGE Module functions

GPO

GPO MANAGEMENT

The application of GPO is important for intranet management. In the zero-trust network, every device must comply with the security policies to lower the possibility of being attacked.

Under a highly completed assets inventory situation, the UGR module can perform GPO inspection on devices in the domain. With network blocking, UGR can force non-compliant devices to apply GPO. In addition, UGR provides GPO application details for each device to ensure security consistency in the intranet.

IPv6

IPv6 MANAGEMENT

The IPv6 module provides comprehensive IPv6 management. It can detect three types of IPv6 addresses, including unicast, multicast, and anycast, and perform compliance checks on IPv6 devices and block foreign devices that use IPv6. It also provides IPv6 real-time information, historical records, and an IPv4-mapped list.

GAM

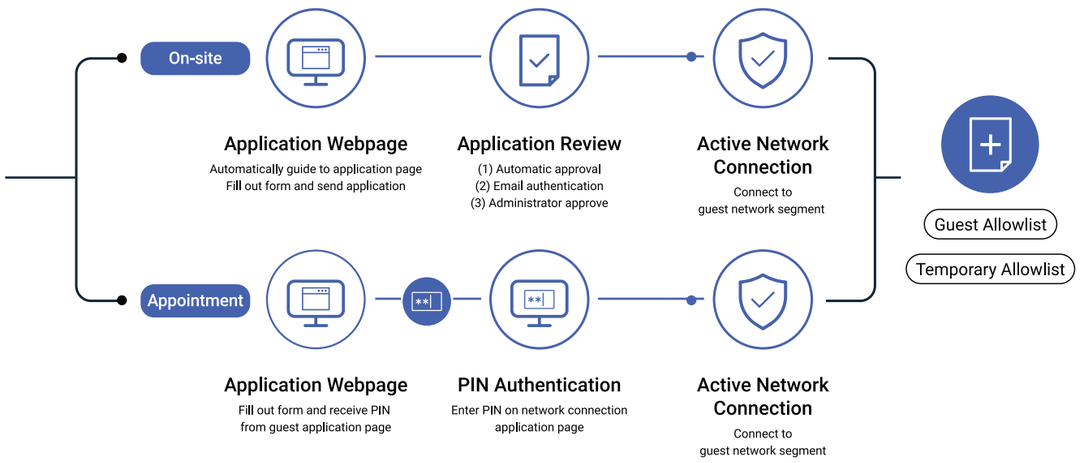
GUEST ACCESS MANAGEMENT

When the guests' devices want to access the corporate network, the GAM module can provide two application methods: guest appointment application and on-site application, through automatic permission, manual permission, and respondent permission to give access.

Guests who apply by appointment will obtain the Pin in advance. After entering the corporate network, enter the Pin on the application connection page to access the network. All guests can be set the intranet and extranet access authorities and access timeliness. The system will automatically invalidate the authorities when the time limit expires. The automated mechanism facilitates the definition and management of guests, and can generate detailed record reports for auditing.

▼ IPv6 Module functions

▼ GAM Module workflow diagram



IDC

IDCHECKER

The module uses AD / LDAP / POP3 / RADIUS server to perform identity verification of BYOD, quickly identify devices and manage connection permissions, and establish zero trust security for personnel and devices.

When a person enters the network, the system will use the redirect page to guide for authentication. After verifying the identity according to the security policy, the system will automatically grant the person corresponding access permissions (extranet/intranet/specific network segment) and effective timeliness. It can also require the devices to be regularly verified every fixed time.

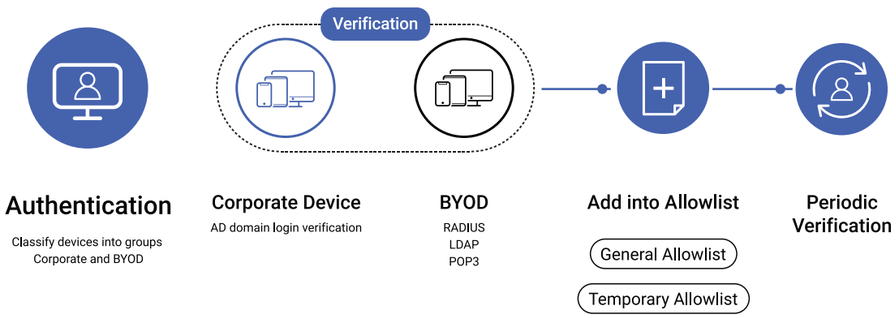
SIM

SECURITY INTEGRATION MANAGEMENT

Without installing Agent on the endpoint device, the module can interface with WSUS host, various anti-virus software (Symantec / Trend Micro / Macfee / Kaspersky) and asset management software (WinMatrix / X-FORT / IP-guard / SmartIT / Ivanti / SCOM) / SCCM) to achieve integrated management and conduct multiple compliance checks. Non-compliant devices can be set with different levels of authority restrictions, such as network blocking and redirecting the page, to force users to repair to compliance.

SIM module uses the IP/MAC system to achieve nearly 100% of WSUS management rate, antivirus software installation and update rates, and asset management software installation and update rates, so that endpoint devices comply with corporate security policies.

▼ IDC Module workflow diagram



▼ SIM Module Orchestrate functions with existing security tools

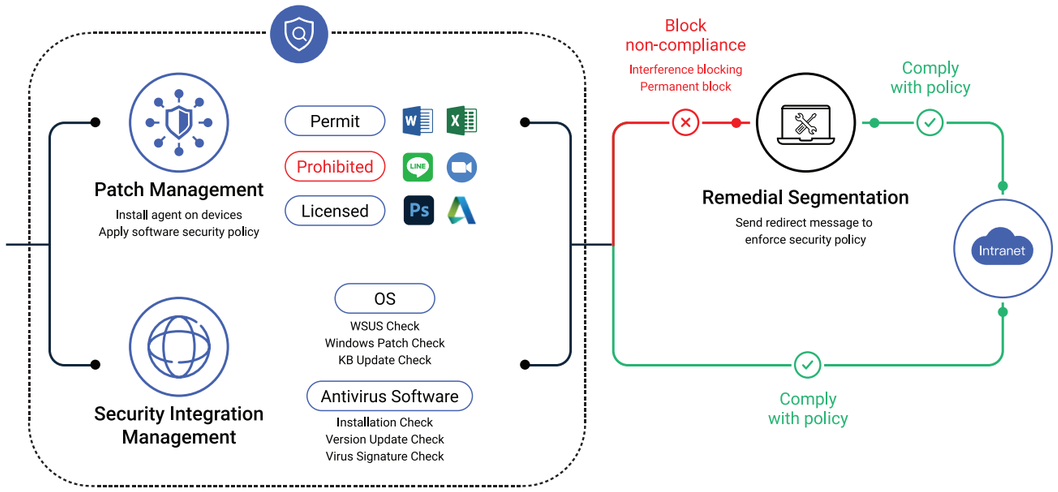
PM

PATCH MANAGEMENT

PM can periodically scan and obtain the software summary of the intranet connected devices, Windows OS version/KB, anti-virus software information and virus signature version by deploying Agent on the endpoint device. Through the collection of the software summary table, the following checks can also be performed: permit software, prohibited software, software copyright quantity, software version.

If there is a non-compliance event (it should be installed but not installed, should not be installed but installed, using pirated software, should be updated but not updated), the network connection can be blocked and the redirect page will show up to inform the reason. Non-compliant devices can be set to different levels of authority to facilitate the stable operation of the device and still guide the repair to comply with the security policy.

▼ PM Module workflows diagram



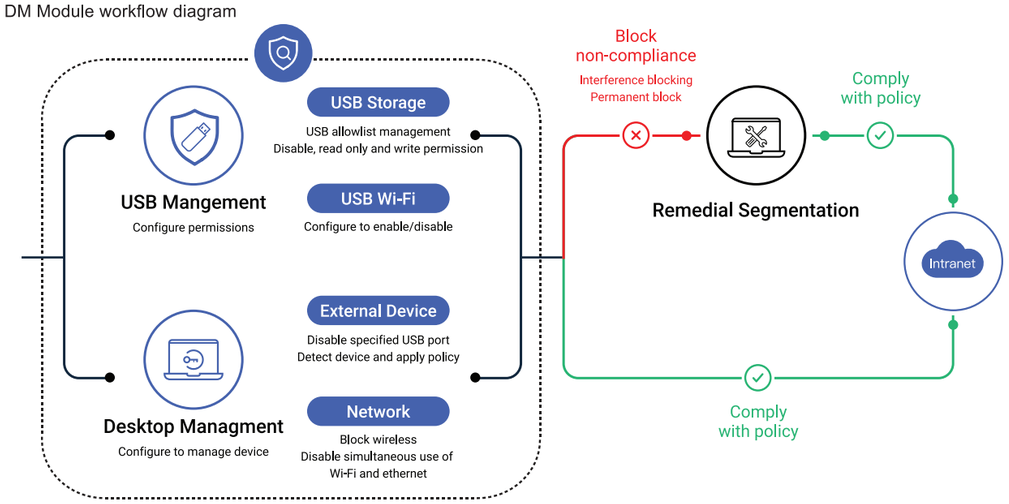
DM

DEVICE MANAGEMENT

By deploying Agent on endpoint devices, DM module can identify and manage USB storage devices, memory cards, USB ports, USB network cards, and optical disk drives. It can set up the authorities for USB devices, such as whether have authority to read and write, to prevent from leaking confidential data, and can set USB device allowlist to prevent unauthorized USB devices from accessing and transmitting data.

In terms of device network management, it can detect and prohibit devices from using wireless networks or Bluetooth, preventing the use of private networks to transmit sensitive data by bypassing corporate networks.

▼ DM Module workflow diagram



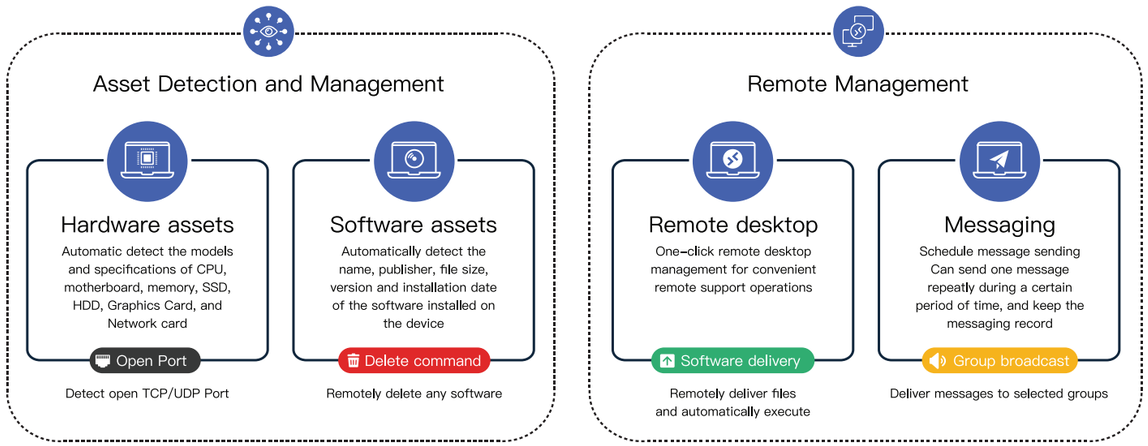
ROM

REMOTE OPERATIONS MANAGEMENT

ROM can automatically detect and collect the hardware and software details of terminal equipment, including software version, CPU, motherboard, memory, SSD, HDD, graphics card, and network card. ROM also provides remote access and control for Windows PC. IT personnel can connect to any PC and perform remote maintenance support by simply one-click on the ROM control interface.

The module can remotely delete any software of multiple operating systems (Windows, Linux, macOS), assisting security team proactively removing risky software. It can remotely deliver files to any certain PC as well, and file types such as exe, msi, and bat can be automatically executed. This feature can combine PM module. Once the PM module detects any PC not installing antivirus software or other permitted software, ROM module can automatically send the installation file to the targeted PC, building an automated vulnerability patching process.

▼ ROM Module workflows diagram



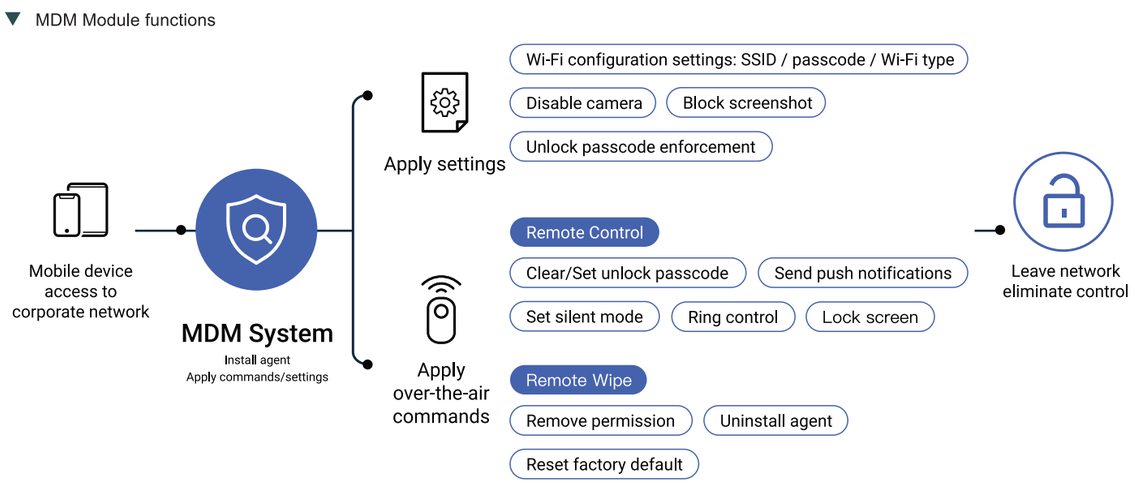
MDM

MOBILE DEVICE MANAGEMENT

Support Android / iOS cross-system management, when the mobile device enters the organization network, MDM module will perform compliance check and identification, collect device information such as IP/MAC/account/mobile phone model/OS version/manufacturer/roaming status/last connection time, apply control policies according to the group settings to protect the security of the organization's information, and provide management tools.

Managers can formulate policies based on the needs. The control items include Wi-Fi connection settings, camera disabling, password strength setting, and screenshot disabling. The management interface can also remotely control the device to lock screen, uninstall agent, restore the factory settings, clear password, mute, and send messages.

▼ MDM Module functions



SCP

SCP CONSOLE

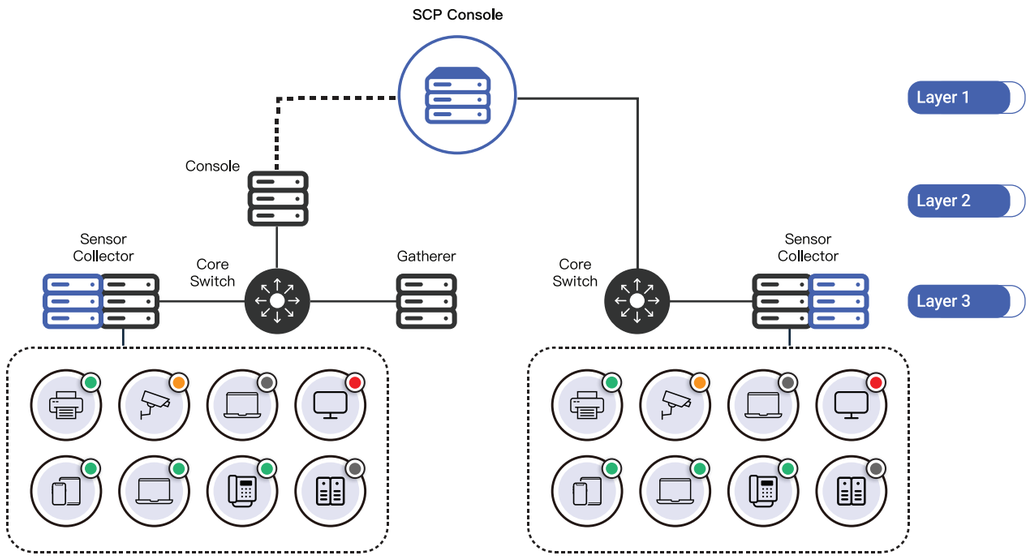
By deploying SCP at the HQ, corporate with more than 5,000 IP/MAC can easily establish cross-border and cross-regional management. With three-layer architecture, which is SCP console/sub-Console/-Sensor, SCP module can unify the management of other areas, prevent the connection error of sub-Consoles, and can check the intranet status in real-time, integrate the intranet data to assist the managers in analyzing the trend of local events and managing security policies. It can also instantly synchronize allowlist devices information and business-trip allowlist to every sub-Consoles, simplifying the authority management of travelers and maintaining global synchronization updates.

UDA

UPAS DATA ANALYSIS

Integrate with internationally renowned data analysis software-Tableau, the UDA module has built-in 99 types of reports with a total of 198 intranet statistical and analysis items. UDA module provides the most complete information security report function in the industry, assists managers to visually analyze intranet data from multiple angles, and various trend statistical charts make it easy for managers to formulate security policies.

Users can customize the contents of the reports, based on different industries, management needs, or regulatory audit requirements by using the UDA module, to pass ISO27001, financial regulation audits easily.

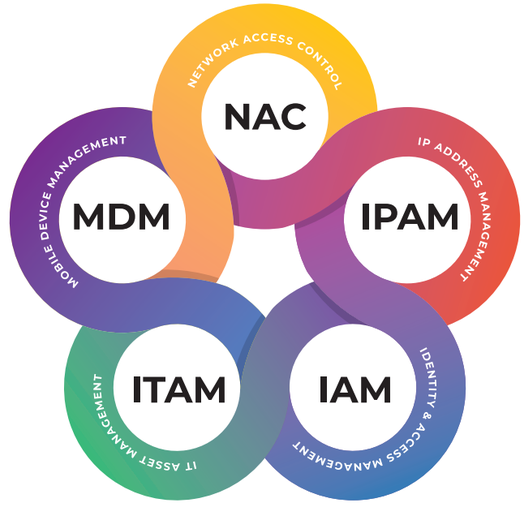


▲ SCP Module network architecture diagram

UPAS NOC provides multiple composite solutions to strengthen the control intensity of multiple management levels such as network access and identity authentication

UPAS Solutions

In response to the main intranet information security and management problems faced by enterprises, UPAS provides five solutions that integrate the 13 modules of UPAS NOC.



NAC

IP IPL SIM

As the types and numbers of devices that access the internet have grown significantly, enterprises and governments must consider the security risks of these devices. Based in the goals of security and efficiency management, enterprises and governments should focus on strengthening the network visibility, access control, and compliance capability.

There are blind spots in using Agent as an endpoint security solution. In most corporate network environments, the number of devices that are unable to install Agent is continuously growing. Needless to say, the devices produced with the trend of “intelligent manufacture” are not able to install Agent due to processing efficiency and interruption risk.

The NAC system can block non-compliant devices from accessing the network, or give only the lowest permissions to reduce the security risk of insecure endpoint devices. In addition, a vulnerability repair process can be formulated to guide devices to grant access permissions after compliance.

UPAS has excellent adaptability and flexibility. With an integrated information security platform, we provide comprehensive management of endpoint devices used Windows/Linux/macOS/Android/iOS and other different operating systems, strengthen the mastery of the intranet on the basis, and help customers to avoid dealing with different products.

The system can automatically collect device attributes, names, IP/MAC, and physical location, formulate security management policies and centralized management, instantly block the non-compliant devices, set repair processes to guide devices to comply with the policy. In addition, it can form various of IP security management, and prevent risks by detecting and prohibiting specific IP using behaviors.

IPAM

IP IPv6 UDS

With the expansion of the scale of the corporates and governments, complex network resources are urgently needed to be effectively managed and used. The management problems caused by the confusion of IP addresses not only affect the normal operation, but also greatly increase the time consumed by the management personnel in basic maintenance.

The IPAM system can automatically identify the device attributes, display IP/MAC information, centrally manage intranet devices, and offer complete IP usage records. The allowlist mechanism is combined to achieve IP/MAC corresponding management and IP management.

IAM

IP IDC AD GAM

The devices that enter intranet must be identified, managed, and granted minimal authority based on their identity to provide managers the visibility of digital identities. But the trend of BYOD (Bring Your Own Device) has brought a new challenge. The devices belonging to corporate are easy to identify and manage. However, if the BYODs have no corresponding management process, they will become a high-risk node.

The UPAS IAM system can comply with corporate security regulations by automatically scanning for privately exiting AD domain devices, prohibiting local login, binding the AD account to the computer, and forcing every employee to use AD account to log in to the designated computer. For BYODs, the LDAP/POP3/RADIUS server can be used for identity verification. Guest can apply for access permissions in two modes: on-site and appointment. In addition, the above verification will produce detailed report for managers to check.

ITAM

IP PM DM

As the application and development of the IoT becoming more popular, the unrecognized and unmanaged devices in the network environment account for the majority. Several security vendors have also confirmed that attacks on IoT devices are becoming more frequent and serious because most of these devices are not regularly updated which makes them are vulnerable to external attacks.

UPAS ITAM can regularly scan all the devices in the intranet, automatically detect information of permit, prohibited, licensed, and uninstalled software, and create software list to help corporate to understand the latest status of all software assets.

If any non-compliant incident happens, immediately block the device and guide the repair, effectively eliminating the vulnerabilities of software assets in the intranet. In terms of hardware assets, you can also set the read and write permissions of each computer, and stipulate that only legal USB devices can access data.

MDM

IP MDM

The popularity of tablets and smartphones shows that the network environment has become more complicated, With the openness of the mobile device's system, the convenience of application development, and the rapid development of application technology, if there is no corresponding information security process, the mobile device will be exposed to high risks. The mobile environment needs to be equally emphasized in the information security strategy.

UPAS MDM combines network access control technology to perform compliance checks and identity identification when mobile devices enter the network, and then apply control policies based on group settings to help companies and governments protect the information security.

Managers can formulate policies based on the needs. The control items include Wi-Fi connection settings, camera disabling, password strength setting, and screenshot disabling. The management interface can also remotely control the device to lock screen, uninstall agent, restore the factory settings, clear password, mute, and send messages.

UPAS NOC Recommended System Requirements

	Console		Sensor	
CPU	<1,000U 1,000～3,000U 3,000U～5,000U	4C8T 8C16T 12C24T	BOX: <500 BOXi7: <1,000 1U: 2,000	J3160（4C4T） i7-8550U（4C8T） E3-12XX（4T8C）
RAM	<1,000U 1,000～3,000U 3,000U～5,000U	8 GB 16 GB 32 GB	BOX: <500 BOXi7: <1,000 1U: 2,000	4 GB 8 GB 8 GB
HDD	<1,000U 1,000～3,000U 3,000U～5,000U	250 GB SSD x4 Raid5 250 GB SSD x4 Raid5 250 GB SSD x5 Raid10	BOX: <500 BOXi7: <1,000 1U: 2,000	250 GB SSDx1 250 GB SSDx1 250 GB SSDx1
Remark	Please contact us if more than 5,000U		Single network card with 2,000U / 20 VLAN / 20 network segment	

Get Insight, Analysis & News Straight
Talk to Our Security Expert Now

UPAS Official Website

Visit our website to know more about UPAS intranet management solutions, including NAC, IPAM, IAM, ITAM, MDM.

UPAS LinkedIn

Follow UPAS to get more real-time information on intranet security, information security news, tips and UPAS product information

Resources Library

Read the UPAS product eBook, which provide various contents such as regulatory audits, industry solutions, and corporate proposals.

Apply for POC Test

Experience the UPAS NOC solution, the specialist will conduct a needs assessment with you, and provide you with the best intranet management plan suggestions.

WEBSITE

LinkedIn

UPAS NETWORK OPERATIONS CENTER

www.upas-corp.com/en
Taiwan
Rm. 8, 9F., No. 51, Sec. 2, Keelung Rd., Xinyi Dist.,
Taipei City 110502 , Taiwan (R.O.C.)
+886-2-2739-3226
Channel Partnerships: support@upas-corp.com