TiFRONT AP

Access Point

Network visibility

Wireless network security

Easy management on Cloud

PIOLINK

TiFRONT AP

WiFi and security at one time. Easy management in the cloud

PIOLINK TiFRONT AP is a wireless access point that can be managed from the cloud and web while providing security and visibility.
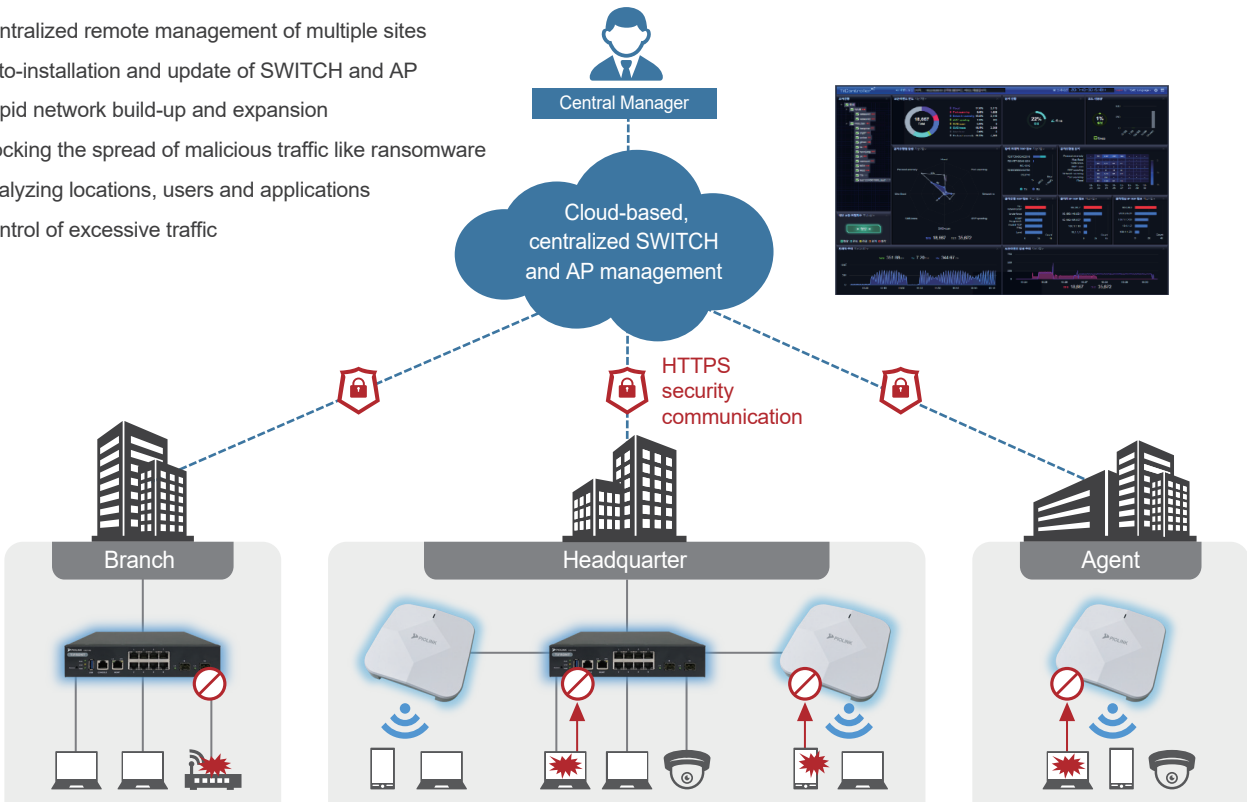
It has the high level of visibility (e.g. showing where multiple AP is installed, the range and rate of each WiFi signal, connected equipment types, and traffic volumes) and blocks various security threats on the wireless network.

We suggest configuring it with TiFRONT SWITCH for simpler management, which will allow the integrated management of wired/wireless networks of various sites on a single screen along with security and visibility.

Security

Visibility
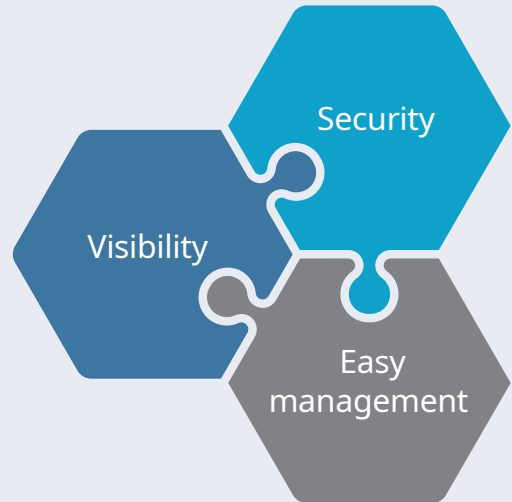
Easy management

Deployment of Cloud-based TiFRONT wired/wireless networks

· Centralized remote management of multiple sites

· Auto-installation and update of SWITCH and AP

· Rapid network build-up and expansion

· Blocking the spread of malicious traffic like ransomware

· Analyzing locations, users and applications

· Control of excessive traffic

Central Manager

Cloud-based, centralized SWITCH and AP management

HTTPS security communication

Branch

Headquarter

Agent

Wireless security

Blocking the spread of malicious traffic like ransomware

It blocks the internal spread of malicious traffic like ransomware via the wireless network. As malicious traffic only is blocked, business continuity can be maintained.
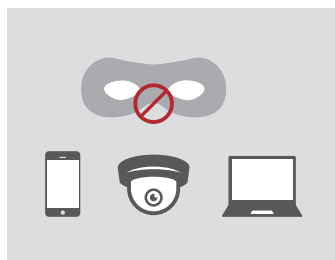
Blocking the leakage of call/video/PC screen

Critical information is protected by blocking APR spoofing attack, which intercepts packets like VOIP phone-call, IP camera video, user PC screen, etc. in the middle of communication.
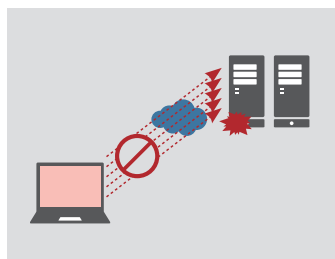
Blocking the source of DoS attack

By blocking a large amount of abnormal traffic from the user terminal to the outside, it protects the internal network and prevents DoS attacks on the external attack.
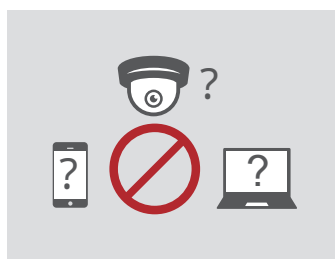
Access control of unauthorized devices and NAT equipment

It automatically identifies access devices. It blocks the WiFi access of unauthorized devices, forged/falsified IP/MAC and NAT equipment.
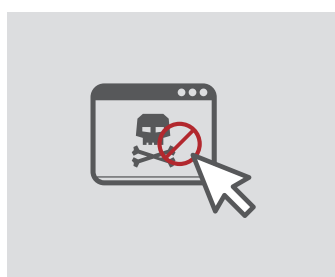
Access control of malicious/ unauthorized sites

It blocks the access of malicious sites by analyzing the domains accessed by users.


High-performance security engine, TiMatrix

· PIOLINK's Engine dedicated to access network security
· Its own security algorithm based on Frequency Matix
· Auto-selecting and blocking malicious traffic without manager intervention
· Responding to Zero Day threat without signature
· Maintaining maximum line performance while performing security functions

Outstanding visibility
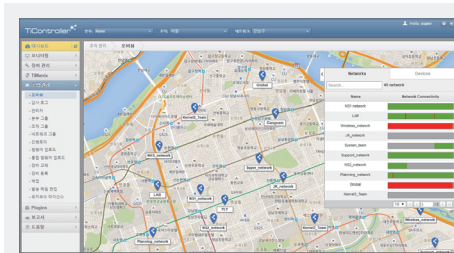
Analyzing AP location and access

Marking AP location on a map and showing analysis indicators such as users who access each AP, access devices, access time, re-access time, etc.
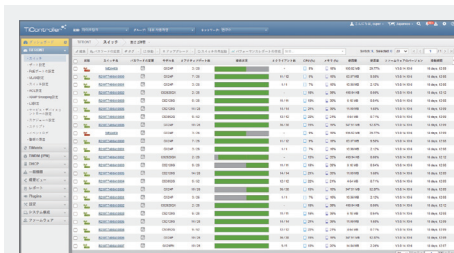
### Identifying applications and analyzing traffic

It can analyze the usage of each application and designate its use priority. It can identify and manage those using excessive traffic which reduces WiFi rate.
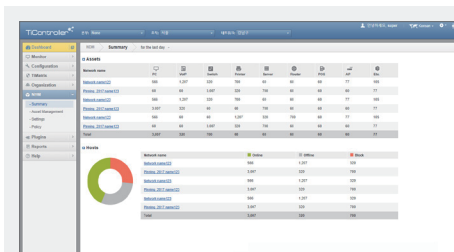
Connection terminal analysis

It collects and classifies OUI data and MAC addresses by matching them with asset types. It can identify unauthorized devices and improve security by managing networks by group

Easy management
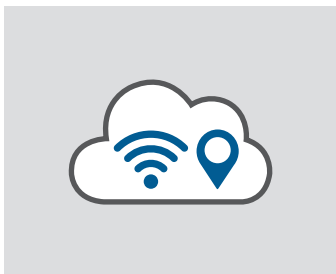
Quick and easy build-up/scalability/ movement of networks

It is automatically installed when AP is connected to the Internet without complicated setup (Zero Touch Installation.) Its multiple network management function allows the quick and easy build-up, expansion, or movement of dispersed areas/large-scale networks.

Intuitive interface and single management system

It reduces the time and costs spent in network configuration/ management / maintenance through an intuitive interface (a few clicks required only) and the integration of NMS, QoS, ESM and NAC functions and automated management on cloud

Auto-issuance of security reports

It issues the periodic reports about security events such as the status of attack detection, the distribution of each attack, number of occurrence, attacker IP, and equipment targeted.

TiFRONT-CA1002C

Product Specification	
Performance	802.11a/b/g/n/ac wireless LAN standard
	5G 2x2 867Mbps + 2.4G 2x2 300Mbps
	up to 128 connective users, 64 users per frequency band
Hardware	flash memory: 128MB
	DRAM: 256MB
Interface	1-port 10/100/1000BASE-T
	1-port RJ-45 connector
	reset button, factory button
	built-in ×2, 2T2R antennas
	1×4 color (red, orange,green, blue)
Power	100~240VAC, 50/60Hz
	power consumption: 12W
	PoE: 36VDC~57VDC
Environmental	0℃ to 50℃
	20% to 90% (non-condensing)
	-30℃ to 80℃
Mechanical	170(W) x 40(H) x 170(D)mm
	weight: under 400g
Antenna Gain	5dBi PIFA antenna
	6dBi PIFA antenna

Key Functions	
VLAN	802.1Q
Network Capability	DHCP server/client
	TCP/IP
	auto channel selection
	PPPoE
	static IP
	NAT
QoS	traffic scheduling (SP, RR, WRR, WDRR)
	traffic shaping
Security	IP, MAC, port number
	ARP spoofing detect
	[Flood] TCP syn, TCP ack, ICMP, ARP detect
	[Network scanning] TCP, UDP, ICMP, non-echo-ICMP, ARP detect
	[Port scanning] TCP syn, TCP ack, UDP, stealth detect
	SMB scan, SMB trace detect
Authentication	802.1x supplicant
	RADIUS
	WPA PSK/WPA2 PSK
	WPA/WPA2 PSK mixed mode
	WPA/WPA2 enterprise
Management	event logging
	firmware upgrade
	SNMP v1/v2c/v3
	NTP

PIOLINK is specialized in network and security.
We ensure the industry's best application availability and performance and
own unrivaled technologies and leadership in this intelligent,
advanced IT environment by offering the build-up of Cloud infrastructure,
the easy management of networks and data protection.
Our flagship products are Application Delivery Controller (ADC)
having Korea's No.1 market share, Web Application Firewall (WAF/WAAP),
Cloud Managed Networking and Hyper Converged Infrastructure and services,
Managed Security Service (MSS or MSSProvider)and Security Consulting.

PIOLINK

M2-B07