illumio

일루미오 플랫폼 소개
Breach Containment 시작

침해를 가정한 보안, 공격 확산을 멈추는 새로운 기준 Zero Trust Segmentation!

일루미오 코리아

2026년 4월

일루미오 회사 소개

글로벌 기업이 선택한 제로 트러스트 세그멘테이션 리더 기업

일루미오 Zero Trust Segmentation으로 공격 범위를 'Contain'하여 피해를 최소화합니다

투자 및 설립

2013년 설립

총 5억 8,300만 달러($583M) 투자 유치
Andreessen Horowitz, Franklin Templeton, Thoma Bravo 등 글로벌 최상위 투자사들의 지원

일루미오 본사
920 De Guigne Drive Sunnyvale, CA 94085

보호 현황

Fortune 100 기업 중
20개 개 기업 보호

4천만+ 워크로드 보호
Fortune 100 대기업부터 중소기업까지, 다양한 규모의 조직을 위한 보호

시장 리더십

Gartner: Microsegmentation Market Guide에서 **시장 인지도와 검증된 대표 벤더(Representative Vendor)**로 선정

Forrester: New Wave for Microsegmentation에서 **Leader**로 평가

Gartner Peer Insights.
4.8 ★★★★★
90% recommend Illumio based on 126 validated reviews

주요 고객사

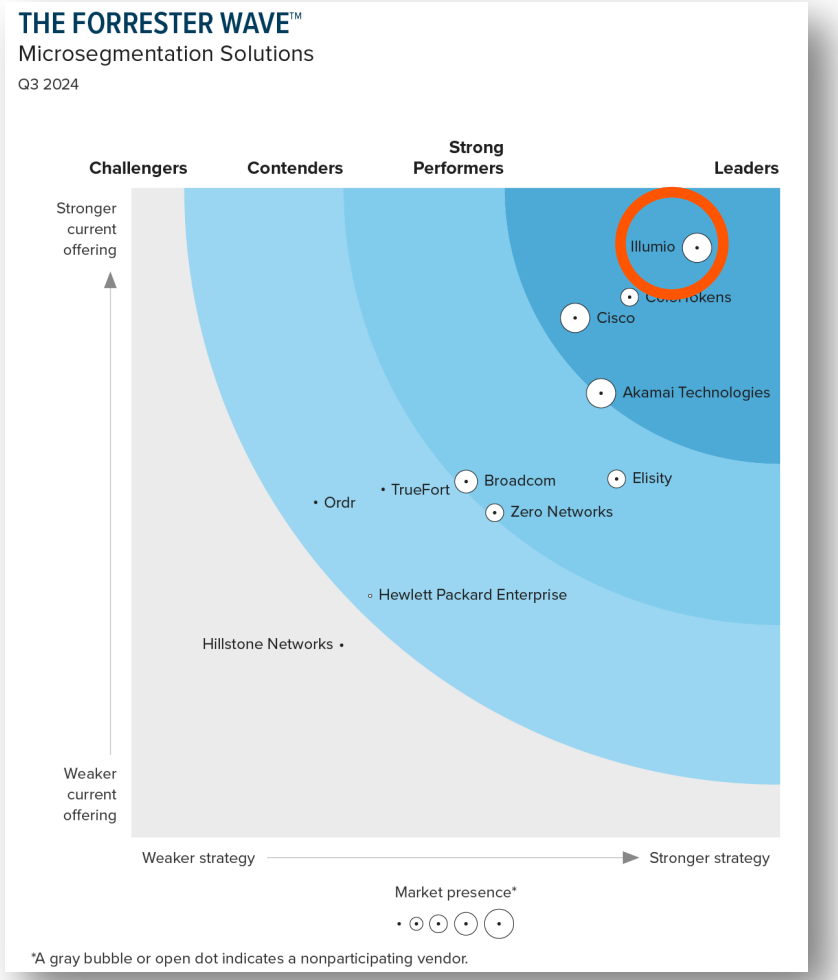
Microsoft citibank HSBC
Ingredion BNP PARIBAS BlueCross BlueShield
BT CATHAY PACIFIC DocuSign
Morgan Stanley ORACLE QBE
WELLS FARGO salesforce servicenow Alaska AIRLINES
FDIC BNP PARIBAS Principal BROOKS

Illumio, Forrester Wave™ Leader 선정

Forrester Wave™에서 Illumio를 마이크로세그멘테이션 Leader로 선정(Q3 2024)

외부 평가로 증명된 시장 리더십

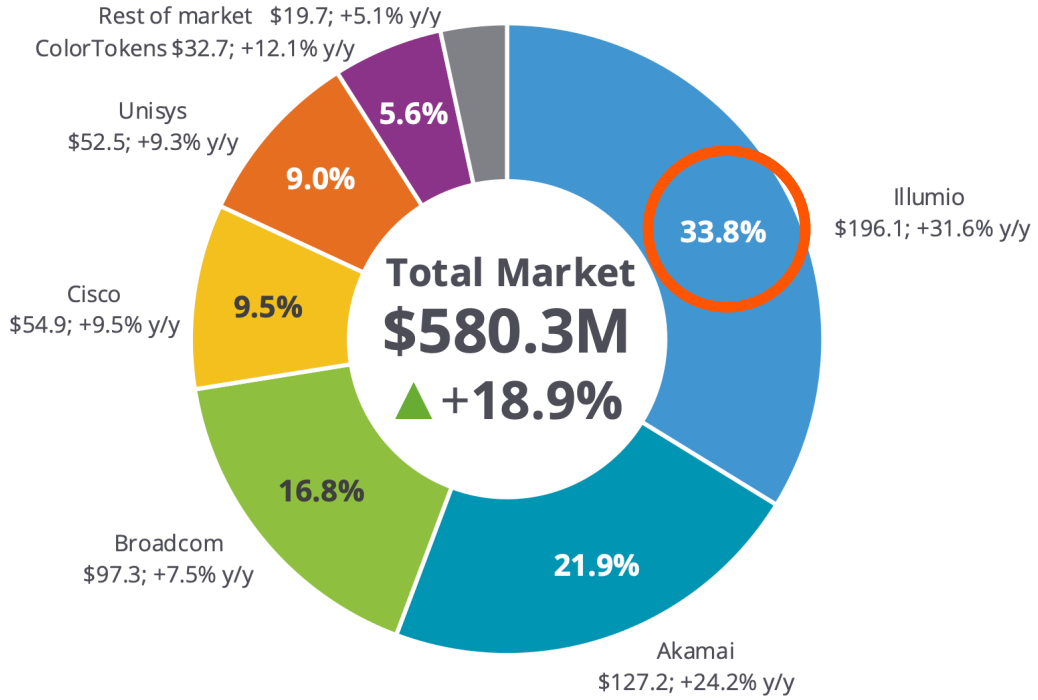
FORRESTER®
WAVE
LEADER 2024
Microsegmentation Solutions



Illumio, 외부 리서치로 입증된 마이크로세그멘테이션 시장 리더

IDC 기준, Illumio는 2024년 글로벌 점유율 **33.8%**로 1위, 가장 빠르게 성장하는 선도 벤더

Worldwide Microsegmentation 2024 Share Snapshot



Note: 2024 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2025

Worldwide Microsegmentation Revenue by Vendor, 2023 and 2024

	2023		2024		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2023–2024 Growth (%)
Illumio	149.0	30.5	196.1	33.8	31.6
Akamai	102.4	21.0	127.2	21.9	24.2
Broadcom	90.5	18.5	97.3	16.8	7.5
Cisco	50.2	10.3	54.9	9.5	9.5
Unisys	48.0	9.8	52.5	9.0	9.3
ColorTokens	29.2	6.0	32.7	5.6	12.1
Other	18.7	3.8	19.7	3.4	5.1
Total	488.0	100.0	580.3	100.0	18.9

Source: IDC, 2025

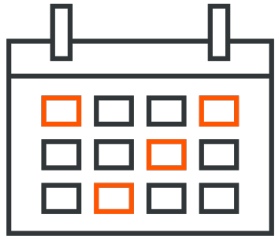
일루미오 플랫폼 소개

보안 동향: 사이버 공격의 비용 증가 및 복구 시간은 장기화

평균 비용은 상승하고, 대응에는 시간이 오래 걸리며, 운영 중단과 손실은 커지고 있습니다

$4.88M USD

2024년 데이터 침해 1건당
전 세계 평균 비용
전년 대비 10% 증가,
역대 최고 수준



277 Days

침해를 식별하고
격리(Containment)하는데
걸리는 평균 기간

25%

악성 공격의 25%는
시스템 운영을 중단시킴

$2.22M USD

침해 탐지 및 예방(Detection & Prevention) 전략을 사용하는 조직이 그렇지 않은 조직 대비 얻는 평균 비용 절감 효과

Source: IBM Cost of a Data Breach Report 2023 & 2024

보안 트렌드 변화: 보안의 관점이 어떻게 바뀌고 있는가?

침해를 막는 것(Stop Breaches)'에서 '침해가 발생해도 비즈니스 재앙을 막는 것(Stop Disasters)'으로 진화

"

SRM(Security & Risk Management) 리더들은
사이버보안을 '예방 중심 사고방식'에서 **'회복탄력성(resilience) 중심'**으로 전환하고 있다.

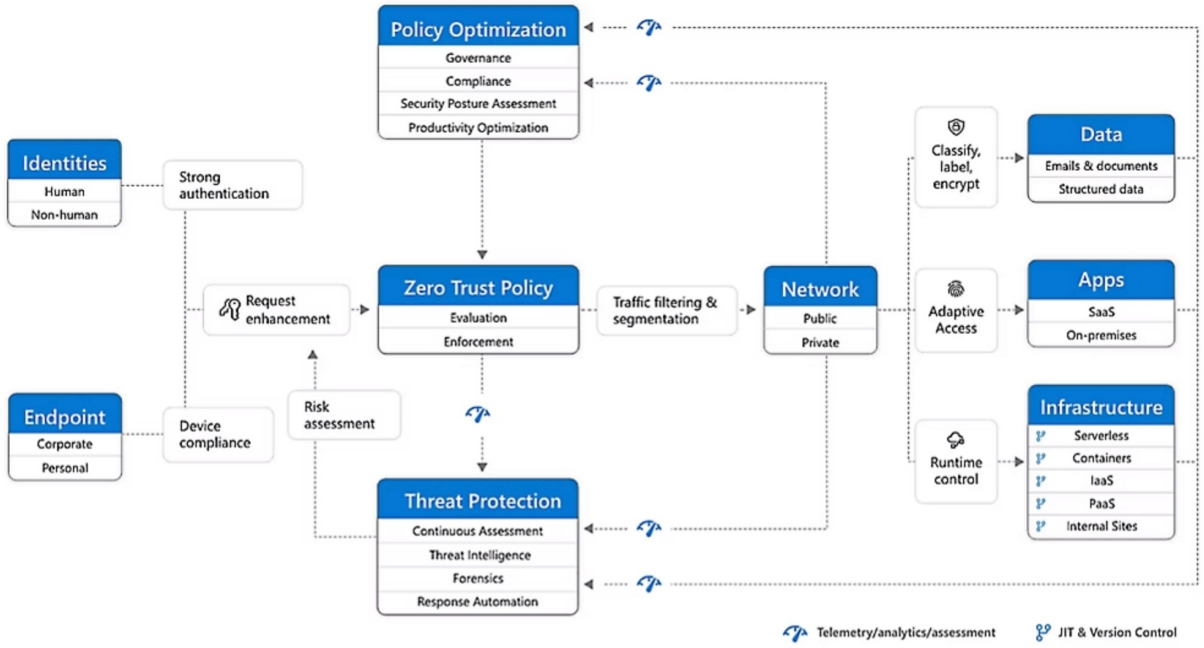
사이버 회복탄력성은 **'만약(if)'이 아니라 '언제(when)' 발생하느냐는 인식을 전제**로 하며, **완전한 예방이라는 잘못된 개념에 집착하기보다는 사이버 인시던트가 기업에 미치는 영향을 최소화**하고 조직의 적응 능력을 강화하는 데 초점을 둔다.

"

Gartner®

Source: "Cybersecurity Trends: Resilience Through Transformation" https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

제로 트러스트 보안 3가지 핵심 원칙



[마이크로소프트 제로 트러스트 보안]

1 명확한 검증
Verify Explicitly

모든 사용자, 장치, 애플리케이션, 데이터 흐름에 대해
명시적이고 엄격한 인증 및 권한 부여를 수행

2 최소 권한 액세스
Least Privilege Access

사용자와 시스템에 필요한 최소한의 권한만 부여하고,
필요한 시간 동안만 접근을 허용
(Just-in-Time 및 Just-Enough-Access)

3 침해 가정
Assume Breach

네트워크 내외부 어디든 공격이 있을 수 있다고 가정하고
보안 체계를 설계하고
마이크로 세그멘테이션(Micro-segmentation)을 통해 네트워크를 분할하고, 엔드-투-엔드 암호화를 적용하며,
위협 탐지 및 대응(EDR, SIEM) 체계를 강화하여 공격의
확산 방지

Source: 마이크로소프트 제로 트러스트란? https://learn.microsoft.com/ko-kr/security/zero-trust/zero-trust-overview

침해를 가정하라 – 확산 통제로 비즈니스 재앙 예방

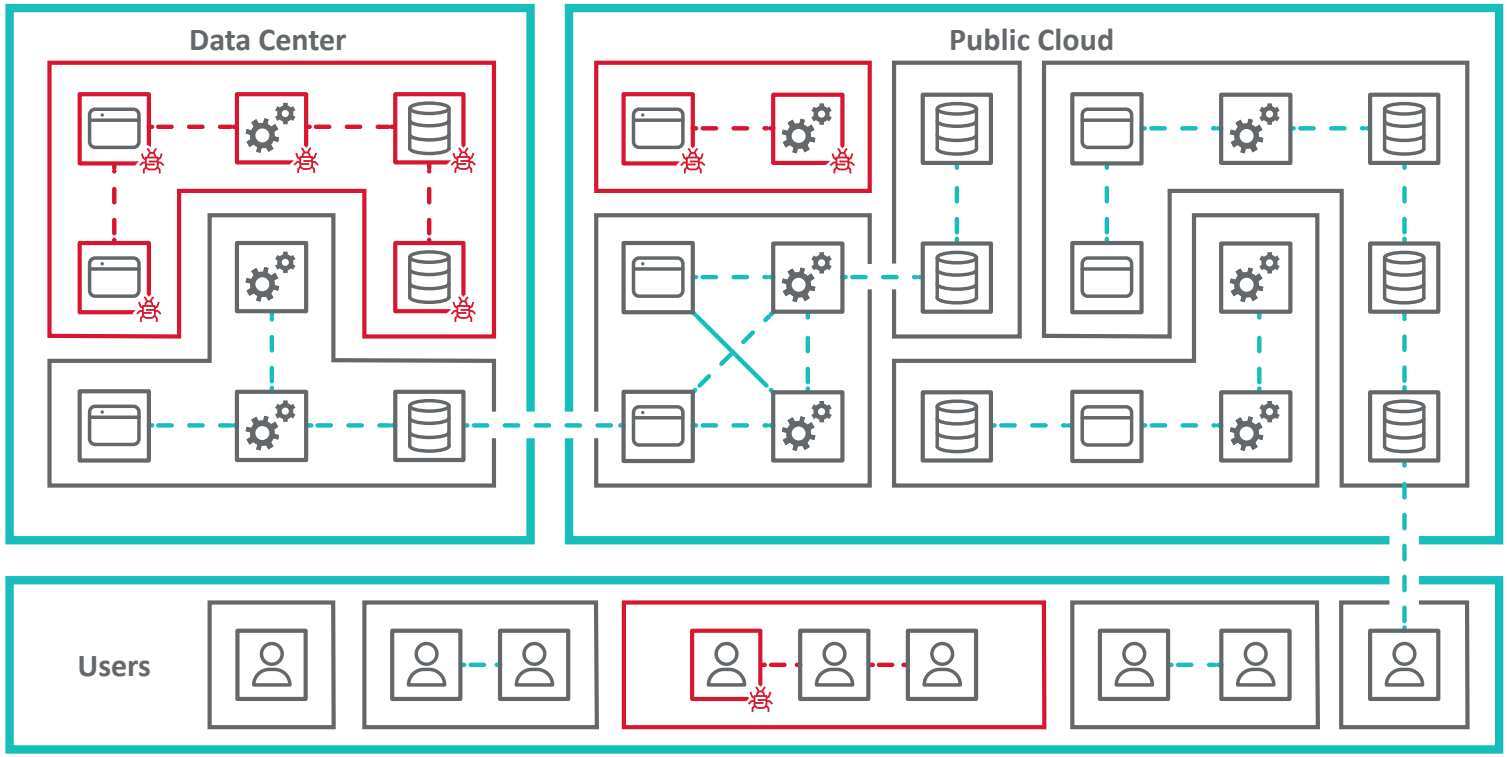
가시화(Map)와 정책(Intelligent Policy)으로 공격의 이동 경로를 차단합니다

실행 프레임워크 (Identify → See → Contain)

1. Identify Asset: Asset Inventory
- 전 자산을 식별하고 **표준화된 레이블(Label) 정책**을 적용
- 예: Environment/Location/APP/Role 기준으로 일관된 분류

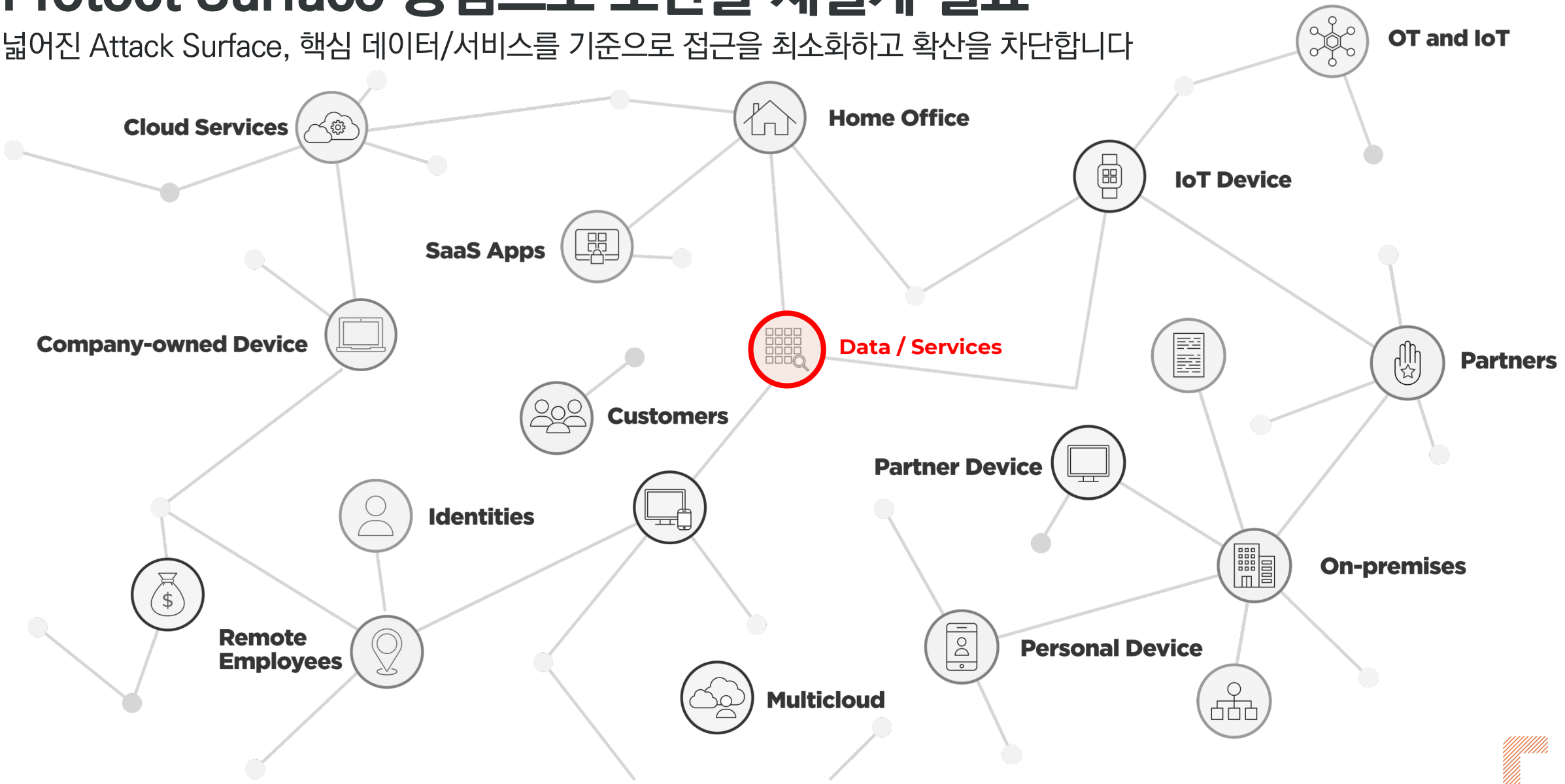
2. See Risk: Map
- 데이터센터/클라우드 전반의 **모든 통신을 시각화**
- 실제 연결 관계를 기반으로 **리스크 경로와 불필요한 통신**을 식별

3. Contain Risk: Intelligent Policy
- 중요 자산 중심으로 **필요한 통신만 허용**(Allowlist)
- 나머지는 차단/제한하여 **공격 확산을 자동으로 격리**
- 결과: 핵심 서비스 보호 + 운영 중단 리스크 최소화



Protect Surface 중심으로 보안을 재설계 필요

넓어진 Attack Surface, 핵심 데이터/서비스를 기준으로 접근을 최소화하고 확산을 차단합니다

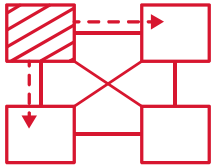


MITRE ATT&CK 관점: 공격 성공의 핵심은 Lateral Movement

Illumio Zero Trust Segmentation은 횡이동 경로를 차단해 공격 킬체인을 끊습니다

예방과 탐지 실패함

- 탐지되지 않은 비인가 침투
- 공격자는 수개월 동안 숨어 지냄(장기 잠복, dwell time)



공격이 확산됨

- Lateral movement를 통해 공격자가 네트워크 전반에 접근 가능
- 세그멘테이션이 없는 일반 네트워크는 방어가 취약함

핵심 자산이 침해됨

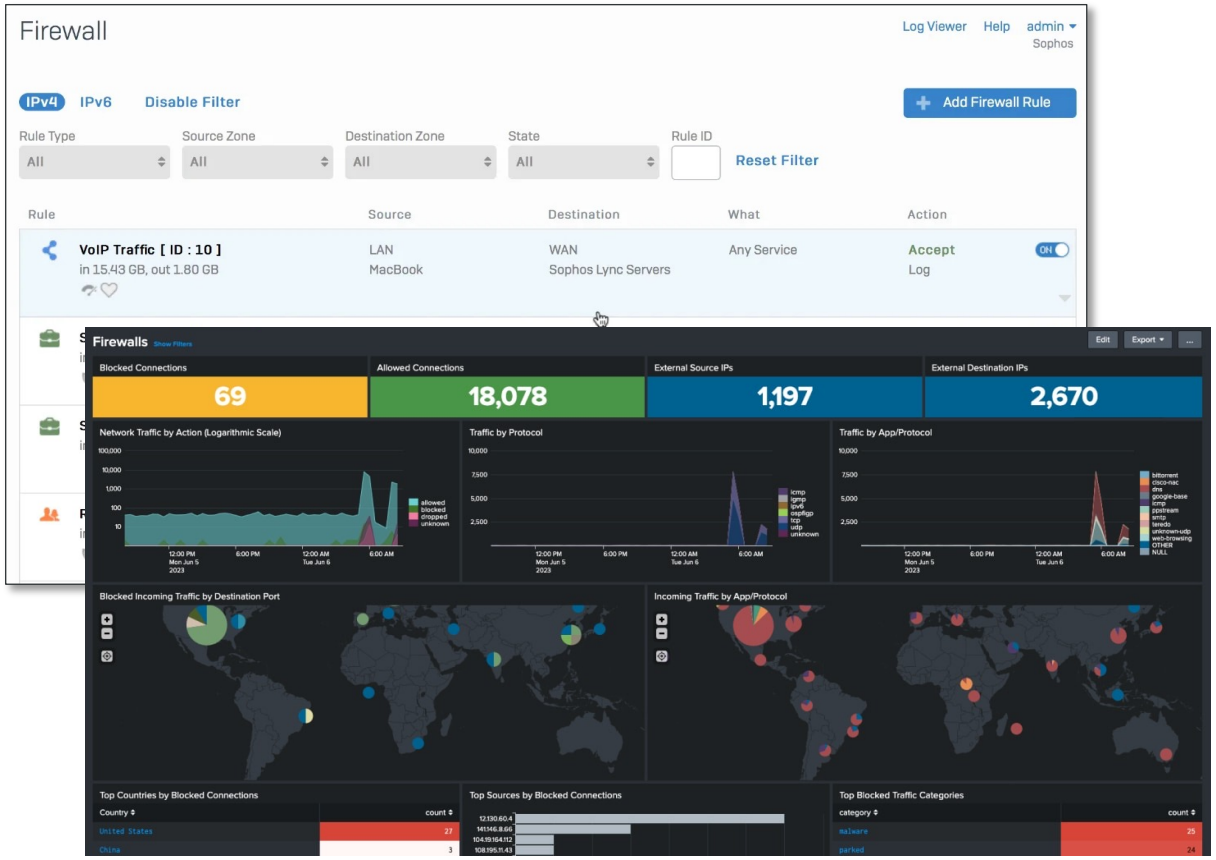
- 악성코드가 시스템을 암호화하고 금전을 요구 (랜섬웨어)
- 데이터 유출 및 규제 위반 리스크

1) 워크로드 간 통신을 “필요한 것만 허용(Allowlist)”
2) 관리 프로토콜/불필요 포트의 동서 트래픽을 최소화
3) 핵심 자산(Crown Jewels) 주변에 강력한 분리(Containment) 적용

리스트에서 그래프로: 공격 경로를 한눈에 보는 보안 운영

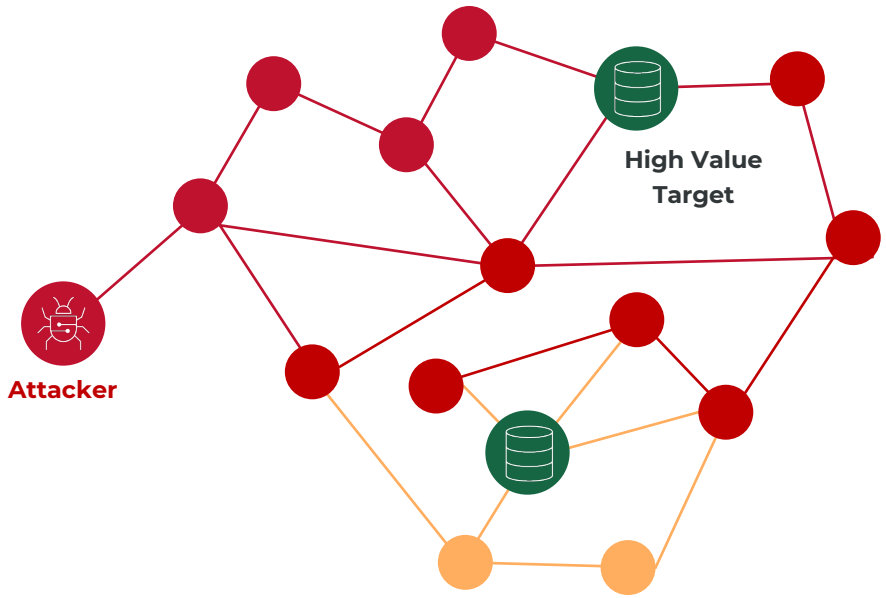
llumio는 그래프 기반 가시성으로 공격 경로를 한눈에 보여주고, 보안 운영 효율을 높입니다

리스트/로그 중심 보안 운영



See Risk: Map (그래프 기반 가시성)

- 실제 환경에서 발생하는 모든 통신을 맵으로 시각화
- 어떤 경로가 위험한지, 어떤 통신이 불필요한지를 한눈에 확인



NOW: Containment Era: Stop Cyber Disasters

Illumio ZTS Platform으로 침해 확산을 차단하고 핵심 자산을 보호합니다

침해 확산 차단(Breach Containment)을 위한 최초의 플랫폼

1

리스크를 이해(가시화)

워크로드, 디바이스, 인터넷 사이에서 발생하는 모든 통신과 트래픽(알려진/알려지지 않은)을 시각화

2

보안 통제를 정의

변경이 발생할 때마다 정밀한 세그멘테이션 정책을 자동으로 설정하여, 불필요하거나 원치 않는 통신을 통제

3

공격을 격리(확산 차단)

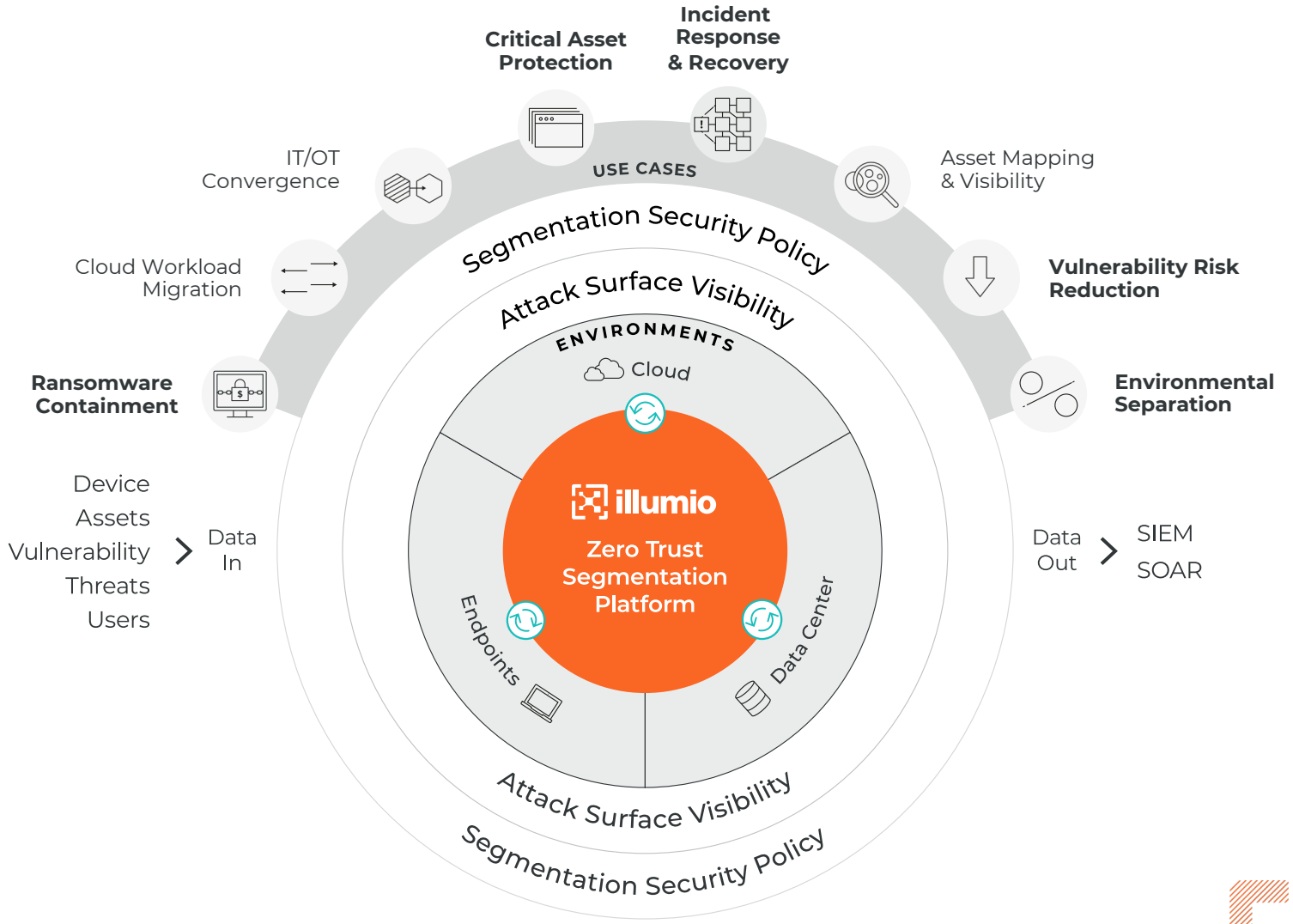
중요 핵심 자산을 사전에 격리하거나, 공격 진행 중 침해된 시스템을 즉시 격리하여 침해 확산을 차단

NOW: Containment Era: 일루미로 ZTS 플랫폼

Illumio Zero Trust Segmentation으로 침해 확산을 차단하고 핵심 자산을 보호합니다

하나의 플랫폼으로 Breach Containment를 위한 새로운 표준

- 랜섬웨어 확산 차단
- 핵심 자산 보호(Crown Jewels)
- 환경 분리(DC/Cloud/OT)
- 자산 맵핑 & 가시성
- 취약점 리스크 감소
- IR/Recovery 및 SIEM·SOAR 연계

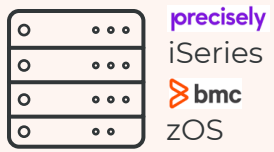


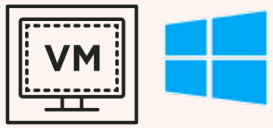
Illumio 아키텍처: 빠르고, 심플하며, 확장 가능

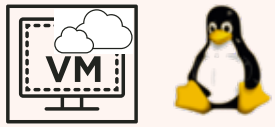
워크로드 트래픽 가시화 → 레이블 정책 기반 정책 계산 → 엔드포인트에서 일관된 집행

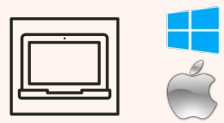
ILLUMIO ZTS PLATFORM

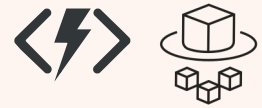
Mainframe / Midrange | Physical servers | Virtual data center / IaaS | Endpoint | Containerized | Cloud native/ IaaS











Network modules

Stateful host firewall

Containerized VEN

Agentless cloud security controls

User Space 기반 경량 에이전트로 안전한 세그멘테이션 구현

커널 인라인이 아닌 Out-of-band 방식으로 OS 기본 방화벽을 제어해, 성능·안정성·확장성을 확보

핵심설계: User Space + OS Built-in Firewall

- User Space**에서 동작**: 커널 인라인 모듈/네트워크 어댑터 방식이 아님
- Out-of-band **정책 적용**: 트래픽 경로에 직접 개입하지 않음(Not inline)
- OS Stateful Firewall **활용**: Linux iptables/nftables, Windows WFP 등 기본 방화벽에 정책을 프로그래밍

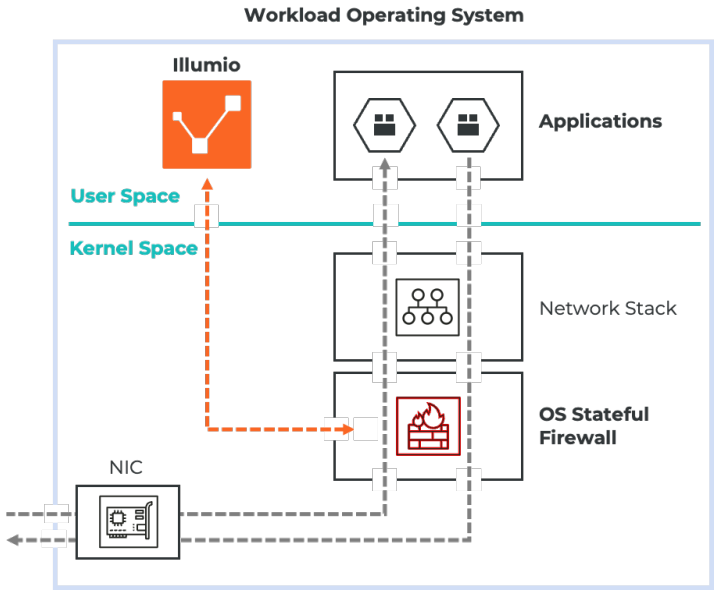
안정성(Fail-safe) & 호환성

- 에이전트 장애/재시작 시에도 적용된 **방화벽 규칙은 유지**(서비스 영향 최소화)
- 서드파티 방화벽/보안 솔루션과 **충돌/간섭 없음**(OS 보안 스택 기반)
- 커널 레벨 드라이버/필터 삽입 대비 리스크 없음

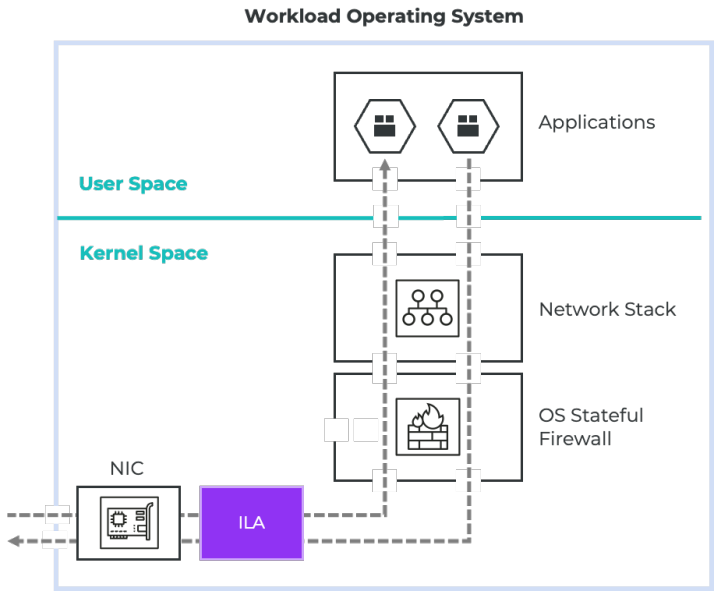
경량화(Performance-friendly) & 확장성

- 트래픽 인라인 처리/패킷 프록시 구조가 아니라 오버헤드가 낮음
- 변경이 많은 하이브리드 환경에서도 정책 배포/운영이 단순
- 대규모 워크로드에서도 일관된 정책 집행(확장성)

[일루미오 최적화된 경량 에이전트]

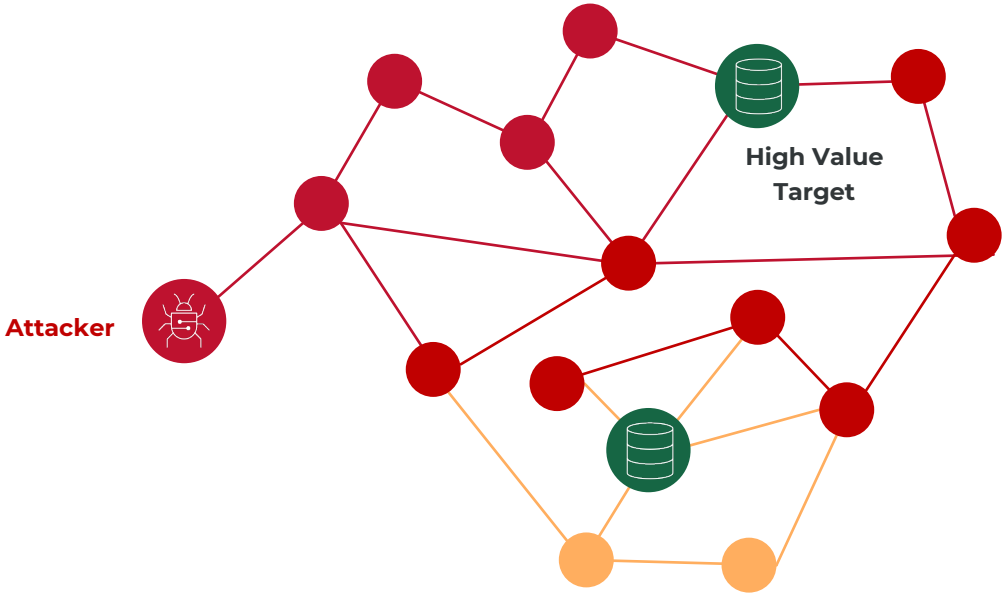


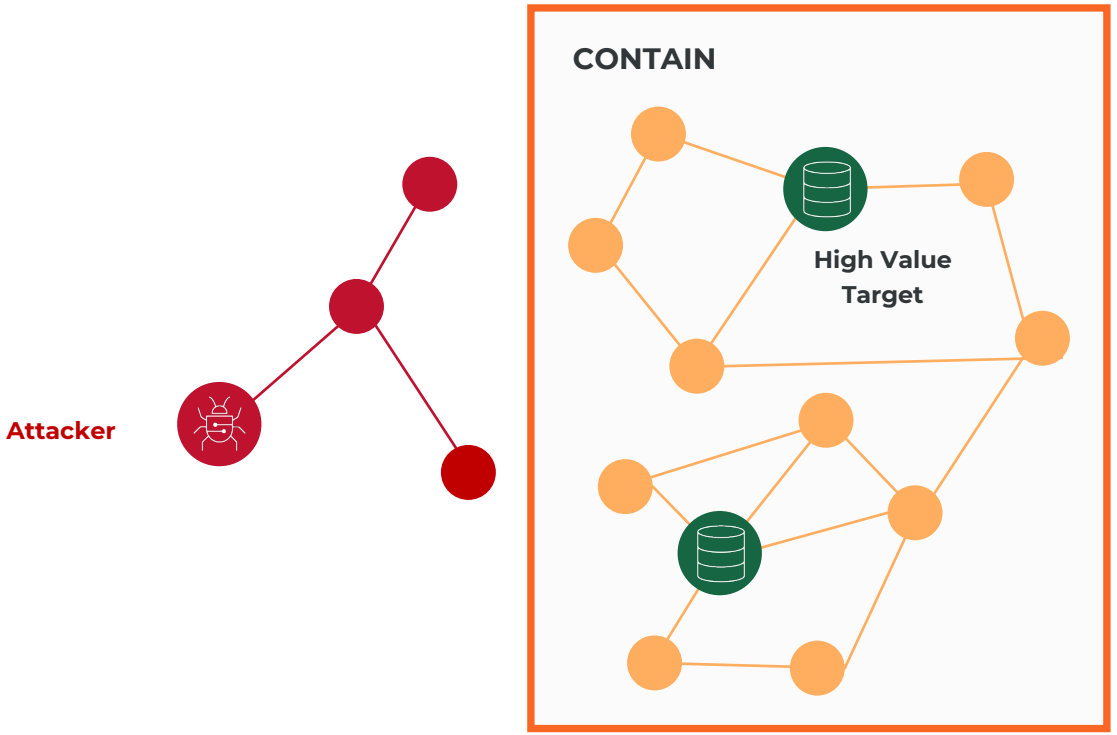
[타사 커널 인라인 동작 구조]



일루미로 Breach Containment 플랫폼

AI Security Graph 기반 Insights로 빠르게 탐지하고, Segmentation으로 공격을 즉시 Contain해 복원력을 강화





IDENTIFY / DETECT

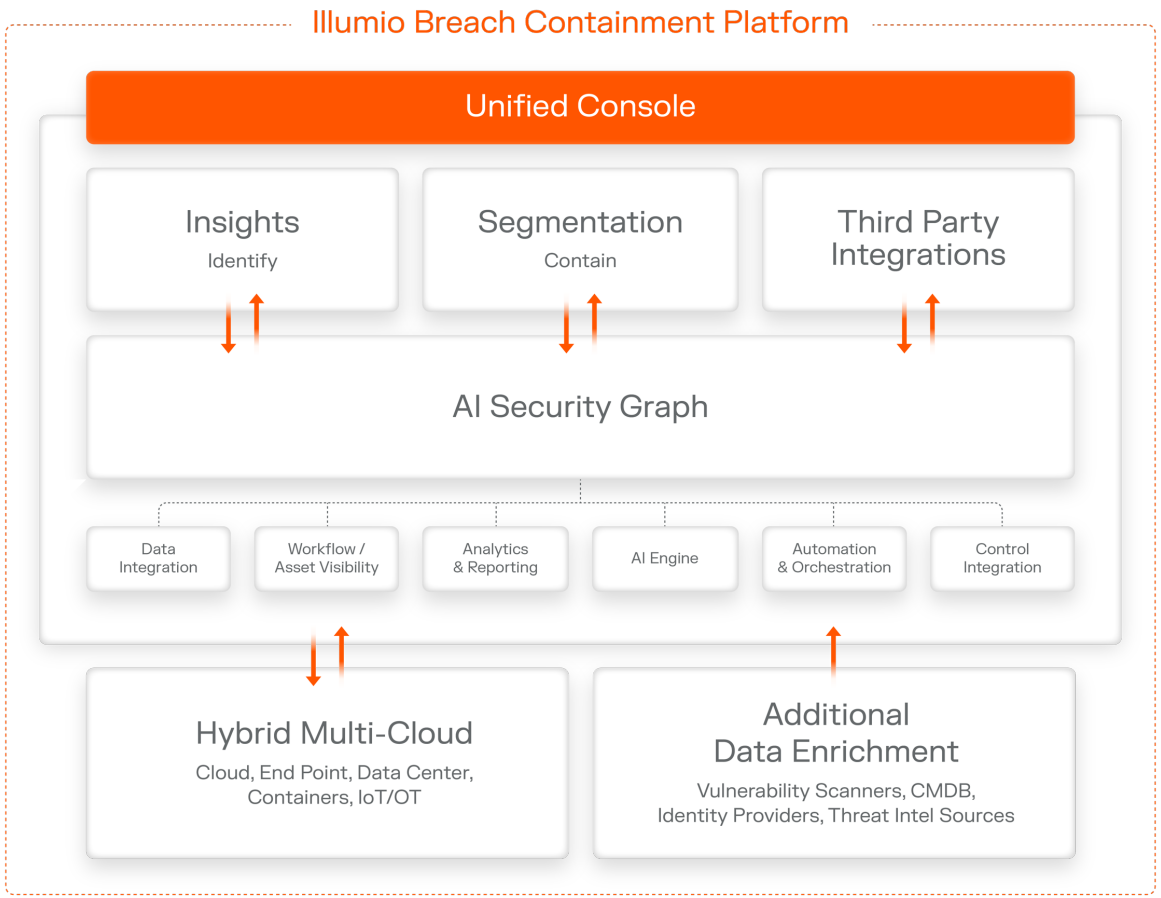
INSIGHTS

PROTECT / RESPOND / MITIGATE

SEGMENTATION

일루미로 플랫폼 – AI Security Graph 기반 Insights

AI Security Graph 기반 Insights로 빠르게 탐지하고, Segmentation으로 공격을 즉시 Contain해 복원력을 강화



1 가시성 그래프 (Visibility Graph)

환경 내에서 실제로 발생하고 있는 일은 무엇인가?

위험을 식별하고, 행위를 모니터링하며,
시스템 간 의존성을 이해하기 위한
심층 가시성 제공

2 정책 그래프 (Policy Graph)

환경에서 허용되어야 하는 행위는 무엇인가?

위험 감소 목표를 달성하기 위해
대규모 환경에서도 적용 가능한
올바른 보안 정책 기준 정의

3 AI / ML 기반 확장 (AI / ML Enrichment)

복잡성 감소, 가시성 향상, 보안 운영 가속화

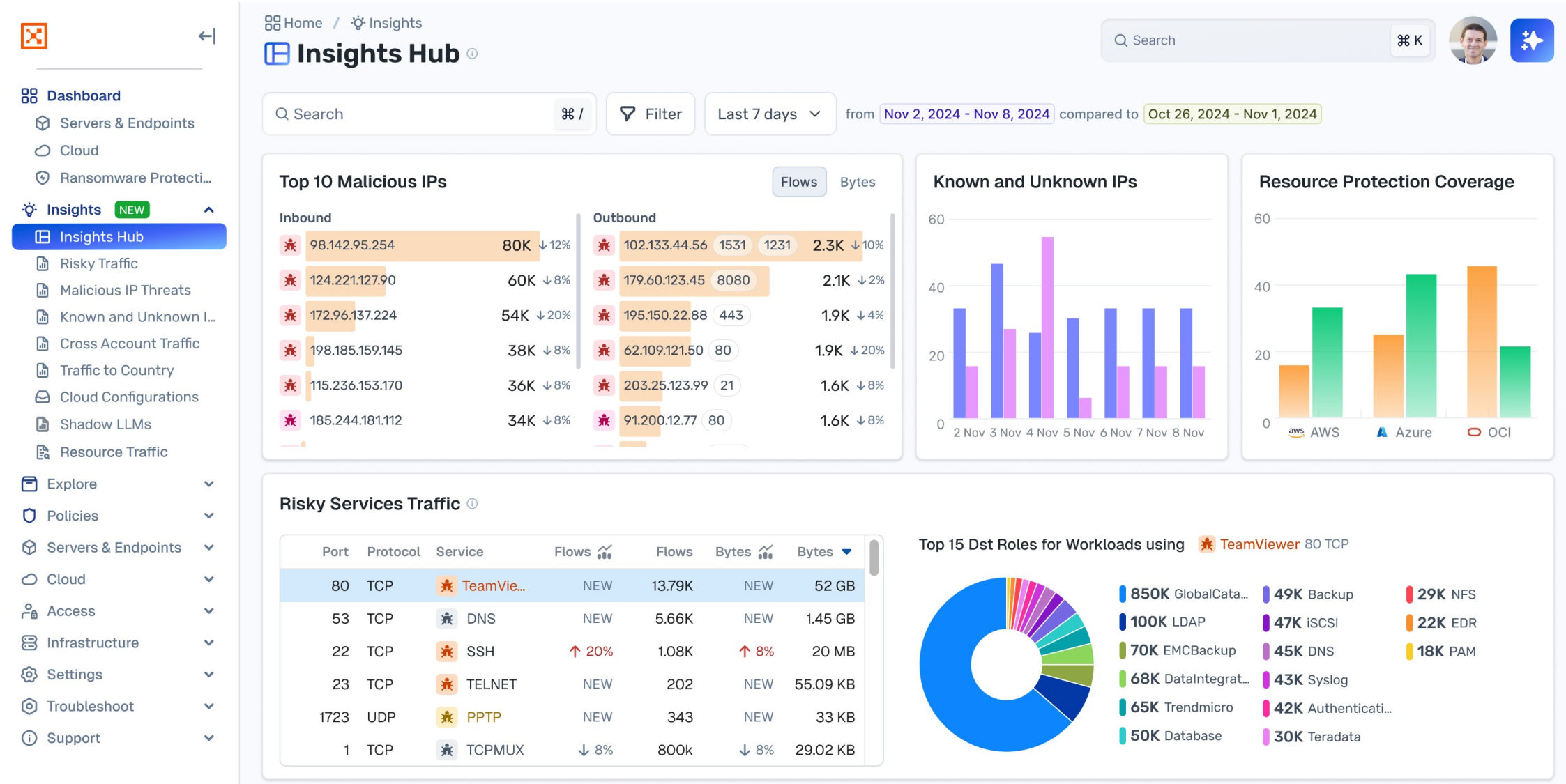
컨텍스트를 파악하고, 이상 행위를 탐지하며,
보안 정책을 자동으로 추천

4 데코레이션 (Decoration)

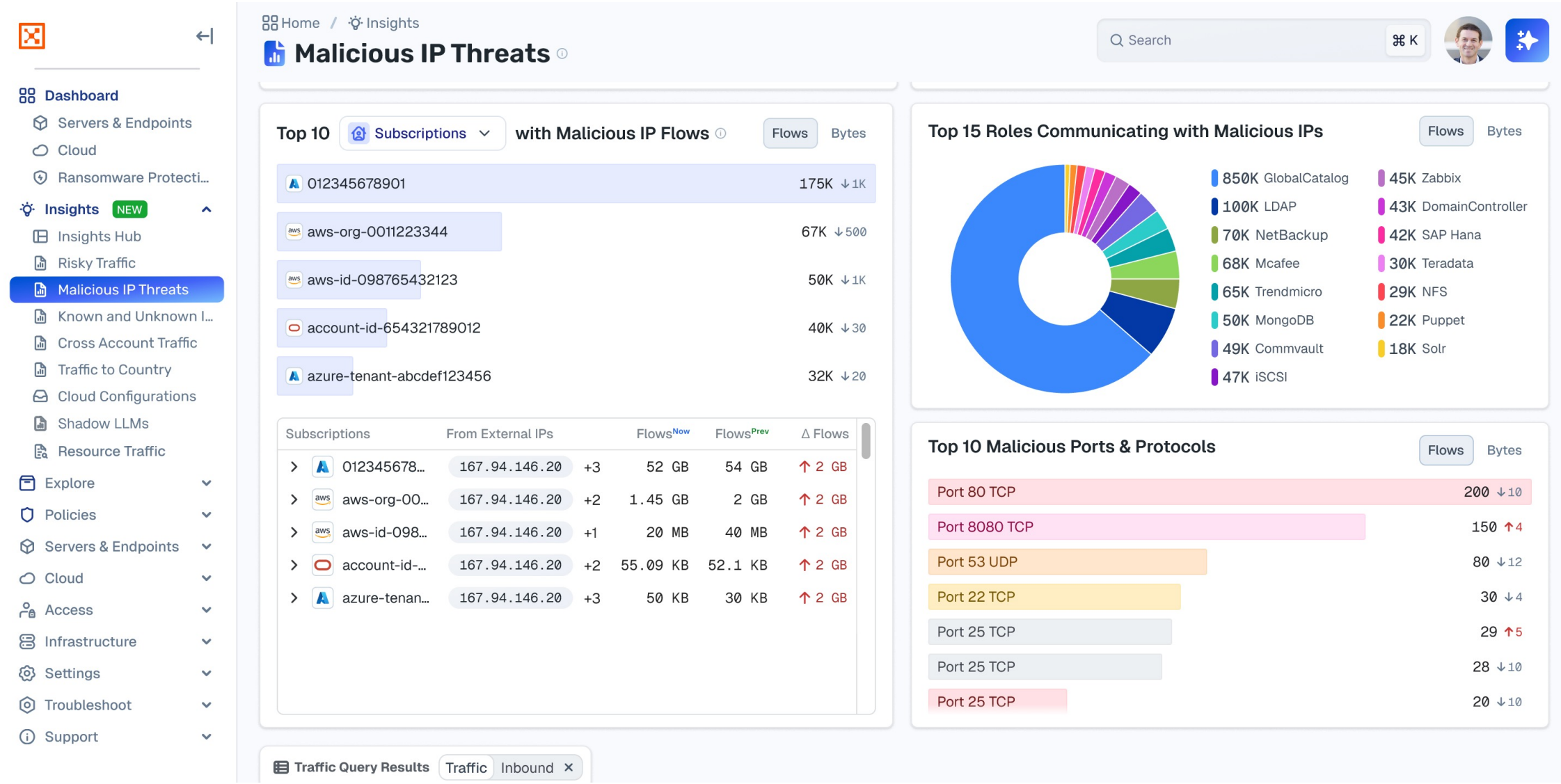
외부(서드파티) 데이터 소스를 활용한 이해도 향상

서드파티 소스를 통해
리소스와 트래픽 흐름에 대한
추가적인 인사이트 제공

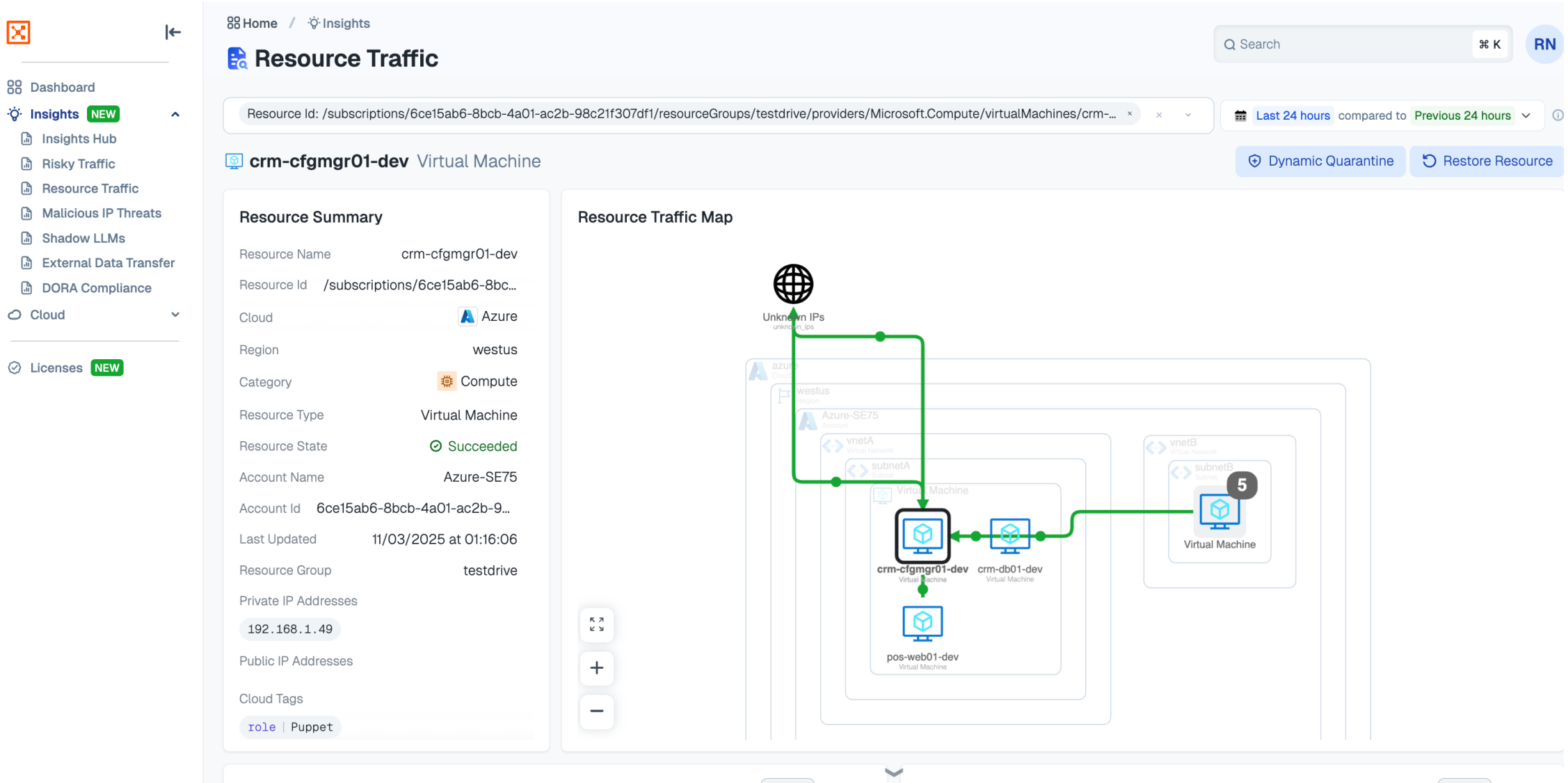
일루미로 플랫폼 – AI Security Graph 기반 Insights



일루미로 플랫폼 – AI Security Graph 기반 Insights



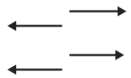
일루미로 플랫폼 – AI Security Graph 기반 Insights



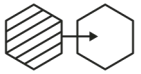
일루미오 주요 유즈케이스

하이브리드 환경 전반에서 '가시성 → 정책 → 차단(Containment)'을 일관되게 구현

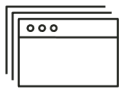
Ransomware Containment



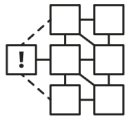
Cloud Workload Migration



IT / OT Convergence

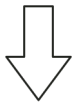


Critical Asset Protection

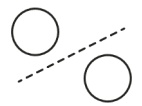


Incident Response & Recovery

Asset Mapping & Visibility



Vulnerability Risk Reduction



Environmental Separation

Microsoft 사례: 실시간 가시성과 세그멘테이션으로 리스크 선제 관리

Illumio의 실시간 가시성 + 제로 트러스트 세그멘테이션으로 위험을 줄이고 사이버 복원력을 강화

"Microsoft 규모에서 동작하고 우리 환경에 deliver 할 수 있는 세그멘테이션 솔루션은 Illumio가 유일했다."

Microsoft Global CISO
Igor Tsyganskiy

1. 도입 배경

- Microsoft는 2024년 1월 12일, Midnight Blizzard(국가 지원 공격) 이후, 내부 확산(Lateral Movement) 차단이 핵심 과제로 부상
- 하이브리드·멀티클라우드 환경에서 실시간 가시성(Observability) 필요
- 백도어 앱(예: TeamViewer) / 특정 국가(예: 러시아) 비정상 통신을 빠르게 확인할 체계 부재

2. 솔루션 선정 및 도입 범위

- 10년 이상의 축적된 기술력한 제로 트러스트 마이크로세그멘테이션 리더 벤더
- Illumio 선택: 대규모 환경에서 확산 경로를 "보고 + 즉시 차단" 가능한 플랫폼
- Insights + Segmentation을 Microsoft Corporate IT 전반에 적용(대규모 하이브리드/멀티클라우드)

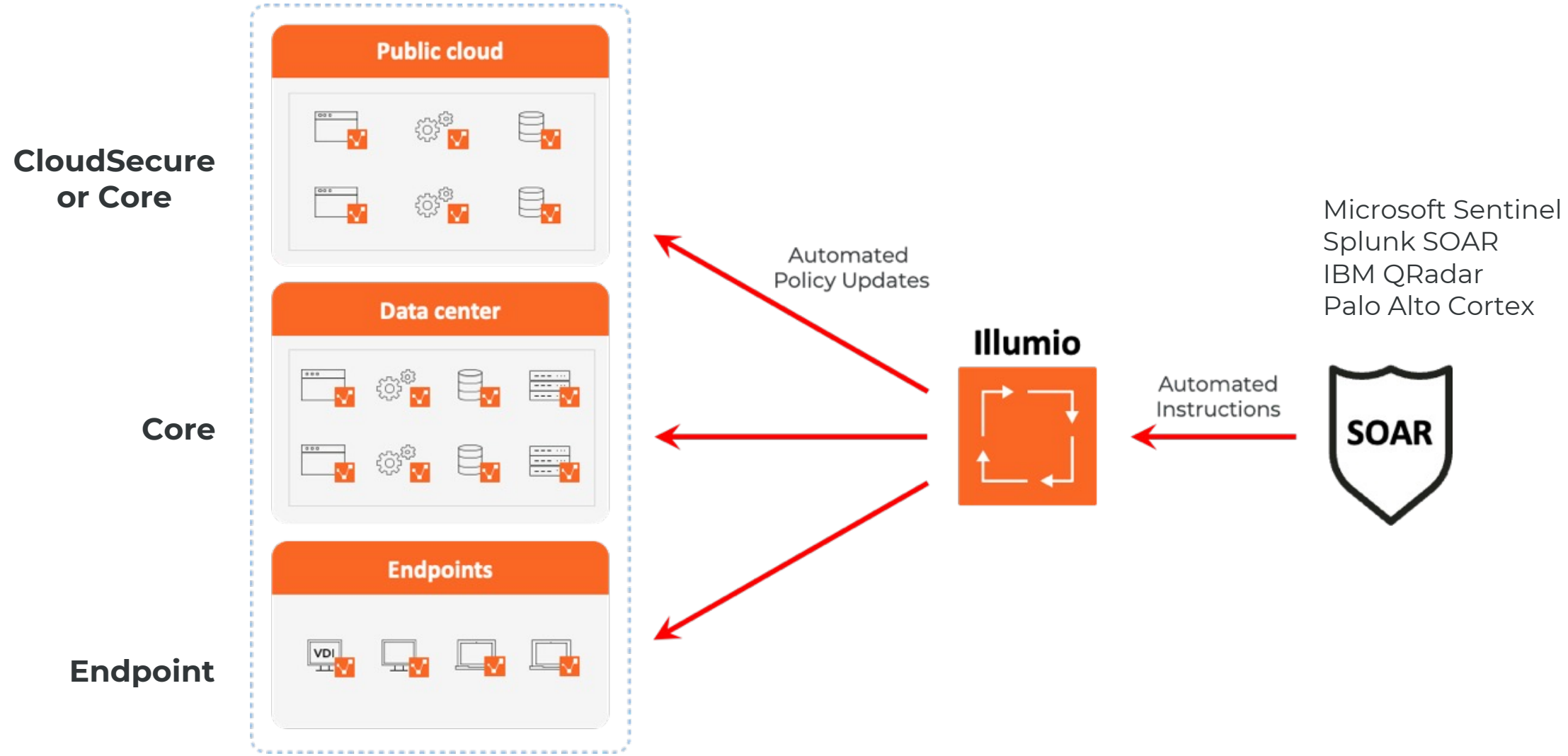
3. 도입 효과

- AI Security Graph 기반 연결/통신 가시화 → 위험 경로 즉시 파악
- 이상 통신·위협 징후 실시간 탐지(Insights)
- 마이크로세그멘테이션으로 즉시 격리/차단 → 침해 확산 억제(Breach Containment), 복원력 강화

Source:
1) https://www.illumio.com/blog/illumio-collaborates-with-microsoft-to-strengthen-companys-cyber-resilience-and-prevent-breaches-at-scale
2) https://www.illumio.com/ko/blog/how-microsoft-illumio-integrations-deliver-your-ai-powered-breach-containment-strategy

일루미오 연동 사례: 자동화된 위협에는 자동화된 대응

SOAR의 플레이북을 Illumio 정책으로 자동 변환해, 클라우드·데이터센터·엔드포인트 전반에서 즉시 차단/격리



고객사에서 일루미오를 선택하는 9가지 이유

1. 마이크로세그멘테이션 시장의 리더
- 마이크로세그멘테이션 시장을 개척·정의해온 선도 기업
- **Gartner MQ No1(2024Q3), Forrester Wave, IDC 마켓쉐어 1등**, 지속적으로 리더로 평가

2. 신속한 보호 (Fast protection)
- 2티어 구조 아키텍처로 네트워크 변경이나 대규모 아키텍처 수정 없이 빠르게 적용
- 침해 발생시 **10분 내 격리, 85% 이상 빠른 대응** 효과

3. 더 강력한 보안, 제로 트러스트 보안 전문성
- 탐지 중심이 아니라 확산 차단 중심 보안
- 공격자가 내부에 들어와도 다음 단계로 이동하지 못하게 차단, **침해 가정(Breach Assumption) 기반의 설계**
- 제로 트러스트 창시자 John Kindervag 직접 참여

4. 안정적이고 예측 가능한 마이크로세그멘테이션
- **포춘 100대 기업 50%** 사용, 글로벌 수천 고객의 대규모 하이브리드 환경에서 검증된 제품
- 운영 중 서비스 장애 없이 예측 가능한 정책 적용

5. 단순성 (Simplicity)
- 복잡한 네트워크 구성이나 방화벽 룰 관리 불필요
- **레이블 기반 정책으로 관리 단순화**
- 쉽고 간편한 운영 및 통합 관리 지원

6. 엔드투엔드 보호
- 온프레미스, 퍼블릭 클라우드, 멀티클라우드, 하이브리드 모두 지원
- 서버, VM, 컨테이너 환경까지 일관된 정책 적용
- **CC(Common Criteria) 인증** 획득

7. 대규모 환경에서 검증된 확장성
- 수만~수십만 워크로드 환경에서 실사용 사례 보유
- 글로벌 대기업, 금융, 제조, 공공에서 검증됨
- 2 티어 기반 확장성 및 효율적인 통합 관리 환경 제공

8. 비용 절감
- 침해 확산 방지로 사고 대응 비용, 다운타임 비용 감소
- 네트워크 장비 증설이나 복잡한 보안 장비 추가 불필요
- 운영 인력 부담 감소

9. 가용성을 고려한 안정 설계(Fail-safe)
- User Space 에이전트 + OS 기본 방화벽 기반 집행
- 에이전트 이슈 시에도 정책 유지(Fail-safe)

illumio

Thank you

Illumio Korea

www.illumio.com/ko-kr