좀비PC 및 APT공격 차단, UC/IPT 구축, 유/무선 트래픽 보안

# TiFRONT

## 액세스 네트워크 보안 솔루션


PIOLINK

# 좀비PC로 인한 **보안사고**

## DDoS 공격, 금융망 마비, 개인정보 및 기업기밀 유출 등

7.7 DDoS공격, 3.3 DDoS공격, 은행 전산망 마비 및 대형 포털 사이트
개인정보 유출 등은 악성코드에 감염된 좀비PC에 의해 발생한 사고였습니다.


# **TiFRONT**로 **해결**할 수 있습니다

## 파이오링크 액세스 네트워크 보안 솔루션

파이오링크는 악성코드 탐지에서 차단까지 모든 단계를 네트워크에서 처리하는
TiFRONT 솔루션을 제공하고 있습니다. PC마다 별도 에이전트를 설치하는 번거로움 없이
간편한 구성으로 개인정보, 기업 자산 유출 및 DDoS 발생 피해를 막을 수 있습니다.

**TiFRONT-보안스위치**

악성코드/유해트래픽 차단

+

**TiFRONT-안티봇**

봇넷 자동탐지/분석

=

좀비PC 방지 솔루션
**안전한**
**네트워크 구축**

# TiFRONT-보안스위치

날로 증가하는 보안 위협에 안전하게 대응하기 위해서는 외부 공격뿐 아니라 내부 네트워크의 출발점이 되는 액세스 네트워크의 보안 대책이 동시에 수립되어야 합니다. 이를 위한 가장 효율적인 솔루션으로 L2 스위칭과 보안 기능을 동시에 제공하는 보안 스위치가 있습니다. 파이오링크 TiFRONT-보안스위치는 액세스 네트워크에 대한 보안과제에 완벽히 대응합니다.

## ARP spoofing 방지

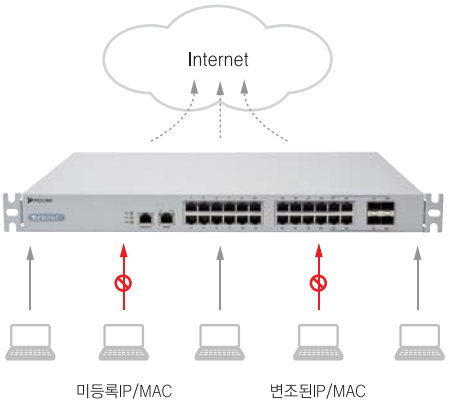
**계정정보탈취, 통화도청으로부터 안전한 네트워크**

포트 단위로 세밀히 판단하기 때문에 공격자와
변조된 MAC 피해자를 구별하여, 공격자만 차단합니다.
TiFRONT-보안스위치로 UC환경에서의 통화도청,
사생활 노출 및 정보탈취 등의 위협으로부터
안전한 네트워크를 구성할 수 있습니다.


## 사용자/IP 강력 접근통제

**비인가 단말로부터 악성코드 및 바이러스 유입 차단**

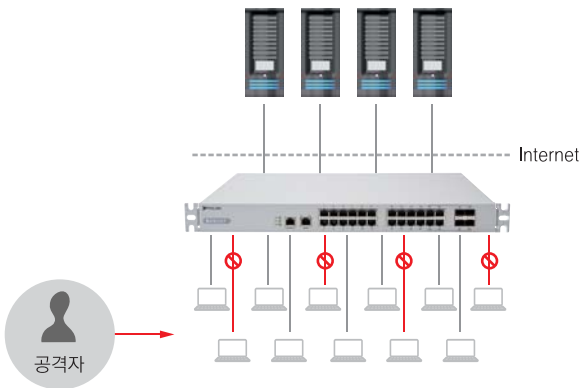
TiFRONT-보안스위치는 IP/MAC 기반의 강력한 접속 제어와
IP자원 관리, 단말의 접속상태 및 이력을 확인할 수 있습니다.
또한 802.1x 기반의 인증서버와 연동 가능하여, 비인가된 단말의
네트워크 접속을 제어할 수 있습니다.




## 유/무선 유해 트래픽 확산 차단

**트래픽 과부화로 인한 속도 저하, 시스템 마비 방어**

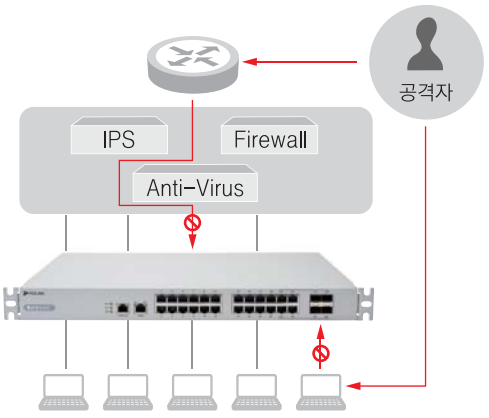
TCP SYN flooding, UDP flooding, ARP flooding 등
액세스 네트워크를 통과하는 각종 유해 트래픽으로부터
네트워크 자원을 안전하게 보호합니다. 유해 트래픽이
보안스위치에 감지되면 자동으로 공격트래픽만 차단하게 되므로,
항상 안정적인 서비스 상태를 유지할 수 있습니다.




## APT공격, 악성코드 차단

**각종 해킹, 좀비PC로 인한 중요 정보 탈취 보호**

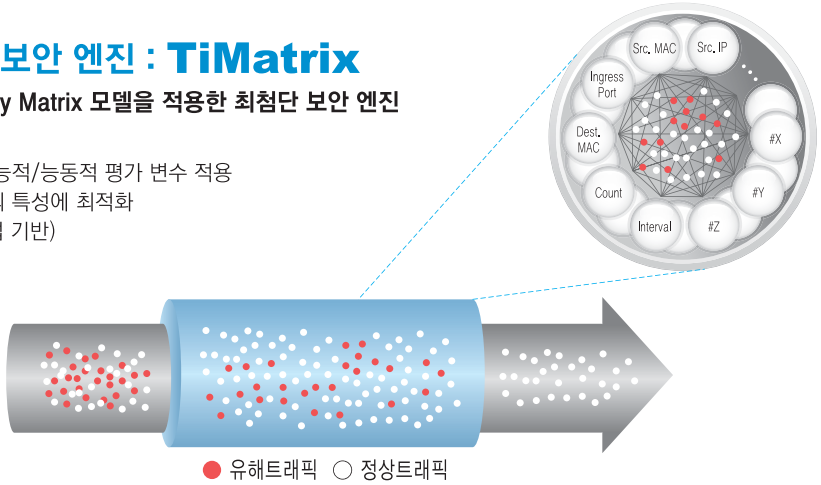
표적형 지속공격이라 불리는 APT(Advanced Persistent Threat) 공격은
특정 사이트에 보안위협을 오랫동안 지속적으로 가하는 행위로,
최근 은행전산망 마비나 포털사이트 이용자계정 유출사건과 같은
방식입니다. TiFRONT-AntiBot과 구성 시, 고성능 커널레벨
행위분석으로 알려지지 않은 악성코드 탐지율을 높일 수 있습니다.



## 파이오링크만의 최첨단 스마트 보안 엔진 : TiMatrix

**패킷의 정확한 위험도 예측을 위해 Frequency Matrix 모델을 적용한 최첨단 보안 엔진**

- 유해트래픽 종류 및 보안 위협별 특성에 맞는 지능적/능동적 평가 변수 적용
- 변수 값의 부재가 빈번한 액세스 네트워크 패킷의 특성에 최적화
  (미래 위험 예측성능 높은 Frequency Matrix 기법 기반)
- 여러 변수에 대한 트래픽별 조합으로 자동 검출
- DoS 공격발생 감지 및 자동대응




## 네트워크 가용성 유지

**Port Redundancy**

- 비관리형 (STP 미지원) 스위치와 연결 시, 랜케이블을 이중화 구성
- 한 케이블에 장애가 생기면, 나머지 한개가 Active되면서 네트워크 중단 예방
- 무중단-무장애 실현으로 네트워크 가용성 유지

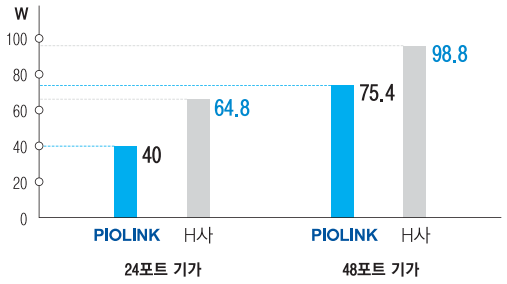

## 네트워크 안정성 보장

**Self-loop 방지**

- ARP broadcasting을 기반으로, 네트워크의 loop 상태에 대한 주기적인 점검을 통해 보다 안정적인 서비스 보장
- loop 방지를 점검하는 패킷이 네트워크 리소스에 부담을 주지 않으며, loop현상에 대한 정확한 탐지율 보장


## RoHS 규정 준수 및 저전력

파이오링크는 TiFRONT-보안스위치 및 모든 제품 제조시,
RoHS 규정을 준수하며 유해물질 사용을 제한한 부품만 사용합니다.
또한 TiFRONT-보안스위치는 타사 동급 모델 대비 사용전력이 낮습니다.




# **TiManager** : 통합 관리 시스템

스위치 + 사용자IP
동시 통합 관리

그룹 및 개별
보안정책 설정

1,000대 이상
스위치 동시 관리

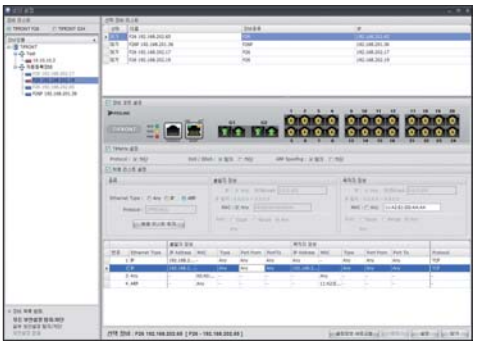
안티봇 연동으로
좀비PC 차단

## 실시간 모니터링

실시간 트래픽, 보안침해 상태뿐 아니라 보안스위치, 사용자 IP 현황을 TiManager로 한눈에 파악할 수 있습니다. 보안로그, 장비상태 로그 및 네트워크 구성상태 등을 실시간 확인할 수 있습니다.

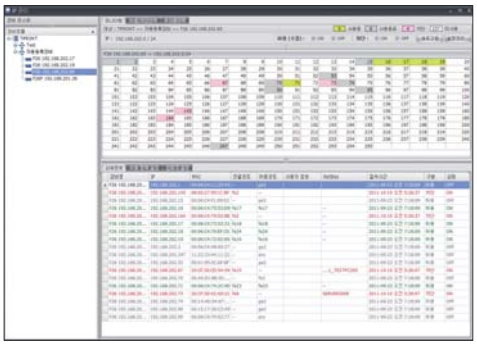
## 세밀한 보안 설정

TiFRONT-보안스위치에 개별 · 그룹별 보안 정책 설정을 내릴 수 있습니다. 포트별 보안정책 설정으로 사용하는 IP/MAC 포트를 지정하여 사용시간을 제한하거나 접속을 허용 · 차단할 수 있습니다.



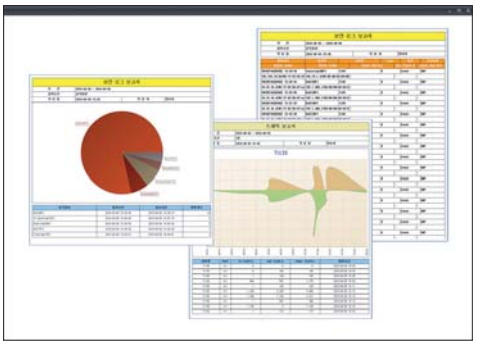
## 사용자 IP 관리

어느 보안스위치의 몇 번 포트에 어떤 IP로 누가 언제 사용했는지 실시간 파악 할 수 있습니다. IP/MAC기반 사용자 인증으로 IP자원 관리 및 단말의 접속 통제 및 이력 조회가 가능합니다.



## 다양한 리포트

보안스위치와 등록된 IP정보에 대한 보고서를 발행합니다.
수십~수백대의 스위치와 각 포트에 연결된 IP 정보를 트래픽 상태, 보안상태,장비상태 등의 보고서로 출력 가능합니다.



**TiManager 최소 서버 사양**

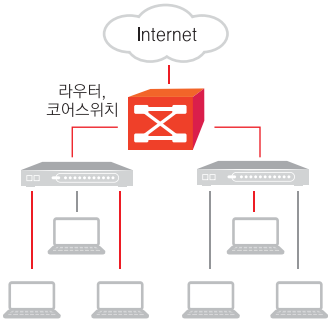
| | | | |
|---|---|---|---|
| C P U | Intel® Core™ i5 2.X이상 | O S | Windows XP 이상, Windows Server 2003/2008 |
| R A M | 3GB 이상 | D B M S | PostgreSQL 9.0.2 이상 |
| H D D | 200MB 이상 | | |

# 구축사례

액세스
보안 & 안전성

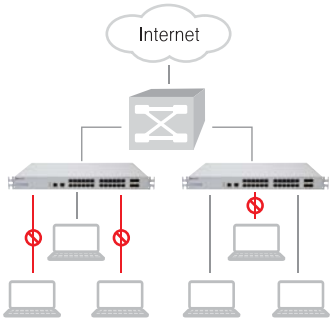
## 피씨방 유해트래픽 차단 및 네트워크 안정화

불특정 다수가 사용하는 PC방은 액세스 네트워크에서 발생되는 다양한 공격에 취약하고 장애도 빈번히 발생합니다.
TiFRONT-보안스위치 도입 후, 상위 네트워크로 유입되는 유해 트래픽 양이 현저히 감소하고,
트래픽 과부하로 인한 CPU Load도 낮아졌습니다. DDoS, Flooding, Scanning 공격 역시 차단되었습니다.




| 도입전 | 구 분 | 도입후 |
|---|---|---|
| 287 | DHCP Deny | 0 |
| 13 | Dest MAC Failures | 0 |
| 540 | IP Validation Failures | 128 |
| 71% | CPU Load | 5% |

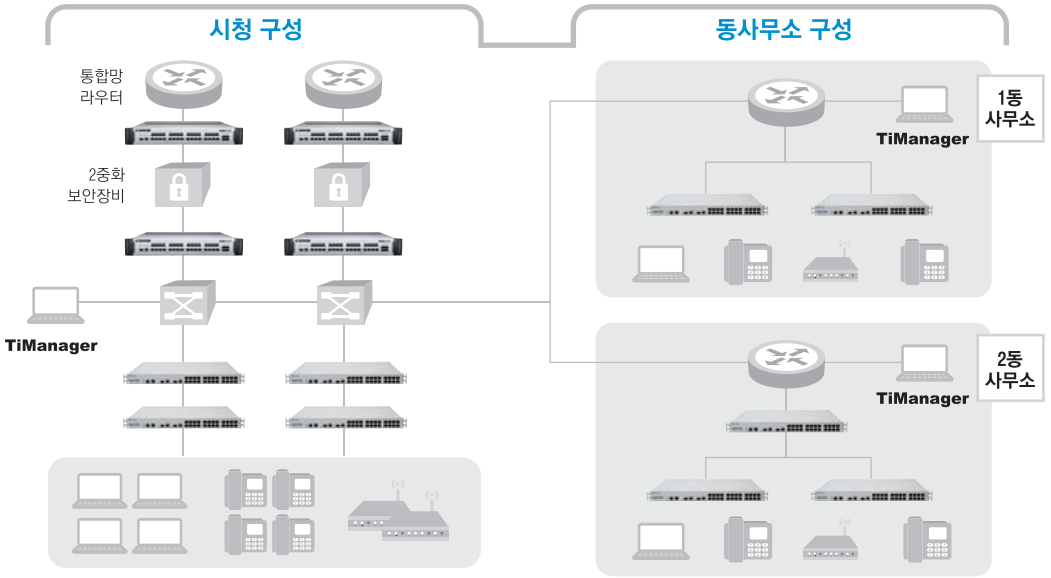
분석기간 : 2010. 10. 27 ~ 11. 19




비용절감 &
관리용이

## 시청과 읍/면/동사무소 IPT망 구축사업

시청과 동사무소들을 연결하는 IPT 구축 사업으로 070전화, 유/무선 AP 등을 위해 PoE 기능이 있는
TiFRONT-보안스위치로 구축하였습니다. PoE 모델로 별도의 전원 공급 장치 설치 없이 전원과 데이터를 동시
전송 가능하고, 통합보안관제 시스템 TiManager로 시청과 동사무소의 통합 또는 개별 보안 관리가 가능해졌습니다.




대규모 환경
동시 관리

## 교육청과 산하 교육기관의 대규모 네트워크 연결

마스터 관리 시스템 TiManager 하나로 전국 시/도/구에 설치된 1000대 이상의 TiFRONT-보안스위치를
동시에 관리 할 수 있습니다. 또한 학교 자체적으로 층별, 교실별 보안 정책을 별도 설정할 수 있습니다.

# 제품사양

| 구분 | TiFRONT-F26 | TiFRONT-F26P | TiFRONT-G24 | TiFRONT-G24P | TiFRONT-G48 | TiFRONT-G48P |
|---|---|---|---|---|---|---|
| |  | |  | |  | |
| 메모리 | Flash : 160MB (OS 32MB, Log Buffer 128MB)<br>Main memory : 512MB SDRAM | | | | Flash : 160MB<br>(OS 32MB, Log Buffer 128MB)<br>Main memory : 1GB SDRAM | |
| 포트 | 24 x 10/100Base-TX port<br>2 x 1G Dual media combo port : Copper & Fiber | | 24 x 10/100/1000Base-TX port<br>(4 x combo port included: 1000BASE-X SFP) | | 48 x 10/100/1000Base-TX port<br>(4 x combo port included: 1000BASE-X SFP) | |
| 입력전원 | 100~240VAC, 50/60Hz (Free Voltage) | | | | | |
| PoE | N/A | IEEE802.3af<br>IEEE802.3at | N/A | IEEE802.3af<br>IEEE802.3at | N/A | IEEE802.3af<br>IEEE802.3at |
| 전원 이중화 | Optional | Optional | Optional | Optional | Optional | Optional |
| 최대 소비전력 | 24.3W (Single)<br>24.9W (Dual) | 35.6W (Single)<br>41.1W (Dual) | 40W (Single)<br>41.1W (Dual) | 41.8W (Single)<br>42W (Dual) | 75.4W (Single)<br>75.2W (Dual) | 96W (Single)<br>110W (Dual) |
| 크기 (WxDxH, mm) | 440x350x44 (WxDxH, mm, 19" 1U) | | | | | 440x470x44 (19" 1U) |
| 무게 | 4.1Kg (Single)<br>4.2Kg (Dual) | 4.5Kg (Single)<br>5Kg (Dual) | 4.1Kg (Single)<br>4.25Kg (Dual) | 4.75Kg (Single)<br>5.25Kg (Dual) | 4.3Kg (Single)<br>4.6Kg (Dual) | 6.1Kg (Single)<br>7Kg (Dual) |
| EMC 인증 | KCC (Class A) | | | | | |
| 보안인증 | CC (EAL2) | | | | | |
| IPv6 | IPv6 ready logo (Phase-II) | | | | | |

# 주요기능

| L2 | |
|---|---|
| Port Management | Autonego/Speed/duplex |
| | Flow control |
| VLAN | Broadcasting Domain |
| | Port-based/Protocol/MAC/Voice/Subnet VLAN |
| | Tagging/Untagging |
| | Hybrid VLAN |
| | Max VLAN (4K) |
| | Ingress/Egress tagging |
| Spanning Tree | STP, RSTP, MSTP, PvSTP, PvRSTP+ |
| MAC learning | MAC address aging |
| | MAC filtering |
| | Duplicate MAC address learning |
| | Reserve MAC learning 방지 |
| | Static entry support |
| | Independent VLAN learning |
| | Max. MAC entry (16K) |
| Port Mirroring | Port Mirroring |
| Link Aggregation | LACP |
| | Link trunking |
| | LACP load balancing |
| | Trunk groups(8) |
| | Members per group (8) |
| | Static Trunk load balancing |
| | 장애 link에 대한 traffic 절체 |
| IGMP snooping | Join/Leave, Multicast group (1K), v1/v2/v3 |
| QoS | L2, L3, L4 header based classification |
| | QoS marking & Remarking |
| | QoS queuing & scheduling<br>- Cos queue mapping<br>- 8 CoS queues per port<br>- Scheduling by SPQ/WRR/DRR<br>- Drop precedence<br>- Congestion avoidance |
| | Ingress rate-limiting (per port/per flow) |
| | Egress rate-limiting(per port) |
| | Diffserv |
| | Shaping & packet drop policy |
| | Min./Max. BW guarantee |
| | Max. rule (G48: 128, F26/G24: 256) |
| ACL | L2/L3/L4기반 filtering |
| | VLAN ACL |
| | ACL filter naming |
| | Max. rule (G48: 256, F26/G24: 512) |
| PoE | PoE+ 표준 지원 (802.3at) |
| | Port별 enable/disable |
| | Port별 공급전력 우선순위 설정 |
| | PoE 동작현황 모니터링 |
| Jumbo Frame | G48: 12K, F26/G24: 13K |

| L3 | |
|---|---|
| Static routing | Static routing |
| Dynamic routing (Option) | RIP, OSPF, BGF, VRRP |

| 보 안 | |
|---|---|
| DoS/DDoS | One-to-One flooding, Random flooding,<br>IP scanning, Port scanning, IP spoofing,<br>ARP spoofing, MAC flooding, counting & logging |
| | 자동 탐지 차단 및 해지 |
| | Source MAC/IP별 차단 |
| | 탐지 예외설정 |
| Protocol Anomaly | Land attack, Teardrop attack,<br>L4 source port range 이상, same port(sPort/dPort),<br>TCP flag이상, TCP fragments, ICMP fragments,<br>Smurf |
| Authentication | 802.1x, RADIUS, TACACS+ |
| | IP/MAC 기반 인증 및 차단 |
| Port Protection | Storm control |
| | Max MAC 지정 |
| Accounting | Login/Logout 기록 |
| | 명령어 수행 기록 |
| 기타보안 | DHCP filtering |
| | NetBIOS filtering |
| | Self loop detect |
| | System Access security |
| | Web alert |

| 관 리 | |
|---|---|
| SNMP | SNMP v1/v2c/v3 |
| | Public MIB (System, Interface, IP address, UCD, Router(RFC-1213), Protocol(TCP, UDP, SNMP, ICMP), RFC1573 Private Interface MIB) |
| | Private MIB (Learning MAC table, 보안설정) |
| | SNMP Trap (Authentication, Port Link up/down) |
| Shell Interface | Telnet, SSH, Console |
| EMS Interface | SNMP, Syslog, SSH |
| Authentication | RADIUS, TACACS+ |
| User관리 | Password 기반 user login, Login timeout 설정,<br>Multi user, User별 권한, Multi-configure |
| 설정 및 OS관리 | OS update via TFTP |
| | 설정저장 |
| Logging | Syslog server, Monitoring, Log임계치 관리, Log백업,<br>System/Security/Panic log |
| Monitoring | Port statistics, CPU/Memory usage, Fan, Watchdog,<br>Temperature sensor |
| 기타 | DHCP server / Relay<br>LLDP |

# TiFRONT-AntiBot

파이오링크 TiFRONT-AntiBot은 대용량 네트워크에서도 다량의 악성코드를 빠르고 정확하게 탐지/분석합니다.
다수의 가상머신을 활용하는 고성능 커널레벨 행위분석은 알려지지 않은 신종 봇에 대한 탐지 및 대응이 가능하며,
시스템 가상화를 통해 물적, 에너지 비용을 절감할 수 있습니다. 또한 보안스위치 연동으로 에이전트 없이
문제PC를 차단할 수 있습니다.

### Smart 분석

- 악성코드 행위기반의 위협분석
- 고성능 커널레벨의 정확한 분석
- 은닉화 및 가상환경 회피 무력화
- 표적형지속해킹(APT*)공격 대응

### Powerful 라인업

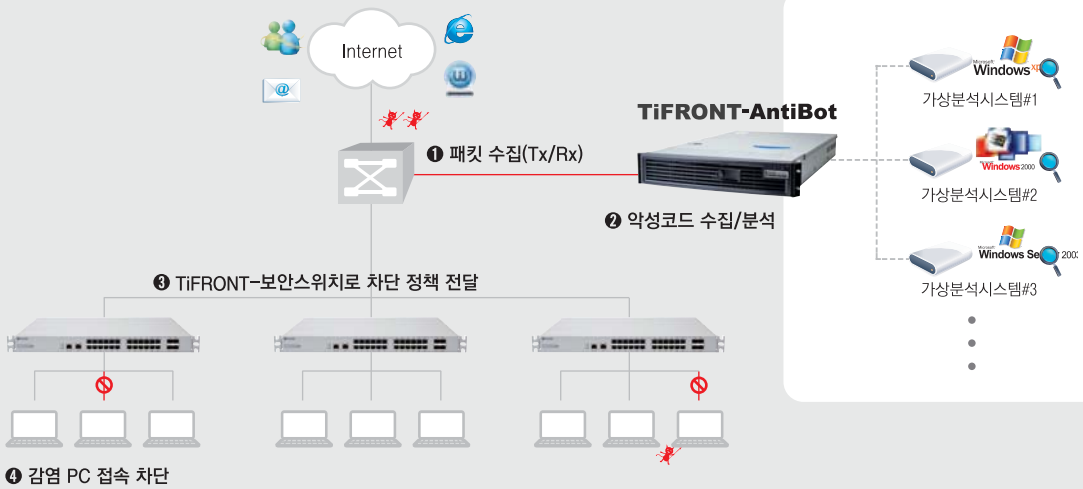
- 1~10Gbps 처리성능 라인업
- 최대 20개 가상머신 동시 분석
- 미러링을 통한 악성코드 수집으로 네트워크 속도 보장

### Agent-less 차단

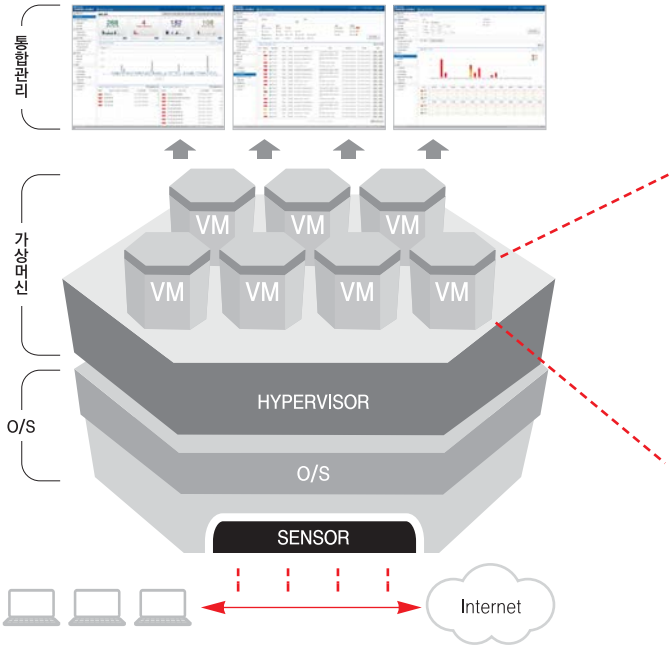
- TiFRONT-보안스위치와 연동하여 PC에 에이전트 설치없이 좀비PC 차단
- 다수의 TiFRONT-보안스위치 동시 차단 제어


* APT(Advanced Persistent Threat)
특정 사이트에 조직적이고 다양한 보안 위협을 지속적으로 가하는 행위로 오랜 기간 공격받더라도 인지 못하는 경우가 많으며 최근 은행 전산망 마비나 포털 사이트 이용자 계정 유출사건도 같은 방식입니다.

## 운영환경



## 적용기술




| 분석목록 | 악성 행위 분석 기준 |
|---|---|
| Process | 프로세스 생성 및 종료, 자식 프로세스 추적, 악성 프로그램 감염 탐지 |
| File | 시스템 파일 생성, 삭제, 변조 행위 탐지 |
| Registry | 시스템 보안 설정 변경, 악성 프로그램 실행관련 레지스트리 변조 탐지 |
| Network | C&C 서버 접속, 블랙리스트 IP/URL 접속, 배포 서버 접속, 악성 프로그램 다운로드 탐지 |

## 제품사양

| 모델 | TiFRONT-AntiBot2000 | TiFRONT-AntiBot4000 | TiFRONT-AntiBot8000 |
|---|---|---|---|
| CPU | Intel Xeon 2.4 Quad x 1 | Intel Xeon 2.4 Quad x 2 | Intel Xeon 2.4 Quad x 2 |
| RAM | 16G | 32G | 64G |
| HDD | 1TB | 1TB | 1TB |
| SSD | 80G | 240G | 500G |
| InterFace | 1G x 2port | 10G x 1port, 1G x 1port | 10G x 1port, 1G x 1port |
| OS | Windows 2008 server R2 Std 64bit | | Windows 2008 server R2 Ent 64bit |
| DB | MS SQL server 2008 R2 | | |
| 가상머신 | 5개 | 10개 | 20개 |

* VM용 클라이언트 라이센스 포함

## 주요기능

| | |
|---|---|
| 악성코드 검사 | 가상머신 행위분석 기반 악성파일 수집 및 자동 검사 |
| 실시간 통합 대시보드 | 검사대상 파일 수집 현황, 악성파일 수, 감염PC, C&C서버 등 실시간 정보 제공<br>트래픽 유입현황 및 분석결과 목록 조회 |
| 사용자 정의 검사 | 사용자 파일 업로드 검사, URL 입력 검사 |
| 다양한 통계/보고 | 탐지추이 분석 및 통계(기간별/발생횟수별/위험도별 분석)<br>악성코드 배포 국가, 포트, C&C서버, 확장자별 통계 분석 (연/월/일 기준 분석)<br>분석 결과 상세정보 제공 및 악성파일 다운로드 |
| 시스템 관리 | 시스템 로그, 시스템 감사<br>분석 행위/범위/종류/대상에 대한 사용자 설정 가능<br>블랙/화이트 리스트 관리, 상세분석 조회, 검색 및 파일 저장 |

## ㈜파이오링크

파이오링크는 애플리케이션 네트워킹 및 웹 보안 전문 기업입니다.
업무의 연속성, 안정성, 보안을 위해 ADC 솔루션(PAS/PAS-K),
웹방화벽 (WEBFRONT), 액세스 네트워크 보안(TiFRONT-보안스위치/안티봇)
등을 제공하며, 최고의 성능으로 IT 투자 비용을 최소화 시킵니다.

### ADC 솔루션

네트워크 가용성, 보안성을 위한 애플리케이션 스위치

PAS-K

PAS

### 웹 애플리케이션 방화벽

비정상적인 웹 트래픽 차단, 웹사이트 안전과 정보보호

WEBFRONT

### 액세스 네트워크 보안

봇넷, 유해트래픽을 탐지·차단하여 좀비PC방지

TiFRONT-SecuritySwitch

TiFRONT-AntiBot

**(주)파이오링크** www.PIOLINK.com

영업문의 **02-2025-6969**

**sales@PIOLINK.com**