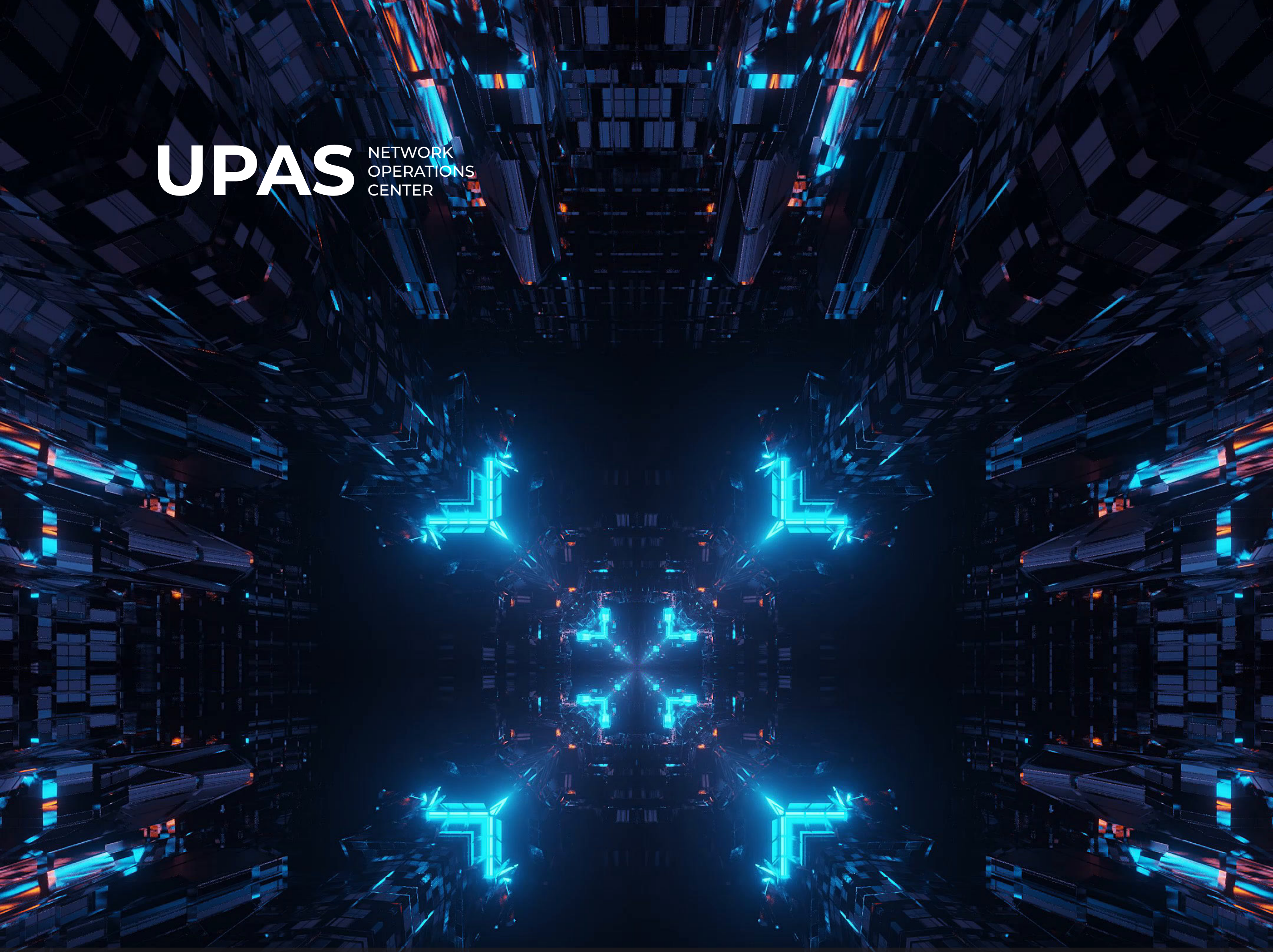
UPAS NETWORK OPERATIONS CENTER



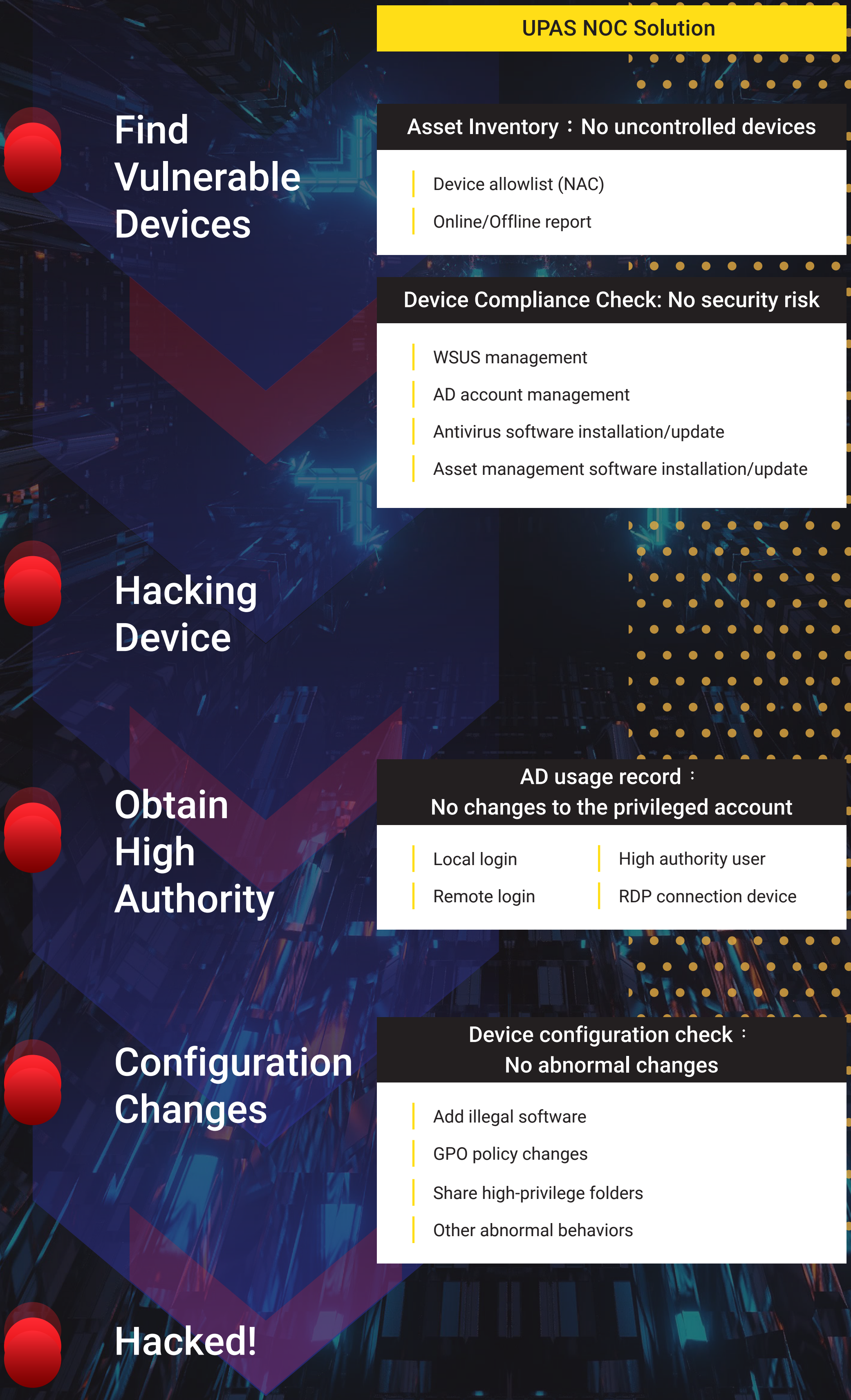
Defense against Ransomware

UPAS NOC

Build the zero trust defense network

UPAS NOC is comprehensive in terms of intranet management, many of its functions can effectively block ransomware from the intranet. UPAS NOC uses the zero trust architecture to minimize the impact of security vulnerabilities, and can instantly detect abnormal events in multiple links when hackers launch targeted invasion.

Facing Ransomware and Hackers
How **UPAS NOC**
Defense against Ransomware



UPAS NOC Solution

Find Vulnerable Devices

Asset Inventory：No uncontrolled devices

- Device allowlist (NAC)
- Online/Offline report

Device Compliance Check: No security risk

- WSUS management
- AD account management
- Antivirus software installation/update
- Asset management software installation/update

Hacking Device

Obtain High Authority

AD usage record：
No changes to the privileged account

- Local login
- Remote login
- High authority user
- RDP connection device

Configuration Changes

Device configuration check：
No abnormal changes

- Add illegal software
- GPO policy changes
- Share high-privilege folders
- Other abnormal behaviors

Hacked!

Comprehensive asset inventory 98% Highest management rate in the industry

Asset management is the source of all information security, and the safest intranet environment can only be achieved when all connected devices are managed. UPAS can achieve the highest 98% device management rate in the industry, manage all equipment on the intranet, and use this as the cornerstone to add a unique device allowlist and compliance check to find the weak device to achieve continuous defense and management so that ransomware can't take advantage.

Integrate multiple servers No blind spots in the device compliance checks

In the past, device compliance checks always had difficulties that were difficult to overcome. Due to the unclear number and status of devices, it was impossible to efficiently confirm whether the device was updated to the latest version. UPAS solved this problem with a 98% device management rate.

The asset list and device status chart show in detail the system and version used by the devices in the intranet. At the same time, it can be integrated with the WSUS server to find out if the latest version should be updated and force the device to update.

UPAS's patch management can also install and update antivirus software and asset management software, ensuring that the virus signature is maintained at the latest version. It can also check whether the permit software is installed correctly, whether illegal or pirated software is installed, and reduce the occurrence of information security events caused by using pirated software.

Online/Offline report Overview of intranet devices

UPAS can produce the online/offline information report of computer equipment, allowing managers to understand the status of the devices through the content of the report. In addition to the online/offline reports, 55 other reports and 198 analysis items are provided to help managers better understand the status of intranet devices.

- *The device has not been turned on for a long time:* OS Patch, anti-virus software, and virus signature have not been updated causing security vulnerabilities.
- *Turn on during abnormal hours:* It may become the target of hackers.
- *Devices abnormal power on/off alarm:* Abnormal activities such as the installation of malicious programs can be monitored.

AD management Complete the minimum authority account management

The control of local accounts is a very important thing for the defense of ransomware. Account management with minimum authority can prevent hackers from damaging the intranet through the permissions of local accounts.

UPAS's AD management can restrict users to only log in with AD accounts and cannot log in with local accounts, preventing hackers from installing malicious software to harm the intranet. At the same time, it provides AD login/logout time records to manage idle devices in the intranet or devices connected using RDP to reduce the chance of being attacked by hackers.

Configuration check Alert in time·Defend in time

When the hacker has obtained permission and wants to send ransomware to devices, UPAS can alert the abnormal behavior of the configuration in time, such as adding illegal software, changing the GPO policy, opening the highest-privileged folder sharing, etc., so that the enterprise can timely prevent the installation and operation of software and reduce the amount of loss.