IPScan® NAC

Network Access Control

User
Authorization

Analyses &
Report

PC Integrity
Status Inspection

NETWORK
ACCESS
CONTROL

Monitoring &
Alarm

Vaccine Information
Collection

Policy-based
Real Time Control

VIASCOPE

OVERVIEW

IPScan® NAC

IPScan NAC provides network surveillance and performs ongoing compliance checks to ensure that all connected devices are automatically identified, classified, authorized, and given policy-based access control. It also provides all the major features that network managers expect, such as NAC-driven IP Address Management (IPAM), Desktop Configuration Management, complete security control over Wi-Fi access, automated IT security operation, IT asset management, and much more.

Network Access Control

- User Authentication
- IPAM, DHCP Server
- Switch Port Control
- Control NIC and AP

Correlated Information

- Network Node
- IP/MAC Address
- OS detection
- Wireless Access

Asset Management

- Control the use of illegal S/W
- Comply with security policy
- Security patches

Features

Site-defined Network Access Control

Centralized Management for All Network End-point

Security & Compliance

Various Analyses & Report Support

S/W Integrity

- Administrator-defined integrity status inspection
- Administrator-defined latest update status inspection

OS Patch/Service Pack

- Security patch auto-apply
- Latest version of OS patch/ service pack apply

Block S/W

- Block target S/W installed or running check
- A specific version or all version of the same S/W check support

Others

- Remote access block
- IP Change Block
- Screen saver enable and other security policy

Visibility. Control. Response.
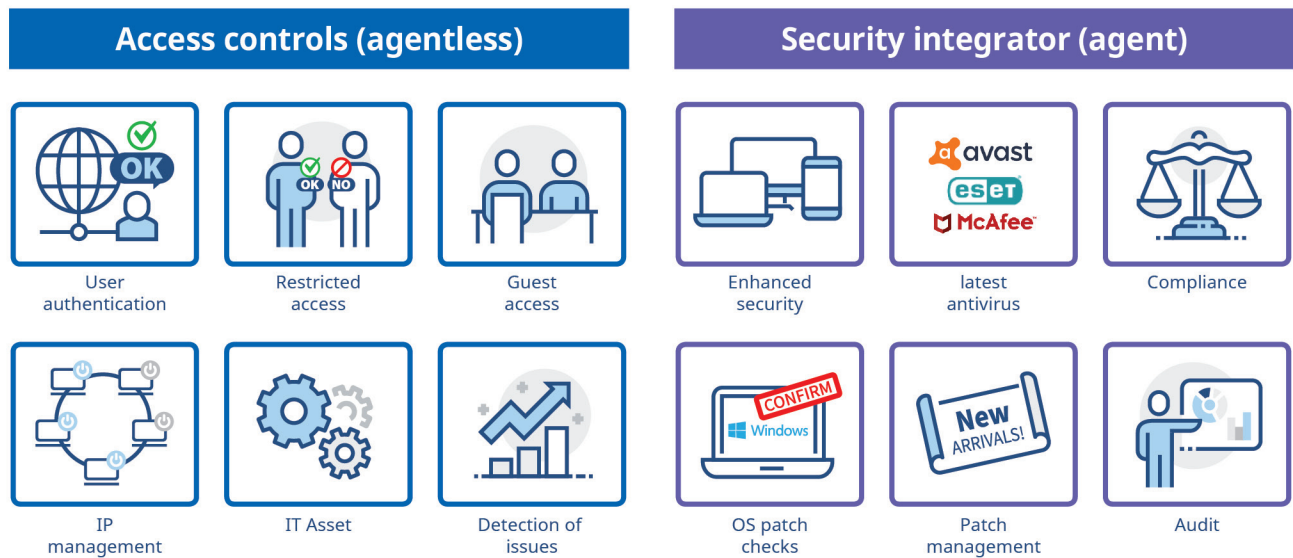*Secure your network without changing it*

THE CONCEPT

Gartner® ►

NAC : Network Access Control

A network access control (NAC) process adds policies to the network for controlling access by devices and users. Policies may be based on device and/or user authentication and the status of endpoint configuration.
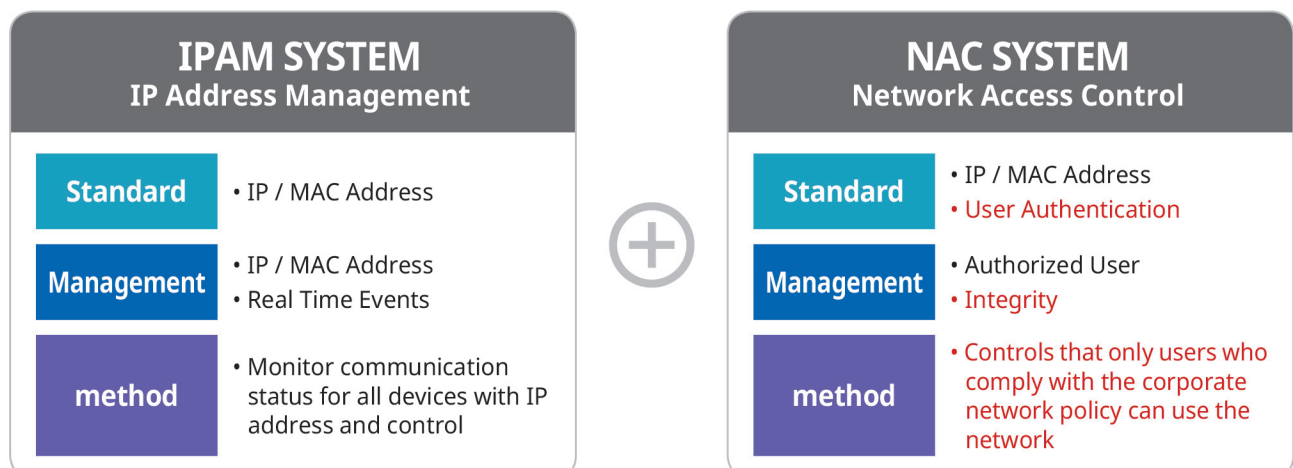
Access controls (agentless)			Security integrator (agent)		
User authentication	Restricted access	Guest access	Enhanced security	latest antivirus	Compliance
IP management	IT Asset	Detection of issues	OS patch checks	Patch management	Audit

IPAM vs. NAC

### Minimize security threats from all devices connected to the network

Main Purpose	Network asset management	**Main Purpose**	Checking reliability of network users Policy compliance real-time management

IPAM SYSTEM
IP Address Management

Standard	• IP / MAC Address
Management	• IP / MAC Address • Real Time Events
method	• Monitor communication status for all devices with IP address and control

⊕

NAC SYSTEM
Network Access Control

| Standard	• IP / MAC Address • User Authentication
Management	• Authorized User • Integrity
method	• Controls that only users who comply with the corporate network policy can use the network

MAJOR FUNCTIONS

Required/Malignant S/W Management

- According to administrator's setting, IPScan NAC can check the installed and running status of Mandatory / Malware software.

- If the software installed/running status is detected by Mandatory / Malware S/W Policy, the network of PC will be blocked.
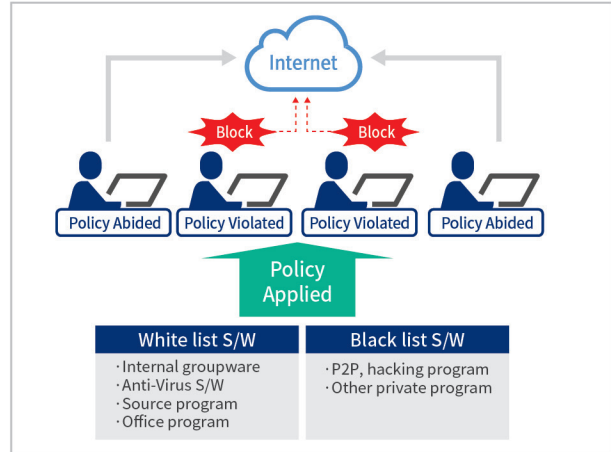
Detouring Communication and Security Setting Inspection

* Block/Control network immediately when exceptional behavior detected.
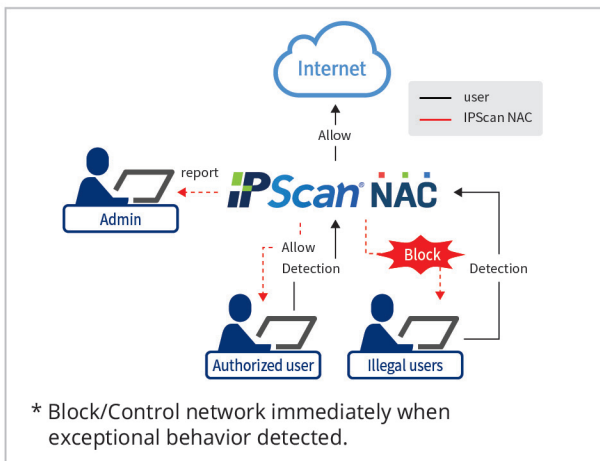
- IPScan can detect and block the end-point device who violated internal network policy and attempted to use detouring communication.

- IF detouring communication attempt is detected, the user's network will be blocked.

Real-time Network Usage Status

Real-time Status

- Real-time IP usage graph GUI
- General IP conflict event monitoring

Warning/Block Status

- Warning Status: shows the status of hosts violated warning policy.
- Block Status: shows the status of hosts violated block policy.

Setting/Exception Status

- Setting Status: shows the status of hosts applied specified policy on.
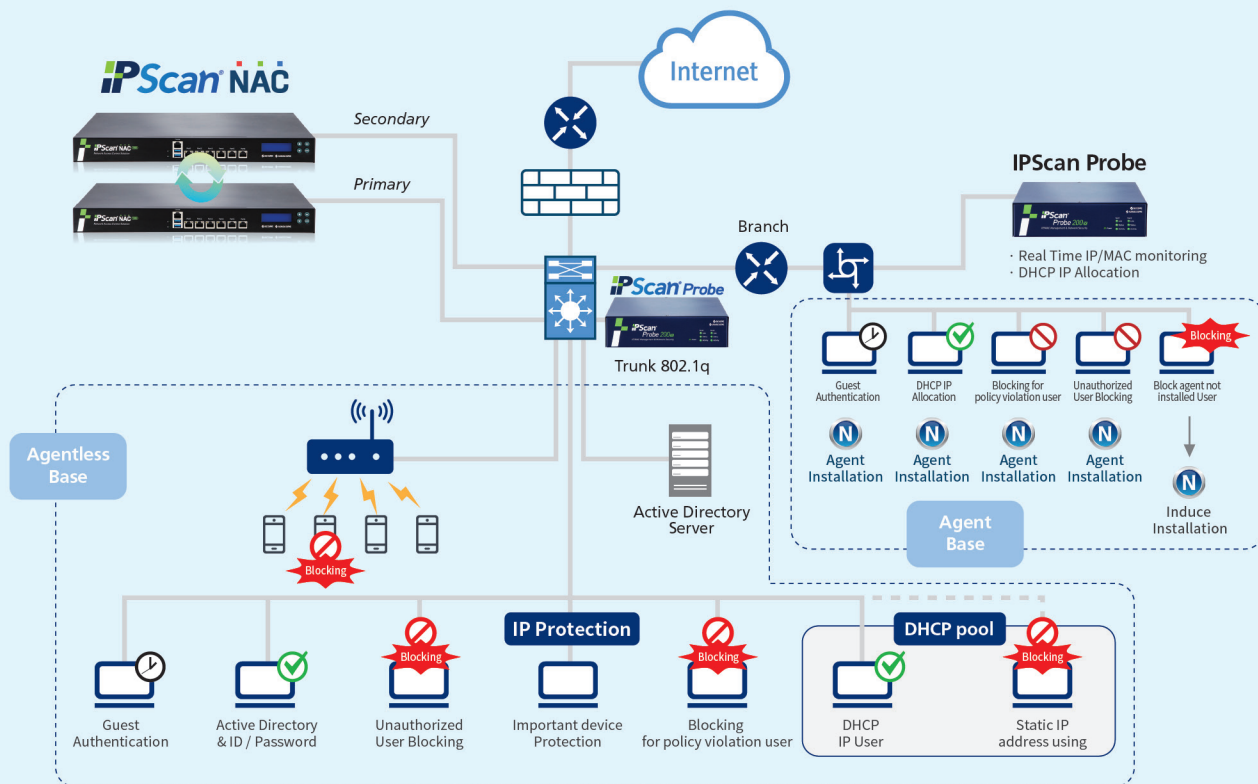- Exception Status: shows the status of hosts under Network Block Exception policy.

General/Assets Status

- General Status: shows the status of authorized/unauthorized hosts, host type and unused hosts.
- Asset Status: shows the status of IP asset and host OS in each IP range.
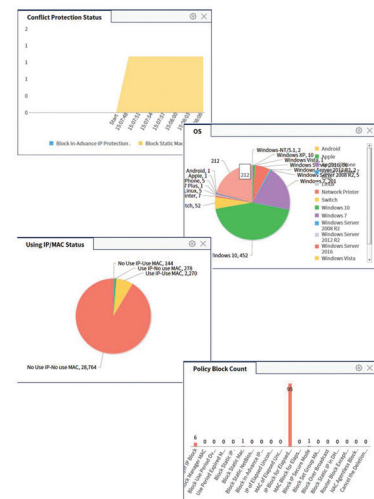
NETWORK CONFIGURATIONS

Easy to control network access by mixed agent and agentless method

IPScan NAC Specifications

	IPScan NAC1000 Plus	IPScan NAC 2000 Plus	IPScan NAC 10000 Plus
image			
CPU	Intel® Pentium® Gold G5400 3.7GHz (2Core)	Xeon® E-2124G 3.4GHz (4Core)	Xeon® Gold 6128 3.4GHz (6Core) * 2
MEMORY	16GB	32GB	128GB
Recommended Active IP	1,000	2,000	10,000
Interface	2 x RJ-45 (Ethernet 10/100/1000Mbps) Ports	2 x RJ-45 (Ethernet 10/100/1000Mbps) Ports 2 x SFP(1G) Module Slots	2 x RJ-45 (Ethernet 10/100/1000Mbps) Ports 2 x SFP(1G) Module Slots 4 x SFP+(10G) Module Slots
Console	1 x RJ45 (to RS-232) Console Port 2 x USB 3.0	1 x RJ45 (to RS-232) Console Port 2 x USB 3.0	1 x RJ45 (to RS-232) Console Port 2 x USB 3.0
Size (mm)	430 (W) x 44 (H) x 330 (D)	430 (W) x 88 (H) x 330 (D)	444 (W) x 88 (H) x 580 (D)
Weight	5.0Kg	10.0Kg	20.0Kg
Power	300W	460W Redundant	600W Redundant
Input Voltage	AC 100 ~ 240V, 50 ~ 60Hz	AC 100 ~ 240V, 50 ~ 60Hz	AC 100 ~ 240V, 50 ~ 60Hz

* Above H/W specifications are subject to change without notice.

IPScan® NAC