

What's UPAS

NETWORK
OPERATIONS
CENTER

Cybersecurity Management Benefits
Beyond Imagination



Core Values

Ensuring Security of Every Device Accessing the Network

The automatic Pre-Check for any devices trying to access the network includes: login domain check, patch update, antivirus installation, virus feature update, required software installation, use of prohibited software, software vulnerability repair, GPO application, etc.

Establishing Internal Border Protection

Full inspection of information assets prevents access of any external device to the network without permission, as well as the prevent possible risk of such access.

IoT Asset Inventory & Statistics

An inventory of connected equipment is completed with the automatic collection of such details as name, attribute, OS, brand, service time, etc.

Complete IP Management Process

Functions include application, reservation, retention, protection, exception, and reclaiming for IP address, providing IP usage record, and online/offline report.

Complete Software Management Policy

Providing a full inventory of the software installed on the equipment, patches, anti-virus, and controls permit prohibited or licensed software.

Complete Equipmen Management Policy

Providing hardware information, and performing USB management, remote desktop, software distribution, software removal, message push, file encryption, etc.

Establishing Employee & Visitor Management Process

An automatic identity verification process is provided for employee BYOD, enterprise equipment, and visitors, with authority restriction and record retention.

Why

UPAS

NETWORK OPERATIONS CENTER

Safe, Stable, and Convenient
Leading Brand of Intranet Management



98%

Compliance Ratio

AD Improvement
Windows Patch Update
Agent Installation & Update
Antivirus Installation & Update
Installation of Required Software

Benefits of UPAS NOC

- Smooth Network Operation
- Prevention of Data Leakage
- Compliance with Supply Chain
- Safeguard from Ransomware



Easy System Deployment

Easy installation and set-up. Connected devices that do not have to support 802.1X, no need for agents, and flexible environmental adaptation.



Easy Settings

A built-in setup wizard helps you to complete the installation quickly without tedious operations and establish the policy right after system implement.



Intelligent & Automated Designs

Automated allowlist, grouping, distributed agents, application of policies, block and repair of non-compliant devices and reconnection of fixed devices.



Information Collection Up to 99%

Complete identification of device information like device property, host name, agent deployment ratio, and compliance rate of terminal equipment up to 99%.



Information Correctness Up to 99%

Automatic real-time update and correct during change of device information, e.g. device property, host name, agent status, OS, and S/W Port up to 99%.



User-friendly UI/UX Design

The NOC page supports customization for the information displayed and provides notification for AgentUI/redirecting page/MSG/message push to increase user visibility.



Improved Agent Deployment Ratio

UPAS agents are distributed through AD, and if it fails, the agents will be pushed through WMI for precise distribution, ensuring the agent deployment up to 98%.



Abundant Statements

The system integrates all Intranet data, producing 55 charts and 198 statistics and analysis items. Enable you to combine statement items according to relevant industry audit requirements at will.



Risk & System Security Mechanism

Your network will not be affected if UPAS system fails. The system can detect any abnormal behavior, automatically switch to safe mode, avoiding incorrect blocking.



100 Intranet Security Checklist

Establishment of Zero Trust Architecture

Device Access Management

| Allowlist mechanism | Compliance pre-check

IP Asset Inventory & Management

| IP asset inventory | Inventory of 10 operating systems
| Virtual Machine list | Detection for non-stop equipment
| Identification of nearly 30 device properties

IPv6 Management

| IPv6 allowlist | IPv6 usage record
| IPv6 identification/compliance check
| Suffix synchronization between IPv6 and IPv4

IP/MAC Management & Record

| IP application/reservation/reclaiming
| IP retention/protection for important hosts
| IP exception/only | IP usage record
| MAC exception/only | IP configuration list
| IP/MAC binding | Online/offline report
| MAC/DHCP binding | IP entity location
| IP exception/only | MAC spoofing detection
| MAC/Port binding | MAC/name/property binding
| MAC/hardware fingerprint binding
| Single port with multiple MAC detection

AD Domain Management

| Local login restriction | Local account management
| PC/AD account binding | AD account login verification
| Leaving domain detection | PC/AD account login record
| SID duplicate detection | Shared folder management
| Server Farm login record | Privileged account login record

Guest Access Management

| On-site application | Appointment application
| Guest equipment compliance check
| Permission management of visitor equipment

Employee Identity Authentication

| BYOD identity Authentication | Periodic verification
| Integration of AD/LDAP/POP3/RADIUS server

Windows Patch Management

| 98% patch update | 98% WSUS managed

Antivirus Software Management

| 98% installation | 98% virus features update

Software Management

| Permit software | Licensed software
| Prohibited software | Software installed list

Desktop Management

| USB devices management | USB access control
| Wireless network management | USB allowlist

Remote Operation Maintenance

| Hardware information collection
| Message push/group broadcast
| Software distribution/deletion | Remote desktop

File Encryption

| Secret key encryption | Password encryption

Vulnerability Notification and Repair

| NVD integration | Automatic repair (ROM)
| Automatic environmental vulnerability detection
| CVE/CPE/device vulnerability inspection
| Microsoft KBID/CPE vulnerability inspection

GPO Management

| GPO compliance check | GPO repair
| GPO compliance report | GPedit disabling
| Configuration reset

Mobile Device Management

| Screenshot management | Camera restrictions
| Password management | Wi-Fi management
| Enterprise removal/device removal
| Remote control of ringing/message/screen locking

UPAS NOC

New Generation CyberSecurity Solutions

Security • Stability • Convenience

SUCCESS CASES

100+

Multinational companies
with more than 10,000 IPs

3,000+

Organizations we have served

SERVICE LOCATIONS

In addition to the Taipei headquarter, UPAS has branches in Hsinchu, Taichung, and Kaohsiung. Overseas service centers can be found in Beijing, Shanghai, Guangzhou, Hong Kong, Fuzhou, and Thailand.

UPAS NETWORK
OPERATIONS
CENTER

WEBSITE



White Paper



Linkedin



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