

시큐아이 제품 소개서

Secuirty Intelligence Platform
For All My Threat Management

Virtual Cloud Generation Firewall

BLUEMAX NGF

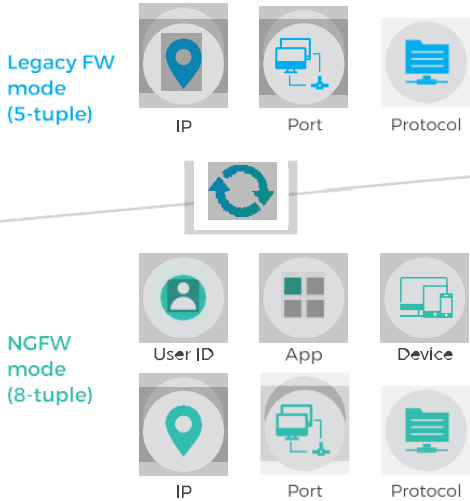
국내 최초 가상화, 클라우드 차세대 방화벽

BLUE MAX NGF는 국내 최초의 가상화 클라우드 네트워크 보안을 위한 차세대 방화벽이며, 유무선 IT인프라 환경의 모든 위협 요소를 탐지, 차단하는 통합보안플랫폼을 제공합니다.

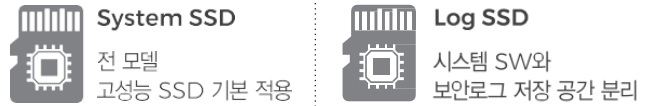
BLUEMAX NGF 특징점

장비 교체 없이 Legacy, NGFW mode 전환

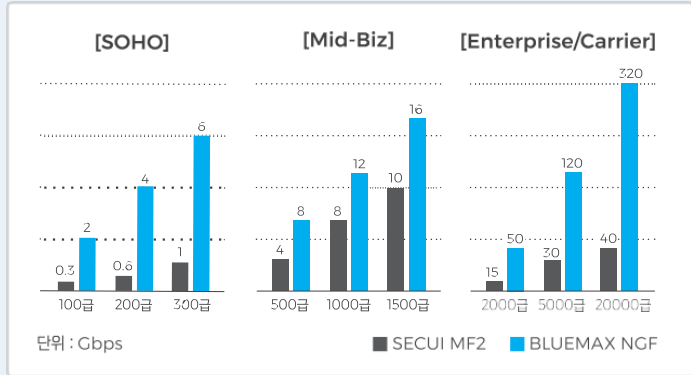
기본 방화벽 성능이 우수한 Legacy FW mode와 정교한 보안 설정이 가능한 NGFW mode 동시 제공



고가용성 HW 아키텍처로 무중단 서비스 제공



자사 제품 최대 성능 비교



주요 기능

App 제어

국내외 애플리케이션의 의한 취약점 증가, 악성코드 배포 등을 방지하기 위해 애플리케이션을 사전 정의하고 분석하여 기존 UTM에서 대응이 어려운 공격에 능동적으로 대처할 수 있는 기능

SaaS App 제어

클라우드 기반 SaaS 애플리케이션 확산에 대한 보안 강화를 위해 글로벌 클라우드 애플리케이션 제어 기능 강화

파일 유형 제어

애플리케이션 사용 시 파일의 유형별 (문서, 압축 파일, 이미지, 멀티 미디어 등), 방향별로 제어하여 비인가 파일 전송과 내부 유출 방지 및 외부로부터 위협 예방

사용자 ID

IP가 아닌 사용자 ID를 인식하여 언제 어디서 네트워크에 접속하여도 동일한 보안 정책을 적용 받아 사용자의 이동성을 보장하고 사용자별 통계 자료 조회 가능

Open API

국내 뿐 아니라 글로벌 벤더의 통합 보안 관리 시스템, 취약점 진단 시스템, 보안 정책 분석 시스템과 유연하게 연동하여 보안 오케스트레이션 & 자동화 구현

Device 제어

사용자 단말의 보안 설정, 필수 SW 설치여부, 보안 업데이트 현황, 백업/암호화 설정 여부를 검사하여 내부망, 중요 업무 시스템에 대한 접근을 제어함으로써 멀웨어 감염을 원천 차단

도메인 객체

IP 대신 도메인명을 방화벽 객체로 사용하는 기능으로 클라우드 환경(포털, 웹하드)을 고려하여 도메인당 2,048개까지 실시간 및 주기적으로 IP수집

SSL Inspection

SSI 세션을 자동 탐지, SSL 패킷을 복호화하여 다양한 차세대 네트워크 보안 기능에 적용하는 기능으로 H/w 가속기를 적용하여 기존 제품 대비 성능 강화

Software Specification

Virtual Cloud Gen Function			
	사용자 기반 정책 제어		
	애플리케이션/디바이스 기반 정책 제어		
NCFW	AD SSO 연동을 위한 AD 설정 마법사	Anti-DDoS	응용계층 방어
	애플리케이션별, 사용자 ID별 QoS		행위기반 웹 공격 방어, DrDoS(N:1) 방어
	자체 사용자 인증(Captive Portal) 및 SSO		스마트 패턴 학습 방어
Virtual System	SaaS 애플리케이션 제어	IPSec VPN	알려지지 않은 공격 및 GRE 공격 차단
	Virtual System별 자원 할당		IKE(v1/v2), PKI(X.509)
	토폴로지 맵으로 직관적 가상 네트워크 구성		GRE/IPIP, L2TP, PPTP Tunneling
APT (위협대응)	관리자별 독립적인 운영 환경	SSL VPN	3DES, AES, SEED, ARIA, CAST, Blowfish, MD5, SHA-1, SHA-256, SHA-512, HAS160 등
	Sandbox 장비와 연동하여 APT 위협 분석 기능 제공 및 Client를 통한 위협 차단 기능 제공		Group VPN 기능
	탐지된 위협 정보(공격자/배포지 IP 및 URL, 악성 파일 Hash 값 등)에 대한 공유 체계 지원		Full Tunnel mode
SSL Inspection	HTTPS, SMTPS, POP3S, IMAPS, FTPS	Contents Filtering Function	
	Hardware Acceleration	Anti-Virus & Anti-SPAM	Anti-Virus Engine(File-based or Stream-based)
	App Control, IPS, DLP, WebFilter 기능 및 외부 보안 장비와 호환화 트래픽 연동	Realtime Blackhole List(RBL)	수신자 수 제한, 대량메일 발송 제한
UTM Function		Web Filter	URL Filtering(Category별 설정)
Legacy Firewall	Active-Active HA with L2/L3/L4		URL 확장 검사(URI 쿼리 검사)
	도메인 정책(URL 객체)		Global Categorized URL(로컬/클라우드 DB)
	중복 정책 및 미사용(미참조) 정책 검사	Anonymizer 서버목록 차단	
IPS	Policy-based NAT & Interface-based NAT	DLP(Data Loss Prevention)	경고페이지 설정 및 편집
	보안 정책 그룹 설정		HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
	보안 정책별 활성화 스케줄		웹메일을 통한 정보유출 제어
Client Security	프로파일기반 시그니처 템플릿		주인등록번호, 카드번호 등록/검사 및 차단
	PCRE(정규표현식)		범용파일 포맷 39가지 이상
	멀티패턴 탐지 기능(병렬탐지)		압축파일(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)
Management Function	취약점 점검 도구 연동, 시그니처 최적화		필터 및 저장(아카이브)
Management			
Monitoring			
Networking			

Hardware Specification

BLUEMAX NGF	50	100	200	300	500	1000	1500	2000	5000	20000
CPU	2 Core	2 Core	4 Core	4 Core	8 Core	2 Core	4 Core	16 Core	24 Core	48 Core
Memory	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB	16 GB	32/64 GB	64/128 GB	96/288 GB
Storage	System	16 GB	16 GB	32 GB	64 GB	128 GB	128 GB	256 GB	128/512 GB	128/512 GB
	Log	-	-	-	1 TB	1 TB	1 TB	1 TB	1.92 TB/RAID	1.92 TB/RAID
Interface	100G Fiber	-	-	-	-	-	-	-	(max 2)	(max 4)
	40G Fiber	-	-	-	-	-	-	-	(max 4)	(max 8)
	10G Fiber	-	-	-	-	-	(max 4)	2(max 10)	10(max 26)	10(max 26)
	1G Fiber	-	-	-	-	4	4	4(max 8)	8(max 40)	8(max 40)
	1G Copper	4	4+4(switch)	4+8(switch)	8	8	8	8	8(max 40)	8(max 40)
	mgmt	-	-	-	1	1	1	1	2	2
Throughput	1 Gbps	2 Gbps	4 Gbps	6 Gbps	8 Gbps	12 Gbps	30 Gbps	60 Gbps	120 Gbps	320 Gbps
CC(Concurrent)	700,000	1,000,000	1,500,000	2,000,000	3,000,000	5,000,000	8,000,000	15,000,000	30,000,000	60,000,000
Power Supply	Adapter	Adapter	Adapter	Single	Single	Single	Redundant	Redundant	Redundant	Redundant
Dimension(WxDxH)	201x191x45	230x237x44	230x237x44	1U (438x432x44)	1U (438x432x44)	1U (438x525x44)	1U (438x525x44)	2U (438x685x88)	2U (438x685x88)	2U (438x685x88)

CERTIFICATIONS

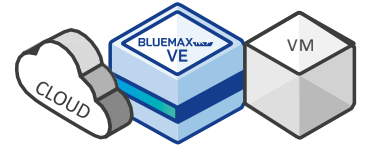


시큐아이 공인 총판
쿠도커뮤니케이션(주)

02-525-0481
secure@cudo.co.kr



Next Generation Firewall Virtual Edition BLUEMAX NGF VE



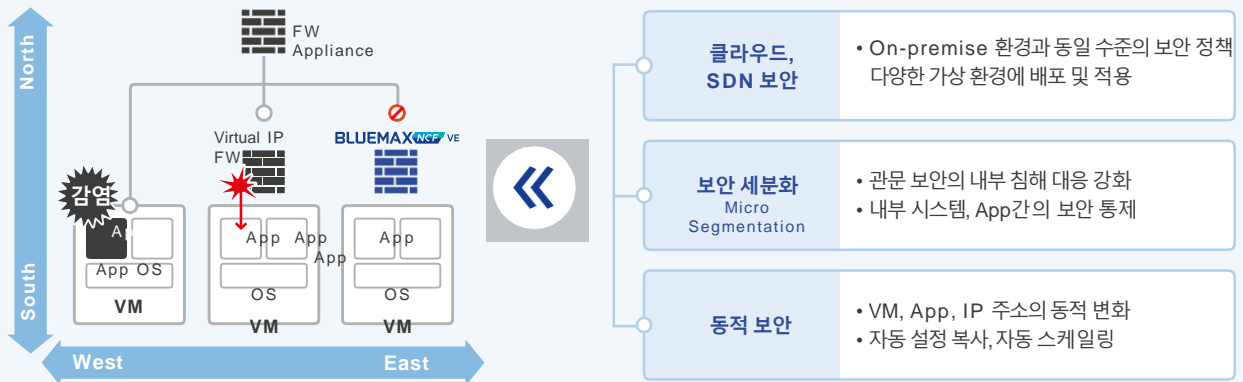
국내 최초 가상화, 클라우드 차세대 방화벽

BLUEMAX NGF VE는 가상화 클라우드 네트워크 보안을 위한 차세대 방화벽이며, 다양한 가상 환경의 모든 위협 요소를 탐지·차단하고 편리한 설치와 Auto Scaling 구현으로 보안 가용성을 제공하는 통합보안 플랫폼의 가상화 버전입니다.

다양한 가상화 클라우드 플랫폼 지원



가상 환경 내외부 위협 차단 최적화



Rest API 연동으로 Security Orchestration 지원



Software Function

Virtual Cloud Gen Function					
	사용자 기반 정책 제어				
	애플리케이션/디바이스 기반 정책 제어				
NGFW	AD SSO 연동을 위한 AD 설정 마법사	IPSec VPN	IKE(v1/v2), PKI(X.509)	Compliance 점검을 통한 단말 보안 상태 정보 제공	단말 보안 정보 수집(업데이트, 보안 설정)
	애플리케이션별, 사용자 ID별 QoS		GRE/IPIP, L2TP, PPTP Tunneling		
	차체 사용자 인증(Captive Portal) 및 SSO		3DES, AES, SEED, ARIA, CAST, Blowfish 등		
	SaaS 애플리케이션 제어		MDS, SHA-1, SHA-256, SHA-512, HAS160 등	Management Function	
APT (인합대)	Sandbox 장비와 연동하여 APT 위협 분석 기능 제공 및 Client를 통한 위협 차단 기능 제공	SSL VPN	Full Tunnel mode	Management	Auto Scaling 지원
	탐지된 위협 정보(공격자,해포지 IP 및 URL, 악성 파일 Hash 값 등에 대한 공유 체계 지원)		Multi-Factor 인증 지원(3차 인증)		Firmware Upgrade and Downgrade (Rollback)
SSL Inspection	HTTPS, SMTPS, POP3S, IMAPS, FTPS	Anti-Virus & Anti-SPAM	Contents Filtering Function		정책 설정 Multi R/W 기능
	Application Control, IPS, DLP, WebFilter, Anti-X 등		Anti-Virus Engine (File-based or Stream-based)	GUI상에서의 CLI 실행 및 Packet Capture	
UTM Function		Web Filter	Realtime Blackhole List(RBL)	Monitoring	LDAP/RADIUS/TACACS+/OTP 등 관리자 접속
Legacy Firewall	도메인 정책(URL 객체)		수신자 수 제한, 대량메일 발송 제한		URL Filtering(Category별 설정)
	중복 정책 및 미사용(미참조) 정책 검사		URL 확장 검사(URI 쿼리 검사)	Open API, 기타 외부 솔루션 연동	
	Policy-based NAT & Interface-based NAT		Global Categorized URL(로컬/클라우드 DB)	SNMP(v1,2,3), Syslog 전송	
	보안 정책 그룹 설정	DLP(Data Loss Prevention)	Anonymizer 서버목록 차단	DB 기반 로그 관리(압축 지원)	
	보안 정책별 활성화 스케줄		경고페이지 설정 및 편집	경고 알람 임계치 설정	
IPS	자동 학습에 의한 시그니처 추출 및 적용 기능		HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS	Report(정책 상세, 리포트 브라우저)	
	PCRE(정규표현식)		웹메일을 통한 정보 유출 제어	애플리케이션, 사용자별 트래픽/세션 모니터링	
	멀티패턴 탐지 기능(병렬탐지)		주민등록번호, 카드번호 등록/검사 및 차단	LACP, VLAN, 동적자산 제어	
	취약점 점검 도구 연동, 시그니처 최적화		범용파일 포맷 39가지 이상	IPv6 트랜지션(설정 터널링, 6to4) & 트랜슬레이션(NAT64/NAT46, DNS64)	
Anti-DDoS	응용계층 방어	Client Security		Networking	DHCP, DHCPv6 및 RA서버
	행위기반 웹 공격 방어, DrDoS(N:1) 방어	SSL VPN Client(PC, Linux, Android, iOS)	압축파일(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)		DNS, DDNS, Split DNS
	지역기반 차단 및 블랙리스트(IPv4/IPv6)	이상 징후 탐지, 격리, 삭제	필터 및 저장(아카이빙)		QoS(IP, Application, 인터페이스별)
	알려지지 않은 공격 및 GRE 공격 차단	이상 트래픽, 파일, URL 수집		Routing Protocol (IPv4-OSPF/RIP/BGP, IPv6-OSPFv3/RIPng/BGP4+)	

Software Specification

BLUEMAX NGF VE	100	200	300	500	1000
Virtualization Platform	VMware, Citrix Xen, Hyper-V, KVM, AWS, Azure, Openstack				
vCPU Support	1	2	4	6	8
Memory Support	4 GB	4 GB	8 GB	8 GB	8 GB
Storage Support (Min/Max)	128 GB / 2 TB				
Throughput	2 Gbps	4 Gbps	6 Gbps	8 Gbps	10 Gbps
CC (Concurrent)	1,000,000	1,500,000	2,000,000	3,000,000	5,000,000

BLUEMAX^{IPS}

고성능 차세대 IPS

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 IPS의 네트워크 보안 위협 선제적 대응 체계



주요 기능

<p>시그니처 기반 방어</p> <p>사이버 킬 체인 기반으로 분석된 시그니처를 제공하여 각 공격 단계별 위협을 실시간으로 모니터링하고, 직관적이고 적시성 있는 시그니처 방어 정책 운영 가능</p>	<p>DDoS 방어</p> <p>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</p>	<p>학습 방어</p> <p>트래픽의 IP, Port, Flag와 같은 다양한 헤더와 데이터 내용을 실시간으로 학습하여, 시그니처로 차단하지 못하는 신규공격까지 방어</p>	<p>APP 제어</p> <p>최신 트렌드에 맞는 애플리케이션의 특징, 제공 기술, 위험 등급(악성), 태깅, 세부적인 프로파일 유형을 제공하여 각 인프라 환경에 최적화된 애플리케이션 제어 기능 제공</p>
<p>UI 편의성</p> <p>자유도 높은 대시보드 위젯 설정으로 맞춤형 운영 가능, 모든 메뉴별 멀티 윈도우 지원으로 가시성 확대, 향상된 Drill Down 기능으로 분석 시간 단축</p>	<p>사용자 정의 시그니처</p> <p>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</p>	<p>상위기관 연동</p> <p>상위기관(NCSC) 정책 동기화로 위협 탐지(PCRE, SNORT, YARA) Rule 연동 편의성을 지원하며, BLUEMAX IPS에서 탐지된 이벤트를 상위기관으로 제공</p>	<p>원클릭 분석기능</p> <p>BLUEMAX IPS에서 탐지된 로그의 즉시 분석 요청 가능하며, 경력 10년 이상의 전문가로 구성된 침해대응센터에서 빠른 피드백 제공</p>

Software Specification

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

Hardware Specification

	BLUEMAX IPS	1000	2000	4000	5000	10000
CPU		4 Core	10 Core	10 Core	24 Core	52 Core
Memory		32 GB	32 GB	64 GB	96 GB	192 GB
Storage	System	SSD 32 GB	SSD 32 GB	SSD 32 GB	SSD 128 GB	SSD 128 GB
	Log	HDD 1 TB	HDD 2 TB	HDD 2 TB	SSD 1.92 TB	SSD 1.92 TB
Interface	40G Fiber	-	-	-	(max4)	(max8)
	10GF FPGA (2 Slot)	-	-	2	4(max8)	4(max8)
	10G Fiber	-	-	(max4)	(max8)	(max8)
	1G Fiber	(max4)	4(max8)	(max8)	(max12)	-
	1G Copper	4(max8)	(max8)	(max8)	(max12)	-
	HA Port / Mgmt	1GC x 2 / 1GC x 1	1GC x 2 / 1GC x 1	1GC x 2 / 1GC x 1	10GF x 2 / 1GC x 2	10GF x 2 / 1GC x 2
Power Supply		Single	Dual	Dual	Dual	Dual
Dimension (WxDxH)		1U (438x481x44)	2U (438x481x88)	2U (438x481x88)	2U (438x685x88)	2U (438x685x88)
Throughput (UDP/64byte)		1 Gbps	2 Gbps	10 Gbps	20 Gbps	40 Gbps

CERTIFICATIONS



시큐아이 공인 총판
쿠도커뮤니케이션(주)

02-525-0481
secure@cudo.co.kr



Anti - DDoS

SECUI MFD는 변화하고 있는 DDoS 공격에 대응하는 차세대 Anti-DDoS 장비입니다.

주요 특징점



주요 기능

다단계/다계층 DDoS 공격 탐지 및 차단

IP 계층부터 애플리케이션 계층까지 다양한 DDoS 공격을 정밀하게 탐지 및 차단

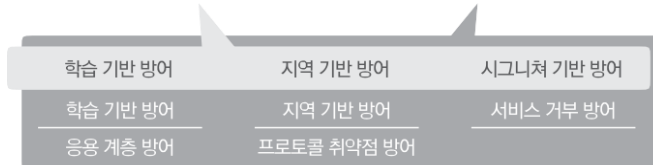
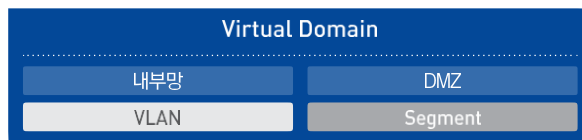
- Flooding 공격부터 다양한 응용 계층 공격까지 완벽한 방어
- 자동 학습을 통한 차단 및 국가별 DDoS 공격 방어



가상 도메인

가상 도메인으로 네트워크 환경에 적합한 유연한 DDoS 방어 정책 적용





- 네트워크를 물리적 및 논리적인 가상 도메인 설정
- 도메인별 별도 보호 프로파일 지정으로 유연한 보안 정책 적용



DDoS Attack Defense List

TCP 공격 방어	HTTP 공격 방어	UDP 공격 방어
TCP SYN Flooding	HTTP Flooding	UDP Flooding
TCP SYN-ACK Flooding	HTTP Post Attack (Session, IP)	UDP Invalid Header Length Attack
TCP RST Flooding	HTTP Caching Behavior Anomaly (CC, Circle Attack)	UDP Land2 Attack
TCP FIN Flooding	HTTP Slow loris Attack	UDP BPS, PPS Rate-Limit
TCP ACK Flooding	HTTP Request Anomaly Attack	UDP Invalid Port Attack
TCP URG Flooding	HTTP XFF Field Based Defense	
TCP PSH Flooding	HTTP Invalid URI Length Attack	DNS 공격 방어
TCP XMAS Flooding	HTTP Slow Read Attack (Session, IP)	DNS Request Flooding
TCP MISC Flooding	HTTP Repeated Pattern Flooding Attack	DNS Response Flooding
TCP Land2 Attack	Server Behavior Anomaly Attack	
TCP CPS, Session, BPS, PPS Rate-Limit	Slow Read Attack	VoIP 공격 방어
TCP Open Connection	SSL Renegotiation Attack	Request Flooding
TCP No Data Connection	SQL Query Flooding Attack	Response Flooding
TCP Invalid Port Attack		Malformed Message
TCP Invalid Flag Attack	ICMP 공격 방어	
FTP 공격 방어	ICMP Flooding	비정상 패킷 공격 방어
FTP Direction Traversal Attack	ICMP Echo Request Flooding	시그니처 기반 방어
FTP Bounce Attack	ICMP Echo Replay Flooding	Anti-Botnet
FTP User Name Overflow	ICMP Unreachable Flooding	
FTP/Telnet Escape Sequence Detect	ICMP BPS, PPS Rate-Limit	지역 기반 방어
	ICMP Ping of Death Attack	Zero-Day Attack & Unknown Attack 방어

Hardware Specification

SECUI MFD	2300	4100	21000	23000	
Chassis					
CPU	4 Core	10 Core	18 Core x 2	24 Core x 2	
Memory	16 GB	32 GB	64 GB	96 GB	
Storage	System	HDD 1 TB	HDD 2 TB	SSD 128 GB	
	Log			SSD 1.92 TB	
Throughput (Max)	10 Gbps	40 Gbps	100 Gbps	120 Gbps	
Interface	40G Fiber	-	-	(Max 4)	
	10G Fiber	-	(Max 8)	8 (Max 16)	
	1G Fiber	8 (Max 12)	8 (Max 16)	(Max 16)	(Max 24)
	1G Copper	8 (Max 24)	8 (Max 32)	(Max 32)	(Max 40)
Power Supply	Redundant	Redundant	Redundant	Redundant	
Dimension (W x D x H)	2U (438 x 580 x 87)	2U (431 x 577 x 88)	2U (437 x 671 x 88)	2U (438 x 685 x 88)	

* CC 인증 평가기준의 성능 및 기능 시험을 모두 통과한 DDoS 전용 제품

* 40G NIC는 추가 CC 인증 평가 진행중



시큐아이 공인 총판
쿠도커뮤니케이션(주)

02-525-0481
secure@cudo.co.kr

CERTIFICATIONS



Next Generation Wireless
Intrusion Prevention System
BLUEMAX WIPS

지능형 무선 위협 대응 시스템 BLUEMAX WIPS

Wi-Fi 6(802.11ax)의 보안위협을 완벽 차단하는 차세대 무선 침입방지 시스템입니다. WPA3™, PMF(802.11w)를 사용하는 비인가/불법 AP와 무선 단말을 차단합니다. 또한, 지능형 심층분석 엔진을 탑재하여 무선 보안 위협을 분석, 탐지 및 차단하며 무선 침입 방지부터 무선 보안사고 포렌식까지 신속하고 지능적으로 대응합니다.

BLUEMAX WIPS 특징점



Wi-Fi 6 완벽 지원

Wi-Fi 표준(802.11 a/b/g/n/ac/ax)에 대한 탐지·차단 뿐만 아니라 PMF(802.11w)를 사용하는 비인가/불법 AP 및 비인가 단말 차단이 가능합니다.



신속한 탐지 및 차단

최적화된 스캔 알고리즘으로 무선 보안 위협을 신속히 탐지하고 차단합니다. (탐지 후 1초 이내 차단 성능)



심층분석 및 사고대응

센서-단말-AP-행위-조치 등의 5단계 심층분석 기능과 포렌식 정보가 제공되어 효율적인 사고대응이 가능합니다.

주요 기능

무선 위협 탐지 및 차단

다양한 무선 위협에 대한 위협 종류별 세분화 정책 설정과 Wi-Fi 전 채널에 대한 신속한 탐지·차단 가능

무선랜 관리

사전 규칙 설정을 통해 탐지된 디바이스의 자동 분류 지원, AP/단말 등 접속 현황, 상세 정보 제공 및 위치 정보 제공

통계 및 리포트

디바이스 분류 기준에 따른 센서, 단말, AP별 통계 현황 제공 및 사용자 정의 일간/주간/월간 리포트 생성

지능형 심층분석 및 사고대응

센서-단말-AP-행위-조치 등 5가지 정보를 기반으로 한 상세분석 기능과 위치 추정, 이동경로 추적 기능을 제공하여 사고대응 및 포렌식 지원

무선랜 보안 관제

Wi-Fi 연결 현황 (AP <-> 단말) 정보, 실시간 이벤트 현황, 심층 분석 기능 등을 제공하여 보안관제에 특화된 모니터링 제공

다양한 구성 환경 지원





다양한 유무선 환경에 대처 가능한 구성 환경을 지원하고 독립모드, 자동 Fail-over 기능을 통해 중단없는 무선랜 보안위협 대응 가능

Software Specification

무선규격	무선 관리
Wi-Fi 6 (IEEE 802.11 a/b/g/n/ac/ax) 지원	위협 등급별 분류 (인가/비인가/위반/불법/외부/방문)
802.11w(PMF) 차단 (AP/단말 차단 가능)	AP/단말 그룹별 정책 설정, 유효기간 설정 및 접속 허용
듀얼 밴드(2.4GHz, 5GHz) 탐지/차단 지원	SSID 다국어 지원 & Hidden SSID 탐지
무선 위협 탐지 및 차단	무선랜 접속 현황 및 세부 정보
비인가/불법/설정 위반 AP 탐지 및 차단	무선 디바이스 위치 추정 및 이동 경로 관리
비인가 디바이스 접속 탐지 및 차단	단말-AP-센서 정보 기반의 무선 보안 분석
SSID 복제, MAC 변조 탐지 및 차단	시계열 기반 이벤트 이력 관리를 통한 포렌식 지원
모바일/휴대용 핫스팟 탐지 및 차단	시스템
Wi-Fi Direct/WDS/WPS/WEP 취약점 탐지 및 차단	컨트롤러 고가용성(HA) 지원 및 장애 시 자동 Fail-over
Malformed 무선 패킷 탐지	통신 단절 시 센서 독립모드 운영
무선 DoS 공격/RF 간섭원 탐지	센서 - 컨트롤러 간 암호화 통신
팝업, syslog, e-mail 등 이벤트 알림 기능	관리자 GUI HTML5/TLS1.3 지원

Hardware Specification

BLUEMAX WIPS (Sensor)	602	604
Appearance		
Wireless Standard	802.11 a/b/g/n/ac/ax, w	802.11 a/b/g/n/ac/ax, w
RF, Antenna	2.4/5GHz, 2 x 2	2.4/5GHz, 4 x 4
Interface	2x 1GbE, 1x 5GbE	1x 1GbE, 2x 5GbE
Power	PoE (802.3af), Adapter	PoE (802.3at), Adapter
Dimension (HxWxD)	175x175x45	235x235x45
Weight (g)	470	870
Temperature (Operation)	0~50°C	0~50°C

BLUEMAX WIPS (Controller)	1000	2000	3000	5000	
Chassis					
CPU	2 core, 2 threads	4 core, 4 threads	4 core, 4 threads	4 core, 8 threads	
Memory	8GB	16GB	16GB	32GB	
Storage	System	250GB	1TB	1TB	2TB
	Log	250GB	256GB	512GB x2	512GB x2
Interface	4x 1GbE	2x 1GbE	2x 1GbE	2x 1GbE	
Power Supply	Adapter	Redundant	Redundant	Redundant	
Dimension (HxWxD)	Desktop (43x254x226)	1U (43x437x507)	1U (43x437x507)	1U (43x437x507)	
Number of Sensors (max)	50	200	400	1,000	

CERTIFICATIONS

BLUEMAX TAMS

BLUEMAX TAMS는 분산된 보안 시스템의 통합 위협 분석, 대량 로그 수집, 직관적 통합 설정, 보안 정책 분석 및 최적화로 Security Automation 통합 보안 플랫폼을 제공합니다.

BLUEMAX TAMS 특징점

위협 분석, 통합 설정, 로그 분석, 정책 분석(신청) 모듈을 1Box 통합

✓ 다양한 기능들을 HW 1 Box에 통합 제공하며, 로그 용량 증가시 시스템 중단 없는 Cluster 시스템 확장

위협관리 + 통합 설정 + 로그 분석 + 정책 분석 = BLUEMAX TAMS

Big Data 기반 아키텍처로 로그 수집 분석 성능 최대 10배 향상

✓ 기존 제품 대비 로그 저장 성능, 분석/검색 성능 대폭 향상
 ✓ 1억 건 통계 분석 시 10초 이내 완료, 최대 20만 EPS
 ✓ 로그 저장 성능 제공 (TAMS 1대 기준)

[통계 분석 성능] [로그 수집 성능]
 SECU TMS vs BLUEMAX TAMS

고가용성 HW 아키텍처로 무중단 서비스 제공

✓ 고성능 SSD 적용
 ✓ 로그 저장 Raid 구성 기본 제공
 ✓ 시스템 SW와 보안로그의 저장 공간 분리

SYSTEM SSD
 LOG HDD
 LOG HDD (RAID)

BLUEMAX TAMS

실시간 다차원 분석

시스템/위협 현황을 실시간 모니터링 및 다차원 분석하여 다양한 위협 대응 정책에 활용



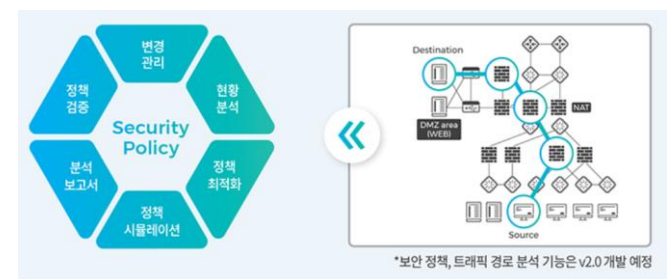
통합 위협 설정 관리

실시간 다차원 위협/정책 분석 결과에 기반한 직관적인 통합 설정 관리로 편의성 제공



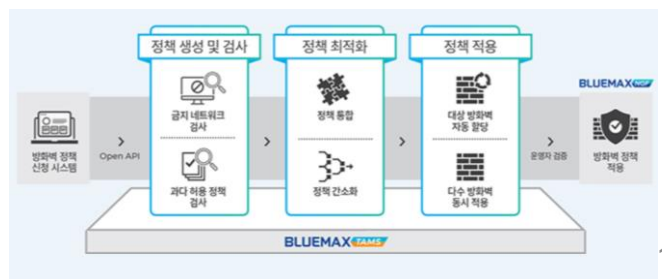
보안 정책 분석, 최적화

모든 관리 대상 장비들의 보안 정책을 자동 수집/유효성 검증/최적화하여 휴먼 에러 방지



보안 정책 관리 자동화

정책 신청부터 적용까지 보안 정책 관리 프로세스를 자동화하는 One-Stop 솔루션



Software Specification

PAMS	모니터링/대시보드
방화벽 정책 신청시스템 연동 지원(IT4U, E-mail 등)	장비 상태(장애) 실시간 모니터링
정책 자동 관리 지원	전체 장비 트래픽 모니터링
정책 적용 감사 기록 관리(신청 정보별, 적용 정책별)	관리 장비 2D/3D 토폴로지 맵 보기
정책 적용 마법사 기능 지원	관리 장비의 항목별 TOP 10(그래프 or 정보)
정책 Merge 기능 지원으로 정책 최적화 유지	사용자 정의 경고 로그 설정
TMS(위협 관리)	로그/리포트
수집된 이벤트로부터 위협 분석	로그 압축 기능(관리 장비별)
종합 상황도 커스터마이징 제공	Cluster 구성으로 로그 분산 저장
글로벌(국가별) 공격 통계 리스트	보안 이벤트 분석/통계를 통한 심층 패킷 분석
국정원 사이버 위기 경보	즉석, 기간별(주간, 월간, 연간) 리포트 제공
해당 공격 Raw Data 보기	통합 리포트 제공
예/경보 이벤트 사용자 정의 설정	미사용 정보(객체/정책) 조회
Central Management	시스템 설정
장비 설정 백업/복원	현재 접속 관리자 정보(현재 상태, 접속 시간)
장비 상태(장애) 관리 기능	관리자 설정(IPv4/IPv6, 역할 기반 관리자, 패스워드 정책)
설정 동기화	시스템 백업/복구
장비 자동 등록	관리 도구 제공(ping, traceroute, whois)
통합 스크립트 기능	시스템 무결성 점검
블랙리스트/ACL 설정	

Hardware Specification

BLUEMAX TAMS	100	1000	5000
CPU	4 Core	10 Core	10 Core x 2
Memory	8 GB	64 GB	128 GB
Storage	System	1TB	256 GB SSD x 2
	Log	-	4 TB x 2 / 4 TB x 4
Interface	10G Fiber	-	(max 2)
	1G Fiber	-	(max 2)
	1G Copper	2	4
Power Supply	Single	Dual	Dual
Number of Devices (max)	100	1,000	5,000
Dimension(WxDxH)	1U(426x356x43)	2U(437x648x89)	2U(437x648x89)

BLUEMAXCLIENT for SCAN

BLUEMAXCLIENTforSCAN은 서버, 네트워크 장비와 같은 IT인프라의 보안 취약점 진단을 상시적으로 자동 수행하고 관리 합니다.
국내외 보안 컴플라이언스(CCE) 및 어플리케이션 취약점(CVE)을 동시 진단하고, 네트워크 보안 솔루션과 연동하여 보안 정책 자동화를 지원하는 능동적 통합 보안 취약점 관리 시스템입니다.

능동적인 통합 보안 취약점 관리



특장점

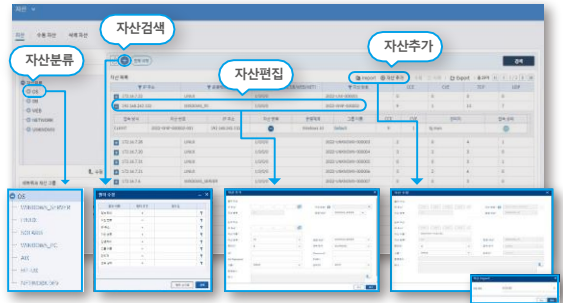
취약점 통합 진단	다양한 진단 방안	진단 최적화 기능 구성	취약점 연동 제공
<p>단일 솔루션에서 다양한 자산의 CCE/CVE 통합진단 제공</p>	<p>강력한 포트 스캔으로 숨겨진 자산 식별</p> <p>Agent 상시점검 및 Agentless 원격 점검</p>	<p>취약점 진단의 최적화된 기능 (자산관리, 취약점 재평가, 조치, 점검, 우선순위 결정, 평가 등)</p>	<p>방화벽, IPS 정책 연동으로 취약점 기반 방어 정책 수립</p>

주요기능

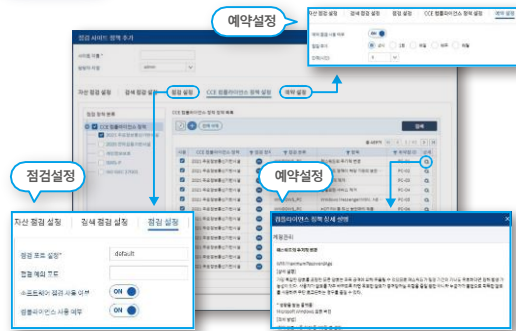
모니터링 자산 및 취약점 정보에 대한 실시간 모니터링 및 관리 수행



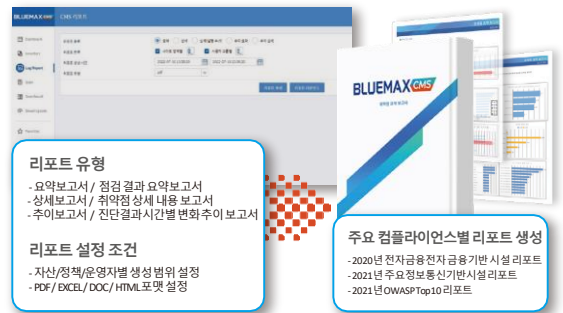
자산관리 직관적이고 간편하게 자산 관리 지원



진단수행 주요 법률에 기반한 완벽한 컴플라이언스 관리 기능



결과보고 자산 및 운영자에 따라 다양한 리포트 생성 지원



지원 플랫폼

	점검 방식	Agent, Agentless, 수동 점검
	점검 정책	CVE : 주요정보통신기반시설, 전자금융기반시설, 개인정보보호법, ISMS-P, ISO/IEC27001 해외법규, OWASP, 산업군별 특화 CVE : 최신 보안 취약점 1만 8천 개 이상 지원
	OS	Linux, Solaris, AIX, HP-UX, Windows Server, Windows PC
	DB	Oracle, MSSQL, MariaDB, MySQL, PostgreSQL, Altibase, MongoDB, DB2, Tiberio
	WEB	Apache, IIS, Tomcat, WebLogic, NGINX, WebtoB, JEU, Jboss, OHS, Resin, Node.js, Django
	NETWORK	CISCO, JUNIPER, Alton, PASSPORT, PIOLINK

CERTIFICATIONS



시큐아이 공인 총판 | 02-525-0481
 쿠도커뮤니케이션(주) | secure@cudo.co.kr

BLUEMAX LMS

최신 빅데이터 기술을 기반으로 대용량 로그에 대한 신속하고 안정적인 분석 및 수집능력을 제공합니다. 또한 직관적인 모니터링 기능을 통해 더욱 편리한 로그 관리가 가능합니다.

BLUEMAX LMS 특징점



하이브리드 데이터베이스

SQL과 No-SQL을 모두 지원합니다. 단일 플랫폼 내에서 동일 데이터로 비정형/정형 분석을 상호보완적으로 운영하여 정확성을 확보합니다.



스마트한 데이터 처리

샘플로그 등록 및 필드 구분 기능과 사용자 정의 필드 생성 기능으로 로그 파서 및 태깅 작업의 편의성을 제공합니다.



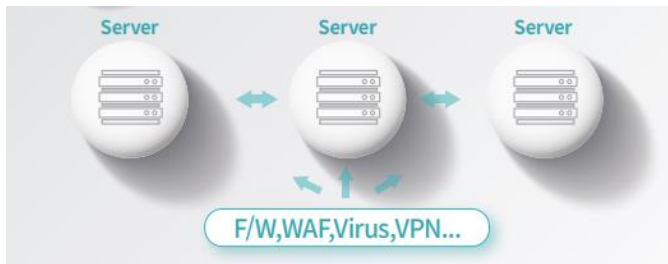
통합분석

인프라 전반의 보안 위협에 대한 가시성 확보를 위해 로그와 네트워크 패킷 분석을 지원합니다. 장비와 플로우를 통합하고 연관하여 분석합니다.

주요 기능

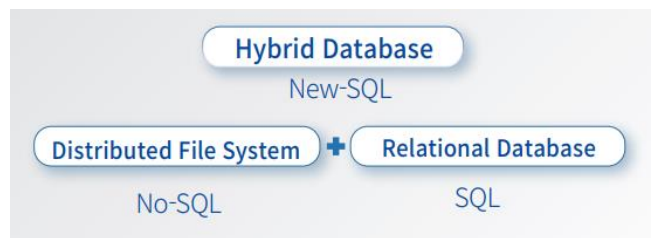
빅데이터 기반 처리

빅데이터 분산처리엔진을 통한 분산수집/저장/검색/분석으로 신속한 분석과 실시간 데이터 처리를 제공하고 수집 서버별 데이터 동기화와 밸런싱을 통해 고가용성을 확보합니다.



하이브리드 데이터베이스

결과에 영향을 주는 Key Factor를 도출하고 상관관계를 분석하는 비정형 분석과, 분석된 상관관계를 데이터 모델로 정립하고 실데이터를 정형모델에 적용하여 분석하는 정형 분석을 복합적으로 운영합니다



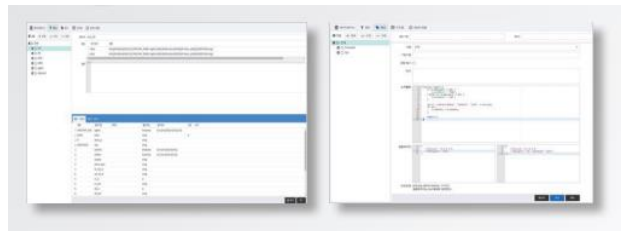
로그 및 네트워크 패킷 통합 분석

인프라 전반의 보안 위협에 대한 가시성 확보를 위해 로그와 네트워크 패킷 분석을 지원합니다. 보안장비, Flow, Payload, 네트워크장비를 통합/연관 분석하여 학습모델을 만들고 관리하며 적용합니다.



스마트 파서 & 태깅

샘플 로그만으로 필드를 구분하고 Pre-defined 정규식을 통해 로그데이터를 자동 인지하는 스마트 파서 기능과 사용자 정의 추가 필드 생성으로 분석 필요 정보를 원시 로그에 자동 변환 및 추가하는 스마트 태깅 기능을 통해 작업 편의성을 제공합니다



제품 구성도

로그 통합관리를 위한 Scale-out, 부하분산, 데이터 동기화 등 최신 빅데이터 처리기술을 적용한 아키텍처



제품 구성 요소

	Composition	Description
Server	BLUEMAX LMS AC	Analytics Server
Distribution	BLUEMAX LMS DM	Distribution Manager
Collector	BLUEMAX LMS DC - 0150	Data Collector (1 GB/Day & 5 Devices)
	BLUEMAX LMS DC - 1000	Data Collector (10 GB/Day)
	BLUEMAX LMS DC - 0010	Data Collector (10 Devices)



시큐아이 공인 총판
쿠도커뮤니케이션(주)

02-525-0481 | secure.cudo.co.kr | www.cudo.co.kr | blog.naver.com/cudo_cybersecurity | seucre_mkt@cudo.co.kr
Copyright CUDO Communication. All rights reserved.