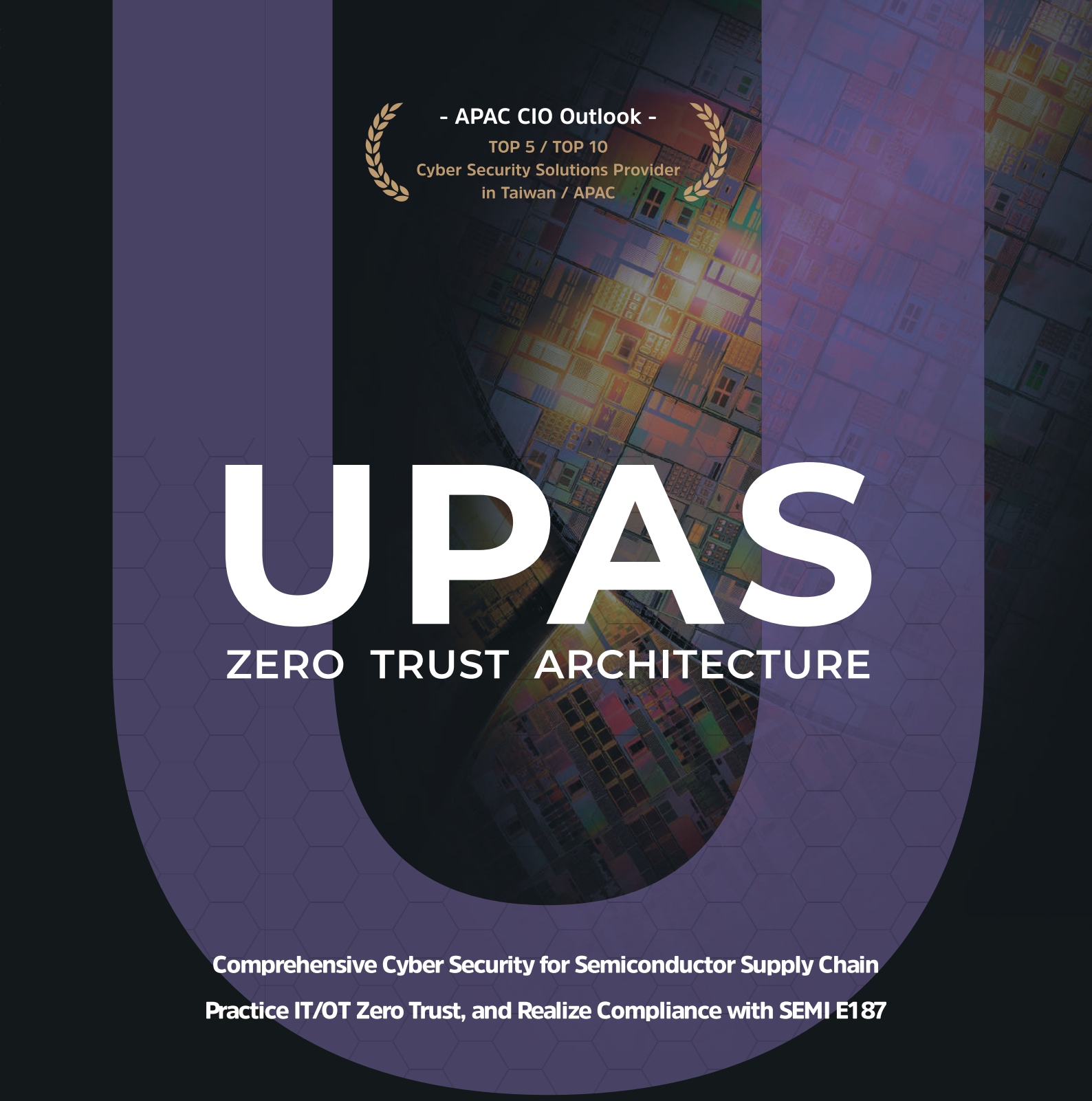


- APAC CIO Outlook -
TOP 5 / TOP 10
Cyber Security Solutions Provider
in Taiwan / APAC

UPAS

ZERO TRUST ARCHITECTURE

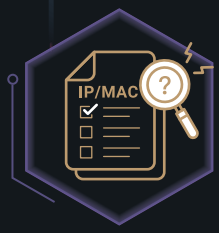
Comprehensive Cyber Security for Semiconductor Supply Chain

Practice IT/OT Zero Trust, and Realize Compliance with SEMI E187

FAB

Compliance solutions for FAB
semiconductor/manufacturing industries

Considering the frequent occurrences of cyber security incidents in recent years, for example, several well-known domesitc semiconductor factories were forced to suspend operation several years ago, and many enterprises suffer from customer data leakage recently....



Difficulty in blocking illegal devices

The allowlist management policy is aimed to clearly know the amount of intranet device assets, and disconnect illegally accessed devices to network.



Low Agent deployment rate

The Agent installation list management is designed to clearly know the Agent deployment rate and build zero-blind-angle defence.



Insufficient device security

Effectively master the update status of Windows OS Patch, antivirus versions, etc., to enhance cyber security defence.



Imperfect software management

Carry out policy management on required, blocked and copyrighted software, direct timely patching of vulnerabilities, and lower risk damage and loss.

UPAS Applicable Domains

Agentless

Complete asset inventory, and device access management

UPAS uses the exclusive NAP patented technology, and supports multi-VLAN environments, and can realizes 100% information asset inventory without installing an Agent, automatically block illegal devices and give an alert for page redirection to ensure that every intranet-accessed device is secured and compliant.

Automatic management with a clear understanding of IoT devices

It dynamically collects assets attributes and identifies IoT device assets by using OUI, interface DB, NMAP, DHCP package resolutions technologies, etc.

Agent

Supply chain audit compliance

It can thoroughly promote device security compliance, Windows Patch update rate, antivirus installation and update rates, required software compliance, blocked software policies, illegal software copyright check, etc. It assists in compliance with ISO27001, NIST CSF, SEMI E187, supply chain security inspection, and other audit standards.

Cross-platform Agent, suitable for complex factory environments

UPAS Agent supports operating systems of Windows, Linus, MacOS, Android, IOS, etc., can meet diverse working environments of factories, and enhance device accommodation rate.

Best Choice, UPAS

Easy to install and set, automatic design

NAP patented technology, simple deployment architecture, and automatic management process; devices automatically added in the allowlist ➔ automatic grouping ➔ automatic Agent distribution ➔ policy compliance inspection by group ➔ automatic isolation ➔ automatic patching ➔ device network re-connection after compliance is ensured

Comprehensive security inspection:
including Windows Patch update, antivirus software installation, and inspection of required and blocked software, USB management, software vulnerability update, etc.

Guaranteed continuing production

In case of a violation, a traditional NAC architecture directly block the connection capability of illegal devices, probably resulting in business suspension in plants, affecting production line operations, and further causing huge business loss.

UPAS values the system security, and uses error-proof design and fault ByPass to ensure uninterrupted production.

The compliance rate of terminal devices is up to 98%

The UPAS system uses the NAP technology to obtain the 100% intranet information asset list; identify IP/MAC, device attributes, computer names, operating systems and other information. It compares with the Agent deployment list to reduce non-compliance and strengthen the Agent deployment rate. The compliance rate of terminal devices is up to 98%.

How does SEMI E187 respond?

SEMI E187, the first semiconductor production line and device cyber security standard initiated by Taiwan, has been officially announced in the website of SEMI in January, 2022. The four focuses of the standard include:

- Network security
- Information security monitor
- Operating system specifications
- Endpoint defence security

ZERO TRUST ARCHITECTURE practices IT/OT zero-trust

UPAS

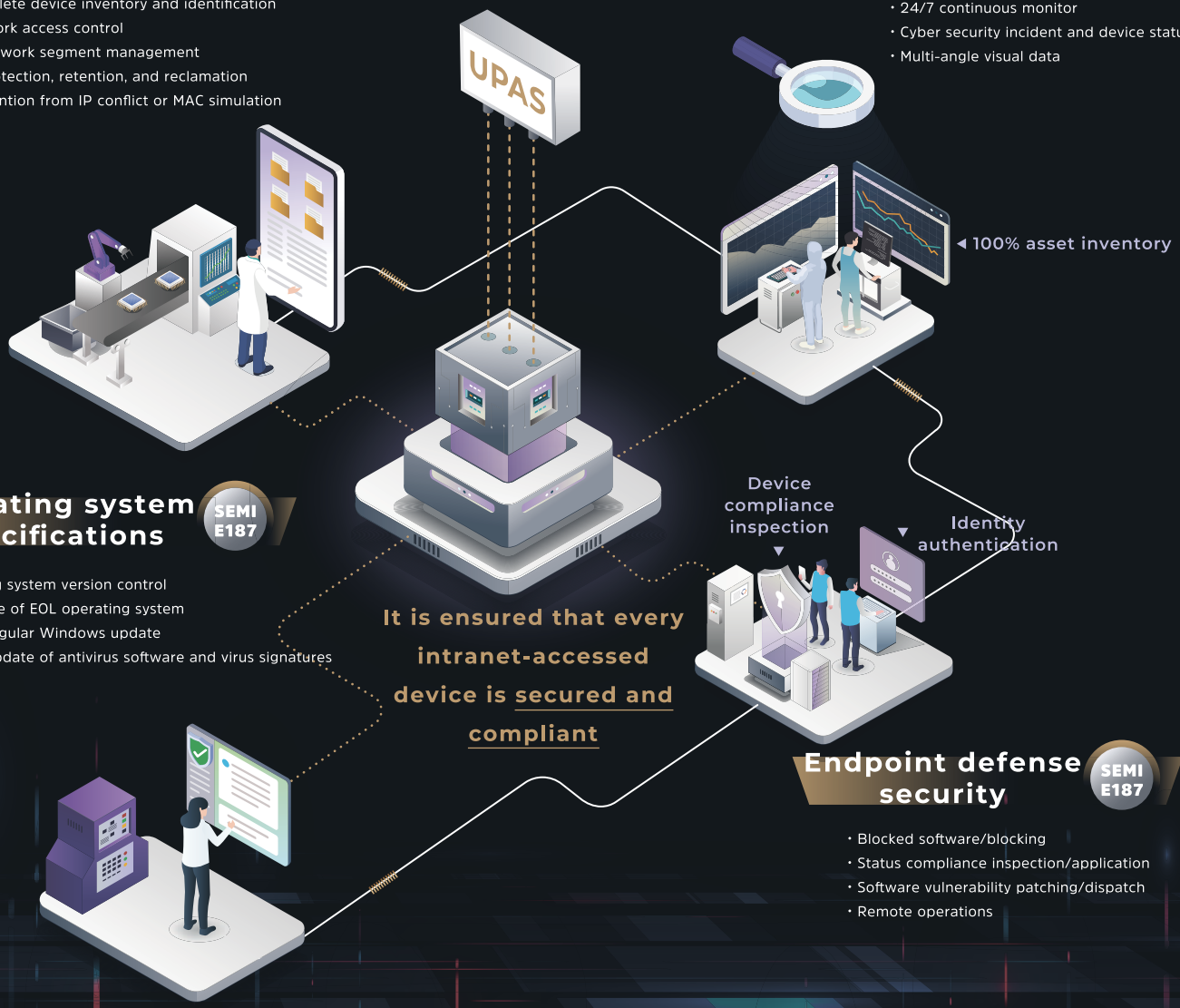
Improving the security resilience of the semiconductor supply chain

Network security (SEMI E187)

- Complete device inventory and identification
- Network access control
- IP network segment management
- IP protection, retention, and reclamation
- Prevention from IP conflict or MAC simulation

Information security monitor (SEMI E187)

- 24/7 continuous monitor
- Cyber security incident and device status logs
- Multi-angle visual data



Operating system specifications (SEMI E187)

- Operating system version control
- Avoidance of EOL operating system
- Ensure regular Windows update
- Ensure update of antivirus software and virus signatures

It is ensured that every intranet-accessed device is secured and compliant

Endpoint defense security (SEMI E187)

- Blocked software/blocking
- Status compliance inspection/application
- Software vulnerability patching/dispatch
- Remote operations

Professional, Dedicated and Trustworthy

Information Director, semiconductor giant enterprise in Taiwan

「UPAS can realize rapid importing, and effectively integrate intranet information. When reporting situations to the Cyber Security Officer, I could state the intranet management policies in detail and make the organization effectively focus on threats and risks.」



Information Specialist, Central Administrative Organ

「Civil servants' network devices and access authority are regulated, and devices are under many restrictions, such as: blocked software, USB access, etc. UPAS can respond to our demands with restricted management methods.」



Information Director, a well-known bank in Taiwan

「The government has strict audit standards, there are management mechanisms that banks need to comply with, such as ISO 27001, NIST CSF, etc.; UPAS can automatically solve the heavy responsibility of management, and assist in perfecting auditing through over 30 types of reports.」



3800+

Being trusted by customers, such as central departments, police affairs and national defence organs, local governments, financial institutions, semi-conductor enterprises, technological industries, key infrastructure enterprises, education and academic units, retail industry, companies, etc.; be professional and dedicated to building the zero-trust architecture for customers, and provide resilient cyber security defence.

100+

Transnational companies with over 10000 IPs

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