SDDC/Cloud 애널리틱스를 위한 최상의 선택 Tetration 애널리틱스

시스코 코리아

한정엽 차장

목차

- 데이터센터 운영 트렌드
- 테트레이션 애널리틱스 소개
- 구축 옵션
- 요약

데이터센터 운영 트렌드

안전한 데이터센터 운영

점점 복잡해지는 어플리케이션

빨라지는 어플리케이션 배포 주기

CI/CD 적용
어플리케이션 모빌리티
마이크로 서비스

보안 정책 강화

이기종 네트워크
제로-트러스트 보안
정책/규정 준수

어플리케이션이 데이터센터 인프라 주도

서버 보호에 대한 전반적인 접근

테트레이션 애널리틱스 소개

테트레이션 – 활용사례

고객측면에서 활용 방안

마이그레이션

- 데이터센터 이전
- 어플리케이션 마이그레이션
- 데이터베이스 마이그레이션

작업 검증

- PM 작업 이후 서비스 점검
- 어플리케이션 변경 자동 감지
- 네트워크 성능 모니터링

방화벽/ACL룰

- 데이터센터간 방화벽/ACL 룰 설정
- ACL룰 적용전 사전 검증
- 방화벽 전체 룰 검증

컴플라이언스

- 사내 규정 준수 여부 파악
- 과거 이력 조회 (최대 1년)
- 품질 지표 확인 (개발/운영 분리)

Tetraition 플랫폼 아키텍처

웹 GUI

REST API

이벤트
노티피케이션

Cisco
Tetration apps

데이터 콜렉션 레이어

소프트웨어 센서와
인포스먼트

네트워크 센서

ERSPAN 센서

Netflow 센서

Cisco Tetration

애널리틱 엔진

써드 파티 소스
(configuration data)

테트레이션 데이터소스

소프트웨어 센서

Virtual, Bare metal and Containers

- 리눅스 서버
- 윈도우즈 서버
- 윈도우즈 데스크탑
- Container host

네트워크 센서

Next-generation Cisco Nexus® Series Switches

- Cisco Nexus 9300 EX
- Cisco Nexus 9300 FX

기타 센서

Other types of sensors

- ERSPAN 센서
- Netflow 센서

*Telemetry augmentation only

Main features

- ✓ 낮은 CPU 오버헤드 (SLA enforced)
- ✓ 낮은 네트워크 오버헤드
- ✓ Enforcement 기능 (소프트웨어 에이전트)
- ✓ 페이로드를 제외한 모든 플로우(샘플링 아님)
- ✓ 서버 프로세스와 소프트웨어 패키지 정보

사용자가 추가한 태그 지원

테트레이션에서 식별된 인벤토리

Cisco Tetration Analytic
텔리메트리 데이터

VMware vCenter
(VM 태그)

AWS
(AWS 태그 연동)

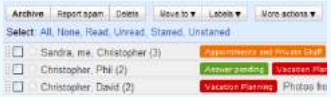
Kubernetes와 Openshift
(container 지원)

인벤토리와 메타데이터 업로드

사용자 태그와 인벤토리 머지

실시간 인벤토리 트랙킹

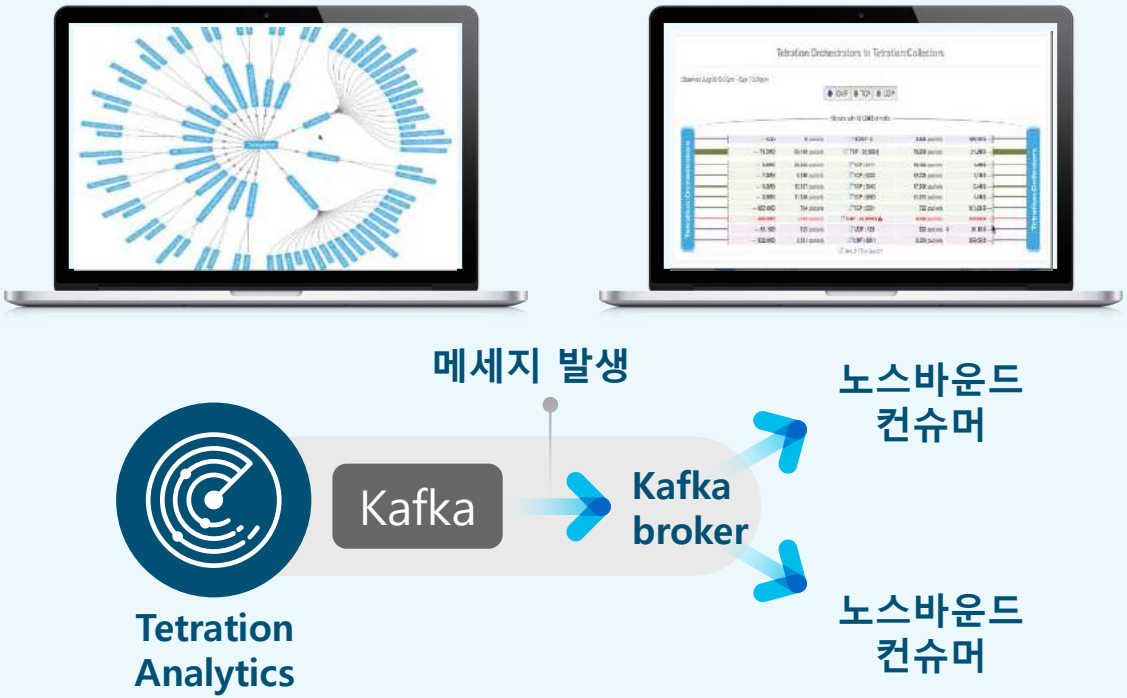
시간 순서대로 쌓인 플로우 데이터와 실시간 인벤토리 데이터 매칭



연결된 네이버후드 그래프

네이버후드 그래프

- 선택된 워크로드에 대한 최대 2홉까지의 이웃 탐색
- 이웃간 통신 상세보기
- 그래프 데이터베이스를 이용한 뷰 대쉬보드 제공
- 두 워크로드간의 서버 홉 계산
- Kafka를 통한 알림 제공

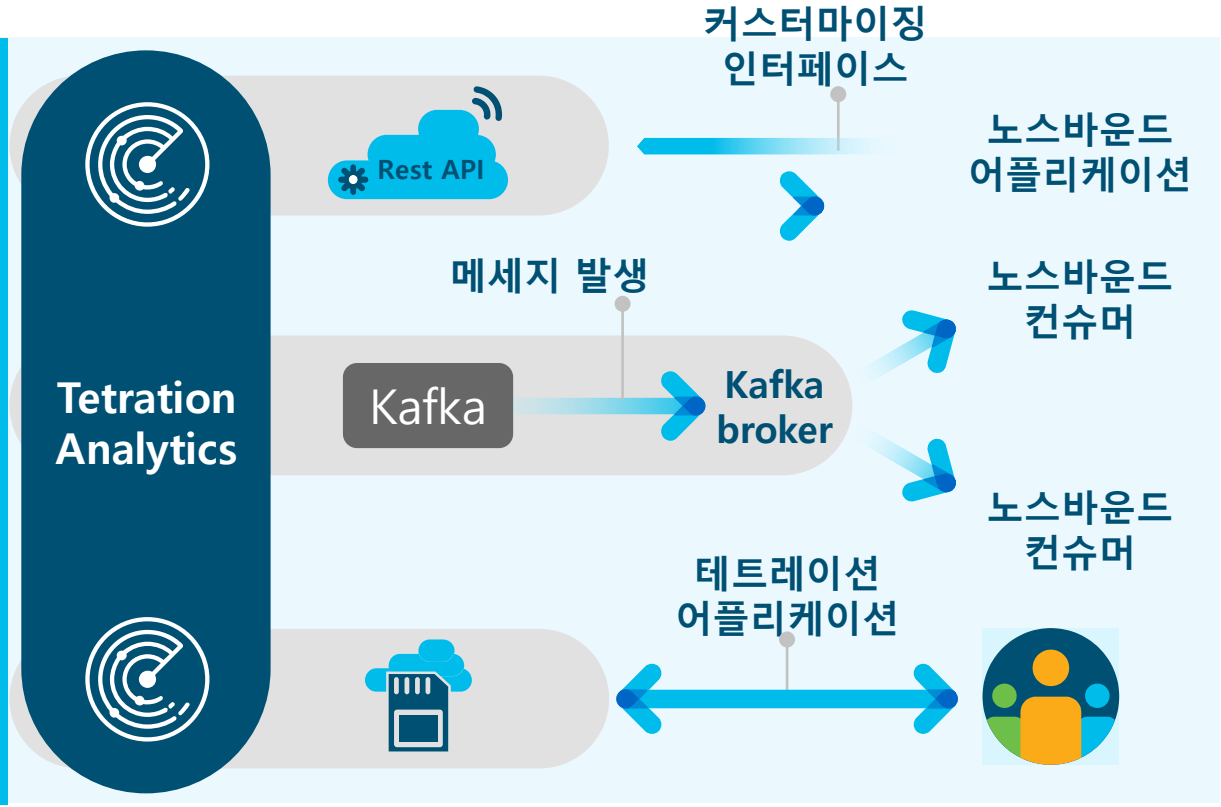


오픈 API 지원

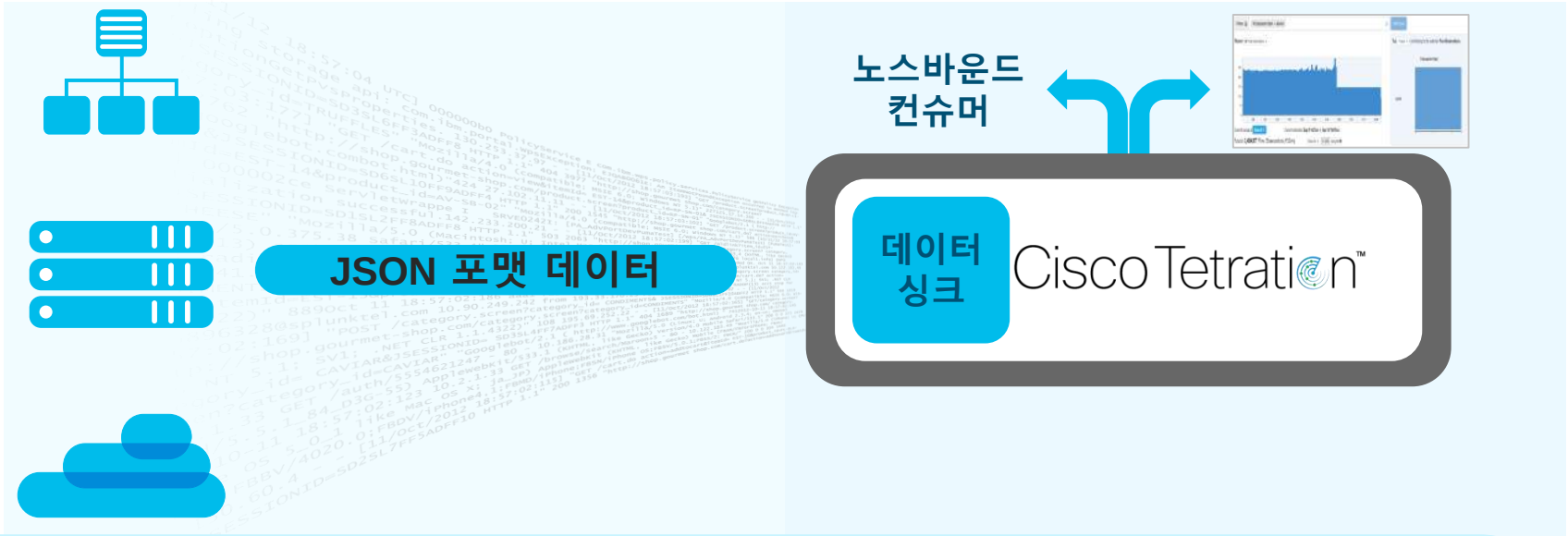
REST API
- 플로우 및 어플리케이션 검색
- 센서, 인벤토리 및 태그 관리

Push notification
- 기본 시스템 이벤트
- 사용자 정의 이벤트

테트레이션 앱
- 시스코/파트너 제공 앱 사용
- 데이터 레이크 접근
- 필요시 어플리케이션 개발 가능



다양한 고객 데이터 수용



Main features

- ✓ 장비에서 JSON기반 텔레메트리 데이터 전달
- ✓ 최대 10개 스트리밍 지원
- ✓ 스트리밍 시간 당 최대 5GB 지원
- ✓ 통지 앱 및 UI를 통한 데이터 분석 지원

Tetration Analytics 특징

네트워크 인사이트

어플리케이션 인사이트

워크로드 프로텍션

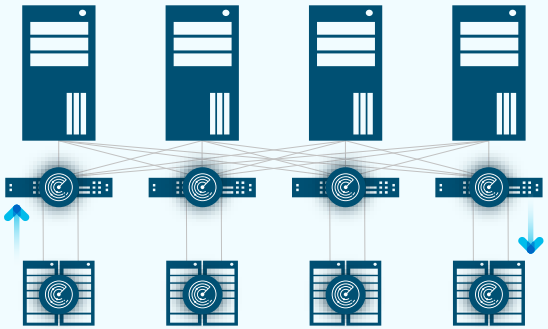
Tetration Analytics 특징

네트워크 인사이트

어플리케이션 인사이트

워크로드 프로텍션

성능 모니터링 (소프트웨어 센서)

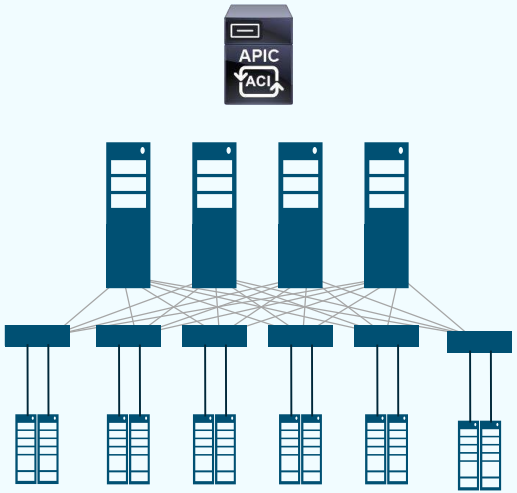


Tetration Analytics

서버 설치된 호스트 센서를 통한 성능 모니터링 기능 제공

- 어플리케이션 성능 이슈
- 네트워크 성능
- 추가된 TCP 메트릭
- 마이크로 버스트 감지

성능 모니터링 (Tetration + ACI)



Tetration Analytics

Nexus 9300 FX Leaf 스위치와 FX Spine 라인카드 조합의 Cisco ACI를 활용

- 네트워크 포톨로지 변경 추적
- 시계열 트래픽 플로우 정보 제공
- 시계열 링크 및 큐 정보 제공
- 추가 플로우 탐색 기능

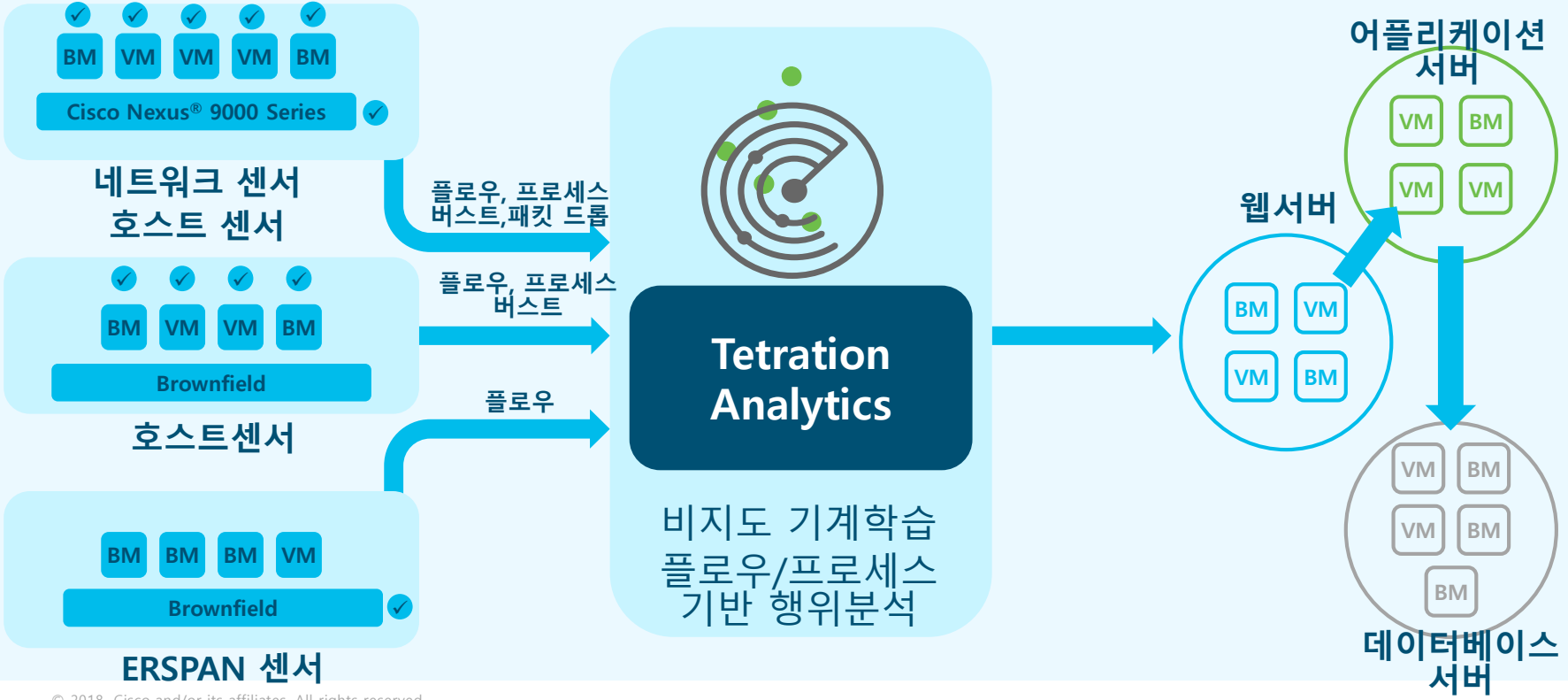
Tetration Analytics 특징

네트워크
인사이트

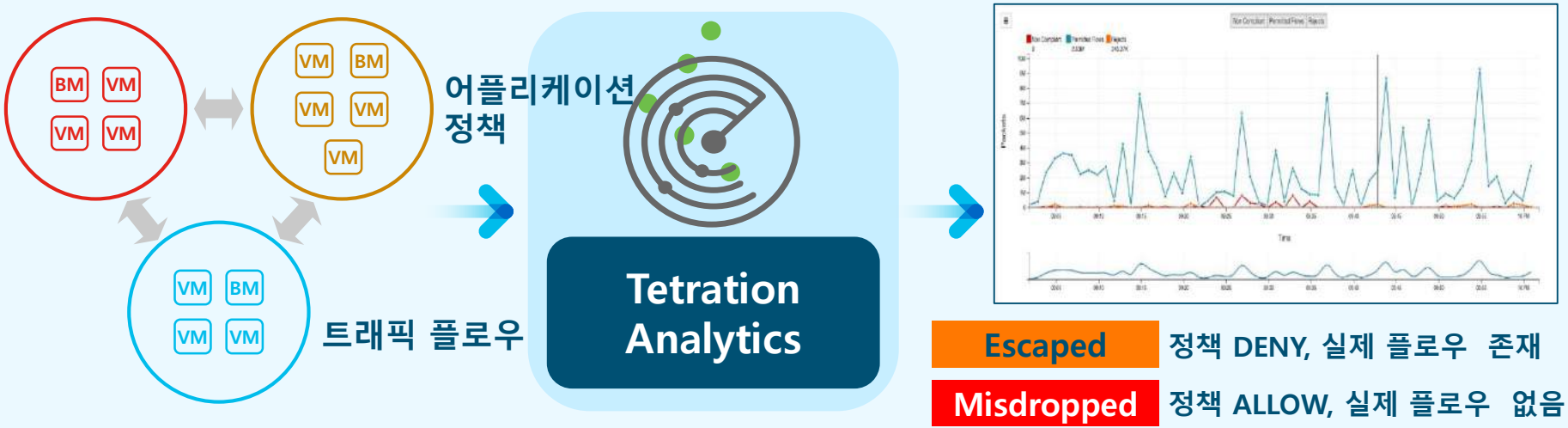
어플리케이션
인사이트

워크로드
프로텍션

어플리케이션 의존관계 파악



정책 시뮬레이션 및 영향도 분석

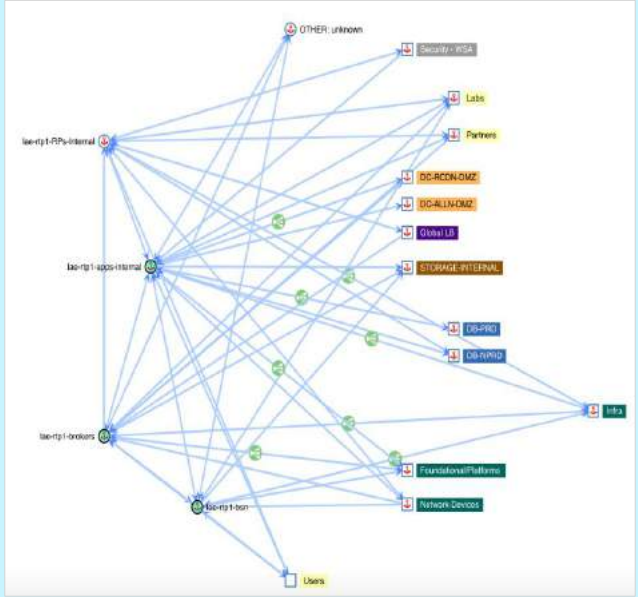


Main features

- ✓ 실시간 트래픽에 대한 정책 검증 및 영향도 분석
- ✓ 과거 데이터를 통한 정책 변화 영향도 분석
- ✓ 특이 트래픽 파악
- ✓ 기계학습기반 감사 기능

화이트 리스트 정책 생성

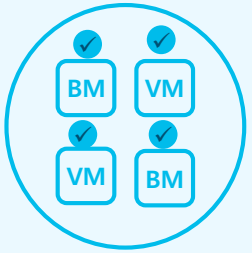
어플리케이션 의존관계



화이트 리스트 정책 (JSON,XML,YAML)

```
{
  "src_name": "WAS서버",
  "dst_name": "웹서버",
  "whitelist": [
    {
      "port": [0, 0],
      "proto": 1,
      "action": "ALLOW"
    },
    {
      "port": [80, 80],
      "proto": 6,
      "action": "ALLOW"
    },
    {
      "port": [443, 443],
      "proto": 6,
      "action": "ALLOW"
    }
  ]
}
```

호스트 센서 방화벽 / 네트워크 장비



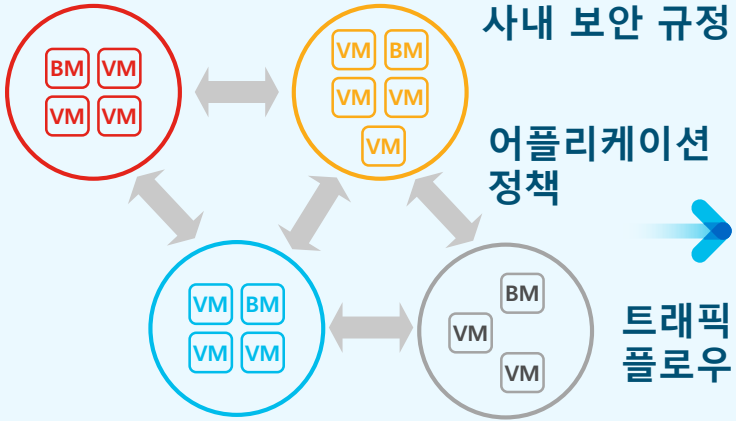
algosec
Security Management at the Speed of Business

tufin

ASA

PaloAlto

정책 준수 모니터링

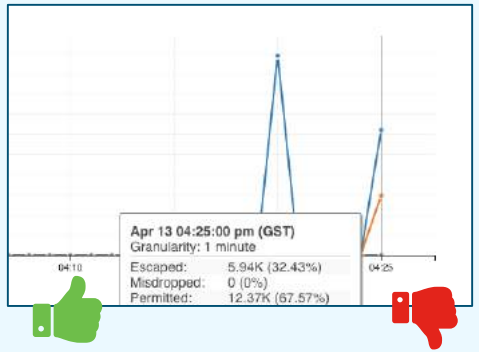


사내 보안 규정

어플리케이션 정책

트래픽 플로우

Tetration Analytics



Kafka 브로커

보안 요약 앱

정기적 보안 리포팅 앱

Main features

✓ 사내 규정 수립
(예, 알려진 서비스 포트 변경)

Main features

✓ 정책 준수 여부 파악
(업무별, 담당자별 통보)

✓ 지속적인 정책 관리

✓ (정책 수립 및 집행에 대한 가시성)

Tetration Analytics 특징

네트워크
인사이트

어플리케이션
인사이트

**워크로드
프로텍션**

하이브리드 클라우드 워크로드 프로텍션

커뮤니케이션 제어

- 애플리케이션 동작에 기반한 자동 화이트리스트 정책
- 세분화를 가능하게하는 정책 시행
- 정책 준수 추적
- 이상치 탐지

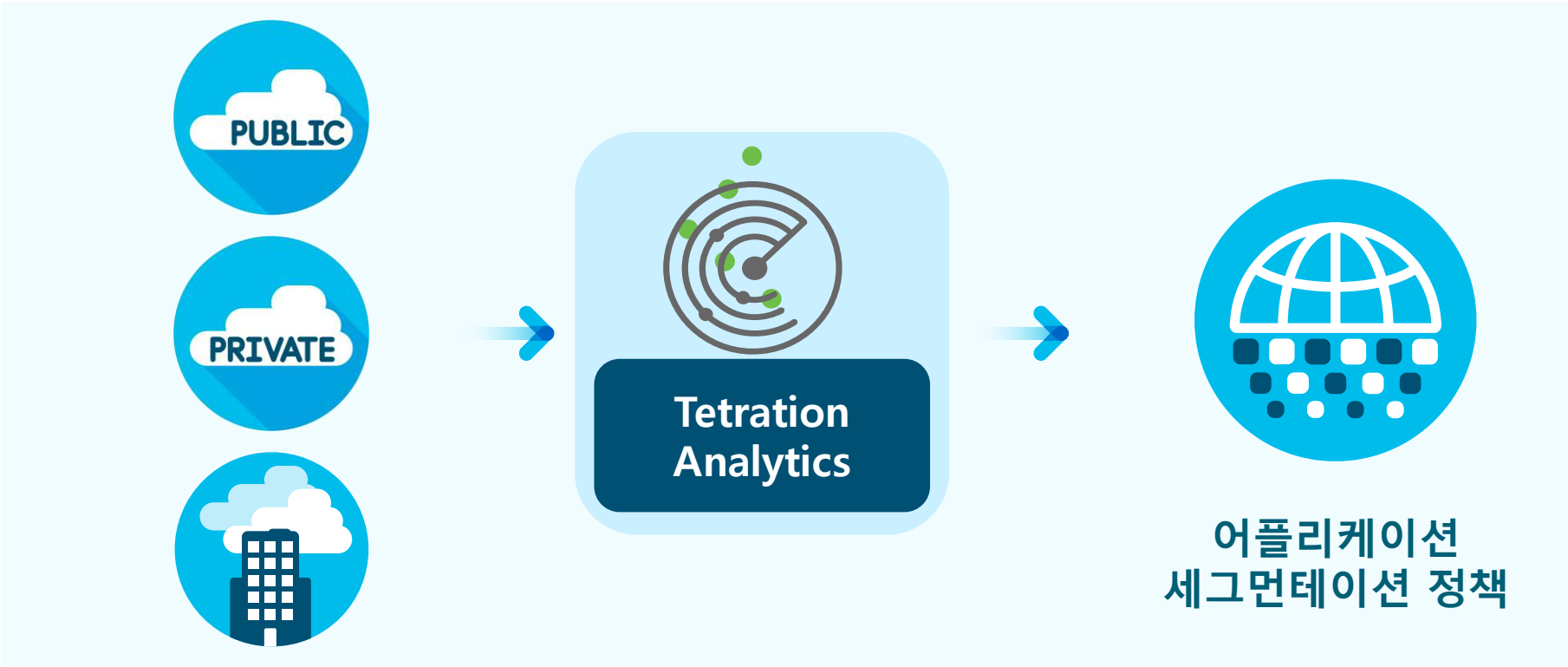
어플리케이션 행위 감지

- 프로세스 해시, 속성 처리
- 새 명령, 새 사용자
- 계정 수정 권한 상승
- 셸 코드 실행

취약성 감지

- 설치된 패키지 추적
- 매주 CVE 추적
- 취약점 스코어링
- 위협 정보 수집

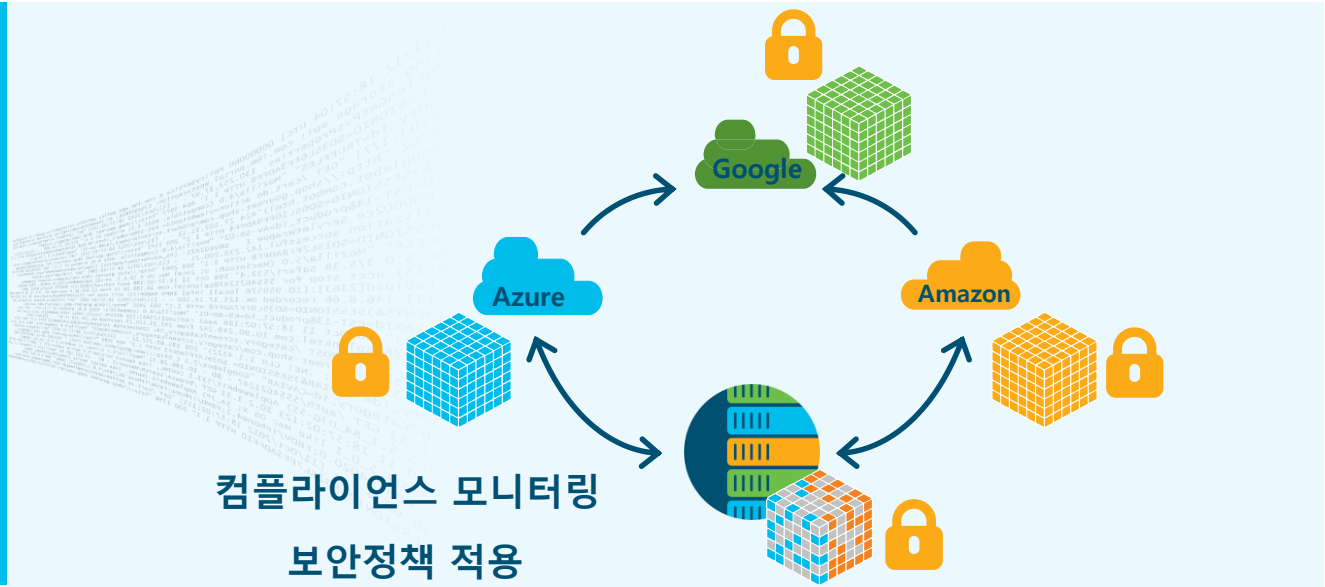
어플리케이션 세그멘테이션 – 정책 추천



다양한 환경에 대한 보안 정책 적용

Tetration Analytics

1. 워크로드별 정책 생성
2. 정책을 모든 워크로드에 적용
3. 워크로드 내부에서 정책 적용
4. 지속적으로 정책 재생성 (선순환)



Public cloud

Bare metal

Virtual

Cisco ACI

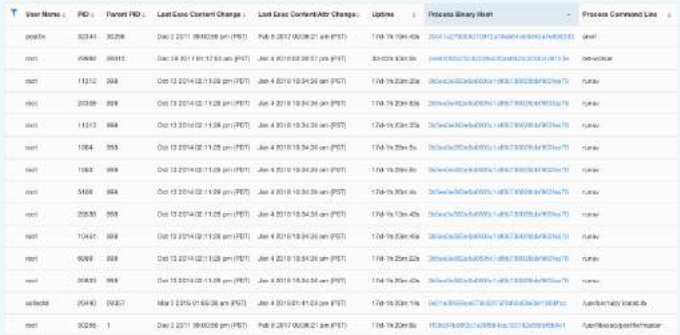
Traditional network

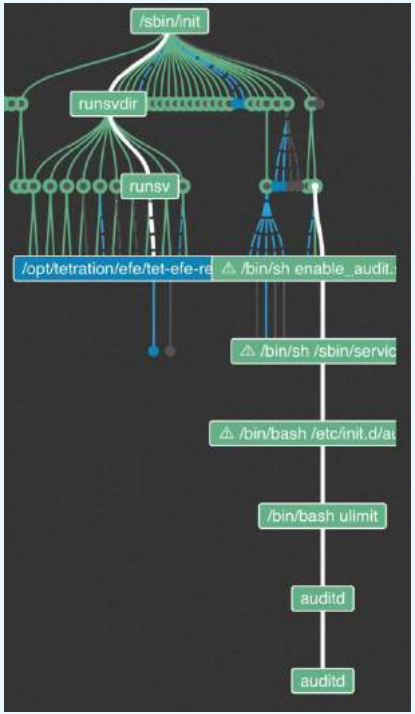
서버 프로세스 분석

Tetration Analytics

1. 수집 되는 프로세스 인벤토리
   - 프로세스 이름
   - 프로세스 ID
   - 사용자 정보
   - 프로세스 실행 정보
   - 프로세스 해시(시그니처)
2. 특정 프로세스 및 프로세스 해시값을 통한 검색

3. 프로세스 스냅샷



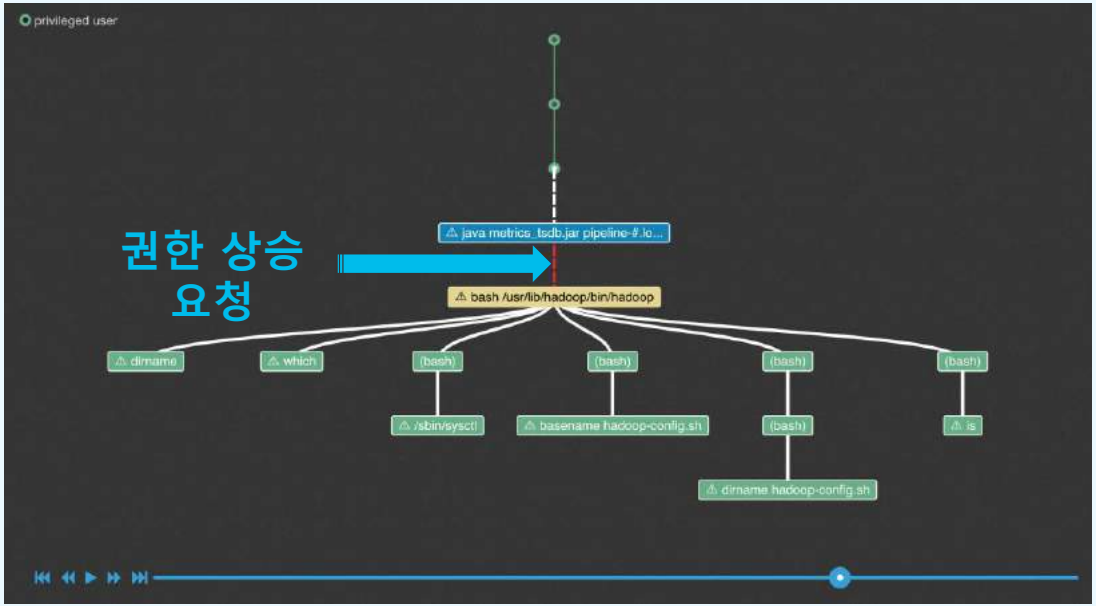


이상 행위 프로세스 식별

Tetration Analytics

1. 프로세스 동작 편차와 멀웨어 동작 패턴을 의심되는 활동과 연결

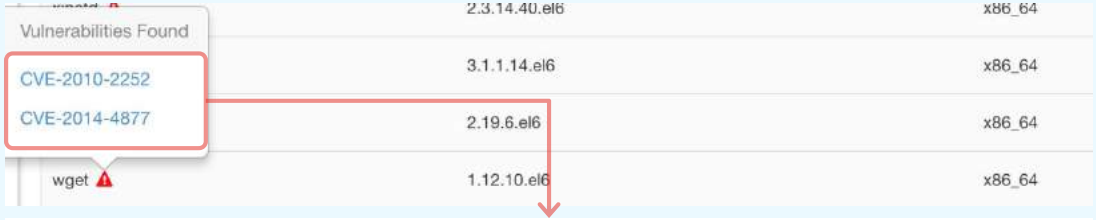
2. 프로세스 이벤트 분석
   - 권한 상승 요청
   - 쉘코드 수행
   - 사이드 채널 공격



서버 소프트웨어 취약점 분석

Tetration Analytics

1. 서버에 설치된 소프트웨어(패키지) 취약점 조사
   - 패키지 이름
   - 버전 정보
   - 배포자
2. 취약점 상세 정보 (0 ~ 10)
3. 취약점 수준에 따른 조치
   - 호스트센서 정책



Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 HIGH
Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

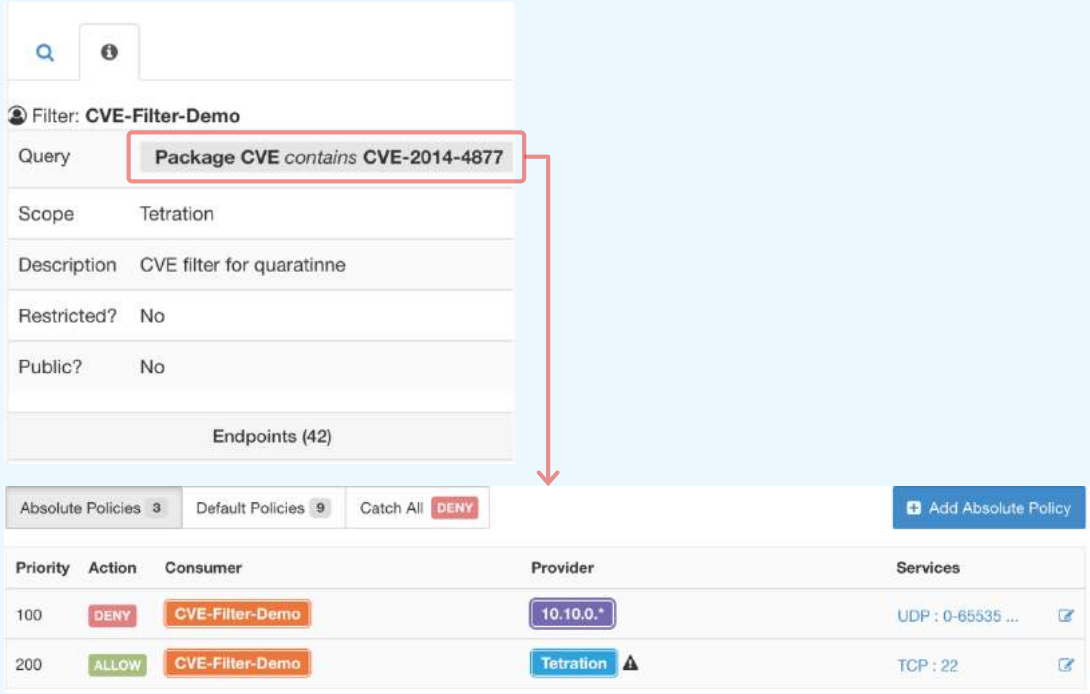
Access Vector: Network exploitable
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

소프트웨어 취약점 분석 - 액션

Tetration Analytics

1. 취약점을 검색하는 필터 설정

2. UI 또는 API를 통해서 액션을 수행할 수 있도록 정책 설정
   - 호스트에 취약점이 존재하는 검역소 정책적용



구축 옵션

온-프레미스 구축 옵션

온-프레미스 어플라이언스

Cisco Tetration™ Platform (large form factor)

- 최대 25,000 워크로드
- 이중화 기반 아키텍처

Includes:

- 39U
- UCS C220 x 36대
- Nexus 9300 스위치 x 3대

Cisco Tetration-M (small form factor)

- 5,000 워크로드 미만
- 이중화 기반 아키텍처

Includes:

- 8U
- Cisco UCS C220 x 6대
- Nexus 9300 스위치 x 2대

버추얼 어플라이언스

Cisco Tetration Virtual(Tetration-V)

- 1,000 워크로드 미만
- VMware ESXi 기반 환경 또는 AWS과 Azure(퍼블릭 클라우드)
- 고객의 퍼블릭 클라우드 인스턴스 사용
- ESXi 기반 배포용 시스템 사양 (CPU 코어, 메모리, 스토리지 등)

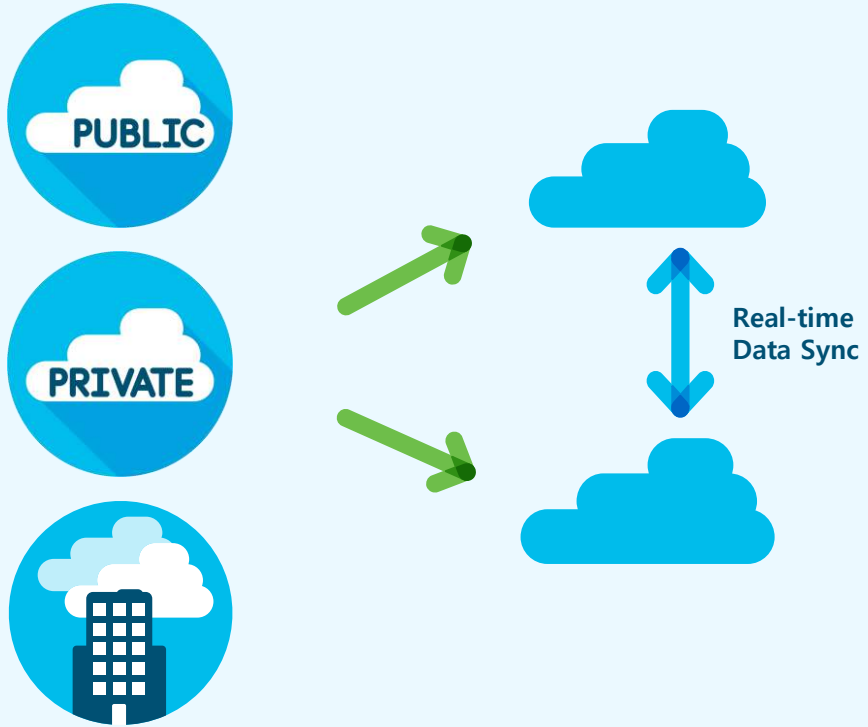
Amazon Web Services

Microsoft Azure

Tetration software-as-a-service(TaaS) 옵션

Tetratio SaaS

- Software-as-a-service 모델: 하드웨어나 소프트웨어를 구매, 설치 및 관리할 필요 없음
- Cisco가 완벽하게 관리하고 운영
- SMB 고객이나 SaaS-first/SaaS-only 고객에게 적합
- 유연한 가격 책정 모델
  (진입 장벽 낮음)
- 최대 25,000 워크로드



요약

대규모 데이터 및 유연성을 제공하는 분석 플랫폼

실시간 및 확장성

- 모든 패킷, 플로우
- 어플리케이션 세그멘테이션 지원
- 최대 1년간 데이터 유지

섬세한 정책 적용가능

- 일관성 있는 정책 적용
- 실시간에 가깝게 정책 변화 감지
- 워크로드 이동성 제공

사용 편의성

- 원-터치 구축
- 자가 모니터링
- 자가 진단

개방성

- HTML5 웹 사용자 인터페이스
- REST API
- 이벤트 Notification
- 테트레이션 앱


CISCO