클라우드 환경 지원을 위한

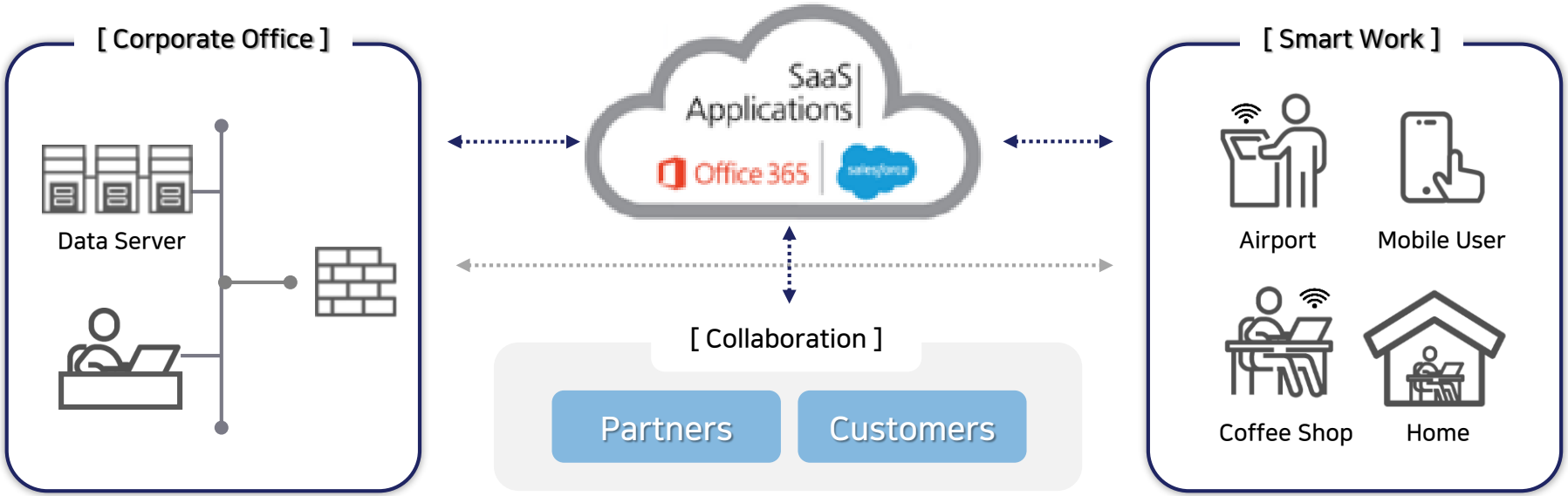
차세대 방화벽 (BLUEMAX NGF)

조원용 팀장

클라우드 확산에 따른 보안의 경계 확대

장소와 환경에 제약 없이 업무 연속성을 보장하는 사용자 중심의 개방형 업무 환경 증가

Anytime, Anywhere, Any device and Collaboration

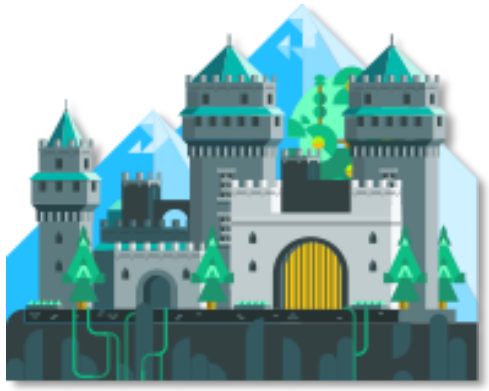


Cloud 기반 협업 어플리케이션 사용 증가, 다양한 단말을 이용한 업무 환경 (Mobile Worker)

새로운 보안 접근 필요

경계선 기반 방어 중심의 **기존 보안 체계 한계점**

기존 보안 체계 (경계선 기반 방어)



신뢰 기반의 네트워크 경계 중심 방어 체계

- 외부에서 유입되는 위협 방어 중심

계층별 방어 체계 (개별 방어 체계)

- Best Effort Security (네트워크/단말 개별 동작)

한계 및 문제점

내부 위협에 대한 대응 부족

- APT 공격을 통한 내부 위협 확산
- 내부자에 의한 보안 사고 증가

업무 이동성, 협업 환경에 대한 지원 부족

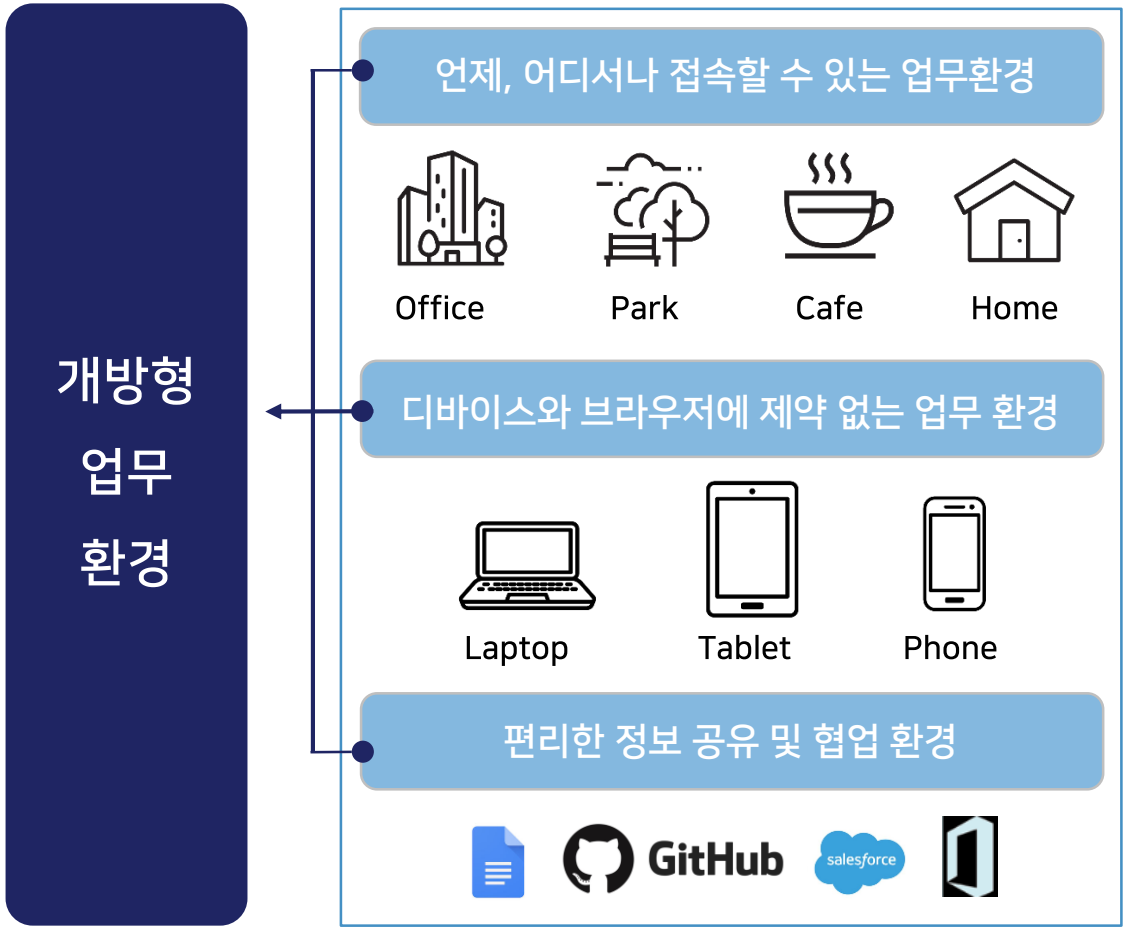
- 클라우드 환경 대한 보안 Risk 존재
- 이동에 따른 정책 신청/적용 시간 소요

신규 위협에 대한 대응 지연

- 알려진 공격 방어 위주 (선제적 대응 어려움)

새로운 보안 접근 필요

클라우드 환경을 고려한 새로운 보안 체계 필요



- 업무 효율 향상을 위한 개방형 네트워크 전환
  - ▸▸ 언제/어디서나 접속 가능한 업무 시스템
- 개방형 네트워크 전환을 위한 보안체계 개선
  - ▸▸ 사용자/애플리케이션/디바이스 중심 보안 정책
- 데이터 중심의 선제적 방어 체계
  - ▸▸ 자산별 보안 정책 관리(Micro-Segmentation)
- On-Premise/Cloud 환경의 일원화된 보안 관리
  - ▸▸ 통합 보안 정책 관리, 자동화 체계 구축

클라우드 환경을 지원하는 보안 체계 구축

On-Premise/Cloud 환경을 모두 지원하기 위한 차세대 방화벽 필요 요소

1. On-Premise/Cloud 환경 지원

- 다양한 환경 지원 ▸ 전용 Appliance 및 클라우드/가상화 지원
- 주요 데이터에 대한 Micro-Segmentation 지원 ▸ Virtual System 지원

2. 위협 대응 플랫폼

- 빠른 위협 대응 ▸ 위협 정보 기반 네트워크/단말/3rd Party 연계 방어
- 위협 인지를 통한 대응 ▸ 이상 상황 인지 > 상세 분석 > 대응

3. 인지 정보 기반 접근 제어

4. 통합 관리/정책 자동화

- On-Premise & Cloud 환경에 대한 일원화된 통합 보안 관리 체계
- 수집된 위협 정보, 보안 로그 등을 종합 분석을 통한 보안 정책 설정 자동화

On-Premise/Cloud 환경 지원

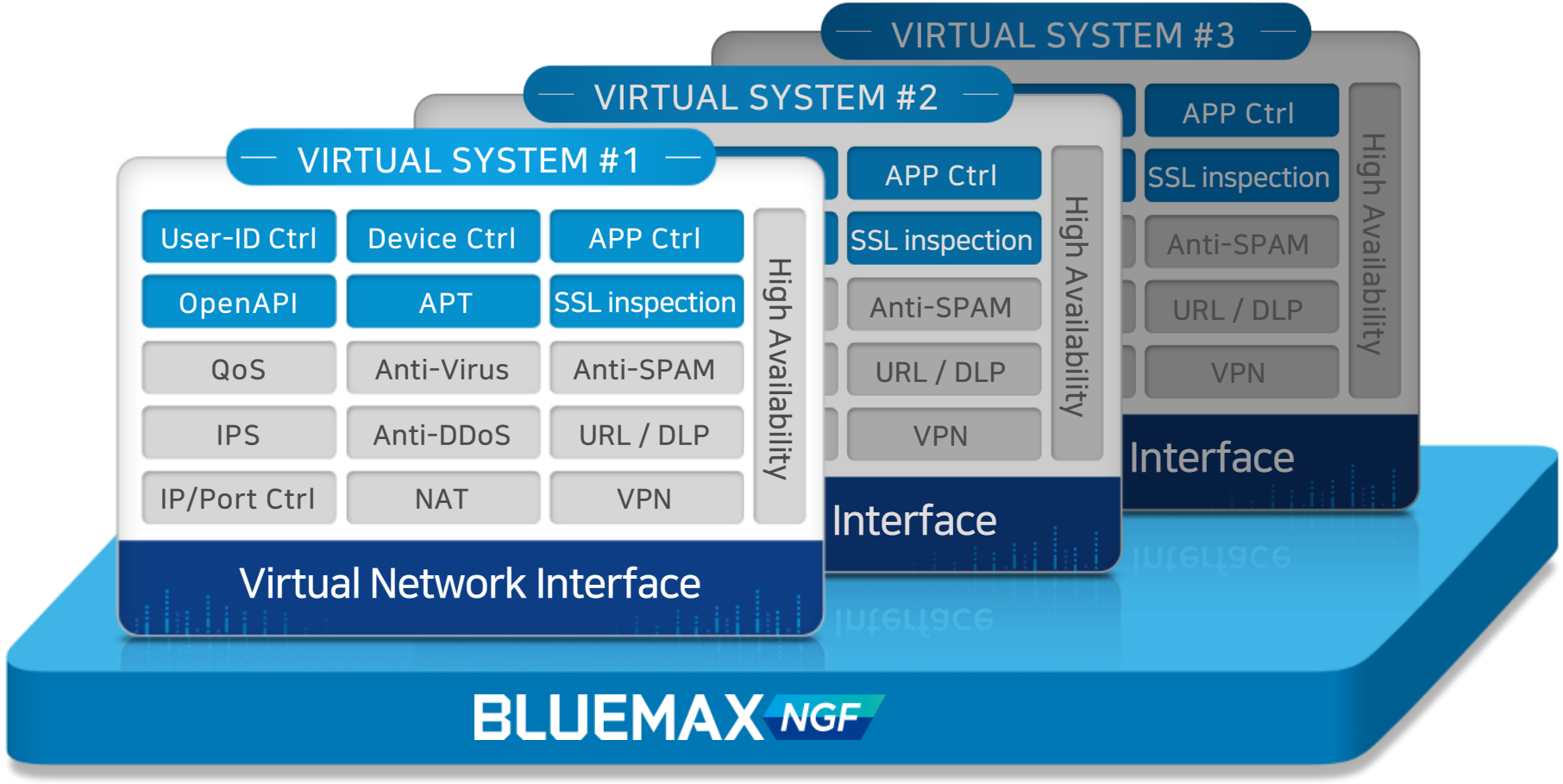
다양한 가상화 플랫폼, 클라우드 환경에 최적화된 BLUEMAX NGF Virtual Edition

BLUEMAX NGF VE

Cloud Auto Scaling / High Availability / Security Policy Backup

On-Premise/Cloud 환경 지원

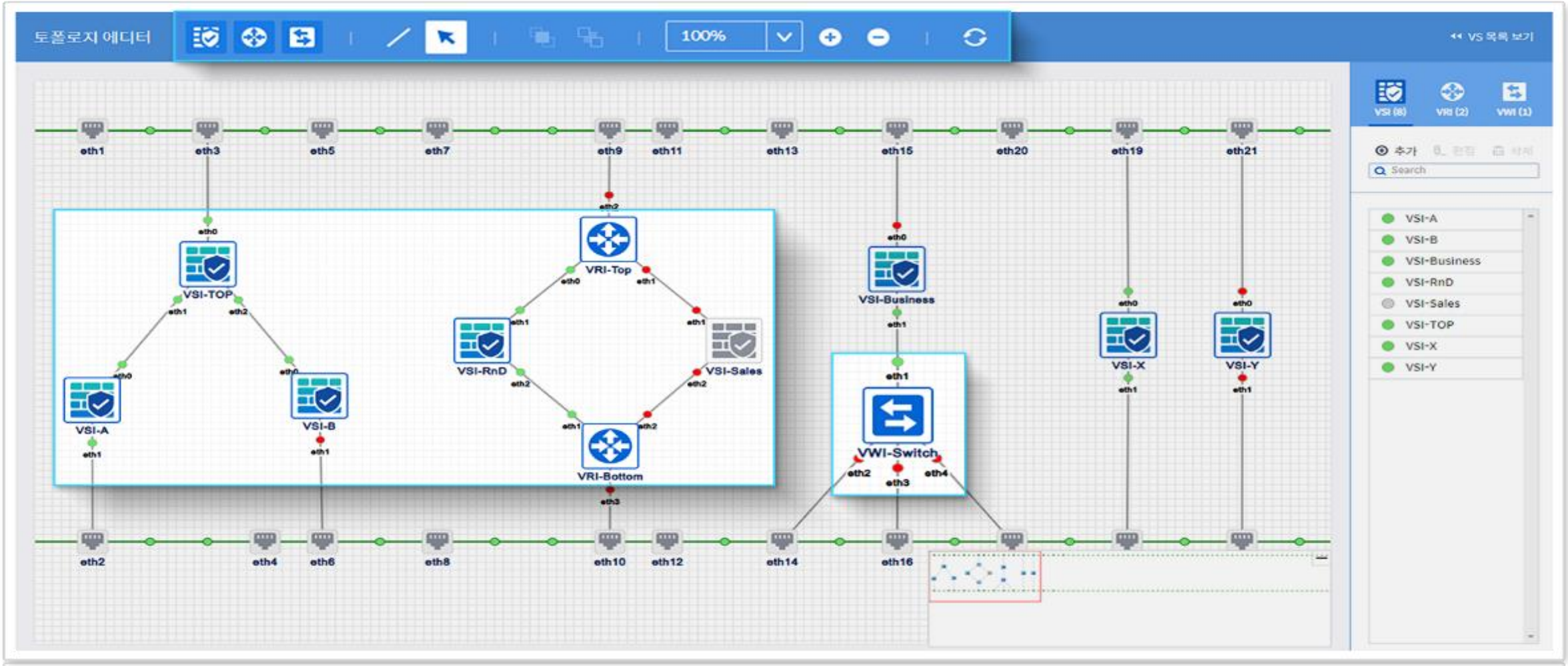
컨테이너 기반 Virtual System 지원으로 완벽하게 독립된 가상 네트워크 보안



* 주요 보호 자원의 Micro-Segmentation 지원

On-Premise/Cloud 환경 지원

Virtual System 토폴로지 에디터로 가상 방화벽의 직관적이고 편리한 구성 관리

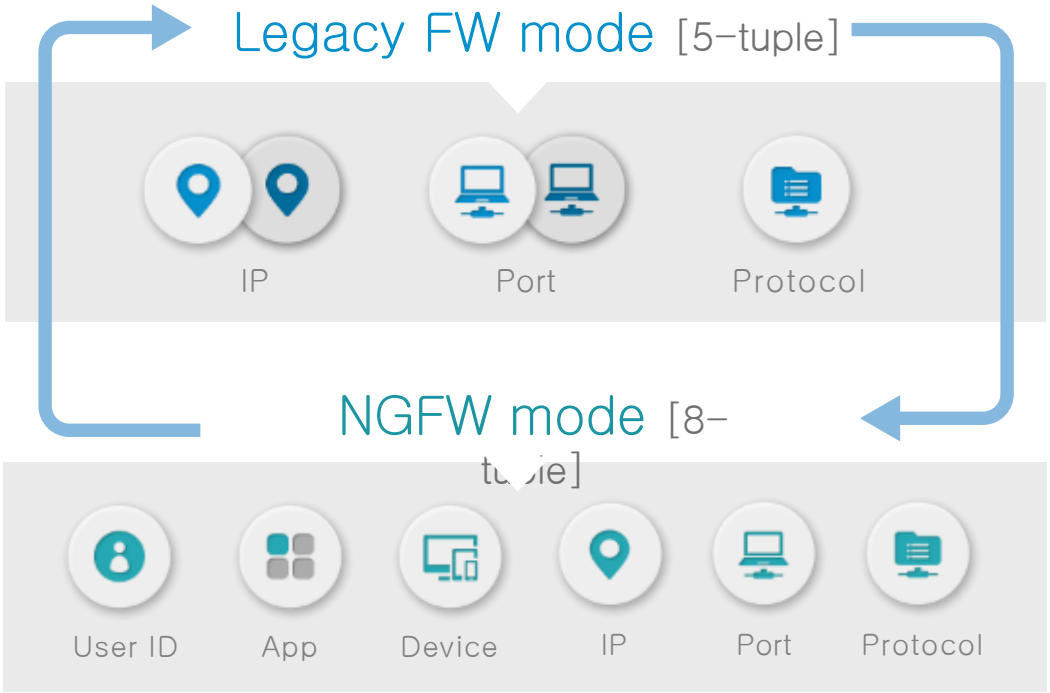


On-Premise/Cloud 환경 지원

고성능 고품질 무중단 서비스, 유연한 방화벽 Mode 전환 제공

고가용성 HW 아키텍처로 무중단 서비스 제공

장비 교체 없이 Legacy FW과 NGFW 지원



위협 대응 플랫폼

ALL MY THREAT MANAGEMENT BLUEMAX NGF

Security Intelligence Platform for All My Threat Management

Virtual Cloud Security

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

BLUEMAX NGF VE

Threat Intelligence

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

STIC CSOC

Malware Protection

· Device의 Compliance 점검, 이상행위, 감염 여부를 실시간 탐지하여 선제적 위협탐지 차단

BLUEMAX CLIENT

Security Automation

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

BLUEMAX TAMS SECUI SCAN

위협 대응 플랫폼

ALL MY THREAT MANAGEMENT BLUEMAX NGF

Open API를 제공하여 다양한 정책제어 및 로그 데이터 연동 가능

위협 대응 플랫폼

ALL MY THREAT MANAGEMENT
BLUEMAX NGF

단말의 모든 이상행위와 감염여부를 실시간 탐지하여 선제적 위협 탐지 차단

알려지지 않은 위협은 이상행위 탐지하며
해당 내용을 멀웨어 탐지(보안 컨텐츠)로 실시간 전환

사전예방

Compliance 점검

취약점 점검

악성멀웨어 탐지

사후처리

이상행위 탐지

랜섬웨어 대응

위협 대응 플랫폼

ALL MY THREAT MANAGEMENT BLUEMAX NGF

단말의 보안 상태에 따른 접근 제어로 내부 위협 확산 차단

Device 환경, 트래픽 정보 분석

BLUEMAX CLIENT

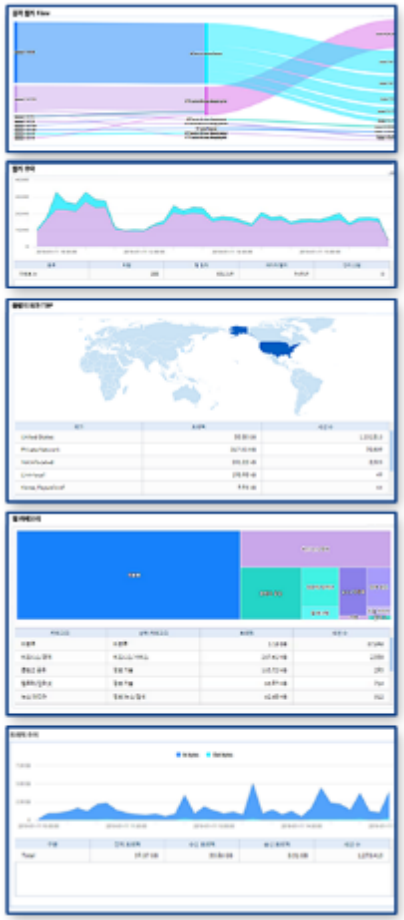
사용자ID, Device, App 제어

BLUEMAX NGF

위협 대응 플랫폼

ALL MY THREAT MANAGEMENT
BLUEMAX NGF

트래픽/위협 현황에 대한 다차원 분석 View 제공



인지 정보 기반 접근 제어

다양한 인지 정보 기반 정책 제어로 관리 편의성 및 접근제어의 정확성 극대화

애플리케이션

사용자

- ACTIVE DIRECTORY
- RADIUS/LDAP/WEB
- 내부 PC AGENT 관리서버

디바이스

보안 설정	업데이트	필수 S/W
정보	정보	설치

도메인

도메인당 IP할당 1,000개 이상

통합관리 / 정책 자동화

위협정보, 로그 분석으로 보안정책 분석 및 자동화

위협 관리

Threat Management

중앙시스템 관리

Centralized Management

보안 로그 분석

Security Log Analysis

보안 정책 분석

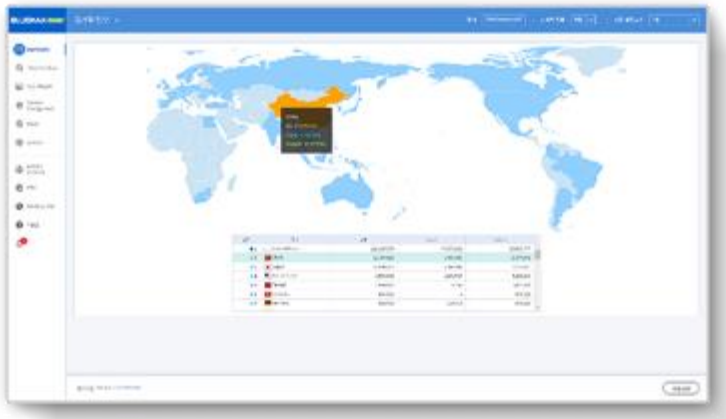
Security Policy Analysis

통합관리 / 정책 자동화

통합 위협 분석, 통합 설정관리

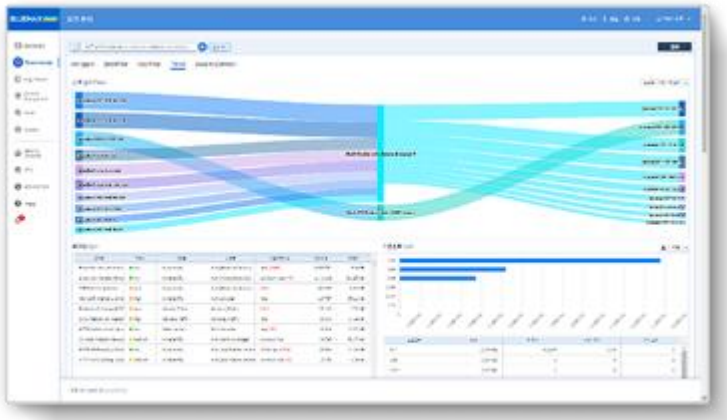
통합관리 / 정책 자동화

실시간 위협 분석, 대응 정책 분석



실시간
모니터링

Real-time
Monitoring

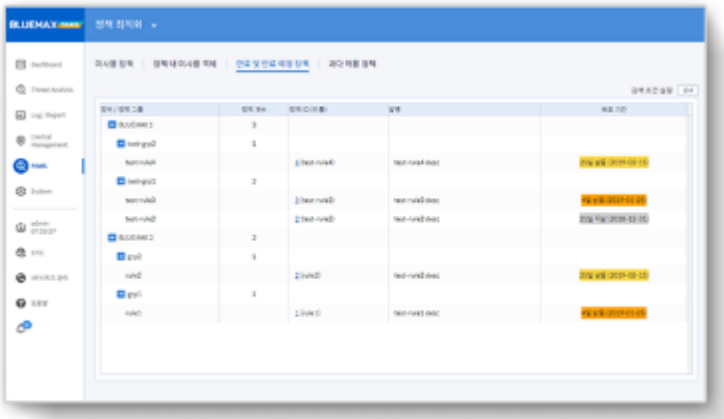


다차원
위협 분석

Multi-Threat
Analysis

보안
정책 분석

Security Policy
Analysis

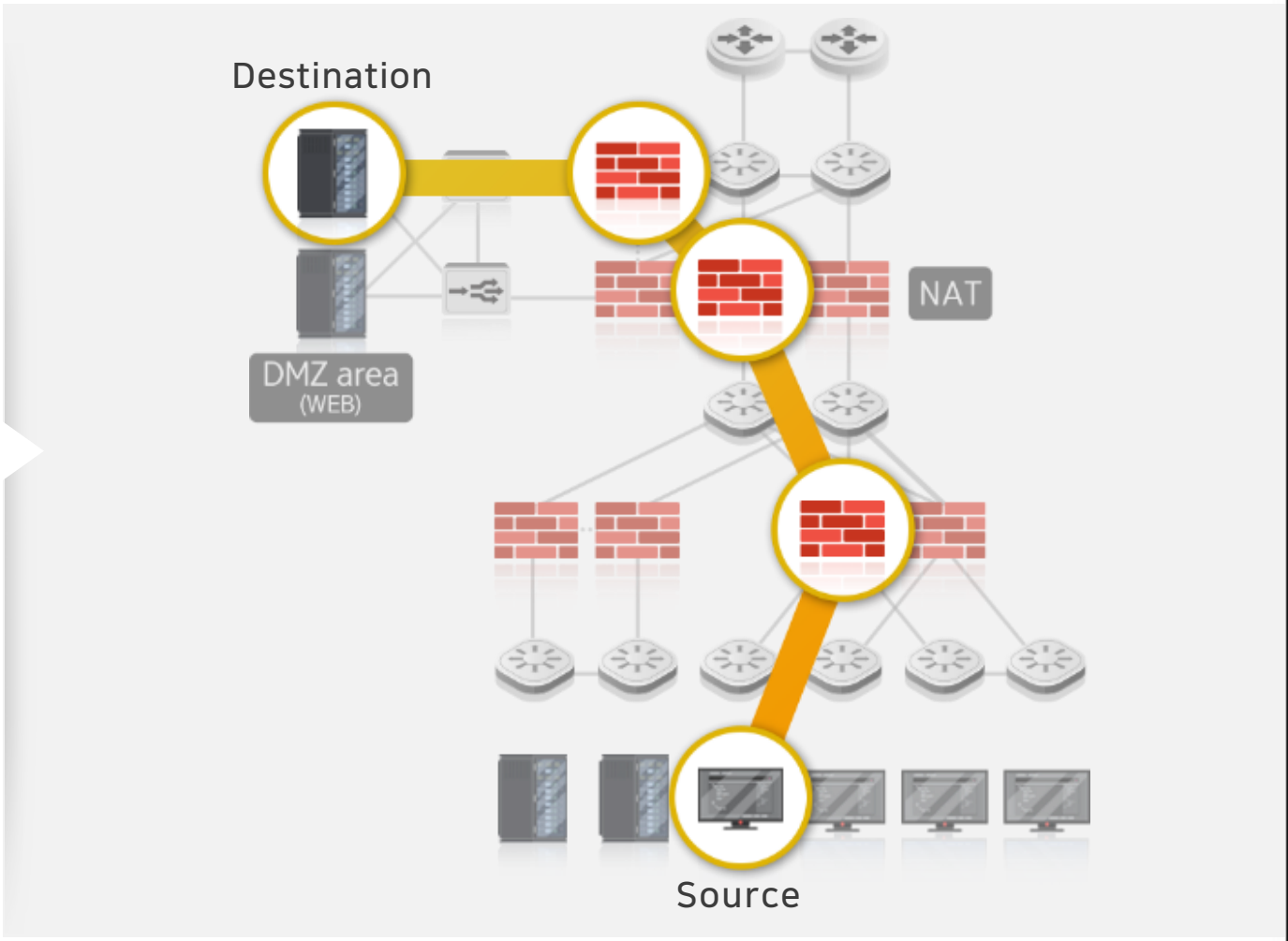


통합관리 / 정책 자동화

보안 정책 자동 신청, 컴플라이언스, 휴먼에러 방지

통합관리 / 정책 자동화

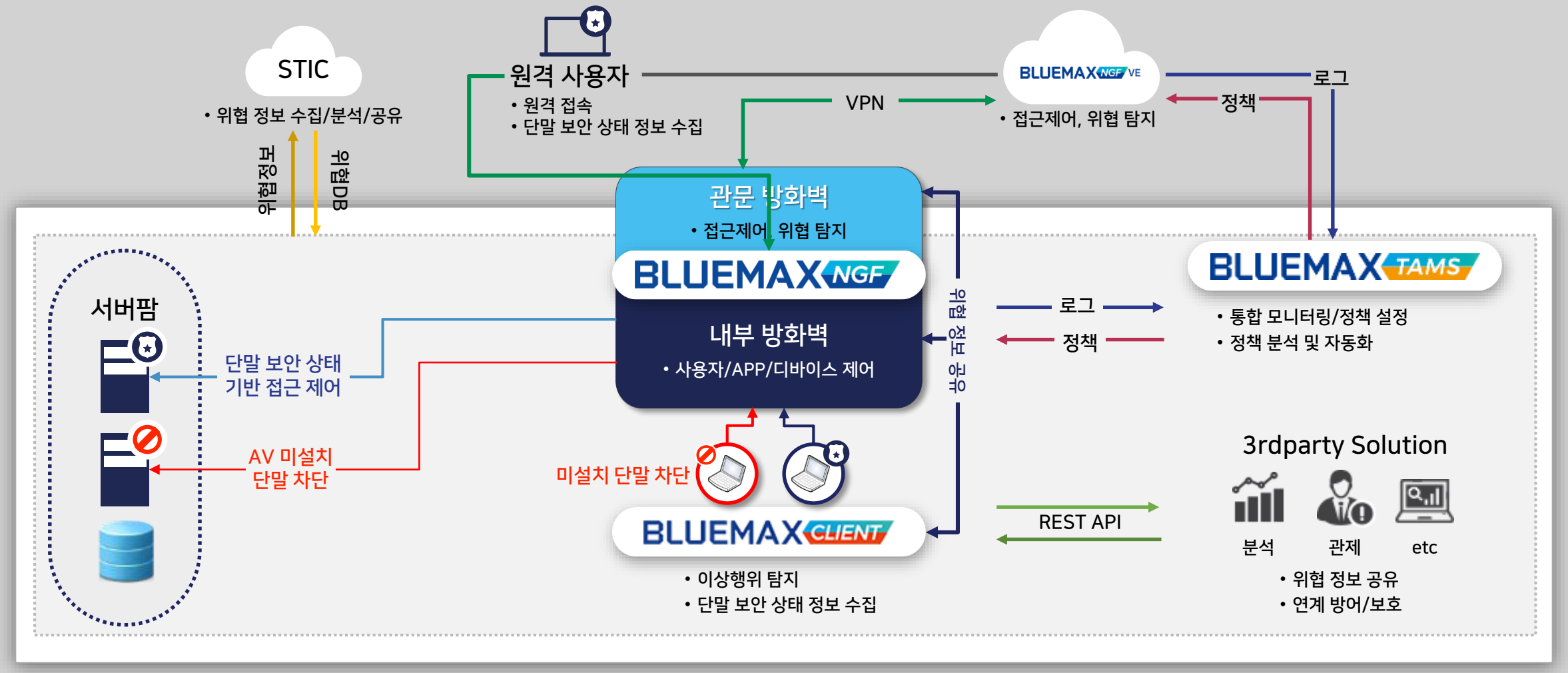
보안 정책 분석, 최적화, 위반 탐지



클라우드 사용 확대에 따른 보안 체계 구축 방안

ALL MY THREAT MANAGEMENT BLUEMAX NGF

Security Intelligence Platform (위협 대응, 개방형/클라우드, 통합 보안)



Thank you

Q&A

SAMSUNG SDS

Realize your vision