

Global
Security
Partner

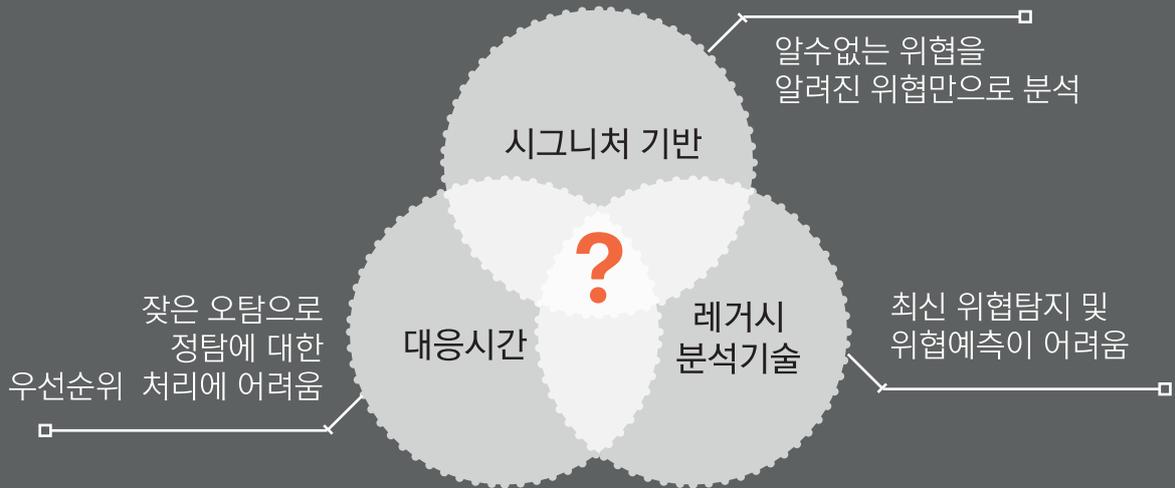
SNIPER ONE-i

지능형 차세대
침입방지시스템

진화하는 사이버 위협

기존 보안솔루션으로

최신 사이버위협에 대응이 어려운 이유는?

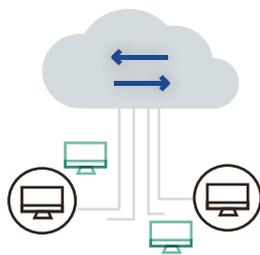


새로운 위협 모델링 분석 기법이 필요



+ 공격자 관점
위협 상황분석

조치 가능한
보안 인텔리전스 확보



+ 네트워크 방어
필수요건

상황인지 분석으로
탐지/차단



+ 효율적인 데이터 제공
+ 위협 가시성 확보

정탐대응에 집중

사이버위협에 대한 능동적 방어

인텔리전트 보안



이상행위 탐지



대응/추적



취약성 탐지



공격성 탐지



악의성 탐지

*인텔리전트 보안 | 조직에서 가용한 모든 정보를 수집, 분석 후 조치 가능한 정보를 도출하는 것

네트워크기반의 위협 트래픽
심층분석 및 상관분석기술로
공격을 방어합니다.

SNIPER ONE-i

SNIPER ONE-i

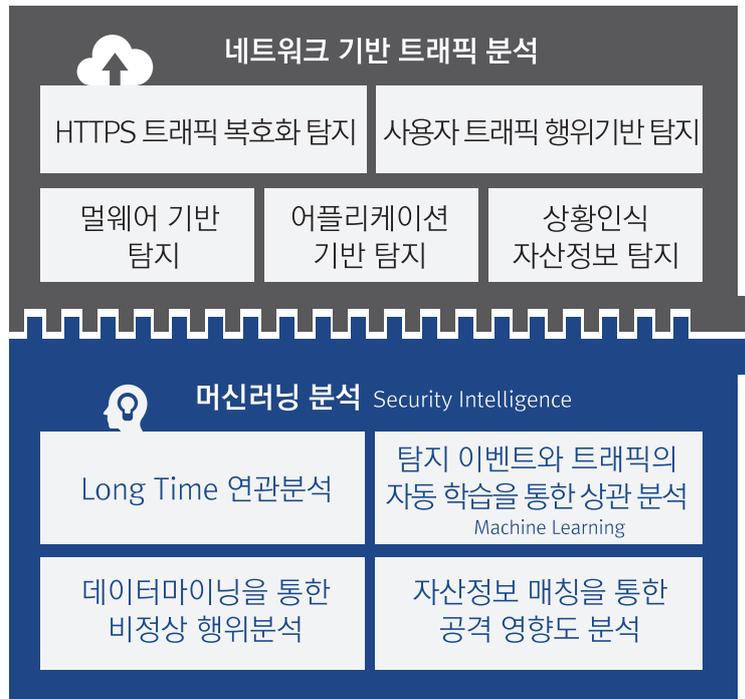
지능형 침입방지시스템

SNIPER ONE-i 는 시스템 및 네트워크 자원에 대한 다양한 형태의 침입 행위를 사용자/멀웨어/어플리케이션 기반 상황인지 엔진과 평판기반으로 실시간 탐지분석/차단을 수행하는 지능형 차세대 침입방지시스템입니다.

SNIPER ONE-i 에 탑재된 다중 보안엔진과 상황인지 엔진은 실시간으로 유입되는 트래픽을 탐지 및 심층 분석하여 비정상 패킷과 세션을 판단하고 차단함으로써 네트워크 자원에 대한 신뢰성과 안정성을 보장합니다.

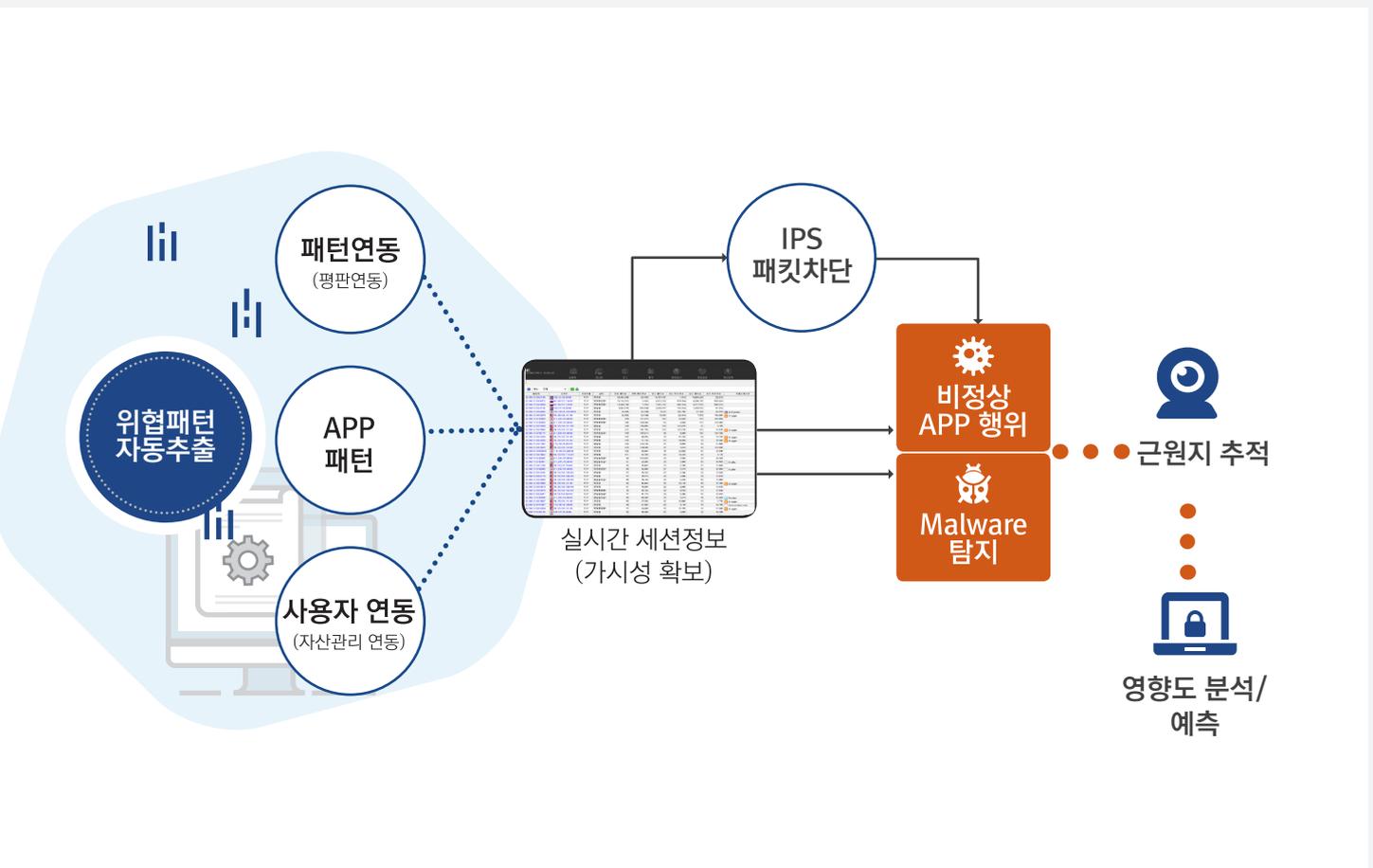
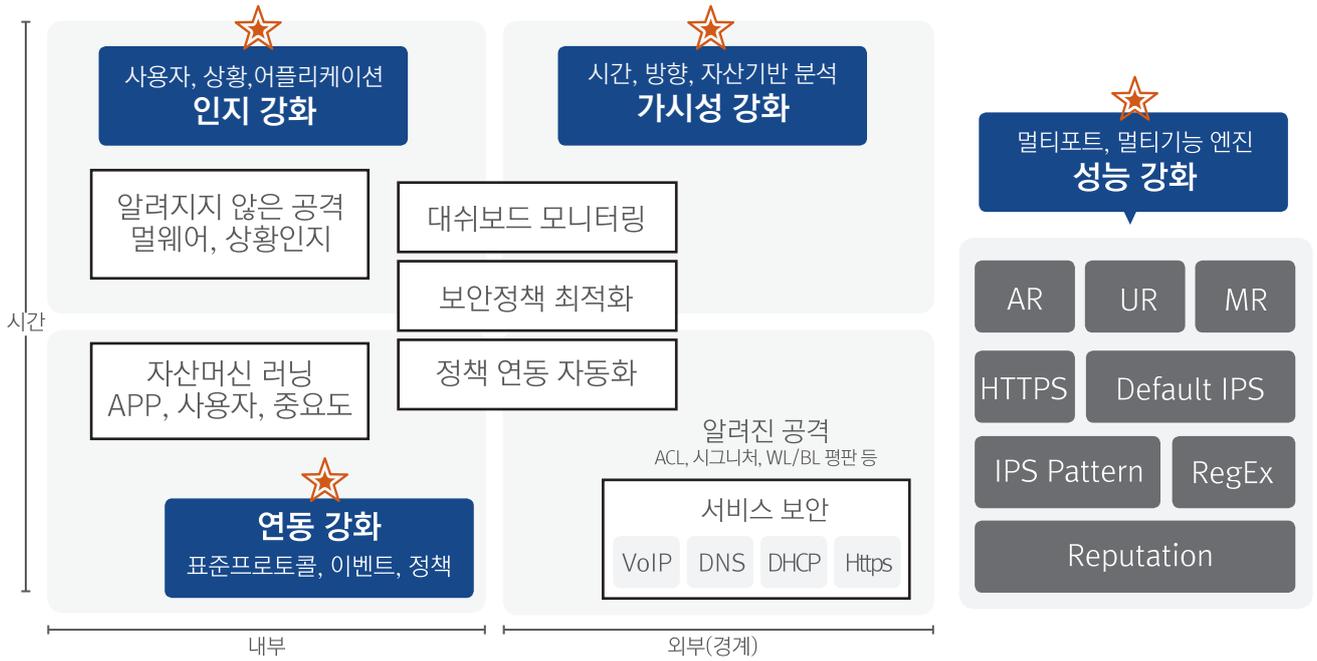


>> 탐지/분석 기술



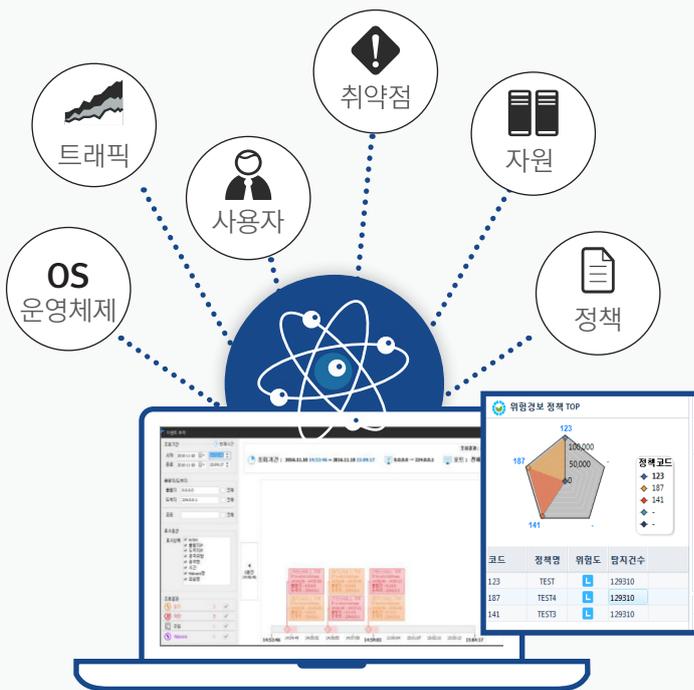
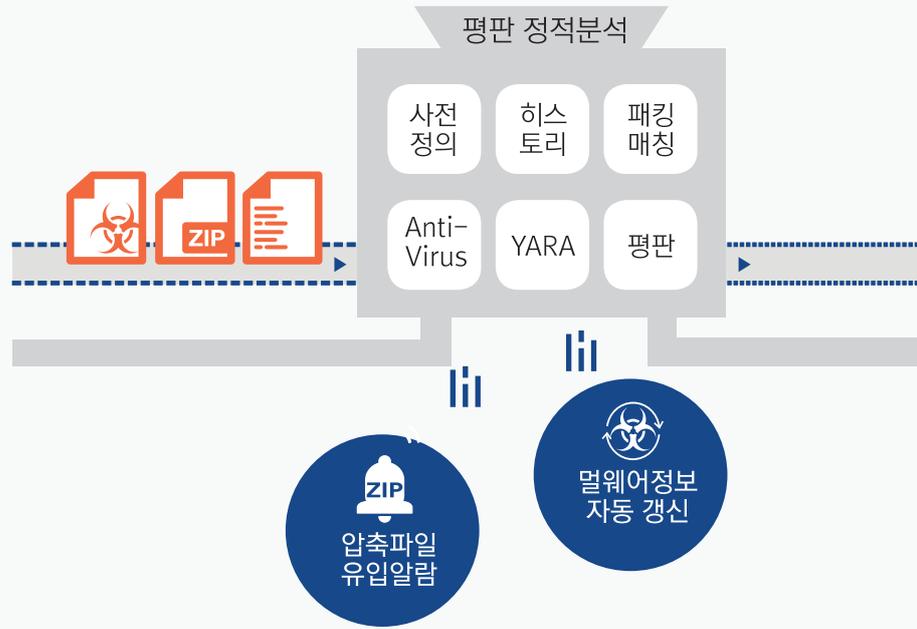
*1 특허등록 10-1713907 | 보안 네트워크에서 이벤트 발생 시점 기반 트래픽 상관 분석 서비스 제공 방법 및 시스템
| 특허출원 10-2016-0031005 | 오토마타 기반 필터 시스템 및 그 방법
| 특허출원 10-2016-0029023 | 사용자 행동분석 공격 감지시스템 및 그 방법

머신러닝과 가시성 확보를 통한 4단계 방어영역 확대



악성파일 추출, 멀웨어 정책 자동화

패킷 재구성으로 멀웨어 탐지 분석을 위한 파일수집 및 평판 정적분석으로 최신 멀웨어 정책을 제공합니다.



자산정보 상관분석으로 공격 위험도 예측

네트워크 기반에서 수집된 모든 가용 정보를 심층분석하여 위협 트래픽을 방어하며, 플로우메타데이터에 대한 상관관계 분석으로 위협 영향도 및 위협 추적기능을 제공합니다.

▶▶▶ 기존IPS vs ONE-i

		기존 IPS	NG-IPS	ONE-i
정적 대응	레거시 위협 방어	✓	✓	✓
	웹 콘텐츠 필터링 URL,URI	✓	✓	✓
	IP평판제어 국가, C&C, YARA등	부분 지원	✓	✓
인지 분석 대응	어플리케이션 제어	✗	✓	✓
	사용자 제어	✗	연동 지원	✓
	멀웨어 위협탐지 및 정책 자동화	✗	부분 지원	✓
	행위기반 상황인지 분석	✗	✗	✓
상관 분석 대응	위협패턴 자동추출	✗	✗	✓
	공격 위협정보 추적	✗	✗	✓
	공격 위험도 예측 분석	✗	✗	✓
	자산정보 연계 분석	✗	✗	✓

▶▶▶ Hardware specification

구분	ONE 1000	ONE 2000	ONE 4000	ONE 4100	ONE 5000	ONE 40G
RAM	32GB	32GB	32GB	32GB	64GB	64GB
HDD	1TB	2TB	2TB	2TB	2TB	2TB
NIC 1G/10G	4/-	4(최대 8)/-	4(최대 12)/-	4(최대 12)/-	-(최대 12) /2(최대 6)	-/4
성능	2Gbps	8Gbps	12Gbps	12Gbps	30Gbps 이상	40Gbps



(주) 윈스

경기도 성남시 분당구 판교로 228번길 17(삼평동) 판교세븐벤처밸리 1동 7층
TEL. 031-622-8600 FAX 031-622-8601

www.wins21.co.kr

Copyright © 2017 WINS. All rights reserved.