엔큐리티

Micro Segmentation is

Essential for Zero Trust Private Networks

2024.01.10

엔큐리티 | CS사업부 기술 2팀

Index

보안 관리자의 운영 챌린지

Chapter 01

보안 관리자의 **운영 챌린지**

자산 식별의 어려움

과중한 업무량

보안 정책 관리의 어려움

엔큐리티

보안 관리자의 **운영 챌린지**

자산 식별의 어려움

Micro Segmentation을 적용하려면
우리의 어떤 자산에 적용을 해야 하지?

우리 회사 자산에 대한 파악은 모두 되어있나?

승인 허가가 되지 않는 자산이 있지 않을까?

클라우드, VM 서버 중 우리가 알지 못하는 자산이 얼마나 되지?

국내·외 분포된 자산이 어떻게 되지?

PoC, BMT 등에 사용되고 더 이상 사용되지 않는 자산은 없나?

엔큐리티

보안 관리자의 **운영 챌린지**

과중한 업무량

1061 ↑

기업당 평균 응용프로그램 수

업무환경의 다양화 및 사용 어플리케이션 증가에 따른 공격표면의 증가

1 in 4

랜섬웨어 공격(2023년)

국내기준 62% 조직에서 랜섬웨어 침해 사고가 두배 증가(전년대비 100%증가)

1 in 3

(IBM/Ponemon Institute)

자체 보안팀에 의한 침해 대응

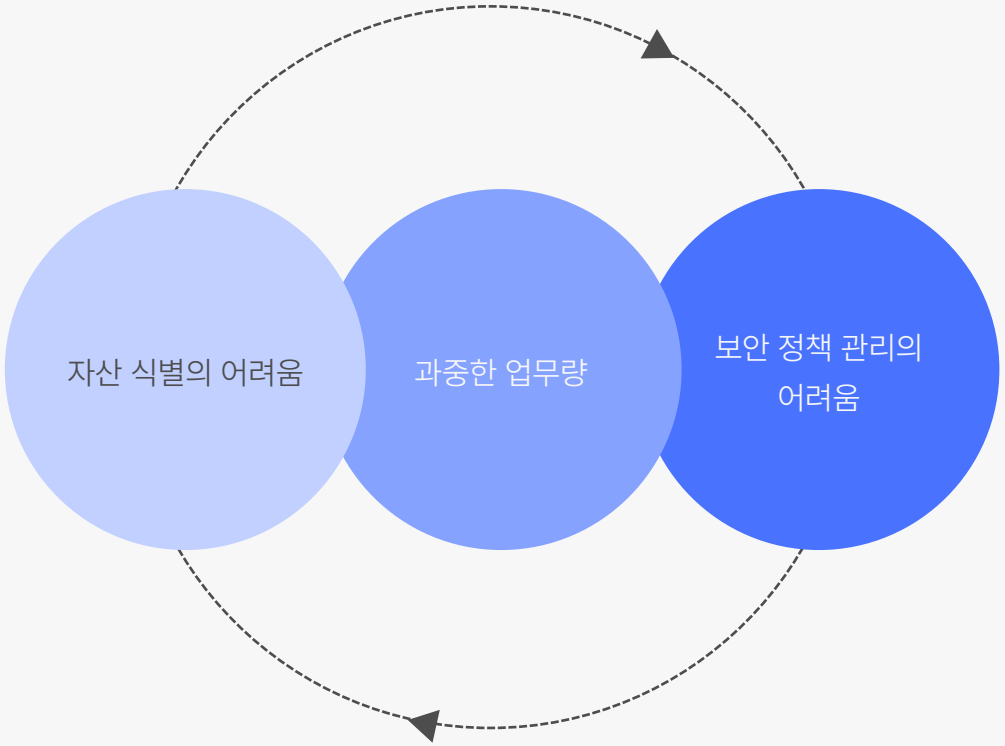
과도한 인시던트 발생에 대한 피로도 증가
정/오탐 분석에 많은 시간 할애

보안 관리자의 **운영 챌린지**

보안정책 관리의 어려움

IT 인프라의 변화에 따라 보다 복잡한 보안구성을 사용

보안 관리자의 **운영 챌린지**



운영 부담 및 오버헤드 증가

비효율적인 자산 관리, 보안 위험 증가,
규정 준수 위반, 운영 비용 증가 등 문제 발생

기업의 전반적인 효율성 및 보안 수준에 부정적 영향 미침

효과적인 자산 관리 및 보안 정책 | 운영 부담과 오버헤드를 감소시켜 비용 절감, 보안 수준 향상 및 규정 준수 보장

엔큐리티

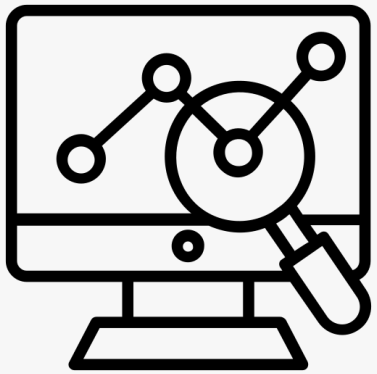
AGS의 해결방안

Chapter 02

AGS의 해결방안

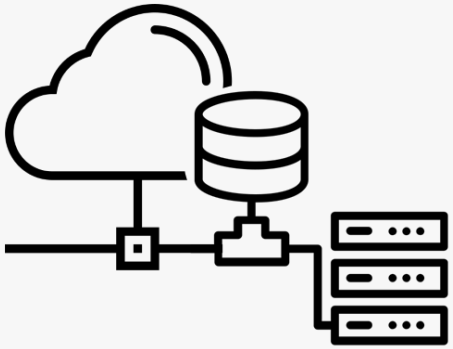
Akamai Guardicore Segmentation

제로트러스트 원칙을 적용한 가장 간단하고 빠르며 직관적인 방법을 제공하는 소프트웨어 기반 Micro Segmentation 솔루션



네트워크 가시성 확보

운영 버든 및 오버헤드 감소
비식별 자산정보 확인



모든 인프라에 대한 지원

모든 인프라 환경에
동일한 정책 적용 및 운용

효율적인 운영 관리

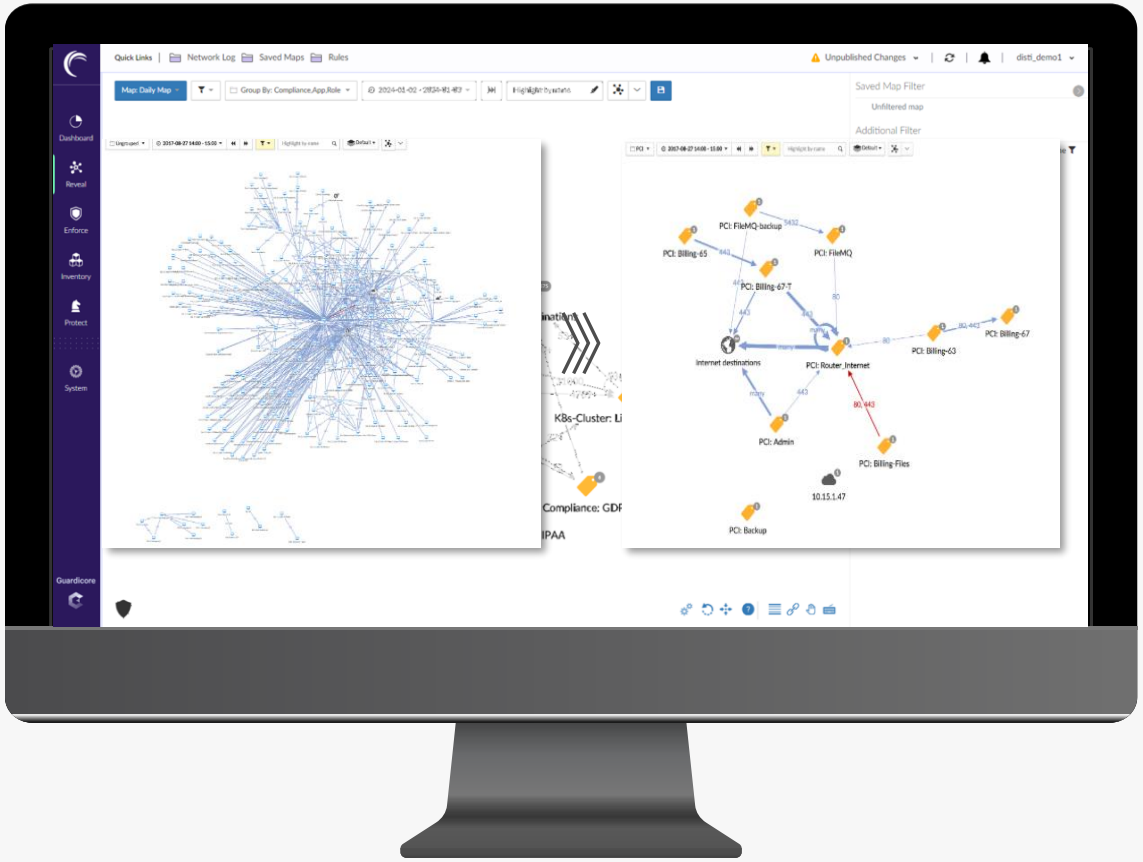
고객의 자산 환경
단순화 및 효율적 관리

AGS의 해결방안

자산 식별의 어려움

실제 트래픽 기반 네트워크 가시성 확보

네트워크 트래픽(L4, L7 Layer)을 시각화하여 네트워크 상태 및 자산 정보 실시간 파악



- 미확인 자산, OT, IoT 장치 통신 정보 확인
- 전사 자산 간 네트워크 통신 이해도 향상
- 규정/규제에 어긋나는 통신 정보 확인
  (PCI-DSS / HIPPA 등)
- 횡 이동 공격 정보 확인 및 대응
- RBAC 기반 차별화된 가시성 제공
  (Role Base Access Control)

엔큐리티

AGS의 해결방안

자산 식별의 어려움

세분화된 자산 식별 및 관리

자산 식별/관리에 도움되는 다양한 기능 제공

네트워크 플로우 분석	• AGS Agent를 설치할 수 없는 환경의 경우 네트워크 트래픽 정보를 미러링하여 통신 중인 모든 자산의 정보 확인 • 중앙집중화된 대시보드를 통한 전체 네트워크 정책 통합적 관리
호스트 기반 탐지	• Agent가 설치되지 않는 자산이 Agent가 설치된 자산으로 접근 시 새로운 자산으로 자동 식별 가능 • Agent가 설치된 자산이 Agent가 설치되지 않은 자산으로 접근 시 새로운 자산으로 자동 식별 가능
Orchestration	• 데이터센터 환경에서 자산에 대한 정보를 가져와 Agent, Collector의 데이터 보완 • 기존 사용중인 태그 정보를 라벨정보로 자동 변환 지원
라벨 기반 정책	• 라벨은 자산 분류 및 그룹화 시 사용 • 라벨을 활용하여 특정 라벨에 대한 정책 설정, 해당 라벨을 가진 워크로드 일괄 정책 적용
Dynamic Criteria 활용	• 다양한 Dynamic Criteria를 활용하여 정책 동적 조정 가능 • 고객사의 IP Table, Hostname 기반 자동 라벨 생성 가능

엔큐리티

AGS의 해결방안

자산 식별의 어려움

ORCHESTRATION

고객사 자산정보 연동으로 더욱 풍부한 가시성 제공

AGS ORCHESTRATION

- 고객사 데이터센터, 클라우드 환경에 배포된 자산에 대한 정보 제공
- 일반적으로 다음과 같은 역할 수행
  - 가시성 강화(이름있는 자산과 IP 주소 매칭)로 AGENT가 설치되지 않은 자산에 라벨링 가능
  - 오케스트레이션 메타데이터(태그)를 AGS 라벨로 변환 및 AWS 태그 정보를 AGS 라벨 정보로 변환 가능
  - INCIDENT 세부 정보 강화
  - 디셉션 리디렉션 로직 지원

Regular Orchestrations

vmware vSphere, Google Cloud, Azure, aws, ORACLE CLOUD, openstack™

Special Orchestrations

Microsoft Active Directory, f5, { api }

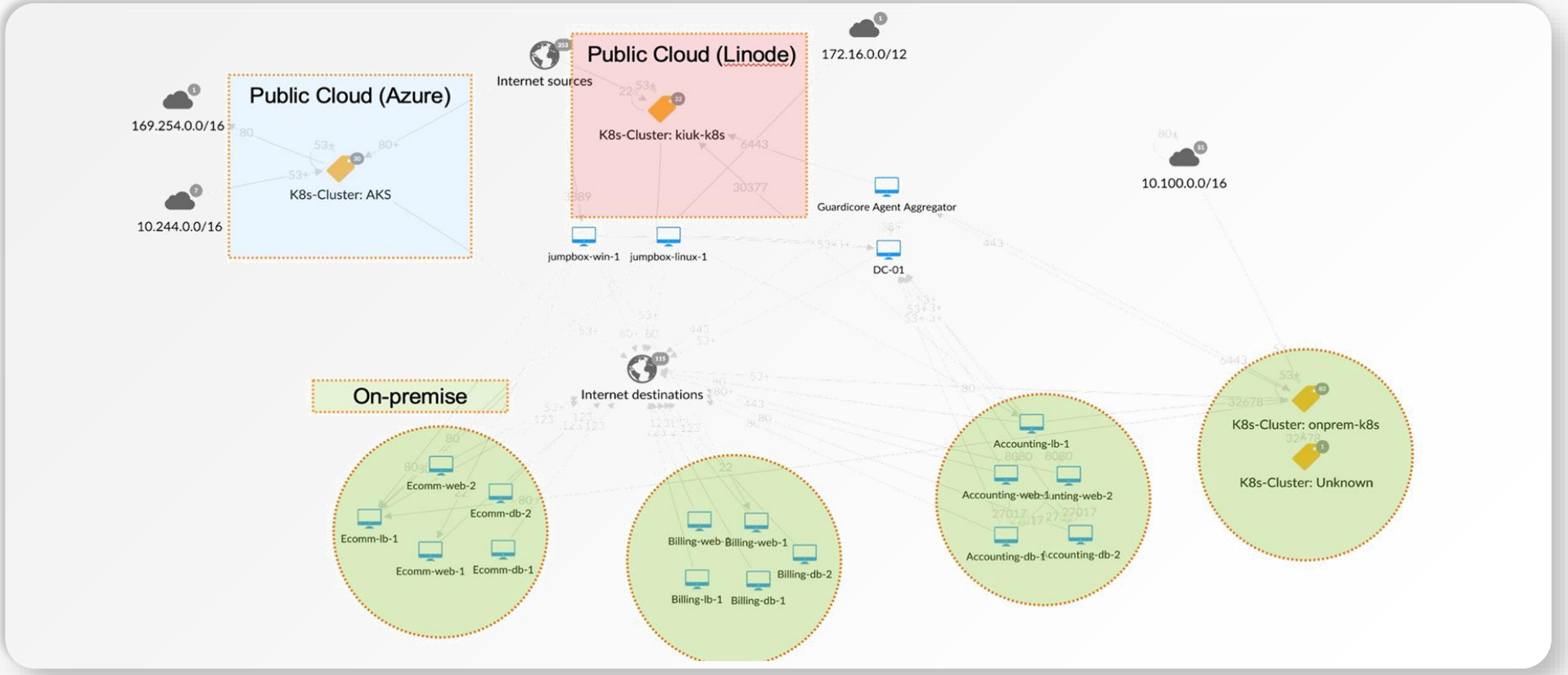
엔큐리티

AGS의 해결방안

운영 주체 모호

모든 인프라 보호

온프레미스, 클라우드 등 모든 고객사 특정 인프라 환경에 귀속되지 않고 동일한 보안 정책 적용 및 운용 가능



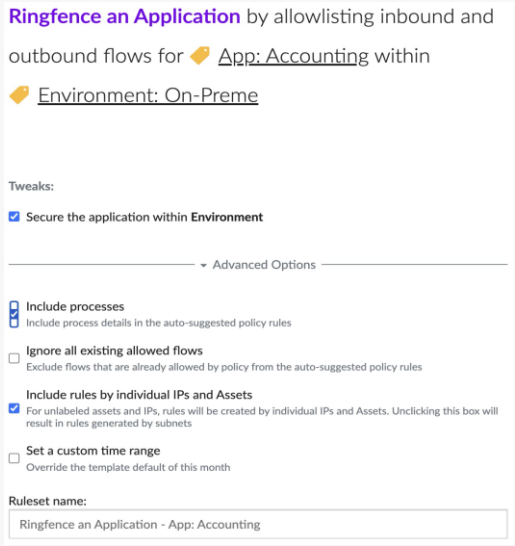
엔큐리티

AGS의 해결방안

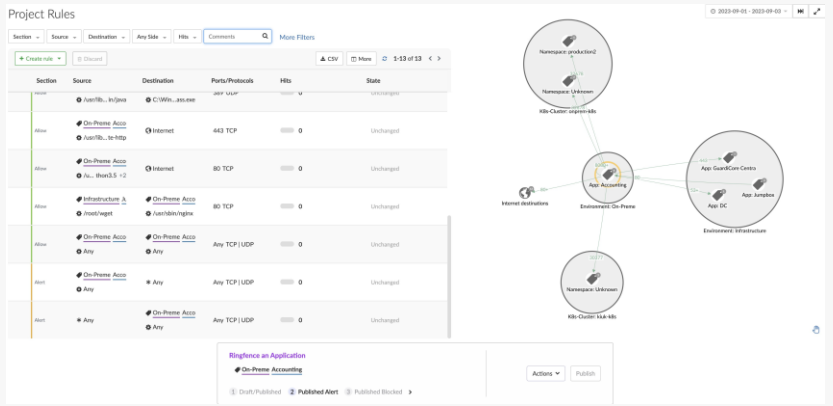
보안 정책 관리의 어려움

AI 기반 정책 추천

모니터링된 네트워크 트래픽 기반 네트워크 정책 추천



- 관리자 설정 없이 원클릭 만으로 수십, 수백 개의 보안정책 생성 지원
- 자동 룰 생성을 통한 시스템 운영 조직의 편의성 및 설정 오류 제거
- 수초 – 분 내 정책 생성을 통한 빠른 보안 대응 가능



- 오류 없는 신속한 AI 보안 정책 설정 지원

엔큐리티

AGS의 해결방안

보안 정책 관리의 어려움

쉽고 유연한 운영과 정책 관리

운영 인프라 증가, 운영환경 다양화에 따른 복잡한 방화벽 접근 정책 수립 자동화

네트워크 가시성 확보

- **트래픽 모니터링**
  실시간 네트워크 트래픽 모니터링, 활동 추적 및 이상 행위 감지
- **플로우 데이터 분석**
  플로우 데이터 분석 통계 및 트렌드 파악, 보안 이벤트 및 패턴 인식 대응
- **라벨을 활용한 네트워크 맵핑**
  네트워크 매핑 및 구조 시각화 및 워크로드 간 관계 파악 후, 가시성 확보

AI 기반 정책 추천

- **라벨 기반 정책**
  라벨 활용으로 자산 정책 간편 구성
- **보안 정책 추천**
  인공지능과 기계학습 알고리즘 사용, 네트워크 환경 분석 및 보안 정책 추천
- **효과적인 정책 수립**
  보안 전문가 네트워크 보안 정책 설정 도움, 더욱 효과적인 정책 수립 가능

쉽고 유연한 정책 관리

- **중앙집중식 관리**
  온프레미스, 클라우드 등 하이브리드 환경에서 중앙집중화된 방식 정책 생성, 관리, 배포
- **Akamai 위협 인텔리전스 (SaaS)**
  매일 업데이트되는 IP 목록 구성, 악성 IP에 대한 블랙리스트 생성

엔큐리티

통합된 운영환경 및 세분화된 보안정책 구현

“Akamai Guardicore Segmentation”

네트워크 보안 강화 및 제로트러스트 환경 실현

네트워크 가시성 확보, 모든 인프라에 대한 지원,
효율적인 운영 관리 기능 제공

제로트러스트 보안에 가장 효과적인 솔루션

Micro Segmentation

네트워크 세분화가 매우 중요한 제로트러스트 모델에서 네트워크 내 애플리케이션과 워크로드를 격리시켜 보안 강화

세분화된 액세스 제어

제로트러스트 모델의 핵심 원칙 중 하나인 최소한의 액세스만 부사용자 및 디바이스 별 필요한 여

동적 액세스 제어

제로 트러스트 모델에서 필요한 동적 액세스 기능을 제공하여 네트워크 트래픽 분석을 통해 실시간 보안 정책 조정 및 위협 식별

정책 강화 및 규정 준수

네트워크 통신을 가시화 하여 규정 준수 의무가 있는 모든 자산에 라벨을 생성/부여 후 규정에 맞는 정책을 생성

엔큐리티

과기정통부, 제로트러스트 구현 핵심원칙 준수

“Akamai Guardicore Segmentation”

Akamai만의 Zero Trust Micro Segmentation Value

Micro Segmentation	• 사용자 통합인증 및 최소한의 권한으로 네트워크 접근 제어 • 차세대 S/W 기반의 마이크로 세그멘테이션 • 간단하고 빠르게 UI를 활용한 L7기반 전사 네트워크 제어
전사 플랫폼의 네트워크 트래픽 가시성	• 현 글로벌 Top1 기업, Akamai만의 독보적인 기술 • 전사 모든 플랫폼 (On-Premise, Cloud, SaaS, K8 등) 트래픽 및 L7정보 네트워크 토폴로지 맵 제공
랜섬웨어 감염 탐지 및 측면이동 공격 방어	• Reputation 기반 네트워크 접근 사전 차단 및 보고 • 내부 감염된 장치 측면이동(Lateral Movement) 접근 시 자동 차단 및 보고 • L7 프로세스 기반의 정책 수립으로 네트워크 차단 및 격리

과학기술정보통신부

< 제로트러스트 구현 핵심원칙 >

핵심 원칙	세부 내용
인증 체계 강화	▲ 각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근 위치 등을 판단)를 핵심요소로 설정하여 인증 정책 수립 ※ 기업내 사용자에 대한 여러 아이디를 허용하여 일관된 정책을 적용하지 않거나, 신뢰도 판단없이 단일 인증 방식만으로 접속을 허용할 경우 **크리덴셜 스터핑에 취약**
마이크로 세그멘테이션	▲ 보안 게이트웨이를 통해 보호되는 단독 네트워크 구역(segment)에 개별 자원(자원그룹)을 배치하고, 각종 접근 요청에 대한 지속적인 신뢰 검증 수행 ※ 개별 자원별 구역 설정이 없으면, 기업망 내부에 침투한 공격자가 중요 리소스로 이동하기 쉬워 **횡적이동 공격 성공 가능성**이 높아짐
소프트웨어 정의 경계	▲ 소프트웨어 정의 경계 기법을 활용하여 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자·단말 신뢰 확보 후 자원 접근을 위한 데이터 채널 형성 ※ 클라우드·온프레미스로 구성된 기업 네트워크 내부에서 단말이 임의 데이터를 전송할 수 있다면 **네트워크 및 호스트 취약성에 따르는 피해 가능성**이 커짐

[NIST SP 800-207, 제로트러스트 아키텍처에 대한 다양한 접근법(3.1절)을 기반으로 작성]

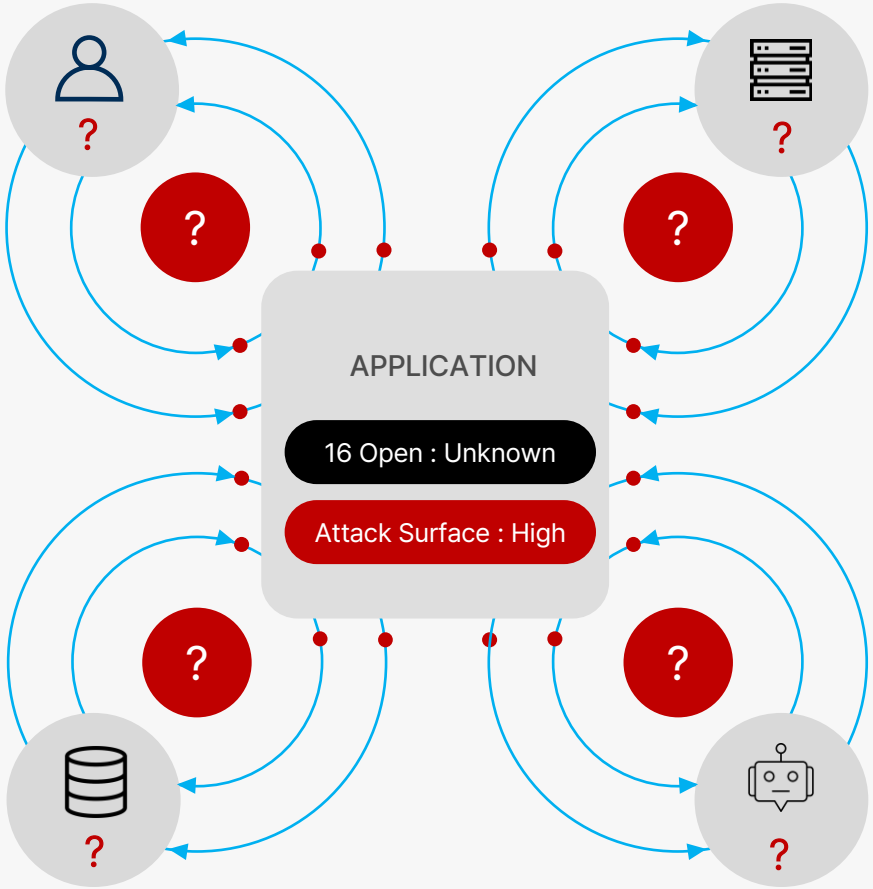
제로트러스트 가이드라인 보기

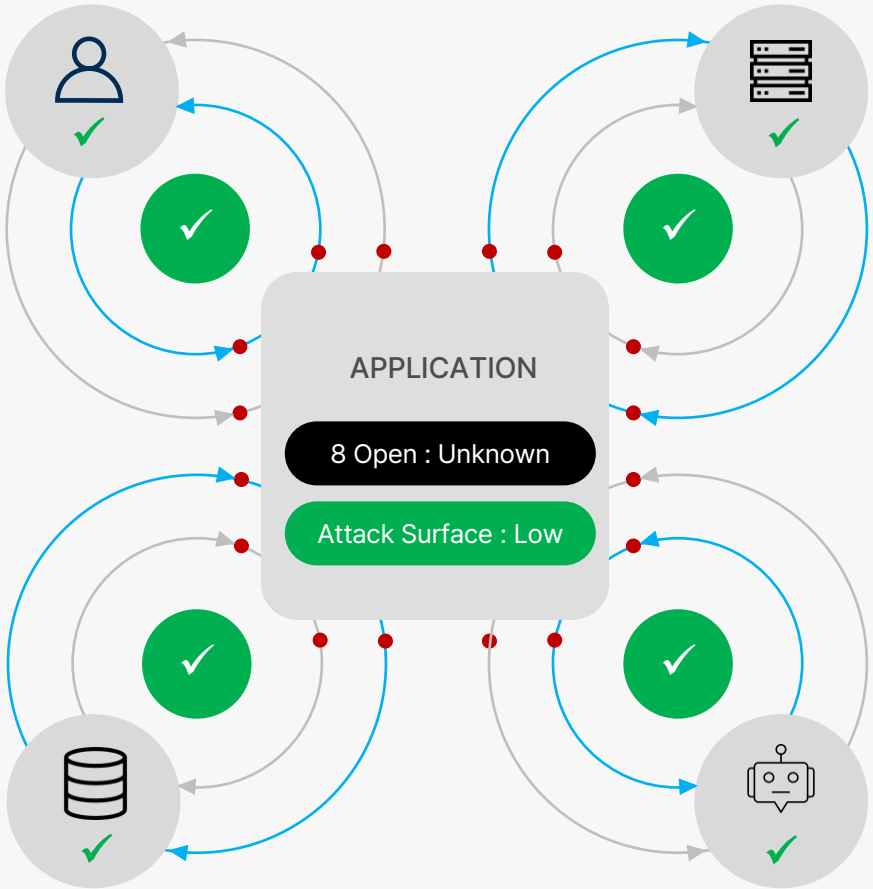
엔큐리티

Micro-Segmentation 이란?

“Zero Trust에 기반한 East-West 트래픽 제어”

공격표면 감소, 침해 탐지 및 각종 규정 준수 강화





엔큐리티

Micro segmentation 의 필요성

Point 1

공격표면 감소

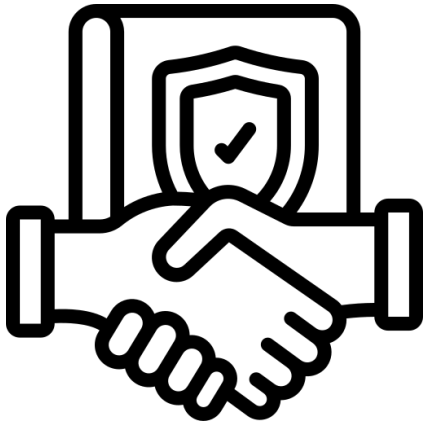
네트워크 시각화를 통한
불필요한 연결 확인

Point 2

보안침해 억제

상호 격리된 네트워크로 침해사고
발생 시 확산 방지

Point 3



유연한 정책 관리

네트워크 모니터링을 통한 정책 설정
및 AI를 활용한 정책 추천

Point 4

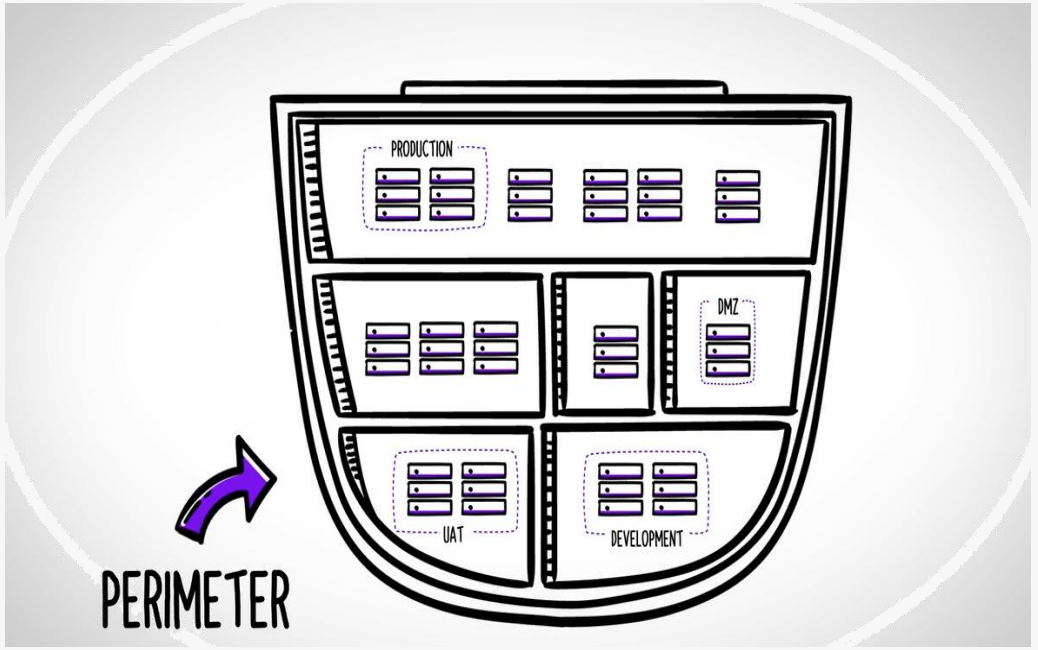
규정 준수 간소화

개별 워크로드에 대한 세부 정책
설정 및 네트워크 통신 제어

엔큐리티

Micro Segmentation이 제로 트러스트에서 차지하는 비중

제로트러스트 실현을 위한 첫 단계는 네트워크 환경 및 자산에 대한 완전한 이해



- Zero Trust 정책에 위배되는 모든 위협 및 위반 사항 지속적인 모니터링
- 측면이동 공격 탐지
- 공격표면 감소
- 중요한 어플리케이션 보안

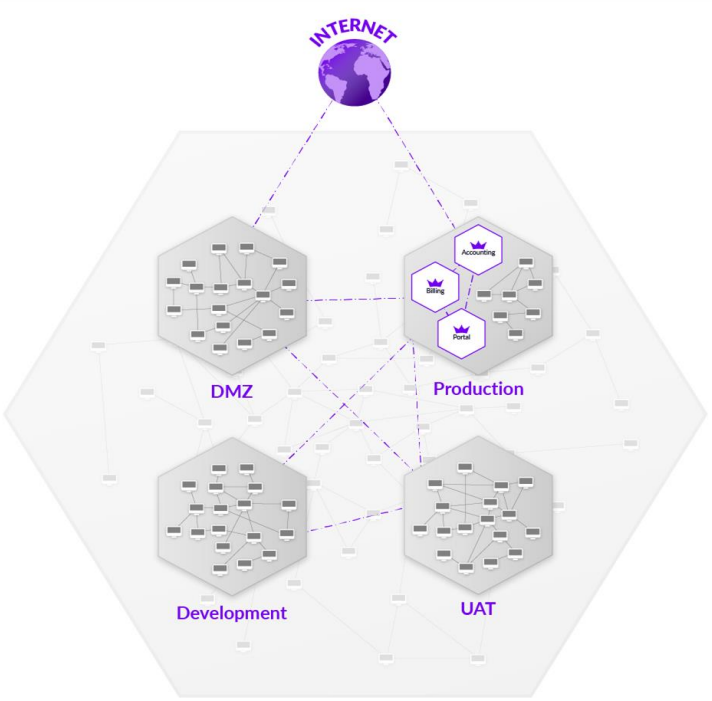
- 보안 정책을 애플리케이션 논리와 일치시키는 프로세스 수준 세분성 제공
- 데이터 센터에서 클라우드까지 보안 정책 일관되게 구현
- 다양한 기본 플랫폼에서 일관된 보안 제공

엔큐리티

AGS Architecture

Chapter 03

Micro Segmentation Architecture



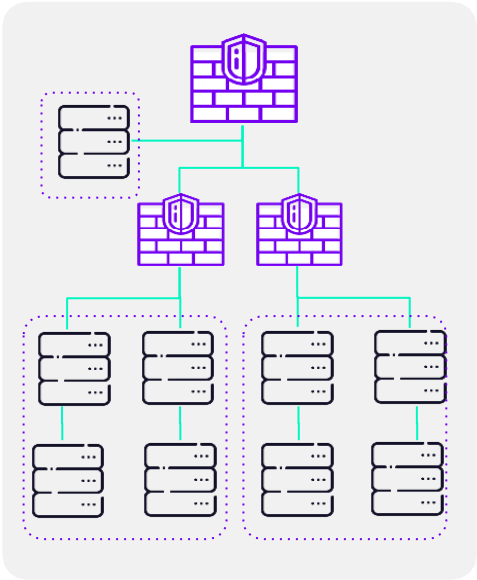
세분화된 특성 기반 Micro Segmentation 구성
(e.g., Process, User, Domain Name)

- On-Premise, 데이터센터, 클라우드, 컨테이너 등 현존하는 거의 모든 플랫폼 일괄 적용 가능
  (단일화된 포괄적인 전사 네트워크 트래픽 및 자산 정보 제공)
- 소프트웨어 기반(Agent 및 SaaS)으로 동작하여 배포가 쉽고 빠름
- 플랫폼 상관없이 Zero trust 기반의 네트워크 접근 제어 정책 적용
- 랜섬웨어 노출&감염 시, 측면 이동공격 선제적 차단 및 Honeypot 기능

엔큐리티

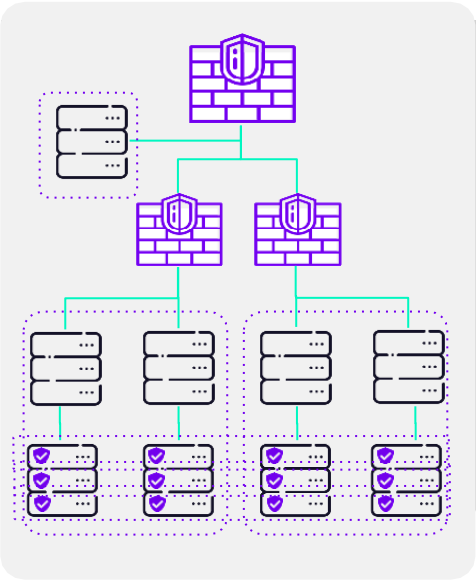
Micro Segmentation 적용 절차

현재



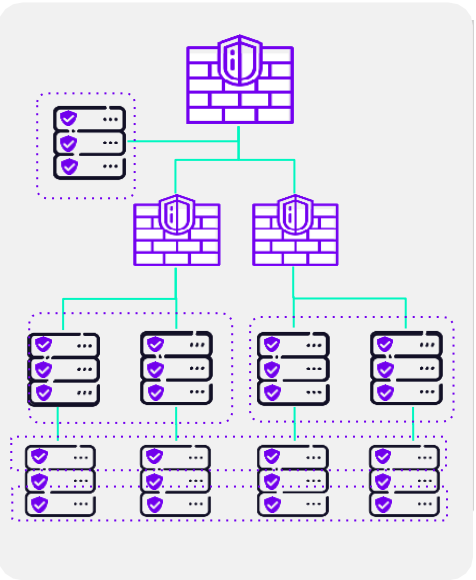
방화벽, VLAN 이용
네트워크 Segmentation 구성

초기 - 일부도입



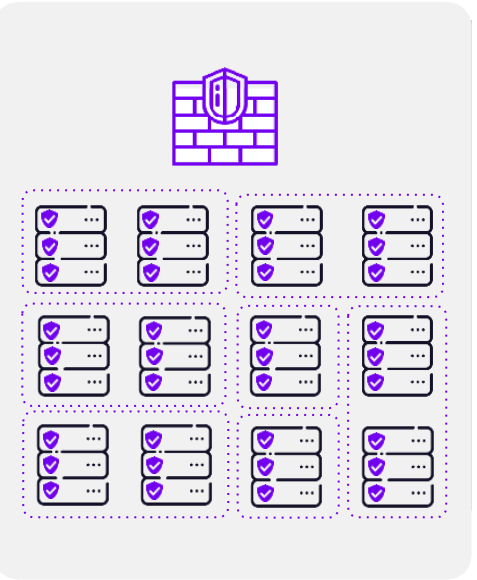
네트워크 위치와 관련 없이
집중 보호 대상 AGS 설치

중기



모든 구간 Agent 설치
(구간 방화벽이 없는 경우에도
정상 동작을 할 수 있는지 확인)

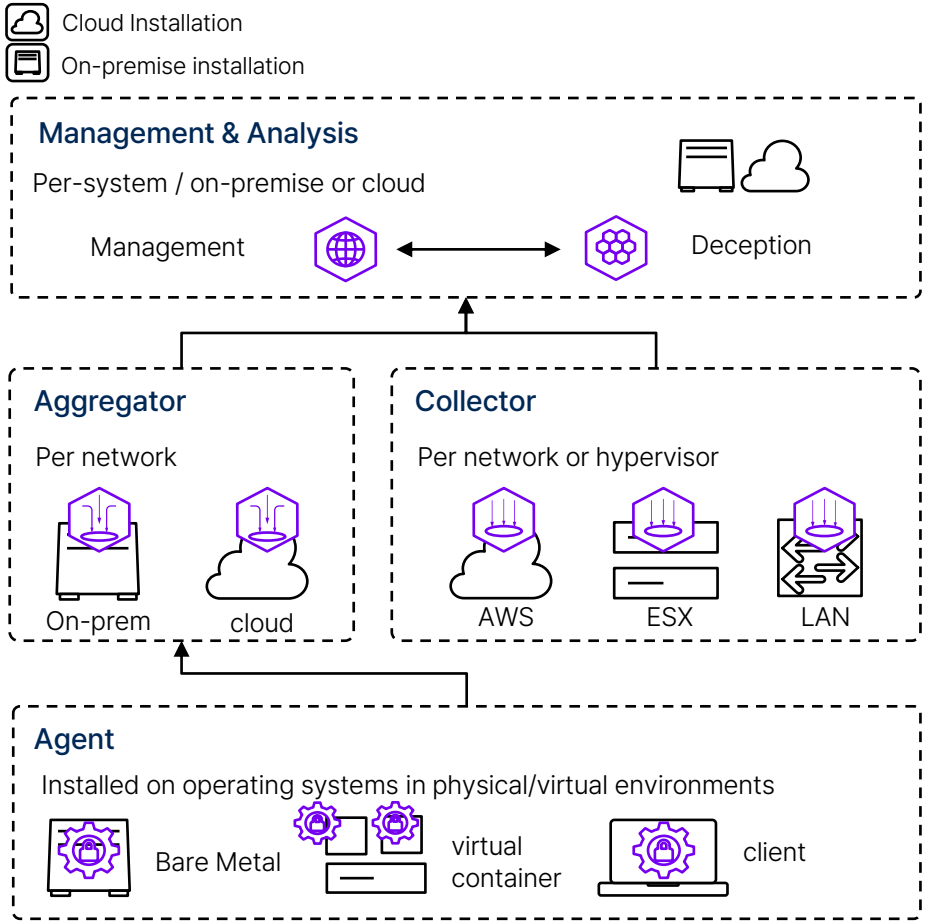
목표



전사 설치 후,
구간 방화벽 제거로 완벽
Micro Segmentation 구현

엔큐리티

전체 구성도



Management (recommendation)

- UI 제공 및 타 시스템과의 연동을 위한 API 제공
- 수집된 데이터 저장 및 분석 및 각 구성요소 관리

Deception (Honeypot)

- 네트워크 차원의 Honeypot 기능 제공
- Incident 정보 기록, 분석 및 알림

Collector (Network Information Collection)

- 스위치 수집 정보를 활용하여 네트워크 스캔 탐지 및 IP/DNS 평판 분석을 위한 흐름 정보 수집
- Agent가 설치되지 않은 디바이스 커뮤니케이션 시각화

Aggregator (Agent management) (recommendation)

- Agent와 Manager 사이에 배치되어 Agent에 대한 설정 관리
- Agent에서 수신 데이터 집계 및 중복 제거

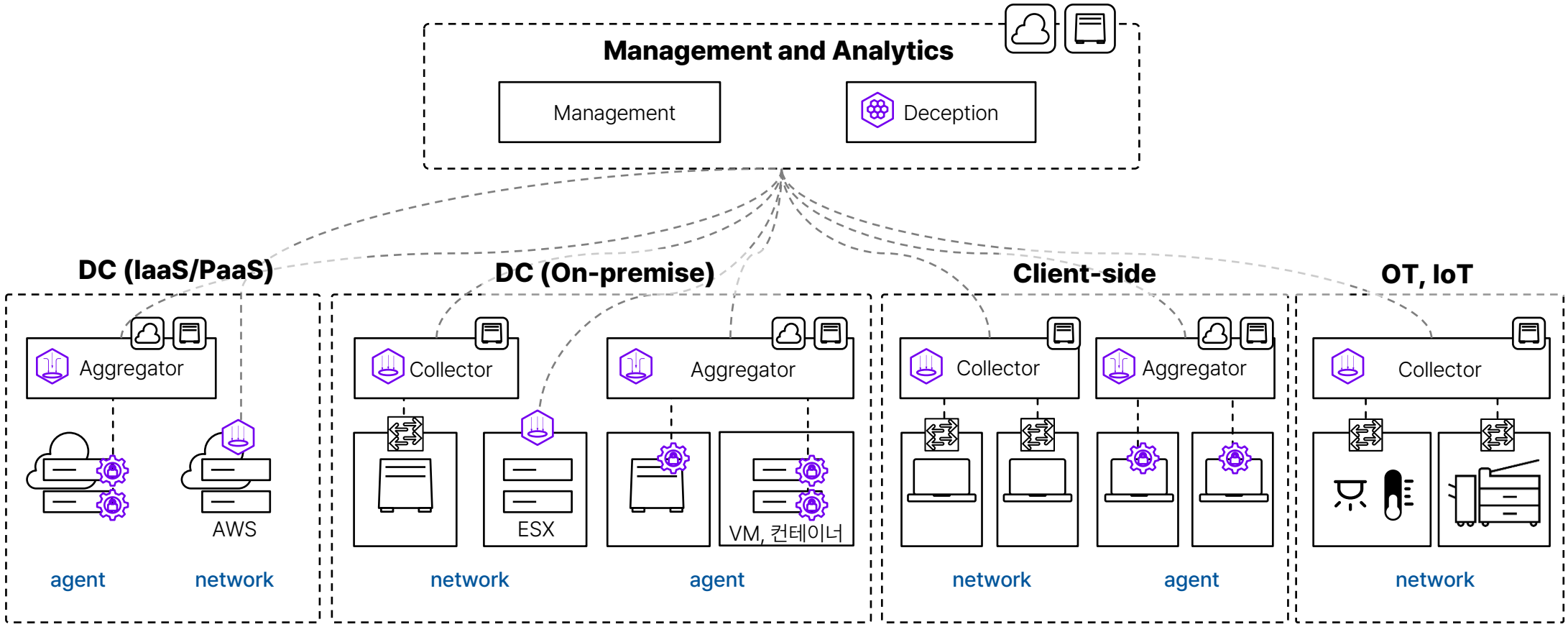
Agent (Device information collection and communication control)

- OS에 설치되어 4가지 기능 제공(Reveal, Enforcement, Detection, Deception)
- 초경량으로 VM, 컨테이너, 클라우드 인스턴스 등 다양한 환경에 배치 가능

엔큐리티

유연한 환경 구성

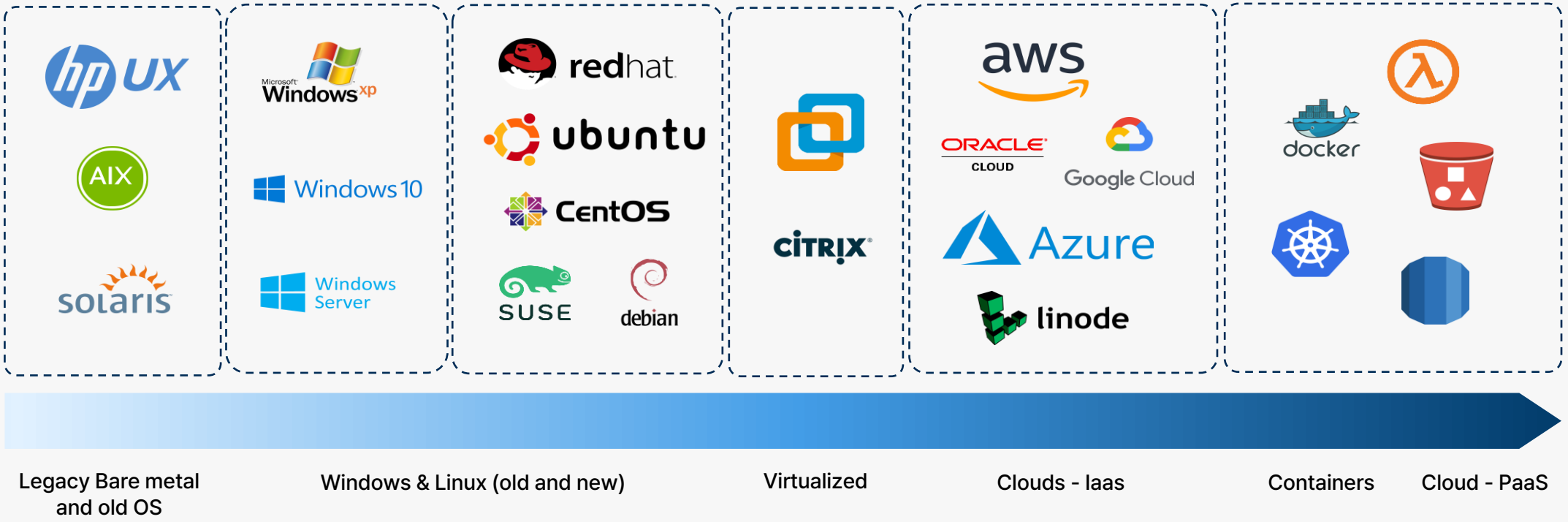
모든 고객사 운영 환경 적용 가능



엔큐리티

모든 인프라 보호

- ✓ 베어메탈, VM, 컨테이너, 퍼블릭, 프라이빗 클라우드 인스턴스, PC 등
- ✓ 다수의 운영 체제 지원 (모든 LINUX 배포 버전, SOLARIS, AIX, AS/400, HP-UX, WIN 2000-WIN 2019, WIN7, WINXP)
- ✓ 컨테이너가 포함된 CORE OS등 (OPENSHIFT/KUBERNETES, DOCKER, GKS, AKS)



엔큐리티

AGS 적용 방안

Chapter 04

Akamai Segmentation 주요 기능

Akamai만의 Zero trust Micro Segmentation Value

Reveal

- 라벨 활용 네트워크 맵을 통해 네트워크 상태 시각적 제공
- 하이브리드 환경 네트워크 실시간 및 과거 활동 정확 모니터링
- 사용자 및 프로세스 레벨 활동 세밀 파악, 보안 이벤트 상세 정보 제공
- Agent 환경(L7 Layer), Agent 리스(L4 Layer) 환경 지원

Enforcement

- 수집된 네트워크 로그, 라벨, 템플릿 활용 손쉬운 정책 설정
- 최소 권한 원칙 기반 안전한 Micro Segmentation 구현
- 세분화된 보안 정책 관리 및 적용하여 워크로드 간 통신 제어
- AI 활용으로 워크로드 실제 활동 기반 정책 생성 및 관리

Detection

- 승인되지 않은 네트워크 통신 시도 확인 및 외부 평판 조회로 위험 감지
- 감지된 위협 IOC정보 추출 SIEM, SOAR 등 활용 가능
- 위험 감지 후, 자동 Deception 서버 라우팅

Deception

- 모든 네트워크 커버 Dynamic Honeypot
- 메타데이터와 스크린샷 저장 및 포렌식 데이터 활용 가능

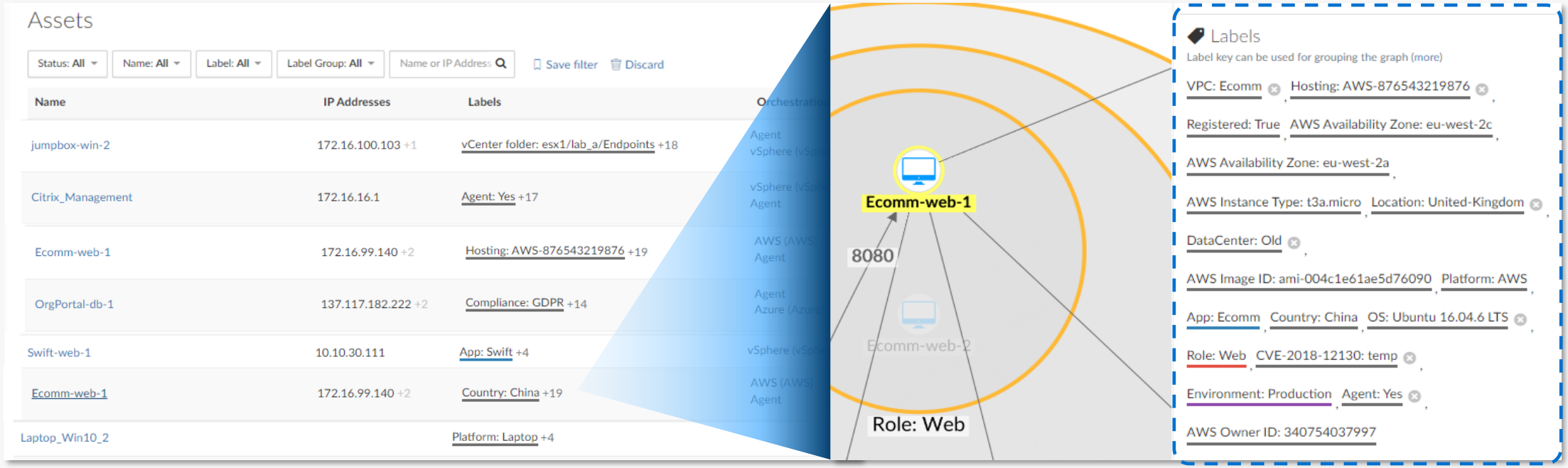
엔큐리티

Reveal 자산 Label 부여

자산 분류를 위해 하나의 자산에 여러 개 라벨 할당 가능
라벨은 Key:Value로 생성, 자유롭게 설정 가능

레이블링 방법

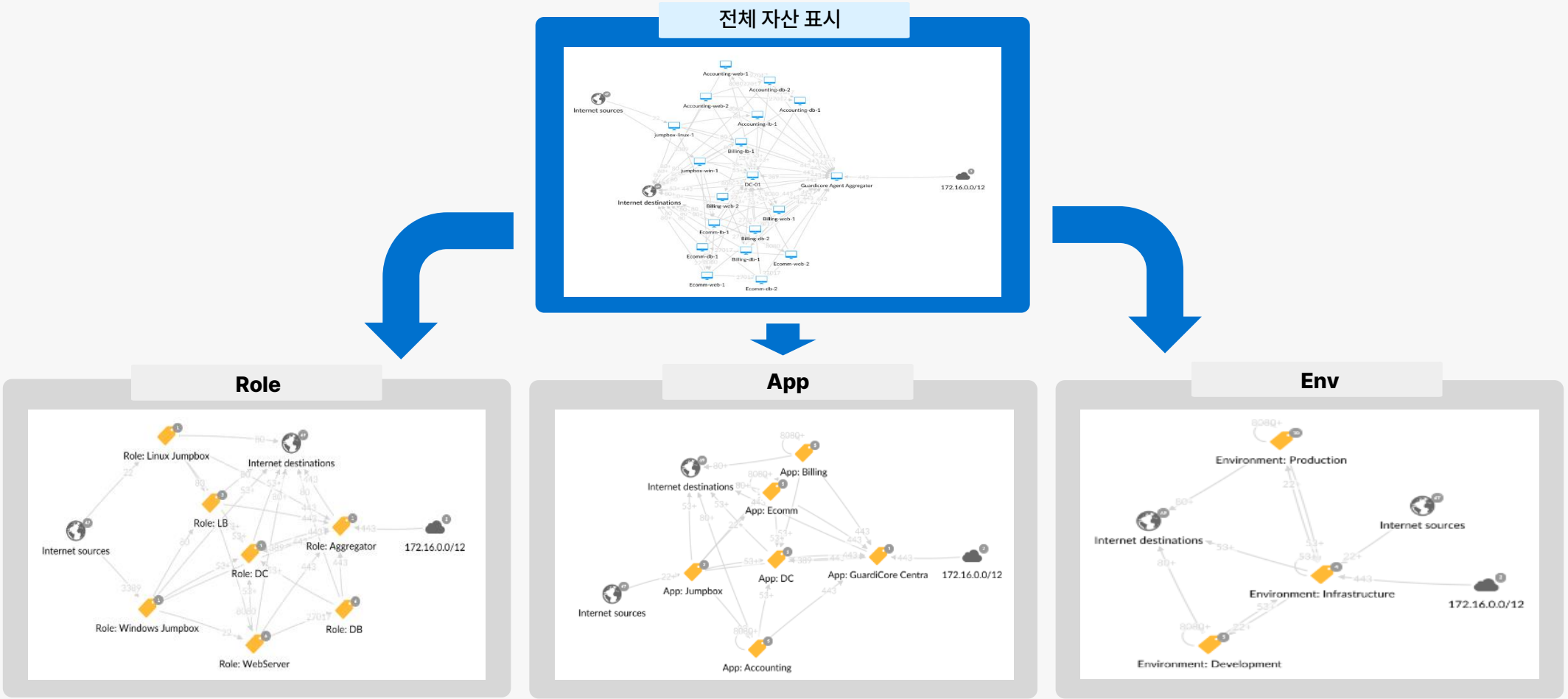
- ✓ DYNAMIC 레이블링(자동 레이블링)
- ✓ REST API 를 활용한 레이블링(CMDB, ORCHESTRATION)
- ✓ AGENT/AI 기반의 레이블링(SAAS 전용)
- ✓ 수동 레이블링
- ✓ EXCEL / CSV 파일을 이용한 대용량 업로드



엔큐리티

Reveal Label 활용 네트워크 맵 생성

라벨 부여 자산은 다양한 관점 네트워크 맵 생성 가능

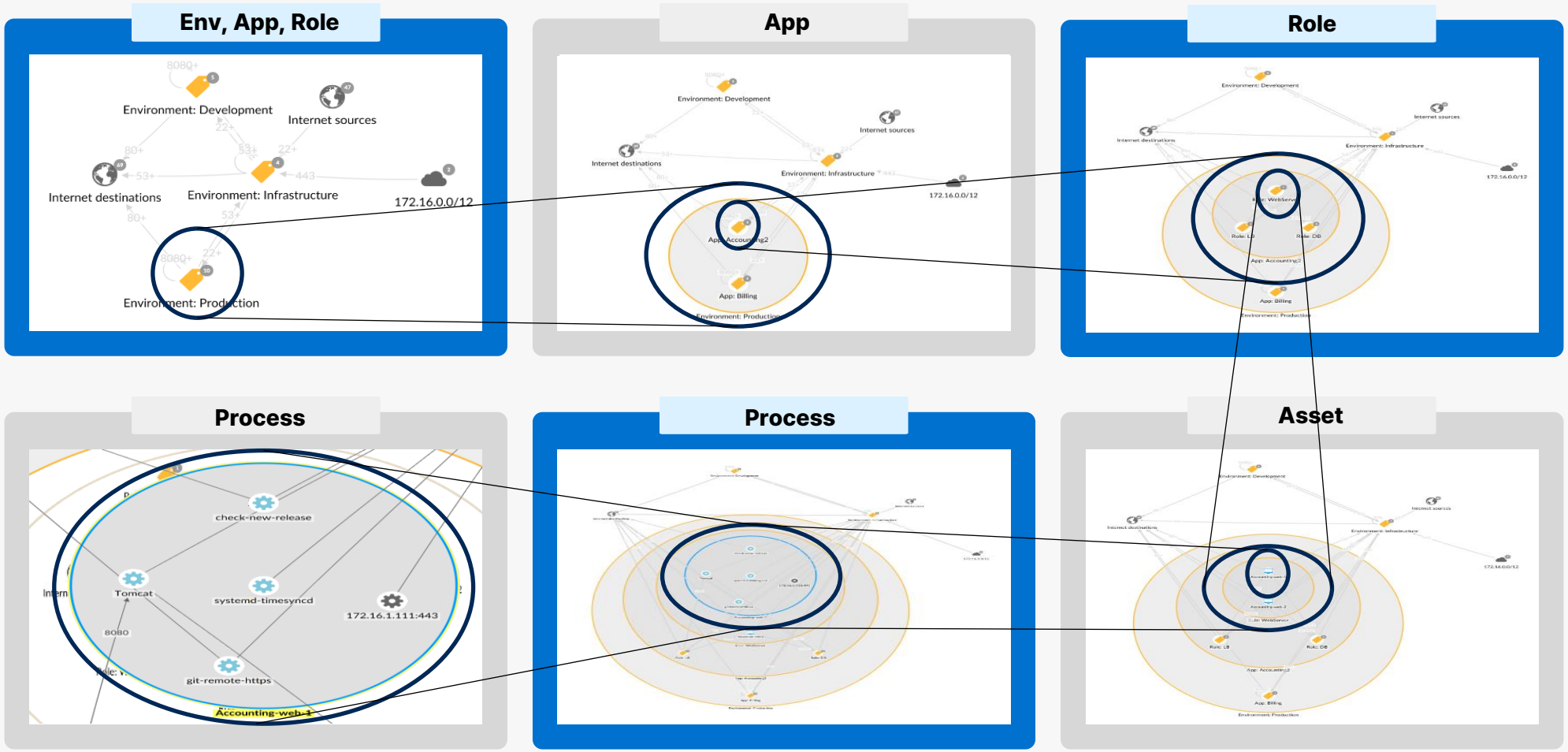


엔큐리티

Reveal

Label의 계층화

자유롭게 설정 가능한 라벨의 계층화



엔큐리티

Enforcement

Label 활용 정책 설정

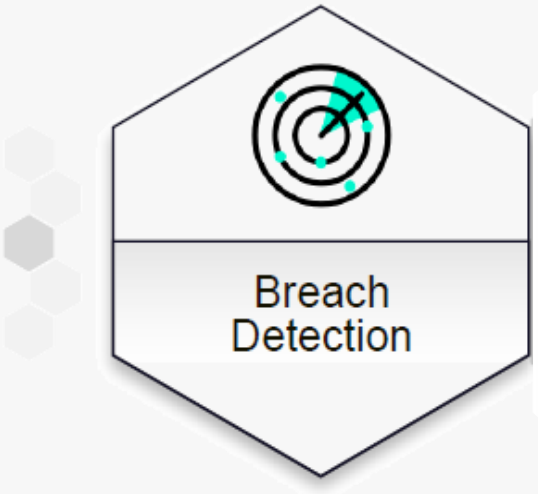
자유롭게 설정 가능한 라벨의 계층화

- **라벨 사용으로 가시성 및 가독성 향상**
- **직접적인 호스트 지정 미필요, 시스템 변경 유연하게 대응**
- 서버의 위치가 이동 되더라도 이전과 동일한 수준의 보안 정책 적용 가능
- 관리자의 변경 등에도 빠른 업무 투입 가능

엔큐리티

Detection 정보유출 탐지(Detection) 및 대응

보안에 관한 새로운 도전, 향상된 인텔리전스 및 더 빠른 침해 예방과 식별



자동화된 분석을 활용, 확장 가능한 다중 탐지 방법

1. 다양한 탐지 방법
   - 평판 기반 탐지
   - 정책 위반 탐지
   - 다이나믹 디셉션 (Dynamic Deception)

2. 서버 맞춤형
   - 서버 및 비즈니스 애플리케이션에 대한 공격 벡터에 집중
   - 확장성 및 리소스 효율성이 우수

3. 분석 자동화
   - 감지된 위협에 대하여 IoC 정보 추출
   - 간단하고 이해하기 쉬운 사고 조사

** IoC (Indicator of Compromise) : 침해 지표

엔큐리티

Detection 프로세스 레벨 무단 액세스 탐지

Incident INC-26D17131 *Severity: Medium*

Affected Assets

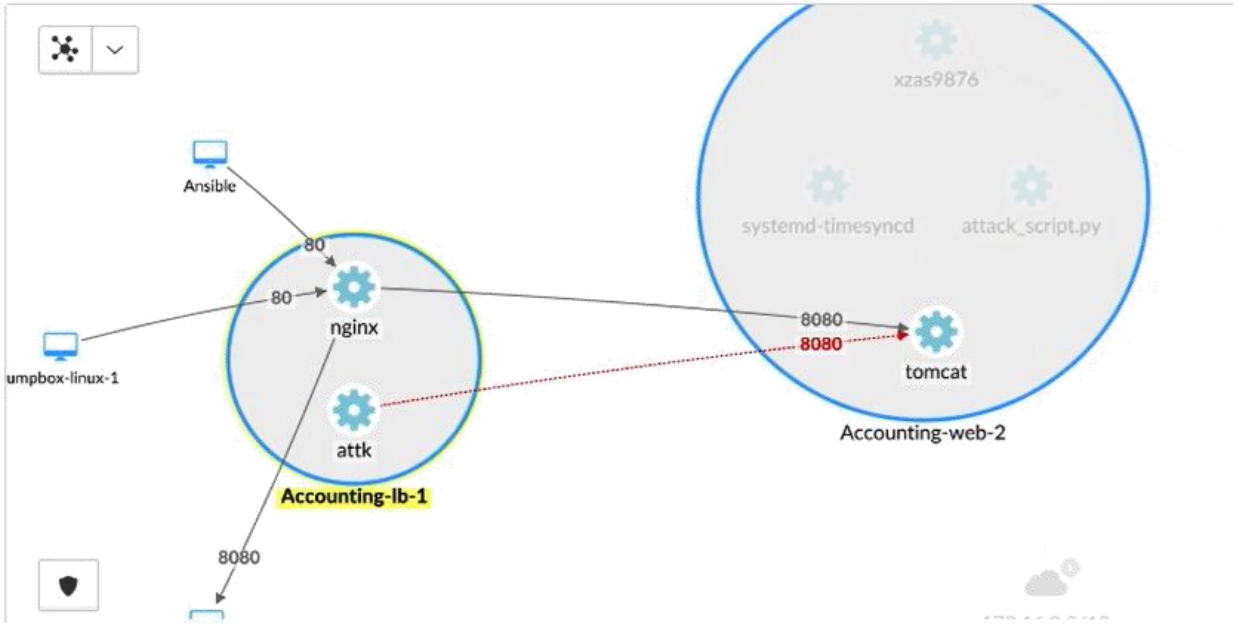
Accounting-lb-1 → Accounting-web-2

Started
2020-01-03 09:16:02

Ended
2020-01-03 09:28:02

Associated Incident Groups
GRP-cb67c20c

Tags
CRM | Blocked Traffic | Internal | Policy Violation
+ Add custom tag



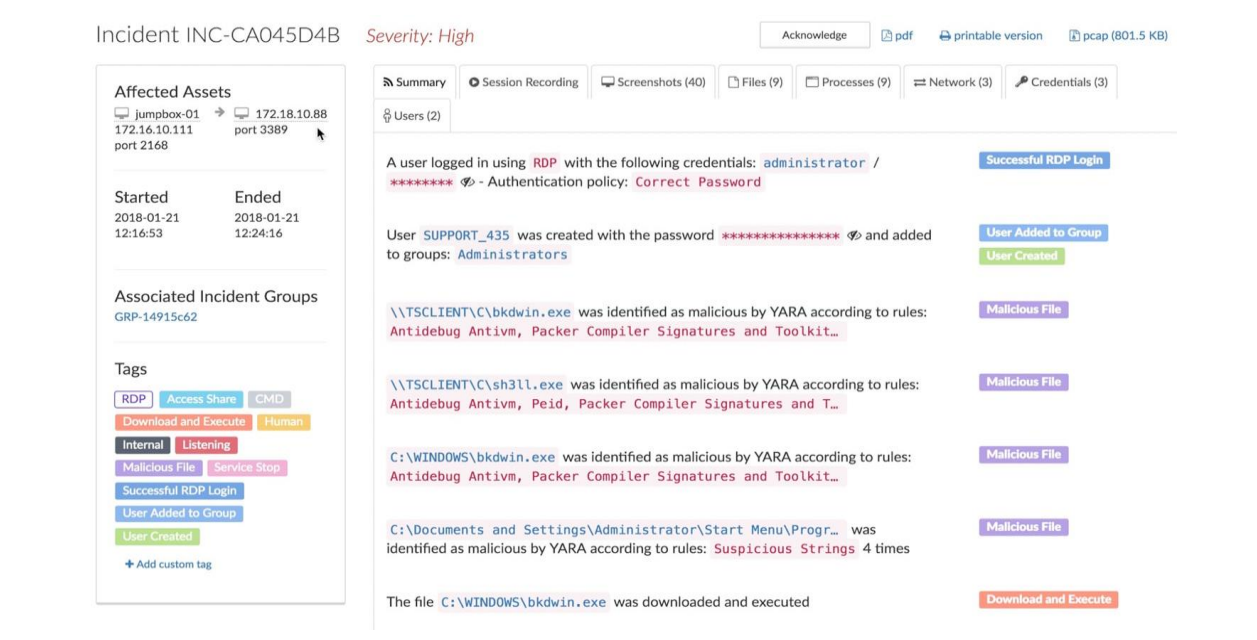
Result

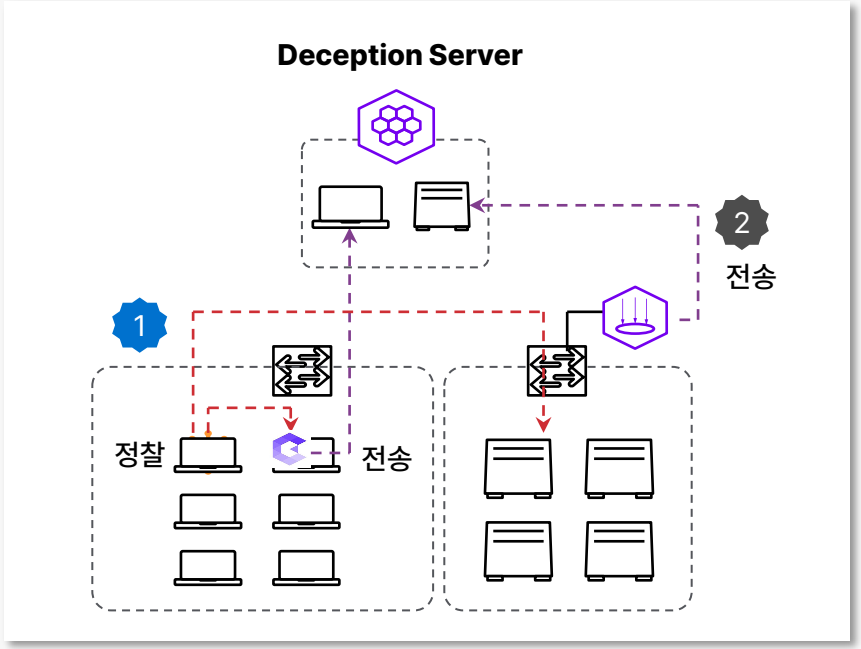
IP 주소/포트가 올바르지만 접속에 필요한 프로세스가 허용되지 않았다면, 통신을 차단하고 Incident를 발행 합니다.

엔큐리티

Deception 공격 분석을 위한 Honeypot

Dynamic Deception





1 Agent

- 모든 연결 실패 측면 이동 시도로 취급 (판단)
- 정책에 의해 차단된 플로우 Honeypot으로 자동 리다이렉션 설정
- 공격자 공격정보 저장 및 새로운 위협정보 수집/분석 후 포렌식 자료 활용 가능

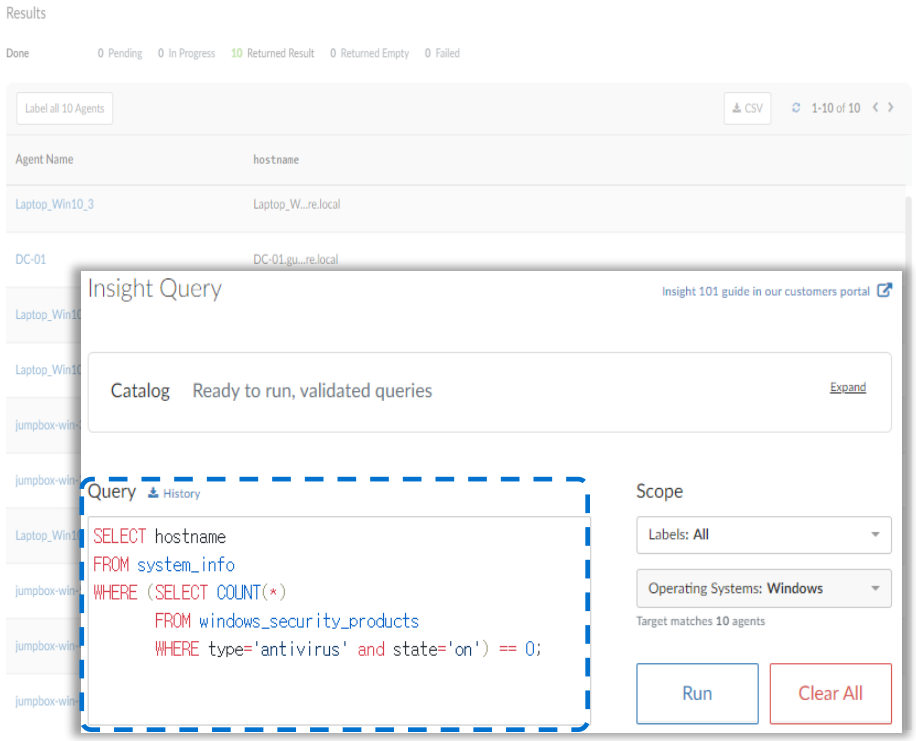
2 Agent Less

- Collector Deception 지원
- 실패한 접속 Deception 서버로 리다이렉션

엔큐리티

Insight Query 지원

보안 전문가가 정교하고 신속하게 보안 데이터 분석 및 이해하는데 도움이 되는 강력한 도구



Detect

OS Query 활용으로 규정 미 준수 고위험 자산 식별

- 각종 Query Github, Windows, Linux 시스템 대응, Query 예약 기능 제공

Assess

자산 위험 수준 평가 및 드러나지 않은 위험 파악

Secure

세분화 정책으로 보안 취약점 제거

엔큐리티

Guardicore 적용 절차

Guardicore 적용 및 설정 변경 시, 다운타임이 필요하지 않음

Step 1

가시성 맵 생성

Agent, Collector 활용
전사 네트워크 트래픽 시각화
및 전체 시스템 이해

Step 2

레이블링&맵핑

수집된 자산정보 레이블링
그룹핑 후 정책 설정 준비
(머신러닝 기반 추천)

Step 3

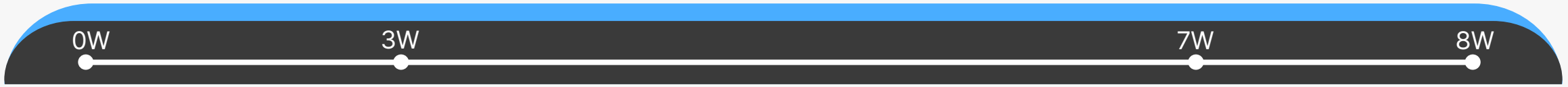
보안정책&침해 확산 방지

정책 템플릿(Custom지원)으로
내부 네트워크 접근
제어 정책 수립

Step 4

지속적 모니터링

최종 전사 네트워크 보안
접근 제어 적용&위반 시 차단



엔큐리티

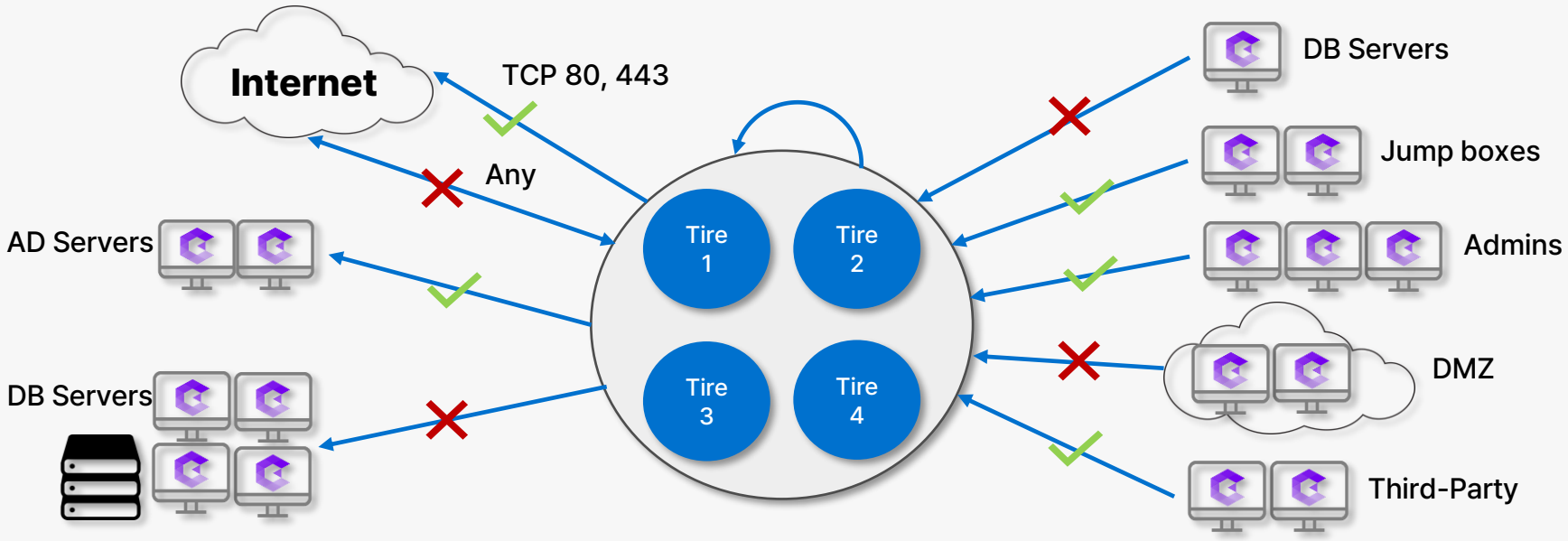
AGS 활용 방안

Chapter 05

중요 어플리케이션 링펜싱

중요 어플리케이션 집중보호

- **중요 애플리케이션 자세히 시각화** : 중요한 애플리케이션이 작동하고 통신하는 방식을 이해하여 효과적으로 보호
- **세분화된 링펜싱 정책 생성** : 애플리케이션이 작동하는 방식을 엄격하게 제어하고 애플리케이션 최대한 격리
- **신속한 공격 탐지 및 대응** : 중요한 자산에 대한 공격을 탐지하고 완화하기 위해 여러 보완 기술 사용

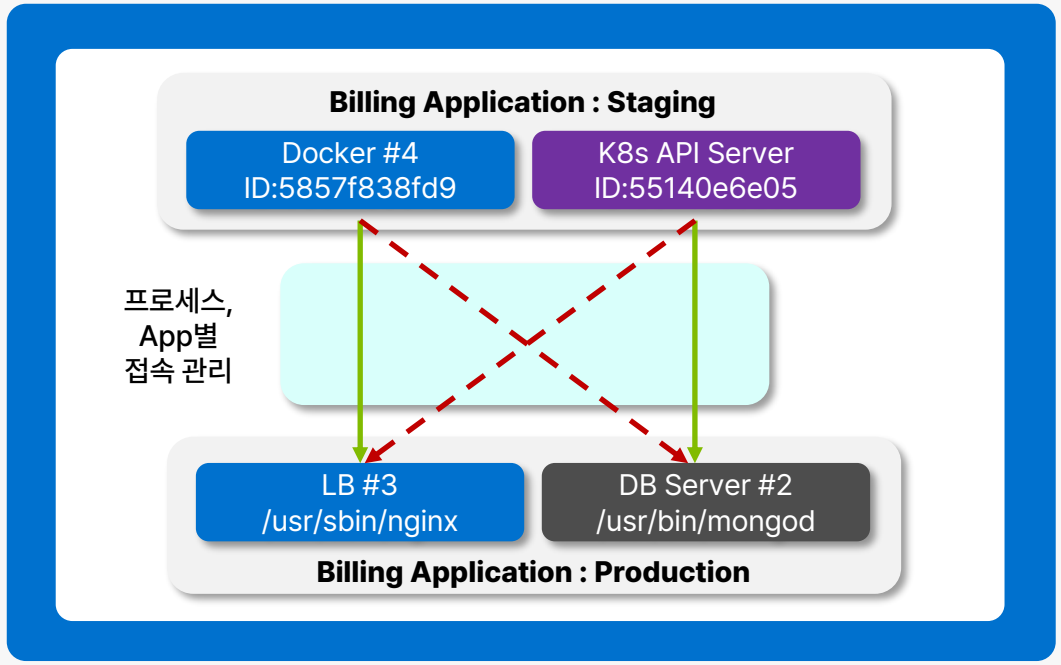


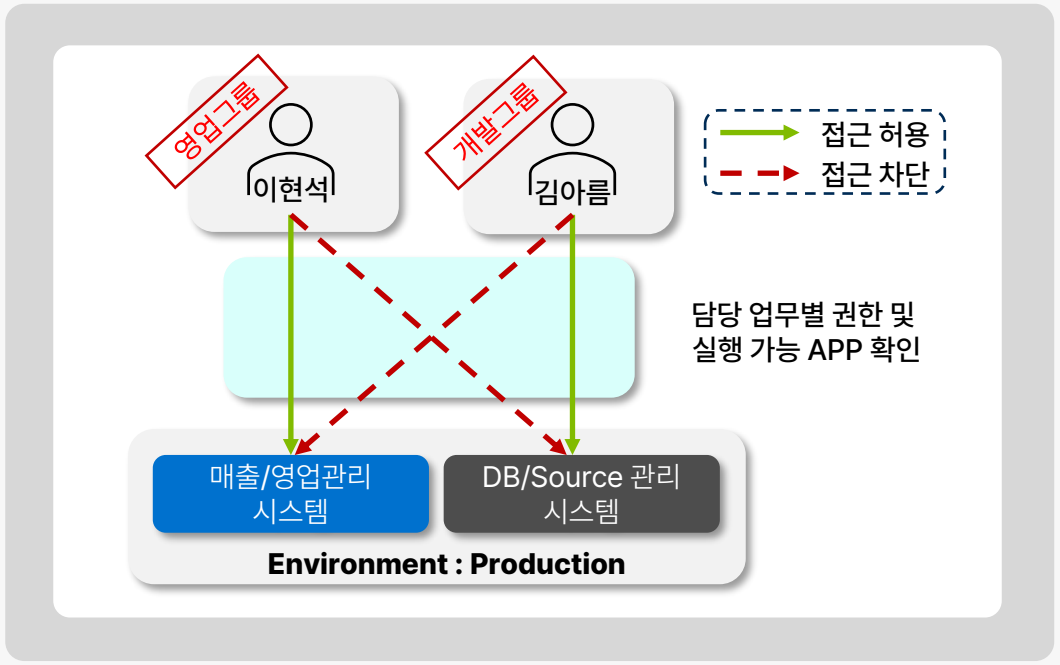
엔큐리티

Third-party 액세스 제어

비즈니스 요구사항에 따라 IT 리소스 액세스 엄격 관리

- **기능별 응용프로그램 보기** : 사용자 지정 가능한 시각적 맵에서 응용프로그램과 응용프로그램의 통신 상황 보기 가능
- **THIRD-PARTY 사용자 액세스 제어** : 사용자가 사용해야 하는 명확한 비즈니스 요구가 있는 애플리케이션에만 액세스할 수 있도록 제한
- **사용자 계정 오남용 탐지** : 허가되지 않은 계정 사용 시도가 발생할 때 적시에 경고 및 지원 정보 수신

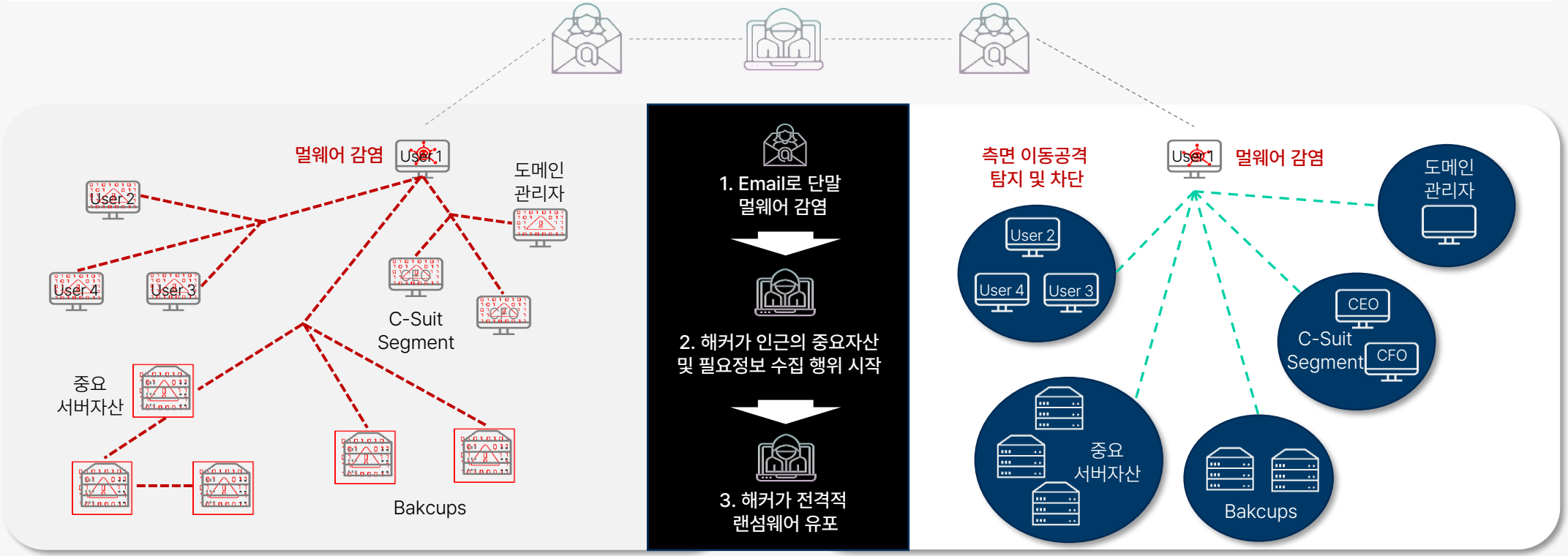




엔큐리티

측면이동 공격 탐지 사례

- ZERO-DAY 공격 특성상 실시간 랜섬웨어 100% 탐지 실질적 불가
- 감염된 단말 이동경로 최소화로 피해 규모 최소화 방안이 최선

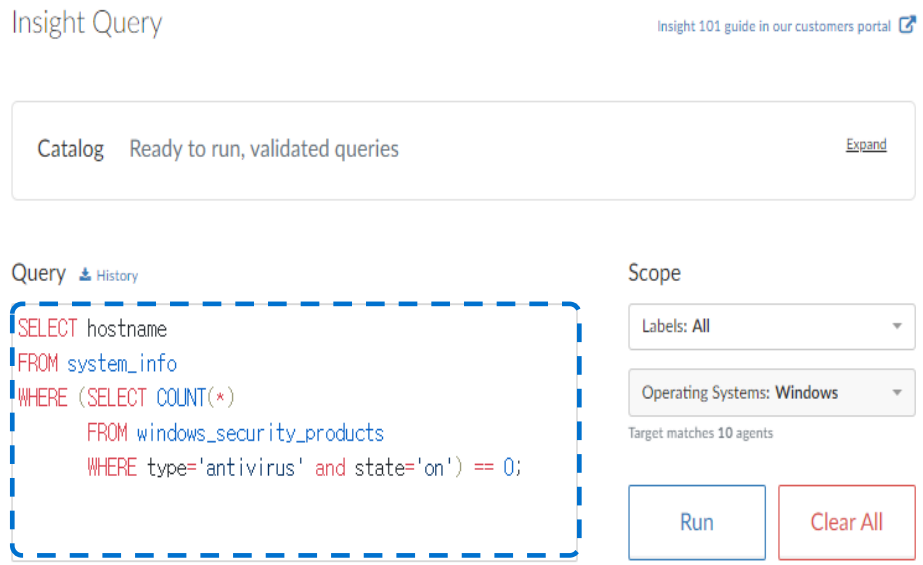


엔큐리티

감지

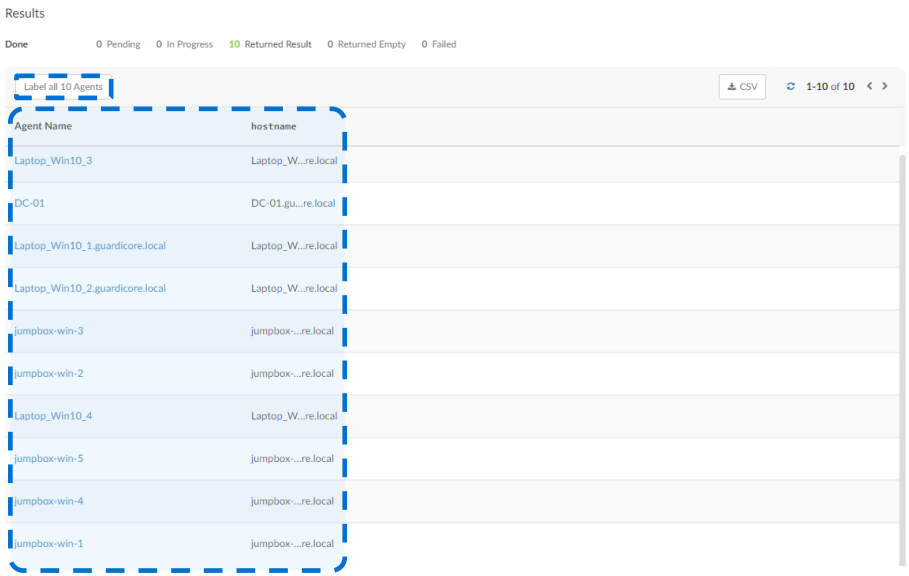
Insight Query 이용 취약점 대응(1)

Windows OS에서 네트워크 파일 공유를 위해 사용하는 보안 취약 프로토콜 SMBv1 사용 대상 확인 후, 차단 정책 생성/적용



취약 자산 검색

Insight Query(OS Query)기능을 활용해
Windows 자산에서 SMBv1프로토콜을 사용하는 자산 검색



Label 부여

조회된 자산에 대하여 라벨을 생성/부여
(ex. 취약점 : SMBv1)

엔큐리티

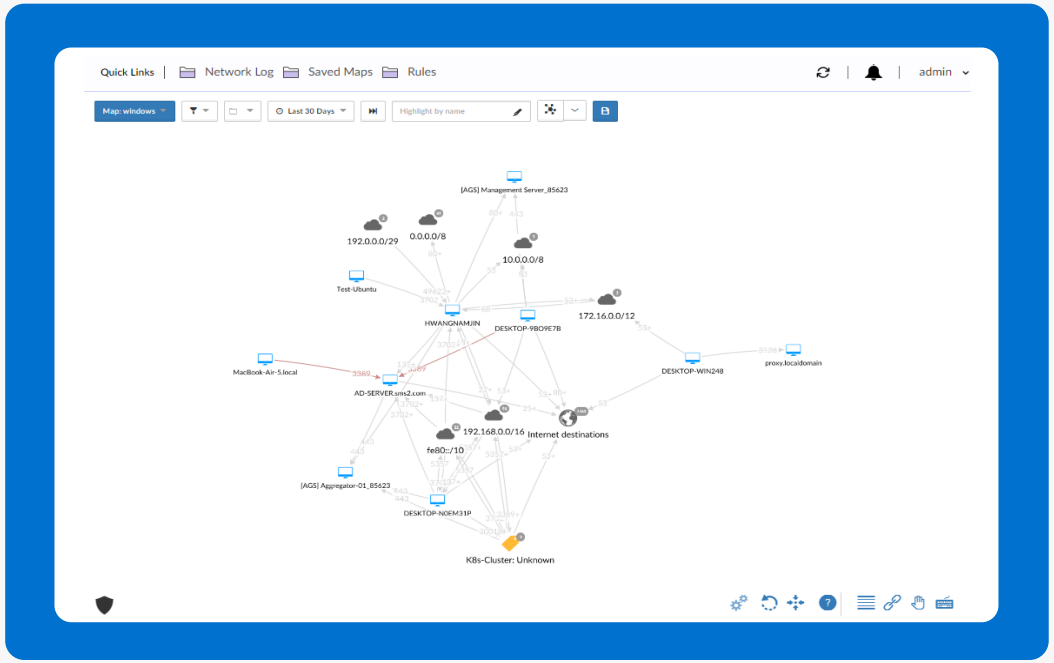
확인/평가

Insight Query 이용 취약점 대응(2)

Windows OS에서 네트워크 파일 공유를 위해 사용하는 보안 취약 프로토콜 SMBv1 사용 대상 확인 후, 차단 정책 생성/적용

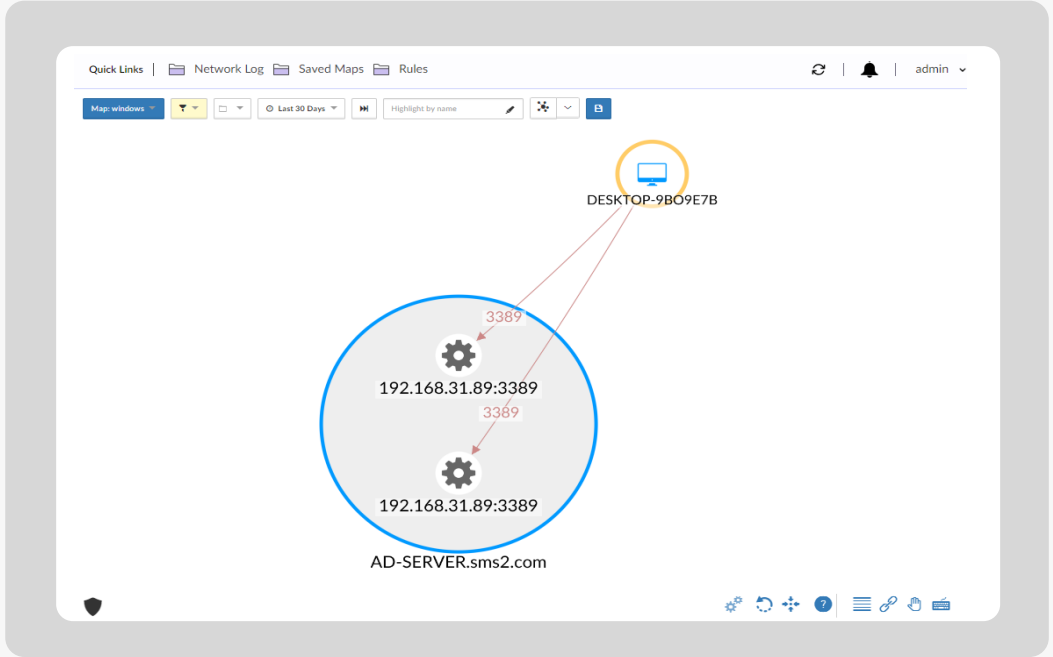
자산 정보 가시화

생성된 라벨을 기준으로 자산간의
네트워크 가시성 맵(REVEAL)을 생성



위험도 평가

자산간의 통신 상태, 프로세스,
통신 포트 확인 및 취약점 상태 평가

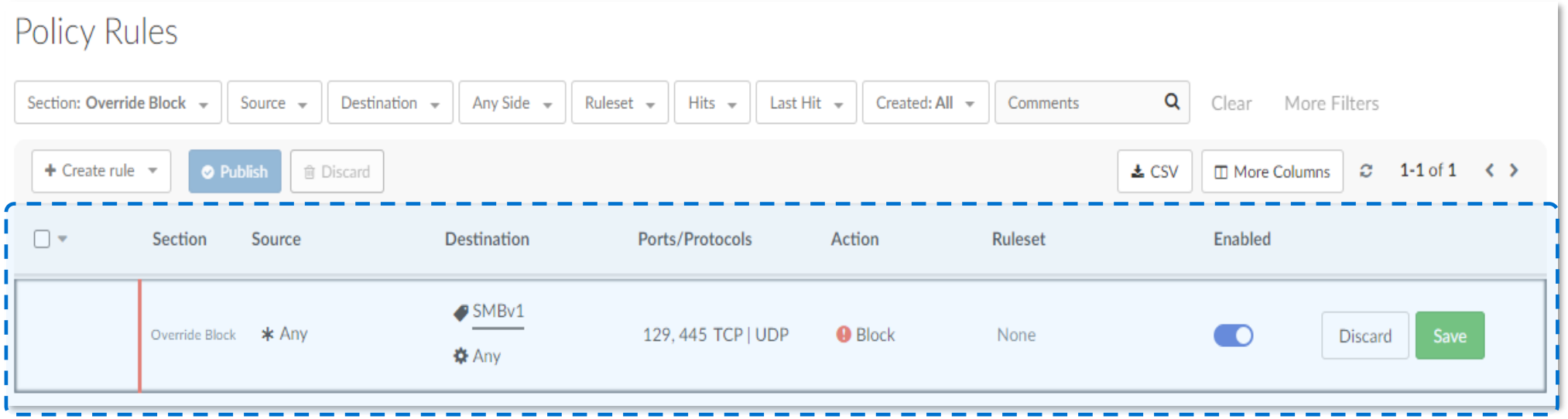


엔큐리티

보안정책 적용

Insight Query 이용 취약점 대응(3)

Windows OS에서 네트워크 파일 공유를 위해 사용하는 보안 취약 프로토콜 SMBv1 사용 대상 확인 후, 차단 정책 생성/적용



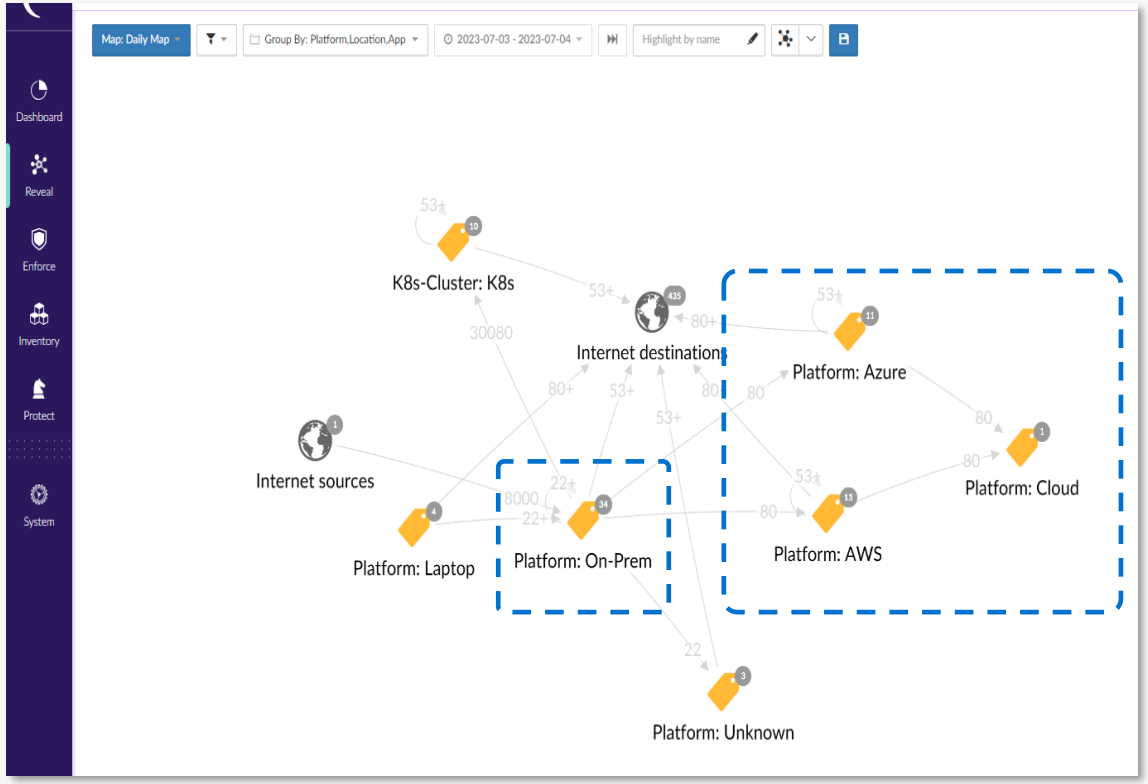
Result

생성한 라벨(취약점:SMBv1)을 사용하여 취약점이 발견 된 모든 자산에
SMB 연결을 완전히 차단하는 정책을 생성하여 취약점 제거

엔큐리티

하이브리드 보안환경과 **Micro Segmentation**

On-premise와 IaaS의 하이브리드 환경 지원



1. 하이브리드 환경(On-premise, IaaS등)을 위한 Micro Segmentation
   - 대시보드에서 하이브리드 클라우드 모니터링 가능

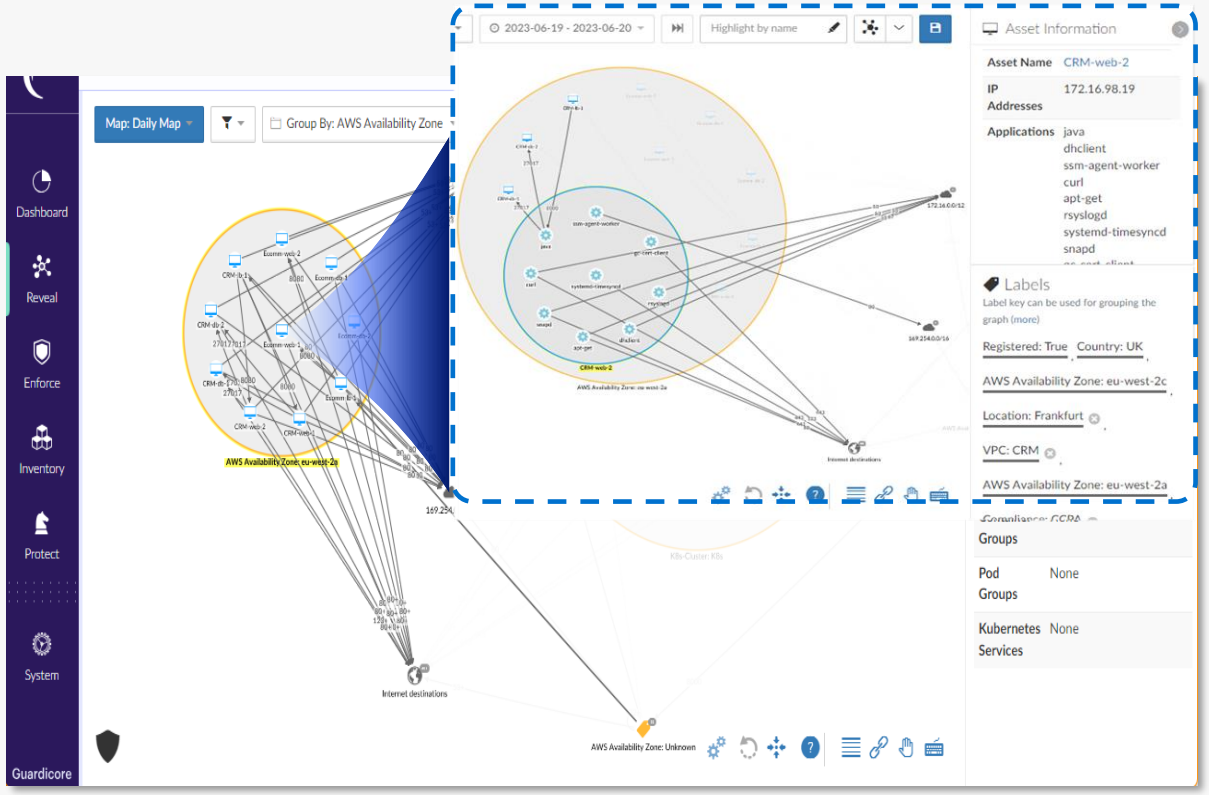
2. 세부적인 가시성
   - 프로세스 레벨까지 인스턴스 관련 가시성 추가

3. 통합 보안 정책 배포와 관리
   - 지역 및 VPC, 컨테이너, VM 및 사내에 걸친 단순한 마이크로 세분화 정책 On-premise 적용 가능

엔큐리티

AWS Micro Segmentation

AWS 클라우드 보안을 통한 공유 책임 모델 간소화



1. **완전히 통합된 AWS용 Micro Segmentation**
   - 대시보드에서 네이티브 클라우드 정보 및 AWS 관련 데이터 확인 가능

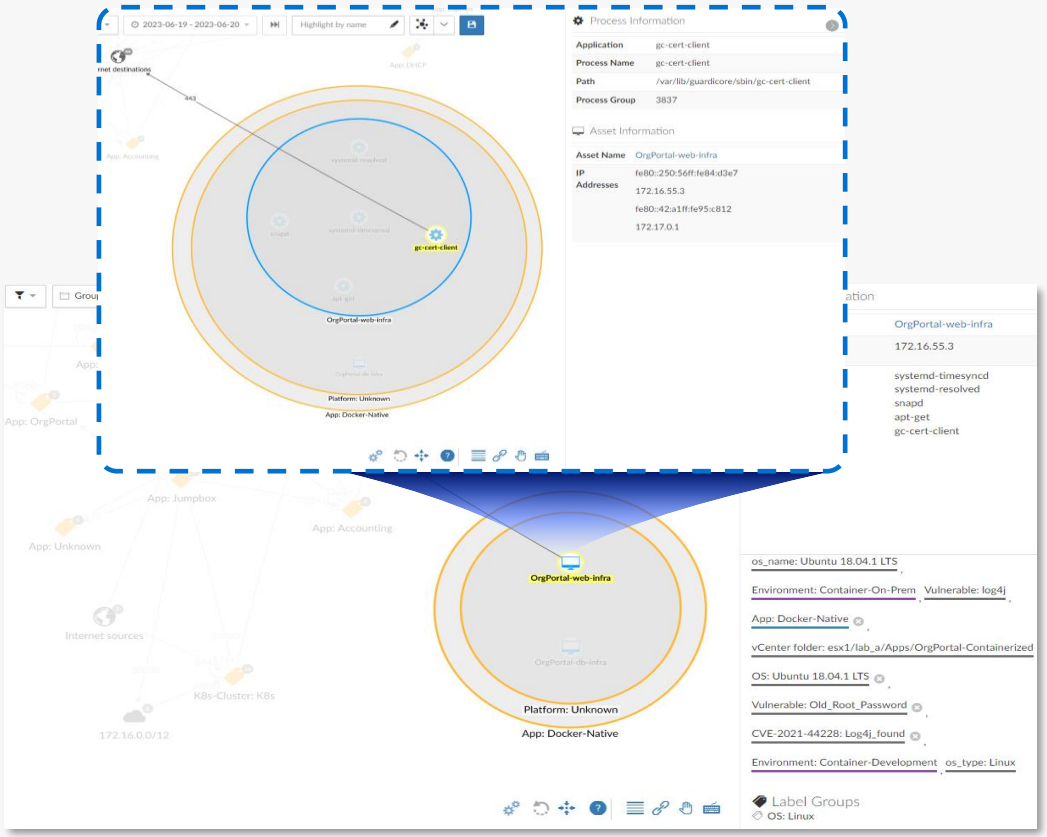
2. **세부적인 가시성**
   - 프로세스 레벨까지 인스턴스 가시성 추가

3. **AWS를 뛰어넘는 Micro Segmentation**
   - 지역 및 VPC, 컨테이너, VM 및 사내에 걸친 단순한 Micro Segmentation 정책 사용 가능

엔큐리티

컨테이너 보안

컨테이너형 애플리케이션을 위한 완벽하고 포괄적인 보안 솔루션



1. **가시성 확보**
   - 모든 포드 및 컨테이너 통신 흐름 검색

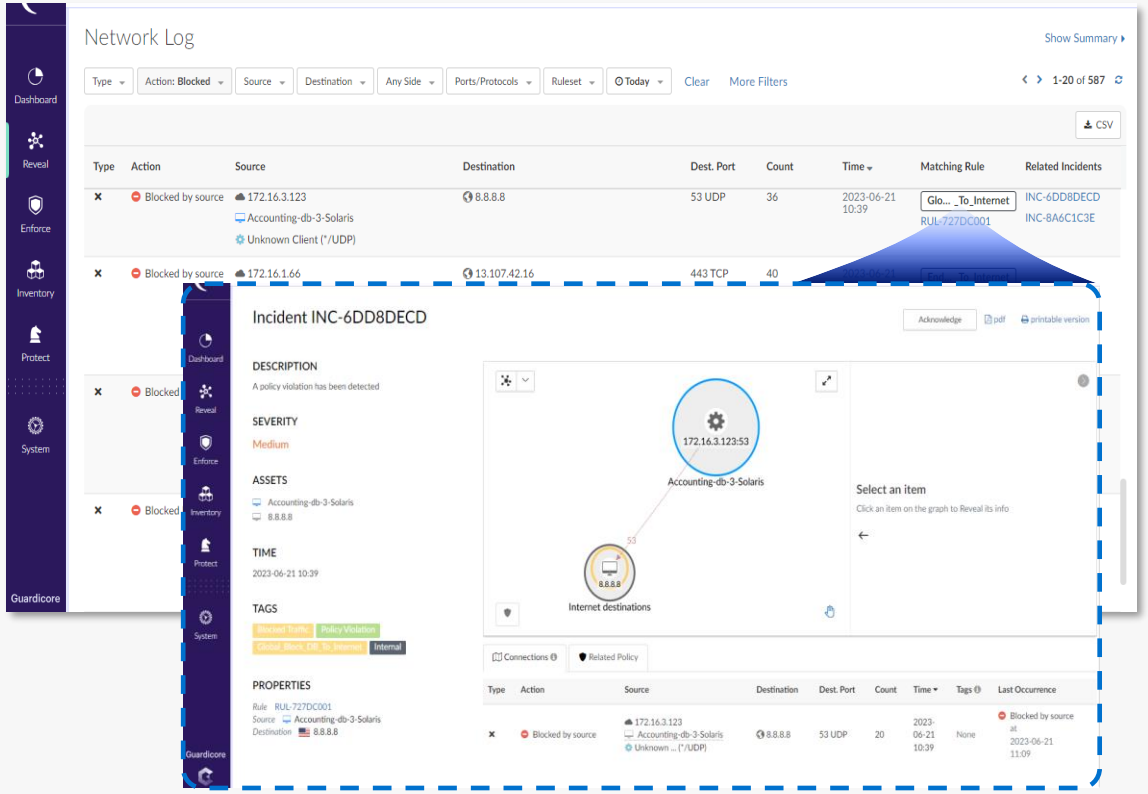
2. **세분화 정책 적용**
   - 보안 제어가 컨테이너와 함께 확장 및 마이그레이션 되도록 보장하는 기본 포드 레이블 기반

3. **컨테이너형 애플리케이션**
   - PCI에 민감한 워크로드 보호 및 규정 준수 입증

엔큐리티

위협 탐지 및 대응

인공지능으로 많은 위협 더 빨리 탐지



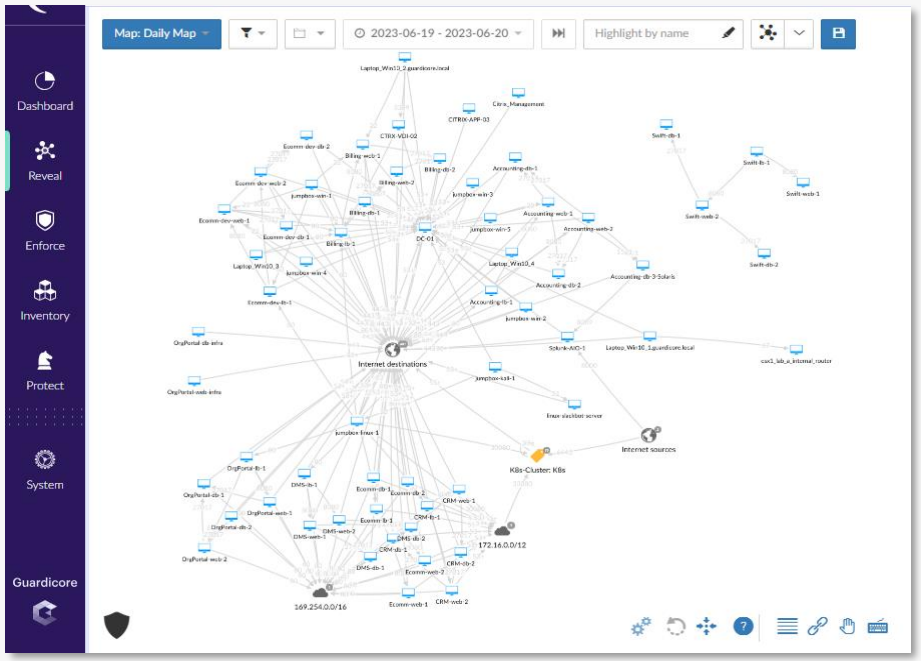
1. 다중 위협 탐지 방법
   - 모든 유형의 위협 해결
2. 위협 조사
   - 자동 분석 및 충실도가 높은 인시던트 데이터
3. 공격에 대응
   - 플랫폼 통합을 통해 사고 대응 가속화 및 완화 권장 사항 대응

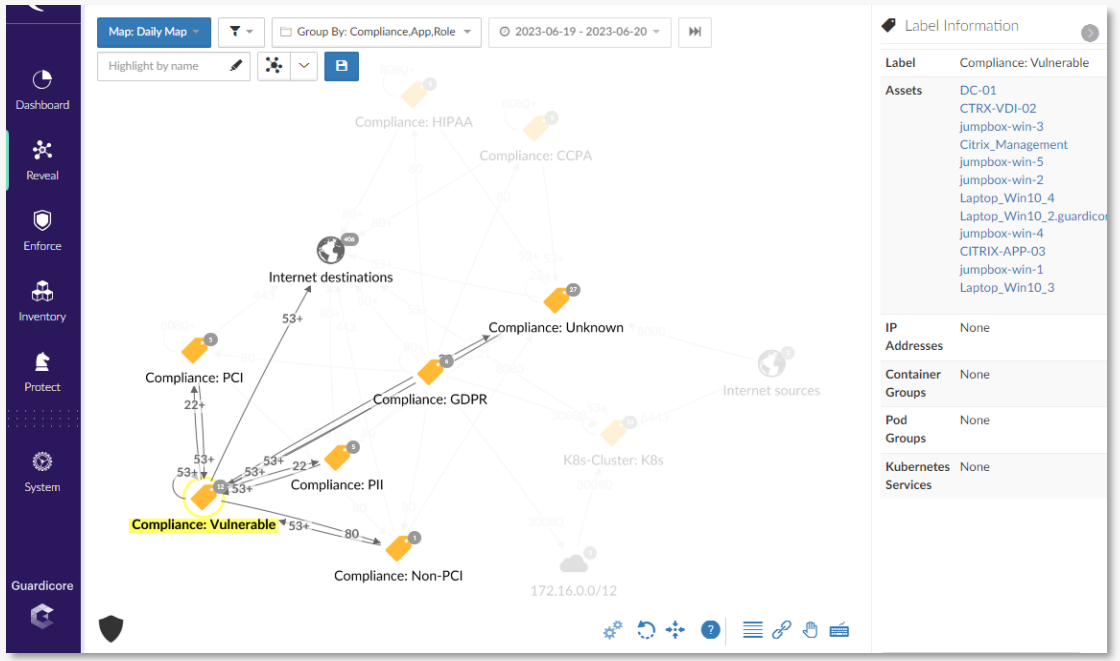
엔큐리티

세분화된 **Zero trust**

중요 애플리케이션을 규정(PCI-DSS, ISMS-P)에 맞게 보호

- **사용자 환경의 가시성** : 애플리케이션 검색 및 종속성 매핑을 통해 신뢰해야 하는 항목과 신뢰해서는 안되는 항목 차이 파악 가능
- **ZERO TRUST 적용** : 신속한 설계, 테스트 및 배포 정책 포함 원칙
- **모니터링** : 위협 인텔리전스, 경고 등을 사용해 네트워크 추적 및 모니터링





엔큐리티

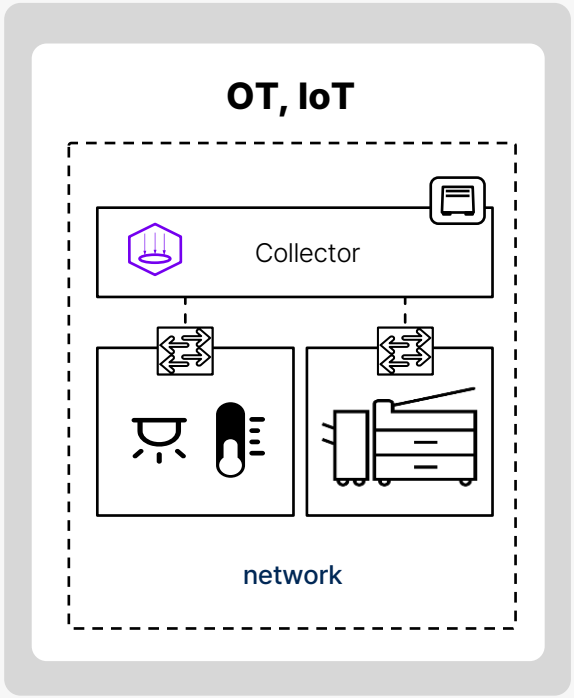
IoT/OT 장치에 대한 Zero trust

규모에 맞게 IoT/OT 장치 보호

- IOT 및 OT 장치를 보호하는 것은 오래 전부터 대부분 조직의 어려운 과제
- AGS를 통해 조직은 공격 영역 감소 및 호스트 기반 보안 소프트웨어를 실행할 수 없는 장치에 ZERO TRUST 정책 적용 가능

주요 기능

- 지속적인 장치 검색
- 로밍 장치 인식
- 통합 장치 지문 채취
- 심층 가시성
- 별도 Agent 설치 없이 Zero trust 세분화



1. **IT 인프라와 모든 IOT 및 OT 시스템 단일 뷰에서 검색, 시각화 및 매핑 가능**
   - 가치가 높은 시스템을 식별 및 세분화하여 침해 확산으로부터 보호 (타사 보안 도구 필요하지 않음)
2. **모든 장치에 고유한 지문 할당, 적절한 보안 정책 적용**
3. **공격이 발생 전 네트워크에 최소 권한 분할 정책 적용, 랜섬웨어 및 기타 악성 프로그램 공격 방지 및 억제**

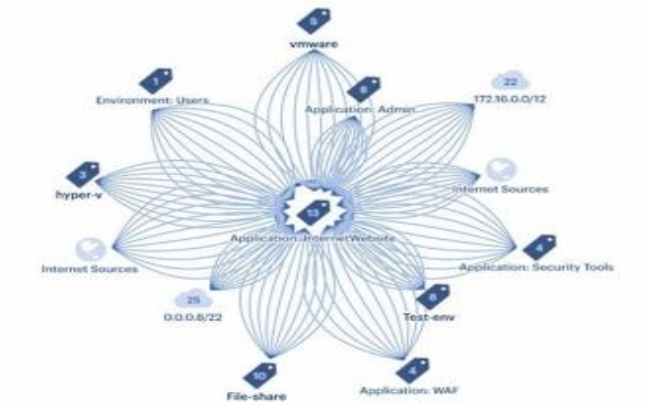
엔큐리티

해외고객 적용 사례

Chapter 06

Micro Segmentation 적용 사례

비즈니스 요구사항에 따라 IT 리소스 액세스 엄격 관리



Application InternetWebsite's attack surface
before segmentation

Application InternetWebsite's attack surface
after segmentation

Before : 350만개 내/외부 연결 확인

After : 120개 필수 연결 허용

Result

99.93% 공격표면 감소 기대효과

엔큐리티

디지털 중요 자산 보호

글로벌 제약회사

Global Pharmaceutical Company

1. 프로젝트 대상
   하이브리드 IT 환경 전반에서 가장 중요한 애플리케이션 보호

2. 프로젝트 범위
- 암묵적 신뢰에 기반한 네트워크 인프라 보안 문제 해결
- 새로운 IT 환경으로 인하여 증가하는 공격 표면 감소
- Active Directory 에 사용자 별 (임직원, 파트너 등) 세밀한 segmentation 정책 적용

Legacy Segmentation

- 지속적으로 변화하는 앱 종속성으로 인해 정적 VLAN 또는 방화벽 제어를 적용할 수 없음
- 네트워크 흐름과 앱 종속성에 대한 가시성 부족
- 측면 이동 위험이 높은 기존 디셉션 인텔리전스 부재

VLAN 구성에만
약 2년 소요 예상

Guardicore Impact

즉각적인 위험 감소, 신속한 배포

- 현재 중요한 앱 및 Active Directory 도메인 컨트롤러를 포함하여 10,000개 이상의 워크로드를 보호
- 앱 종속성 및 연결 범위의 빠르고 정확한 검색
- 완전한 East-West Traffic가시성
- 고급 위협 탐지 및 분석을 위한 디셉션 인텔리전스 구축
- 애플리케이션 다운타임이 없어 구현 및 유지 관리 비용을 절감

엔큐리티

Ransomware 공격 탐지/방어

A US Manufacturer

a fire equipment manufacturer

1. 프로젝트 대상
   전사적으로 Micro-segmentation 확산 적용

2. 프로젝트 범위
- Ransomware 사고 이후 CEO 의 지시사항 이행
- 기존에 이미 GC가 적용하고 있는 3,200 개의 Legacy System 이외의 전사적으로 확대 적용 (VM Workload 포함 10,000 대로 확대)

Legacy Segmentation

- 150개 application이 올라간 legacy 시스템 (대략 3,200 workload)에만 Guardicore을 활용해 Segmentation 적용 중
- 2023년 9월 Ransomware Attack 당하였고 Guardicore에서 보호하고 있는 시스템 외에 피해 발생

$51 Million to get 27 TB back

Guardicore Impact

잠재 보안 침해 사고에 대응

- IT 운영 및 보안사고 대응 효율성의 획기적인 개선
- 무단 측면 이동을 방지하고 침해 감지, 식별 및 완화를 개선하여 침해의 잠재적 비용의 감소
- 이원화 되어 있었던 segmentation 관리 방식의 일원화 및 효율화
- 애플리케이션 다운타임이나 기존 네트워크 구성에 변화 없이 구현

엔큐리티

사이버 위험 감소 목표

유럽 철도 운영 기업

VTG

1. 프로젝트 대상
   랜섬웨어와 같은 실질적 침해에 대한 위험 감소

2. 프로젝트 범위
- 72개 물리적 위치
- 650개의 물리적 서버 및 클라우드 워크로드
- 클라이언트 인스턴스 2,000개
- 70개의 Kubernetes instance

Legacy Segmentation

- VLAN 사용 중 확장성 및 유연성 떨어짐
- 원격 위치의 인프라에 대한 잦은 변경으로 VLAN으로 변경 관리 불가능
- 호스트 기반 방화벽은 네트워크 흐름에 대한 의미 있는 가시성을 제공하지 못함

수작업으로 네트워크를 세분화하는 것은 리소스와 시간이 매우 많이 소요

Guardicore Impact

구축 기간 : 총 6개월

- 단계적 배포 접근 방식, 650에서 시작해서 지금까지 2,200개의 에이전트 배포
- 차단된 작업에 대한 자세한 보기를 통해 네트워크 흐름에 대한 상황 별 이해를 통한 막대한 부가가치 제공
- 멀티 인프라 On-prem, Cloud, VDI, Kubernetes 등 지원
- 구축 과정 중 Ransomware 공격 확인 및 차단 (TEI 분석* 기준 연간 $600K 정도의 침해 방지 효과 확인)

엔큐리티

규정 준수 간소화 및 가속화

Deustsche Bank

Deutsche Bank

1. 프로젝트 대상
   개발/테스트/운영 환경의 분리

2. 프로젝트 범위
- 운영 및 비운영 환경 간의 트래픽 제한
- 애플리케이션에 대한 Ring-Fencing 준비

Legacy Segmentation

- 매우 느린 진행
- 감사 실패, 벌금 및 비즈니스 오류
- 애플리케이션 다운타임 시간으로 인한 비즈니스 중단

VLAN 구성에만
약 2년 소요 예상

Guardicore Impact

구축 기간 : 총 6개월

- 10,000 개의 규정 준수가 불필요한 자산(Non-Production)을 분리
- 애플리케이션 다운타임 불필요
- 10배 더 빠른 구현으로 규정 준수 비용의 절감
- DevOps 프로세스와의 통합으로 수작업 감소

사이버 위험 감소 목표

글로벌 정유 회사

Multinational Oil & Gas Giant

1. 프로젝트 대상
   "Colonial Pipeline"*과 같은 공격 방지, 보다 세분화된 네트워크 세그먼트 구현

2. 프로젝트 범위
- Segmentation Tier 0 + 1 애플리케이션 수준 구현 (예 : SAP)
- 클라우드 VM, 온프레미스 레거시 머신, 컨테이너 혼합 환경에 대한 일관된 Segmentation 구현

Legacy Segmentation

- 네트워크팀이 방화벽과 VLAN을 사용하여 구현 시도
- 이 방식으로 네트워크를 원하는 수준까지 세분화하는 것은 불가능하다고 판단
- 중요한 애플리케이션이 취약한 상태로 방치됨

연간 수백만 달러 상당의 피해 예상

Guardicore Impact

No network changes
No app downtime

- 1단계 구축을 위해 온-프레미스 및 퍼블릭 클라우드에서 1,000여 개의 자산 보호
- 레거시 OS 지원
- 더 쉬운 자산 라벨링 시스템
- 추가적인 위협 방지를 사용자 단말기로의 확대 및 DNS 평판 기반 접속 방지 서비스 확대 고려
- 향후 계획을 위한 모델 : 제로 트러스트 네트워크 프레임워크 확립

엔큐리티

규정 준수 및 확장성

Major US Carrier

Giant US Telecommunications

1. 프로젝트 대상
   보안 태세 격차 (Security Posture Gap) 우려 및 PCI 규정 만족 필요

2. 프로젝트 범위
- 개정된 PCI Compliance의 만족을 위한 Micro-segmentation 필요
- Hybrid Cloud 환경에 걸쳐 있는 200K 이상의 서버로의 확장 기반 마련

Legacy Segmentation

- 기존 방화벽과 VLAN을 사용하여 구현 시도하였으나 실패

✓ 2021년부터 2년 동안 Micro-segmentation 검토

- 너무 많은 벤더의 솔루션이 도입되어 있어 일관된 가시성 및 정책 관리 불가능

Micro-Segmentation 필요성 확신

Guardicore Impact

200K 이상의 Workload에 대한 확장성

- 보안 아키텍처 및 관리를 단순화 및 PCI규정* 준수와 관련된 비용을 절감
- IT 운영 및 보안사고 대응 효율성 획기적인 개선
- 무단 측면 이동을 방지하고 침해 감지 / 식별 및 완화를 개선하여 침해의 잠재적 비용의 감소
- 기 사용 중이던 Akamai의 다른 솔루션과의 시너지 및 관리 효율성 증대

Compliance 만족

Global Retail 회사

Global Retailer

1. 프로젝트 대상
   30개 이상의 PCI-DSS을 만족해야 하는 application

2. 프로젝트 범위
- PCI와 Non-PCI 어플리케이션 간의 분리
- 전사적 보안 통제에 대한 일관성 가시성 및 통제
- Multi-Cloud 지원

Legacy Segmentation

- Compliance 만족에 위배되는 위험요소 파악에 한계
- OpenStack, VMware, Azure, Oracle Cloud 등 다양한 환경에 걸친 일관된 보안 통제 곤란

VLAN 구성에만
약 2년 소요 예상

Guardicore Impact

Multi 및 Hybrid Cloud 환경에
일관된 지원

- 30여 개의 PCI Compliance 가 요구되는 어플리케이션에 대한 Ring-Fence 정책 적용
- 5개의 분리 보안 정책 엔진 1개로 통일
- PCI와 관련된 Network Traffic에 대한 real & historic 가시성의 확보
- DevOps 절차와 통합
- 위협 및 침해 대응 서비스와 통합을 통한 보안 서비스 질 향상

엔큐리티

Cloud로 안전하게 Migration

의류 매장 체인

A chain of retail clothing stores

1. 프로젝트 대상
   SaaS 서비스를 OCI로 Migration

2. 프로젝트 범위
- SaaS 애플리케이션의 단계적 Migration
- Hybrid 서비스에서 tenant 분리
- 규제 대상 애플리케이션 (특히 PCI)의 규정 준수 기반 Migration

Cloud Migration

- Cloud Migration에 대한 가시성 부재
- Hybrid Cloud 환경에서 보안 제어를 관리하기 곤란

Cloud Migration의 서비스 연속성 보장 곤란

Guardicore Impact

안전한 Cloud 로의 이관

- 애플리케이션 종속성 매핑 및 Migration에 대한 완전한 가시성
- On-prem에서 설정되고 Migration 중에 유지/관리되는 정책 집합
- Hybrid 환경에서 Migration 중에 관리하는 동일한 도구

엔큐리티

환자 데이터 및 의료 기기 액세스 보호

헬스 케어

US Healthcare Provider

1. 프로젝트 대상
   중요한 애플리케이션 (환자데이터, 결제) 보호

2. 프로젝트 범위
- 6,000대 서버에서 생성된 traffic에 대한 가시성 확보
- 의료기기 IoT 에서 서버로의 Access 제한
- 중요 애플리케이션에 Ring-Fencing 적용

Legacy Segmentation

- FW을 사용하여 의료기기 IoT을 데이터센터 트래픽과 분리 시도
- Azure 환경 분리를 위한 Cloud-Native Control 방식 활용
- Segment 되지 않은 네트워크에서 실행되는 아웃소싱 IT

보안정책을 생성하고
검증할 수 있는 가시성 부재

Guardicore Impact

완전한 트래픽 가시성

- 클라우드 마이그레이션을 위한 애플리케이션의 종속성 매핑
- 중요한 애플리케이션에 대한 Ring-Fencing
- 의료기기 IoT에 대한 Access Control
- Azure 환경에 대한 보안은 가시성 및 검색 제어를 통해 유효성 검사

컴플라이언스 준수 및 N/W 가시성 확보

OCBC 은행 (싱가폴)

OCBC Bank

1. 코어 뱅킹 시스템 및 어플리케이션 세그멘테이션 필요
2. 싱가폴 로컬 뱅킹 regulation MAS-644 컴플라이언스 지원 필요
3. 조직 내 대외 서비스에 필요한 중요 코어 시스템 위험 제거 및 워크로드 보호 필요

Legacy Segmentation

- 클라우드 및 하이브리드 환경 상에서 전사 네트워크 가시성 매우 떨어짐
- 내부 감사 결과, 컴플라이언스 점수 및 레벨 점검결과 저조
- 확장성이 떨어져 공격표면 증가

VLAN 구성에만
약 2년 소요 예상

Guardicore Impact

구축 기간 : 총 9개월
수행 인원 : 아키텍트 1명

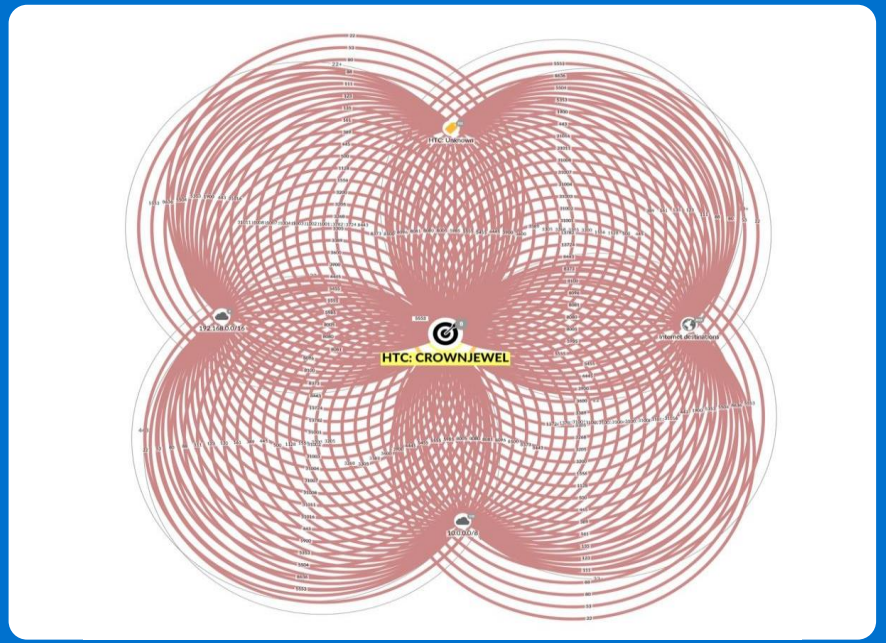
- 75개 코어 뱅킹 시스템 및 애플리케이션 Micro Segmentation 적용
  - ✓ 워크로드 보호 및 접근제어 정책
- Zero trust 기반의 인증 정책
  - ✓ 8개의 중요 사용자 그룹 및 권한 지정
- 클라우드, On-Premise, 단말 네트워크 트래픽 및 자산 정보(L4-L7)확보
  - ✓ 상관관계 분석, 불필요 연결 및 차단 정책 확인
  - ✓ 전사 트래픽 실시간 모니터링 및 트래킹
- 기가몬 스위치와 연동, 비 Agent 영역 (OT, IoT)까지

엔큐리티

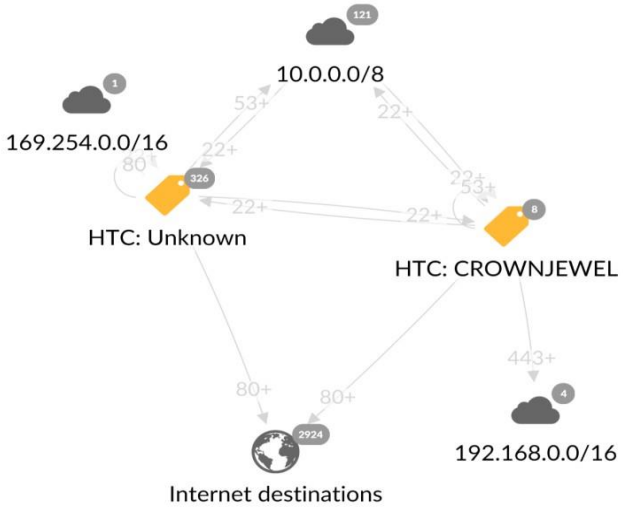
N/W 가시성 확보를 통한 공격표면 감소

북미 IT서비스 회사

7,076,278개의 네트워크 연결이
무분별하고 광범위하게 허용되어 실제 통신 중



Micro Segmentation 정책 적용 후,
13,563개의 필수 네트워크 연결



엔큐리티

구간 방화벽, **VLAN** 대체

유럽 최대 IT 서비스 회사

Guardicore 최대 고객사

- 총 6개월 프로젝트에 3명의 전문 아키텍트 참여
- 기존 HW 기반 세그먼테이션 VLAN 구성 총 2년 소요 예상, Guardicore SW 방식으로 프로젝트 전환
- 약 10,000개의 자산 Micro Segmentation 적용
- 제로 어플리케이션 다운타임 기록 (무 장애 서비스 보장)
- 기존 HW 기반 세그먼테이션보다 10배 이상 빠른 구축 및 운영 체감 (시간과 비용절감 효과)

주요 고객사

FINANCIAL SERVICES

UBS, TD Bank, OCBC Bank, Santander, Deutsche Bank, MetLife, CaixaBank, kotak Kotak Mahindra Bank, ICICI Bank, HDFC BANK

COMMERCIAL & SERVICES

Campbell's, teleflora, UNITE STUDENTS, CIRCLE K, Staples, Tom LANGE, GAP, PEOPLES

TELECOM

Telefónica, MBNL, Globe, BT

INSURANCE

UNIVERSAL PROPERTY & CASUALTY INSURANCE COMPANY, BFL CANADA

HEALTHCARE & PHARMA

Intermountain Healthcare, NOVARTIS, BlueCross BlueShield, NATIONAL INSTITUTES OF HEALTH, BECKMAN COULTER, ARA DIAGNOSTIC IMAGING, DIAMOND, Fondation Cognacq-Jay

LEGAL

Davis Polk, EVERSHEDS SUTHERLAND, Dickie McCamey ATTORNEYS AT LAW, Hogan Lovells

TECH

NVIDIA, magic leap, ORACLE, WiX, KEYSIGHT TECHNOLOGIES

엔큐리티

Demo

Thank you

sales@ncurity.com | +82 70-7308-9288 | ncurity.com