UPAS NOC

ZERO TRUST · INTRANET SECURITY

FAB Access Control Solution

Meet Apple / HP / HUAWEI Supply Chain Requirements

WEBSITE

image: Freepik.com

"
The IP/MAC management system allows me to effectively manage unauthorized computers, and the automated group policy also greatly reduces the workload, and the entire management work is like a duck to water.

Electronic manufacturing
Director of information security
"

"
A complete grasp of endpoint devices and IP resources is an indispensable goal of intranet management. UPAS NOC provides a comprehensive management interface that can easily find out the personnel, time, and features associated with IP.

Chemical manufacturing
Information Office Manager
"

"
Nowadays, there are many and complicated unknown devices entering the intranet, UPAS NOC can support different operating systems, and is also in place in terms of compliance check and authorization procedures.

Automotive supplier
Information Engineer
"

"
Inspections can be performed in different environments such as OA / OT / FAB, and multiple safety inspections are integrated, which speeds up the entire management process! The cooperation during the deployment also made the system very suitable for the needs.

Semiconductor manufacturing
Information Specialist
"

Low interference blocking technology

A variety of alarm methods to adapt to the network environment of the factory

UPAS NOC provides Sensor Proxy technology. When the device violates the security policy, it can block the internet connection and allow specific IP or intranet connection permission to avoid interruption of the production line while eliminate risks.

According to the use environment of the factory, the alarm method can be set to redirect the webpage / MSG / Agent UI three methods to avoid the lack of implementation of the security policy due to the habit of not being aware of the alarm in time.

Automated access control

Significantly improve intranet visibility and reduce management pressure

UPAS NOC provides an asset inventory mechanism superior to the industry through patented technology by using technologies such as server IP segment, OUI, SNMP, WSUS/antivirus/SAM hosts' database, Agent, NMAP, DHCP to collect device attributes.

The devices will be automatically applied group policies based on their attributes. System will automatically check whether the devices comply to the corresponding policy and generate repair processes to reduce the window period of manual management.

Security integration management

Enhance maintenance rate to 98% by easily implementing security policies

UPAS NOC integrates with WSUS host, various of antivirus software, and asset management software to achieve integration security management. Patch and virus code version can be automatically checked, and the maintenance rate can be increased to 98% through patented technology, effectively reducing the risk of security vulnerabilities.

Antivirus Software：Symantec / Trend Micro / Macfee / Kaspersky ｜Asset management software： WinMatrix / X-FORT / IP-guard / SmartIT / Ivanti / SCOM / SCCM

Agent deployment technology

Adapt to the complex factory environment

Various Agent deployment technologies

UPAS NOC provides Agents for different OS such as Windows, Linux, and macOS to meet the complex OS environment of FAB. Agent installation options such as GPO, web page redirection, and WMI push installation are provided. With the use of asset list, the Agent installation rate can be increased to more than 98%.