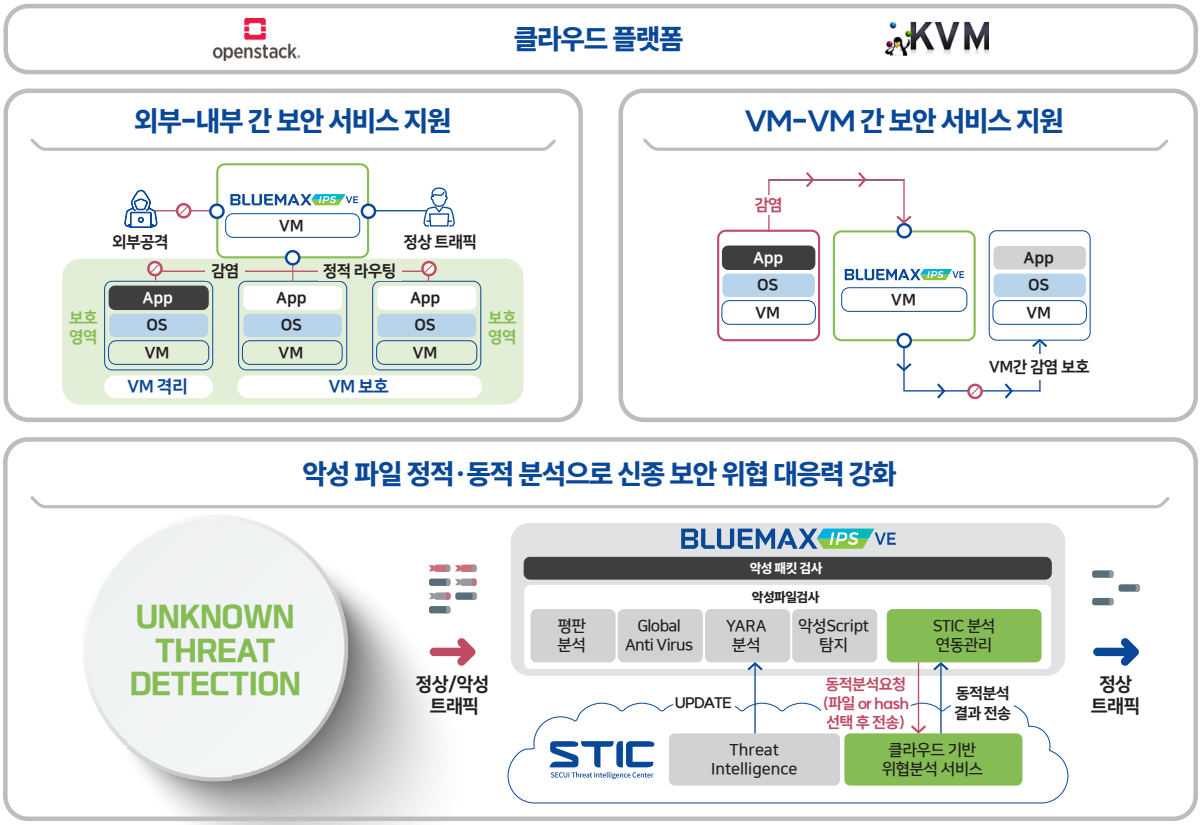
Next Generation IPS Virtual Edition

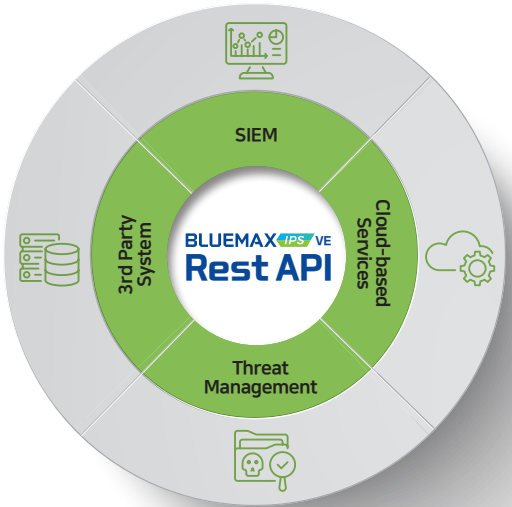
BLUEMAX IPS VE

BLUEMAX IPS VE는 가상화 클라우드 네트워크 보안을 위한 차세대 IPS이며, 다양한 가상 환경의 악성 트래픽 및 파일을 검사하여 위협 요소를 탐지·차단하는 기능을 제공하는 가상화 버전의 솔루션 입니다.

01 가상화/클라우드 플랫폼 지원



02 Rest API 연동으로 Security Orchestration 지원



Policy
- 정책 컴플라이언스 준수 확인
- 정책 다운로드를 통한 이력관리

Profile / Object
- URL/파일유형 객체 목록 조회
- 공격 시그니처 업데이트
- 정책 예외 객체 및 사용자 설정

Log / Management
- 다양한 방식의 로그 제공으로 시스템간 로그 통합 및 분석 가능
- 컴플라이언스에 따른 보고서 제공

System Configuration
- 시스템 운영정보조회 및 SW패치
- 시스템 백업 및 복구 관리

03 BLUEMAX IPS VE 주요기능

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

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

애플리케이션 제어
트렌드에 맞는 애플리케이션의 특징 (SaaS, Bandwidth), 제공기술 (C/S, P2P, Web-base), 위험 등급(악성), 태깅, 세부적인 프로파일 유형을 제공, 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 정책 동기화로 위협 탐지(PCRE, SNORT, YARA) Rule 연동 편의성을 지원하며, BLUEMAX IPS VE에서 탐지된 이벤트를 상위기관으로 제공

원클릭 분석기능
BLUEMAX IPS VE에서 탐지된 로그의 즉시 분석 요청 가능하며, 뛰어난 IPS 전문 엔지니어로 구성된 침해대응센터에서 빠른 Feedback 제공

04 Software Specification

BLUEMAX IPS VE	1000
Virtualization Platform	Openstack, KVM
vCPU	8Core
vMemory	32GB
vStorage	128GB
Throughput	1Gbps

SECUI
(주) 시큐아이
서울특별시 종로구 종로 51 3~6F(종로2가, 종로타워)
TEL 02-3783-6600 FAX 02-3783-6499
www.secui.com
대표 전화 080-331-6600
기술지원/침해대응센터 02-3783-6500
보안관제센터 02-3782-4030
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)
Copyright® SECUI All Rights Reserved 본 카탈로그에 게재된 호명, 상품명은 당사의 등록 상표입니다. 사양은 개량을 위해 예고 없이 변경 되는 경우가 있습니다.