데이터센터 네트워크 애널리틱 솔루션
Cisco Tetration Analytics

한정엽 과장, 시스코 코리아

시스코 데이터센터 서밋 2017

목차

1. 데이터센터 동향 및 요구사항
2. Streaming Telemetry
3. Cisco Tetration Analytics
4. Tetration 주요 기능
5. Summary

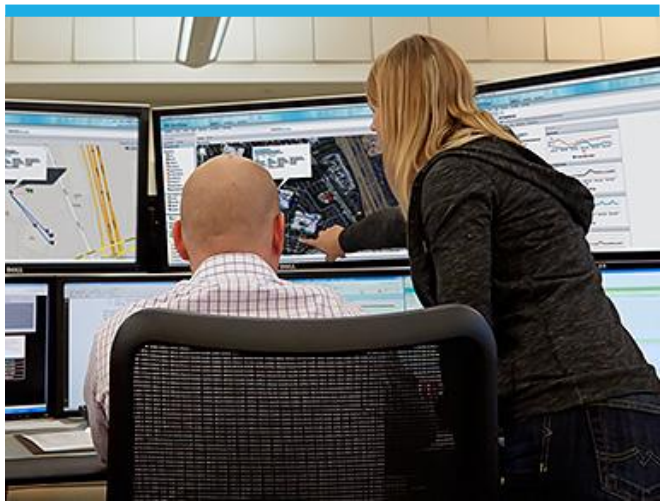
점점 더 복잡해지는 오늘날의 데이터 센터

빅 데이터와 패스트 데이터

East-West 트래픽 증가

확장된 공격 표면

오픈 소스



하이브리드 클라우드

제로 트러스트 모델

멀티클라우드
오케스트레이션

애플리케이션 이동성

신속한 앱 구축

지속적인 개발

애플리케이션 모빌리티

마이크로 서비스

고객이 새로운 접근방식을 필요로 하는 분야

비즈니스 정책
추진을 위한
IT 투자 매핑

1

조직간
장벽 극복

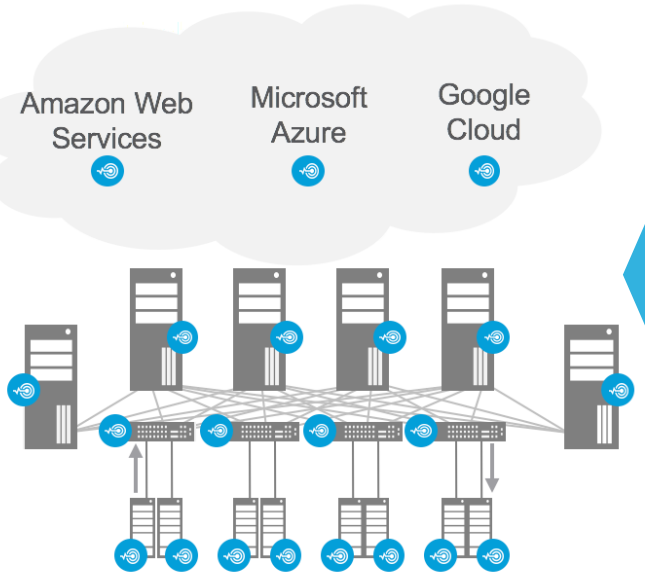
2

공격자 및
재해로부터의
위험 완화

3

전통적인 모니터링 방법의 한계

데이터가 생성되는 위치



Non Real time

Incomplete

Scale Issues

SNMP

Syslog

CLI

Unstructured

Subject to Change

SNMP Server

Syslog Collector

Scripts

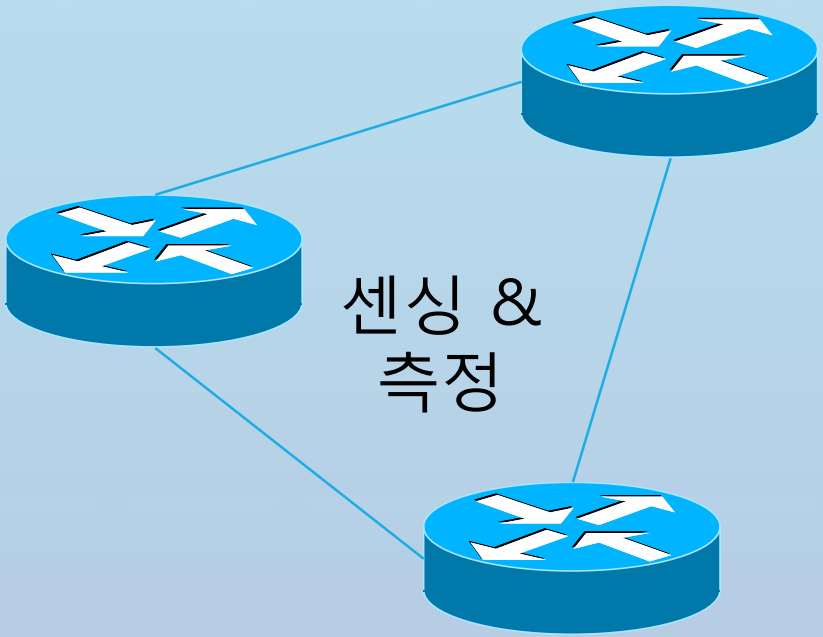
데이터가 유용한 위치

Storage & Analysis

다양한 애플리케이션, 전송,
데이터 모델, 타임 스탬프

Streaming Telemetry 패러다임

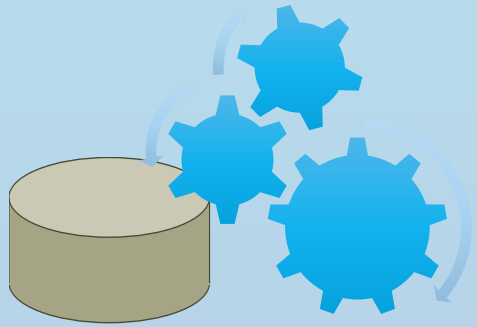
데이터가 생성되는 위치



센싱 &
측정

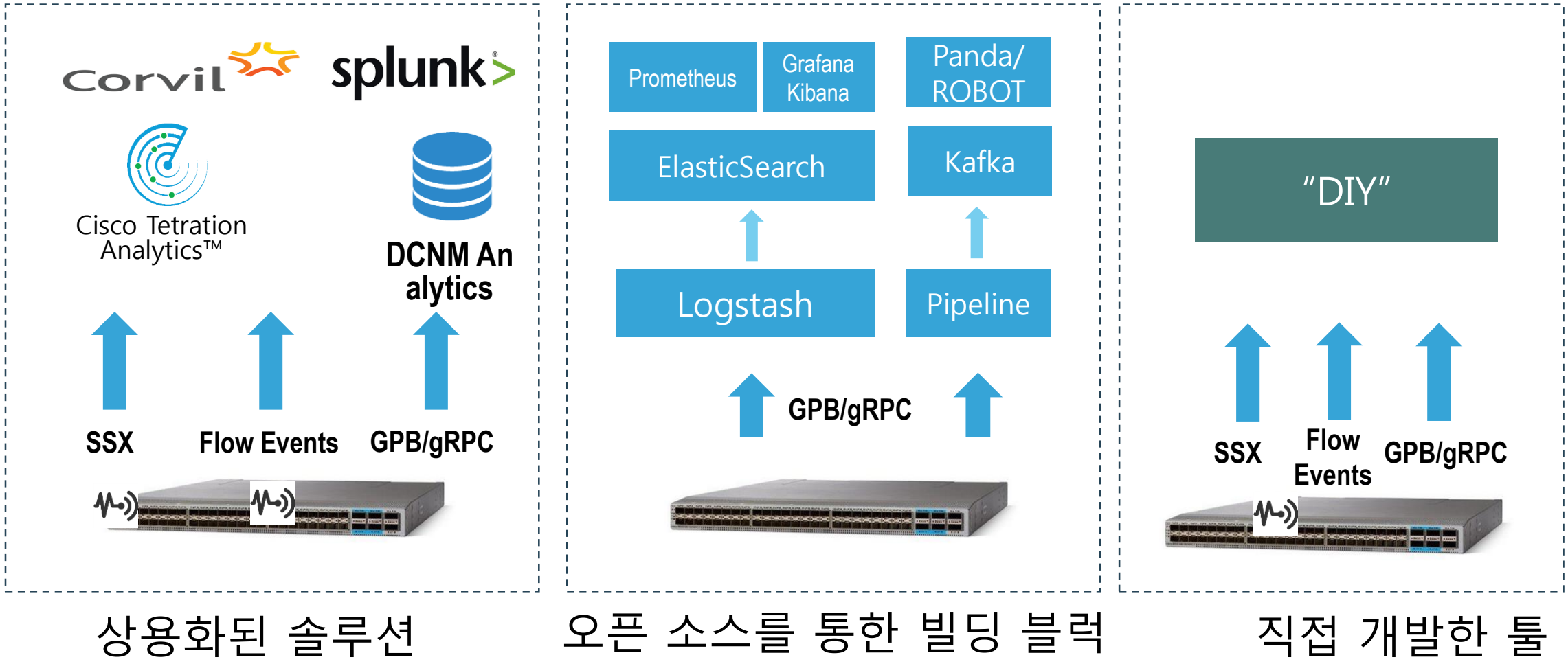
많은 관련 데이터
빠르게
유용하게
쉽게
가능하게

데이터가 유용한 위치



storage &
analysis

Telemetry와 Analytics

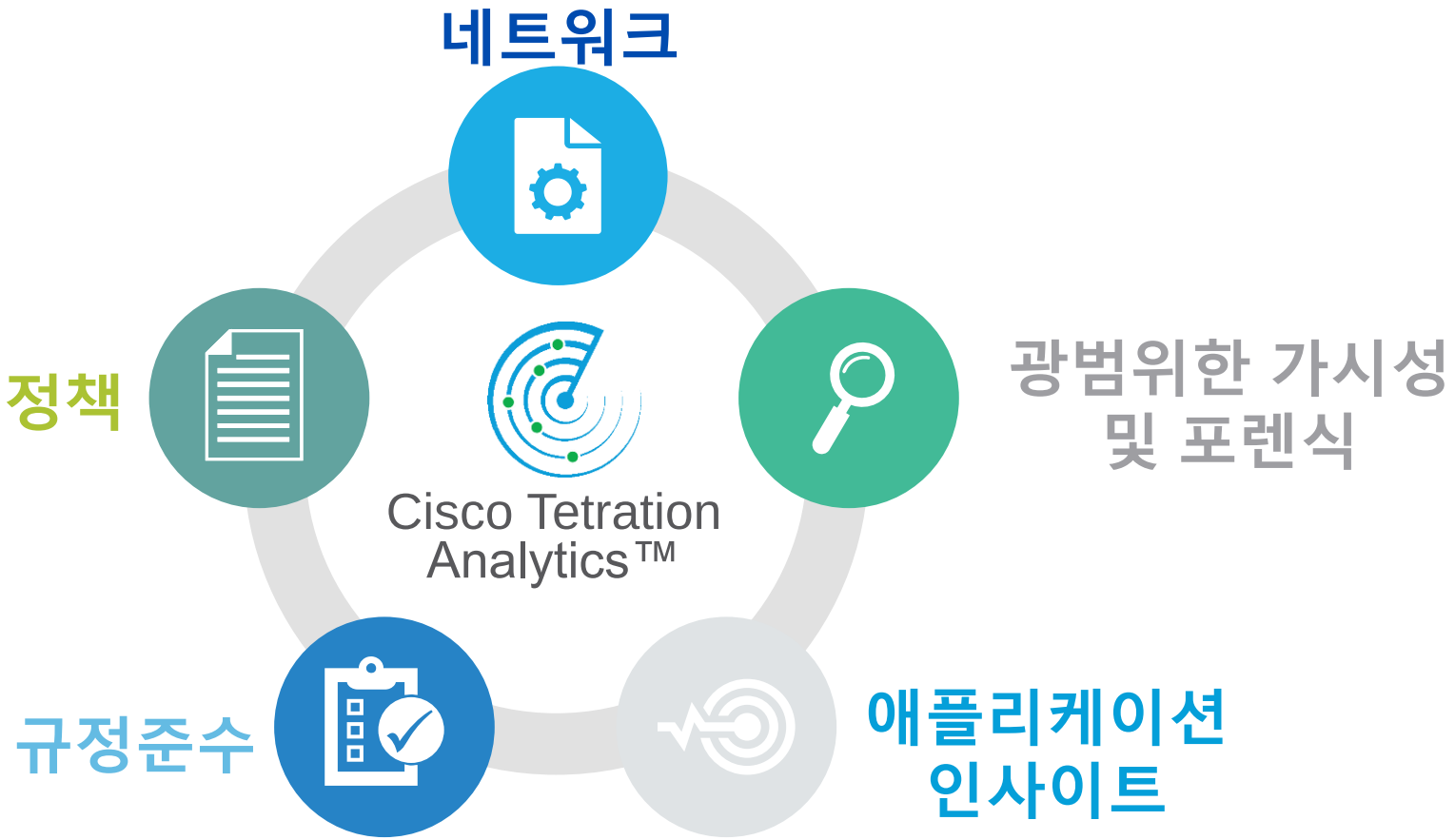


상용화된 솔루션 | 오픈 소스를 통한 빌딩 블럭 | 직접 개발한 툴

Tetration Architecture

시스코 데이터센터 서밋 2017

모든 패킷, 흐름, 속도를 한눈에 파악



Cisco Tetration Analytics

애플리케이션
인사이트

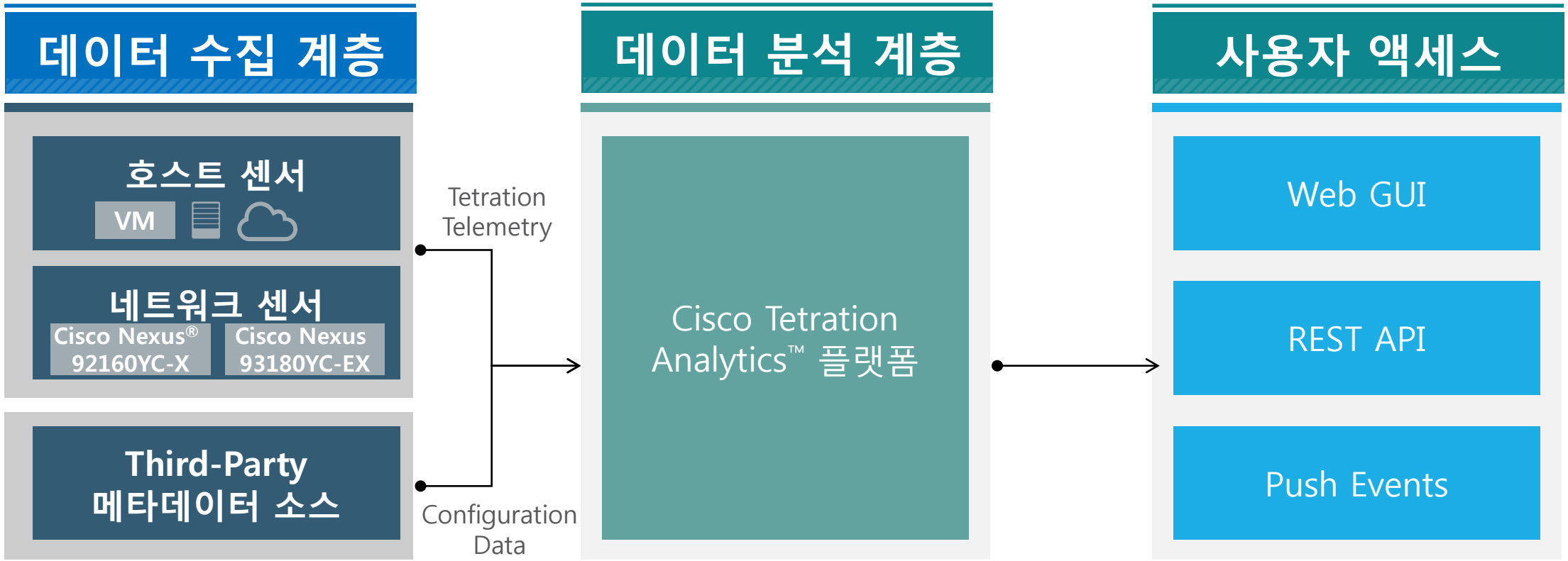
정책
시뮬레이션
및 영향 평가

자동화된
화이트리스트
정책 생성

포렌식:
모든 패킷,
흐름, 속도를
한눈에 파악

정책 규정
준수
및 감사 기능

Cisco Tetration Analytics 아키텍처



ADM
(Application Dependency Mapping)

자동화된 화이트리스트 생성

정책 컴플라이언스 시뮬레이션

포렌식
플로우 탐색 및 이상행위 분석

다양한 센서와 데이터 소스

호스트 센서

- 리눅스 VM
- 윈도우 서버 VM
- 베어메탈 서버 (리눅스/윈도우 서버)
- 하이퍼바이저
- 컨테이너

네트워크 센서

- Nexus 9200-X
- Nexus 9300-EX
- Nexus 9300-FX

서드파티

- Geo
- Whois
- IP Watch Lists
- Load Balancers
- …

FCS에서 지원 | Nexus 9200X 및 9300EX 버전 | 로드맵 예정 | 3rd party 데이터 소스

- ✓ 최소의 CPU 소모 (SLA 적용)
- ✓ 최소의 네트워크 오버헤드 (SLA 적용)
- ✓ 높은 보안성 (코드기반 서명, 인증)
- ✓ 실시간 전체 플로우 , NO PAYLOAD
- ✓ Enforcement Point (소프트웨어 에이전트)

다양한 센서와 데이터 소스 - 호스트센서

지원 OS

- **Windows 2008 & Windows 2008R2**
  Datacenter, Enterprise, Essentials, Standard
- **Windows 2012 & Windows 2012R2**
  Datacenter, Enterprise, Essentials, Standard
- **RedHat Enterprise Server**
  5.3 버전 이상 , 6.x
- **CentOS**
  5.11 버전 이상 , 6.x
- **Ubuntu**
  12.04, 14.04, 14.10

주요 기능

- WinPCAP/libpcap 을 통한 Header 값 추출
- Host 전체 트래픽의 1% 미만 SLA 보장 가능
- FLOW 테이블 포맷으로 메타데이터 전송
- CPU Core당 3% 미만의 점유율
- 설치 시 직접 배포 가능
- 배포 후 Puppet, Chef, Ansible 연동으로 업데이트 가능

다양한 센서와 데이터 소스 – 네트워크 센서의 진화

1세대 9000 시리즈 모델

Nexus 9000 28nm

BROADCOM CISCO

상용칩 + Cisco

Scale
- Encap normalization/ VXLAN Routing 지원

Telemetry
- Atomic Counter 지원
- Latency Metrics 지원

Optimization
- DLB/ Flow Prioritization

Nexus 3000 BROADCOM 40nm

상용칩

2013–2015

2세대 9000 시리즈 모델

Nexus 9000 16nm

CISCO

Cisco ASIC

Scale
- Route/ Host 테이블 확장
- ACI Multi-site 구성 지원
- Enhanced EPG/ SGT/ NSH 지원

Telemetry
- Analytics 지원
- Netflow 지원

Optimization
- Programmability/SDK 확장

Nexus 3000 BROADCOM 28nm

상용칩

2016+

하드웨어 & 소프트웨어 센서 기반의 플로우 분석

소프트웨어 센서

프로세스매핑

프로세스 ID

프로세스 소유자

하드웨어 센서

터널 엔드포인트

버퍼 사용량

버스트 탐지

패킷 드롭

모든 플로우 정보에 대한 분석

무중단 확장이 가능한 플랫폼

실시간 탐지/확장성

모든 패킷, 플로우...

장기간 데이터 보존

데이터센터 전체 탐지

보안

시큐어 디자인

Role 기반 접근

투팩터 인증

손쉬운 사용

원터치 설치 방식

자가 모니터링

자가 진단

개방형

표준 웹 UI

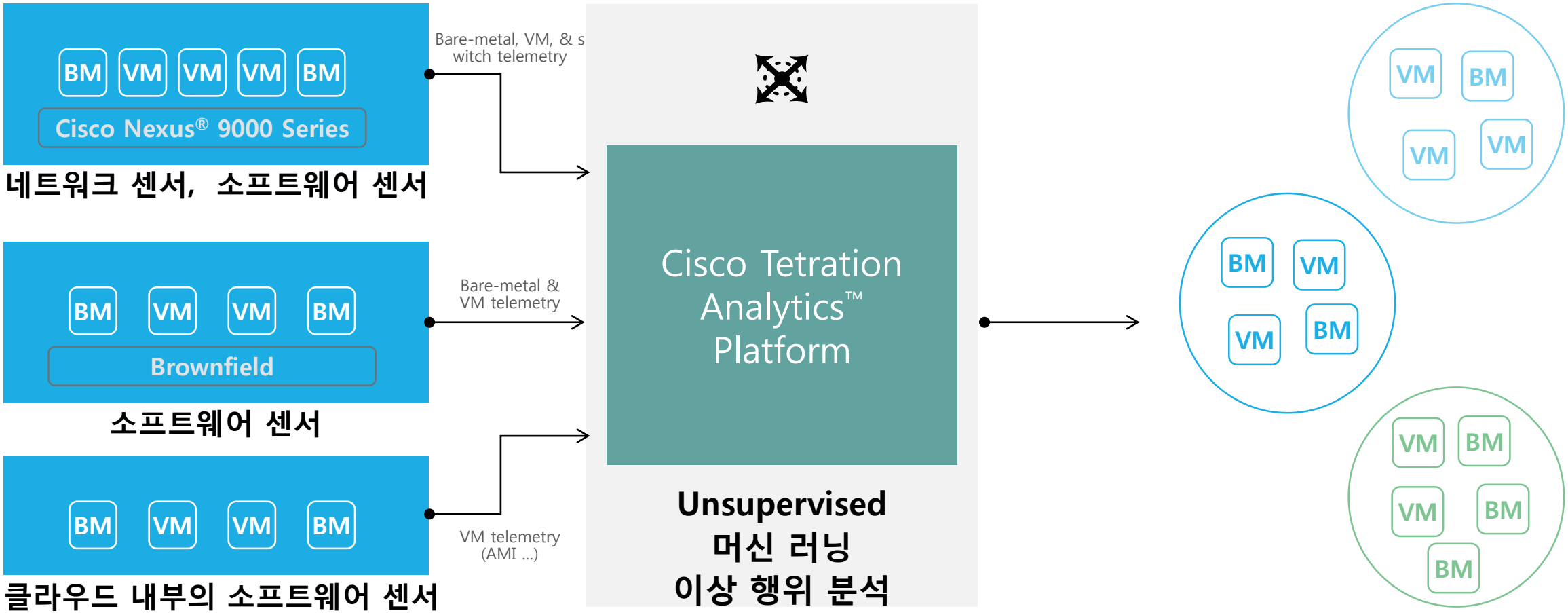
REST API (Pull)

Event Pub/Sub (Push)

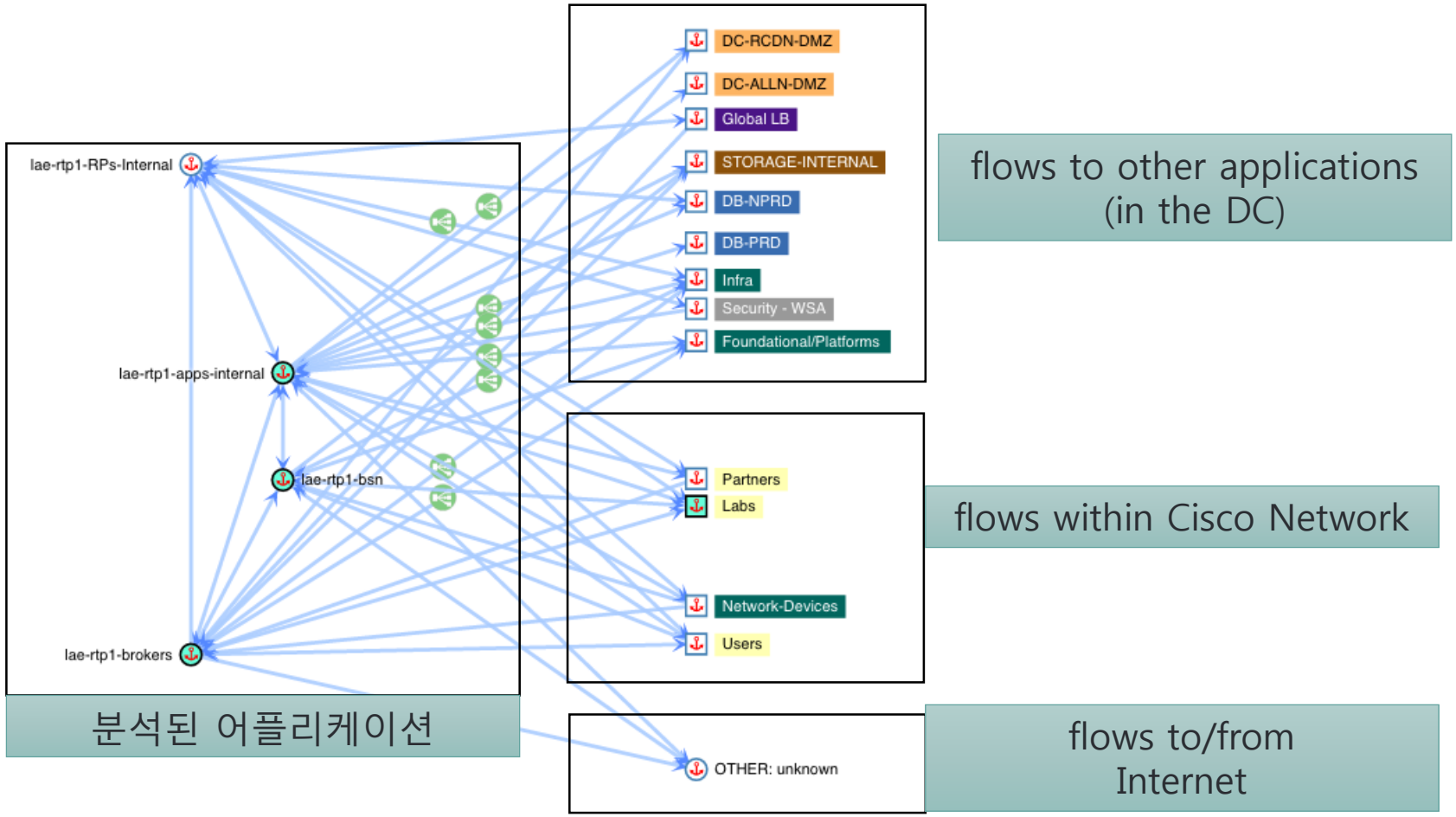
Tetration 주요 기능
ADM /Application Insight

시스코 데이터센터 서밋 2017

Tetration 기반의 어플리케이션 탐색 및 EPG 매핑



실제 네트워크에서 사용 중인 트래픽 확인
Application Insight—Dependency Map



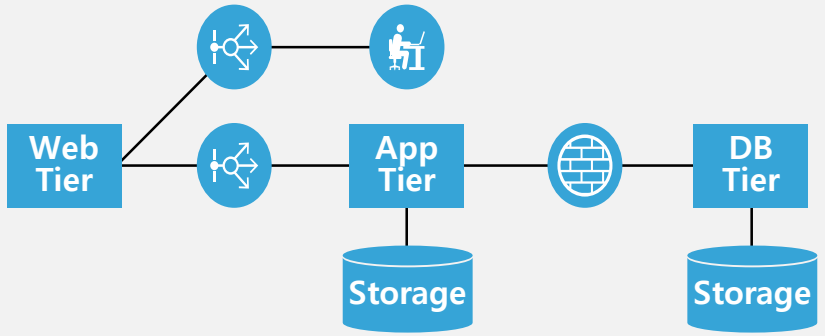
Cisco Tetration 분석 기반의 어플리케이션 서비스 상관관계 분석 제공

Tetration 주요 기능
Policy Compliance

시스코 데이터센터 서밋 2017

화이트 리스트 정책 추천 방식

1. 어플리케이션 디스커버리



2. 화이트리스트 정책 추천
(REST API 적용 가능 - JSON, XML, YAML)

3. 정책 적용
(향후 로드맵)

실시간 정책적용 유효성 탐지

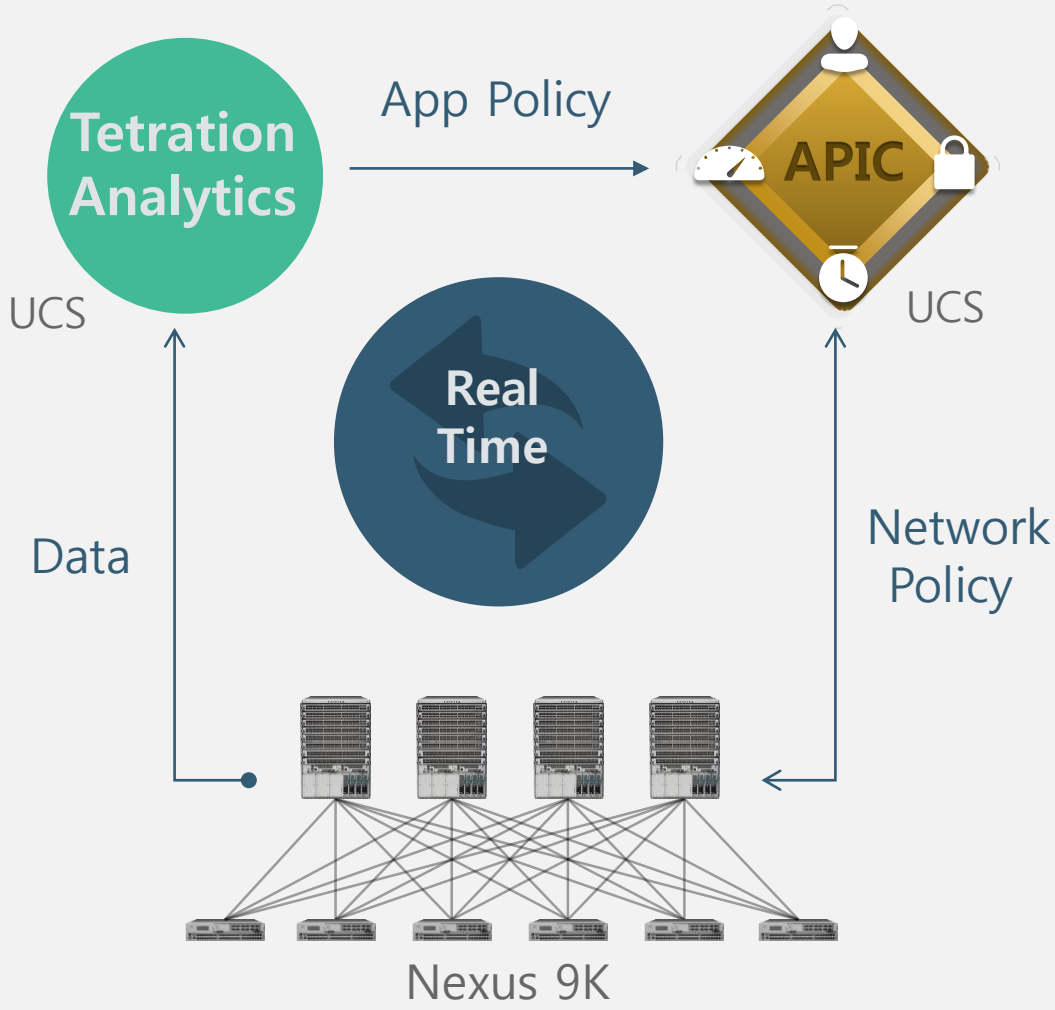
정책 적용 전 시뮬레이션

정책 LifeCycle 관리 기능

향후 ACI와 연동 가능

향후 보안 장비와 연동 가능

ACI와의 최적의 Zero Trust 모델기반 정책 적용



ACI 어플리케이션 정책 추천

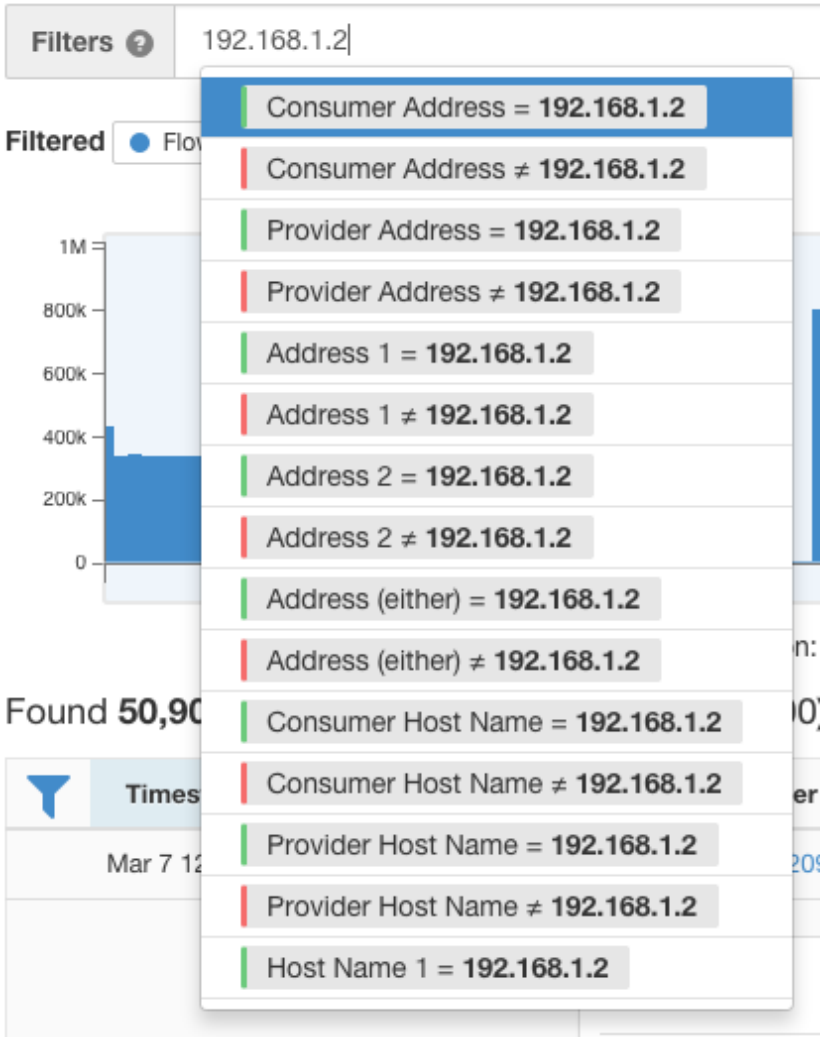
ACI 프로그래머빌리티 기반 정책 적용

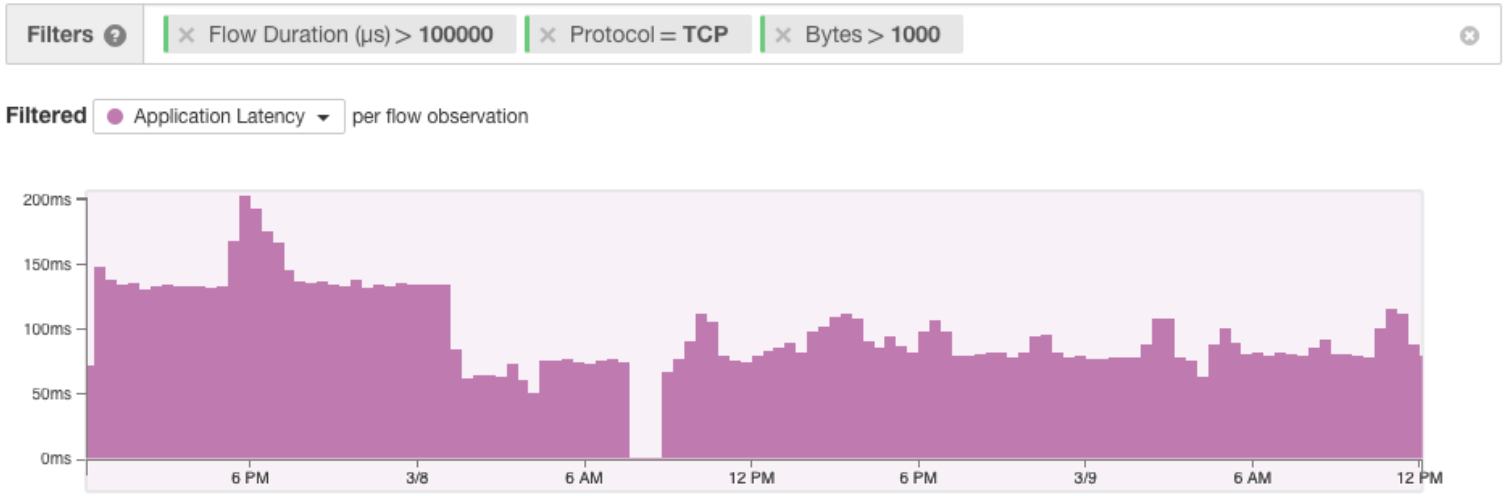
자동화된 ACI EPG, Contract 적용

Tetration 주요 기능
플로우 탐색 및 포렌식

시스코 데이터센터 서밋 2017

데이터센터 전체 트래픽의 가시성 확보



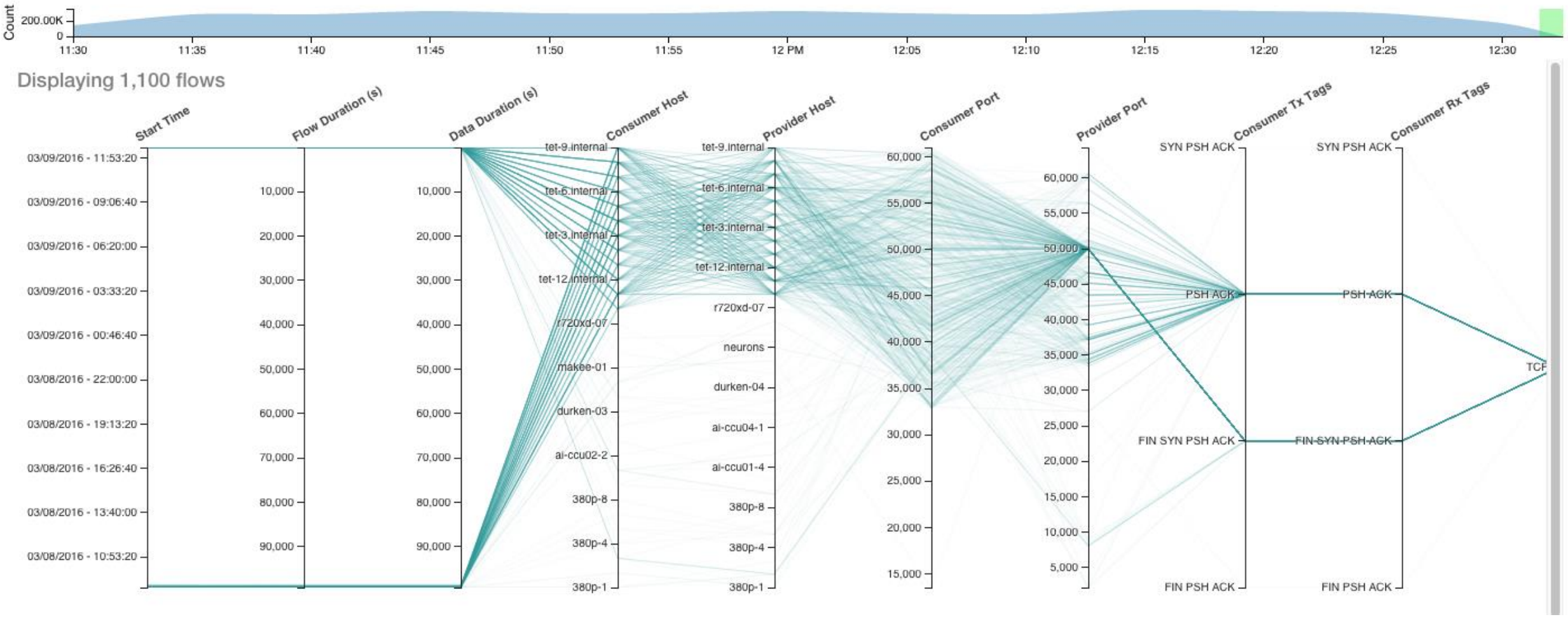


상세 플로우에 대한 시각화 및 포렌식(수집/보존/분석)

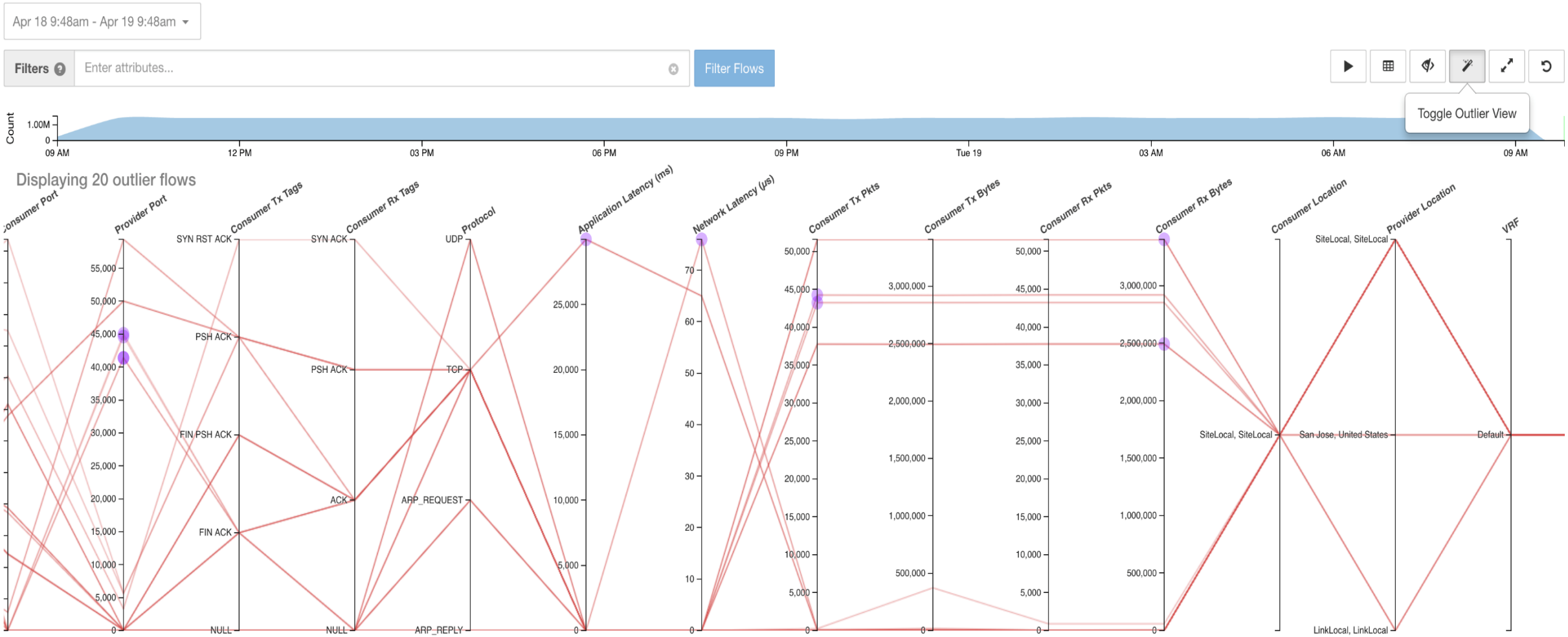
mSec 단위의 상세 분석

과거 데이터에 대한 상세 조회, 분석

데이터센터 내부 과거 트래픽의 조회 및 시뮬레이션



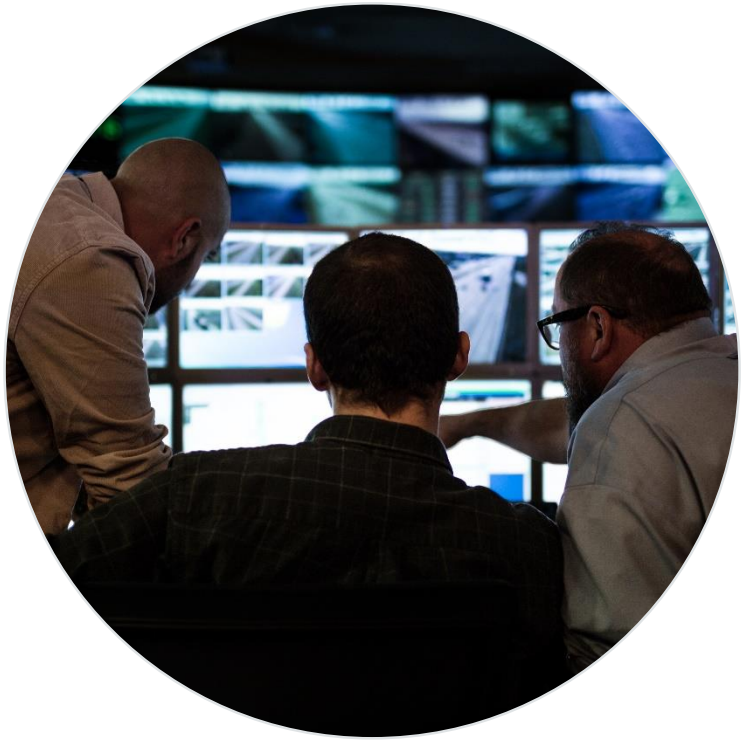
비정상 트래픽에 대한 상세 탐지



Why Tetration?

Cisco Tetration Analytics

조직간 장벽을 허무는 플랫폼



네트워크 운영

정책 규정 준수 및 시뮬레이션
트러블슈팅 및 포렌식
레이턴시 모니터링

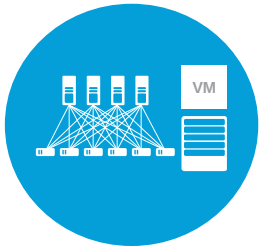
IT 운영 및 LOB(Lines of Business)

애플리케이션 인사이트 및 행동
엔드포인트 행동 위반 사항

보안 운영

화이트리스트 정책 권장 사항
정책 시뮬레이션
정책 규정 준수
향후: 이상 징후 탐지

Why Tetration 입니까?



확장 시
여러 데이터센터에
대한 인프라를
지원하는
광범위한
플로우 텔레메트리

주요 데이터 센터
운영 사용 사례를
지원하는,
즉시 사용가능한
솔루션

셀프 모니터링 및
사내
빅 데이터
전문성 불필요

개방형 플랫폼 및
노스바운드 API로
투명한 통합 지원

도입 가속화
및 포괄적인
솔루션
지원과 서비스

THANK YOU

시스코 데이터센터 서밋 2017