

# Proactive Threat Response Next Generation IPS

# BLUEMAX IPS 1000



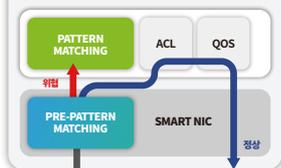
BLUEMAX IPS는 국내 네트워크 보안 1위가 만든 고성능 차세대 IPS입니다.  
고성능 위협 차단 플랫폼 기반으로 악성 트래픽 및 파일을 검사하고, 자산 취약점에 최적화된 운영과 가상화/클라우드 환경까지 지원하여 복합적이고 급변하는 보안 환경에 선제 대응이 가능합니다.

## BLUEMAX IPS 특징점

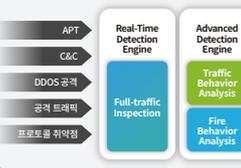
### HIGH PERFORMANCE

H/W - S/W 통합 프레임워크로 차세대 고성능 탐지 엔진 구현

고속 패턴 매칭 H/W 아키텍처

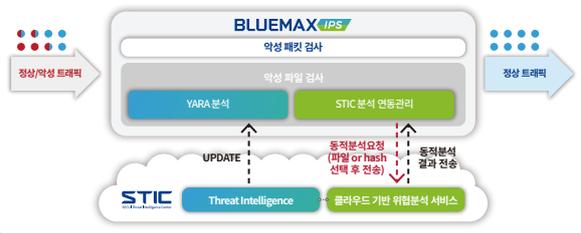


고효율 하이브리드 S/W 아키텍처



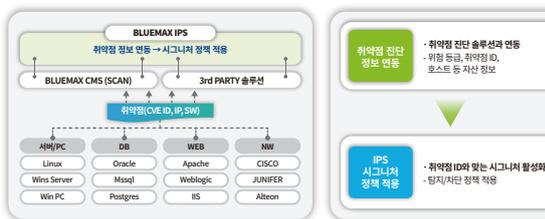
### UNKNOWN THREAT DETECTION

악성 파일 정적·동적 분석으로 신종 보안 위협 대응력 강화



### ENHANCED ASSET PROTECTION

자산 취약점 분석으로 고객 맞춤형 보안 정책 수립



### AGILE SERVICE

구축에서 운영단계까지 고객 맞춤 1-2-3 전문 서비스 제공

구축 후 1개월 내



시그니처 최적화

매월 2회



심층보안 위협정보 제공

3개월 간격



운영점검 서비스

## BLUEMAX IPS 주요 기능



### 시그니처 기반 방어

Cyber Kill Chain 기반으로 분석된 시그니처를 제공하여 각 공격 단계별 위협을 실시간으로 모니터링하고, 직관적이고 적시성있는 시그니처 방어 정책 운영 가능



### DDoS 방어

Anti-DDoS 전용 엔진을 탑재하여 DRDoS, SCAN 방어, 발신지 기반 방어, 내부 발신지별, 1:1 Flooding 등 다양한 형태의 DDoS 공격 탐지 및 차단 대응



### 학습 방어

트래픽의 IP, Port, Flag와 같은 다양한 헤더와 데이터 내용을 실시간으로 학습하여, 시그니처로 차단하지 못하는 신규공격까지 방어



### APP 제어

최신 트렌드에 맞는 애플리케이션의 특징(SaaS, Bandwidth), 제공기술 (C/S, P2P, Web-base), 위험 등급(악성), 태깅, 세부적인 프로파일 유형을 제공하여 각 인프라 환경에 최적화된 애플리케이션 제어 기능 제공



### UI 편의성

자유도 높은 대시보드 위젯 설정으로 맞춤형 운영 가능, 모든 메뉴별 멀티 윈도우 지원으로 가시성 확대, 향상된 Drill Down 기능으로 분석 시간 단축



### 사용자 정의 시그니처

인프라용 유형과 보안수준에 따른 시그니처 템플릿을 제공하고, Snort 옵션의 완벽한 지원 및 문법 오류 검사 기능으로 편리하면서도 휴먼 에러도 방지할 수 있는 최적화된 운영 기능 제공



### 상위기관 연동

상위기관(NCSC) 정책 동기화로 위협 탐지 (PCRE, SNORT, YARA) Rule 연동 편의성을 지원하며, BLUEMAX IPS에서 탐지된 이벤트를 상위기관으로 제공



### 원클릭 분석기능

BLUEMAX IPS에서 탐지된 로그의 즉시 분석 요청 가능하며, 경력 10년 이상의 전문가로 구성된 침해대응센터에서 빠른 Feedback 제공

# Software Specification

Intrusion Prevention		Anti - DDoS		Log Monitoring	
Application Awareness	HTTP, FTP, POP3, IMAP, SMTP, IP, TCP, ICMP, IPv6 비정상 프로토콜 탐지	Anti - DDoS	DoS, DDoS, DRDoS 방어	Dashboard	실시간 모니터링 제공 (이벤트, System, Network, 장비상태, 작업내역 등)
	App 탐지/제어/차단 동작 지원		HTTP, DHCP, SMTP, POP3, IMAP, SIP 방어		실시간 HA 모니터링 지원
	네트워크 트래픽 내 App 정보 인지		발신기반 세션 제어		실시간 SSL 세션 현황 모니터링 지원
	웹 메일, 메신저별 세부 기능 제어		패턴 학습 방어		실시간 공격 순위 제공
Context Awareness	네트워크 트래픽 내 사용자/자산정보 수집 및 토폴로지 제공	SSL Inspection	트래픽 학습 방어	Monitoring	사용자 정의 위젯 및 구성 가능
	외부장비/DB시스템과 사용자 정보 연동		양방향 트래픽 복호화 지원		위협 탐지 및 차단 모니터링
	취약점 진단 솔루션과 시그니처 정책 연계		SSL 트래픽 자동 탐지		탐지 및 차단 특화 상세 이력 제공
	평판 DB 연동 (IP, URL)		SSL 예외 정책 지원 (5-tuple / SNI / CN)		평판 탐지 결과 제공
Content Awareness	사용자 정의 평판 (IP, URL)	SSL Inspection	TLS 1.3 지원	Log Statistic	로그/통계 도구 기능
	클라우드 기반 악성 URL 검사		TLS 버전 제어		로그/통계 가시성 및 사용자 편의성 강화
	국가/지역별 제어 기능 제공		사설 인증서 제어		사용자 정의 트렌드 및 통계 기능 제공
	행위분석 기능을 통한 신변종 유형 대응		SSL 트래픽 Cipher-Suite 제어		
Legacy Rule	악성 유형에 대한 보고서 및 정보 제공	Security Setting & Interworking		Management Function	
	YARA 룰 지원	Security Setting & Interworking	통합위협관리시스템 연동	Network / IP / Session / Audit Management	세그먼트, 네트워크 정책 설정 및 관리
	첨부파일 내 Anti-Virus 탐지		위협 이벤트 및 로그 전송		네트워크 대역별 통계, 모니터링, 로그 지원
	다중, 암호화된 압축 파일 해제 지원		원클릭 이벤트 분석 요청		VLAN, GRE, IPinIP, GTP, DHCP, IP(v4,v6), ICMP(v4,v6), IGMP, TCP/UDP 프로토콜 지원
사용자 정의 Snort Rule	상위기관 정책 동기화		TCP 세션 관리 및 통계 기능 제공		
PCRE(정규표현식)	블랙리스트 차단 지원	화이트리스트 등록 지원	시스템 운영 환경에 따른 설정 기능 제공	관리자 별 보안 기능 및 권한 유형 제공	정책 및 설정 백업/복구 기능 제공
멀티패턴 탐지 기능(병렬탐지)	ACL 및 MAC 주소 제어 지원		탐지 및 제어 방식 최적화 대역폭 보장	정책/동적기반 QoS TCP Flag별 제어 (SYN, FIN, RST, PSH, ACK 등)	동적 QoS TCP/UDP/ICMP/ETC PPS 제어

# Hardware Specification

Model Name		BLUEMAX IPS 1000
CPU		4 Core
Memory		32 GB
Storage	System	SSD 32 GB
	Log	HDD 1 TB
Interface	1G Fiber	(max4)
	1G Copper	4(max8)
	HA Port / Mgmt	1GC x 2 / 1GC x 1
Power Supply		Single
Dimension (WxDxH)		1U (438x481x44)
Throughput (UDP/64byte)		1 Gbps

## SECUI (주)시큐아이

서울특별시 종로구 종로 51 3~6F (종로2가, 종로타워)  
 tel 02 3783 6600 fax 02 3783 6499 www.secui.com

대표전화 080-331-6600

기술지원/침해대응센터 02-3783-6500

보안관제센터 02-3782-4030

평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

## CERTIFICATIONS

