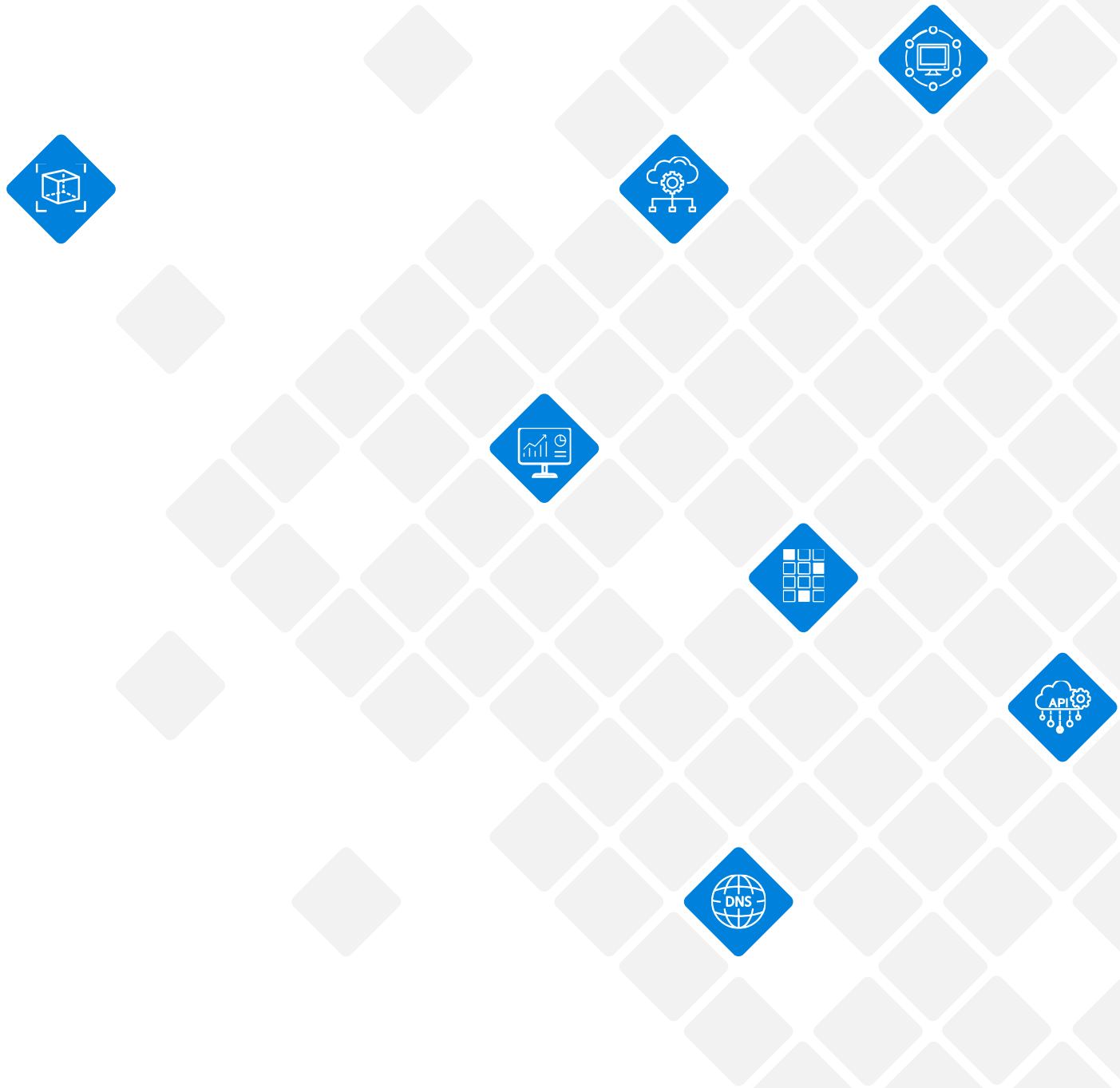
SECURITY INTELLIGENCE PLAFORM
FOR ALL MY THREAT MANAGEMENT

BLUEMAX NGF

V 3.0

BLUEMAX NGF



BLUEMAX NGF

AGENDA

01 개요

02 특장점

03 상세기능

04 라인업 · 인증

01

- 개방형 네트워크 보안
- 가상화 클라우드 보안
- VIRTUAL CLOUD

  GENERATION FIREWALL

BLUEMAX NGF

개요

개방형 네트워크 보안

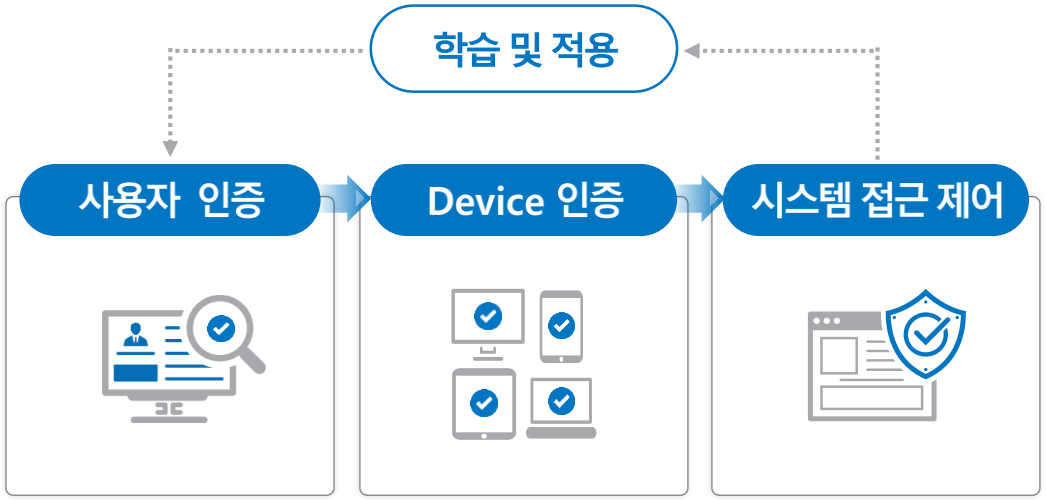
클라우드, 모바일 환경의 보편화로 **IT인프라 관문 중심의 경계보안 한계**

개방형 네트워크 환경		개방형 네트워크 보안 위협
언제 어디서나 접속	home, office, cafe, Park	**Any Location**	내외부가 구분되지 않는 트래픽, 암호화 트래픽으로 가시성 확보 어려움
내부 사용자 정보와 연동	MSAD, LDAP, radius, SQL, TACACS+	**Any User**	ID 해킹, 도용으로 내부 시스템 불법 접속
모든 디바이스, 브라우저 통신	desktop, laptop, tablet, mobile	**Any Device**	BYOD로 경계선 내부 시스템 접근
자유로운 소통	Kakaotalk, facebook, Youtube, Twitter, Instagram	**Any Application**	App 취약점, APT 공격으로 내부 감염
편리한 정보 공유	Amazon Web Services, Microsoft Azure, Salesforce Inc, Microsoft office 365, GitHub	**Any Service**	클라우드 환경 증가로 경계선방어 불가

네트워크 보안 중심의 통합 보안 플랫폼으로 **개방형 네트워크를 위한 보안 체계** 구현

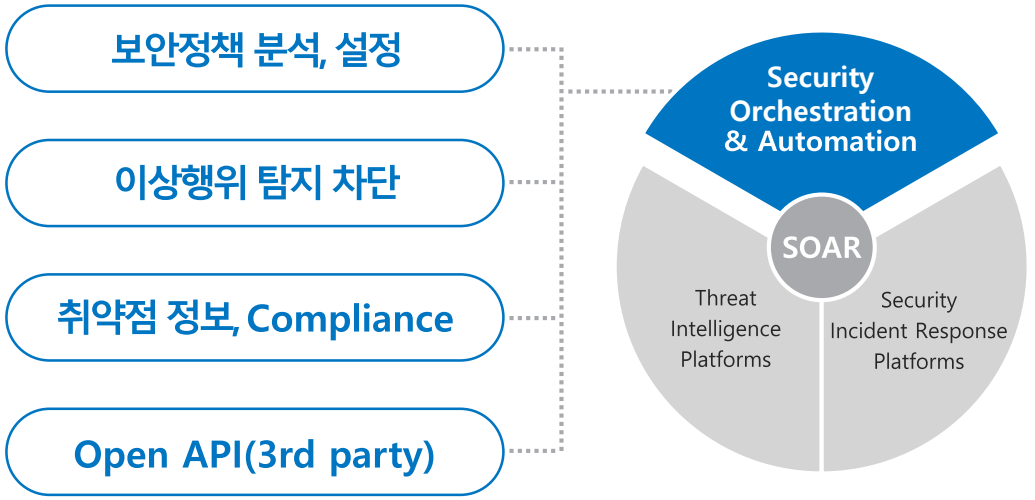
개방형 네트워크 보안 체계

Zero Trust Security



- "Developing a Framework to Improve Critical Infrastructure Cybersecurity" [NIST, Forrester Research, 04/2013]
- "Enterprise Architecture Beyond the Perimeter" [USENIX, Google, 08/2013]

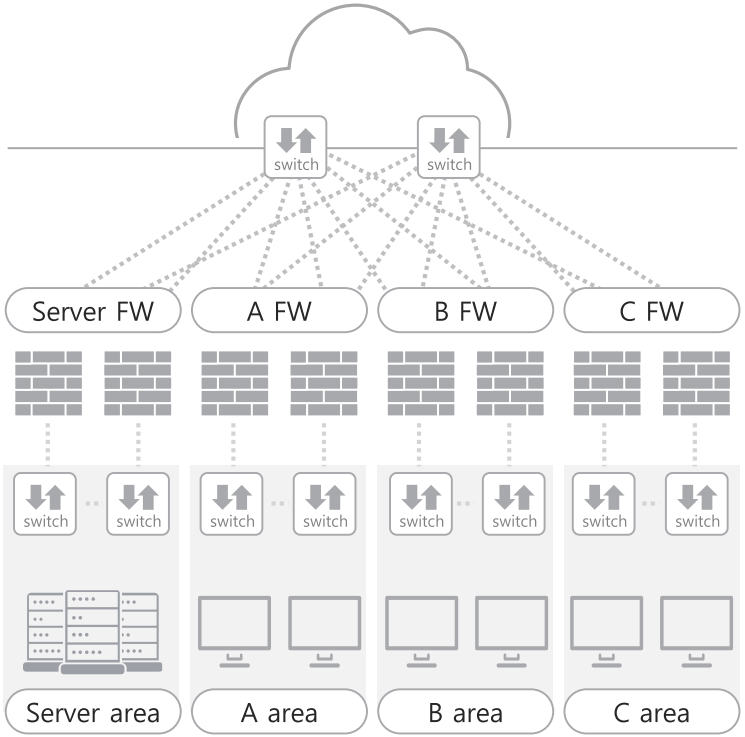
Security Automation



- "Network Security Policy Management Solution Have Evolved" [Gartner 10/2015]
- "Security Orchestration, Automation and Response" (SOAR)[Gartner 11/2017]

복잡한 네트워크 보안 구성을 단일 HW장비의 Virtual System으로 효율화

기존 네트워크 방화벽 구성

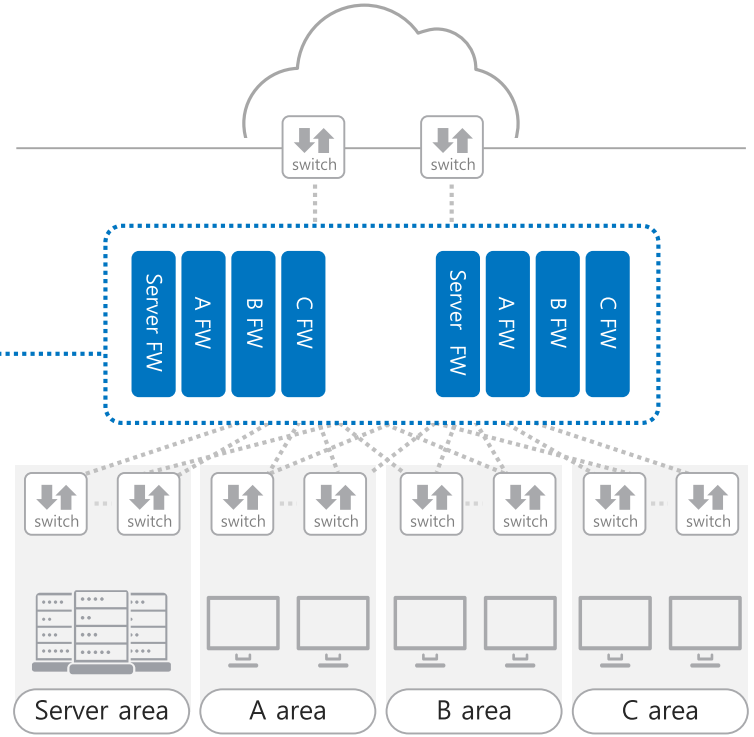


기존
랙실장도

개선 후
랙실장도

- 구축 비용, 상면적 75% 절감
- 구성 단순화로 장애 요소 저감
- 통합 및 개별 관리 편의성 동시 확보

Virtual System 네트워크 보안 구성



Virtual Cloud Generation Firewall이 갖추어야 할 7가지

01 Advanced Virtual System	방화벽 가상화로 다양한 네트워크 환경의 유연한 구성
02 Virtual Cloud Network	다양한 가상화/클라우드 환경 지원
03 User, App, Device Control	User, App, Device 인지/제어로 정교한 보안 정책
04 Malware Protection	랜섬웨어 등 엔드포인트의 위협 탐지 차단
05 Security Automation	보안정책 분석 설정의 Automation으로 관리 편의성 향상
06 Open API	개방형 연동 환경을 위한 Open API 제공
07 Threat Intelligence	Intelligence Platform 기반의 Threat Intelligence

SECURITY INTELLIGENCE PLATFORM

02

BLUEMAX NGF

특장점

- 통합보안 플랫폼(Security Intelligence Platform)
- 가상화 시스템(Virtual System)
- 보안 SD-WAN(Secure SD-WAN)
- 제로 트러스트 네트워크(Zero Trust Network)
- OT 보안(Operational Technology Security)
- 안정된 고성능 & 유연한 구성

SECURITY INTELLIGENCE PLATFORM

for All My Threat Management

BLUEMAX NGF VE

- Public, Private 클라우드 환경의 통합보안
- On-Premise의 복잡한 보안 구성을 Virtual System으로 효율화

Virtual Cloud Security

Malware Protection

BLUEMAX CLIENT

- Device의 Compliance 점검, 이상행위, 감염여부를 실시간 탐지하여 선제적 위협탐지 차단

NETWORK SECURITY

- App 제어로 트래픽 가시성 보장
- User 인증으로 비인가 접근 방지

BLUEMAX NGF

STIC CSOC

SECUI Threat Intelligence Center / Cyber Security Operation Center

- STIC : Smart Update, 글로벌 위협정보 서비스
- CSOC : AI 기반 위협분석, 원격관제 서비스

Threat Intelligence

Security Automation

BLUEMAX TAMS

- 수집된 위협정보, 보안로그, 취약점진단 결과를 종합 분석하여 보안정책 설정 자동화

V3.0 New Feature

개방형 환경 대응

Secure SD-WAN

- 애플리케이션 기반 라우팅 기능 제공
- 회선에 대한 품질 상태 체크를 통한 안정적이고 최적화 된 서비스 제공

ZTNA

- BLUEMAX CLIENT기반 디바이스 정보 수집 및 방화벽 정책 연동
- 외부 사용자의 인증 강화(생체/OTP인증)

차세대 가상화 방화벽

BLUEMAX NGF

Network Security

User ID, App, Device

IP, Port, Protocol

가상화 방화벽 다중 운영

Virtual F/W | Virtual F/W | Virtual F/W

신종 위협 대응

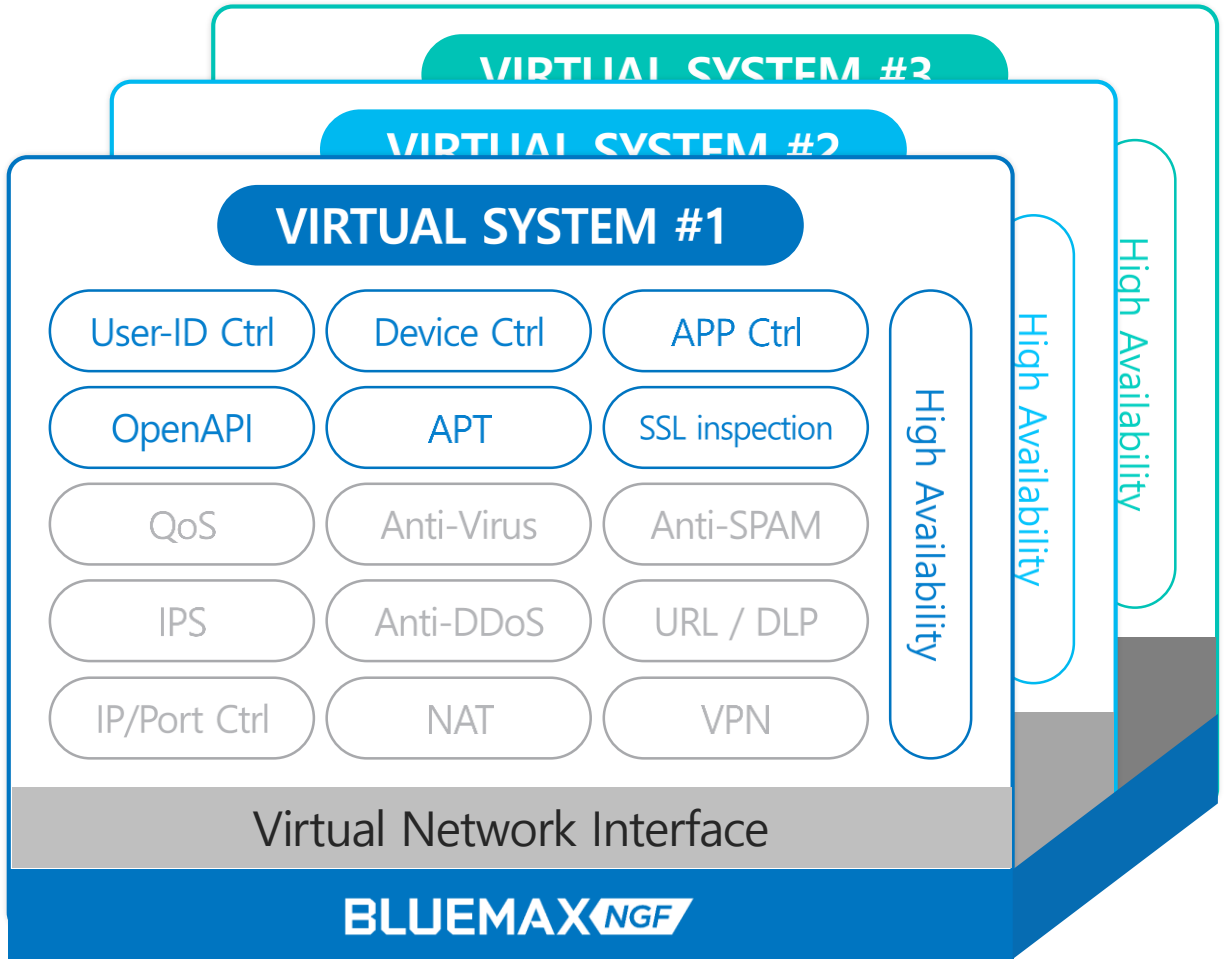
DNS Security

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

SaaS Application

- SaaS 전용 애플리케이션의 계정별 접근 제어 제공 (HTTP 헤더 제어)

최신 **Virtual System** 아키텍처로 완벽하게 독립된 가상 네트워크 보안



최신 기술을 활용한 가상 환경 지원

- 간편한 가상 시스템 생성 / 가상 시스템 별 자원 할당

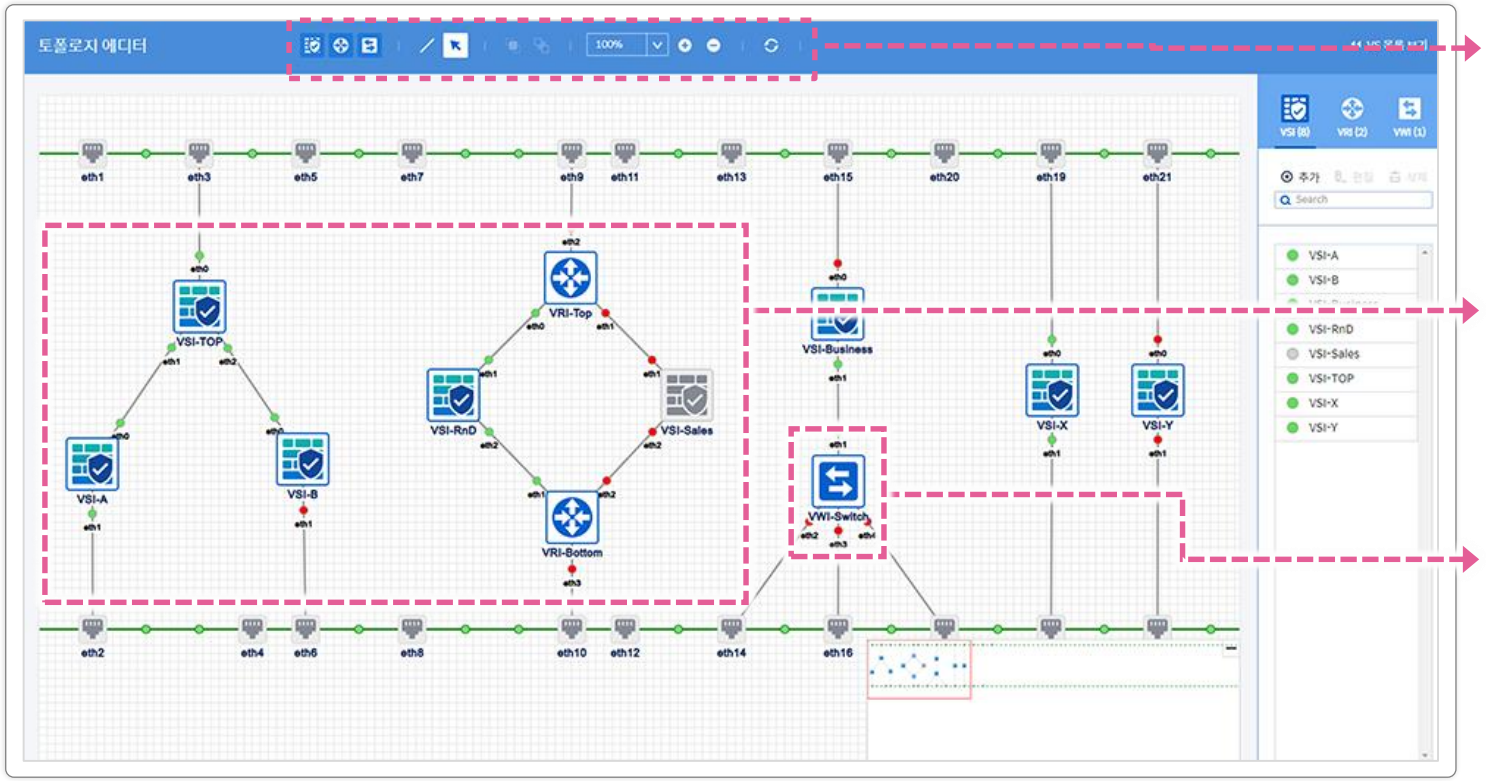
다양한 Virtual Network 구성 지원

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

독립된 Virtual System 자원 할당

- VS에 필요한 시스템 자원(CPU, MEM 등)을 유연하게 개별 할당하여 완벽한 독립 운영

Virtual System 토폴로지 에디터로 가상 방화벽의 직관적이고 편리한 구성 관리



직관적인 가상 네트워크 구축

- 아이콘 Drag & Drop
- 네트워크 맵으로 가시성 제공

다양한 가상 네트워크 구성

- High Availability with L2/L3
- Multi-Layered Security Zone

가상 네트워크 구성 요소

- VSI : 가상 방화벽 (Virtual Security Instance)
- VRI : 가상 라우터 (Virtual Router Instance)
- VWI : 가상 스위치 (Virtual sWitch Instance)

보안 SD-WAN

차세대 방화벽 기반의 Secure SD-WAN으로 최적화된 네트워킹과 보안 위협 동시 대응

1. 신종 위협 탐지/차단

- NGF에서 제공하는 IPS, 웹필터 기능으로 최신 보안 위협 대응 가능

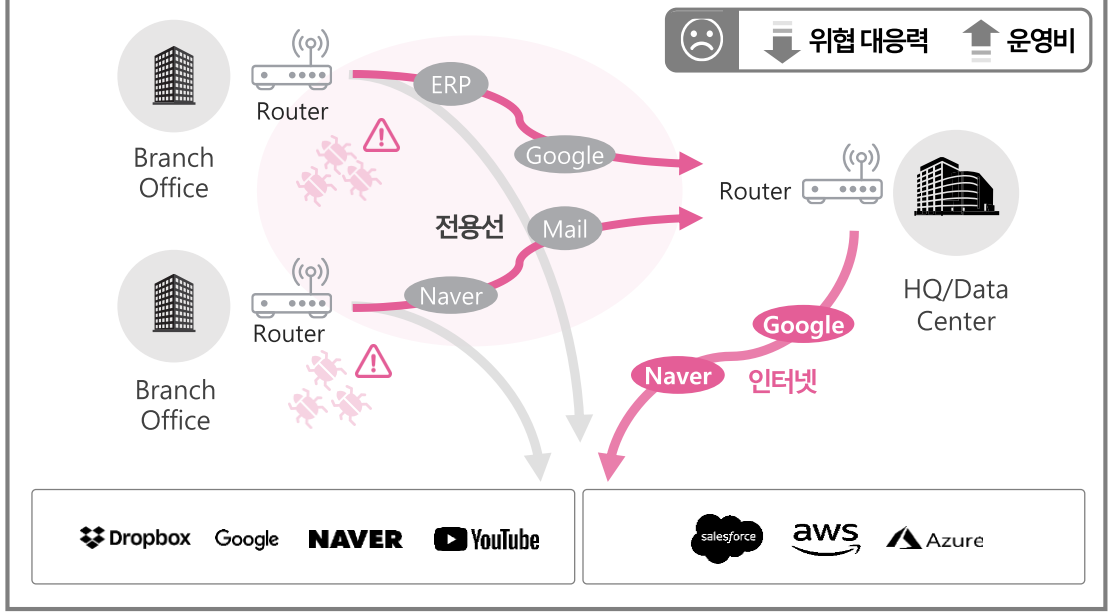
2. Zero-Touch Provisioning

- 회선 연결만으로 지사 장비 설치 및 운영 가능

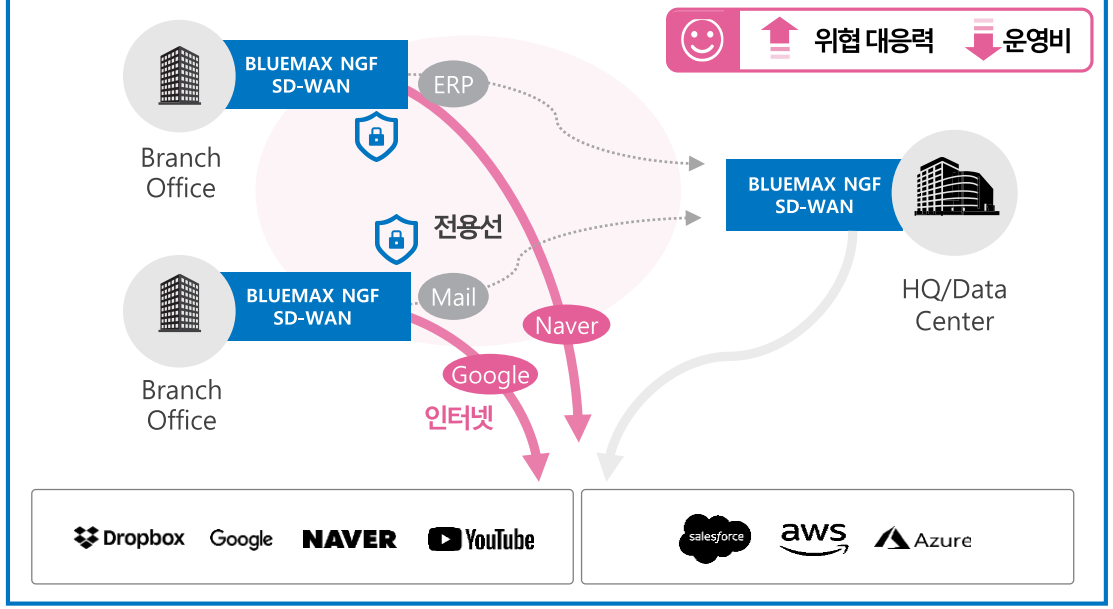
3. 애플리케이션 기반 /회선 품질 기반 트래픽 경로설정

- 애플리케이션 3300개 설정 가능
- Latency, Jitter, Packet Loss 실시간 체크
  ('24. 3Q 지원 예정)

다지점 일반 WAN 환경

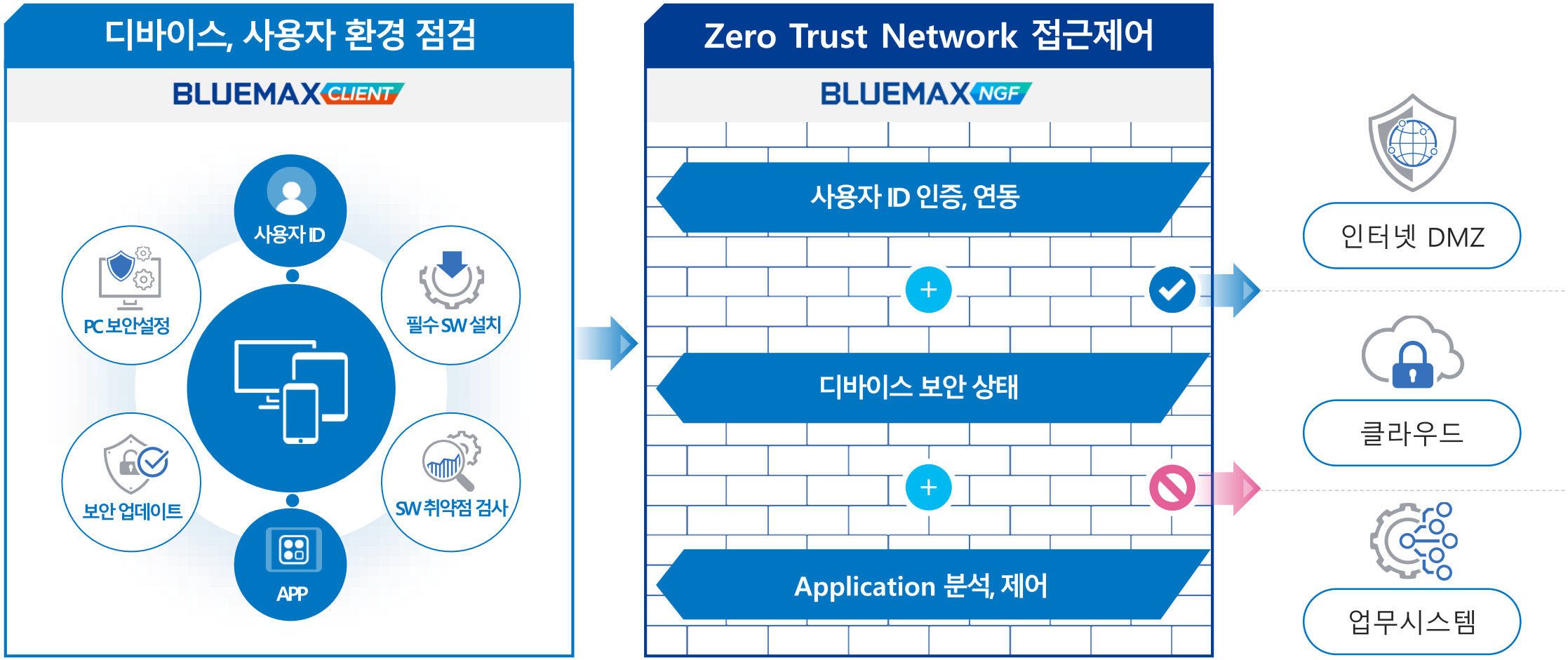


다지점 Secure SD-WAN 환경



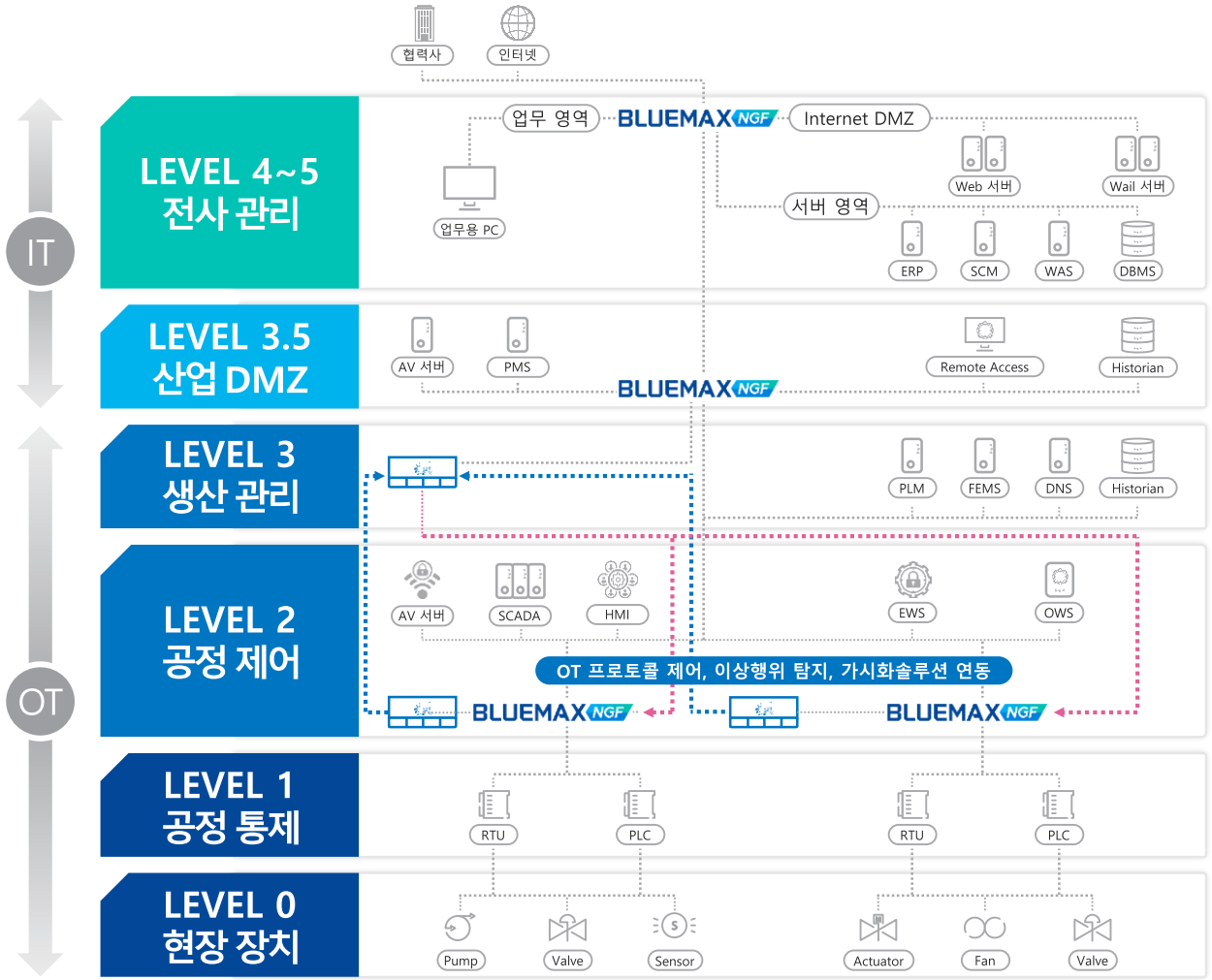
제로 트러스트 네트워크

디바이스의 보안상태, 사용자 ID, App 정보기반으로 **Zero Trust Network** 정책 적용



OT(Operational Technology)보안

OT 프로토콜 제어 및 이상행위 탐지, 가시화솔루션 연동으로 OT보안 강화



OT 프로토콜 제어

- OT 산업용 프로토콜 13종 제어
  (Modbus, DNP3, CIP, BACnet, CoaP, ADDP, OPC UA, S7, Profinet, XGT, EtherCat, mtconnect, DLMS)

OT 프로토콜 이상행위 탐지

- OT 프로토콜 분석을 통한 정교한 제어
  (Operation Function & Value Control)

OT 가시화솔루션 연동

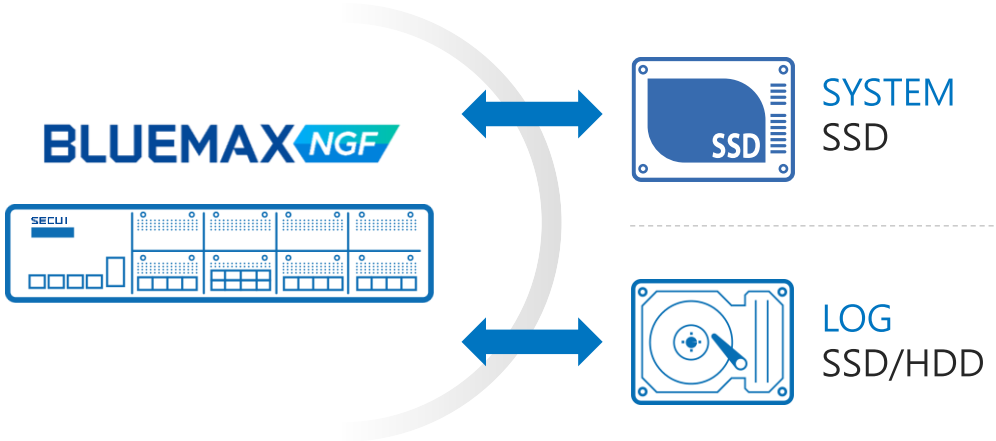
- 산업용 자산/자산그룹 및 통신정보 연동
  * 가시화솔루션 → 방화벽
- 연동정보를 활용한 OT 방화벽 정책 추천

안정적 고성능과 유연한 구성

안정된 고성능 고품질 무중단 서비스, **유연한 방화벽 mode 전환 제공**

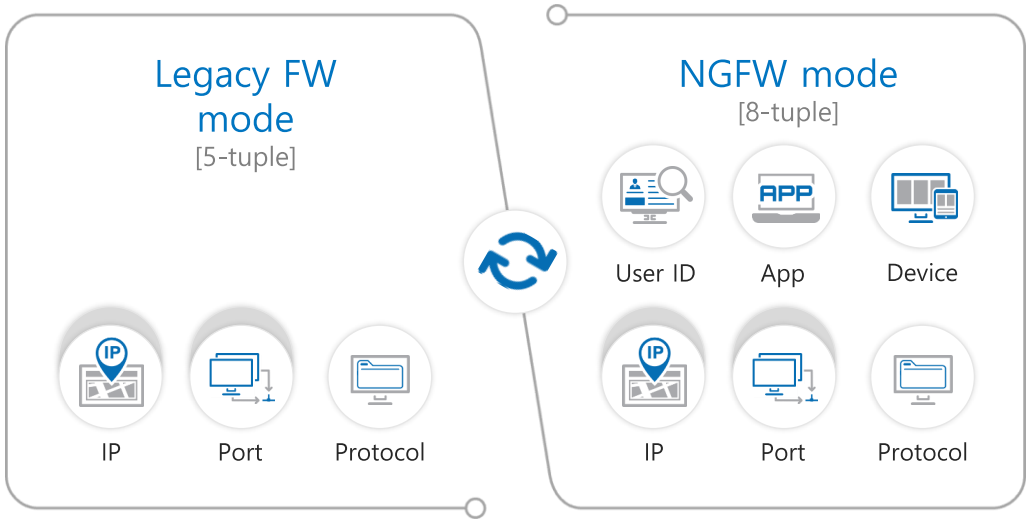
고가용성 HW 아키텍처로 무중단 서비스 제공

- **전체 모델 고성능 SSD(Solid State Drive) 기본 적용**
- 시스템 SW와 보안로그 저장 공간 분리
- Log 용 SSD의 RAID 구성, 주요 부품 Hot Swap 지원

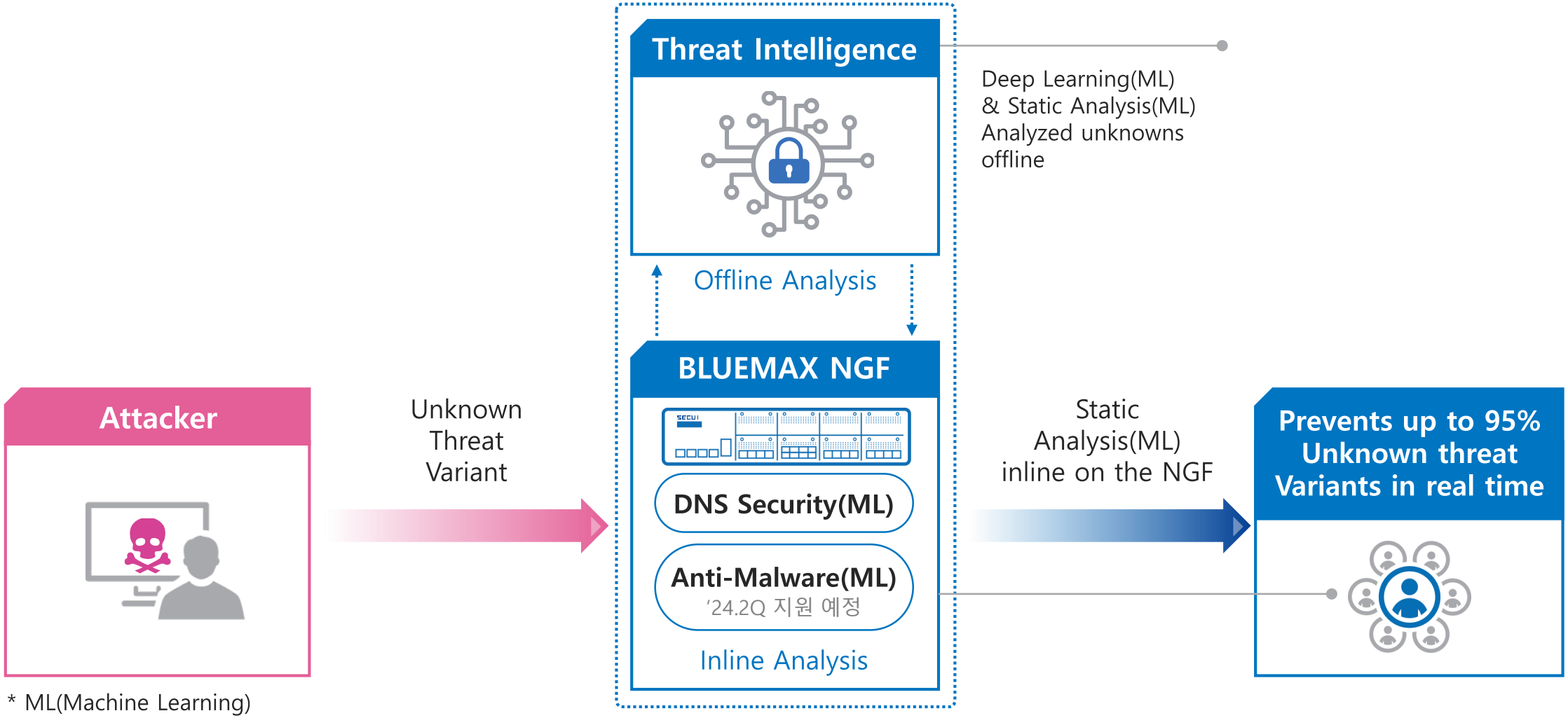


장비 교체 없이 Legacy FW과 NGFW 지원

- **Legacy FW mode, NGFW mode 전환**
- 기본 방화벽 성능이 우수한 Legacy FW mode와 정교한 보안 설정이 가능한 NGFW mode 동시 제공



ML-Powerd NGFW는 알려지지 않은 공격을 방어하는데 큰 도움



* ML(Machine Learning)

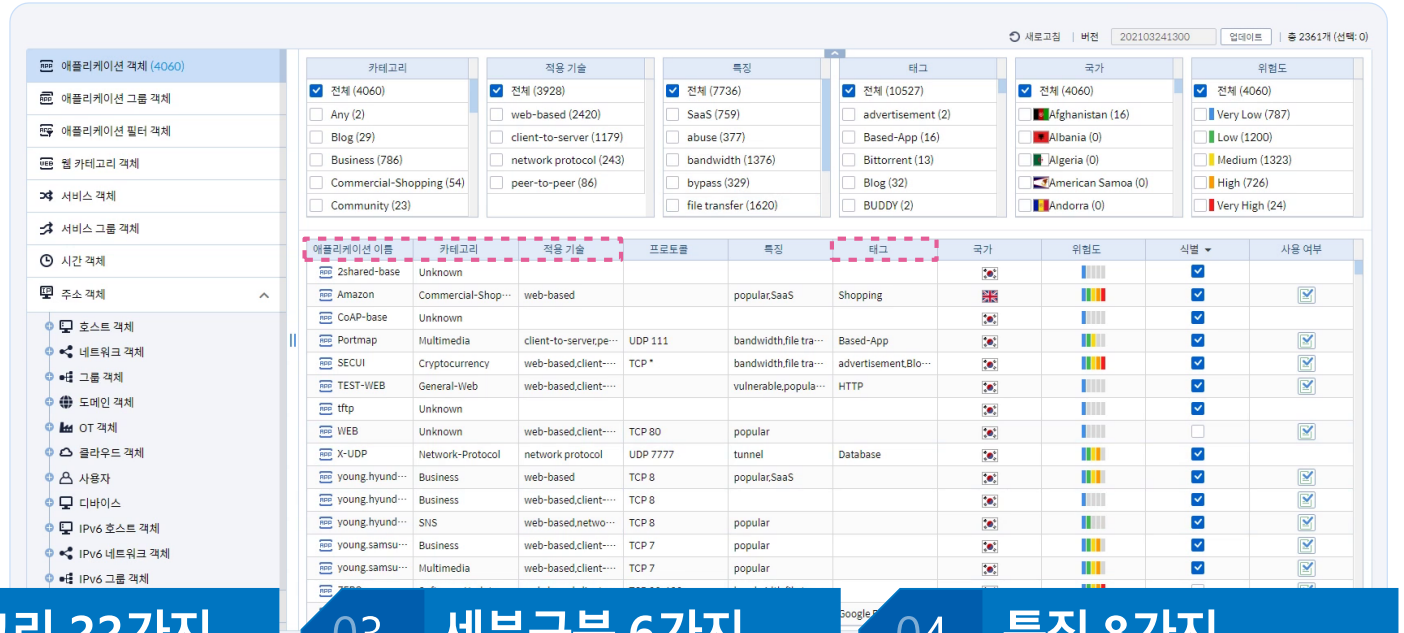
03

- Application 제어
- Cloud Access Security Inspection
- 도메인 객체(Domain Object)
- 사용자-ID 연동
- IPS & DDoS
- DNS 보안
- VPN(IPSec VPN)
- VPN(SSL VPN)
- BLUEMAX CLIENT
- BLUEMAX NGF Open API

BLUEMAX NGF

상세 기능

다양한 인터넷 프로토콜 분석과 정밀한 인지기반 정교한 Application 제어



01 어플 3,300가지

+ 3,300

02 카테고리 22가지

- Mail
- Game
- Community
- SNS
- Blog
- Multimedia
- Business
- Proxy-and-Tunnel
- Instant-Messenger
- Remote-Access-Tool
- Voice-over-IP
- Commercial-Shopping
- Finance-Stock
- P2P-File-Sharing

외 다수

03 세부구분 6가지

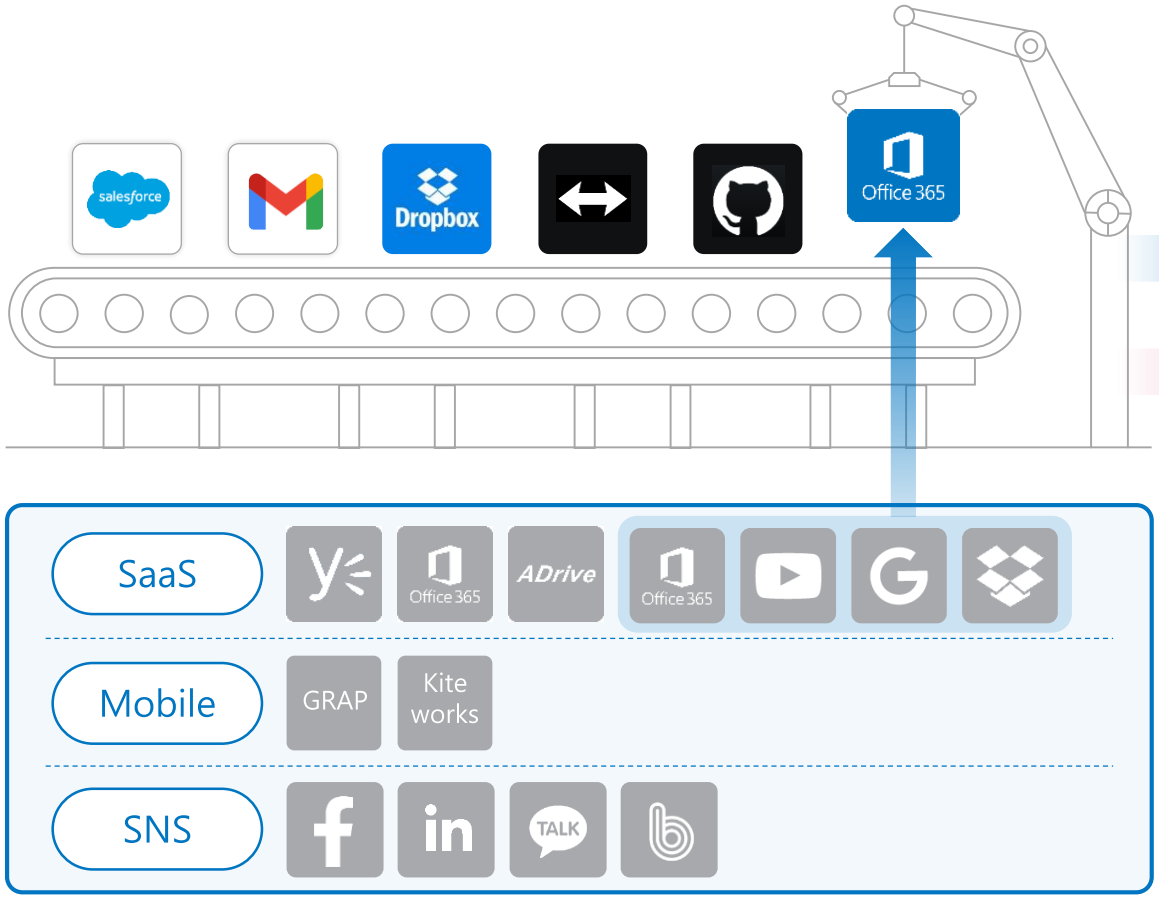
Base, Login, Video, Audio, File, Message

04 특징 8가지

Band width, File transfer, Bypass, Vulnerable, Tunnel, Popular, Abuse, SaaS

웹 카테고리 기반 애플리케이션 제어 및 SaaS HTTP Header Insertion

- 웹 카테고리 기반의 애플리케이션 상세 분류
- 약 700개의 SaaS 전용 애플리케이션 인지/제어



Enterprise 계정

개인 계정

SaaS Application HTTP Header Insertion

Access Allow

GET / HTTP/1.1
Host: login.microsoft.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0)
Restrict-Access-To-Tenants: secui.com

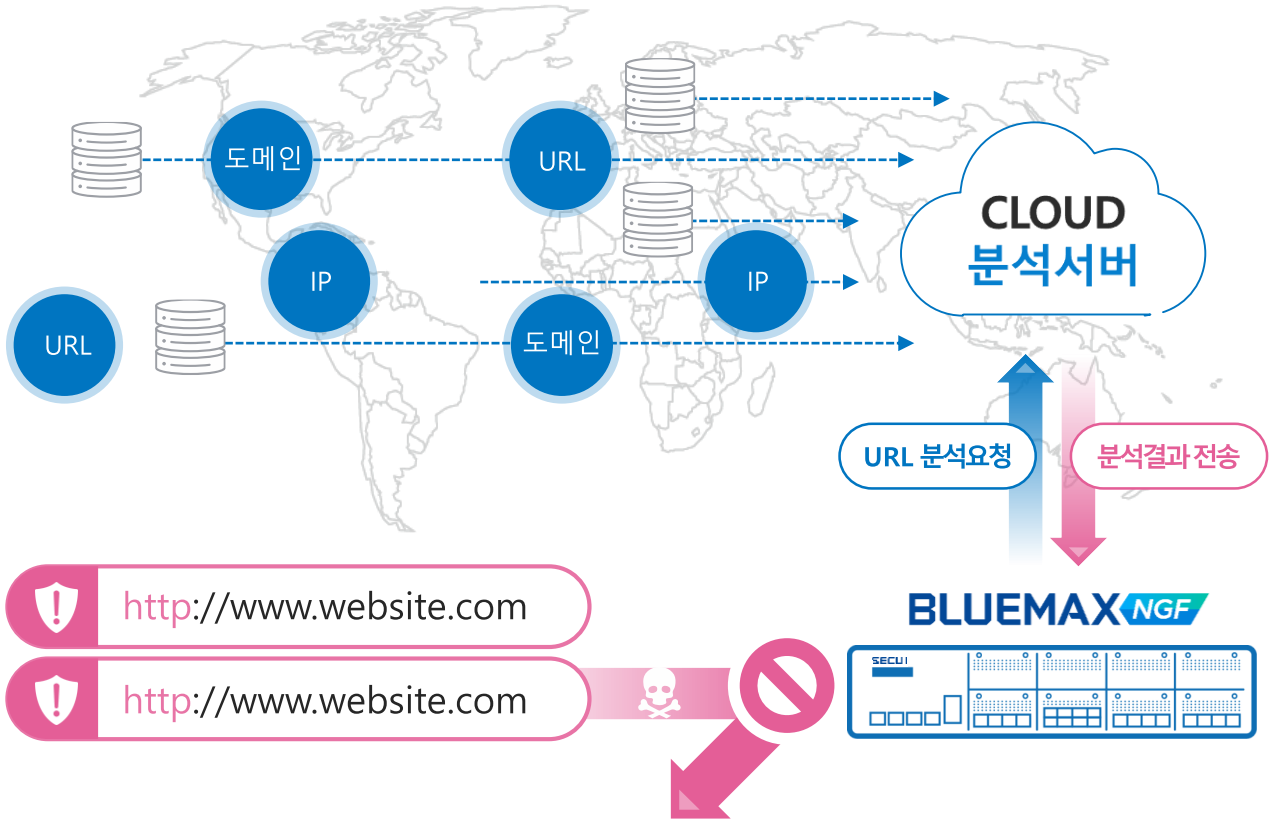
Access Denied

GET / HTTP/1.1
Host: login.microsoft.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0)
Restrict-Access-To-Tenants: gmail.com

- SaaS 전용 주요 애플리케이션 (Google G Suite, Dropbox, MS Office 365, Youtube) 도메인 제어
- HTTP 헤더, 헤더 값 제어를 통한 SaaS 애플리케이션 접근 관리

Global Web Filter인 **Brightcloud Threat Intelligence Service** 제공

- 7억개 이상의 도메인, 320억개의 URL정보 등을 82개의 카테고리로 분류된 웹필터 기능 제공
- 미 분류 URL은 CLOUD 서버로 분석 요청하여 업데이트 수행



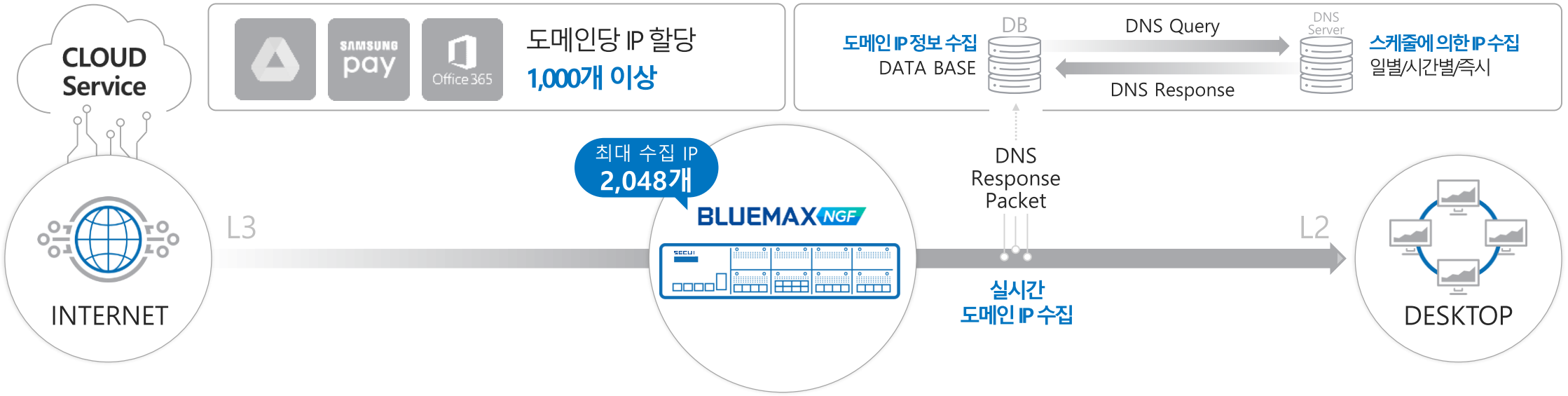
- 카테고리별 URL 검사
- 클라우드 기반 악성 URL 검사
- IP 주소 접근 제어
- Anonymizer 서버 우회 접속 차단

도메인 객체(Domain Object)

클라우드 서비스를 고려한 **도메인 IP 수집의 효용성 극대화**

기존 방식	BLUEMAX NGF 방식
관리자가 도메인의 IP를 직접 찾아(nslookup) 객체로 입력	도메인명을 객체로 입력 → 방화벽에서 자동 IP 수집, 업데이트 • 실시간 수집, 스케쥴 수집, 도메인당 최대 2048개 까지 지원 • 효율적 도메인 인식을 위한 Wild Card(* - Asterisk) 적용

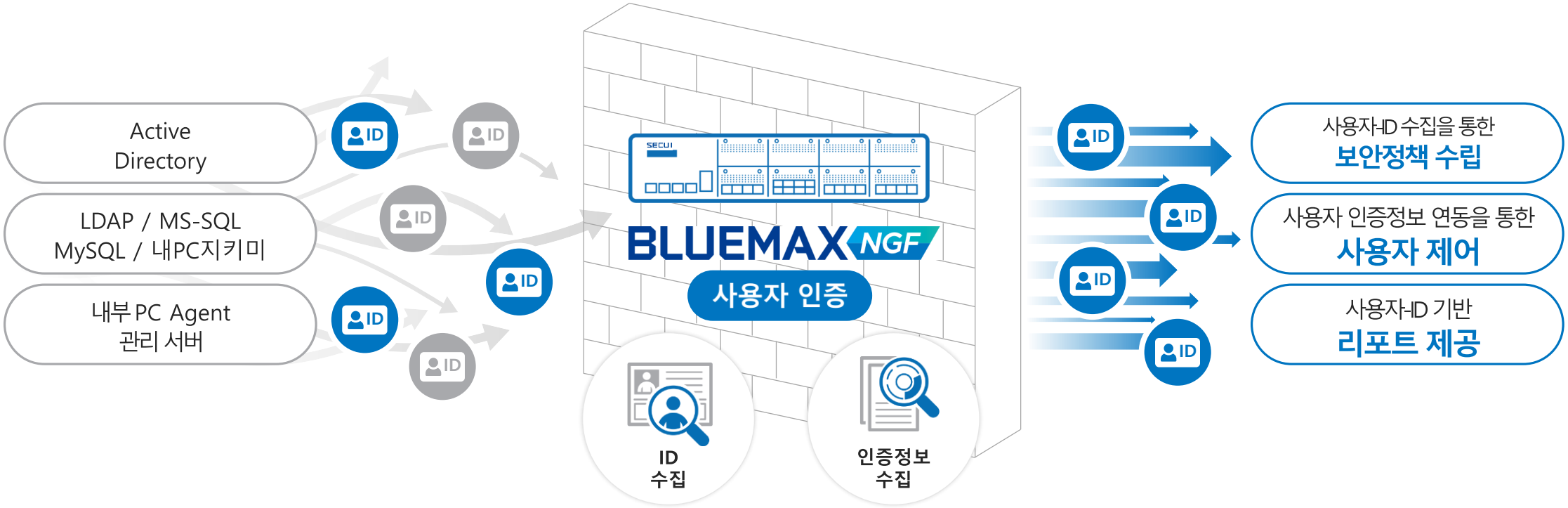
BLUEMAX NGF 도메인IP 수집 방식



사용자 -ID 연동

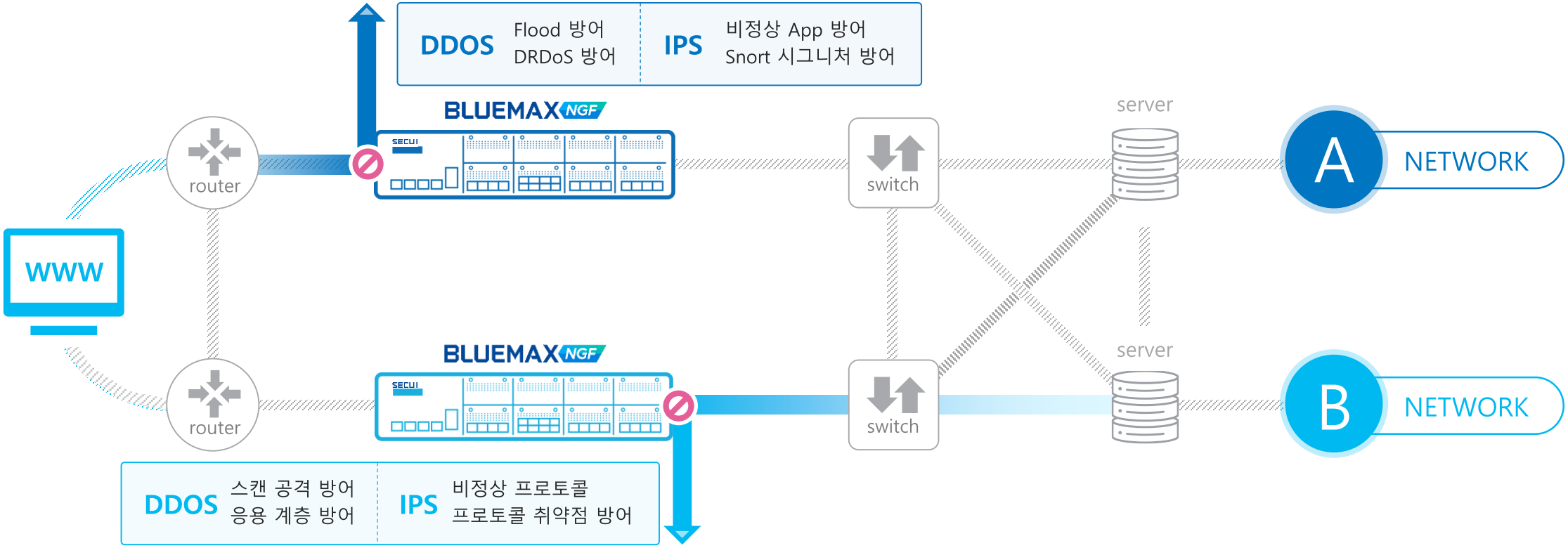
정보를 관리하는 인증서버와 연동하여 **방화벽 정책 적용**

- 사용자-ID 기반 정책 설정 제공
- DHCP 환경에서도 사용자-ID 권한별 정책 설정 적용
- 방화벽간 사용자 인증 정보 연동으로 정책 수정 없이 접속 가능



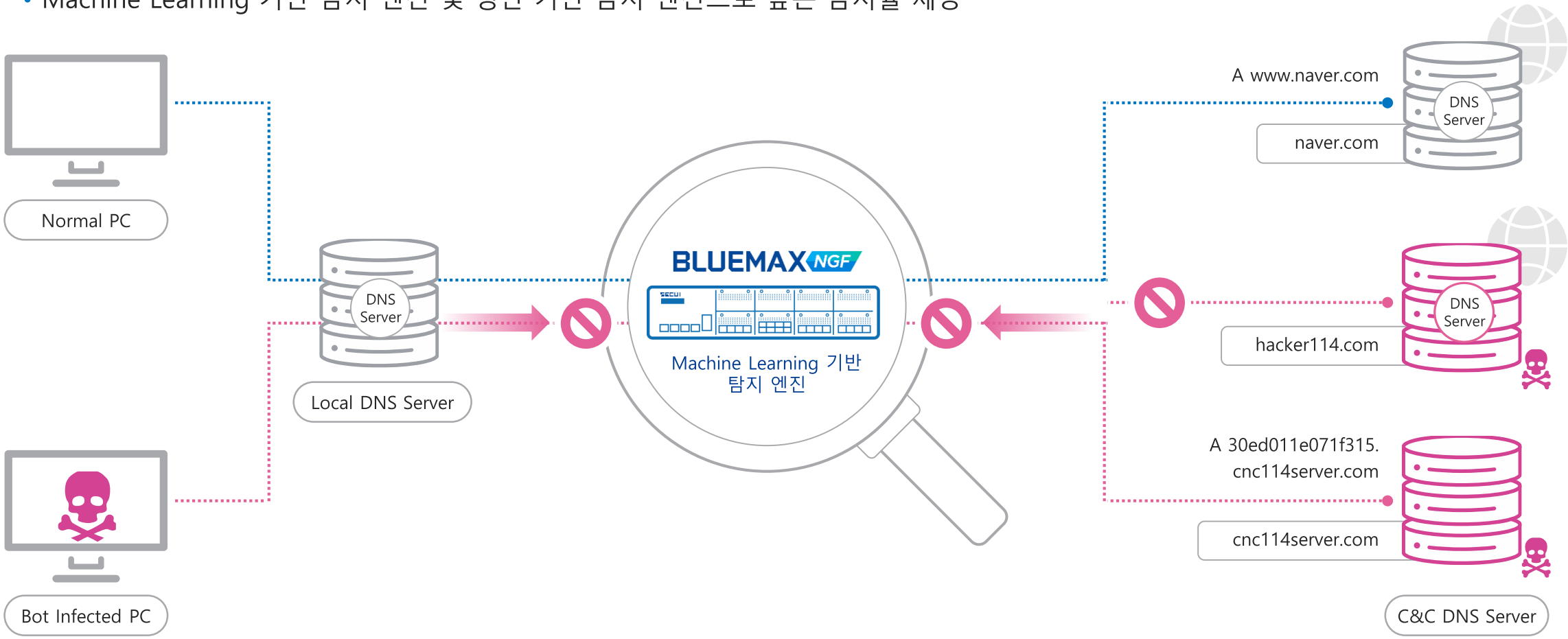
프로파일 기반 IPS, 보호 도메인 기반 DDoS로 강력한 계층적 방어

- 보호 대상의 성격과 보호 요구 수준에 따른 자동 프로파일 선택으로 관리 편의성 제공
- NCSC(국가정보원), PCRE(정규표현식) 시그니처 및 옵션 완벽 지원



DNS 도메인 필터링, 터널링 탐지를 통한 **DNS 기반의 위협 탐지 및 차단**

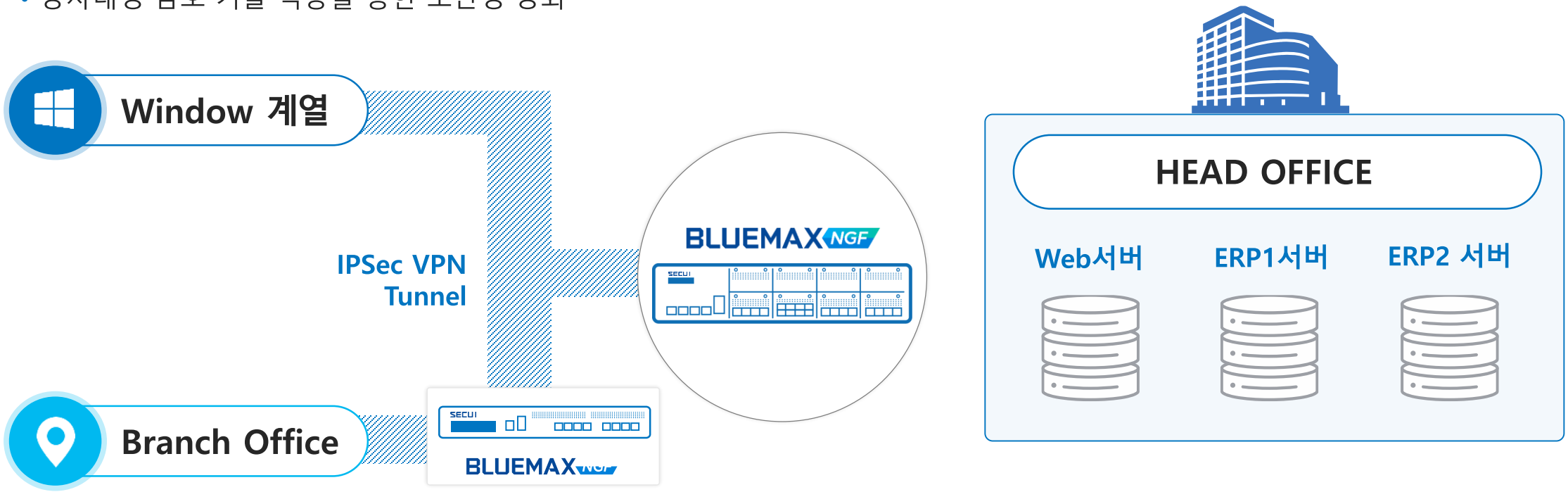
- DNS 프로토콜 데이터 유효성 검사 및 비정상적인 DNS 트래픽 검사
- Machine Learning 기반 탐지 엔진 및 평판 기반 탐지 엔진으로 높은 탐지율 제공



VPN(IPSec VPN)

국제 표준 인증 프로토콜과 **암호화 알고리즘 지원**

- 회선 상태 확인을 위한 DPD/DLD 기능 강화
- Group VPN 지원으로 관리 편의성 증대
- 양자내성 암호 기술 적용을 통한 보안성 강화

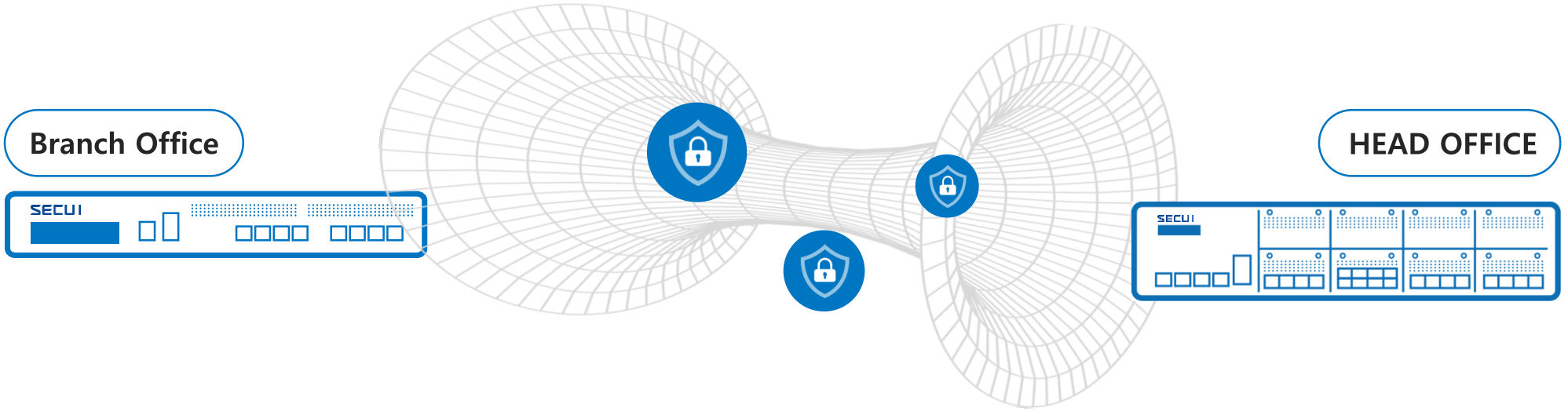


- DPD (Dead Peer Detection) VPN 장비/단말 상태 정보 확인
- DLD (Dead Link Detection) 시큐아이 자체 회선 장애 감지 기능

국제 공인 차세대 암호 기술 **양자 내성 암호화 PQC 알고리즘 탑재**

기존 방식	BLUEMAX NGF 방식
양자 컴퓨터 등장으로 기존 공개키 암호 방식으로는 해결 불가하며, 새로운 보안 문제 등장 ➡ 단순 암호/난수 복잡도로는 해결 불가	양자 컴퓨터를 활용한 공격에도 대응 가능한 새로운 양자 내성 암호화 알고리즘 지원 • 상용화 된 공개 암호 자체를 보호하는 양자 내성 알고리즘 적용

양자 내성 암호 알고리즘



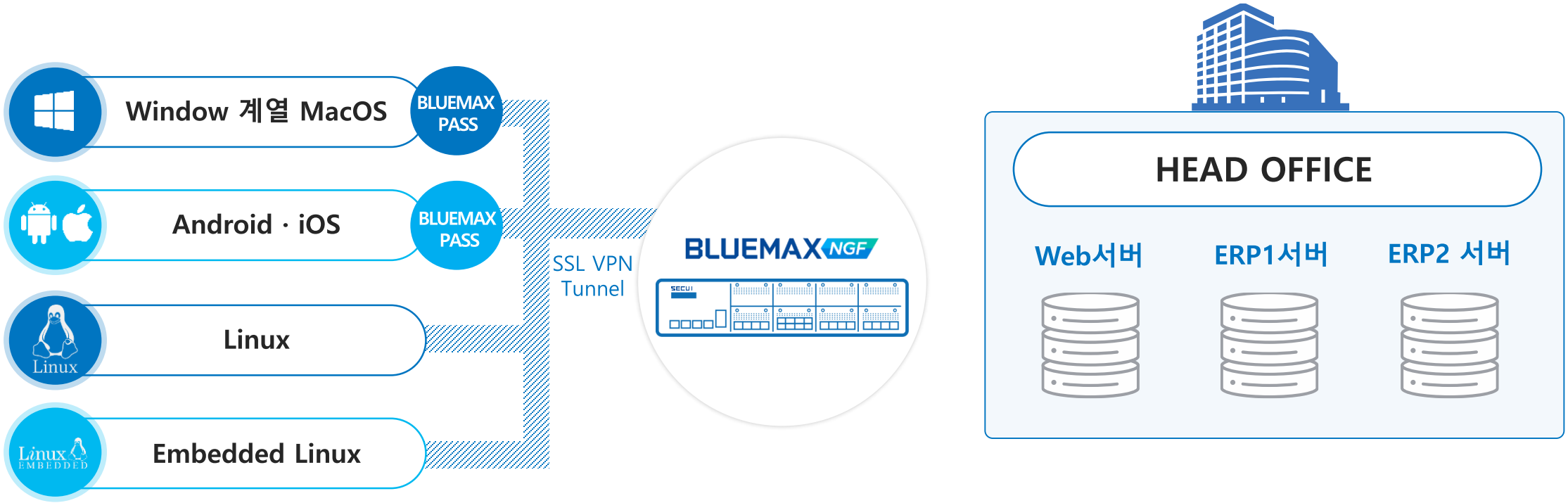
* PQC(Post Quantum Cryptography) : 양자컴퓨터의 모든 공격에 대한 안전한 내성이 있는 암호

VPN(SSL VPN)

웹 표준 암호화 기술 적용으로 네트워크 구조 변경 없이 암호화 통신 지원

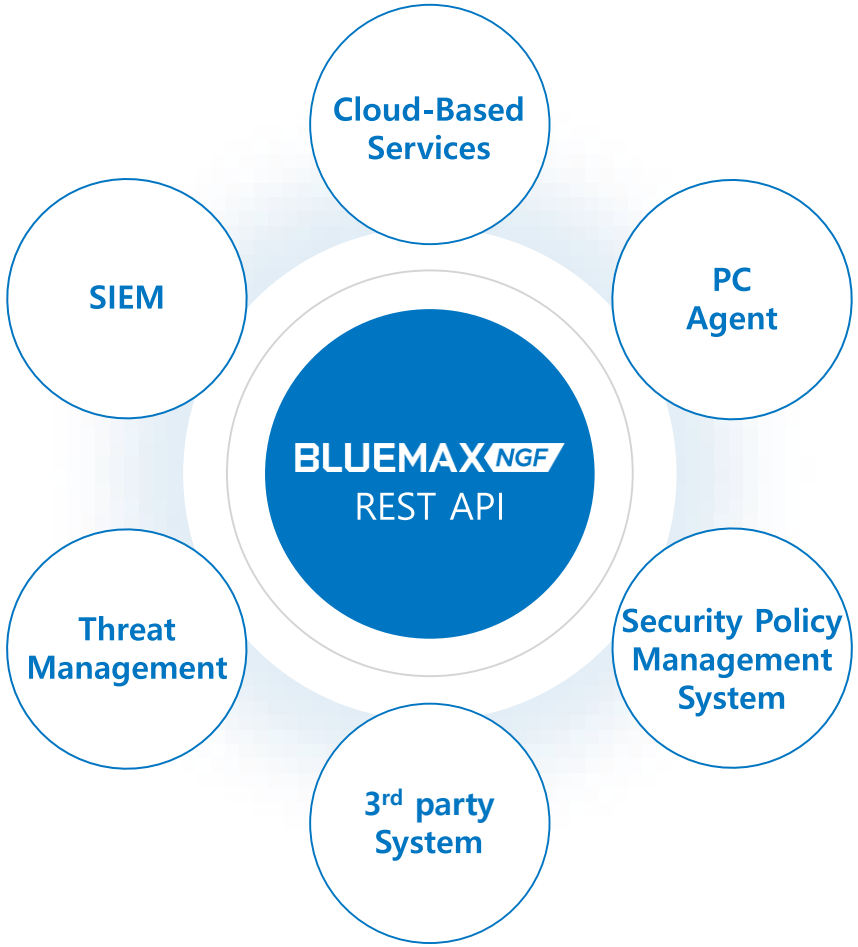
- 다양한 OS를 지원하는 CS방식의 SSL VPN Client
- 손쉽고 강력한 FIDO 생체인증을 포함한 BLUEMAX PASS 간편인증

* FIDO: Fast Identity Online



BLUEMAX NGF Open API

Open API를 제공하여 다양한 정책제어 및 로그 데이터연동 가능



Policy

- 방화벽 정책 통합관리
- 정책 컴플라이언스 준수 확인
- 정책 다운로드를 통한 이력관리

Log/Management

- 다양한 방식의 로그제공으로 시스템간 로그 통합 및 분석가능
- 컴플라이언스에 따른 보고서 편집

Profile/object

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

System Configuration

- 시스템 운영정보조회 및 SW패치
- 시스템 백업 및 복구 관리

04

- 라인업 (SMB, Mid-Biz)
- 라인업 (Enterprise Carrier)
- 인증

BLUEMAX NGF

라인업·인증

SMB, Mid-Biz

BLUEMAX		NGF 50	NGF 100	NGF 200	NGF 300	NGF 310	NGF 500	NGF 510	NGF 800ED	NGF 1000	NGF 1100
CPU		2 Core	2 Core	4 Core	4 Core	4 Core	8 Core	8 Core	8 Core	2 Core	4 Core
Memory		4GB	4GB	4GB	8GB	8GB	8GB	8GB	8GB	8GB	8GB
Storage	System	16GB	16GB	32GB	64GB	64GB	128GB	128GB	128GB	128GB	128GB
	Log	-	-	-	1TB	1TB	1TB	1TB	1TB	1TB	1TB
Interface	1GF	-	-	-	-	-	4	4	4	4	4(max8)
	1GC	4	4+4	4+8	8	8	8	8	8	8	8
Power Supply		Adapter	Adapter	Adapter	Single	Single	Single	Single	Single	Single	Single
Throughput		1 Gbps	2Gbps	4Gbps	6Gbps	8Gbps	8Gbps	12Gbps	12 Gbps	12Gbps	16Gbps

Enterprise / Carrier

BLUEMAX		NGF 1500	NGF 1510	NGF 2000	NGF 2100	NGF 5000	NGF 5100	NGF 20000
CPU		4 Core	10 Core	16 Core	20 Core	24 Core	32 Core	48 Core
Memory		16GB	16GB	32/64GB	32/64GB	64/128GB	64/128GB	96/288GB
Storage	System	256GB	256GB	128/256GB	128/256GB	128/512GB	128/512GB	128/512GB
	Log	1TB	1TB	1.92TB/RAID	1.92TB/RAID	1.92TB/RAID	1.92TB/RAID	1.92TB/RAID
Interface	100GF	-	-	-	-	-(max2)	-(max2)	-(max4)
	40GF	-	-	-(max4)	-(max4)	-(max8)	-(max8)	-(max8)
	10GF	-(max4)	-(max4)	2(max10)	2(max10)	10(max26)	10(max26)	10(max26)
	1GF	4(max8)	4(max8)	8(max40)	8(max40)	8(max40)	8(max40)	8(max40)
	1GC	8	8	8(max40)	8(max40)	8(max40)	8(max40)	8(max40)
Power Supply		Redundant	Redundant	Redundant	Redundant	Redundant	Redundant	Redundant
Throughput		30Gbps	40Gbps	60Gbps	80Gbps	120Gbps	160Gbps	320Gbps

국내외 다양한 인증 기관의 보안성, 기능, 성능 검증 테스트 완료

CC인증	GS인증	IPv6 Ready	IPv6 TTA
인증 번호 NISS-1275-2023	인증 번호 21-0075	Logo ID 02-C-001857	모델명 BLUEMAX NGF 전 모델
모델명 BLUEMAX NGF V3.0	모델명 BLUEMAX NGF V3.0	Version SecuiOS V4.0(64bit)	인증 범위 IPv6 Router Core 적합성 및 상호운용성
인증 범위 FW+VPN(EAL4)	인증 범위 1등급	인증 범위 IPv6 Router	

BLUEMAX NGF

Copyright © 2024 SECUI Co., Ltd. All rights reserved

sales.secui@secui.com