SECURITY
SOLUTION
GUIDE

SECUI Security Solution Guide ver. 1.0
시큐아이 제품 및 서비스 가이드
제작 : ㈜ 시큐아이 편집 : 마케팅기획팀 발행 : 2026.8

SECUI

Youtube Linkedin

서울특별시 종로구 종로 51 3~6F(종로2가, 종로타워)
대표전화 02 3783 6600 **홈페이지** www.secui.com

SECURITY SOLUTION GUIDE

시큐아이 제품 및 서비스 가이드

Second Edition

SECUI

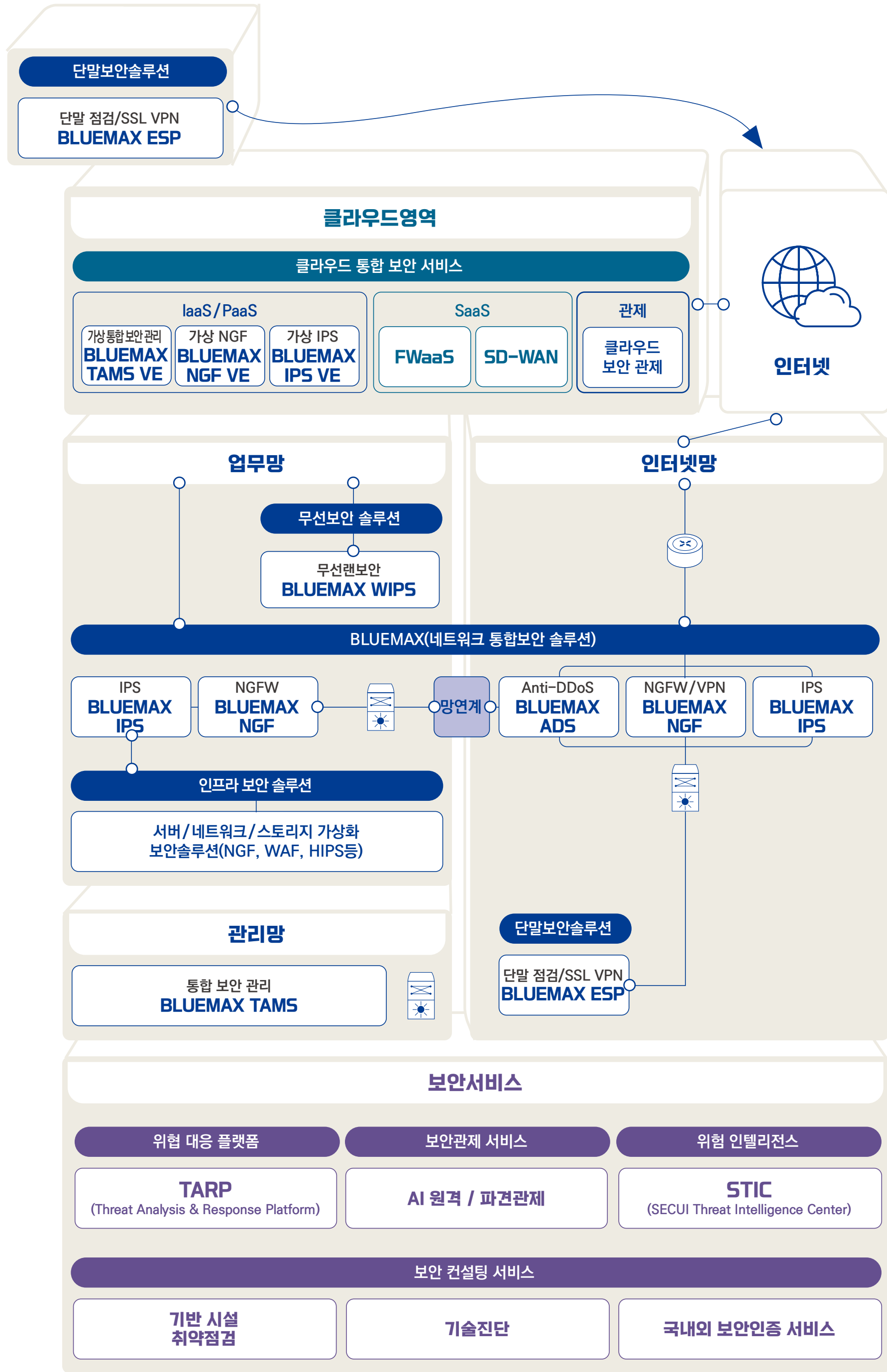
SECURITY SOLUTION GUIDE

시큐아이 제품 및 서비스 가이드

Second Edition

SECUI

Table of Contents



SECUI

SECUI
01 회사 소개

㈜**시큐아이**(대표 정삼용, www.secui.com)는 대한민국을 대표하는 네트워크 보안 기업으로 뛰어난 기술력과 전문적인 제품 및 서비스 역량을 갖춘 글로벌 기업입니다. 시큐아이는 국내 제1호 정보보호 전문 서비스 기업이라는 자부심으로 고객의 안전한 비즈니스 환경을 구현하기 위해 최선을 다하고 있습니다.
시큐아이는 20년 이상 쌓아온 보안 노하우를 기반으로 국내 보안 기업 선두에 서서 시장을 개척해 왔습니다. 그 결과 설립 이래 지속적인 매출 성장을 이루며, 대한민국 1위 보안 기업으로 고객들에게 인정받고 있습니다.
국내 최초 차세대 방화벽인 BLUEMAX NGF를 시작으로 차세대 침입 방지 시스템 BLUEMAX IPS, 무선 침입 방지 시스템 BLUEMAX WIPS를 제공하고 있습니다. 또한 급변하는 디지털 환경에 맞추어 고객들의 정보 자산을 지킬 수 있는 새로운 보안 솔루션을 지속적으로 선보이고 있습니다.
또한 국내 네트워크 보안 1위 기업의 노하우로 클라우드 보안 서비스인 SASE(Secure Access Service Edge)를 시장에 선보이고 있으며, FWaaS(Firewall as a Service)를 시작으로 클라우드 환경에서도 고객의 자산을 안전하게 지키고 있습니다.
이러한 전문적인 기술 노하우로 보안 컨설팅과 보안 관제 등 전문 보안 서비스를 제공하는 시큐아이는 On-Premise, Cloud 서비스가 모두 융합된 새로운 보안 패러다임을 선도하고 있습니다.
대한민국 대표 보안 전문 기업 시큐아이는 글로벌 수준의 경쟁력을 기반으로 일본, 베트남, 인도네시아 등 해외 시장에서도 성과를 내고 있으며, 대한민국의 위상을 높이기 위해 시장을 적극적으로 확대해 나갈 계획입니다.

회사명	㈜시큐아이	사업 분야	네트워크 보안 솔루션 클라우드 보안 솔루션 정보보호 컨설팅 보안 관제 서비스
CEO	정삼용		
설립일	2000년 3월		

SECUI
02 RECORDS

해외 시장
51개국

국내 네트워크 보안 15년 연속 1위
15years
IDC 기준

누적판매
170,000대

방화벽 국내 점유율
42%
나라장터 국가종합전자조달 기준

SECUI

03 인증 현황 ('26년 2월 기준)

CC(Common Criteria) 인증	GS(Good Software) 인증
• BLUEMAX NGF • BLUEMAX IPS • BLUEMAX ADS • BLUEMAX TAMS • BLUEMAX WIPS	• BLUEMAX Client for SCAN V2.5 • BLUEMAX NGF • BLUEMAX IPS • BLUEMAX ADS • BLUEMAX TAMS • BLUEMAX WIPS • BLUEMAX ESP

IPv6 TTA 인증	IPv6 Ready Logo
• BLUEMAX NGF 전 모델 • BLUEMAX IPS 전 모델 • BLUEMAX ADS 전 모델	• SecuiOS v5.0 – BLUEMAX IPS – BLUEMAX ADS • SecuiOS v4.0 – BLUEMAX NGF

SECUI

04 주요 특허 취득 현황 ('26년 2월 기준)

국내 / 외 187개의 네트워크 및 IT관련 기술 특허 최다 보유

날짜	발명의 명칭
2022.02	특허 제 10-2359805 호 : 센싱 장치, 센싱 장치를 포함하는 무선 침입 방지 시스템 및 그것의 동작 방법 외 1건
2021.01	특허 제 10-2203828 호 : 네트워크 보안 장치 및 방법
2020.09	특허 제 10-2157661 호 : 무선 침입 방지 시스템 외 2건
2019.09	특허 제 10-2026447 호 : 가상 네트워크를 위한 오프로드 장치 및 방법 외 4건
2019.07	특허 제 10-1997211 호 : 네트워크 보안 장치 및 그의 공격 탐지 방법
2019.05	특허 제 10-1976794 호 : 네트워크 보안 방법 및 그 장치
2019.03	특허 제 10-1959440 호 : 네트워크 보안 장치 및 그의 트래픽 처리 방법 외 1건

01

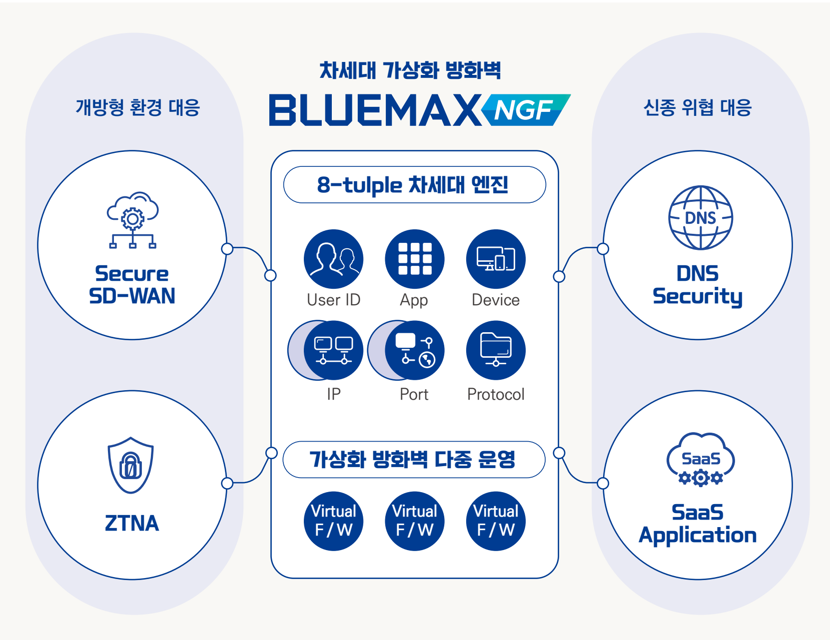
Network Security

네트워크 보안 솔루션

BLUEMAX NGF

15년 연속 국내 시장 점유율 1위, 차세대 가상화 방화벽

클라우드, 모바일 등 새로운 업무 환경의 확대로 시스템과 사용자는 기존의 관문 중심 환경에서 개방적인 환경으로 변화하고 있습니다. 차세대 방화벽 BLUEMAX NGF는 개방형 네트워크 환경과 가상화 지원으로 고도화된 사이버 위협에 대응하는 통합 보안 플랫폼입니다.
이를 통해 개방형 네트워크 환경 및 가상화 환경에서의 고도화된 사이버 위협에 안정적으로 대응합니다.
특히 가상화 기능을 통해 단일 제품으로도 다수의 방화벽 운영이 가능하며 안정된 고성능, 고가용성 HW 아키텍처와 애플리케이션 인지, 디바이스 인지 등 차세대 방화벽 기능과 SD-WAN 환경 지원, DNS/VPN의 최신 위협 대응을 위한 보안 기능을 모두 제공합니다.



BLUEMAX NGF V3.0 New Feature

01

BLUEMAX NGF

특장점

Virtual System
- 단일 물리적 장비 내 여러 대의 가상 방화벽 동시 운영 가능
- 토폴로지 에디터로 가상 방화벽, 스위치, 라우터의 편리한 구성 관리

Secure SD-WAN
- 애플리케이션 기반 라우팅 기능 제공
- 회선에 대한 품질 상태 체크를 통한 안정적이고 최적화된 서비스 제공

ZTNA 환경 지원
- BLUEMAX ESP 기반 위협 정보 수집 및 방화벽 정책 연동
- 외부 사용자에 대한 생체인증, OTP 인증으로 신원 확인 강화

애플리케이션 인지
- 3,300개 국내 최대 애플리케이션 인식 지원
- SaaS 전용 애플리케이션의 계정별 접근 제어 제공

VPN 보안 강화
- 국제 공인 차세대 암호 기술 양자 내성 암호화(PQC) 알고리즘 탑재
- Group VPN 지원으로 관리 편의성 향상

ML 기반 DNS 보안 강화
- 악성 및 비정상 DNS 트래픽 검사
- Machine Learning 및 평판 기반 탐지 엔진 탑재로 보안성 강화

정책 운영 편의성
- 기간별 방화벽 정책 탐지 횟수 및 초기화 제공
- 만료, 중복, 미사용 정책에 대한 검사 기능을 통한 정책 최적화

유연한 제품 연동
- Open API를 제공하여 이기종 시스템들과 다양한 정책 제어 및 로그 데이터 연동 가능

BLUEMAX NGF
02 주요 기능

구분	상세 내용	
NGFW	• 사용자 기반 정책 제어 • 애플리케이션/디바이스 기반 정책 제어 • AD SSO 연동을 위한 AD 설정 마법사 • 애플리케이션별, 사용자 ID 별 QoS	• 자체 사용자 인증(Captive Portal) 및 SSO 지원 • SaaS 애플리케이션 제어 • OT 프로토콜 인지 및 접근 제어
Virtual System	• Virtual System 별 자원 할당 • 관리자별 독립적인 운영 환경	• 토폴로지 맵으로 직관적 가상 네트워크 구성
APT 대응	• Sandbox 장비 연동한 APT 위협 분석 기능 제공	• 탐지된 위협 정보에 대한 공유 체계 지원
SSL Inspection	• HTTPS, SMTPS, POP3S, IMAPS, FTPS • Hardware Acceleration	• APP Control, IPS, DLP, Web Filter 기능 및 외부 장비와 복호화 트래픽 연동
Legacy Firewall	• Active-Active HA with L2/L3/L4 • 도메인 정책(URL 객체) • 중복 정책 및 미사용(미참조) 정책 검사 • Policy-based NAT & Interfaced-based NAT • 정책 타임라인 관리 및 롤백	• 보안 정책 그룹 설정 • 보안 정책별 활성화 스케줄 • VXLAN 패킷 제어 정책 • 머신러닝 기반 DNS 위협 탐지 • 정책 설정 화면과 로그 조회/분석 기능 연계
IPS	• 프로파일 기반 시그니처 템플릿 • PCRE(정규표현식) • 사용자 정의 시그니처 검증 기능	• 멀티패턴 탐지 기능(병렬 탐지) • 취약점 점검 도구 연동, 시그니처 최적화
Anti DDoS	• 응용계층 방어 • 행위 기반 웹 공격 방어, DRDoS(N:1) 방어	• 스마트 패턴 학습 방어
IPSec VPN	• IKE(v1/v2), PKI(x509) • GRE/IPIP, L2TP, PPTP Tunneling • 3DES, AES, SEED, ARIA, LEA, CAST, Blowfish, SHA-1, SHA-256, SHA-512, HAS160 등	• Group VPN 기능 • 양자 내성 암호화 PQC (Post Quantum Cryptography) 알고리즘 탑재 • 회선 장애 감지 기능
SSL VPN	• Full Tunnel mode • Multi-Factor 인증 지원(3차 인증)	• FIDO 생체인증 • PASS 앱 기반 간편 인증

BLUEMAX NGF
02 주요 기능

구분	상세 내용	
Anti-Virus & Anti-SPAM	• Anti-Virus Engine (File-based or Stream-based)	• Realtime Blackhole List(RBL) • 수신자 수 제안, 대량 메일 발송 제안
Web Filter	• URL Filtering(카테고리별 설정) • URL 확장 검사(URL 쿼리 검사) • Global Categorized URL (로컬/클라우드 DB)	• 경고페이지 설정 및 편집 • IP 주소 도메인 차단 • HTTP 헤더 제어 • Anonymizer 서버 목록 차단
DLP	• HTTP/HTTPS, FTP/FTPS, SMTP/ SMTPS, POP3/POP3S, IMAP/IMAPS • 웹메일을 통한 정보 유출 제어 • 주민등록번호, 카드번호 등록/검사 및 차단	• 범용파일 포맷 39가지 이상 • 압축파일 (ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP) • 필터 및 저장(아카이브)
Device 제어	• SSL VPN Client (Windows, Linux, Android, iOS) • 단말 보안 정보 수집(업데이트, 보안 설정)	• Compliance 점검을 통한 단말 보안 상태 정보 제공
네트워크	• LACP, VLAN, 동적 자산 제어 • IPv6 트랜지션(설정 터널링, 6to4) & 트랜슬레이션(NAT64, DNS64), NAT46 • DHCP, DHCPv6 및 RA 서버	• QoS(IP, Application, 인터페이스별) • Routing Protocol(IPv4-OSPF/RIP/ BGP, IPv6-OSPFv3/RIPng/BGP4+) • DNS, DDNS, Split DNS
모니터링	• SNMP(v1, 2, 3), Syslog 전송 • DB 기반 로그 관리(압축 지원) • 경고 알람 임계치 설정	• Report(정책 상세, 리포트브라우저) • 애플리케이션, 사용자별 트래픽/ 세션 모니터링
관리 기능	• Firmware Upgrade and Downgrade (Rollback) • Setup Wizard, 설정 Multi R/W (Read/Write) • GUI 상에서의 CLI 실행 및 Packet Capture	• LDAP/RADIUS/TACACS+/OTP 등 관리자 접속 • 관리자 권한 프로파일 • Open API, 기타 외부 솔루션 연동 • 보안 컴플라이언스 자체 점검 지원
SD-WAN	• 애플리케이션 기반 트래픽 경로 설정 • ZTP(Zero Touch Provisioning)	• 회선 품질 기반 트래픽 경로 설정 ('24년 하반기 예정)

BLUEMAX NGF

03 제품 사양

SMB, Mid-Biz

BLUEMAX NGF		50	60	100	110	200	310	510	1100
CPU		2 Core	3 Core	2 Core	4 Core	4 Core	4 Core	8 Core	4 Core
Memory		4 GB	4 GB	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB
Storage	System	SSD 16 GB	SSD 16 GB	SSD 16 GB	SSD 32 GB	SSD 32 GB	SSD 64 GB	SSD 128 GB	SSD 128 GB
	Log	–	–	–	–	–	SSD 1 TB	SSD 1 TB	SSD 1 TB
Interface	1GF	–	–	–	–	–	–	4	4(max8)
	1GC	4	4+4 (switch)	4+4	4+8 (switch)	4+8	8	8	8
Power Supply		Adapter	Adapter	Adapter	Adapter	Adapter	Single	Single	Single
Throughput		1 Gbps	1.5 Gbps	2 Gbps	3 Gbps	4 Gbps	8 Gbps	12 Gbps	16 Gbps

Enterprise Carrier

BLUEMAX NGF		1300	1510	2100	5100	20000
CPU		4 Core	10 Core	20 Core	32 Core	48 Core
Memory		8 GB	16 GB	32/64 GB	64/128 GB	96/288 GB
Storage	System	SSD 256 GB	SSD 256 GB	SSD 128 / 256 GB	SSD 128 / 512 GB	SSD 128 / 512 GB
	Log	SSD 1 TB	SSD 1 TB	SSD 1.92 TB/RAID	SSD 1.92 TB/RAID	SSD 1.92 TB/RAID
Interface	100GF	–	–	–	(max2)	(max4)
	40GF	–	–	(max4)	(max8)	(max8)
	10GF	(max4)	(max4)	2(max10)	10(max26)	10(max26)
	1GF	4(max8)	4(max8)	8(max40)	8(max40)	8(max40)
	1GC	8	8	8(max40)	8(max40)	8(max40)
Power Supply		Redundant	Redundant	Redundant	Redundant	Redundant
Throughput		18 Gbps	40 Gbps	80 Gbps	160 Gbps	320 Gbps

BLUEMAX NGF

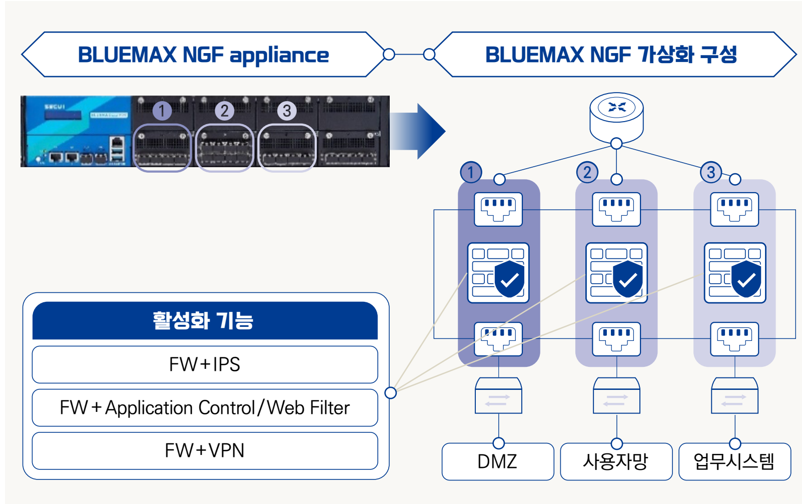
04 구성 사례

Virtual System 구성 사례

기업의 내부 자산이 늘어나면서 복잡한 네트워크 보안 구성이 증가하고 있으며,
이로 인한 구축 비용은 지속적으로 증가하고 있습니다.

구성 방식

- 단일 물리적 장비 내 여러 대의 가상 방화벽 동시 운영 가능
- 토폴로지 에디터를 활용한 간단한 인터페이스만으로 가상 방화벽 설정 가능
- DMZ, 사용자망, 업무 시스템에 따라 물리적으로 독립된 가상 방화벽을 구성하고 보호 대상에 맞는 보안 기능을 활성화



Virtual System 구성 시 효과

- 구축 비용, 상면 적 75% 절감 가능
- 구성 단순화로 장애 요소 저감
- 통합 및 개별 관리 편의성 동시 확보 가능
- 보호 대상에 보안 기능 활성화로 최적화된 운영 가능

BLUEMAX NGF

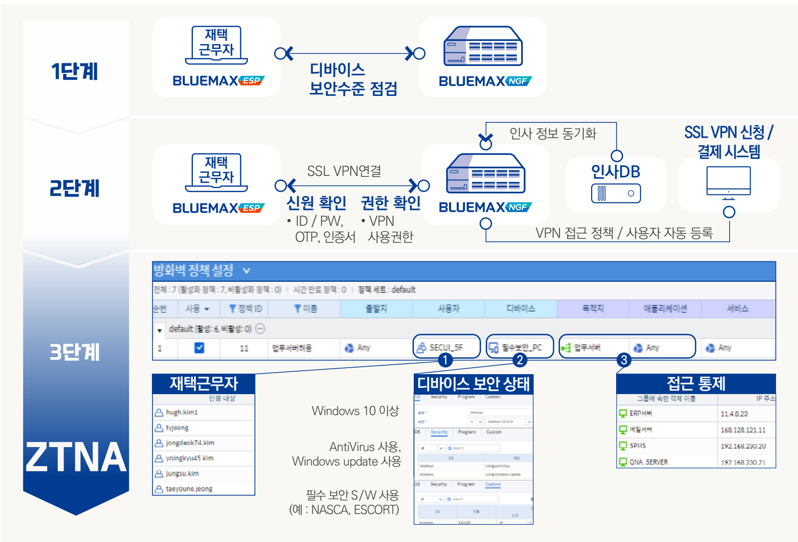
04 구성 사례

ZTNA 재택근무 보안 구성 사례

기존 기업들의 정보 자산은 기업 내부에 존재했습니다. 이를 보호하기 위해 고객들은 네트워크 경계선 중심의 보안을 중점적으로 생각했습니다.
그러나 최근 디지털 대전환으로 기업의 정보 자산이 확장되고, 원격 근무의 확산으로 기존의 경계선 중심의 보안으로는 완벽한 보안을 이룰 수 없습니다.
BLUEMAX NGF는 사용자 인증, 디바이스 인증, 시스템 제어 연동을 통한 완벽한 Zero Trust를 적용한 차세대 방화벽입니다.

ZTNA 구성을 위한 단계별 절차

- **[1단계]** 재택근무자 디바이스 보안 신뢰성 점검
- **[2단계]** NGF-인사 정보 시스템 연계한 재택근무 사용자 인증
- **[3단계]** 디바이스 보안 상태 기반 접근 제어를 통해 안전한 단말만 접근 허용



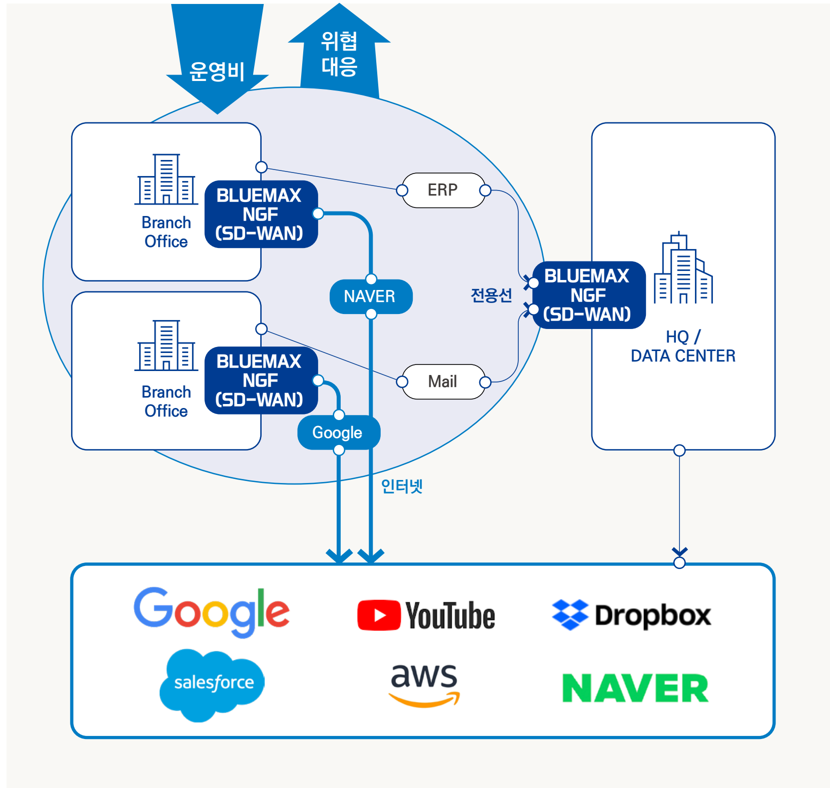
기대 효과

- 원격 연결 전 단말 상태 점검을 통한 안정성 사전 판단 가능
- 정보 유출 및 악성코드 내부 유입 사전 방지
- 보안 상태가 양호한 단말에 대해서만 기업 내부 접근 가능

BLUEMAX NGF

04 구성 사례

다지점 Secure SD-WAN 구성 사례



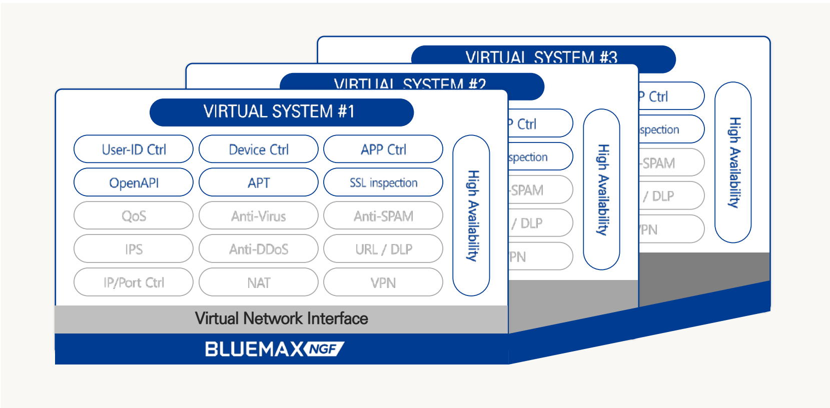
기대 효과

- 차세대 방화벽에서 제공하는 IPS, 웹필터 등 보안 기능으로 다지점에 대한 최신 보안 위협 대응 가능
- 애플리케이션 기반 회선 분배로 지점의 전용선 비용 절감
- Zero-Touch Provisioning 지원하여 지사 장비 설치 및 운영비 절감

05 우수 도입 사례

우수 도입 사례

고객사에서는 차세대 보안 인프라를 새롭게 구축하면서 ZTNA(Zero Trust Network Access) 보안 전략을 위한 마이크로 세그멘테이션(Micro-Segmentation)을 검토하고 있었습니다. 마이크로 세그멘테이션을 위해서는 다수의 방화벽이 필요하나, 다수의 어플라이언스 방화벽 제품을 도입하는 것이 간단하지 않기 때문에 고민하고 있었습니다.
BLUEMAX NGF 제품은 가상화 방화벽(Virtual System) 기능으로 마이크로 세그멘테이션을 위한 다수의 방화벽이 필요한 요구조건에 유연하게 대응할 수 있어서 가상화 방화벽 구축을 제안 드렸으며, 고객사에서도 가상화 기능에 관심이 있었던 상황이라 BLUEMAX NGF의 가상화 방화벽을 도입하여 신규 보안 인프라를 구축하기로 했습니다.



최신 기술을 활용한 가상 환경 지원

- 간편한 가상 시스템 생성 / 가상 시스템 별 자원 할당

다양한 Virtual Network 구성 지원

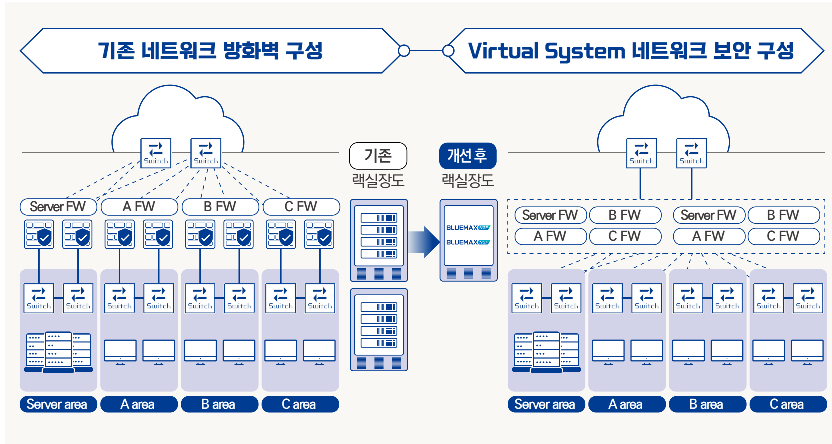
- Real NIC와 다양한 네트워크 연결
- Virtual Switch/Router로 다양한 네트워크 구성

독립된 Virtual System 자원 할당

- 시스템 자원(CPU, Memory 등)을 유연하게 개별 할당하여 완벽한 독립 운영

05 우수 도입 사례

기존의 방화벽 구성 방식은 물리적 서버나 네트워크 장비의 한계로 확장이 제한될 수 있는 반면, 가상화 기반의 방화벽은 필요에 따라 리소스의 확장이 가능하고 변화하는 IT 인프라 환경에 유동적으로 대처할 수 있습니다. 따라서, 트래픽이 지속적으로 증가하고, 다양한 보안 위협이 등장하는 개방형 네트워크 환경에 훨씬 적합한 방식이라고 할 수 있습니다.
시큐아이는 고객사 기존 장비의 스펙과, 향후 트래픽 증가 등을 고려하여, 엔터프라이즈 급인 BLUEMAX NGF 5000 모델 2대와 BLUEMAX NGF 2000 모델 2대를 통해 다수의 가상화 방화벽을 구축했습니다.



BLUEMAX NGF의 도입은 효율성 측면에서도 많은 효과가 있습니다.기존의 복잡한 네트워크 보안 구성을 버츄얼 시스템으로 구성하면서 구축 비용과 랙의 상면적을 절감하였습니다. 특히 상면적의 경우 약 75% 가까이 줄어들었으며, 중소형 망으로 분산 구축된 망을 통합하면서 전력소비효율도 약 10% 이상 개선하였습니다.
가상화 지원으로 다양한 구성이 가능한 BLUEMAX NGF를 도입한 고객사에서는, 팬데믹 이후 늘어난 트래픽과 새로워진 IT업무 환경에 문제없이 대처할 수 있었고 현재까지 추가적인 확장이나 교체 없이 안정적으로 운영되고 있습니다. 해당 고객사에 가상화 방화벽 도입 이후 여러 국내, 해외 기업에서 시큐아이의 가상화 방화벽 신규 도입을 검토 중에 있습니다.
시큐아이는 고객사가 BLUEMAX NGF를 포함한 다양한 정보보호시스템을 선택하고 사용하시는 모습을 가장 가까이에서 지켜보고 있습니다. 앞으로도 고객들의 소중한 IT 자산이 안전하게 보호되고, 업무와 운영의 효율성을 높일 수 있도록 시큐아이가 함께 하겠습니다.

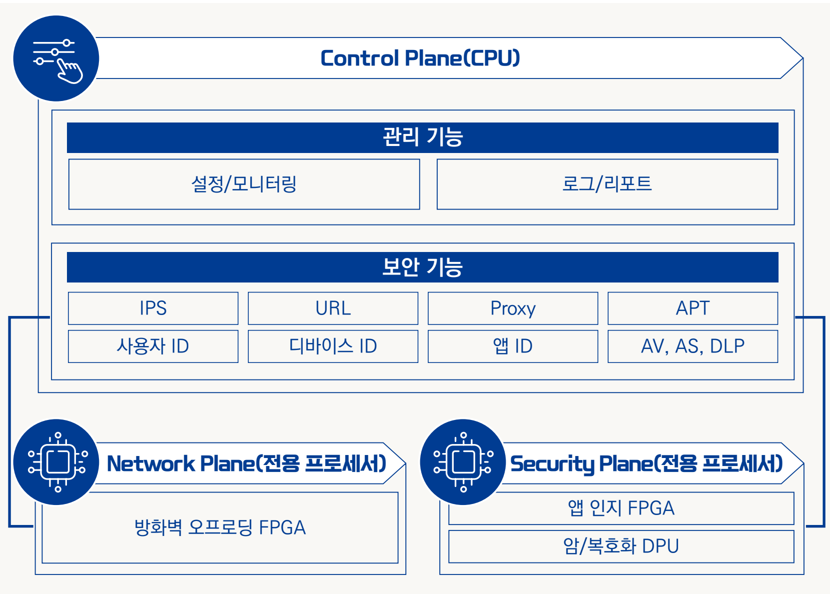
BLUEMAX NGF PRO

고성능 프리미엄 방화벽

BLUEMAX NGF PRO는 고성능과 AI 기반 위협 대응력을 갖춘 프리미엄 방화벽 입니다. 고속 패킷 처리 전용 프로세서를 탑재하여 기존 CPU 기반 방화벽의 한계를 뛰어넘어 고성능 패킷 처리와 고도화 된 위협 탐지를 제공합니다.

방화벽 오프로딩 FPGA와 앱인지 FPGA로 고속 패턴 매칭을 통해 학습 된 세션에 대해 CPU의 부하를 줄이고, 암복호화 DPU를 통해 HTTPS 패킷에 대한 암복호화 속도를 크게 향상 시켰습니다.

경량화된 인라인 머신러닝 엔진을 통해 악성 파일을 탐지하고 AI 기반 위협 분석 서비스와 연계하여 신규 위협을 탐지합니다.



고속 패킷 처리 전용 프로세서 아키텍처

01

BLUEMAX NGF PRO

제품 사양

레거시 라인업

BLUEMAX NGF PRO		3000B	5000B
CPU		24 Core	32 Core
Memory		128 GB	256 GB
Storage	System	SSD 256 GB	SSD 256 GB
	Log	SSD 1.92TB(RAID)	SSD 1.92TB(RAID)
Interface	40GF/100GF	6	6
	1GF/10GF	18	18
	1GC	8	8
Power Supply		Redundant	Redundant
Firewall		190 / 160 Gbps (UDP 1518B / 64B)	390 / 320 Gbps (UDP 1518B / 64B)
SSL Inspection / Latency		–	–
Latency		4.0 ㎲	4.0 ㎲

차세대 라인업

BLUEMAX NGF PRO		3000	5000
CPU		32 Core	48 Core
Memory		256 GB	256 GB
Storage	System	SSD 256 GB	SSD 256 GB
	Log	SSD 1.92TB(RAID)	SSD 1.92TB(RAID)
Interface	40GF/100GF	6	6
	1GF/10GF	18	18
	1GC	8	8
Power Supply		Redundant	Redundant
Firewall		60 Gbps (App-Ctrl 64KB)	100 Gbps (App-Ctrl 64KB)
SSL Inspection / Latency		6 Gbps	11 Gbps
Latency		–	–

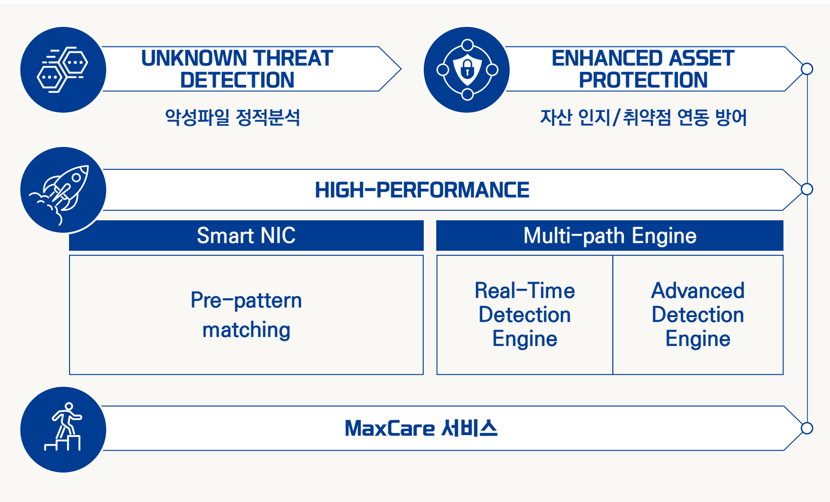
※ 본 제품 사양은 출시 시점 및 SW업데이트에 따라 변경될 수 있습니다.

BLUEMAX IPS

차세대 IPS (침입방지시스템)

4차 산업혁명으로 인한 클라우드/5G 확산과 온라인 플랫폼 산업의 급성장으로 트래픽 사용량은 나날이 급증하고 있으며, 멜웨어 기반의 Zero Day 공격이 더 지능화되고 대형화되고 있습니다. 이를 위해 BLUEMAX IPS는 고성능 위협 차단 플랫폼 기반으로 악성 트래픽 및 파일을 검사하고, 내부 자산 취약점 점검 결과와 연동하여 선제적 맞춤형 대응 체계를 제공합니다.
운영자의 업무 피로도와 운영 시간을 절약하는 MaxCare 서비스, 이벤트 분석/탐지 보고서를 제공하는 원클릭 이벤트 분석 서비스 등 국내에서 가장 선도적인 IPS 전문 서비스를 제공합니다.

시장 요구사항에 맞춰 시큐아이는 대량의 트래픽을 실시간으로 처리할 수 있도록 BLUEMAX IPS 제품에 고성능 위협 차단 플랫폼을 적용했습니다.
유입되는 트래픽 중 하드웨어 패턴 매칭을 통해 위협이 의심되는 패킷을 실시간으로 구분하는 'Smart NIC', Smart NIC에서 위협이 의심되는 패킷으로 분류된 트래픽을 다양한 보안 위협으로부터 신속하게 탐지 및 차단하는 'Multi-path 엔진'이 BLUEMAX IPS에 적용된 고성능 아키텍처의 핵심입니다.



BLUEMAX IPS의 Proactive Threat Response 아키텍처

01 BLUEMAX IPS 특장점

고성능 Smart NIC
- 하드웨어 패턴 매칭을 통해 위협이 의심되는 트래픽을 실시간 대응
- IPS의 리소스를 효율적으로 사용하여 트래픽을 고속으로 처리

Multi-path 엔진
- Real-Time 엔진 기반 실시간 위협 방어
- Advanced 엔진 기반 세션 및 파일 위협 방어

시그니처 기반 방어
- 제조사의 정제된 10,000개 이상의 IPS 시그니처 제공
- 국내 최대 Snort 옵션 지원
- 사용자 정의 시그니처 입력 오류 방지 기능 지원

악성파일 정적/동적 분석 지원
- 평판 분석, YARA 탐지 Rule, 악성 Script 탐지, Anti-virus 엔진을 통한 악성 파일 검사 및 탐지 기능 제공

선제적 보안 위협 대응
- 위협 인텔리전스 플랫폼인 STIC을 활용하여 글로벌 TI 정보 수집
- 위협 대응센터 및 AI 보안관제센터의 심층분석 체계로 양질의 보안 위협 대응 정보 제공

효율적인 유해사이트 차단
- 카테고리별 URL 분류에 따른 비업무/유해 사이트를 차단하는 웹 필터 기능 제공
- 글로벌 Database 기반 강력한 접근 제어 정책 및 실시간 업데이트

원클릭 이벤트 분석 서비스
- 침해 대응센터로 탐지된 이벤트를 전송하여 이벤트 분석 결과 보고서 제공
- 로그 추출 과정 필요 없이 원클릭으로 IPS 장비에서 자동으로 추출 및 분석 의뢰

MaxCare 서비스
- IPS 도입 초기에 조기 안정화를 위한 IPS 최적화 서비스 제공
- 구축 후 정책 최적화, 매월 2회 심층 보안 정보 제공, 3개월마다 운영 가이드 제공

BLUEMAX IPS

02 주요 기능

구분	상세 내용	
Application Awareness	• HTTP, FTP, POP3, IMAP, SMTP, IP, TCP, ICMP, IPv6 비정상 프로토콜 탐지 • 웹 메일, 메신저별 세부 기능 제어	• App 탐지/제어/차단 동작 지원 • 네트워크 트래픽 내 App 정보 인지
Context Awareness	• 네트워크 내 사용자 / 자산정보 수집 및 네트워크 내 토폴로지 제공 • 외부 장비/DB시스템과 사용자 정보 연동 • 취약점 진단 솔루션 – 시그니처 정책 연계 • 평판 3rd Party 연동 (IP, URL) • IP, URL 평판 DB 사용자 정의 • 클라우드 기반 외부 악성 URL 검사 지원	• 국가/지역별 제어 기능 제공 • 행위분석 기능을 통한 신변종 유형 대응 • 악성 유형에 대한 보고서 및 정보 제공 • IP, URL 차단 • Anti-Virus, YARA 룰 지원 • 다중, 암호화된 압축 파일 해제 지원
Legacy Rule	• 사용자 정의 Snort Rule • PCRE(정규표현식), YARA 룰	• 멀티패턴 탐지 기능(병렬 탐지)
Anti-DDoS	• DoS, DDoS, DRDoS 방어 • HTTP, DHCP, SMTP, POP3, IMAP, SIP 방어	• 발신 기반 세션 제어 • 패턴 학습 방어 • 트래픽 학습 방어
SSL Inspection	• 양방향 트래픽 복호화 지원 • SSL 트래픽 자동 인지 • DHE/ECDHE 지원 • SSL 예외 정책 지원(5-tuple/SNI/CN)	• TLS 1.3 지원 • SSL/TLS 버전 제어 • 사설 인증서 제어 • SSL 트래픽 Cipher-Suite 제어
Security Setting & Interworking	• 통합위협관리시스템 연동 • 위협 이벤트 및 로그 전송 • 원클릭 침해사고 분석 요청	• 상위기관 정책 동기화 • 블랙리스트 차단 지원 • 화이트 리스트 등록 예외 기능 제공
Log Monitoring	• 실시간 모니터링 제공(이벤트, System, Network, 장비 상태, 작업내역 등) • 실시간 HA 모니터링 지원 • 실시간 SSL 세션 현황 모니터링 지원 • 실시간 공격 순위 제공 • 사용자 정의 위젯 및 구성 가능	• 위협 탐지 및 차단 통합 • 탐지 및 차단 특화 상세 이력 제공 • 평판 탐지 결과 제공 • 로그/통계 도구 기능 • 로그/통계 가시성 및 사용자 편의성 강화 • 사용자 정의 트렌드 및 통계 기능 제공
Management Function	• 세그먼트, 네트워크 정책 설정 및 관리 • 네트워크 대역별 통계, 모니터링, 로그 지원 • VLAN, GRE, IPinIP, GTP, DHCP, IP(v4,v6), ICMP(v4,v6), IGMP, TCP/UDP 프로토콜 지원 • TCP 세션 관리 및 통계 기능 제공 • 시스템 운영 환경에 따른 설정 기능 제공	• 관리자 별 보안 기능 및 권한 유형 제공 • 감사 및 파일 복구 이력 제공 • 탐지 및 제어 방식 최적화 대역폭 보장 • 정책/동적 기반 QoS TCP Flag 관리 및 제어 기능(SYN, FIN, Rst, Psh, Ack) • 동적 QoS TCP/UDP/ICMP/ETC PPS 제어

BLUEMAX IPS

03 제품 사양

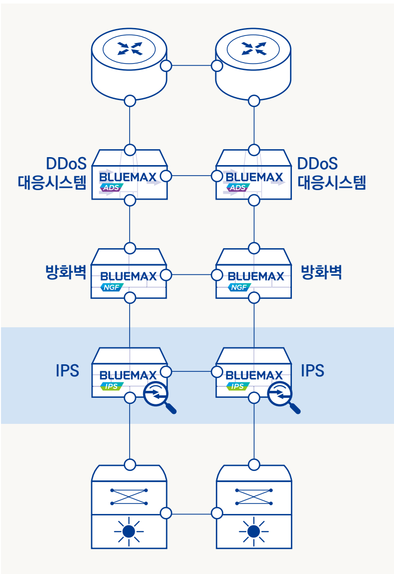
BLUEMAX IPS		1000	2000	4000	5000	10000	21000
CPU		4 Core	10 Core	10 Core	24 Core	52 Core	104 Core
Memory		32 GB	32 GB	64 GB	96 GB	192 GB	512 GB
Storage	System	SSD 32 GB	SSD 32 GB	SSD 32 GB	SSD 128 GB	SSD 128 GB	SSD 256 GB
	Log	HDD 1 TB	HDD 2 TB	HDD 2 TB	SSD 1.92 TB	SSD 1.92 TB	SSD 1.92 TB RAID
Interface	100GF (Smart NIC)	–	–	–	–	–	2(max4)
	100GF	–	–	–	–	–	(max4)
	40GF (Smart NIC)	–	–	–	–	(max4)	–
	40GF	–	–	–	(max4)	(max8)	–
	10GF (Smart NIC)	–	–	2	4(max8)	4(max8)	–
	10GF	–	–	(max4)	(max8)	(max8)	–
	1GF	(max4)	4(max8)	(max8)	(max12)	–	–
	1GC	4(max8)	(max8)	(max8)	(max12)	–	–
Power Supply		Single	Redundant	Redundant	Redundant	Redundant	Redundant
Throughput (UDP/64byte)		1 Gbps	2 Gbps	10 Gbps	20 Gbps	40 Gbps	100 Gbps
Throughput (UDP/MAX)		4 Gbps	10 Gbps	40 Gbps	80 Gbps	120 Gbps	200 Gbps

BLUEMAX IPS
04 구성 사례

BLUEMAX IPS는 사용자 네트워크 및 시스템 환경에 적합한 인라인(Inline), 탐지 모드(Tap) 방식의 유연한 구성 방식을 동시에 지원합니다.

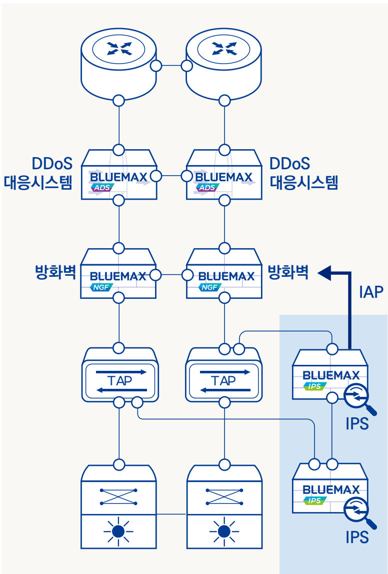
인라인(Inline)

- 일반적인 IPS 구성
- 네트워크 경로상에 직접 연결하여 공격 차단
- Bypass 및 LLCF(Link Loss Carry Forward) 기능 제공



탐지 모드(Tap)

- 미러링 구성으로 차단 정보를 다른 장비로 전송
- 서비스 연속성을 최우선으로 하는 구성에 적합
- IAP(Intrusion Alert Protocol) 연동으로 공격 차단



BLUEMAX IPS
05 MaxCare 서비스

MaxCare 서비스는 시큐아이만의 차별화된 고객 맞춤 서비스입니다.
IPS 도입 초기 운영의 혼란을 최소화할 수 있도록 IPS 전문 엔지니어가 구축 후 정책 최적화 서비스 제공합니다. 또한 매월 2회 신규 취약점에 대해 신속하게 대응할 수 있도록 심층 보안 위협 정보 제공하고, 3개월마다 운영 현황 분석을 통해 분석 내용에 따른 운영 가이드를 제공합니다.

구축 완료 후

보안정책 최적화

고객	구축은 완료되었는데, 정책은?
시큐아이	구축 완료 후 IPS 전문 엔지니어를 통한 정책 최적화 서비스를 제공합니다.

매월 2회

심층보안위협 정보 제공 서비스

고객	신규 취약점이 발표되었다는데, IPS에서 잘 방어하는지…
시큐아이	매월 2회의 신규 보안 위협분석 및 시그니처 대응 방안 제공합니다. (신규 위협에 대한 대응 방안 제공)

매 3개월마다

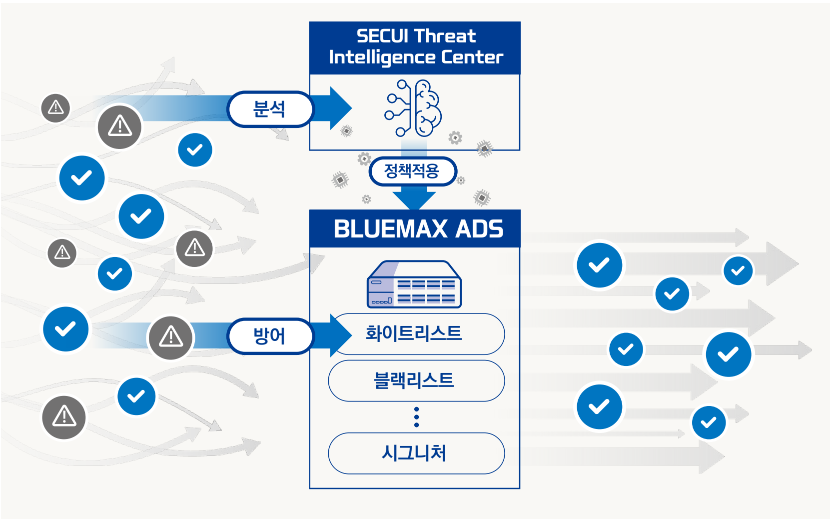
운영 점검 서비스

고객	정기적인 시스템 점검이 아닌 전체적인 위협 방어가 잘 되는지…
시큐아이	분기마다 시스템 점검 외에도 운영점검 서비스를 제공하여 탐지현황, 운영 가이드 제공합니다.

BLUEMAX ADS

DDoS 대응시스템

DDoS 대응시스템인 BLUEMAX ADS는 신속하고 정확한 공격 탐지와 대응을 위해 머신러닝 기술을 활용합니다. 시큐아이에서 수집한 글로벌 위협 정보를 머신러닝을 이용하여 정제합니다. 정제된 양질의 위협 정보는 실시간으로 배포하며, 악의적인 DDoS 공격에 선제적으로 대응합니다. 이를 통해 네트워크의 가용성과 안정성을 보장하며 서비스 연속성을 유지합니다. 지속적으로 학습하고 발전하는 BLUEMAX ADS는 다양한 DDoS 공격을 방어하고, 자산을 보호하기 위한 최고의 선택입니다.



머신러닝 기반 DDoS 방어 기능

BLUEMAX ADS

01

특장점

Technology

- 위협에 대한 정보를 수집, 머신러닝을 통한 분석 및 연동기반 DDoS 방어 정책
- Inline, Out-Of-Path 등 다양한 환경에서의 유연한 네트워크 구성
- 높은 신뢰성을 보장하는 인증 방어 기능으로 DDoS 공격 시에도 서비스 연속성 보장
- 자동으로 학습하고 제안하는 스마트한 DDoS 방어 체계

Defense-mechanism

- DDoS 공격의 특성에 맞춘 독자적인 다중 레이어 방어 메커니즘
- 신속하고 정확하게 다양한 유형의 DDoS 공격을 탐지 및 효과적 대응
- 효율적인 탐지와 신속한 차단으로 DNS 보안 위협에 빠르게 대응

High-performance

- 최신 하드웨어 플랫폼 적용으로 DDoS 공격에 안정적으로 대응하는 고성능 제품
- 다단계 QoS 기능으로 트래픽 최적화, 안정성과 신뢰성의 동시 확보

Analytics

- 사용자 중심의 인터페이스 및 위젯 제공으로 DDoS 공격 대응에 특화 된 직관적인 분석

Efficiency

- 사용자의 운영 편의성을 고려한 Lightning Fast 컨셉의 GUI 적용
- 원스텝으로 이벤트 인지, 분석, 대응 정책 적용을 지원하여 운영 효율성 극대화
- 리포트 관리 편의성 높여주는 리포트 브라우저

Support

- 정책 설정 화면과 로그 조회/분석 기능 연계
- 마우스 클릭 한번으로 신속하고 정확한 탐지 이벤트 분석 서비스
- 우수한 기능들을 손쉽게 연동하는 Open API

BLUEMAX ADS

02 DDoS 방어 기능

비정상 프로토콜 방어
TCP/IP 표준에 부합하지만, 보안 문제가 발생할 수 있는 패킷 탐지/차단

서비스 공격 방어
DoS, DDoS, DRDoS 공격 등에 대한 방어

접근 차단 / 시스템 격리
5 Tuple 기반 패킷 탐지/차단

사전에 확인된 공격자 정보기반 임시적으로 차단/격리

정책 예외
화이트리스트 기반 DDoS 방어 기능 검사 예외

국가 방어
특정 국가로부터 DDoS 공격이 발생하는 경우, 해당 국가 트래픽 차단

학습 방어
패킷 데이터 기준 패턴 정보를 추출하고 패턴 매칭 기반 탐지/차단

학습 데이터 기반 임계치 기준 이상 트래픽 탐지/차단

사용량 제한
정책 기반 임계치만큼의 트래픽만 허용

QoS 기반 TCP, UDP, ICMP 등의 트래픽 공격 탐지/차단

인증 방어
프로토콜의 특성을 이용하여 인증 기반의 접근 제어

DNS 방어
악의적이거나 금지된 웹 사이트와 애플리케이션을 DNS 수준에서 탐지/차단

시그니처 방어
공격 시그니처에 포함된 패턴과 일치하는 시그니처 탐지/차단

BLUEMAX ADS

03 주요 기능

구분	상세 내용	
DDoS 대응	• IP, VLAN ID, 세그먼트 등 맞춤형 보안 설정 • 다수의 블랙리스트 일괄 등록/삭제 • 제조사에서 제공하는 블랙리스트 연동 지원 • DDoS 방어에 최적화된 맞춤형 탐지 정책 프로파일 • 공격에 대한 선택적 차단 설정 (IP 주소, 포트 등) • 서비스 공격의 5단계 위험도 표시 • 자동 학습 방어 • 제조사 배포 시그니처 및 사용자 정의 시그니처 적용 • DNS 도메인 차단 • 시간 만료 정책 검색 • 정책 및 동적 기반 QoS • IP의 트래픽 플로우 검색 • SSL Inspection • 매뉴별 멀티 윈도우 기능 제공	• 화이트리스트/블랙리스트 차단 • 만료된 블랙리스트 전체 삭제 • 다양한 비정상 프로토콜 방어 (IP, TCP, UDP, ICMP 등) • DoS, DDoS, DRDoS 공격 방어 • 탐지 및 차단 임계치 설정 • 맞춤형 학습을 위한 조건 설정 (기간, 요일, 시간 등) • TCP, UDP, HTTP, DNS 등 인증 방어 • 사용자 정의 국가/대륙별 DDoS 공격 차단 • 트래픽에 대한 ACL 설정 • MAC 주소 제어 • 우회 라우팅 제어 • X-Forwarded-For를 포함한 HTTP 우회 IP 주소 로깅 • 보안 기능에서 사용하는 객체 관리
Analysis	• 외부 시스템 연동 없이 로그 기반 자체 분석 지원 • 전역 필터 및 위젯별 개별 필터 등 다양한 필터 지원	• 세션 및 트래픽 통계 분석 • 분석 화면에서 로그 조회 연계
Dashboard	• 프로파일 기반 맞춤형 대시보드 • 위젯별 확대 및 시각화 변경 지원 • DDoS 방어 결과 요약 위젯 (전체/도메인별)	• 크기 조절, 위치 이동을 지원하는 20개 이상의 대시보드 위젯 제공 • 위젯에서 조회 대상 장비 선택 지원
Monitoring	• 실시간 차단 제어 현황 모니터링 • QoS 및 우회 라우팅 제어 현황 모니터링	• 트래픽 방향, 프로토콜, 세그먼트 등 트래픽에 대한 다양한 모니터링
Log/Report	• 로그 순서 정렬 (내림차순/오름차순) • 리포트 브라우저를 이용한 리포트 관리 • 정기 리포트 원격 자동 전송 • 장비 실행 이력, 관리자 접속 이력 등 감사 로그 제공	• 과거 조회했던 로그 필터 히스토리 지원 • 다양한 형식의 리포트 지원 (PDF, HTML, DOC, EXCEL, HWP, PPT 등) • 프로파일 기반 맞춤형 리포트 생성
Management	• Active-Active HA 지원 및 설정 자동 동기화 • Open API 제공으로 종속성 없는 3rd party 연동 • 온라인 도움말 • 관리자 권한과 상관없는 읽기 전용 모드 지원 • 라이선스 자동 업데이트 지원 • 데이터 무결성 점검 기능 제공 • 컨텍스트 메뉴 지원 • 시스템 설정, 정책, 로그에 대한 수동/자동 백업, 복구 기능 (비밀번호 설정 기능)	• Out-Of-Path 구성 지원 • HTML5 기반 WEB UI 제공 • 관리자 IP 접근제한 및 권한 프로파일 • 관리자 로그인 2-Factor 인증 (OTP) • USB 포트 사용 제한 GUI 설정 지원 • 패킷 수집 기능 제공 (인터페이스, IP 주소, 포트, 프로토콜) • DDoS 방어 설정 변경 시, 기본 및 이전 설정 변경 사항 비교

BLUEMAX ADS

05 제품 사양

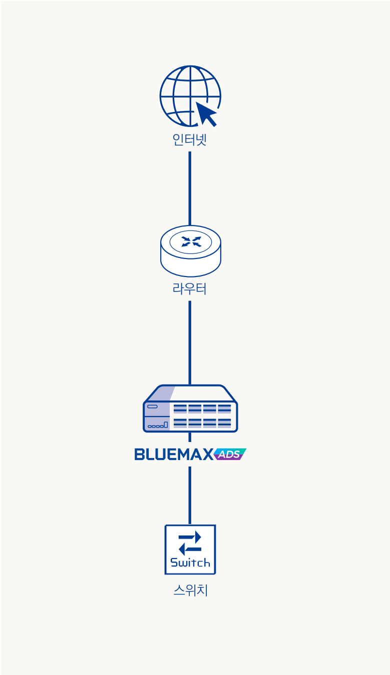
BLUEMAX ADS		4000	5000	10000
CPU		10 Core	24 Core	52 Core
Memory		64 GB	96 GB	192 GB
Storage	System	SSD 32 GB	SSD 128 GB	SSD 128 GB
	Log	HDD 2 TB	SSD 1.92 TB	SSD 1.92 TB
NIC	40GF (Smart NIC)	–	–	(max4)
	10GF (Smart NIC)	–	2(max8)	4(max8)
	1GF	4(max16)	(max12)	–
	1GC	4(max16)	4(max12)	–
Power Supply		Redundant	Redundant	Redundant
Throughput (UDP/64byte)		2 Gbps	20 Gbps	40 Gbps
Throughput (UDP/MAX)		16 Gbps	80 Gbps	160 Gbps

BLUEMAX ADS

06 구성 사례

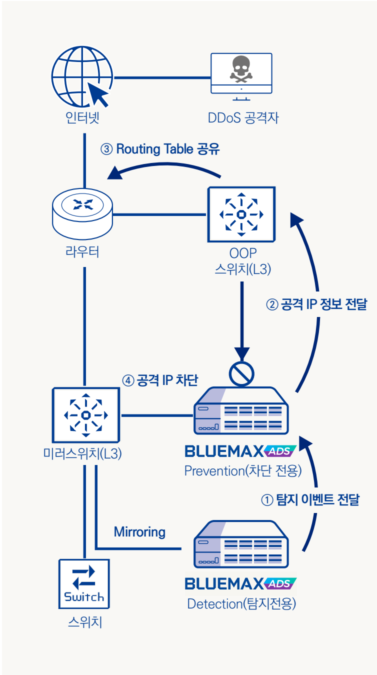
인라인(Inline)

- 일반적인 DDoS 대응시스템 구성
- 네트워크 경로상에 직접 연결하여 DDoS 공격 차단
- Bypass 및 LLCF(Link Loss Carry Forward) 기능 제공



아웃 오브 패스(Out-Of-Path)

- 미러링 방식 구성으로 공격 의심 트래픽 우회 및 공격 트래픽만 차단
- 확장성이 우수하여 ISP 등 대형망 구성에 적합



BLUEMAX WIPS

Wi-Fi 7 위협 대응 가능한 차세대 무선침입방지

원격/재택근무, 소규모 오피스의 활용 증가로 무선 랜을 사용하는 디바이스의 수는 지속적으로 증가하고 있습니다. 최근 신규 주파수인 6GHz를 지원하는 Wi-Fi 7 기술이 상용화되고, 이를 지원하는 장비가 증가하면서 새로운 위협에 대한 대응이 필요합니다.
시큐아이 BLUEMAX WIPS는 Wi-Fi 7(802.11be)과 Wi-Fi 7에서 신규 주파수인 6GHz에서 발생하는 무선 보안 위협을 완벽 차단하는 차세대 무선 침입방지시스템입니다.

BLUEMAX WIPS 특장점

BLUEMAX WIPS

01 특장점

차세대 무선 표준 Wi-Fi 7 지원

- 802.11 a/b/g/n/ac/ax /be 지원
- 2.4GHz, 5GHz, 6GHz Tri-band 지원
- H/W 교체 없이 기존 센서의 펌웨어 업데이트로 Wi-Fi 7 환경 지원 예정

신속한 탐지 및 차단

- 최적화된 무선 주파수 채널 스캔 알고리즘 적용
- 3개 주파수 총 98개 전체 채널 탐지 및 1초 이내 차단 성능 지원

무선 보안 전용 센서

- 기능 제약 및 성능 저하가 없는 무선 보안 전용 센서로 안정적인 서비스 제공

중단 없는 탐지/차단 운영 제공

- 컨트롤러와 센서의 연결 중단 시, 독립 운영 모드 지원
- 센서 최신화된 보안 정책 연동으로 무중단 탐지/차단 서비스 제공

최적의 무선 위협 정책 설정

- 네트워크 침입 방어, 외부 네트워크 접속, 데이터 유출, 무선 인프라 공격 등 종류별 정책 설정 지원

지능형 무선 분석 및 대응

- 물리적 디바이스(센서, 단말, AP) 상세 정보 제공
- 보안 사고 시 시계열 중심의 분석 기능 제공

BLUEMAX WIPS

02 주요 무선 보안 방어 유형

내부 네트워크 침입

- 비인가/불법 AP를 연결하여 보안 정책 우회한 침입 방어
- 보안 정책이 취약한 AP 대상 내부망 침입 및 데이터 탈취 방어
- 내부 사용자의 정보 유출, 공격자의 내부망 침입 방어
- 인가 단말의 정보 유출 및 인가 단말을 통한 내부망 침입 방어
- WEP 해킹을 통한 인가 AP 권한 획득 후 내부망 침입 방어

외부 네트워크 접속을 통한 데이터 유출

- 외부의 비인가/불법 AP로 접속, 단말 내 기밀 정보 탈취 방어
- Hotspot(테더링)을 활용한 스마트폰 및 통신사 에그 접속을 통한 기밀 정보 유출 방지
- SSID 복제하여 인가된 AP로 오인하여 접속 유도한 기밀 정보 탈취 방지
- WEP 해킹을 통한 인가 AP 권한 획득 후 내부망 침입 방어

무선 인프라 공격

- Flooding/Spoofing 공격, RF jamming 공격, 비정상 패킷 공격 등을 통한
- 무선 업무망 마비 및 업무 활동 방해 방지

BLUEMAX WIPS

03 주요 기능

구분	상세 내용	
무선 규격	• Wi-Fi 7 (IEEE 802.11 a/b/g/n/ac/ax/be) 지원	• 802.11w(PMF) 차단 (AP/단말 차단 가능) • Tri-Band(2.4GHz, 5GHz, 6GHz) 동시 탐지 및 차단
무선 위협 탐지/차단	• 비인가/불법/설정 위반 AP 탐지 및 차단 • 비인가 디바이스 접속 탐지 및 차단 • SSID 복제, MAC 변조 탐지 및 차단 • 모바일/휴대용 핫스팟 탐지 및 차단 • Wi-Fi Direct/WDS/WPS/WEP 정책 위반 탐지 및 차단	• Malformed 무선 패킷 탐지 • 무선 DoS 공격/RF 간섭원 탐지 • 팝업, syslog, SNMP, e-mail 등 이벤트 알림 기능
무선 관리	• 위협 등급별 분류 (인가/비인가/위반/불법/외부/방문) • AP/단말 그룹별 정책 설정, 유효기간 설정 및 접속 허용	• SSID 다국어 지원, Hidden SSID 탐지 • 무선랜 접속 현황 및 세부 정보 • 무선 디바이스 위치 추정 및 이동 경로 관리
시스템	• 컨트롤러 고가용성(HA) 지원 및 장애 시 자동 Fail-over • 통신 단절 시 센서 독립모드 운영 • 센서-컨트롤러 간 암호화 통신	• 무선랜 컨트롤러(APC) 연동 지원 및 AP 허용/차단 • 유·무선랜 통합 인증 서버 사용자 정보 연동 • 관리자 GUI HTML5/TLS1.3 지원, RESTAPI/CLI 제공

BLUEMAX WIPS

04 무선 보안 전용 센서 장 / 단점

구분	전용 센서	일체형 / 모듈형
구성 방식	• 전용 WIPS 센서	• 무선 AP + WIPS 기능/무선 AP + WIPS 모듈
동작 방식	• [수신 안테나] 채널 스캔, 탐지 수신 • [송신 안테나] 전 채널 필요시 차단 패킷 송신	• [수신 안테나] 무선랜 미 동작 시, 채널 스캔, 탐지 수신 가능 • [송신 안테나] 무선랜 서비스 미 동작 시, 차단 패킷 송신
장/단점	• 무선 보안 100% 수행 가능 • H/W 장애 시, 영향도 낮음 • 외부 공격에 대한 보안 위협도-낮음 (무선 해킹 노출도 낮음)	• 무선 보안 기능 일부 지원 및 성능 저하 가능성 존재 • H/W 장애 시, 서비스 동시 불가 • 무선랜 사용 시, 탐지 불가

BLUEMAX WIPS

05 제품 사양

센서

BLUEMAX WIPS		S602	S624	S714	S624 OD
Wireless Standard		802.11 a/b/g/n/ac/ax 지원	Wi-Fi 7 지원 802.11 a/b/g/n/ac/ax/be 지원		
CPU		4 Core	4 Core	4 Core	4 Core
Memory		1 GB	2 GB	2 GB	2 GB
Flash Memory		256 MB	512 MB	512 MB	512 MB
Interface	5GC	1	1	1	1
	2.5GC	–	–	–	–
	1GC	2	2	2	2
Power Supply		PoE(802.3af/at) 최대 15.4W 이하	PoE(802.3bt) 최대 60W 이하	PoE(802.3bt) 최대 60W 이하	PoE(802.3bt) 최대 60W 이하
Antenna		내장 안테나 : 2 x 2	내장 안테나 : 4 x 4	내장 안테나 : 4 x 4	외장 안테나 : N type

※ Wi-Fi 6E/7 표준 사용 시, PoE(802.3bt) 환경 권장

컨트롤러

BLUEMAX WIPS		C1000	C2100	C3100	C5100
CPU		2 Core	4 Core	6 Core	8 Core
Memory		8 GB	16 GB	16 GB	32 GB
Storage	System	SSD 250 GB	HDD 1 TB	HDD 1 TB	HDD 2 TB
	Log	SSD 250 GB	SSD 500 GB	SSD 500 GB * 2 (RAID)	SSD 500 GB * 2 (RAID)
Interface	1GC	4	2	2	2
Power Supply		Adapter	Redundant	Redundant	Redundant
Sensor(max)		50	200	400	1,000

BLUEMAX WIPS

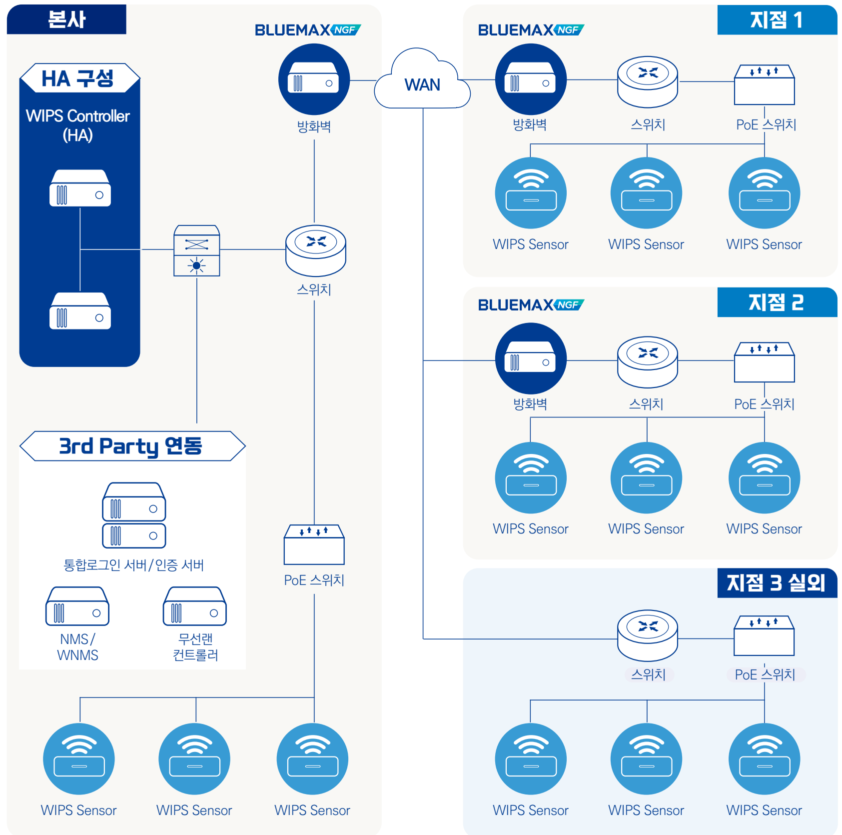
06 구성 사례

N-Site 구성

- WIPS Controller 본사/DC 구축
- VPN을 통한 지점 센서 통합 관리

HA 구성

- Active-standby 지원
- 장애 발생 시 자동 Fail-over 지원



기존 시큐아이의 Wi-Fi 6 센서를 도입한 고객의 경우, 별도의 컨트롤러 증설 없이 Wi-Fi 6E 센서 도입만으로 추가 위협 대응 가능

BLUEMAX TAMS

BLUEMAX 제품 통합 관리 시스템

BLUEMAX TAMS는 다양한 보안장비로부터 로그를 수집해 각종 보안 위협 정보를 분석하고 보안정책 관리기능을 제공하는 통합보안관리 시스템입니다. 실시간으로 보안 장비와 글로벌 위협 정보가 연동되어 위협 현황을 모니터링하고 분석하여 가시성을 제공하고, 변화하는 IT 인프라 환경에 맞는 최적의 보안 운영과 능동적인 위협 대응이 가능합니다.

위협 분석·관리
(Threat Management)

정책 신청·분석
(Security Policy Analysis)

통합 설정 관리
(Centralized Management)

보안 로그 분석
(Security Log Analysis)

BLUEMAX TAMS 아키텍처

BLUEMAX TAMS

01 특장점

관리 및 설정 편의성 제공

- 토폴로지를 통해서 최대 5,000대 관리 장비 등록 및 확인 가능
- 장비의 상태(정상/비정상)에 따라 목록 구분 및 관리 편의성 제공

심층적인 보안 대응/분석 제공

- 시스템/위협에 대한 실시간 모니터링 기능을 통한 위협 대응
- 사용자 고급 분석을 통해 사용자의 편의에 맞는 분석 차트 및 대시보드 제공
- 중앙 집중형 관리 기능 제공을 통해 저장 로그 조회/분석 편의성 강화

보안 정책 자동화 기반 정책 관리

- Open API를 활용한 장비 연동을 통해 자동화된 보안 정책 관리 프로세스 제공

BLUEMAX TAMS

02 주요 기능

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

BLUEMAX TAMS

03 제품 사양

<table>
<tr><th colspan="2">BLUEMAX TAMS</th><th>110</th><th>1100</th><th>5100</th></tr>
<tr><td colspan="2">CPU</td><td>6 Core</td><td>12 Core</td><td>12 Core * 2</td></tr>
<tr><td colspan="2">Memory</td><td>16 GB</td><td>64 GB</td><td>128 GB</td></tr>
<tr><td rowspan="2">Storage</td><td>System</td><td>SSD 512 GB</td><td>SSD 512 GB * 2</td><td>SSD 512 GB * 2</td></tr>
<tr><td>Log</td><td>SSD 1 TB</td><td>HDD 4 TB * 2/
4 TB * 4/8 TB * 4</td><td>HDD 4 TB * 2/
4 TB * 4/ 4 TB * 6/
8 TB * 6/12TB * 6
16 TB * 6/ SSD 4TB * 6</td></tr>
<tr><td rowspan="3">Interface</td><td>10GF</td><td>-</td><td rowspan="2">(max2)</td><td rowspan="2">(max2)</td></tr>
<tr><td>1GF</td><td>-</td></tr>
<tr><td>1GC</td><td>2</td><td>4</td><td>4</td></tr>
<tr><td colspan="2">Power Supply</td><td>Single</td><td>Redundant</td><td>Redundant</td></tr>
<tr><td colspan="2">Number of Devices(max)</td><td>10</td><td>1,000</td><td>5,000</td></tr>
</table>

BLUEMAX ESP

단말 보안 플랫폼

단말 보안은 기업 및 기관이 직면한 가장 중요한 보안 과제 중 하나입니다. 단말 보안 플랫폼인 BLUEMAX ESP는 내PC지키미를 포함한 다양한 PC 보안 점검 컴플라이언스와 멀티 플랫폼 점검을 지원합니다.
또한 SSL VPN, 화면 캡처 차단 등 다양한 보안 기능과 함께 차세대 방화벽인 BLUEMAX NGF 연동에 기반한 강력한 접근제어를 제공합니다.

PC보안 점검 컴플라이언스	OS 점검 유형
사이보보안 진단의 날 (내PC지키미)	Windows
주요정보통신 기반시설	Linux
ISMS-P	Grooroom OS
금융보안원 재택근무 보안	macOS
SSL VPN	

BLUEMAX ESP 주요 기능

01 BLUEMAX ESP 특장점

점검항목
- 사이버 보안 진단의 날(내PC지키미) 점검 항목 이외에 다양한 컴플라이언스를 지원(사이버 보안 진단의 날, 주요 정보 통신 기반시설, ISMS-P, 금융보안원 재택근무 보안)
- Windows기준 81개 항목 점검
  ※ ISMS-P, 금융보안원 재택근무 보안 규정은 PC보안 관련 항목만 지원

관리자 정의 점검 지원
- 레지스트리, 프로세스, 파일, 네트워크, 프로그램 등 19개의 항목에 대해 관리자의 점검항목 커스텀 지원

취약점 조치
- 원클릭 자동조치 기능 제공
- 웹 기반의 사용자 수동조치 가이드 제공

스케쥴 점검
- 관리자 지정한 스케쥴에 의한 점검(수동/자동)기능 지원
- 백그라운드 자동 점검 지원

연동 점검
- 관리자가 지정한 프로세스를 실행 시 자동 점검 기능

화면 캡처 차단
- Windows 기본 캡처 기능 차단
- 각종 캡처 프로그램을 이용한 캡처/녹화 기능 차단(정보 유출 방지)

지원 편의성
- 다국어(영어) 지원
- 멀티 플랫폼(Windows/Linux/Gooroom OS/macOS) 지원
- PC정보(OS, S/W, H/W) 수집기능 제공

BLUEMAX ESP

02 제품 사양

Agent

BLUEMAX ESP	Agent 설치 환경(최소 사양)			
	Windows	Linux	Gooroom OS	macOS
CPU	2 Core 이상		4 Core 이상	Silicon M1 이상
Memory	4 GB 이상			8 GB 이상
Storage	HDD 2 GB 이상 여유공간			

Manager Server

BLUEMAX ESP		SW Version(최소 사양)	Appliance	
			100	1000
CPU		2 Core 이상	4 Core	10 Core
Memory		8 GB 이상	8 GB	64 GB
Storage	System	HDD 128 GB 이상	HDD 1 TB	SSD 256 GB * 2
	Log	–	–	HDD 4 TB * 2
Power Supply		–	Single	Redundant
Number of Agent(max)		10,000(최대)	2,000	10,000

BLUEMAX ESP

03 지원 플랫폼

구분		상세 내용
OS	Windows	Windows 10, Windows 11
	Gooroom OS	Gooroom OS 2.0, Gooroom OS 3.0
	Linux	Ubuntu 20.04, CentOS 7.9
	macOS	macOS 10.15 이상

02

Cloud Security

클라우드 보안

SASE
(Secure Access Service Edge)

클라우드 보안 서비스

최근 4차 산업혁명, 디지털 전환의 가속화로 고객 IT 인프라 환경은 지속적으로 다양화되고 고도화되고 있습니다. 특히 온프레미스뿐만 아니라 클라우드를 활용하는 기업들이 늘어나면서 방어해야 하는 영역은 더 넓어지고 있는 상황입니다. 또한 고객의 정보자산을 노리는 공격자와 보안 위협은 지속적으로 강력해지고 있으며, 전문성을 갖춘 전문가의 신속한 대응이 중요합니다. 시큐아이 SASE(Secure Access Service Edge)는 국내 네트워크 보안 1위의 노하우와 기술력을 기반으로 클라우드 보안 서비스를 제공합니다.

01

SASE
왜 SASE 인가?

SASE 도입 배경
- 고객들의 자산이 멀티 클라우드 전환
- 비대면 근무, 지점/지사 등으로 분산되고 복잡한 IT 환경
- 모바일, PC, IoT 다양한 접속 단말 증가로 보안 복잡도 증가

필요 고객
- 증가하는 지사/지점에 따라 빠른 보안 솔루션 구성이 필요한 기업
- 스타트업, 소규모 기업 등 전문적인 보안 담당자 부재한 기업
- 재택 및 출장 등 원격 업무 사용자 많은 고객

02

SASE
특장점 및 구성 요소

구분	상세 내용
Service Portal	• 고객/서비스별 운영 현황(이용 추이, 과금 현황 등), 이미지/콘텐츠 배포 관리 • 이용 중인 서비스에 대한 정책 설정 및 모니터링 기능 제공(고객사별)
내부 보안 기능 Inline Security Edge	• NGFW의 정책 기반 보안 기능 수행 • SSL 암/복호화, QoS, VPN, NAT 등 네트워킹 기능 수행 • 인증/계정 관리, 과금, 정책 적용 등
외부 보안 기능 Out-Of-Band Security Edge	• AV, 정적/동적 분석, AI/ML 분석을 통한 멀웨어 탐지 • 민감한 정보 및 조직의 주요 정보 유출 검사 및 Compliance 점검 • 시그니처, Blacklist, URL DB, TI 정보 등 위협 관련 정보 제공
로그 관리 기능 DataLake	• Big Data 기반 Security Edge에서 발생한 로그 저장 • 고객/서비스별 로그 조회 및 Top 정보 제공 등 • 로그 분석을 통한 이상 행위 탐지 및 고객사별 리포트 생성

03

SASE
지원 서비스

구분	상세 내용
FWaaS	• 차세대 방화벽의 애플리케이션 인지, 사용자 인지 등 모든 보안 기능 서비스 제공
SD-WAN	• 애플리케이션 기반 라우팅 기능 제공 • 회선에 대한 품질 상태 체크를 통한 안정적이고 최적화된 서비스 제공
SWG	• 위협 차단을 위한 유해사이트 접속 차단 • 악성코드 탐지, 파일 유형 제어, DLP 기능수행
ZTNA	• 단말 보안 상태에 따른 신뢰성 점검 • 사용자의 Multi Factor 인증 및 최소 권한 접근제어
CASB	• 멀티 클라우드 환경에서 SaaS 데이터 보호 및 사용자 권한 관리 • SaaS 모니터링, 위협 방어, 규제 준수

FWaaS
(Firewall as a Service)

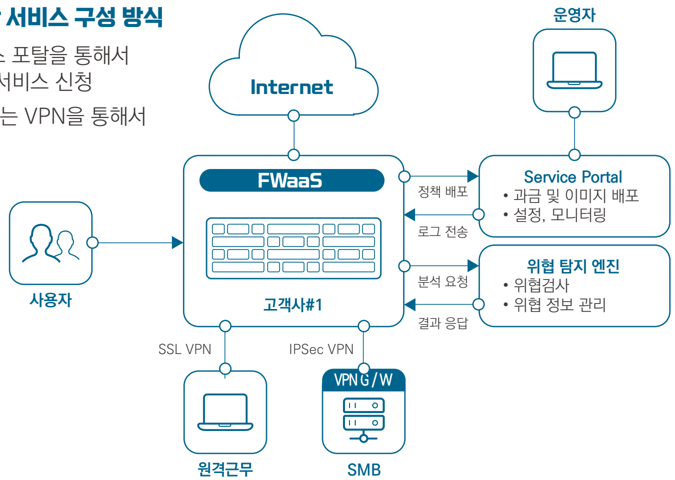
클라우드 방화벽 서비스

최근 증가하는 보안 위협으로 보안에 대한 투자가 필요한 환경에서 고객들은 환율, 부품 등 외부적인 환경 어려움으로 고객들은 즉각적인 보안 투자와 대응이 어려운 상황이 발생하고 있습니다. 이를 해결하기 위한 대안으로 최근 클라우드 방화벽 서비스(FWaaS)가 높은 관심을 받고 있습니다. 시큐아이는 기존 네트워크 보안 1위 기업의 보안 노하우와 기술력을 바탕으로 FWaaS를 제공합니다.
이제 고객들은 간단한 회원가입으로 차세대 방화벽이 제공하는 애플리케이션 인지, 사용자 인지 등 모든 보안 기능 및 서비스를 제공받을 수 있습니다.

01 FWaaS
서비스 구성도

클라우드 보안 서비스 구성 방식

- 사용자는 서비스 포탈을 통해서 클라우드 보안 서비스 신청
- 원격 근무, 지사는 VPN을 통해서 FWaaS와 연결



02 FWaaS
주요 기능

구분	상세 내용
NGFW	• 사용자 기반 정책 제어 • 애플리케이션/디바이스 기반 정책 제어 • 애플리케이션별, 사용자 ID 별 QoS • 자체 사용자 인증(Captive Portal) 및 SSO • SaaS 애플리케이션 제어
방화벽	• 도메인 정책(URL 객체) • 중복 정책 및 미사용(미참조) 정책 검사 • Policy-based NAT & Interfaced-based NAT • 보안 정책 그룹 설정 • 보안 정책별 활성화 스케쥴 • 머신러닝 기반 DNS 위협 탐지
IPS	• 프로파일 기반 시그니처 템플릿 • PCRE(정규표현식) • 멀티패턴 탐지 기능(병렬 탐지) • 취약점 점검 도구 연동, 시그니처 최적화
IPSec VPN	• IKE(v1/v2), PKI(x509) • GRE/IPIP,L2TP, PPTP Tunneling • 3DES, AES, SEED, ARIA, CAST, Blowfish, MD5, SHA-1, SHA-256, SHA-512, HAS160등 • Group VPN 기능 • 양자 내성 암호화 PQC(Post Quantum Cryptography) 알고리즘 탑재
SSL VPN	• Full Tunnel mode • Multi-Factor 인증 지원(3차 인증) • FIDO 생체인증 • PASS 앱 기반 간편 인증
Anti-Virus & Anti-SPAM	• Anti-Virus Engine(File-based or Stream-based) • Realtime Blackhole List(RBL) • 수신자 수 제한, 대량 메일 발송 제한
APT 대응	• Sandbox 장비 연동한 APT 위협 분석 기능 제공 • 탐지된 위협 정보에 대한 공유 체계 지원
모니터링	• SNMP(v1, 2, 3), Syslog 전송 • DB 기반 로그 관리(압축 지원) • 경고 알람 임계치 설정 • Report(정책 상세, 리포트 브라우저) • 애플리케이션, 사용자별 트래픽/세션 모니터링

FWaaS

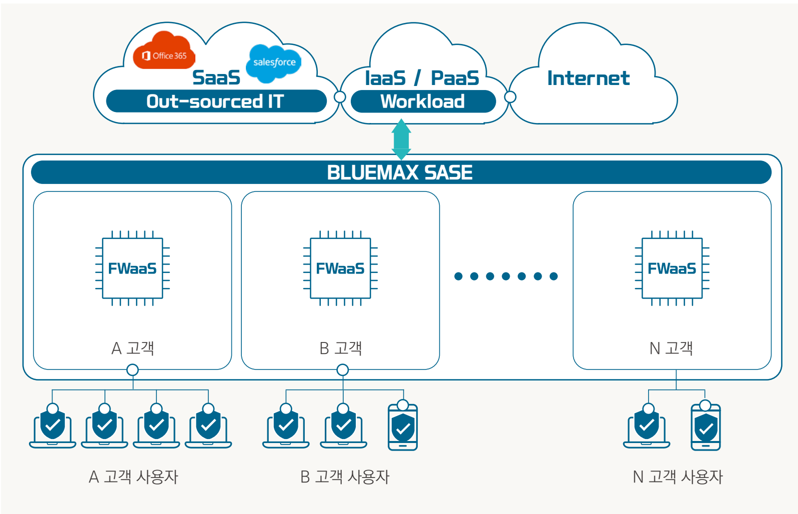
03 구성 사례

소규모 사업장 활용

보안 전문가가 부재하고, 보안에 많은 투자를 할 수 없는 스타트업, 소규모 사업체의 경우, FWaaS를 활용하여 보안성을 강화할 수 있습니다. 특히 장비 구축이 어렵거나, 운영이 어려운 부분을 보안 서비스로 해결할 수 있습니다.

구현 방식

- SSL VPN을 통한 사용자 트래픽 암호화
- APP ID, User ID 기반 네트워크 접근 통제
- 악성 사이트 차단, Anti Virus, IPS 등의 위협 차단 기능을 통한 단말 보호



기대 효과

- 별도의 장비 구축 없이 보안 환경 구축 가능
- 전문적인 운영자가 없어도 안전하고 전문적인 보안 운영 가능
- 사용량/과금 형태로 투자비 절감 가능

FWaaS

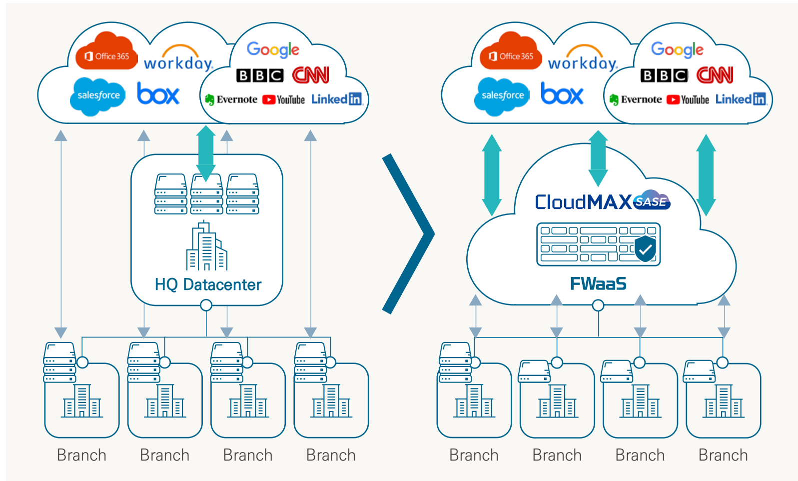
03 구성 사례

지사/지점 규모급 활용

대규모 지사를 보유한 기업체의 경우, 다양한 전문적인 보안 장비 구축이 필요합니다. 또한 외부의 사용자가 많은 경우, 보안성이 취약한 지사의 트래픽이 본사로 집중되어 비용이 증가하게 됩니다. FWaaS를 사용하는 경우, 트래픽을 분산하여 비용을 절감할 수 있습니다.

구현 방식

- VPN, GRE 등의 터널링을 통해 트래픽을 FWaaS로 전달
- 지사 트래픽의 본사 집중을 Edge로 분산 (지사 〉 FWaaS 〉 외부)
- 기존 Security Stack을 FWaaS가 대체하여 보안 처리 수행
- FWaaS의 위협 차단을 통한 내부 유입 위험 사전 조치



기대 효과

- 본사와 일관 된 보안 정책을 외부에 동일하게 적용 가능
- 트래픽 비용 감소 효과를 통한 비용 절감 기대
- 보안 투자 필요시, 즉시 대응 가능

BLUEMAX NGF VE

클라우드 향 차세대 방화벽

BLUEMAX NGF VE는 국내 1위 방화벽 제품으로 기술력, 성능, 편리성 측면에서 고객에게 인정받는 BLUEMAX NGF의 모든 기능을 클라우드 환경에서 사용할 수 있도록 구현한 클라우드 차세대 방화벽입니다. BLUEMAX NGF VE는 클라우드 환경 내에서 위협 요소를 탐지 및 차단하고 Auto Scaling을 통해 보안 가용성을 제공합니다. 특히 글로벌 대표 클라우드 서비스 환경(AWS, MS Azure, openstack)에 최적화되어 있어 고객의 사용 환경에 상관없이 높은 편의성을 제공합니다.

01

BLUEMAX NGF VE

특장점

차별화된 클라우드 차세대 방화벽

- 차세대 방화벽 BLUEMAX NGF 모든 기능을 클라우드 환경에 구현
- 국내 차세대 방화벽 제품 중 가장 많은 클라우드 플랫폼 지원

유연한 사용 환경 대응

- 글로벌 주요 클라우드 네트워크 보안 서비스 환경 최적화

Auto Scaling 기반 보안 가용성 강화

- 가상 환경의 네트워크 트래픽 증가 및 사용량 과부하 시, 자동 확장하여 보안 가용성 강화

02

BLUEMAX NGF VE

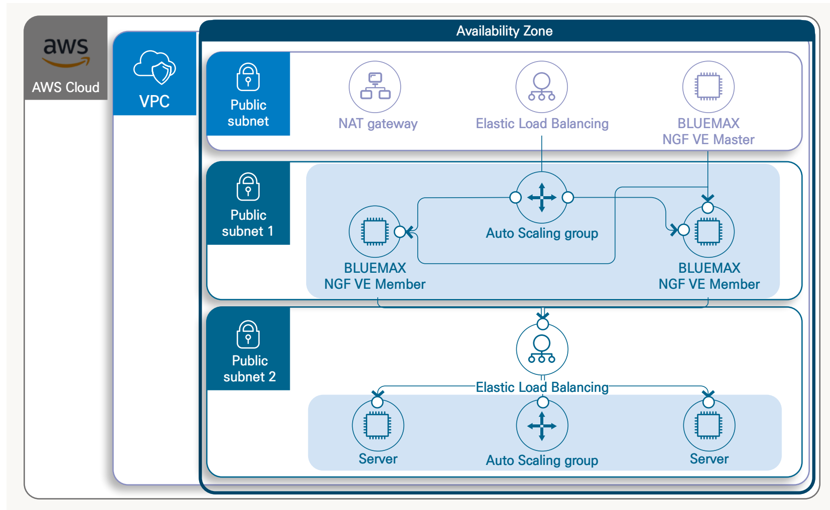
제품 사양

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(Min)	4 GB	4 GB	8 GB	8 GB	8 GB
Storage Suppor(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

03

BLUEMAX NGF VE

CLOUD 구성 사례 (AWS 클라우드 Auto Scaling 구성)



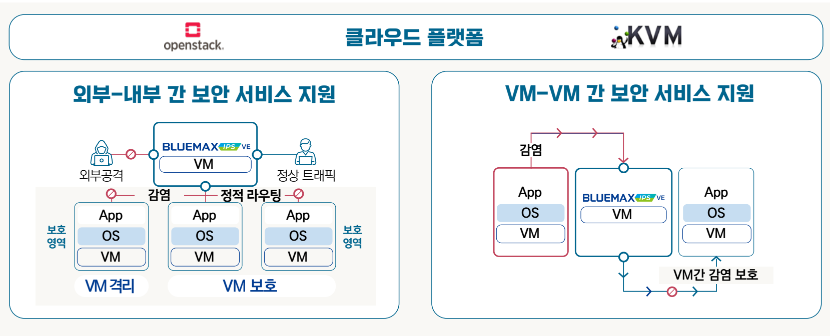
Public subnet 1 — BLUEMAX NGF VE Member 인스턴스를 포함하는 Auto Scaling Group(ASG)이 존재

Public subnet 2 — 내부 Elastic Load Balancing(ELB)과 내부 보호 대상 서버들을 연결

BLUEMAX IPS VE

클라우드 향 차세대 IPS

클라우드 환경에서의 네트워크 보안은 새로운 도전과 기회를 제시하고 있습니다. BLUEMAX IPS VE는 가상화 클라우드 환경의 특성을 고려하여 설계된 차세대 IPS입니다. 다양한 가상 환경의 악성 트래픽 및 파일을 검사하여 네트워크 보안의 위협 요소를 실시간으로 탐지하고 대응하는 가상화 버전의 차세대 IPS 제품입니다.

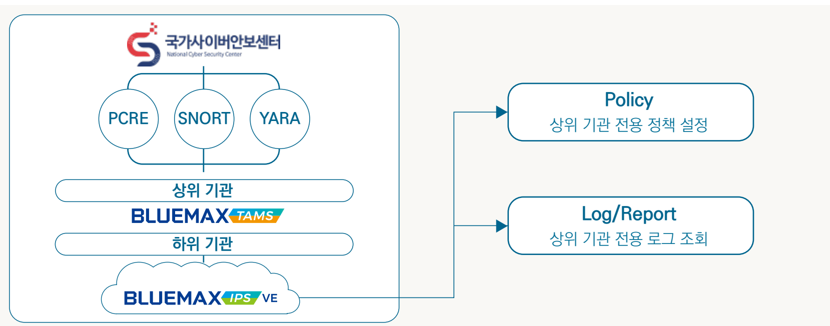


가상화 / 클라우드 플랫폼 지원

01

BLUEMAX IPS VE

특장점



상위 기관 PCRE 연동

02

BLUEMAX IPS VE

주요 기능

구분	상세 내용
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), 위협 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

03

BLUEMAX IPS VE

제품 사양

BLUEMAX IPS VE	500	1000
Virtualization Platform	Openstack, KVM	
vCPU Support	4 Core	8 Core
vMemory	16 GB	16 GB
vStorage	128 GB	128 GB
Throughput	4 Gbps	6 Gbps

BLUEMAX TAMS VE

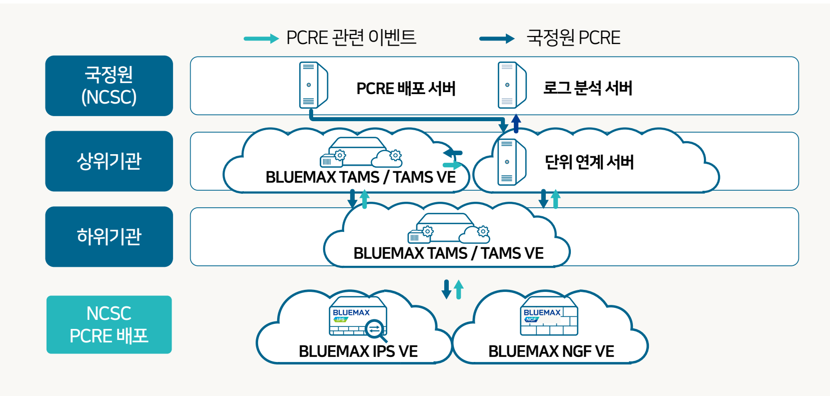
클라우드 향 통합보안관리시스템

클라우드 전환이 가속화 되면서 다수의 보안장비를 통합관리하는 통합보안관리시스템이 필수적인 시스템으로 부상하고 있습니다. BLUEMAX TAMS VE는 클라우드 환경에서 분산된 보안 시스템의 통합 위협 분석, 대량 로그 수집, 직관적 통합 설정, 보안 정책 분석 및 최적화로 Security Automation 환경을 제공합니다.

01

BLUEMAX TAMS VE

특장점



02

BLUEMAX TAMS VE

주요 기능

구분	상세 내용
위협 관리	• 시스템/위협 현황 다차원 분석하여 다양한 위협 대응 정책에 활용 • 글로벌 위협정보 연동으로 다차원 위협 탐지 및 가시성 제공 • 위협 분석 프로파일 기반 심층적 위협 분석 수행 • 온프레미스, 클라우드 구분 없는 안정적인 PCRE 연동 체계 지원
통합 설정 관리	• 직관적인 통합 설정 관리로 편의성 제공 • 네트워크 구분 없이 관리장비 자동 등록 • 자동 동기화 제공으로 편리한 통합 설정 관리 • Background 수행으로 동기화 중 개별 기능 수행
보안 로그 분석	• 연속적 위협 로그추적으로 상세 로그 정보 확인 • 고성능 HW 플랫폼을 적용하여 향상된 로그 분석 성능
보안 정책 분석	• 관리 대상 장비의 보안 정책을 수집, 동기화, 분석, 유효성 검증하여 최적화된 보안 정책 제공 • 방화벽 정책 신청 자동화와 신청 이력 관리로 휴먼 에러를 방지하는 One-stop 정책 관리 제공 • 7단계로 입력 값 점검, 신청 정보 최적화, 대상 장비 입력을 확인하는 정책 관리 마법사

03

BLUEMAX TAMS VE

제품 사양

BLUEMAX NGF VE			100	1000	5000
Virtualization Platform			Openstack		
vCPU Support			4 Core	10 Core	20 Core
vMemory			8 GB	64 GB	128 GB
vStorage			-	8 TB	8 TB
Number of Devices	모니터링전용	권장	50 대	300 대	2,000 대
		최대	80 대	600 대	3,000 대
	설정 모드	권장	30 대	150 대	300 대
		최대	60 대	300 대	600 대

03

Security Service

보안 서비스

TARP
(Threat Analysis & Response Platform)

자동화된 분석 및 대응 체계를 지원하는 AI-powered SOC platform

현대의 사이버 보안 위협은 매우 빠르고 자동화된 형태로 이루어 집니다. 기업들은 조직을 보호하기 위해 다양한 최신 보안 솔루션을 지속 도입하고 있습니다. 때문에 하루 수천, 수만 건의 보안 경보가 발생되고 있으며, 과다한 경보로 인해 보안담당자가 위협에 대응하는 것보다 공격의 확산 속도가 더욱 빠르기 때문에 적절한 대응을 위해서는 AI 기반의 자동화된 플랫폼 필요합니다. 자동화된 위협 대응 플랫폼은 복잡한 보안 환경을 통합 관리하며, 보안 인력의 업무를 효율화/고도화하여 기업의 사이버 회복 탄력성(Cyber Resilience)을 획기적으로 향상시키는 핵심 솔루션 입니다.

01

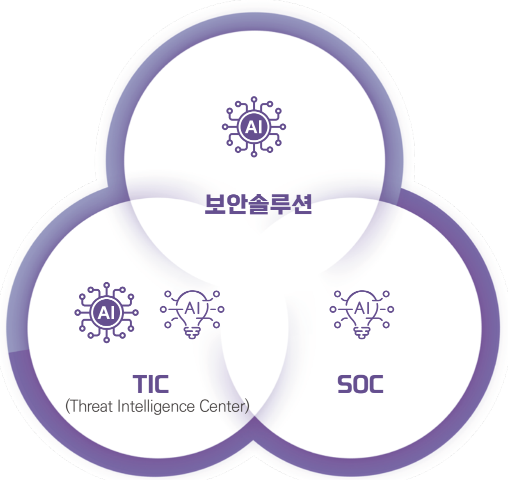
TARP

AI 보안 기술

최신 위협에 대하여 효과적인 방어 체계를 갖추기 위해서는 보안솔루션-TIC-SOC가 유기적으로 결합한 위협대응체계가 요구되며, 각 요소들 필요한 AI 기술이 적용되어야 합니다.

AI-Powered	
기반 기술	ML 기반의 AI 기술
주요 역할	학습된 모델을 통한 기능 수행 └ **Co-Pilot 역할**
핵심 요소	정확도 및 신뢰도

AI-Driven	
기반 기술	LLM, RAG, NLP 등 고도화된 AI 기술
주요 역할	복잡한 작업의 효율적인 수행 └ **Agent 역할**
핵심 요소	문제해결 방안제시

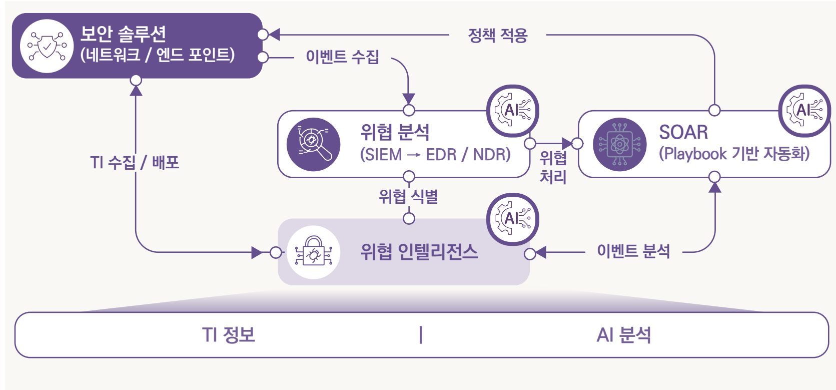


02

TARP

시큐아이 AI 기반 위협 대응 플랫폼

자체 개발한 AI 기반 통합보안플랫폼을 기반으로 보안관제 서비스 체계 구현



03

TARP

특장점

AI 기반 분석 기능 지원으로 신속한 위협 대응
- 이상 징후를 빠르게 탐지하고 실시간으로 조치 가능
- 평균 대응 시간(MTTR) 단축
- AI 어시스턴트 및 XAI 기반의 상관관계 분석 결과를 제공하는 STIC(TI)과 연동

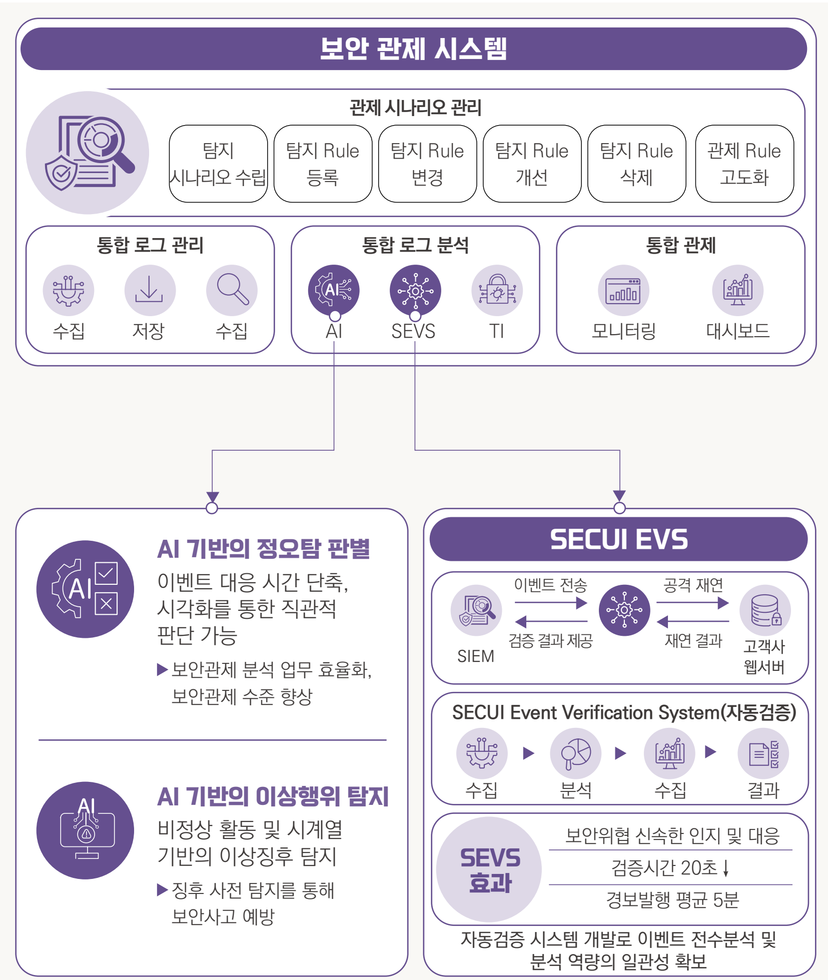
SOAR 플레이북 에디터 제공
- 보안 운영의 효율성 및 일관성 향상
- 반복 업무 자동화로 관제요원의 업무 부담 경감
- 표준화된 대응 프로세스로 휴먼 오류 최소화

BLUE EYE(고객 포털)과 연계한 상세 분석 결과 및 로그 조회
- 위협 탐지 이벤트 티켓 조회 더불어 상세 로그
- 관제 현황에 대한 일간,주간,월간 보안리포트 제공

Security Service 03

04 주요 기능

AI 기반 SIEM



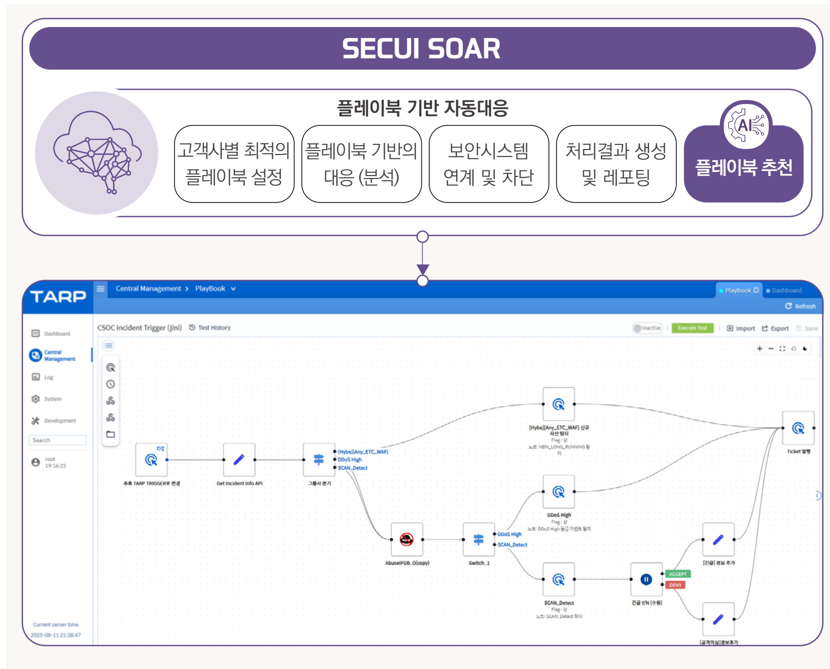
AI 기반의 정오탐 판별 및 이상로그/트래픽 탐지를 통해 빠르고 효율적인 사고 예방

웹 취약점 공격 유효성 검증 자동화를 통해 공격 이벤트 전수 분석 및 대응 강화

04 주요 기능

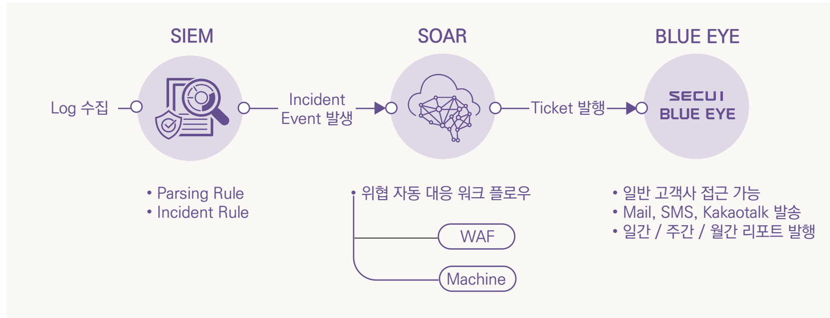
SOAR

다양한 보안 도구(솔루션)와 연동하여 반복 업무에 대한 자동화를 지원하여 보안 위협에 신속하고 표준화된 대응 체계 구현



탐지된 위협에 대해 원격관제고객 포털인 BLUE EYE와 연계하여 티켓 자동 발행

BLUE EYE 포털을 통해 탐지된 로그 상세 및 리포트 조회 지원



CSOC
(Cyber Security Operation Center)

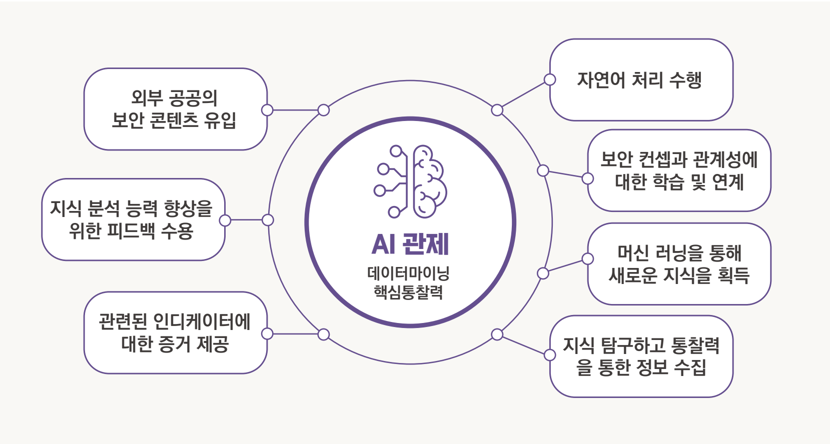
AI 기술 접목 보안관제 서비스

다양한 경로를 이용한 해킹 공격 시도와 Zero-day 공격 등 증가하는 보안 위협과 지능화된 공격에 대응하기 위해 훈련된 전문 인력과 글로벌 최고 수준의 기술력을 갖추는 것이 중요합니다. 시큐아이는 AI 기술을 접목한 차별화된 원격 관제 서비스를 시작으로 클라우드 관제 서비스와 보안 전문가를 파견하는 파견 관제 시스템을 제공합니다. 고객은 대한민국 1위 네트워크 보안 기업이 제공하는 관제 서비스를 통해 실시간 위협 식별 및 잠재적인 위협 탐지를 위한 보안 대응 체계를 확보하여 기업 내부 보안 역량을 강화할 수 있습니다.

01

CSOC
보안관제 서비스란?

보안관제 서비스는 보다 고도화되고 지능화된 잠재적 위협으로부터 기업의 자산을 효율적으로 보호하고, 더 나아가 고객 보안 솔루션에 대한 운영 및 전문적인 관리를 제공하는 보안 서비스입니다.



시큐아이 관제 서비스

02

CSOC
보안관제 서비스 필요성

기업 내/외부 위협 요소에 대해 효율적인 예방, 탐지, 대응 체계를 마련하기 위해 정보시스템에 대한 전문 보안관제 서비스가 필요합니다.

업무시간 경계 모호
- 글로벌 서비스 업무 대응을 위해 야간/휴일 보안관제 부재 등 자체 보안관제로는 대응 한계
- 24×365 체계의 신속한 침해사고 대응이 어려워 양질의 보안관제 서비스 필요

보안 위협 증가
- 일반 기업의 임직원들이 악성코드에 감염되어 업무에 피해를 입은 사례 지속적으로 증가
- 홈페이지 변조 및 서비스 저해 공격 시 기업 이미지 추락 및 비용 손실 초래

보안 담당자 업무 수행 과다
- 방화벽 정책 등 단순하고, 자주 발생하는 업무로 인해, 분석/침해 예방 등 고가치 업무 수행 한계
- 보안 서비스 품질 관리를 지속적으로 수행할 수 있는 보안 전문 파트너 필요

03

CSOC
보안 관제 서비스 유형

구분	상세 내용
원격 관제	• 시큐아이 관제센터와 고객의 보안관제 대상 연동 • 24×365 모니터링 제공 • 개방형 통합 MDR 서비스 제공 • AI 기반 침해 위협 대응 원격 지원 • 고객사 운영 도메인(URL) 악성코드 경유지 및 유포지 탐지 • 모의해킹 및 취약점 점검 개선 과제 수립 • 해킹 메일 모의훈련
클라우드 관제	• 클라우드 보안 운영 지원 • 멀티 클라우드 관제 • 클라우드 보안 현황 및 설정에 대한 진단 제공 점검 (CCE) • 클라우드 트래픽 플로우 가시화를 통한 네트워크 구조 점검
파견 관제	• 보안관제 인력을 파견하여 자체 구축한 SIEM 기반 관제 서비스로 사이버 위협 대응과 안정적인 보안 모니터링을 제공하는 서비스

Security Service 03

CSOC

04 시큐아이 관제 서비스 특장점

글로벌 수준의 사업 수행 역량

- AI 기반 최신 글로벌 보안 위협 선제적 대응
- 네트워크 보안 솔루션 개발을 통해 축적된 시큐아이 자체 보안 기술력
- ITO 운영, 보안 솔루션 구축/운영, 보안 관제 영역 리더십 확보

전문적인 보안 관제 인력 보유

- 네트워크 보안 솔루션 개발을 통해 축적된 시큐아이 자체 보안 기술력
- 악성코드 분석, 모의해킹, 보안 컨설팅 등 최고 수준의 보안 전문가 보유계

특화된 품질 보증

- 시큐아이만의 선진화된 사업 관리 방법론 적용을 통한 서비스 질 향상
- 보안관제 및 운영 서비스 수준 관리(SLA) 경험 기반 고품질 서비스 제공

최신 위협 대응

- 시큐아이의 자체 최신 보안 위협 정보 제공
- 글로벌 위협 정보 제공 및 분석 활용

CSOC

05 보안 관제 서비스 기대 효과

TCO 절감	운영 비용 절감	• 보안 장비 구축 운영 비용 절감(임대) 및 전문 인력 보유에 필요한 비용 절감 • 24시간 365일 감시 체계 • 운영 비용 절감
운영 시스템 안정성 확보	안정적인 비즈니스 환경 구축	• 고객 서비스 및 내부 업무 관련 운영 시스템에 대한 사이버 침해 대응 강화 • 보안 취약점 점검 및 신규 위협 정보 제공을 통한 시스템 안정성 확보 • 휴일, 야간 등 비근무 취약 시간대에도 안정적인 IT 자산 운영 가능
비즈니스 경쟁력 제고	체계적인 보안관리 노하우 적용	• 네트워크, 홈페이지, 클라우드까지 다양한 영역 보안관제 적용 • 예방부터 조치 확인까지 취약점 점검 방법 및 수행 체계에 대한 노하우 활용

CSOC

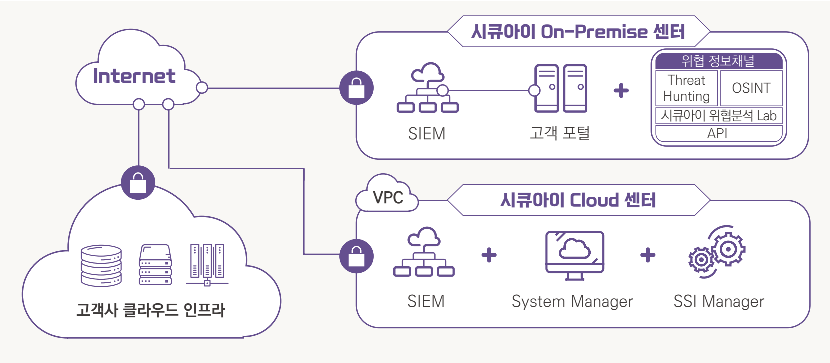
06 원격관제 서비스 유형

항목	기본서비스	부가 서비스
방화벽/IPS DDoS/WAF Anti-APT/웹쉘	**솔루션 통합 이벤트 모니터링(24 * 365)** • 보안시스템 장애/성능 모니터링 (Alive Check) • 보안 이벤트 통합 감시 • 장애 감시	**보안솔루션 운영 서비스** • 실시간 로그 백업
	침해 사고대응 서비스 • 침해사고 발생 시 HotLine 지원 • 침해사고 대응 및 분석 리포트 제공	**보안솔루션 Delivery** • 보안솔루션 임대 서비스
	Reporting 서비스 • 월간 관제 서비스 보고서 발송/정기적인 보안정보 제공 • Web을 통한 고객사 리포트 조회 가능	**보안솔루션 운영 서비스** • 보안솔루션 원격 관리/운영 • 보안정책 구성 및 원격 Update
	기술 지원(24시간) • 보안 기술 지원 • 서비스 개선 및 불만 사항 접수	
엔드포인트 (EDR)	• MDR 서비스 • 이상행위 모니터링 및 분석 • 상세분석을 통한 정/오탐 대응	• 보안 정책 최적화 방안 가이드 • 침해사고 대응 서비스 • 침해사고 발생 시 분석 전문가 현장 투입
악성 URL 탐지	고객사에서 운영하는 도메인(URL)에 대한 악성코드 경유지 및 유포지 탐지	
취약점 진단	**대상 시스템 분석** • 정보흐름 분석 및 예상 취약점 도출 • 취약점 점검 대상 시스템 정의	**모의침투 테스트** • 외부 해커와 동일 환경에서 고객사 운영 시스템의 침투 테스트
	모의해킹 및 취약점 점검 • 시스템/서비스 대상으로 해커와 동일한 입장에서 모의해킹 • 악성코드/APT 공격 형태의 자료 유출 및 내부 접근 가능성 점검	
	접근 가능성 점검 • 취약점 점검 프로그램을 통한 취약점 확인 및 추가 모의해킹	
	개선과제 수립 • 취약점 및 원인 분석에 대한 진단 결과 보고서 • 진단 영역별 주요 원인에 대한 조치 방안 제시 • 우선순위에 따른 Quick Fix/단기/장기 개선 과제 제시	
해킹메일 모의훈련	**실제 악성 메일과 유사한 패턴으로 모의훈련 실시** • 가상의 계정으로 직원에게 해킹 메일 (악성/스팸메일) 발송 • 첨부 파일 열람 및 링크 클릭할 경우 '경고창' 알림 • 해킹 메일 열람자는 감염 사실을 인지 후 신고	

CSOC

07 클라우드 보안 관제 서비스 구성도

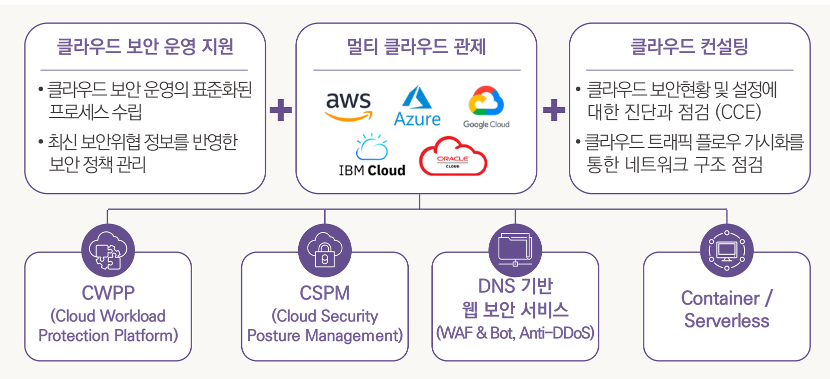
On-Premise와 클라우드 환경에 구축된 시큐아이의 AI 기반 보안관제 전문 플랫폼을 통해 실시간 보안 위협에 대해 즉각적이고 체계적인 분석 및 대응 서비스를 제공합니다. 글로벌 사이트의 보안관제 경험과 시큐아이 위협분석 Lab을 통해 수집된 다양한 위협 정보를 관제 정보(이벤트)와 결합하여 위협 정보 연관 분석 체계를 구축하여 운영합니다.



CSOC

08 클라우드 보안 관제 서비스 유형

멀티 클라우드 구축/운영 전문 역량을 바탕으로 시큐아이의 보안관제 전문 인력이 24×365 클라우드 환경의 실시간 보안 위협 탐지 및 대응·분석 서비스를 제공합니다. 또한 클라우드 보안 현황 진단/점검 등 보안 체계 강화를 위한 시큐아이 고유의 클라우드 전문 컨설팅 서비스를 제공합니다.



STIC
(SECUI Threat Intelligence Center)

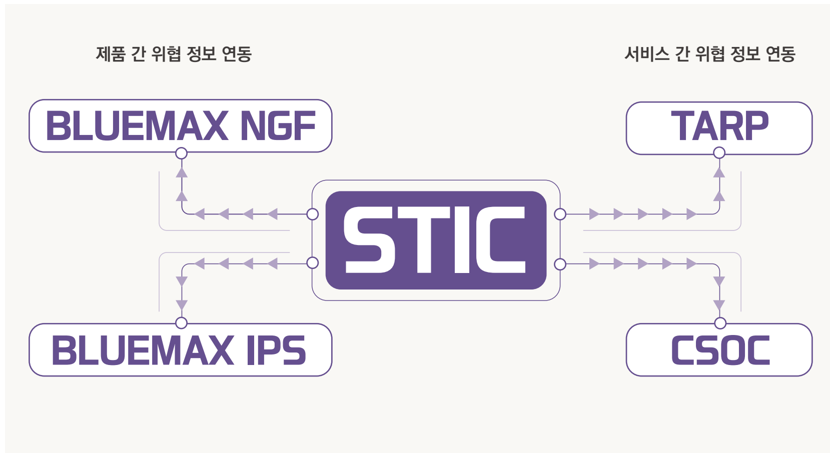
시큐아이 위협 분석 플랫폼

STIC은 시큐아이만의 위협 심층 분석 기술과 분석 전문가의 노하우가 집약된 위협 인텔리전스 플랫폼입니다.
강력하고 신뢰할 수 있는 인텔리전스를 통해 고도화된 지능형 위협에 대한 포괄적이고 심층적인 인사이트를 제공합니다.

STIC

01 서비스 개요

지능적이고 고도로 발전하는 위협 공격에 신속하게 대응하기 위해서는 실시간으로 발생하는 위협을 정확히 분석하는 것이 필요합니다. STIC(SECUI Threat Intelligence Center)는 위협 정보를 빠르게 확보하고 분석한 결과를 토대로 보안 이슈가 발생하기 전에 '위협 인텔리전스-TI (Threat Intelligence)'을 제공하는 서비스입니다.



STIC

02 특장점

글로벌 보안 위협 정보 수집력

- 글로벌 TI 정보 수집(VirusTotal, Webroot, Kaspersky 등)
- 자사 헌팅 센서를 통한 국내 유입 공격 정보 수집

글로벌 Top Tier 수집·분석 체계

VirusTotal	Webroot	Kaspersky
글로벌 TI (위협 정보)	글로벌 URL/Domain/IP 위협정보	글로벌 악성코드 위협정보

시큐아이 수집·분석 체계

전문가 수집	직접 구축한 수집 네트워크	고객 네트워크
OSINT 정보 수집	자체 구축 Threat Hunting	4만여 대 고객 네트워크

전문적인 분석 체계

- 위협 분석 전문가들과 AI 보안 관제 센터 조직 연계 심층 분석 체계 구축
- 양질의 위협 대응 정보 추출 및 분석 제공
- 블랙리스트, C&C, 악성 URL 최신 위협 정보 제공 시큐아이 시스템 자동 연계

조직	프로세스	시스템
역할별 전문가 조직 보유	체계적인 운영 프로세스 확립	통합된 위협 정보 플랫폼 보유
관제(CSOC) 침해대응센터(CERT) 연구/개발(R&D)	수집 · 분석 · 대응 · 조치	위협 분석 플랫폼 STIC

STIC

02 특장점

심층 분석 제공

- 심층 분석을 통한 위협 분석 정보는 위협에 대한 높은 가시성 제공
- 발생한 위협에 대해 신속한 의사 결정 및 사전 보안 정책 수립 활용 가능

딥 러닝 기반 파일/URL 분석

대량의 학습 데이터를 기반으로 만들어진 딥러닝 기반 AI 엔진이 알려지지 않은 피싱 사이트, 악성코드 등을 탐지합니다.

샌드박스 행위 분석

실제 감염 시스템과 동일한 환경에서 악성코드 동적 행위를 로깅하고 강력한 행위 기반 시그니처로 악성코드를 탐지합니다.

안티바이러스 스캔

세계 최고 수준의 기술력을 갖춘 안티바이러스를 활용한 악성코드 탐지 결과를 제공합니다.

평판 정보 분석

신뢰도 높은 다양한 출처에서 수집된 방대한 양의 평판 정보를 활용해 알려진 위협에 대한 신속한 탐지가 가능합니다.

동적 메모리 분석

악성코드 동작 시에 사용되는 메모리 데이터를 분석하여, 안티바이러스와 샌드박스에서 놓치는 위협을 효과적으로 탐지합니다.

실시간 URL 스캔

URL 평판 정보 분석과 동시에 실시간으로 URL에 접속하여 다양한 분석 엔진들로 위협 요소를 찾아내고, 관련 도메인, IP에 대한 추가 정보를 제공합니다.

위협 상관관계 분석

발견된 위협 정보들의 연관성을 분석해 과거에 발견되지 않은 위협 탐지와 미래 위협에 대한 사전 대응이 가능하도록 합니다.

Security Service 03

SECUI Consulting Service

정보보호 컨설팅 서비스

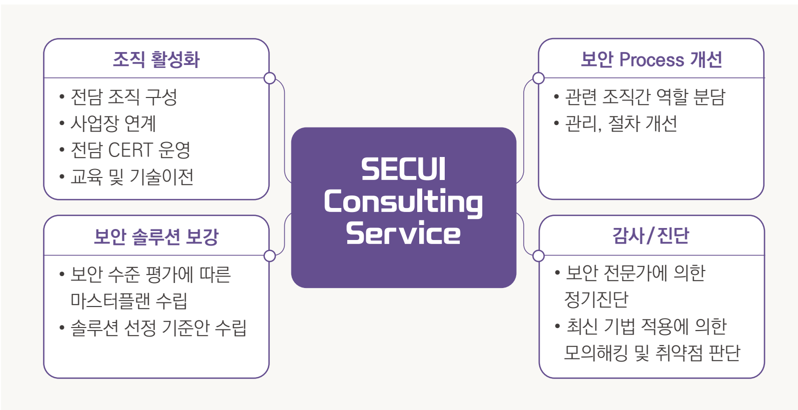
시큐아이는 국내 1호 정보보호 컨설팅 전문 업체로 정보보호 컨설팅 분야에서의 풍부한 경험과 전문성을 바탕으로 고객 지향적인 서비스를 제공하고 있습니다.
검증된 GAUSS 컨설팅 방법론을 통한 전문적인 분석으로 완벽한 프로젝트 관리를 지향합니다.

SECUI Consulting Service

01 특장점

고객 지향적 보안 컨설팅 서비스 제공

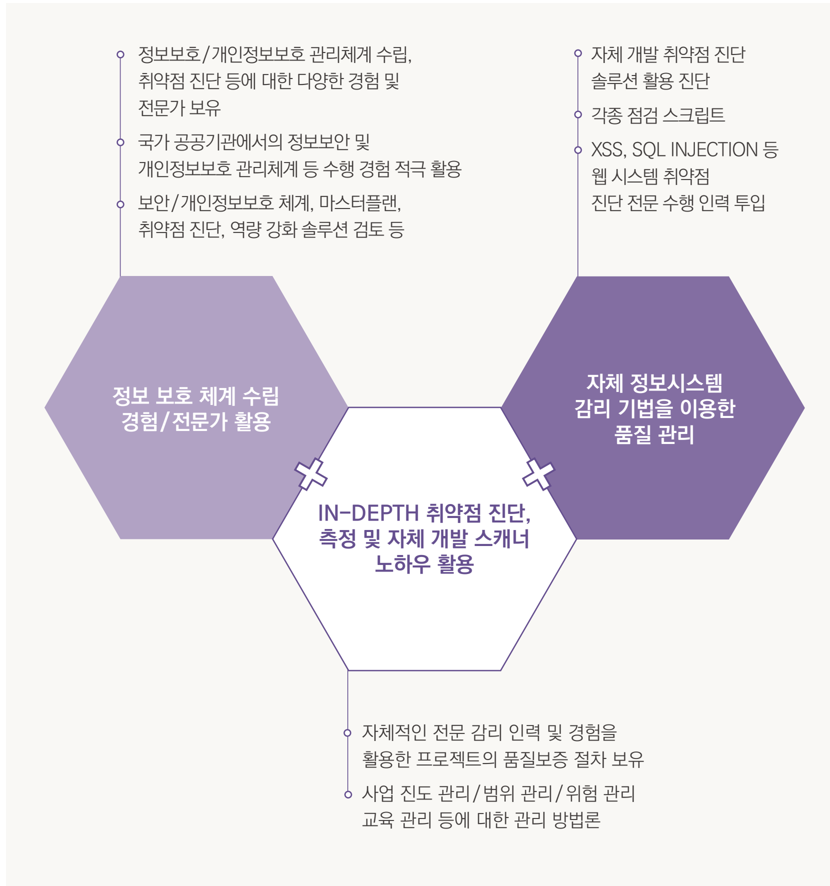
- 고객 요구 사항 기반 정보보안 솔루션 도입에서 시스템 운영까지 전 영역 보안 컨설팅 서비스 제공
- 고객과 함께 프로젝트를 수행하여 컨설팅 노하우 전수
- 프로젝트 종료 후, 지속적인 고객 서비스를 통해 문제점 및 방안 제시



SECUI Consulting Service

02 시큐아이 보안 컨설팅의 차별성

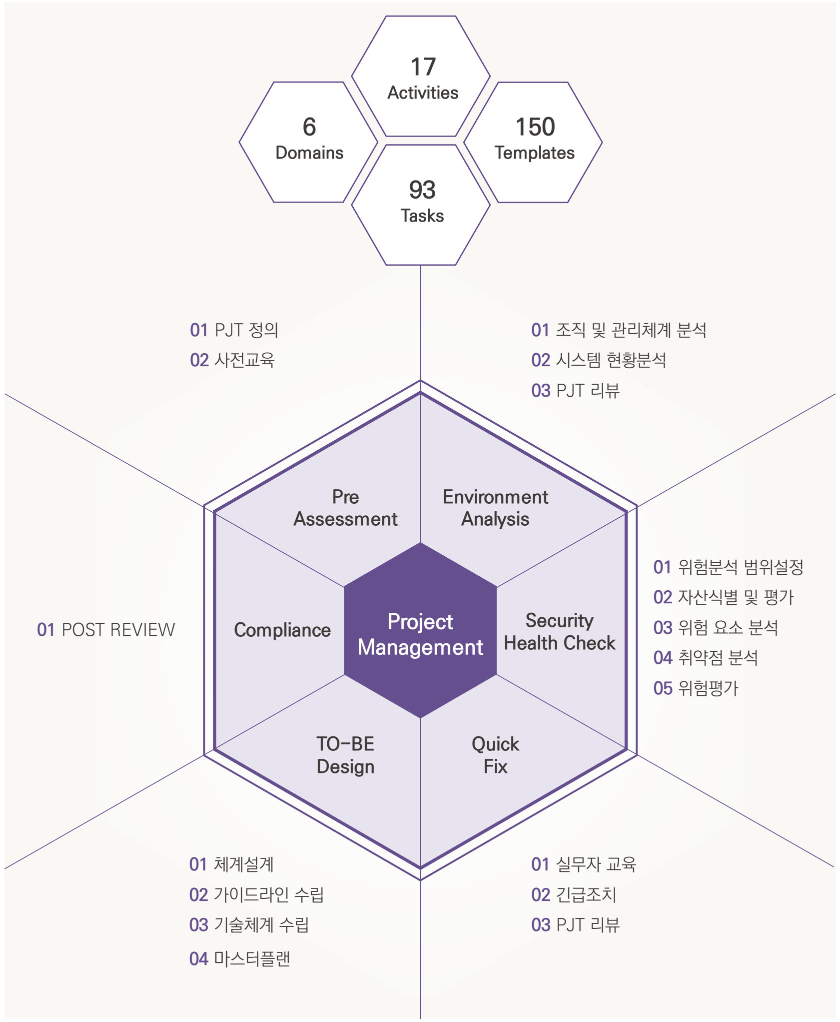
시큐아이 보안 컨설팅의 차별성은 다양한 프로젝트 수행 경력이 있는 전문가를 투입하고, 심층적 취약점 진단 노하우를 활용하며, 정보시스템 감리 기법을 이용한 품질 관리를 통해서 성공적 사업 수행을 보장하는 것입니다.



SECUI Consulting Service

03 컨설팅 방법론 (GAUSS, The Global Architecture of Unified Security Scheme)

GAUSS 방법론은 정보시스템에 대한 체계적인 감사, 통제 및 보안을 위해 필요한 정책, 수행 방법, 도구 등을 체계적으로 정리, 6개 영역으로 표준화한 시큐아이 고유의 컨설팅 방법론입니다.



GAUSS 방법론은 국내외의 표준 및 다양한 수행 경험을 통하여 국내 환경에 맞도록 개발되었으며 고객 요구 및 프로젝트 특성에 따른 최적화, 수행 단계별 품질 검토 및 사후 관리를 통하여 생산성 및 품질 향상을 통한 성공적인 프로젝트 수행을 보장합니다.

현장 중심의 종합 방법론	• 고객 사업 특성 분석에 기반한 수행 최적화 • 체계적인 교육 및 기술이전, 고객 참여 극대화로 고객의 역량 강화 • 정보보호 영역 및 기술 요소 전반에 대한 분석 및 진단 • 최신의 다양한 분석 및 진단 기법 활용 – 자동화 도구, 모의해킹, 보안 테스트
지속적인 개선과 진화	• 표준 프로세스 준수와 사후관리 수행 풍부한 템플릿, 체크리스트 등의 활용 및 개선 • 다양한 프로젝트 수행 경험과 지식의 축적 및 관리 • 수행 단계별, 모듈별로 계획, 실행, 검토, 개선의 순환 모델 적용
국내외에서 검증된 방법론	• 국내외 보안 및 감리 표준 수용 – COBIT, ISO27001, KISA ISMS, 금감원 보안 기준 • 다수의 공공기관 및 기반 시설에 적용하여 성공적으로 프로젝트 수행 • 체계적이며 일관된 프로젝트 관리 기법 적용

SECUI Consulting Service

04 컨설팅 기대효과

성공적인 컨설팅을 통하여 대내적으로는 보안 관리 수준 향상, 정보보호 투자 기반 마련, 효과적 취약점 관리는 물론 대외적으로 법적 준거성 확보와 대고객 신뢰도 향상을 기대할 수 있습니다.

정보보호 관리 수준 향상
• 정책 지침 제/개정 및 프로세스 설계를 통한 보안 실행 수준 향상
• 정량적 보안 수준 도출 및 지속적인 수준 향상

보안 및 개인정보 관련 법적 준거성 확보
• 상위기관의 지침 및 현행 법 규정에 대한 준거성 구축
• 향후 예상되는 개인정보/방재 등의 관련 법규에 유연하게 대응할 수 있는 분석의 틀 마련

비용 효과적인 정보보호 투자 기반 마련
• 보안 아키텍처 현행화를 통한 기술 보안 투자 근거 도출
• 마스터플랜 수립을 통한 중장기적 정보보호 투자 로드맵 활용

대고객 신뢰도 향상
• 안정된 정보보호 기반 수립으로 대외 신뢰도 제고
• 정보서비스에 대해 안전이 보장된 서비스 제공을 위한 기반 조성

정보보안 취약점의 효과적 관리
• 네트워크, 서버, DB 등 정보통신 시설 보안성 확보
• 자체 개발 운영 중인 애플리케이션에 대한 보안 관리 방안 도출

Security Service 03

SECUI Consulting Service

05 주요 정보보호 컨설팅 서비스

국가의 주요 정보통신 기반 시설과 민간 기업들을 대상으로 전문적이고 고객 지향적인 정보보호 컨설팅을 제공하고 있습니다.

컨설팅 구분	특징
주요 정보통신 및 전자금융 기반 시설 취약성 분석·평가	주요 정보통신 및 전자금융 기반보호법상의 주요 정보통신기반시설에 대한 취약성 분석·평가 및 보호 대책 수립을 위한 정보보호 컨설팅 서비스
ISO/IEC27001, KISA-ISMS/PIMS 인증 지원	국제적인 정보보호 관리체계인 ISO/IEC27001 또는 과학기술정보통신부의 정보보호 관리체계(ISMS)인증 및 개인정보보호 관리체계 획득을 위한 인증지원 컨설팅 서비스
모의해킹/보안 취약점 진단	CERT 조직에 의한 모의 침투를 포함한 대상 시스템의 기술적인 진단을 수행하고 그에 따른 대응책을 제시하는 서비스
통합 보안	일반 기업이나 기관의 관리적, 기술적, 물리적 보안을 대상으로 진단, 분석, 설계, 마스터플랜 수립을 수행하는 고객 맞춤형 컨설팅 서비스

시큐아이는 고객 환경에 적합한 맞춤형 정보보호 컨설팅 서비스를 제공하고 있습니다.

서비스 구분	특징
파스칼 서비스	컨설팅 수행 후 연간 유지보수 계약 프로그램 형태로 정기적인 취약성 진단 및 모의 심사(감사)를 통해서 인증 사후 심사 또는 기반 보호시설보호 대책 수립을 지원하는 서비스
솔루션선정 및 BMT 지원 서비스	신기술의 정보 보호시스템을 성공적으로 도입하고자 하는 기업 및 기관을 대상으로 BMT 주관 및 정보 보호 체계 수립을 지원하는 서비스
웹 애플리케이션 코드 감사 서비스	E-biz 의존성의 높은 기업/기관을 대상으로 웹 애플리케이션의 보안 개발 가이드라인 제시 및 애플리케이션 코드 감사를 지원하는 서비스
보안 감사 대행 서비스	내부 보안 강화를 위하여 제 3자에 의한 보안감사를 필요로 하는 기업 대상의 서비스
맞춤형 보안 진단 서비스	일반 기업이나 기관의 보안 요구사항을 기준으로 정보보안의 대응책을 제시하는 서비스

04

Appendix

SECUI End of Service Life

유지 관리 종료 정책

제품은 기술 혁신, 제품 발전, 부품 단종 등으로 수명 주기를 마치게 됩니다. 이러한 과정은 최신 보안 기술에 대한 시장의 요구사항을 반영하고 나아가 고객에게 우수한 제품을 제공하기 위함입니다. 이를 위해 시큐아이는 더 나은 기능, 우수한 성능 보장, 제품 안정성 보증을 위해 제품 사용 연차에 따른 유지관리 종료 정책 EOSL(End of Service Life)을 시행하고 있습니다.

01

SECUI End of Service Life

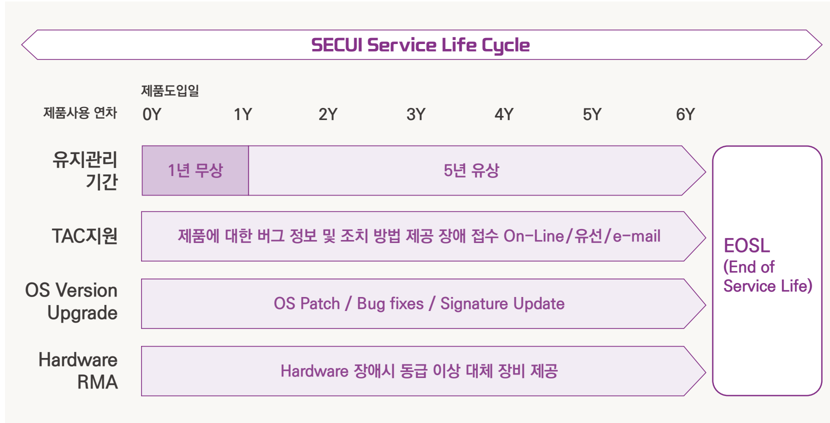
용어 정의

유지관리 서비스 종료 EOSL(End of Service Life)	유지관리 서비스를 중단하는 날짜로 고객사 도입일로부터 만 6년 초과 시 유지관리 서비스 종료
최종 유지관리 계약 LOS(Last Order for Service)	유지관리 서비스 종료(EOSL) 1년 전 마지막 유지관리 연장 계약(최대 12개월)

02

SECUI End of Service Life

유지 관리 종료 안내



03

SECUI End of Service Life

유지관리 서비스 종료 정책 안내

01 고객사 도입일로부터 만 6년까지 유지관리 서비스 제공

02 도입일로 부터 1년까지는 무상 서비스를 제공하며, 이후 5년간은 유상 유지관리 계약을 통하여 서비스 제공

03 시큐아이 기술지원 센터(TAC)는 유지관리 서비스 계약에 따라 도입 후 6년간 고객지원 서비스를 제공하며, OS 버전 업그레이드, 하드웨어 수리 및 장애 대체 장비 지원(RMA) 서비스를 제공

04 최종 유지관리 계약은 EOSL 도래 시점으로부터 1년 전 체결되며, 계약 기간은 최대 12개월 내로 제한

05 제품 도입일로부터 만 6년이 초과할 경우 유상 유지관리 서비스는 종료(EOSL) 되며, 더 이상 관련 서비스를 제공하지 않음

06 유지관리 서비스를 제공하는 시큐아이 공식 파트너는 시큐아이의 유지관리 서비스 종료 정책을 고객사에 공지할 의무가 있음

SECUI Security Solution Guide ver. 1.0

시큐아이 제품 및 서비스 가이드 **Second Edition**

제작 : ㈜ 시큐아이
편집 : 마케팅기획팀
발행 : 2026.8

시큐아이는 대한민국 최고의 공급 파트너와 함께 고객 환경에 맞는
보안 솔루션을 신속하고 전문적으로 제공하고 있습니다.
시큐아이 전문 파트너사 정보는 시큐아이 홈페이지에서 확인하실 수 있습니다.

시큐아이 전문 파트너사 안내
https://www.secui.com/support/distributor