

Proactive Threat Response Next Generation IPS

BLUEMAX IPS 10000



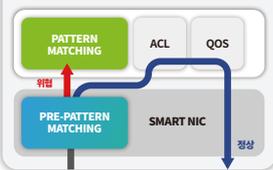
BLUEMAX IPS는 국내 네트워크 보안 1위가 만든 고성능 차세대 IPS입니다.
고성능 위협 차단 플랫폼 기반으로 악성 트래픽 및 파일을 검사하고, 자산 취약점에 최적화된 운영과 가상화/클라우드 환경까지 지원하여 복합적이고 급변하는 보안 환경에 선제 대응이 가능합니다.

BLUEMAX IPS 특징점

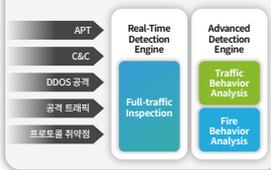
HIGH PERFORMANCE

H/W - S/W 통합 프레임워크로 차세대 고성능 탐지 엔진 구현

고속 패턴 매칭 H/W 아키텍처

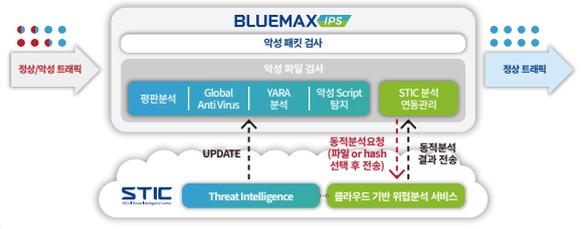


고효율 하이브리드 S/W 아키텍처



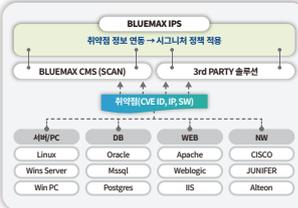
UNKNOWN THREAT DETECTION

악성 파일 정적·동적 분석으로 신종 보안 위협 대응력 강화



ENHANCED ASSET PROTECTION

자산 취약점 분석으로 고객 맞춤형 보안 정책 수립



취약점 진단 정보 연동

- 취약점 진단 솔루션과 연동
- 위험 등급, 취약점 ID, 포트 등 자산 정보

IPS 시그니처 강제 적용

- 취약점 ID에 맞는 시그니처 활성화
- 탐지/차단 정책 적용

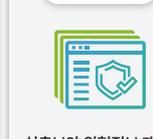
AGILE SERVICE

구축에서 운영단계까지 고객 맞춤 1-2-3 전문 서비스 제공

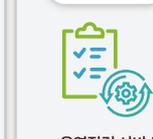
구축 후 1개월 내



매월 2회



3개월 간격



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

인프라망 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

