
CLOUD
INFINITY
CONFERENCE

AI in the Cloud Summit : AI, Cloud, Virtualization, and Server Synergy

# 클라우드 환경에서의 물리 네트워크 보안

한드림넷 진한상 이사

# 클라우드 환경으로의 IT 변화

- 디지털 트랜스포메이션
- IT자산의 효율적 운용
- 클라우드 전환
- 공간과 비용

# 클라우드 전환, 어떻게 준비할 것인가?

가상화 및 소프트웨어 정의 기술을 이용한 클라우드 인프라로의 전환

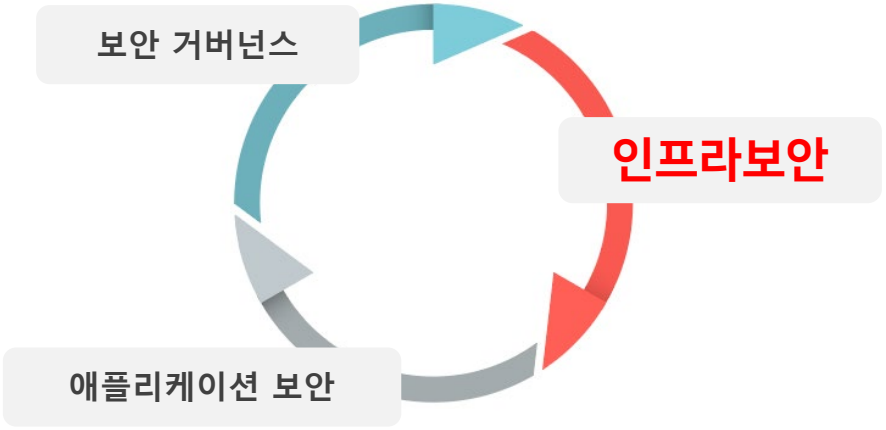
ABLESTACK

ABLESTACK Cloud Platform

- 내장 디스크 기반 스토리지/외장 스토리지
- 자동화된 데이터베이스
- 가상 데스크톱
- 가상 네트워크 서비스
- 클라우드 관리

- 프라이빗 클라우드
- 자동화된 멀티 클라우드 배포
- 멀티 하이퍼바이저

## 클라우드 전환, 보안문제는?

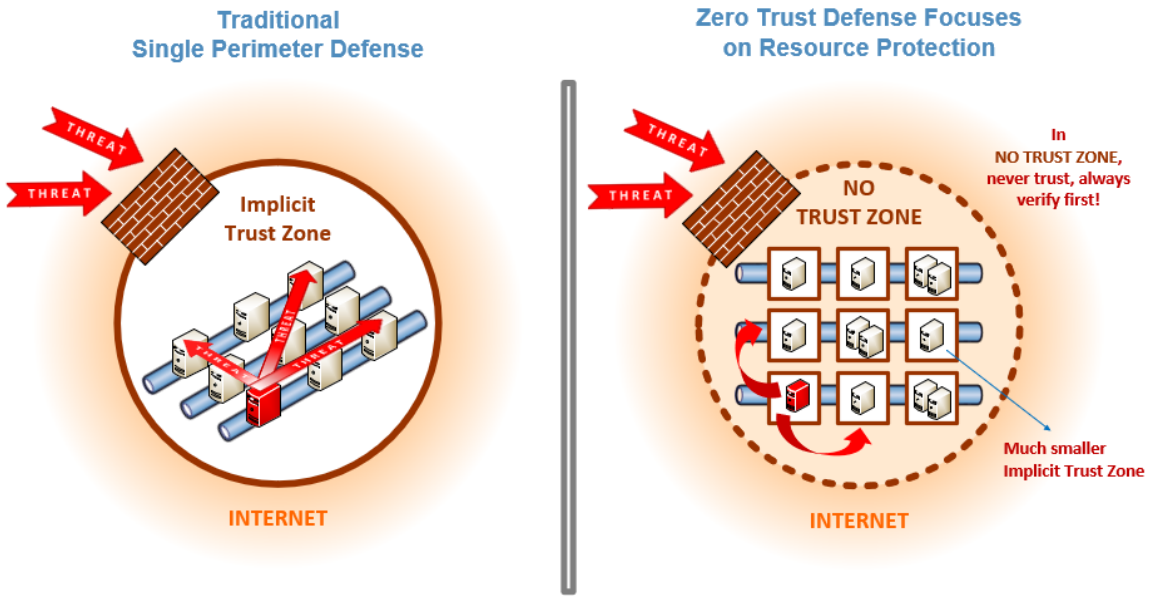



- 보안거버넌스 : 정책적인 부분에 대한 관리 (물리보안, 규정, 기준, 승인절차 등)
- 애플리케이션보안 : 불특정 다수가 이용하는 웹서비스 등 애플리케이션 취약점 이용한 공격
- **인프라보안** : 클라우드 환경에서 네트워크 경계 관점의 전통적인 보안으로는 충분하지 않음

# 클라우드 전환, 보안문제는?


- 보안거버넌스 : 정책적인 부분에 대한 관리 (물리보안, 규정, 기준, 승인절차 등)
- 애플리케이션보안 : 불특정 다수가 이용하는 웹서비스 등 애플리케이션 취약점 이용한 공격
- 인프라보안 : 클라우드 환경에서 네트워크 경계 관점의 전통적인 보안으로는 충분하지 않음
- **선제방어, 위협 탐지와 대응 전략을 "제로 트러스트" 관점의 보안 프로세스에 통합**

# 클라우드 인프라에서의 네트워크 보안 전략

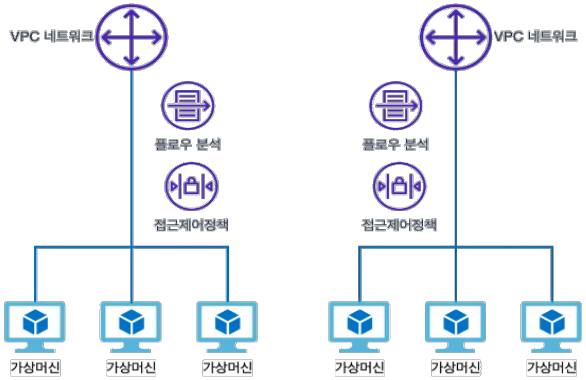



( 출처: 미국표준기술연구소(NIST), Zero Trust Cybersecurity: 'Never Trust, Always Verify' ]

- **"Never Trust, Always Verify"** : 절대 신뢰하지 말고, 늘 검증하라.
- 방화벽, IPS 등 전통적인 경계보안 시스템만으로는 데이터센터 보안위협 방어 한계
- 제로트러스트는 보안 전반에 걸친 광범위한 개념으로 단계적 구현 계획 필요
  (사용자, 기기, 네트워크, 인프라, 애플리케이션, 데이터. 워크로드 등)
- "접근" 관점에서의 **"제로트러스트 네트워크 액세스(ZTNA)"** 모델 우선 고려

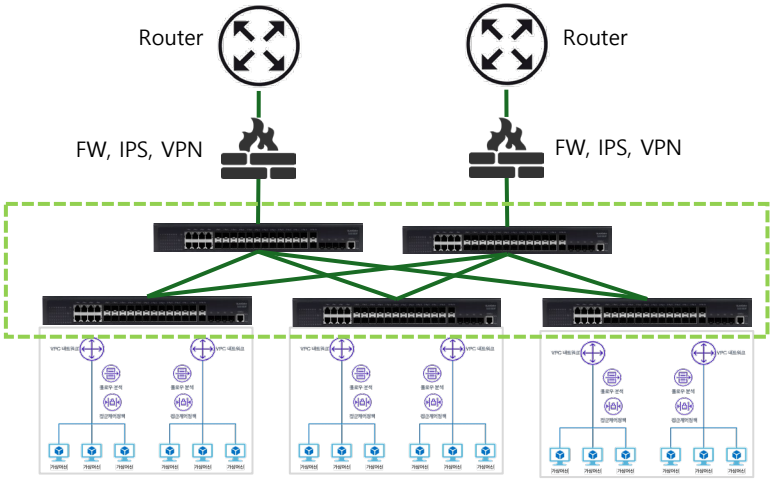
# 제로트러스트 네트워크 보안모델

## 가상화 영역




- 외부->가상머신 접근에 대한 Gateway Keeping
- 가상머신 ->외부 접근에 대한 허용정책 제공
- 가상머신간의 통신에 대한 명시적 정책 설정
- 가상화 구간에 대한 보안정책 적용
- 관리툴 제공을 통한 가시성, 운용편의성 확보

## 물리적 영역




- 물리영역 경계보안시스템 : FW, IPS, VPN 등
- 물리네트워크 화이트리스트 정책 적용
- 물리네트워크 구간 암호화
- 로그, 트래픽 데이터 등 네트워크 관련정보 수집
- AI기반 보안분석을 통한 네트워크 위협대응

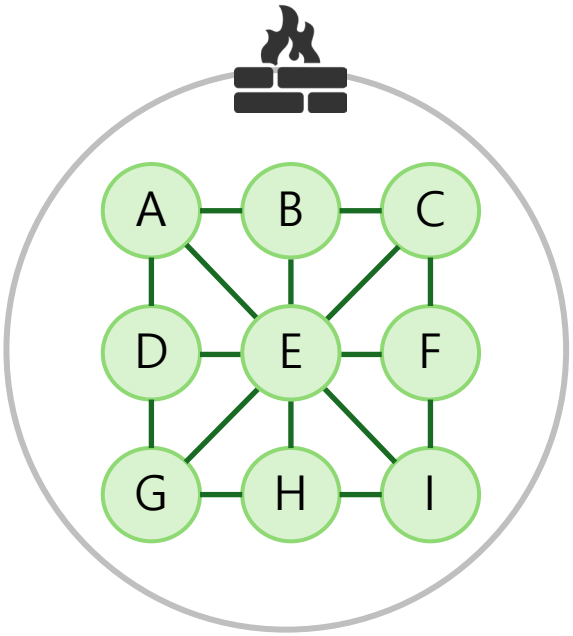
# 단계별 제로트러스트 네트워크 전략

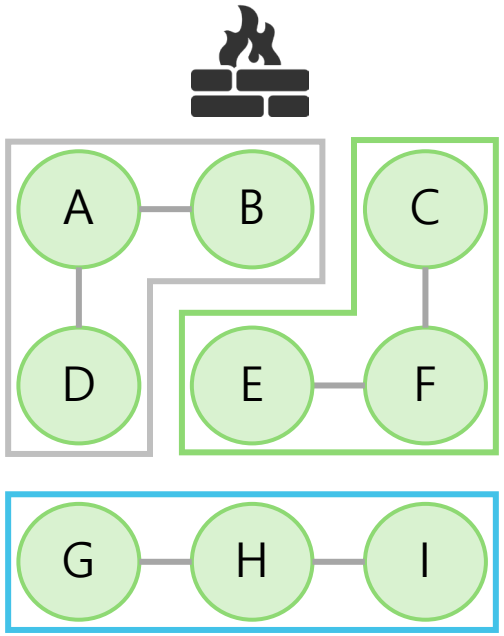
| 기능 | 기존 수준 | 향상 수준 | 최적화 수준 |
|---|---|---|---|
| **네트워크 세분화** | 대규모 경계·분리를 사용하는 네트워크 구조 정의 | 일부 내부적인 세분화를 갖는 송수신 소규모 경계를 통해 더 많은 네트워크 구조 정의 | 네트워크 구조는 주변 응용 워크플로우를 기반으로 완벽히 분산된 송수신 세부 경계 및 더욱 깊은 내부 세분화로 구성 |
| 암호화 | 최소한의 내외부 트래픽에 대한 명시적 암호화 | 내부 응용에 대한 모든 트래픽 및 일부 외부 트래픽 암호화 | 가능한 경우, 내외부로 전달되는 모든 트래픽 암호화 |
| 위협대응 | 알려진 위협 및 정적 트래픽 필터링을 핵심 기반으로 위협 보호 수행 | 위협을 사전에 발견하기 위한 기본 분석 포함 | 컨텍스트 기반 신호와 기계학습 기반 위협 보호 및 필터링 통합 |
| 가시성 및 분석 | 중앙 집중식 수집 및 분석을 통하여 경계에서 가시성 제공 | 수동 정책기반 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 | 자동화된 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 |
| 자동화 및 통합 | 변경 관리 워크플로우에 따라 네트워크 및 환경 변경을 수동으로 초기화 및 실행 | 수동으로 네트워크 및 환경 변화를 시작하기 위한 자동화된 워크플로우 사용 | 네트워크 및 환경 설정을 위해 지속적 통합·지속적 배포(CI/CD) 배포 모델에 따라, 자동화와 함께 코드로서의 인프라를 사용 |

# 제로트러스트 네트워크 핵심요소 - #1.네트워크 세분화

**마이크로 세그멘테이션 (Micro Segmentation)**

- 데이터센터를 개별 워크로드 수준까지 서로 다른 보안 세그먼트로 논리적 분리
- 세그먼트 별로 보안 제어를 정의하고 서비스를 제공하는 네트워크 보안 기술
- 암묵적 신뢰 구간에서의 보안위협 발생시 전체 네트워크로 확산 방지
- 네트워크 세분화로 구성된 신뢰구간의 피해 범위는 세분화된 단위 내로 축소

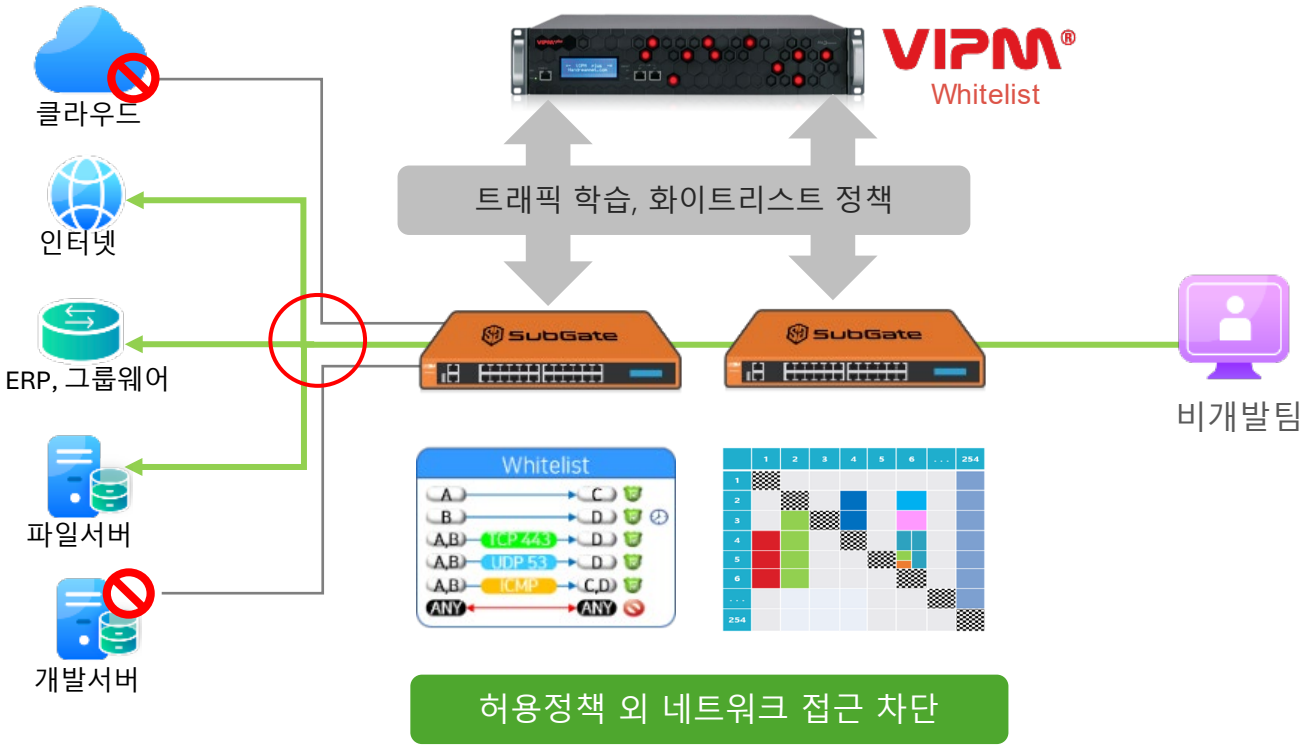


# #1.네트워크 세분화 : HDN - 화이트리스트 기술

**차세대 보안스위치 + VIPM WL**

- 네트워크 기반의 화이트리스트 보안
- 인증된 단말이라 할지라도 권한에 따라 접근 가능한 서비스는 달라야 함
- 허용된 보안정책 외의 서비스, 시스템 접근 원천 차단



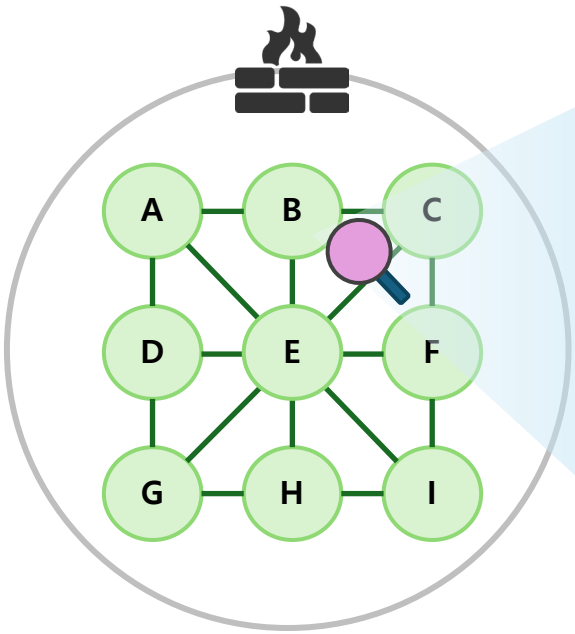
# 단계별 제로트러스트 네트워크 전략

| 기능 | 기존 수준 | 향상 수준 | 최적화 수준 |
|---|---|---|---|
| 네트워크 세분화 | 대규모 경계·분리를 사용하는 네트워크 구조 정의 | 일부 내부적인 세분화를 갖는 송수신 소규모 경계를 통해 더 많은 네트워크 구조 정의 | 네트워크 구조는 주변 응용 워크플로우를 기반으로 완벽히 분산된 송수신 세부 경계 및 더욱 깊은 내부 세분화로 구성 |
| **암호화** | 최소한의 내외부 트래픽에 대한 명시적 암호화 | 내부 응용에 대한 모든 트래픽 및 일부 외부 트래픽 암호화 | 가능한 경우, 내외부로 전달되는 모든 트래픽 암호화 |
| 위협대응 | 알려진 위협 및 정적 트래픽 필터링을 핵심 기반으로 위협 보호 수행 | 위협을 사전에 발견하기 위한 기본 분석 포함 | 컨텍스트 기반 신호와 기계학습 기반 위협 보호 및 필터링 통합 |
| 가시성 및 분석 | 중앙 집중식 수집 및 분석을 통하여 경계에서 가시성 제공 | 수동 정책기반 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 | 자동화된 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 |
| 자동화 및 통합 | 변경 관리 워크플로우에 따라 네트워크 및 환경 변경을 수동으로 초기화 및 실행 | 수동으로 네트워크 및 환경 변화를 시작하기 위한 자동화된 워크플로우 사용 | 네트워크 및 환경 설정을 위해 지속적 통합·지속적 배포(CI/CD) 배포 모델에 따라, 자동화와 함께 코드로서의 인프라를 사용 |

# 제로트러스트 네트워크 핵심요소 - #2. 네트워크 트래픽 암호화

## 데이터 암호화 (Data Encapsulation)

- 신뢰구간 내의 데이터 송수신은 암호화 되지 않은 평문형태의 전송이 일반적
- 전송데이터의 암호화 필수여부 미비, 비용 이슈 등으로 인한 데이터 비암호화
- 평문데이터의 악의적 탈취 시 다양한 보안위협 우려




**http**

{"request":{"auth_password":"**********","host":"*.*.*.*:*
***","index":1,"method":"HEAD","referer":"http://*.*.*.*:****/","
server":"*.*.*.*","uri":"/tuc/xml/TeamClass_4570000_0.zip","us
er_agent":"Mozilla/4.0","username_auth":"msger_attach"}}

**tns**

{"request":{"username":"Administrator"}},
{"request":{"password":"**********","que
ry":"SELECT USER FROM DUAL","username":"****"}},
{"request":{"query":"BEGIN DBMS_OUTPUT.DISABLE; END;"}},
{"request":{"query":"SELECT
ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VA
LUE FROM @SYSTEM.PRODUCT_PRIVS WHERE
(UPPER('SQL*Plus') LIKE UPPER(PRODUCT₩****)) AND
(USER LIKE USERID)"}},

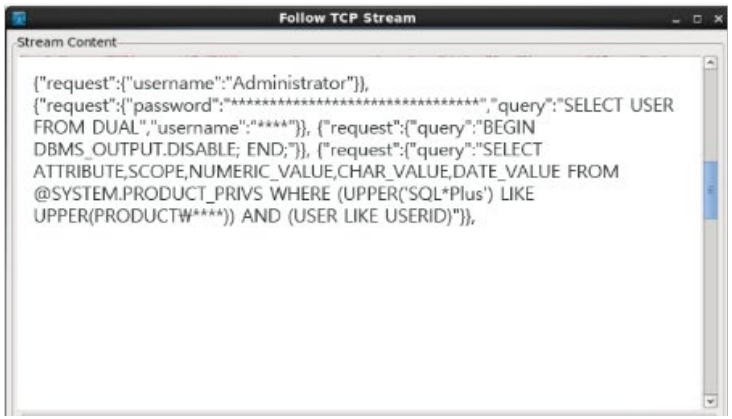
**ftp**

{"request":{"index":1,"method":"CWD","password":"********","
username":"root"}}, {"request":{"index":2,"method":"TYPE"}},
{"request":{"index":3,"method":"PASV"}},
{"request":{"filename":"xxxx","index":4,"method":"SIZE"}},
{"request":{"filename":"xxxx","index":5,"loadway":"Download",
"method":"RETR"}}, {"request":{"index":6,"method":"CWD"}},

# #2. 네트워크 암호화 : HDN - 네트워크 트래픽 암호화 기술

**차세대 보안스위치**

- 이더넷 구간의 암호화를 통해 모든 전송데이터의 위/변조 방지
- 데이터 기밀성과 무결성 보장
- 네트워크상에서의 데이터 스니핑 위협에 대한 보안 강화

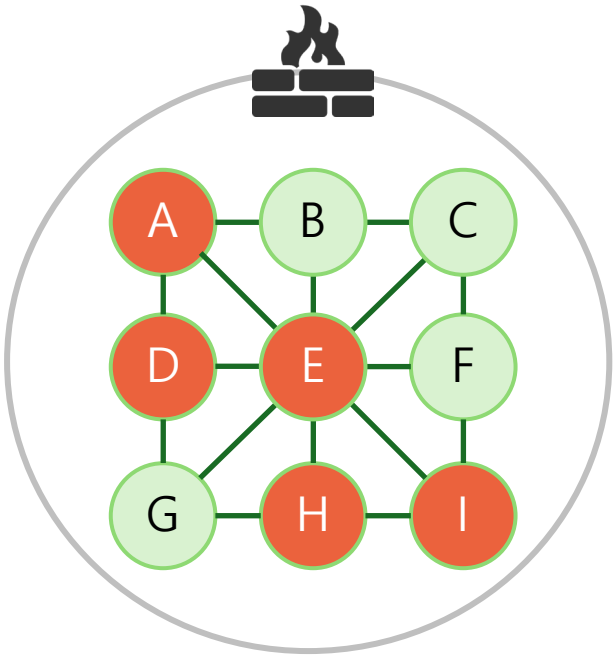

# 단계별 제로트러스트 네트워크 전략

| 기능 | 기존 수준 | 향상 수준 | 최적화 수준 |
|---|---|---|---|
| 네트워크 세분화 | 대규모 경계·분리를 사용하는 네트워크 구조 정의 | 일부 내부적인 세분화를 갖는 송수신 소규모 경계를 통해 더 많은 네트워크 구조 정의 | 네트워크 구조는 주변 응용 워크플로우를 기반으로 완벽히 분산된 송수신 세부 경계 및 더욱 깊은 내부 세분화로 구성 |
| 암호화 | 최소한의 내외부 트래픽에 대한 명시적 암호화 | 내부 응용에 대한 모든 트래픽 및 일부 외부 트래픽 암호화 | 가능한 경우, 내외부로 전달되는 모든 트래픽 암호화 |
| **위협대응** | 알려진 위협 및 정적 트래픽 필터링을 핵심 기반으로 위협 보호 수행 | 위협을 사전에 발견하기 위한 기본 분석 포함 | 컨텍스트 기반 신호와 기계학습 기반 위협 보호 및 필터링 통합 |
| **가시성 및 분석** | 중앙 집중식 수집 및 분석을 통하여 경계에서 가시성 제공 | 수동 정책기반 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 | 자동화된 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 |
| **자동화 및 통합** | 변경 관리 워크플로우에 따라 네트워크 및 환경 변경을 수동으로 초기화 및 실행 | 수동으로 네트워크 및 환경 변화를 시작하기 위한 자동화된 워크플로우 사용 | 네트워크 및 환경 설정을 위해 지속적 통합·지속적 배포(CI/CD) 배포 모델에 따라, 자동화와 함께 코드로서의 인프라를 사용 |

# 제로트러스트 네트워크 핵심요소 - #3.위협대응, 가시성, 분석, 자동화

**AI/머신러닝 기반의 지능형 보안 (Intelligence-based Security)**

- 코로나19를 통해 기존 경계보안 모델에서 제로트러스트 모델로 대응체계 전환
- 사이버 보안 관점에서 데이터 수집,관리를 통한 가시성 확보
- 방대한 데이터 분석을 위한 기계학습(머신러닝) 기술 적용 필요
- 분석 내용을 기반으로 자동화된 보안 대응체계 구축




가시성 확보

데이터 관리

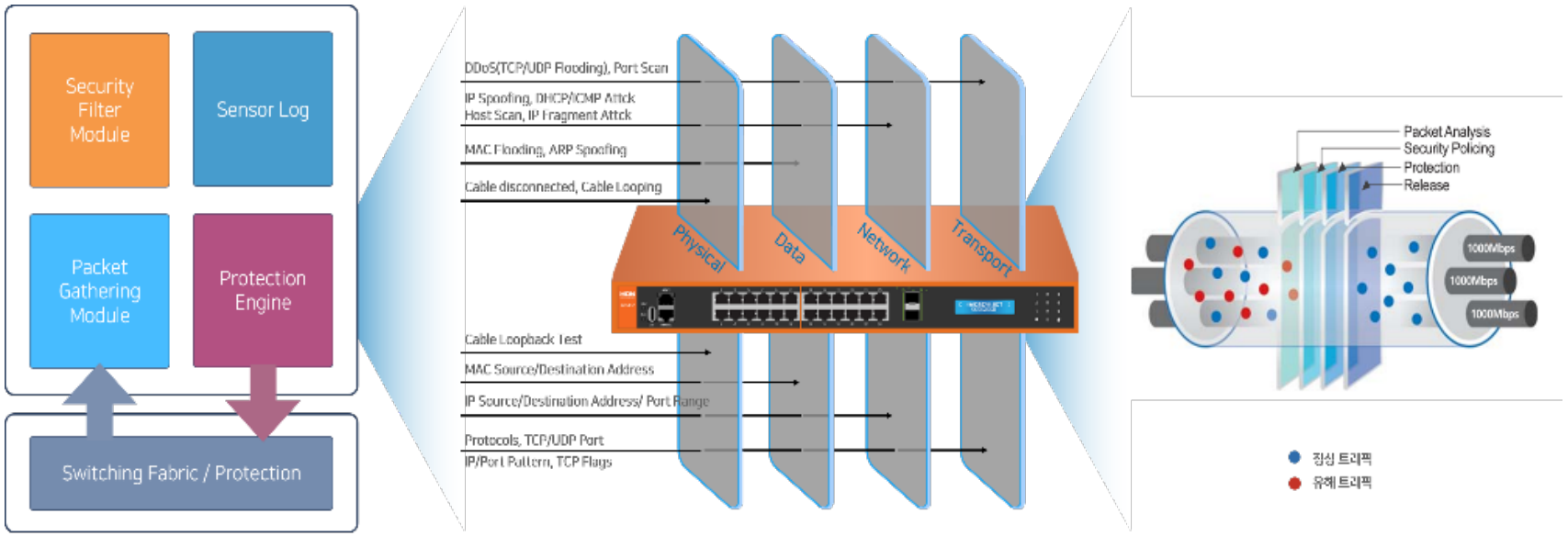
AI /머신러닝

대응

# #3-1.위협대응 : HDN - 보안스위치

## 보안스위치 MDS 엔진

- 특허받은 MDS 보안엔진 기술 및 알고리즘
- 정상트래픽은 통과, 유해트래픽만 선별 차단




MDS 보안 스위치 엔진
(Multi Dimension Security)

4 Layer Anaysis & Control
계층별 선별 차단

Smart Mirroring
원격지 트래픽 분석

# #3-2.가시성, 자동화 : HDN – 통합관리 시스템

## 통합관리 시스템 (VIPM)

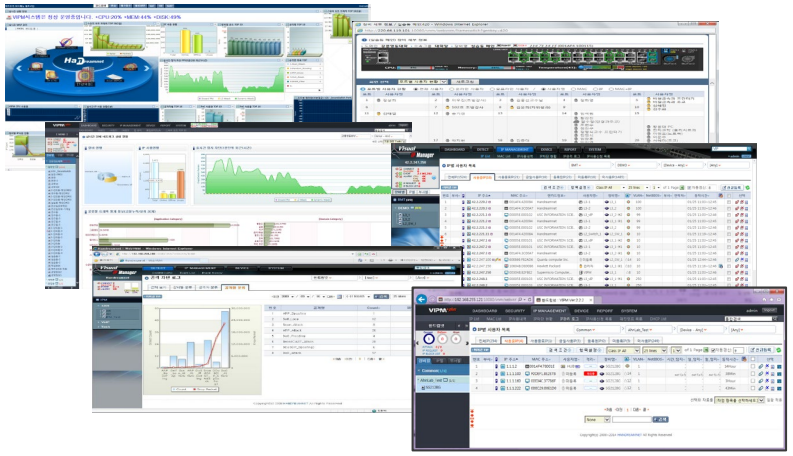
• 보안스위치 네트워크 가시성 제공 및 다양한 제어기능의 통합관리 시스템

VIPM®
Visual IP Manager
VIPM®
Whitelist

비인가 시스템의 네트워크 접속 제어

IP Management

네트워크 공격 및 해킹 차단



**WEB UI를 통한 간편한 설정**
- 별도의 소프트웨어 설치 없는 웹브라우저 환경
- SG보안스위치에 대한 각종 통합설정 기능
- 보안스위치 로그정보 통합관리 모니터링

**부가솔루션과 연동한 진보된 보안기능**
- APT, UTM, FW, IPS 등 다양한 보안솔루션과 연동
- VIPM USM 연동을 통한 유해호스트 차단 기능

**Network 가시성**
- SG보안스위치에 대한 장비 통합관리 및 제어
- 네트워크 문제발생시 직관적인 모니터링 표출
- 네트워크 관리자를 위한 가시성 제공

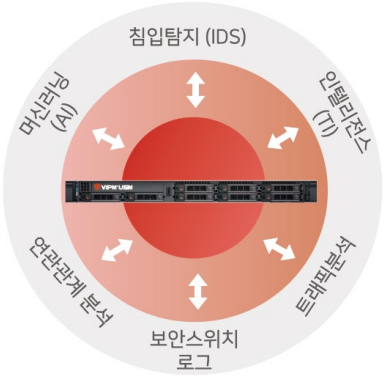
**Non-Agent 기반의 네트워크 관리**
- 별도의 Agent와 Probe 없이 네트워크 관리
- 보안스위치를 통한 IP, Mac 정보 수집 및 모니터링
- 차세대 보안스위치 화이트리스트 룰 설정 및 배포

# #3. 위협분석, 자동화대응 : HDN - 위협분석 시스템

## 위협분석 시스템 (VIPM USM)

• AI/머신러닝 기반의 로그, 트래픽 분석 및 상관관계 분석을 통한 위협관리

VIPM® USM




**네트워크 탐지 및 대응 구성**

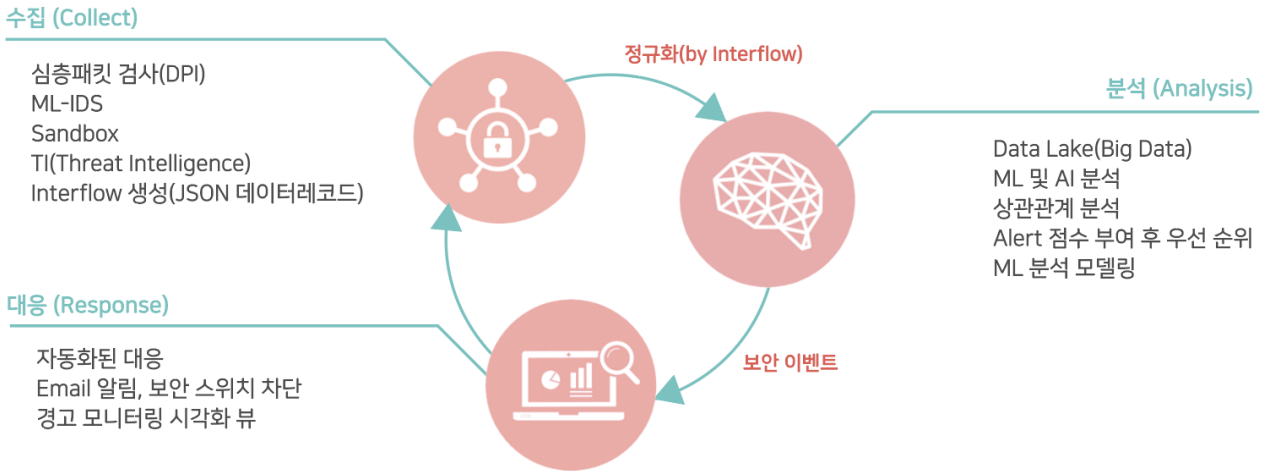
• 트래픽 수집을 통한 보안위협 탐지 및 보안스위치 연계 대응

**보안위협 현황 가시성 제공**

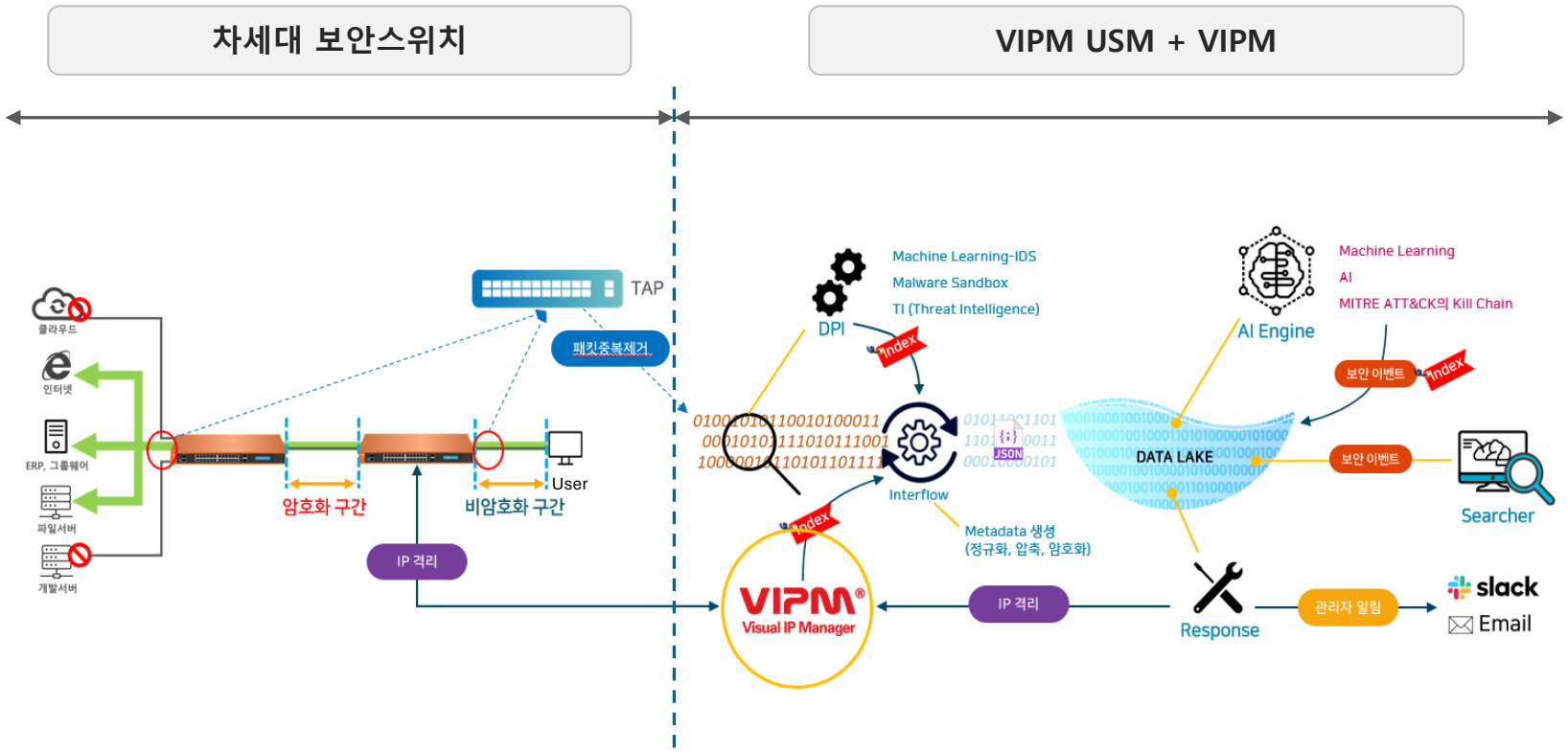
• MITRE ATT&CK 킬체인 보안위협 현황 제공 및 AI기반 분석

**강력한 보안위협 상관관계 분석**

• 빅데이터/머신러닝/AI 기반 보안위협 상관관계 분석 제공



# HDN - 제로트러스트 네트워크 모델 (AS-IS)



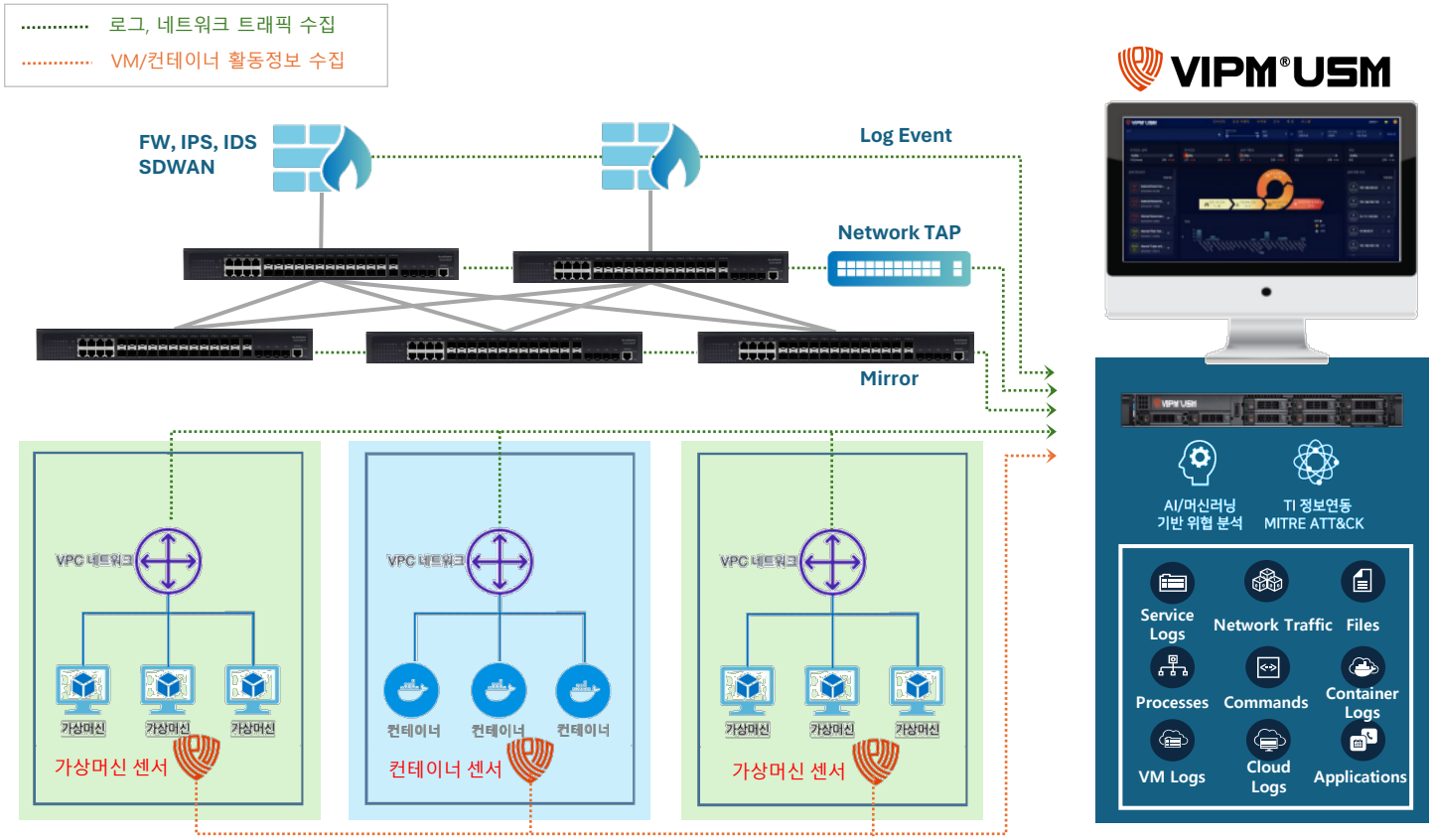

- 네트워크 세분화
- 암호화
- 위협대응

- 가시성 및 분석
- 자동화 및 통합

# HDN - 제로트러스트 네트워크 모델 발전방향 (TO-BE)

**클라우드 + 물리네트워크 통합 보안 분석체계**

- 가상화, 컨테이너 활동 환경을 포함한 데이터 수집 및 통합 분석
- 분석 데이터 수집범위 확대로 위협분석 데이터의 신뢰성 향상



# 한드림넷은?

HDN HANDREAMNET

한국형 보안스위치 최초개발 마켓 리더, 네트워크 보안 전문 기업

## 주요제품 포트폴리오

SubGate






## 데이터센터 클라우드 & 네트워크 보안을 위한 최적의 파트너

ABLECLOUD

All about data & cloud

HDN

HANDREAMNET

글로벌 네트워크 보안 전문기업