paloalto NETWORKS

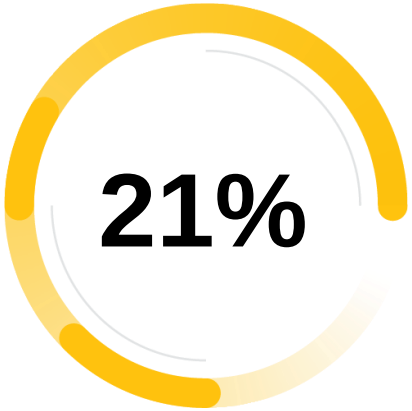
MPIS 2020
Medical Center Privacy Information Security Conference 2020
2020 의료기관 개인정보보호&정보보안 컨퍼런스

의료용 IoT 장비
찾아내고, 보호하고,
최적화 시켜라

IoT – Internet of Things

급증하는 IoT 디바이스

IoT 디바이스 2020



2019년 대비 증가율

일반 기업의 IoT 디바이스 보급률

급증하는 IoT 디바이스

가장 많이 사용되는 IoT 디바이스

Utilities

1.37B

IoT endpoints in 2020

Physical Security

1.09B

IoT endpoints in 2020

가장 큰 성장세를 보이는 IoT 디바이스

42% Building Automation

31% Automotive

29% Healthcare

“

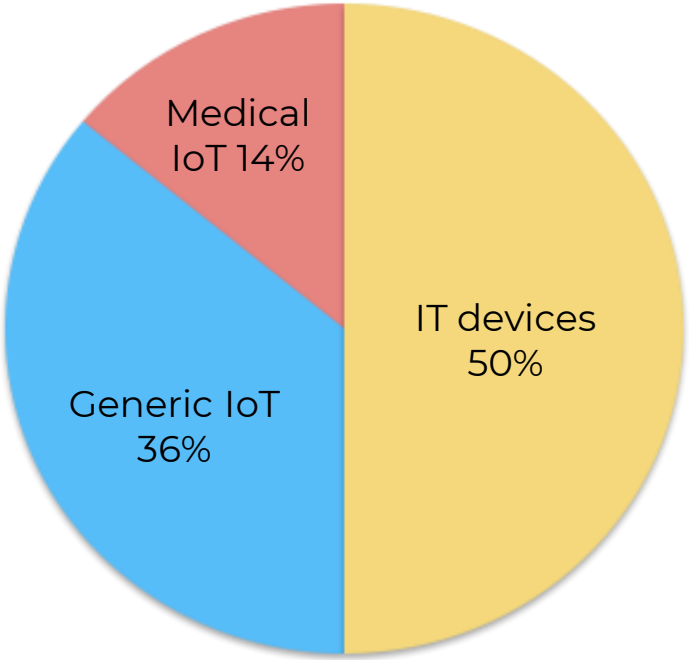
기업들의 75 %가 IoT 보안이 최우선이지만 오직 16 %만이 보안이 준비되었다고 인식

”

McKinsey

Digital McKinsey and Global Risk Practice, March 2019: Perspectives on transforming cybersecurity

의료 IoT 보안 과제



병원 내 장치의 50 %가 제대로 관리되지 않음

의료용 IoT 기기

- Infusion pump (46%)
- Imaging system (19%)
- Patient monitor (17%)

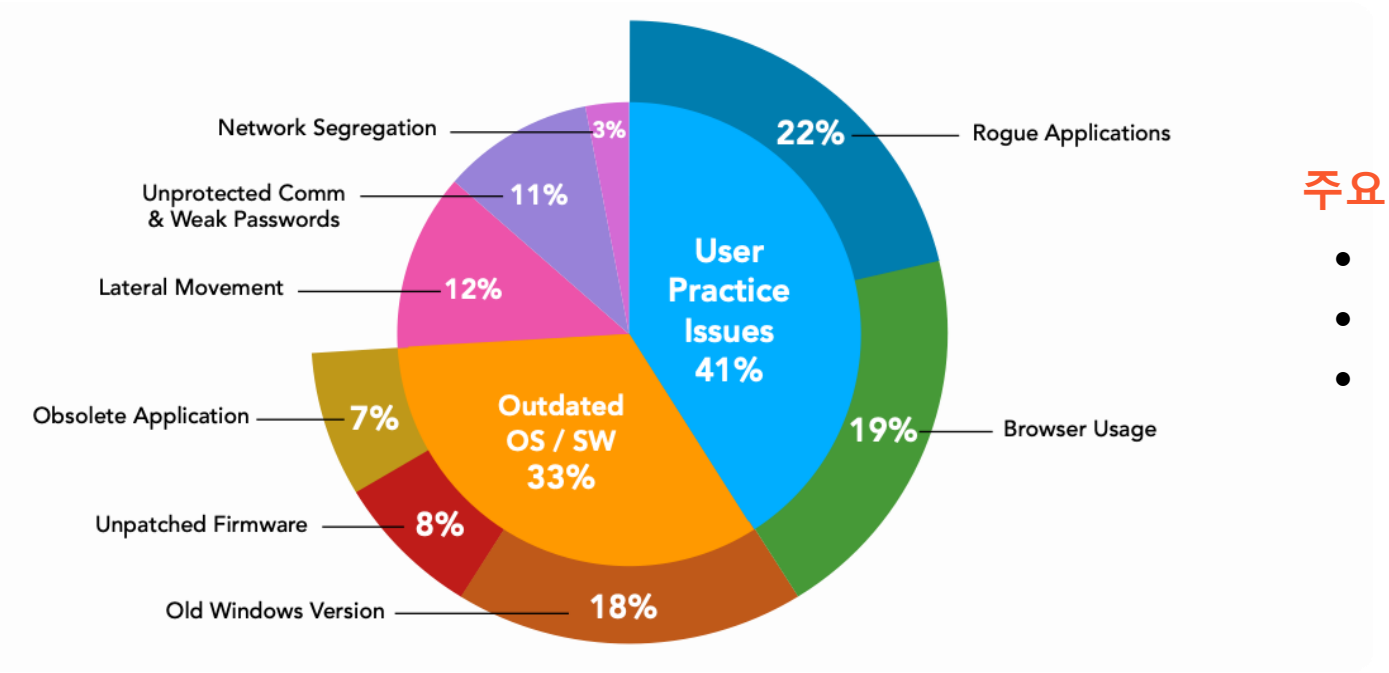
보안 문제가 가장 많은 의료용 IoT 장치

- Imaging system (51%)
- Patient monitor (26%)
- Medical device gateway (9%)

대부분의 보안 문제가 있는 일반 IoT 장치

- Camera (33%)
- Printer (24%)
- Video gaming devices(10%)

의료 기기의 보안 문제



주요 이슈 :

- 사용자 실무 관련(41%)
- 오래된 OS/SW (33%)
- 위협 전파 (12%)

기존 솔루션의 한계

Limited Visibility

이전에는 볼 수 없었던 IoT 장치를
식별하기 어려움

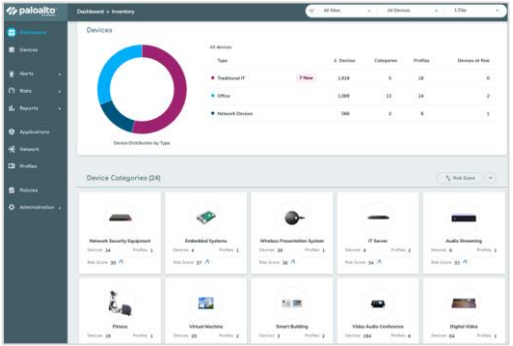
No Protection

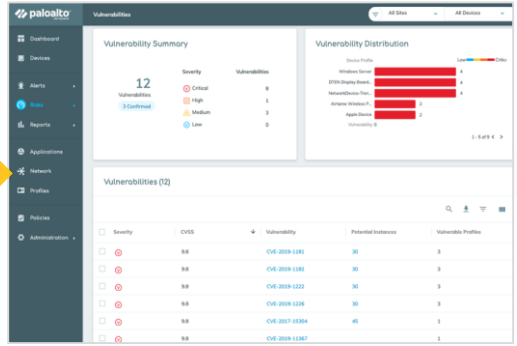
기존 가시성 중심의 솔루션들은
예방조치를 제공하지 않음

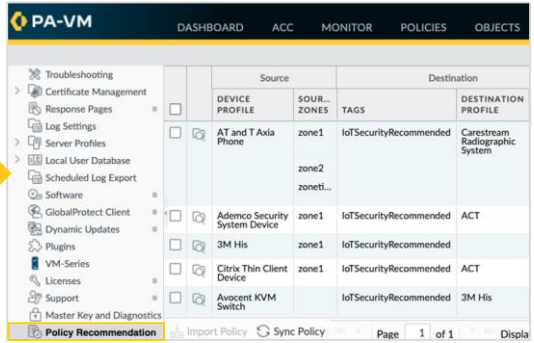
Hard to Implement

네트워크 인프라 구조 및
보안팀의 워크 플로우 변경 필요

IoT Security : 관리되지 않은 IoT 보안 위협 대응







완벽한 가시성

기업 내 식별되지 않은 IoT 디바이스에 대해 Machine Learning 기반으로 모든 장치를 정확하게 식별하고 분류

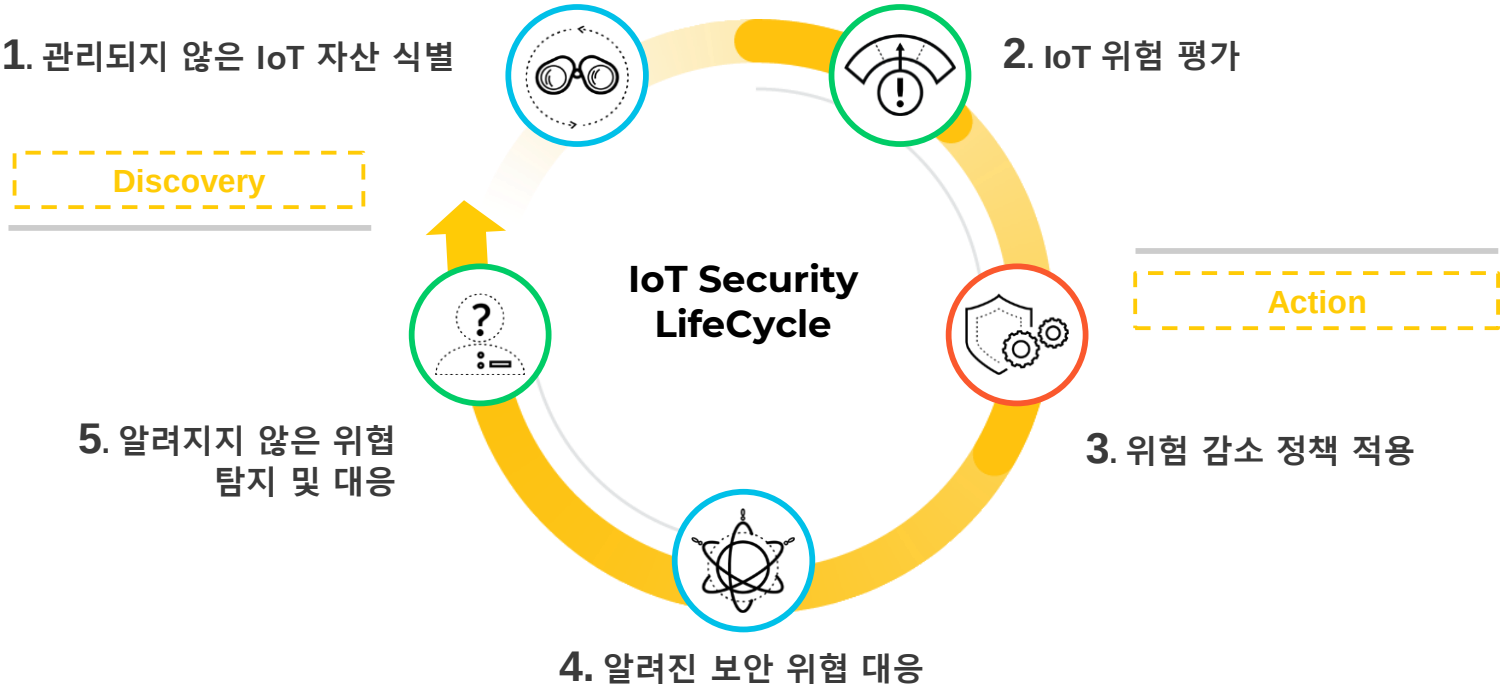
심층 위험 분석

이상행위, 취약점 및 보안 위협의 심각도를 신속하게 이해하여 확실한 의사 결정

보안 위협 대응

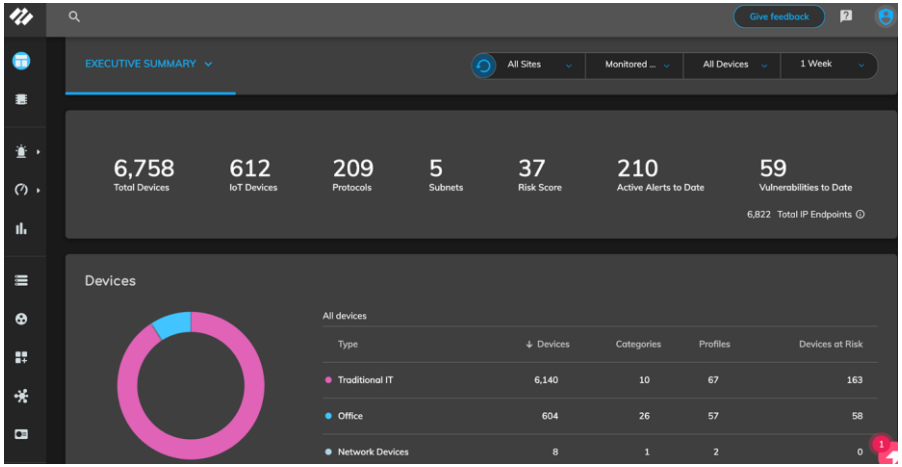
물리적 방화벽 또는 가상 방화벽을 통한 알려진 또는 알려지지 않은 위협 차단

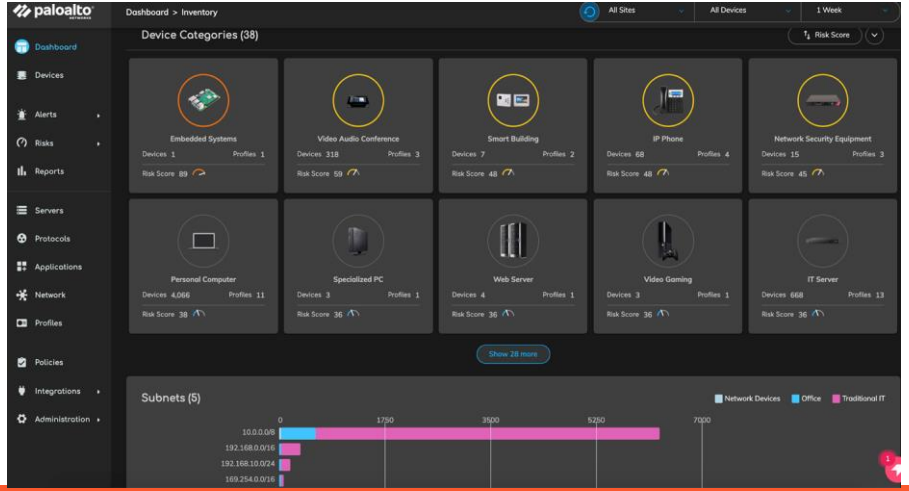
IoT Security : 관리되지 않은 IoT 디바이스를 보호하는 프로세스



1. 관리되지 않은 IoT 자산 식별

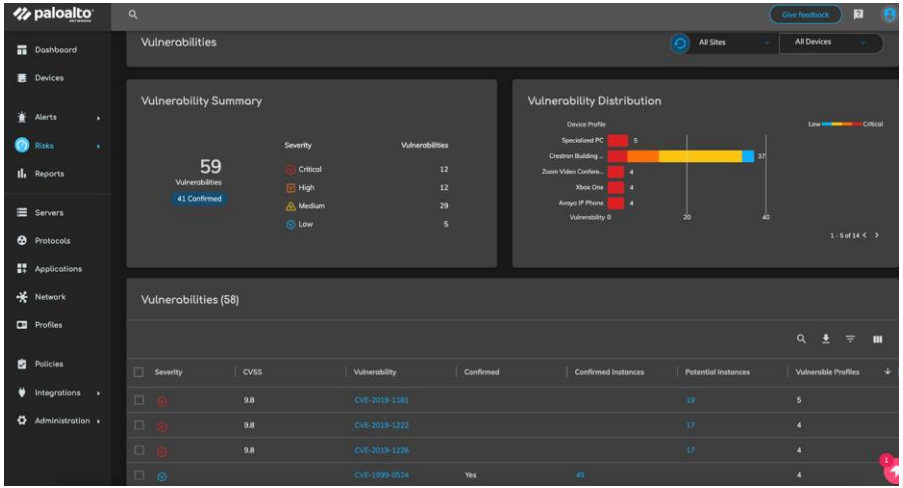
- 전체 장치 검색
  - 전통적인 IT
  - 네트워크 장치
  - IoT 변형
- Device-ID로 추적되는 모든 IoT 장치를 머신러닝 기반으로 식별 및 분류
  - 제조사, 모델 & OS
  - 카테고리
  - 프로파일
- Deep insights
  - VLAN 과 서브넷
  - App-ID 통합
  - 행위 기반

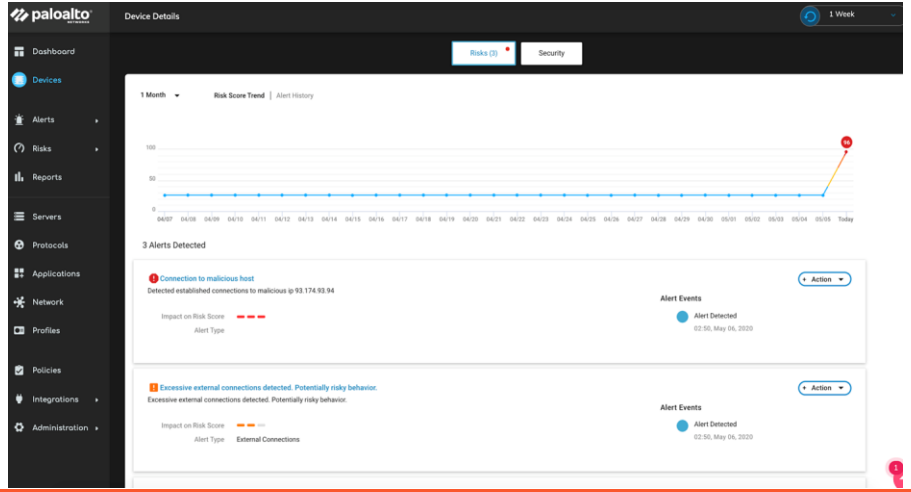




2. IoT 위험 평가

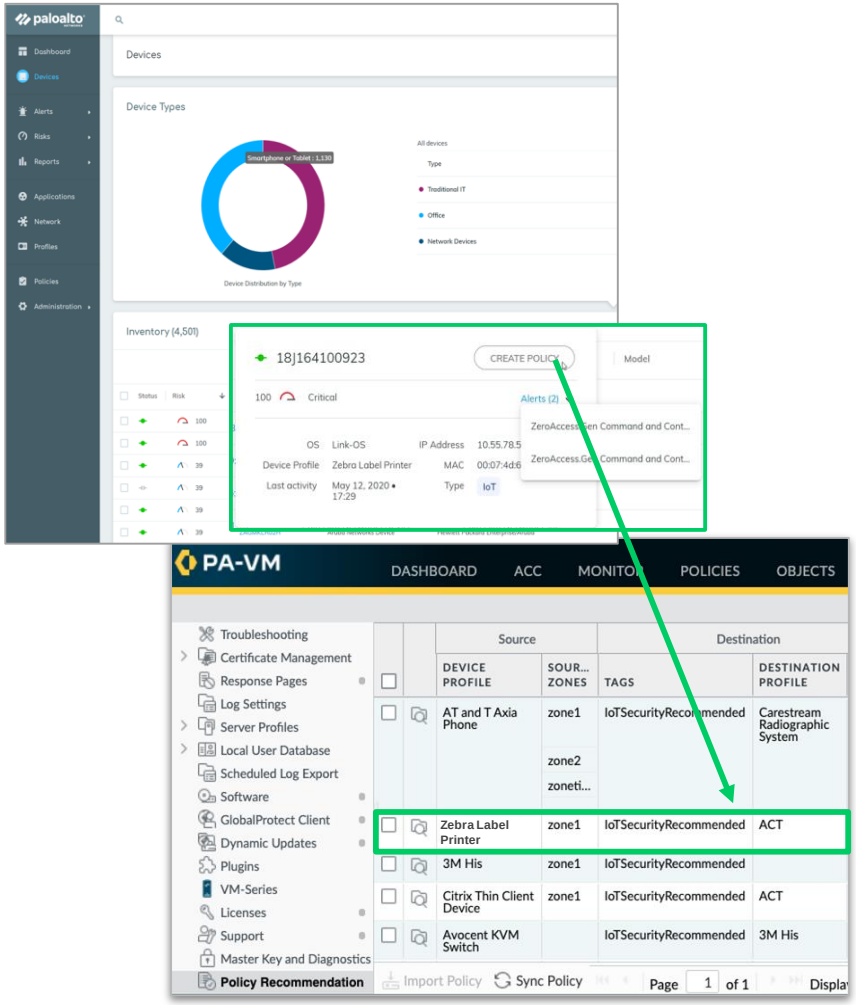
- 24x7 위험 모니터링
  - 행위기반 및 프로파일
  - 경보 및 위협
  - 취약점 확인
- CVE 인벤토리와 통합
- 자동화 된 위험 기반 정책 권장 사항





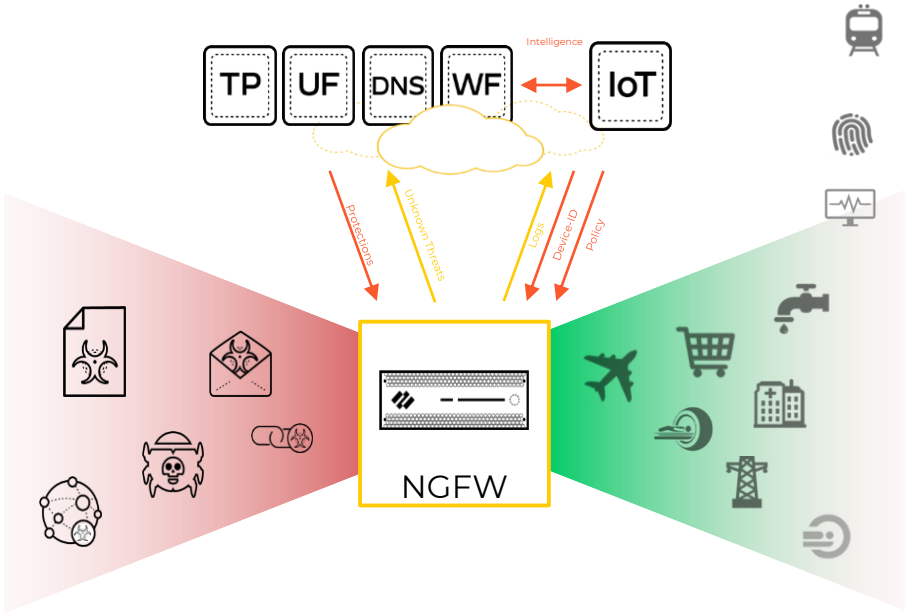
3. 위험 감소 정책 적용

- 딥 디바이스 컨텍스트를 위해 수집 된 디바이스 속성
- 위험, 분류 및 행위에 따른 세분화를 위한 정책 권장 사항
- Device-ID, App-ID 및 User-ID를 기반으로하는 유연하고 일관된 정책 시행



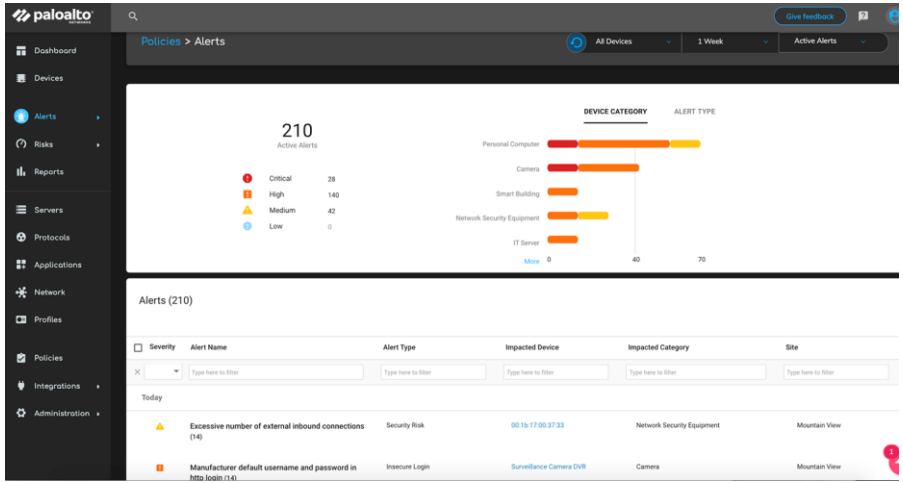
4. 알려진 보안 위협 대응

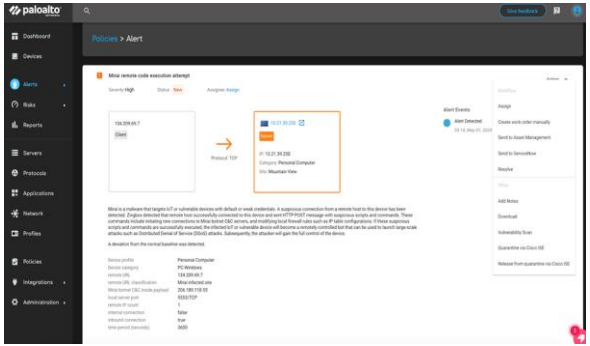
- IoT Security는 Context-ID를 통해 경보에 대한 장치 컨텍스트를 추가하고 정책 시행을 제어함으로써 기존 보안을 향상시킴
  - Threat Prevention: 알려진 IoT 맬웨어를 차단하기 위해 컨텐츠 시그니처로 업데이트
  - URL Filtering: IoT 공급업체와의 통신을 위한 안전한 웹 액세스 제공
  - DNS Security: DNS를 사용하는 IoT디바이스에 대한 공격 차단
  - WildFire: 파일 기반 IoT 위협 탐지 및 방지
- Device-ID는 장치 ID 및 속성 기반 정책 시행을 허용

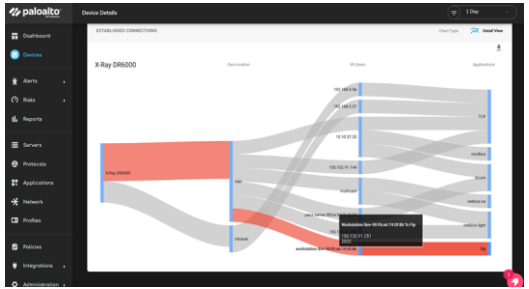


5. 알려지지 않은 위협 탐지 및 대응

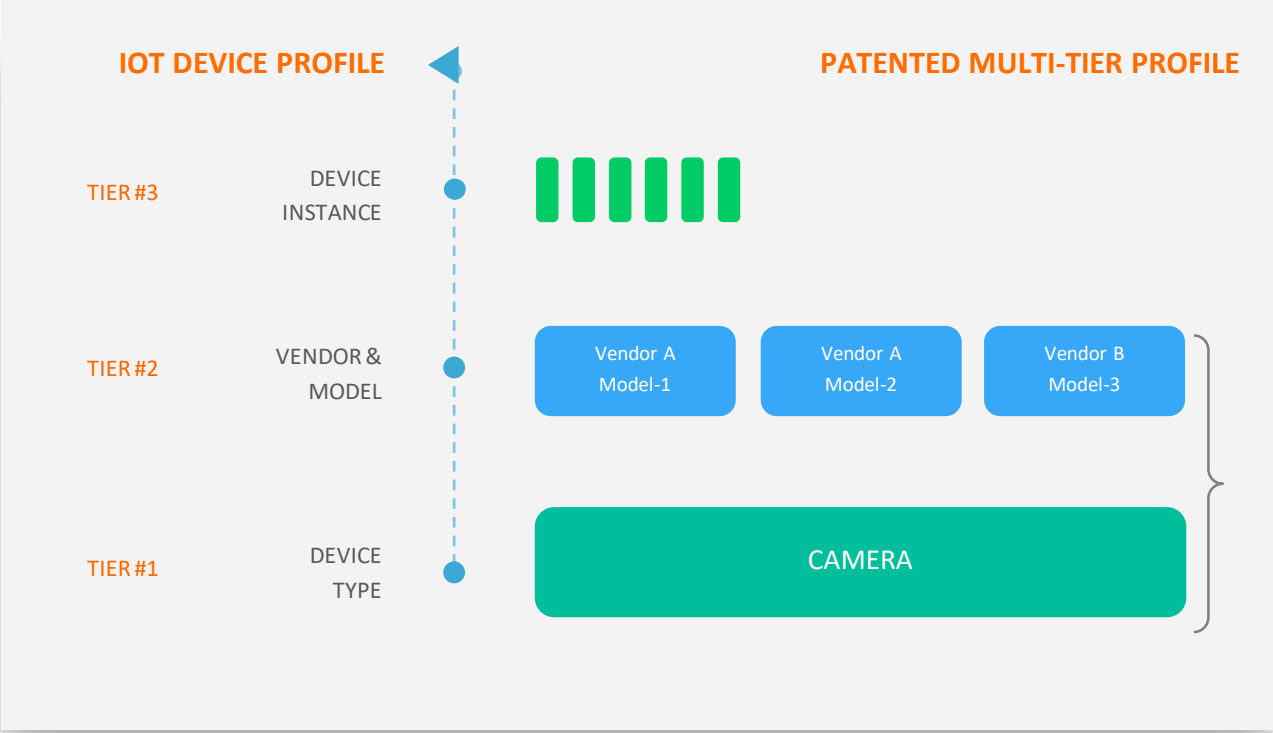
- 위협 모델링으로 강화 된 머신 러닝 기반으로 실시간 위협 감지
- 세부 위협 상황 컨텍스트 및 대응에 대한 명확한 권장 사항 제공
- 장치를 격리 및 격리하는 데 사용되는 ACL 및 DAG



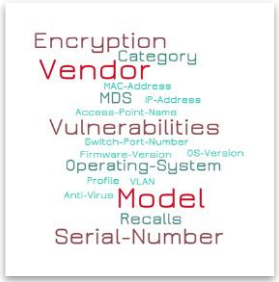




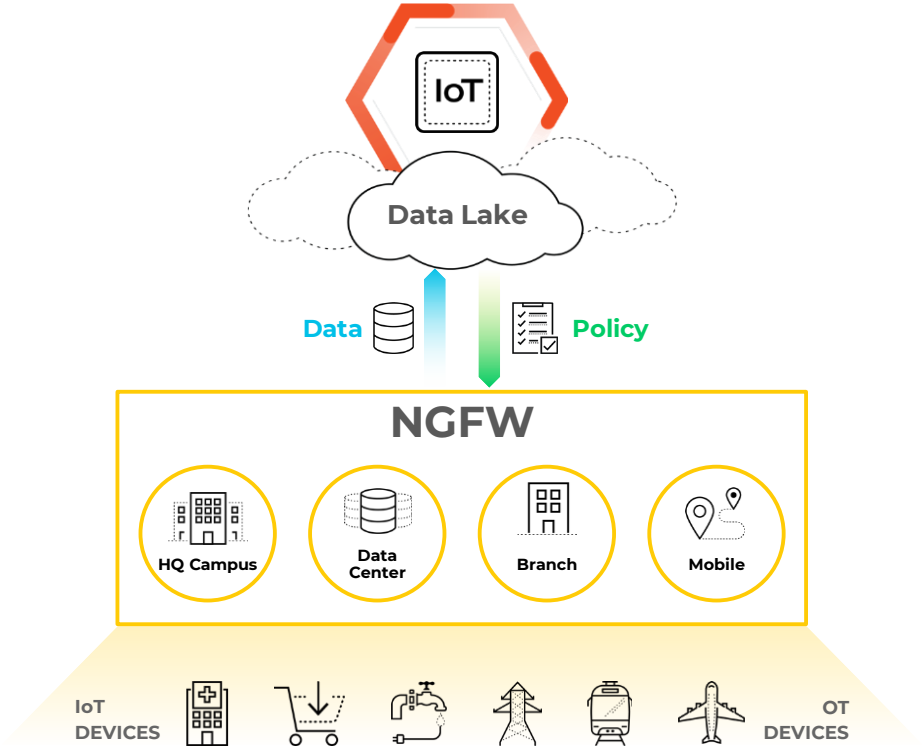
IoT Security : 컨텍스트 기반의 식별



1. 행동 모델을 기반으로 식별에 접근
2. 이전에는 볼 수 없었던 장치를 식별하고 계층 별 프로필과 점진적 성장을 사용
3. IoT 디바이스의 빠른 식별 및 미세 조정 가능



IoT Security : 관리되지 않은 IoT 보안 위협 대응



- 하드웨어, 소프트웨어, 클라우드 서비스-모든 NGFW 폼 팩터에서 사용 가능
- 기 구축된 NGFW를 이용가능
- 멀티테넌트 클라우드 인프라 환경에서 확장성 제공
- 기존 NGFW의 서브스크립션을 이용한 선제방어 기능 제공

paloalto NETWORKS

Thank you

www.paloaltonetworks.com