CLOUDSEC 2023
ENVISION IT

클라우드 공격 표면 위험 관리 및 네이티브 애플리케이션 보안

김 석 주 이사 / 트렌드마이크로

Hosted by

TREND MICRO™

하이브리드 클라우드 여정

데이터센터

클라우드 환경

클라우드 네이티브
애플리케이션 개발

멀티 클라우드

물리 서버 &
가상 서버

인스턴스 &
자동 확장

컨테이너

스토리지

3rd
라이브러리

서버리스

Private
Cloud

GCP

보안 &
위험 관리

클라우드 여정의 보안 과제

클라우드 환경의 변화

사용자의 비즈니스 변화 전반 (데이터센터 보호, 워크로드 전환, 애플리케이션, 그리고 클라우드 네이티브 아키텍처)

하이브리드 중점

하이브리드 워크로드, 데이터센터 또는 클라우드에 적용 가능한 보안 툴

멀티 클라우드 복잡성

가시성과 지속적인 런타임 보호 그리고 멀티 클라우드의 보안 정책 관리

보안 사고 예방/대응

가시성 보장, 편리한 위험 우선순위, 클라우드 공격의 프로세스 인지

클라우드 보안 필요성

통합

보안 계층과 서비스 제공업체 전반에 걸쳐 중앙 집중화된 가시성과 관리 기능을 갖춘 통합 클라우드 보안 제어

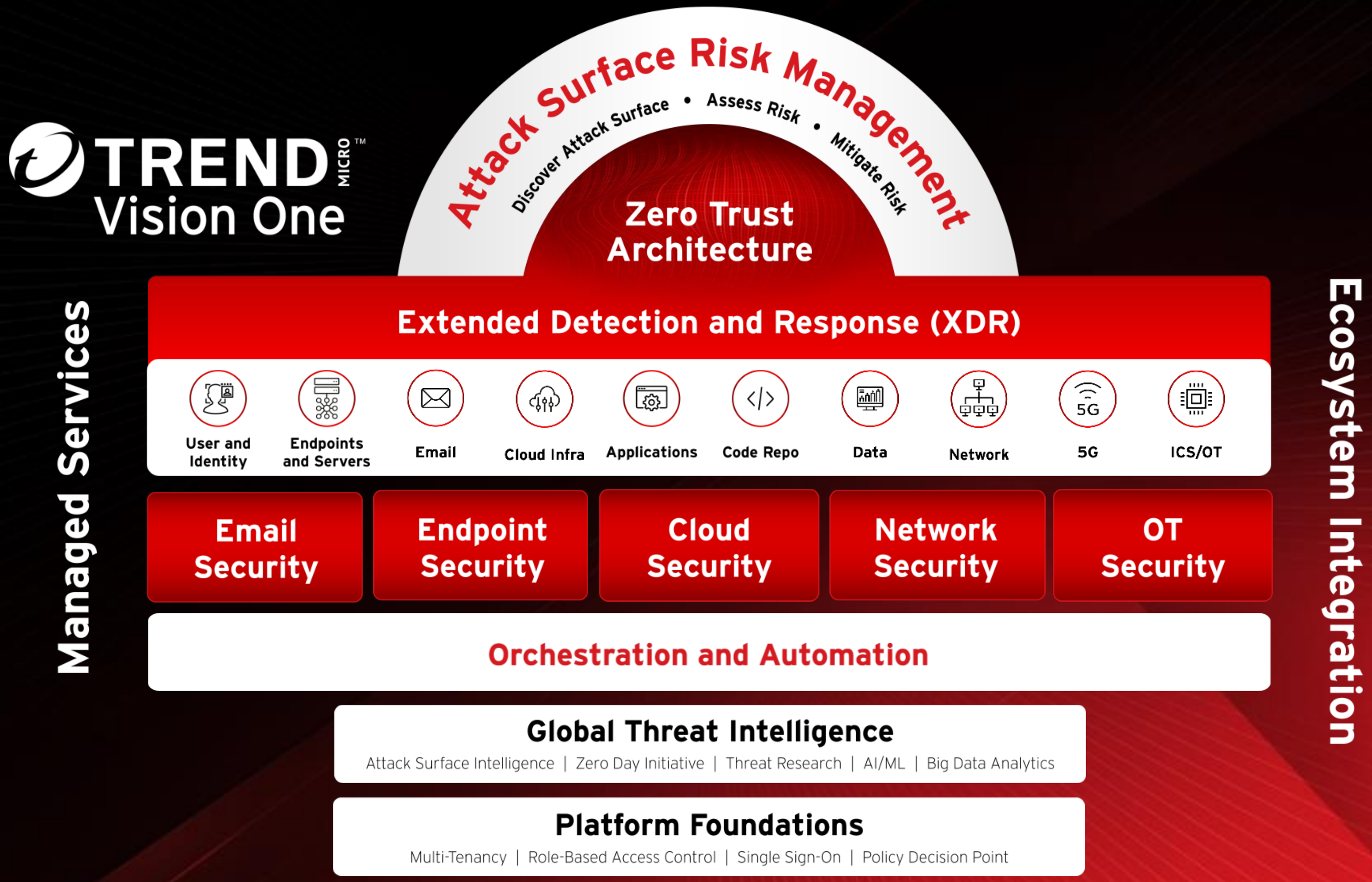
간소화

연결된 플랫폼 워크플로우와 클라우드 자동화 및 오케스트레이션 프로세스를 통해 최적화된 사용자 경험

표준화

자산 검색, 보안 정책 관리, 라이센싱 등과 같은 클라우드 플랫폼 기능 전반의 일관성

보안 툴에서 사이버 보안 플랫폼으로 전환



클라우드 공격 표면 위험 관리

Contextual Visibility of Cloud Risk

Cloud Asset Inventory | Cloud Asset Graph | Attack Path Analysis | Risk Summary & Explorer

Risk Prioritization

Vulnerability | Compliance | Misconfiguration | Threat/Attack

Risk Reduction

Workloads | Containers | Serverless (Lambda) | API | IAM (Identity, Role) | Storage

Frictionless Data Ingestion

aws | Azure

TREND MICRO

Trend Vision One™ – 클라우드 보안

조직이 하이브리드 클라우드 환경 전반에서 위협을 신속하게 식별하고 침해 노출을 줄이며 보안 위협에 대응할 수 있도록 지원

HYBRID CLOUD STRATEGY
On-premise + Multi Cloud – AWS, Azure, GCP, and Others

ASRM for Cloud

(Attack Surface Risk Management)

하이브리드 클라우드 중심의 내부 및 외부 공격 표면 발견, 위험 우선순위 지정 및 해결

XDR for Cloud

(Cloud Detection & Response)

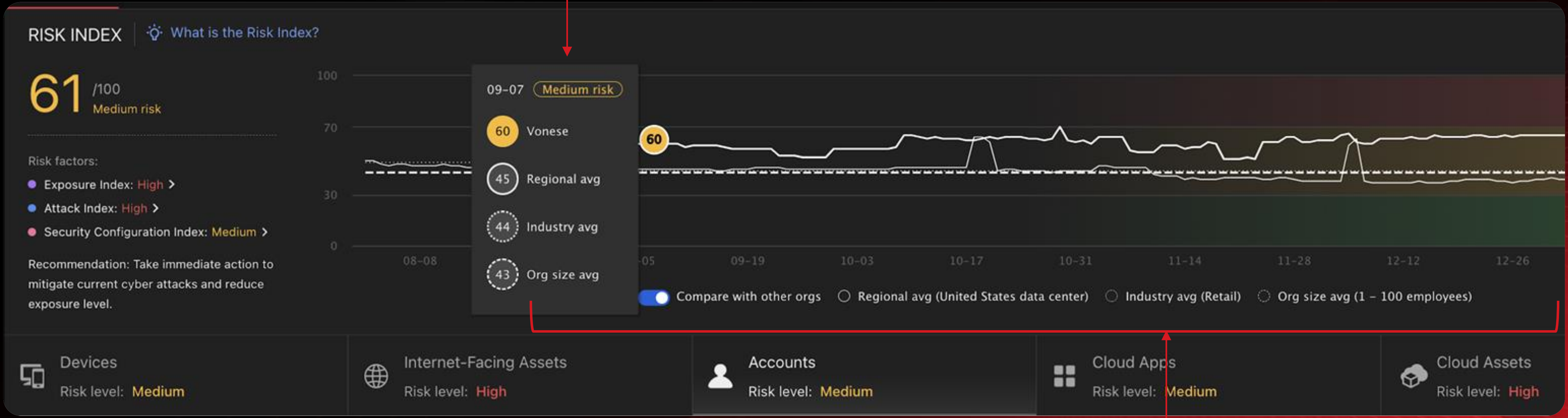
빠른 감지 및 대응을 위한 맞춤형 하이브리드 클라우드 원격 상관 관계 분석

Protection

하이브리드 클라우드를 위한 주문형 및 런타임 보호. 서버, 가상 머신, 컨테이너, 스토리지 등 모든 워크로드에서 취약점과 멀웨어를 발견하고 차단

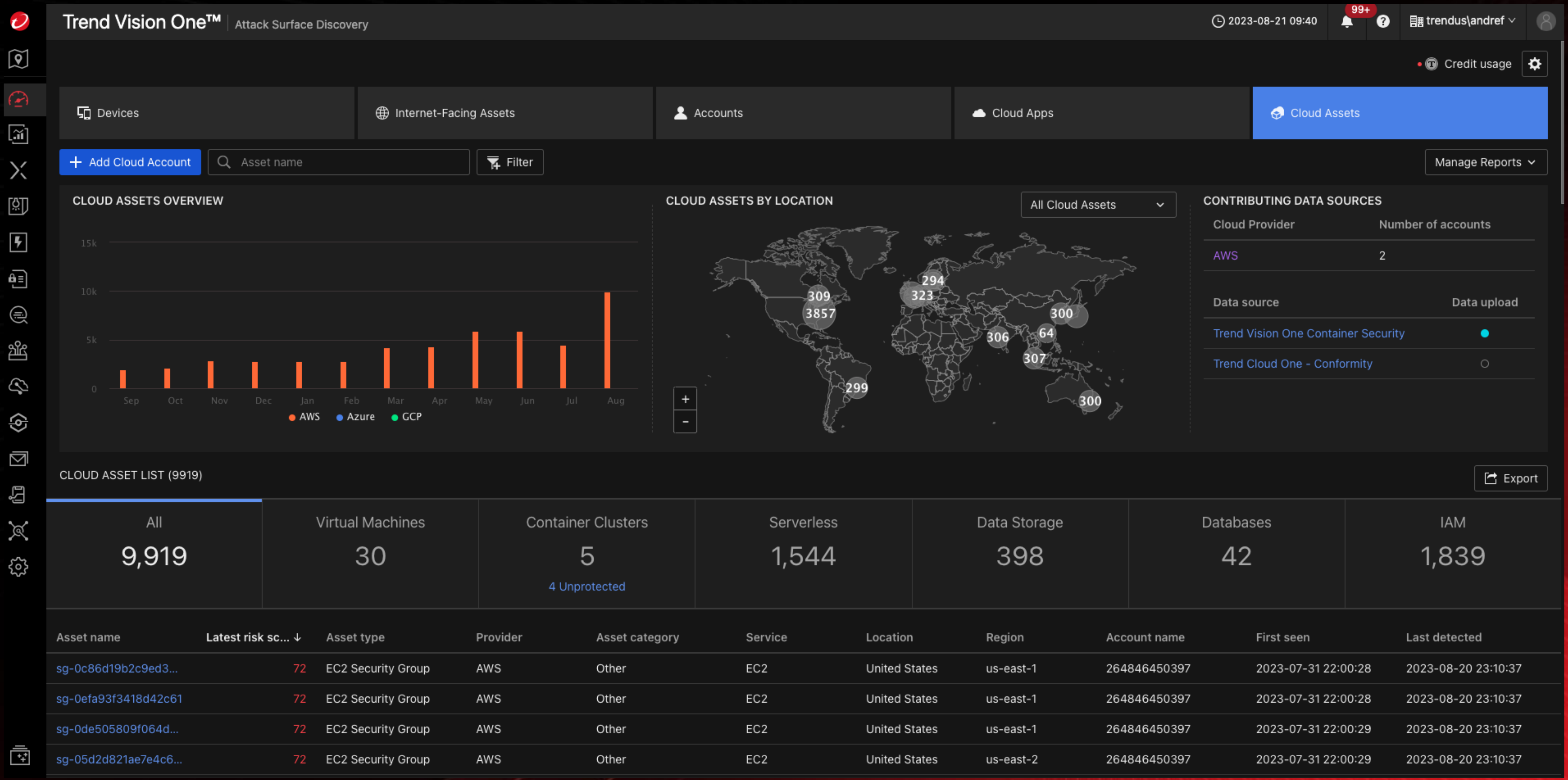
중앙 집중식 위험 가시성 및 벤치마킹

기준별 비교 분석

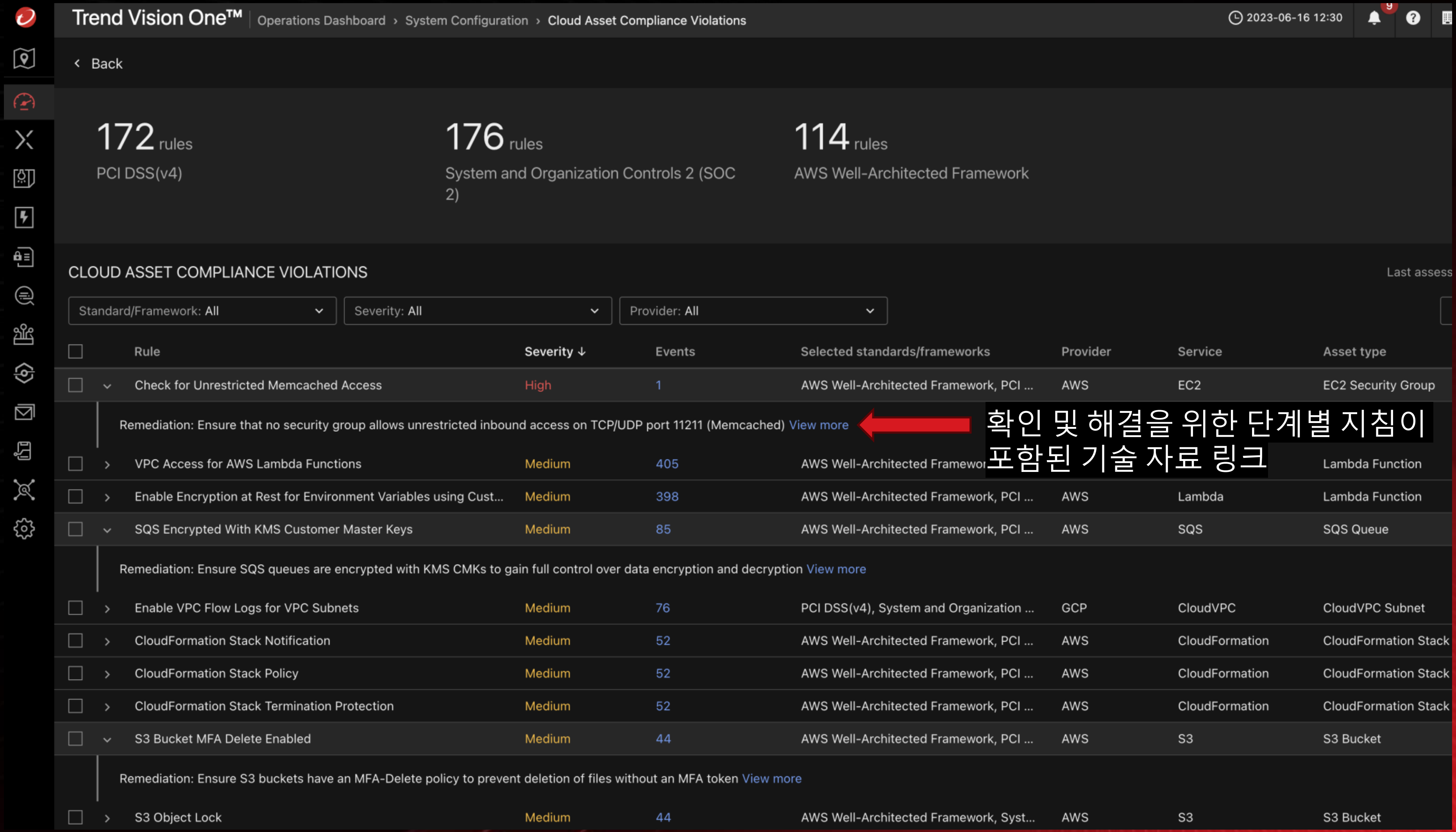


시간대별 위험 레벨

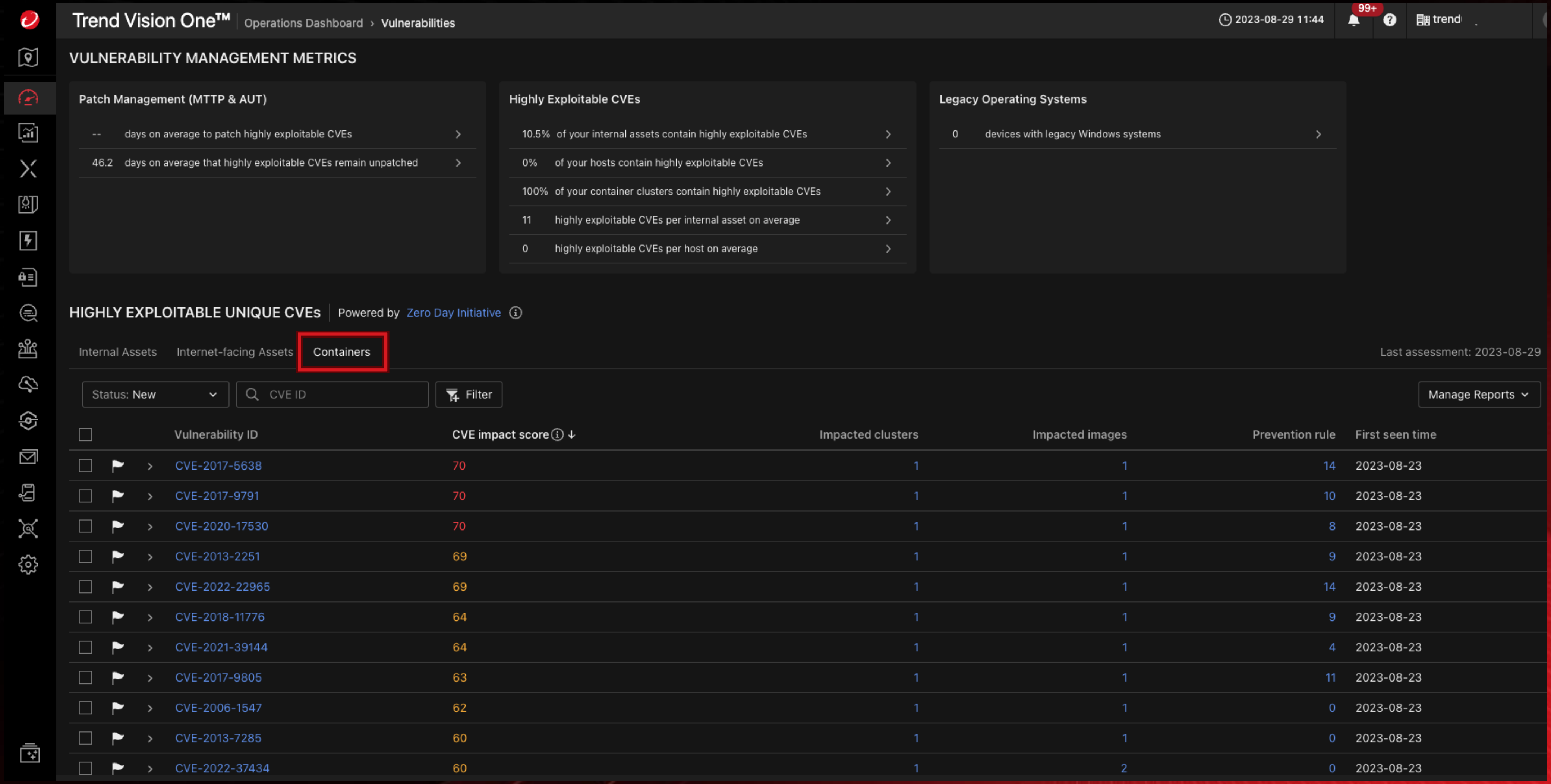
클라우드 자산 시각화와 위험 관리



대응 가이드가 포함된 보안 취약한 구성 가시성



컨테이너 취약점 우선순위 가시성



Trend Vision One™ – 클라우드 보안

조직이 하이브리드 클라우드 환경 전반에서 위협을 신속하게 식별하고 침해 노출을 줄이며 보안 위협에 대응할 수 있도록 지원

HYBRID CLOUD STRATEGY
On-premise + Multi Cloud – AWS, Azure, GCP, and Others

ASRM for Cloud
(Attack Surface Risk Management)

하이브리드 클라우드 중심의 내부 및 외부 공격 표면 발견, 위험 우선순위 지정 및 해결

XDR for Cloud
(Cloud Detection & Response)

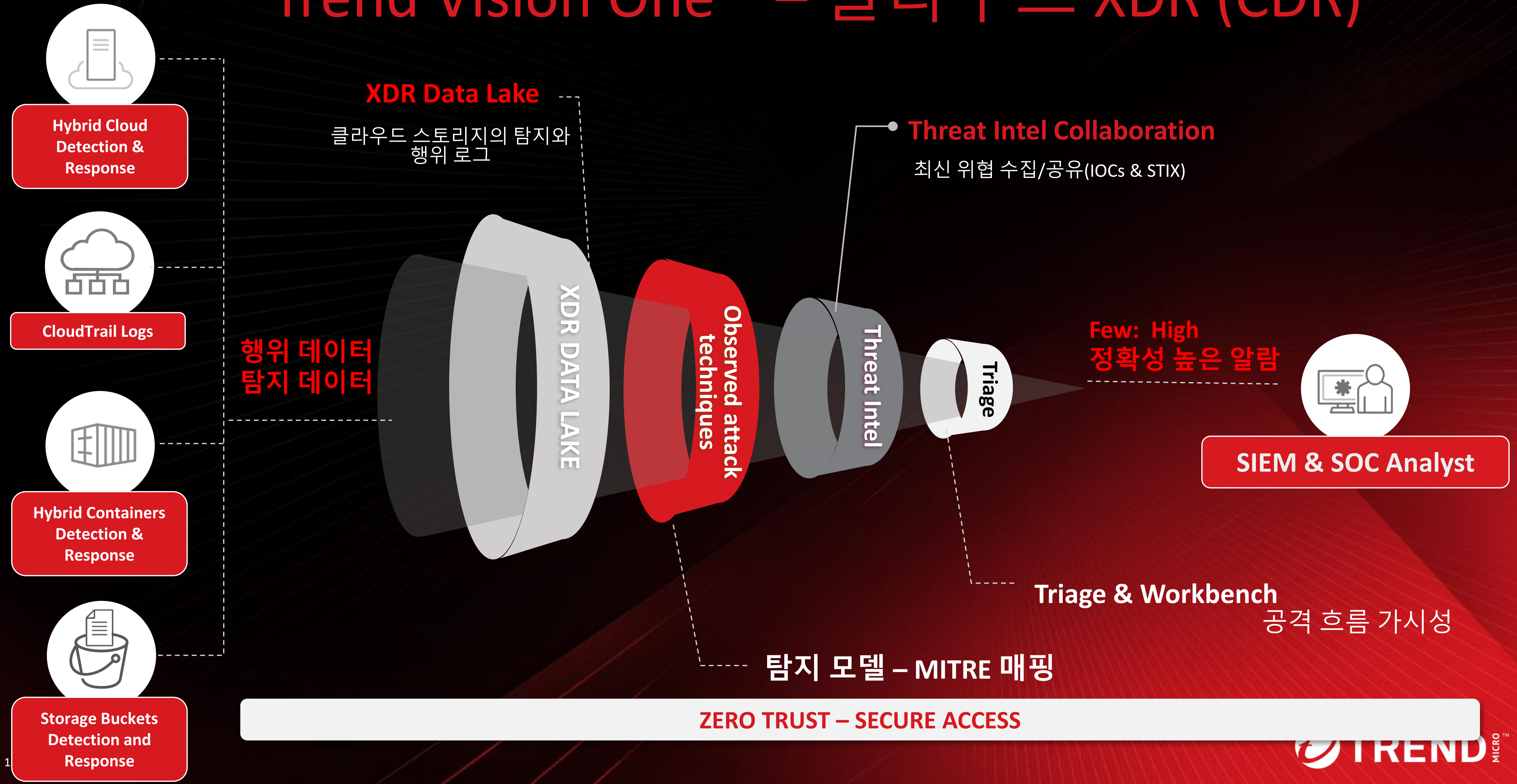
빠른 감지 및 대응을 위한 맞춤형 하이브리드 클라우드 원격 상관 관계 분석

Protection

하이브리드 클라우드를 위한 주문형 및 런타임 보호. 서버, 가상 머신, 컨테이너, 스토리지 등 모든 워크로드에서 취약점과 멀웨어를 발견하고 차단

TREND MICRO

Trend Vision One™ – 클라우드 XDR (CDR)



Trend Vision One™ – 클라우드 XDR (CDR)

탐지 모델

- 700 개 이상 탐지 모델
- 순도 높은 경고 알람
- 위협 인텔리전스 기반 데이터 레이크 로그

하이브리드 클라우드 통합 XDR

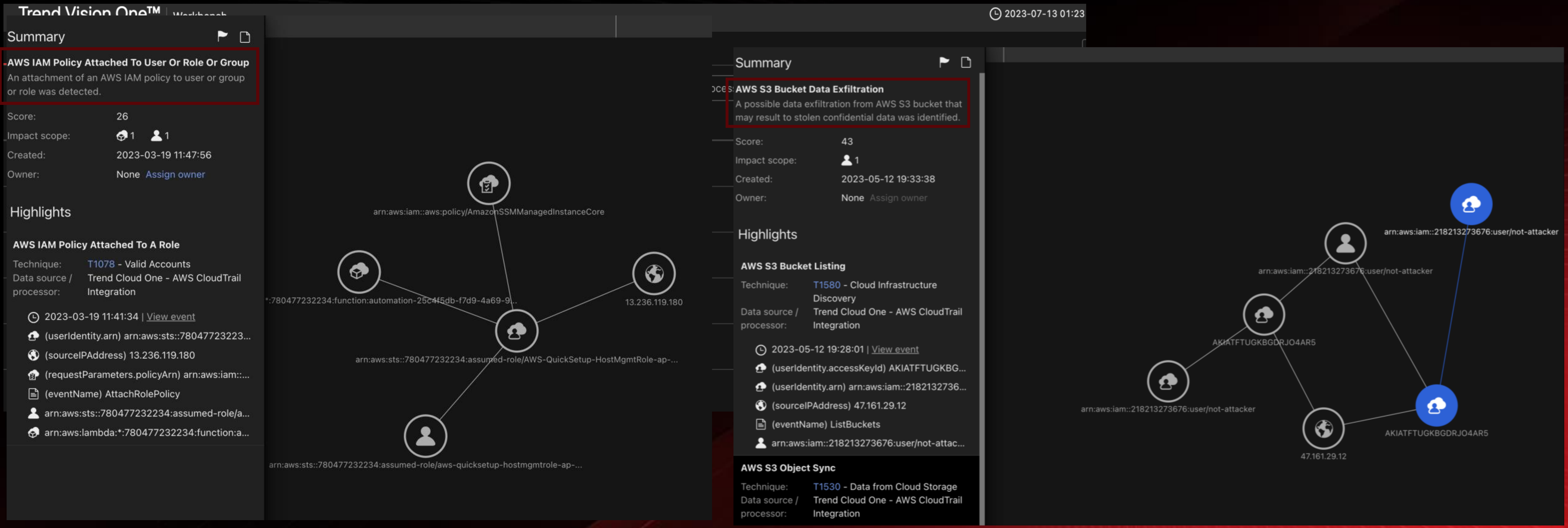
- SOC 팀을 위한 폭넓은 가시성을 위한 하이브리드 워크로드의 텔레메트리 수집
- 하이브리드 서버, 인스턴스, 컨테이너를 위한 특징적 XDR
- 클라우드 사업자의 모니터링 리소스와 연동하여 가시성 확대

사용자 정의 탐지 모델

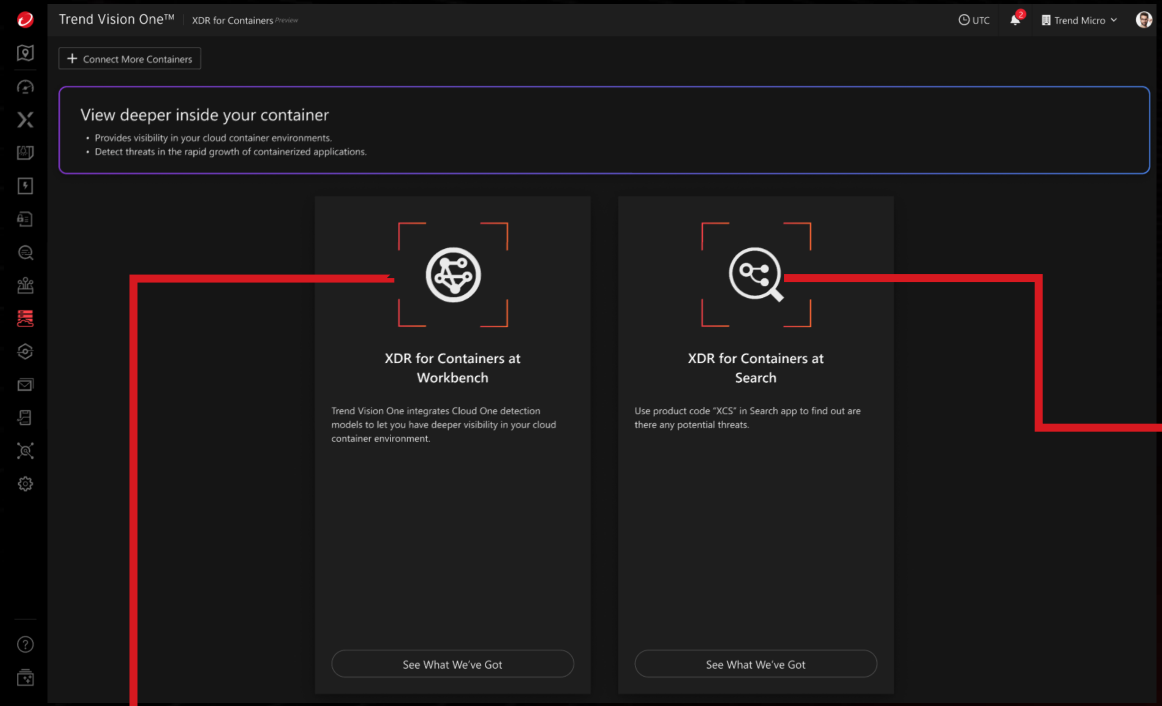
- 정책의 유연한 생성
- 독립적, 관계적 사용자 정의 정책 생성 가능
- 행위 데이터를 수집하는 정책의 실행 빈도를 스케줄로 지정

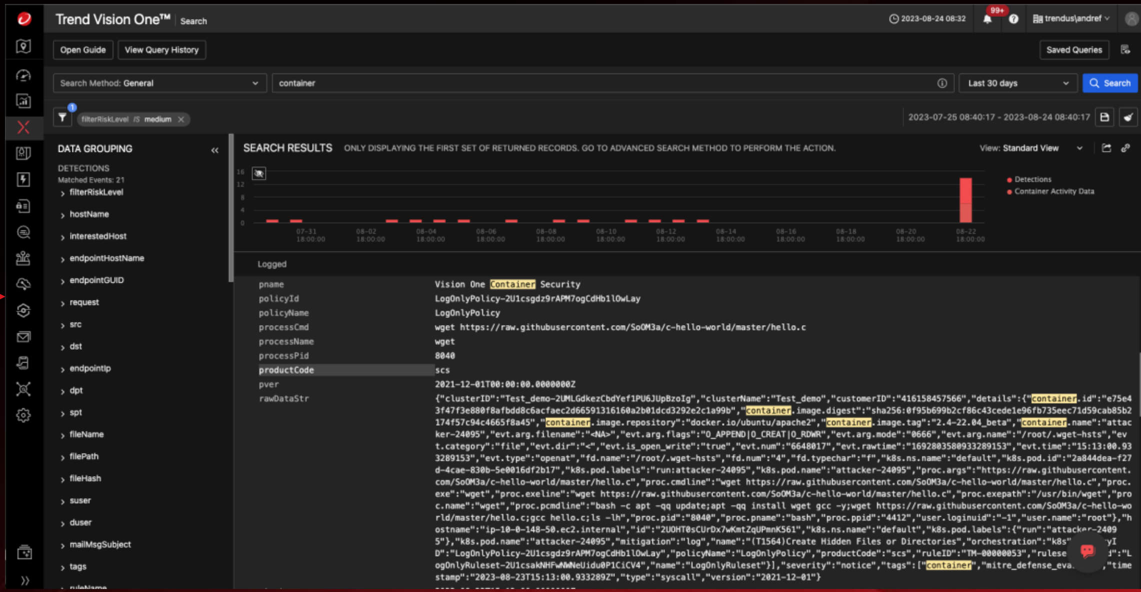
XDR for Cloud – AWS Cloud Trail 연동

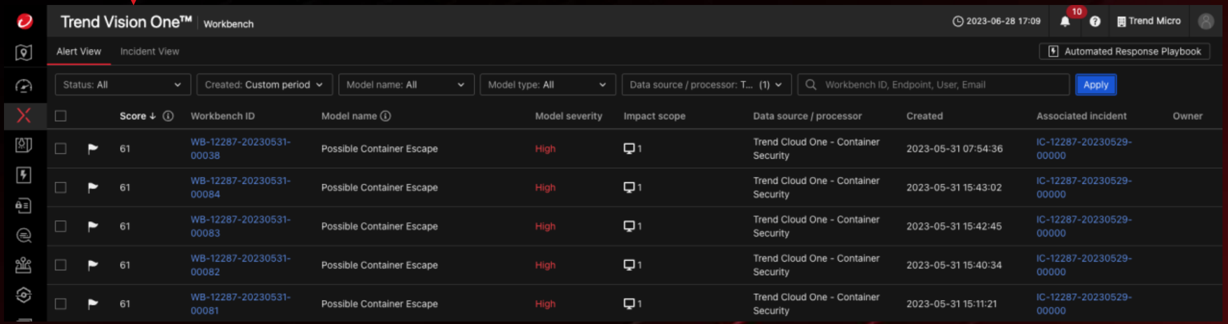
워크로드, 컨테이너 및 추가 클라우드 리소스에 대한 XDR을 포함하여 빠른 감지 및 대응을 위한 클라우드 보안 상관 관계



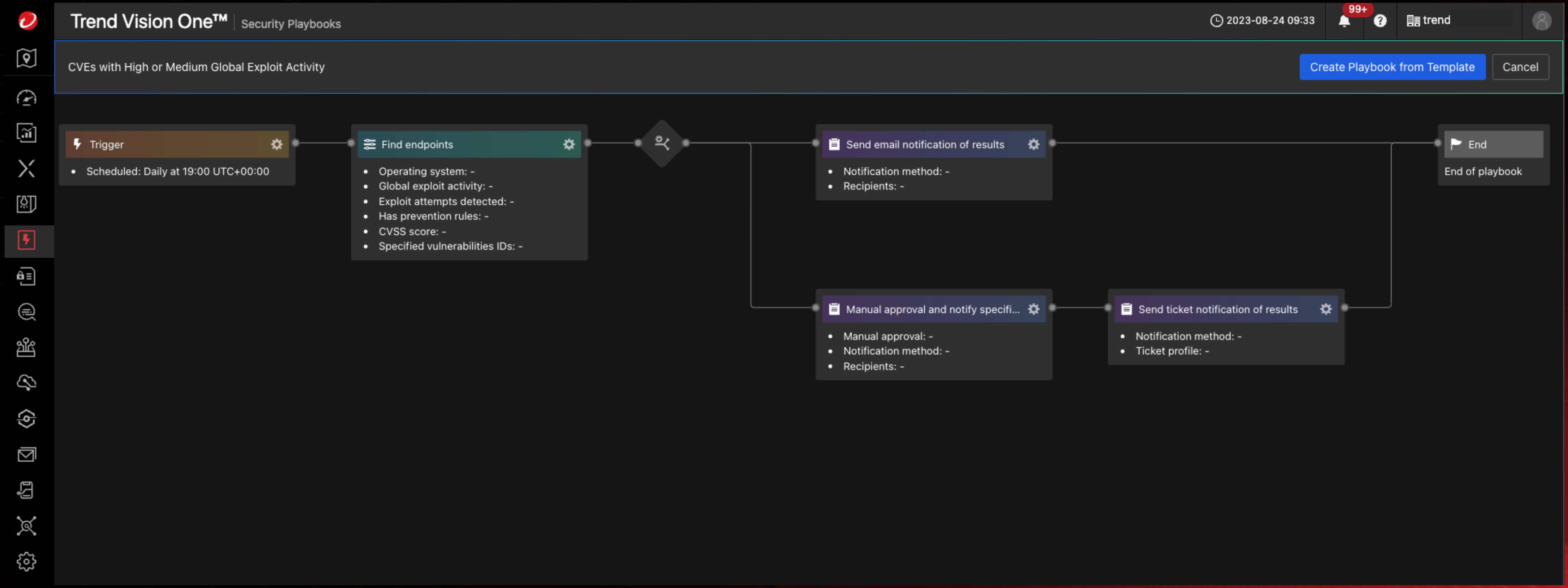
XDR for Cloud – 컨테이너 로그 조사/분석





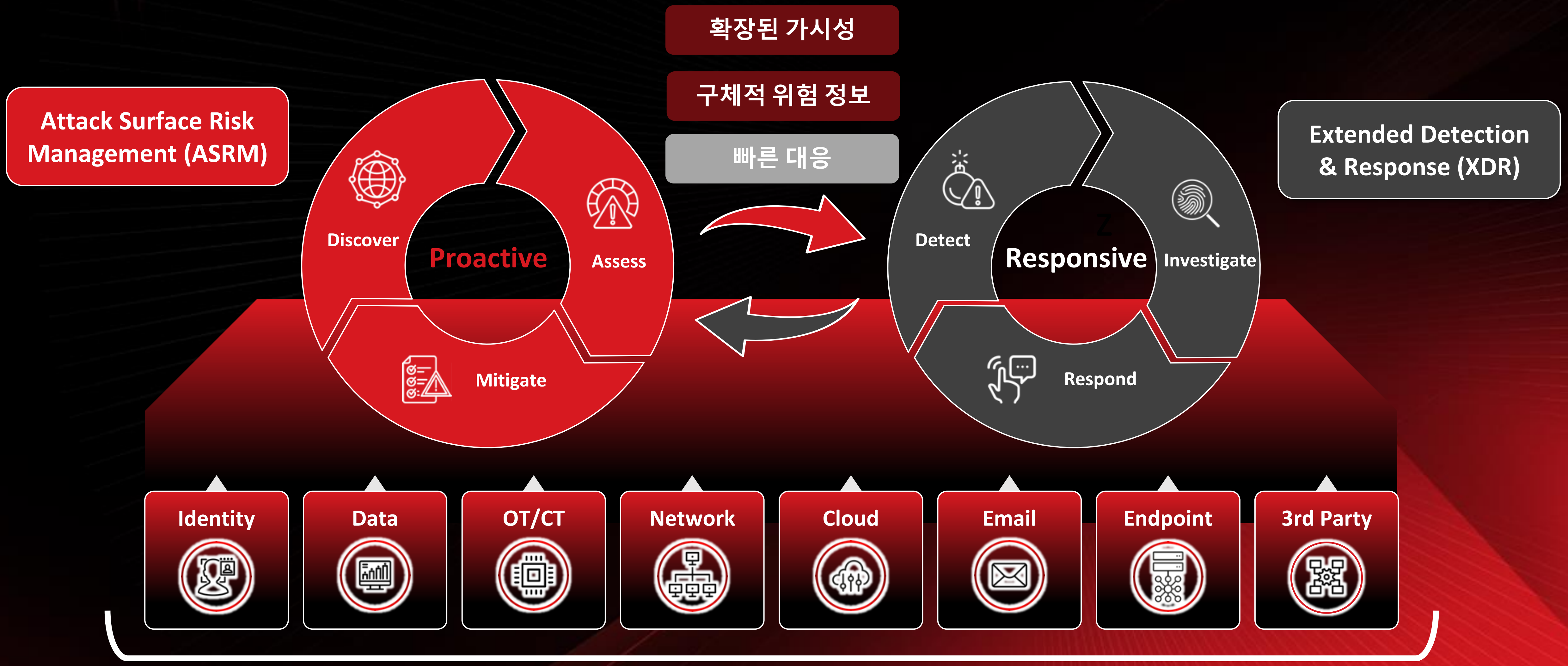


보안 플레이북



자동화 | 통합 보안 Playbook을 통해 수동 대응에서 자동화된 워크플로 및 AI 지원 대응으로 전환

Cloud: CDR/XDR + ASRM



글로벌 마켓에서 가장 광범위한 센서 범위

Trend Vision One™ – 클라우드 보안

조직이 하이브리드 클라우드 환경 전반에서 위협을 신속하게 식별하고 침해 노출을 줄이며 보안 위협에 대응할 수 있도록 지원

HYBRID CLOUD STRATEGY
On-premise + Multi Cloud – AWS, Azure, GCP, and Others

ASRM for Cloud
(Attack Surface Risk Management)

하이브리드 클라우드 중심의 내부 및 외부 공격 표면 발견, 위험 우선순위 지정 및 해결

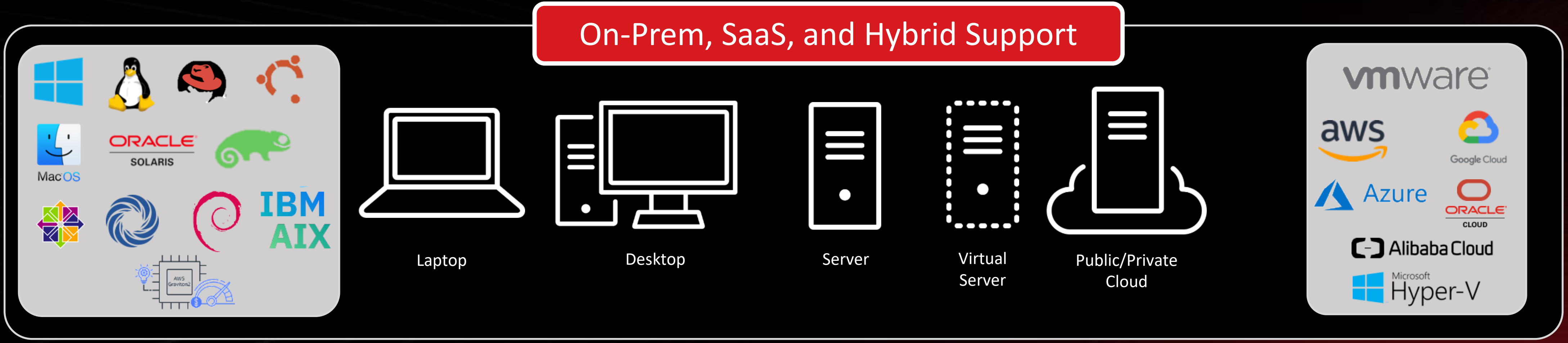
XDR for Cloud
(Cloud Detection & Response)

빠른 감지 및 대응을 위한 맞춤형 하이브리드 클라우드 원격 상관 관계 분석

Protection

하이브리드 클라우드를 위한 주문형 및 런타임 보호. 서버, 가상 머신, 컨테이너, 스토리지 등 모든 워크로드에서 취약점과 멀웨어를 발견하고 차단

Trend Vision One™ – 서버 & 워크로드 보안



중앙 집중식 가시성 & 관리

EPP & EDR/XDR을 위한 통합 플랫폼

하이브리드 워크로드의 전체 통합 보안 적용

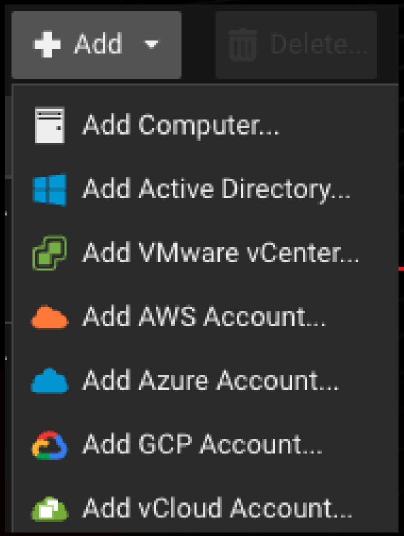
보안 규정 준수를 지킬 수 있는 보안 범위

더 나은 분석 및 해결을 위해 보안 정보를 집계하는 데 도움이 되는 유연한 3rd Party 통합

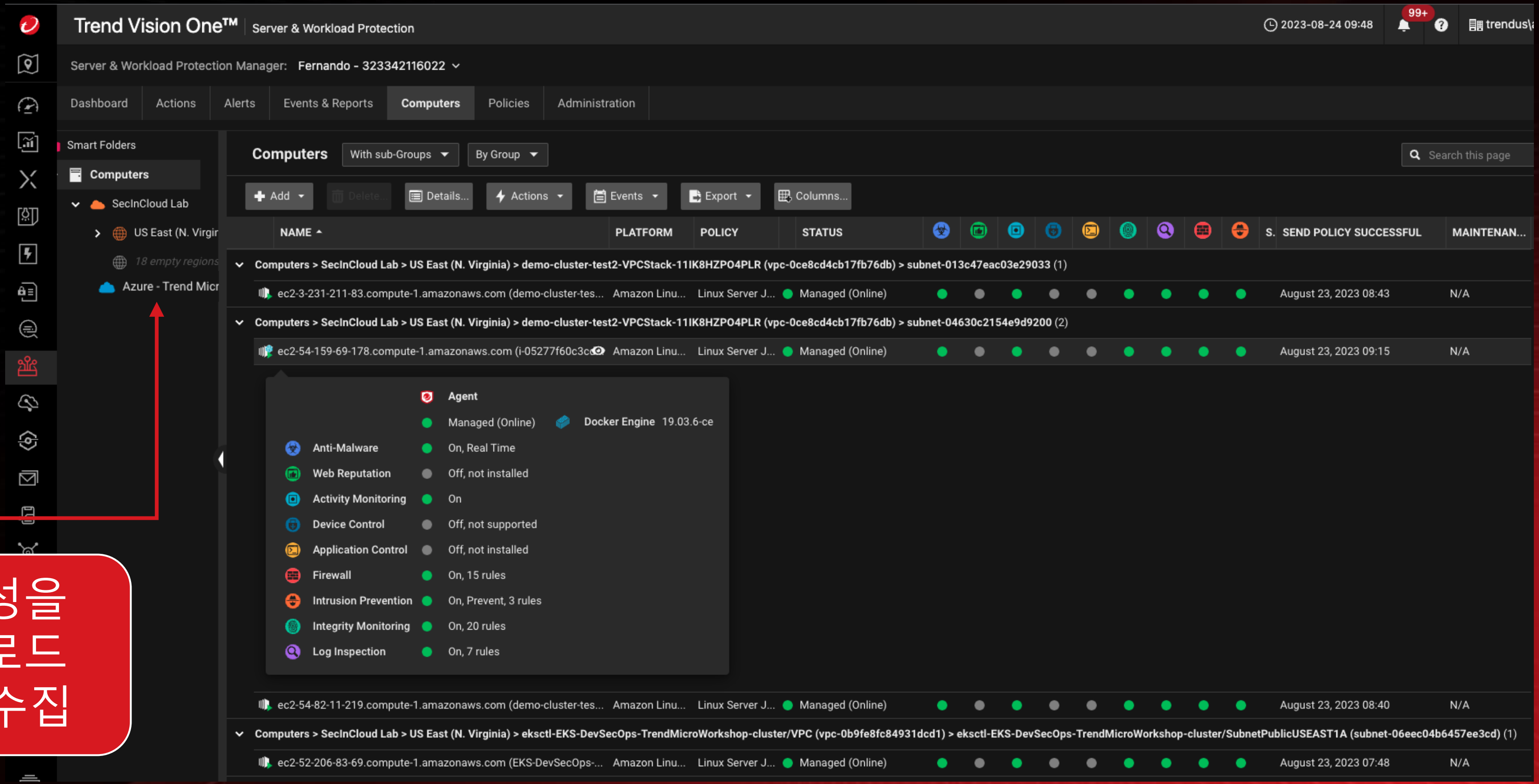
TREND MICRO

하이브리드 클라우드 워크로드 가시성 통합

하이브리드
클라우드
서비스로
유연한 연동

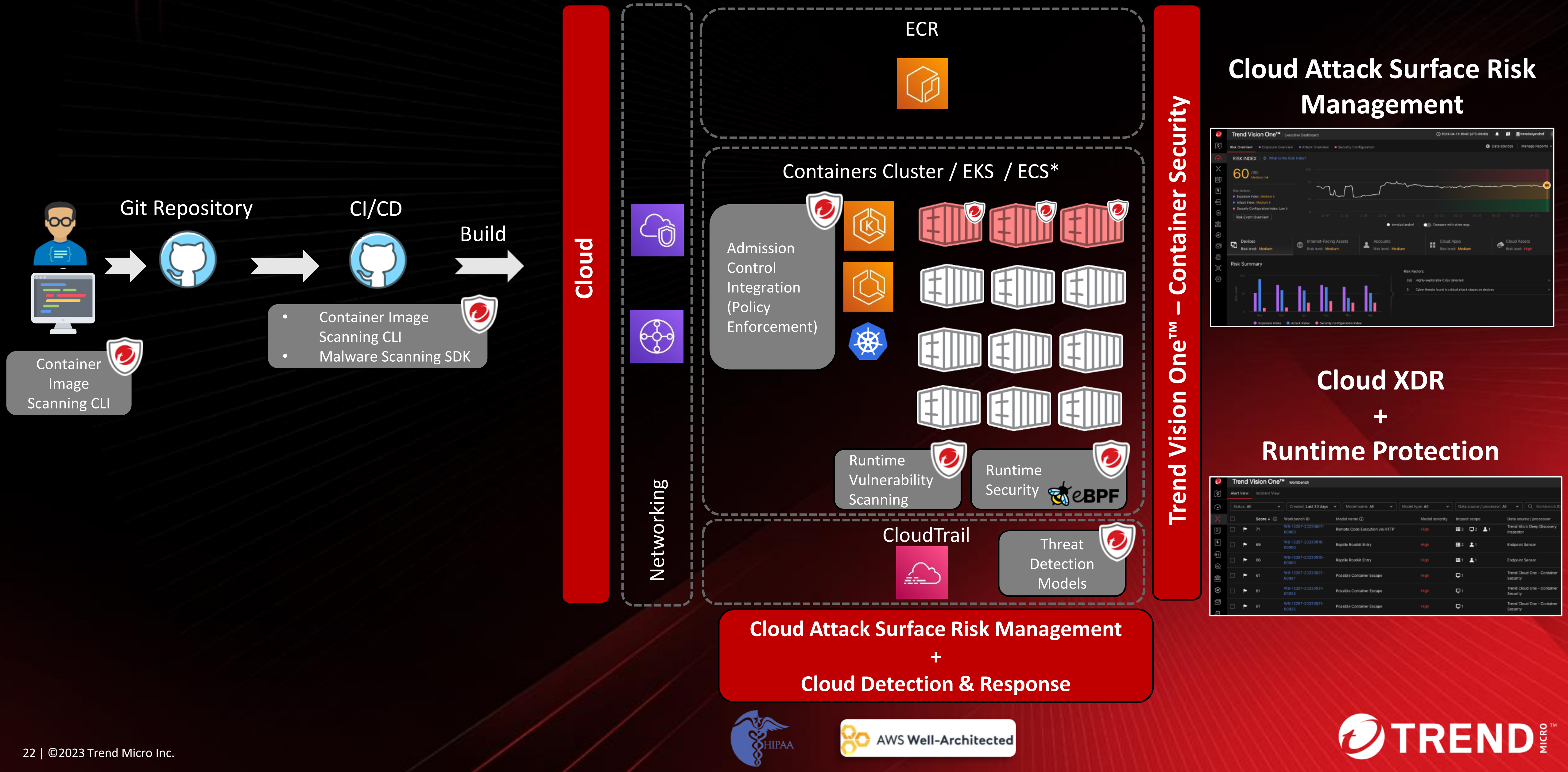


보안 가시성을
위해 워크로드
정보 자동 수집



TREND MICRO

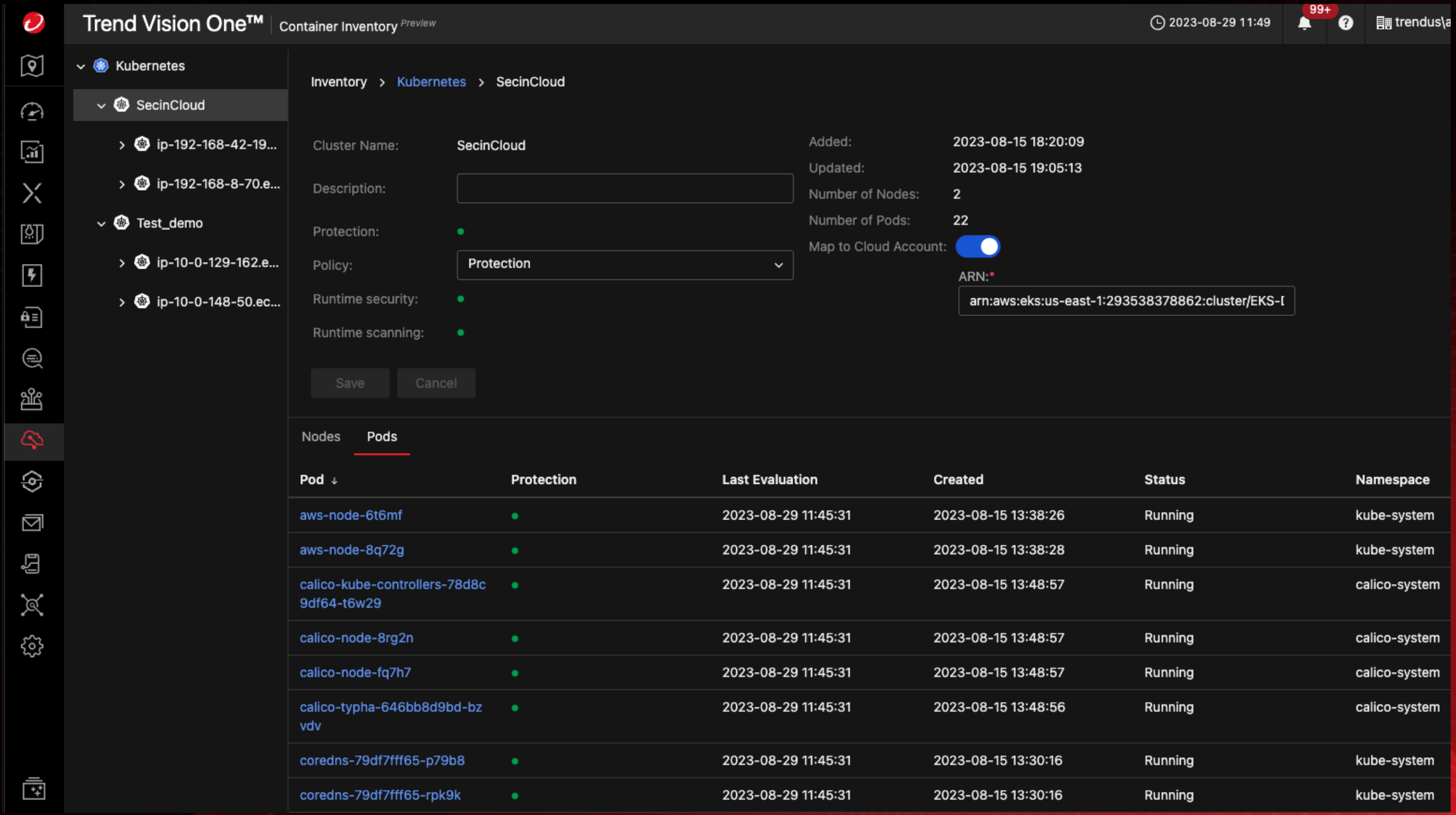
Trend Vision One™ – 컨테이너 보안



클러스터 인벤토리 시각화

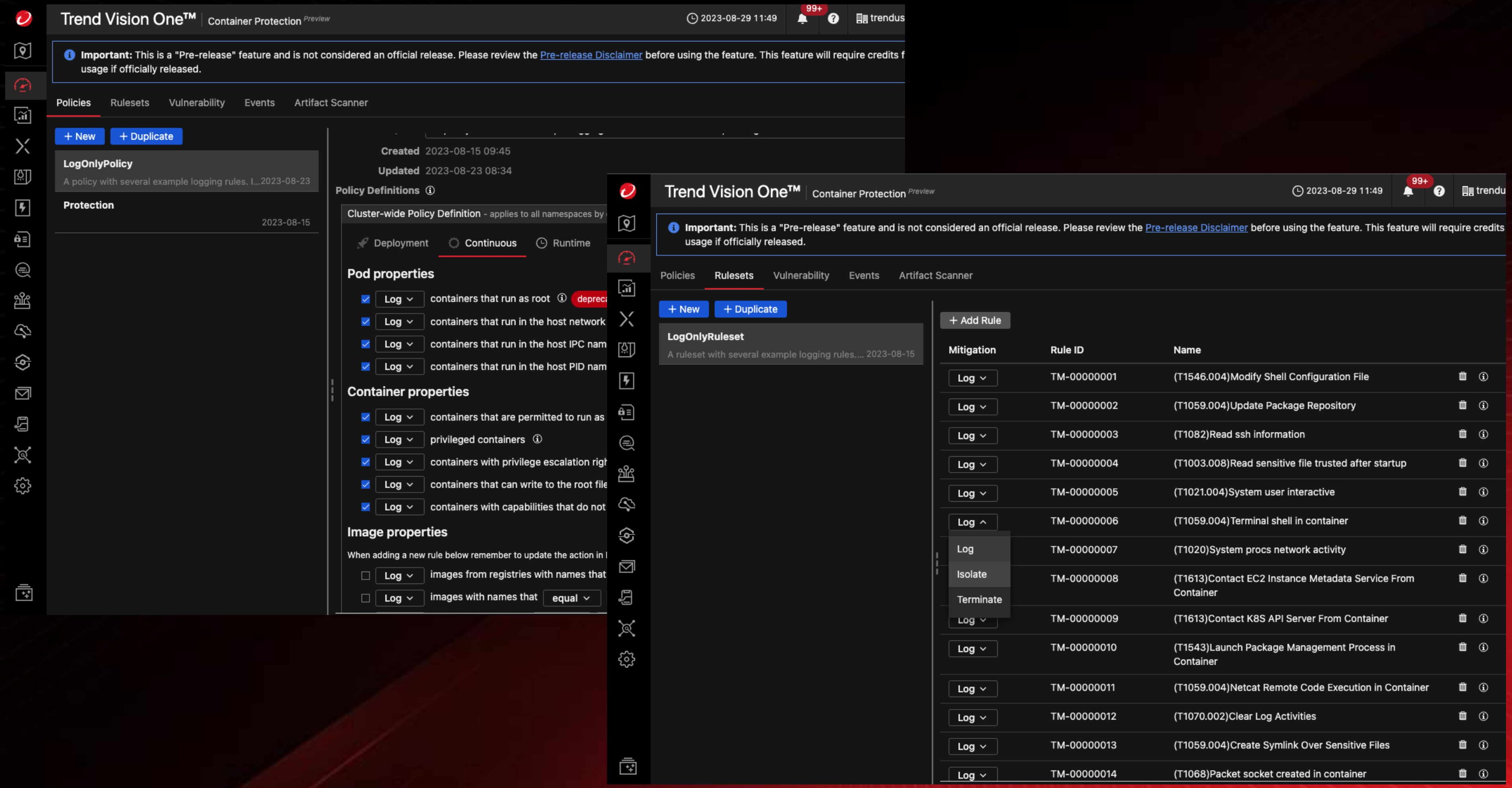
클러스터 인벤토리에 대한 명확하고 체계적인 개요를 확보하여 리소스를 효과적으로 관리하고 추적하기 쉬움

클러스터, 노드, 파드!

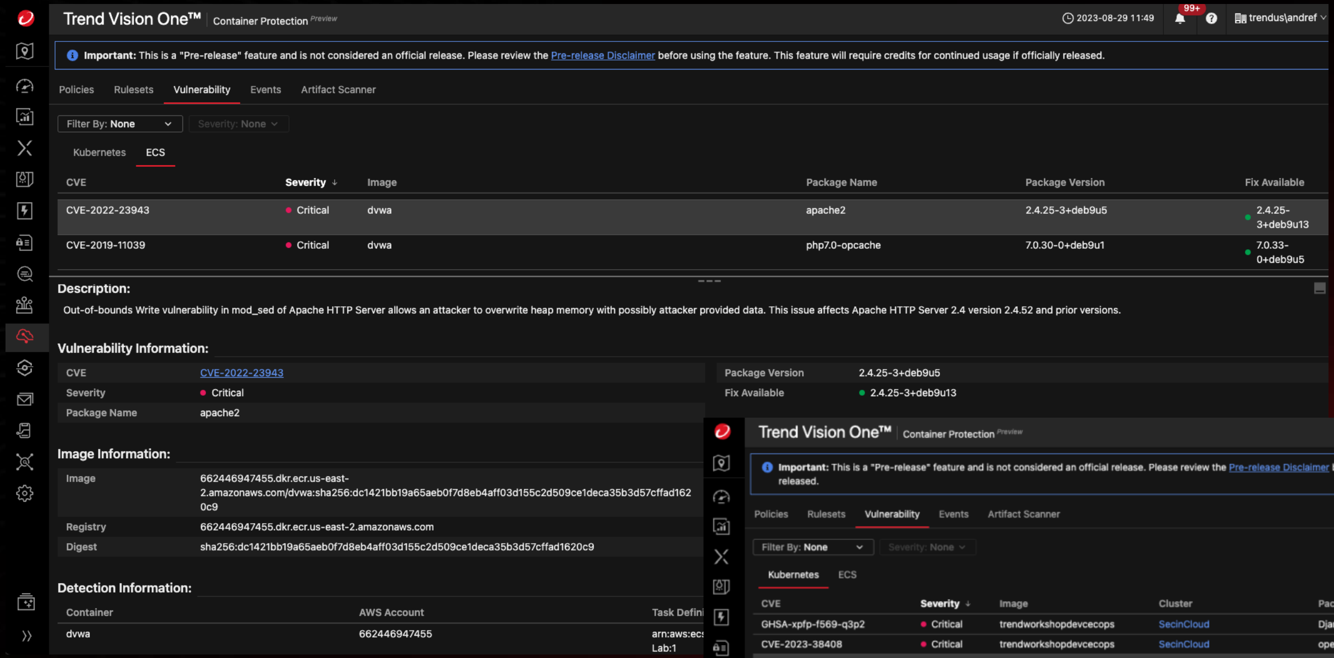


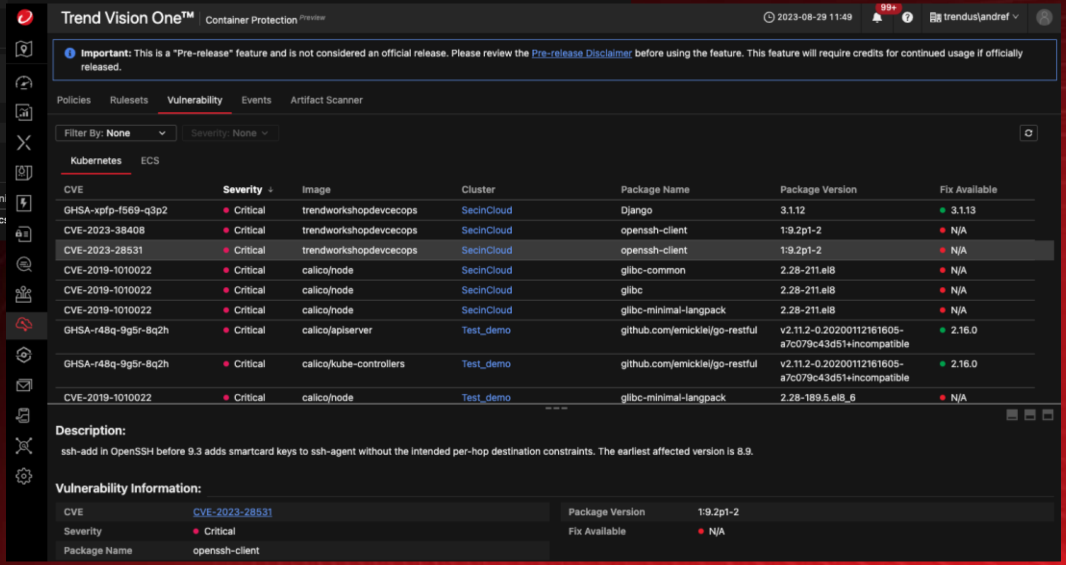
정책 관리 & 이벤트 시각화

Trend Vision One
콘솔에서 정책, 규칙,
이벤트를 모두
원활하게 관리하고
모니터링하여 보안
운영 및 워크플로를
간소화



보안 취약점 검사 & 시각화

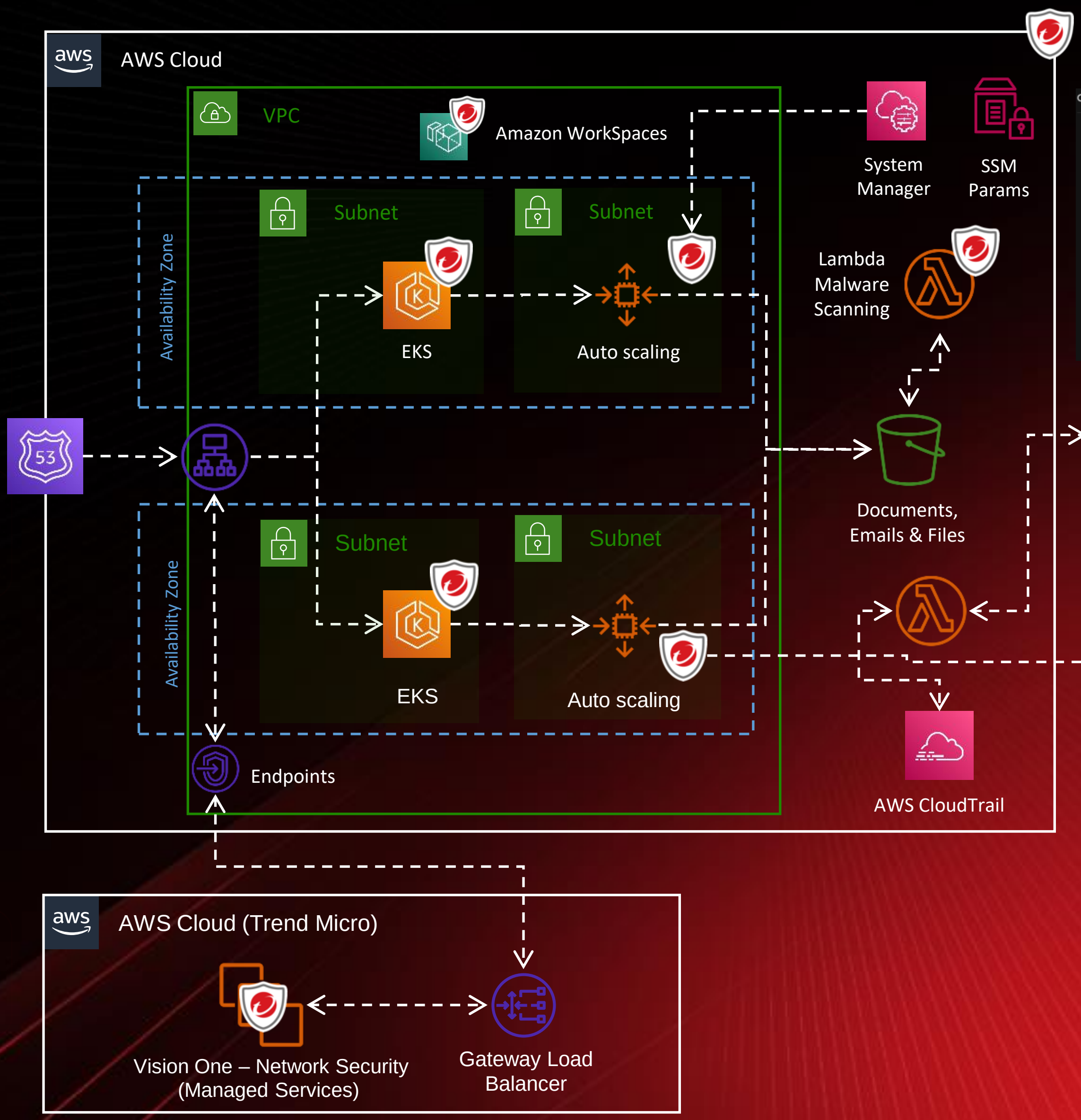




Kubernetes 외에도 Amazon ECS를 지원하도록 확장된 취약성 검사를 통해 고객은 컨테이너 환경을 보호하기 위한 사전 조치 가능

클라우드 고객을 위한 상호 보완적 보안(AWS Case)

- 컨테이너 런타임 보호
- 자동화된 EDR 에이전트 배포
- 보안 규정 준수 목표를 위한 넓은 보안 범위
- 클라우드 보안 취약 구성 & 컴플라이언스 규칙 매핑
- 서버리스 클라우드 네트워크 IDS/IPS
- Amazon S3를 위한 클라우드 네이티브 멀웨어 검사
- 기업의 보안적 위험 감사를 위한 통합적 XDR 연계



AWS Well-Architected

Trend Vision One XDR Platform

- Antimalware + Web reputation
- Firewall
- Device control
- App control
- IPS (Desktop OS)
- EDR/XDR
- IPS (Server applications)
- Integrity monitoring / Log inspection
- Container protection
- SAP scanner (add-on)

TREND MICRO™ | Global Leader in Cybersecurity

김석주 이사

Anthony_kim@trendmicro.com

트렌드마이크로