솔루션 개요

HPE aruba networking

오늘날의 IoT 기반 네트워크에 대한 가시성 및 인사이트

Client Insights를 통한 네트워크 엔드포인트 보안을 위한 AI 기반 접근 방식

HPE GreenLake

네트워크에서 엔드포인트 클라이언트의 폭과 복잡성이 놀라운 속도로 계속 증가함에 따라 많은 조직이 확장되는 공격 표면을 해결하는 데 어려움을 겪고 있습니다. 사물 인터넷(IoT)이 보편화되고 디지털 트랜스포메이션 이니셔티브를 통해 새로운 사용 사례가 창출됨에 따라 IoT의 도입이 운영 효율성과 비즈니스 성과 개선을 위해 중요한 보안 및 규제 준수 성공 사례를 앞질렀습니다.

이러한 변화로 인해 IT 및 보안 팀은 언제, 어디서, 어떤 유형의 새로운 클라이언트가 네트워크에 연결되는지 알지 못하는 경우가 많습니다. 이러한 가시성 부족으로 인해 적시에 보안 및 규제 준수 보호 조치를 구현할 수 없습니다. 성공 사례에 따르면 각각의 신규 클라이언트를 정확하게 식별하고 온보딩하고 정책을 할당해야 하지만 IT 부서는 종종 대비하지 못하는 경우가 많습니다.

현재 접근 방식의 '맹점'

기존 네트워크 가시성 도구 집합은 기본적인 검색 및 프로파일링 기술을 사용하여 쉽게 식별할 수 있는 매우 좁은 범위의 클라이언트에 초점을 맞춰 왔습니다. 여기에는 일반적인 데스크톱이나 모바일 운영 체제를 실행하는 인기 있는 스마트폰과 노트북과 같은 것을 찾는 것이 포함됩니다. 이러한 기술은 Windows를 실행하는 노트북에서 Android를 실행하는 스마트폰을 식별하는 것이 일반적이었습니다.

IoT 장치와 같은 클라이언트를 식별하는 것은 다음과 같은 여러 가지 이유로 특히 어렵습니다.

- 많은 IoT 장치는 신흥 벤더가 생산하며 표준 검색 및 프로파일링 기술을 사용하여 통신할 수 없어 정확한 프로파일링이 어렵습니다.
- 라즈베리 파이처럼 다양한 역할을 하는 일반적인 하드웨어와 소프트웨어로 제작된 IoT 장치도 흔하기 때문에 구분하기가 어렵습니다.
- 프로파일링이 부정확하거나 일부만 이뤄지므로 종종 클라이언트가 일반 'Windows' 또는 'Linux' 클라이언트로 식별되며, 이로 인해 정확한 정책을 적용하기 어렵습니다.
- 대부분의 네트워크 가시성 솔루션에는 수집기나 에이전트가 필요하며, 적절한 규모로 여러 위치에 수집기를 배포하는 일이 항상 가능하지는 않습니다.

컨텍스트의 중요성

이러한 변화로 인해 IT 팀은 유선 및 무선 인프라 전체의 가시성에 대한 전체 스펙트럼 접근 방식이 필요합니다. 이 접근 방식은 대상을 파악할 때 에이전트를 사용하거나 클라이언트에 로그인할 필요가 없어야 합니다. 이는 장치의 실제 동작(사용 중인 프로토콜, 액세스되는 애플리케이션 및 URL, 궁극적으로 네트워크에서 클라이언트가 제공하는 기능)을 이해하는 것을 의미합니다. 병원이나 제조 공장에 있는 것과 같은 대다수의 특수 목적 IoT 장치의 경우, 이러한 풍부한 컨텍스트만이 정확하게 지문을 채취할 수 있는 유일한 방법입니다.

HPE Aruba Networking 솔루션: AI 기반 Client Insights

HPE Aruba Networking의 네트워크 관리 솔루션인 HPE Aruba Networking Central 클라우드에는 이제 업계에서 가장 세부적인 프로파일링과 가시성을 제공하는 AI 기반 Client Insights가 포함됩니다. Client Insights는 실제 수집기나 에이전트를 설치할 필요 없이 액세스 포인트, 스위치, 게이트웨이, 클라이언트 등에서 기본 인프라의 원격 측정을 활용합니다. ML 기반 분류 모델을 활용하여 전체 유무선 인프라에 걸쳐 다양한 클라이언트의 핑거프린팅, 식별, 정확한 프로파일링이 가능합니다.

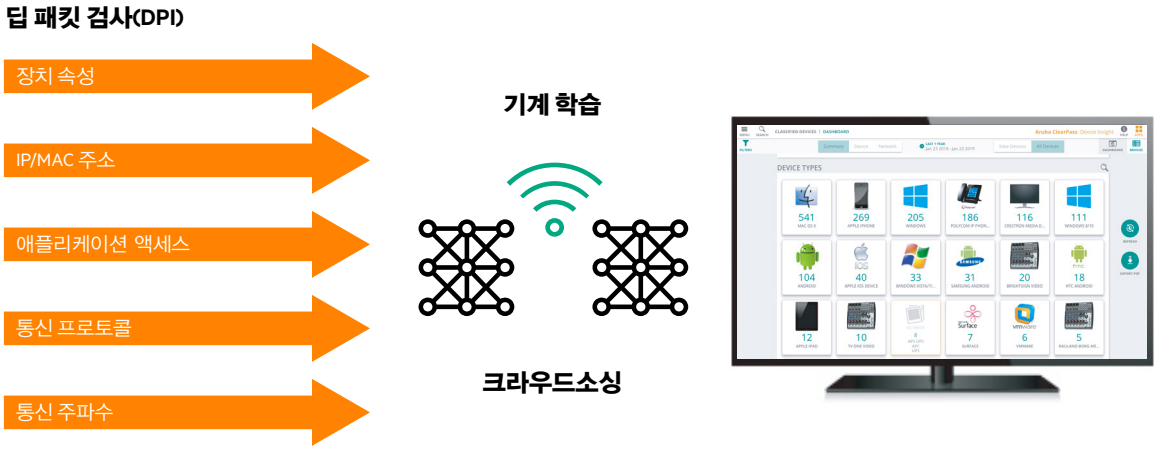


그림 1. Client Insights는 고급 기계 학습 및 크라우드소싱을 활용하여 모든 클라이언트 유형을 정확하게 식별합니다.

이러한 역량은 감지하기 어려운 IoT 장치를 정확하게 식별하는 데 도움이 되는 추가적인 컨텍스트 및 동작 정보를 제공하는 DPI(딥 패킷 검사)를 통해 더욱 향상됩니다. DPI를 활용하면 Client Insights는 더 다양한 장치 속성을 활용해 식별의 정확도를 높일 수 있습니다. 통신 및 행동 패턴을 포함한 클라이언트 속성을 분석하여 유사한 장치의 클러스터를 동적으로 구축합니다.

기계 학습 모델은 이러한 속성을 지속적으로 학습하고 업데이트하여 지문을 동적으로 업데이트하고 분류 추천을 제공하는 데 사용됩니다. 제어형 크라우드 소싱 기술을 사용하여 여러 고객 사이트에서 지문을 검증한 후 HPE Aruba Networking 분류 데이터베이스에 추가합니다. 이를 통해 분류 엔진의 정확도와 포괄성이 향상됩니다.

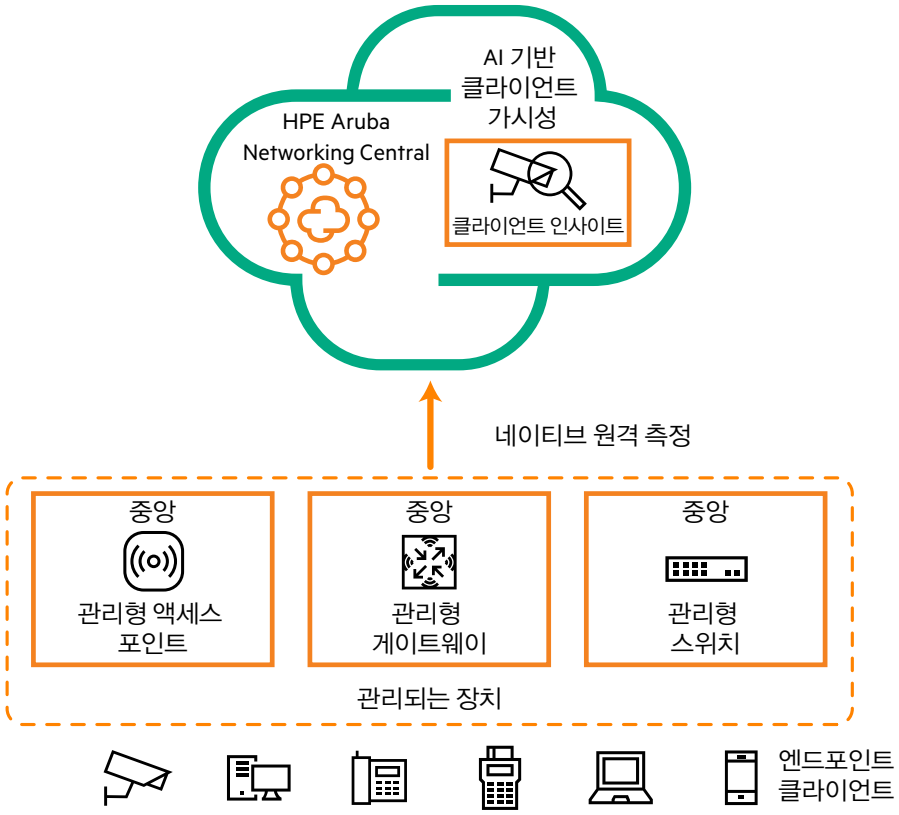


그림 2. HPE Aruba Networking 인프라의 네이티브 원격 측정은 기계 학습 기반 분류로 연결된 클라이언트를 정확하게 식별하는 데 사용됩니다.

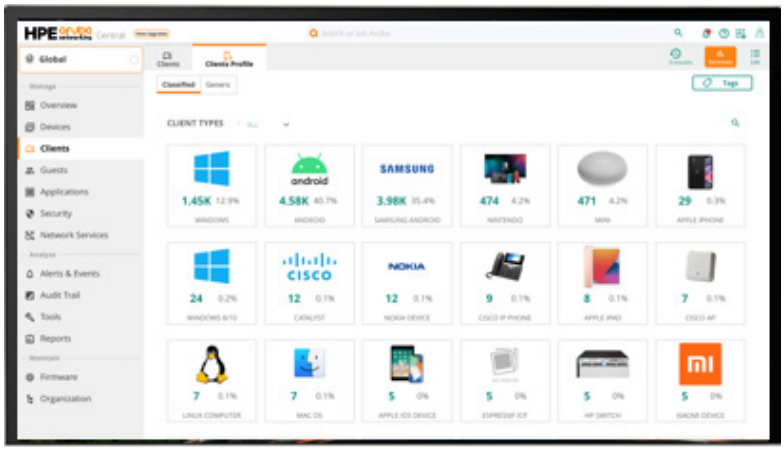


그림 3. HPE Aruba Networking Central 클라우드 Client Insights 대시보드는 카테고리별로 연결된 모든 장치를 표시합니다.

이전에는 일반적이라고 간주되었던 장치의 경우, 정교한 기계 학습 모델을 사용하여 속성을 분석하고 유사한 클라이언트를 그룹화합니다. 클라이언트를 그룹화하면 주요 속성을 기준으로 쉽게 레이블을 지정할 수 있습니다. 레이블이 지정되면, 네트워크에 연결되는 새로운 클라이언트는 자동으로 해당 클러스터에 추가되고 그에 따라 레이블이 지정됩니다.

현재 HPE Aruba Networking Central 클라우드로 관리되지 않는 환경이나 타사 네트워크 장치가 있는 환경의 경우 CPDI(HPE Aruba Networking ClearPass Device Insight)를 활용하여 클라이언트를 기계 학습 기반으로 식별하고 프로파일링할 수 있습니다. CPDI를 사용하려면 실제 또는 가상 수집기를 설치해야 하며 별도의 라이선스가 필요합니다.

자동화된 정책 시행의 가치

전체 상태만 파악하고 적절히 제어하지 않으면 보안이 어렵고 규제를 준수하지 못할 수 있습니다. Client Insights를 사용하면 클라이언트를 지속적으로 모니터링할 수 있으며, HPE Aruba Networking ClearPass Policy Manager와 함께 사용할 경우 폐회로 엔드 투 엔드 접근제어가 가능합니다. 이를 통해 가시성과 자동화된 정책 시행이 가능해지고, 멀티 벤더가 연결된 유무선 네트워크에서 수동 개입의 필요성이 크게 줄어듭니다. CPDI는 ClearPass Policy Manager와도 완벽하게 통합됩니다.

자동화된 정책 시행은 클라이언트가 처음 네트워크에 참여하는 순간부터 보안 또는 규제 준수 문제로 인해 원치 않는 이벤트가 발생하여 클라이언트를 삭제해야 하는 경우까지 다양한 사용 사례를 해결합니다. 예를 들어, 새로운 카메라가 네트워크에 처음 연결되면 자동으로 알 수 없는 클라이언트 유형으로 분류되어 중요한 인프라나 서버에 영향을 미치지 않도록 할 수 있습니다. 클라이언트가 손상되었거나 의심스러운 방식으로 행동하는 경우 테스트, 수리, 교체를 위해 완전히 격리될 수 있습니다.

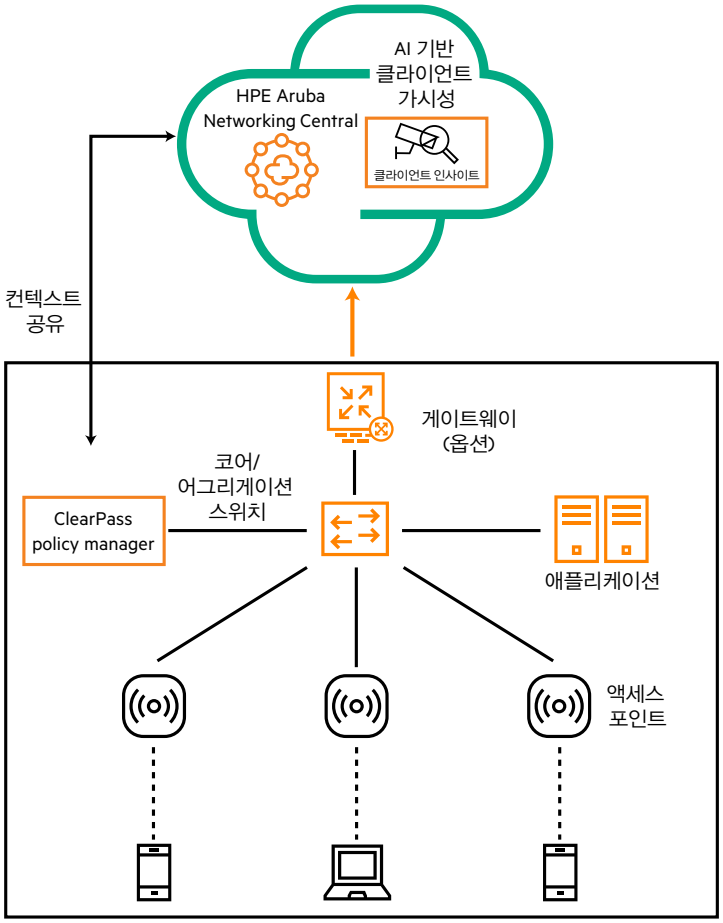
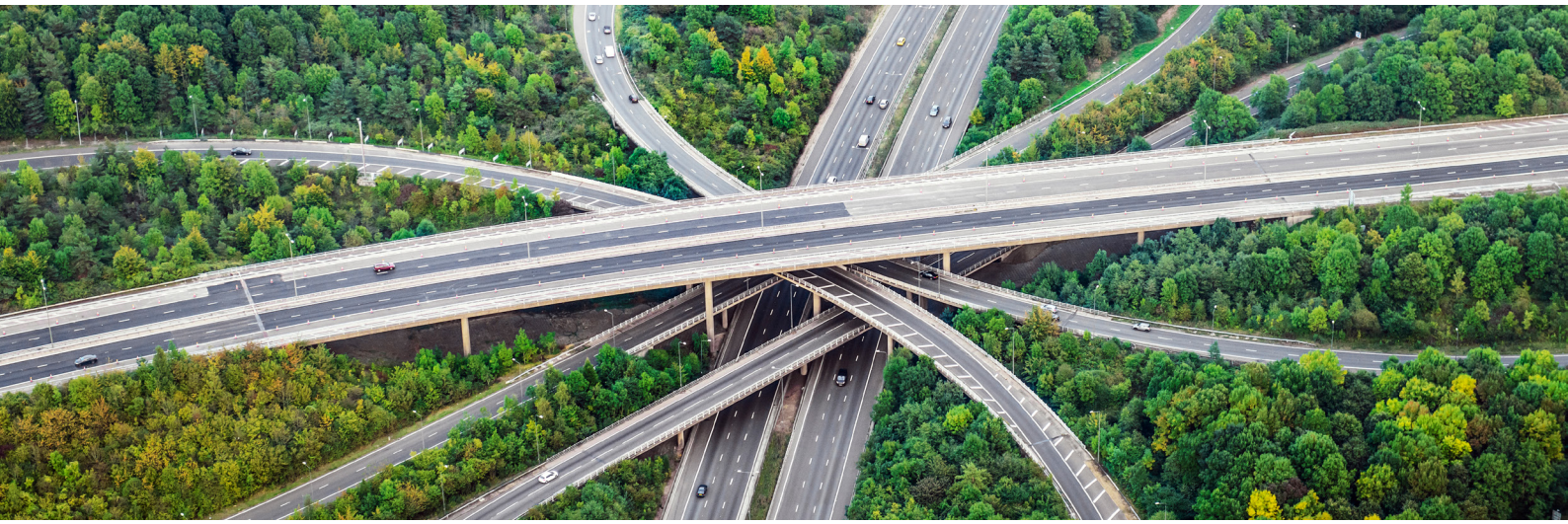


그림 4. Client insights, 자동화된 세분화 및 적용을 위해 HPE Aruba Networking ClearPass Policy Manager와 통합

HPE Aruba Networking Central 클라우드 및 Client Insights 수익 창출 시간 단축

점점 더 분산되는 환경에서 비즈니스 크리티컬 애플리케이션을 관리하면 가용성, 성능 및 보안이 향상될 것으로 예상됩니다. HPE Aruba Networking Central 클라우드는 고급 AI/ML 및 보안 기능을 포함한 현대적인 기능, 확장성, 관리 및 오케스트레이션을 제공하여 모든 규모의 IT 조직이 놀라울 정도로 간편하면서도 탁월한 사용자 체감 만족도를 제공할 수 있도록 지원합니다.

Client Insights는 이러한 고유 기능과 네트워크 인프라의 네이티브 원격 측정을 활용하여 구축 시간과 비용을 줄이고 수익 창출 시간을 단축합니다. 이러한 접근 방식은 분산된 구축 환경에서 네트워크 엔드포인트를 중앙에서 중단 없이 검색하고 모니터링하는 동시에 가시성과 보안 태세를 강화합니다.



요약

IoT 디바이스의 도입이 가속화됨에 따라 고객 네트워크의 클라이언트 수는 계속 증가하여 새로운 사용 사례를 창출하는 동시에 공격 영역을 확장하고 있습니다. IoT 도입에 따른 운영 효율성에 맞춰 보안과 성공 사례 준수를 보장하려면 포괄적인 가시성이 필수적입니다.

세분화된 역할 기반 정책에 따라 클라이언트를 정확하게 식별 및 프로파일링하고 각 클라이언트에게 전반적인 위험 수준을 낮추는 적절한 수준의 접근제어가 있는지 확인하는 일은 더 이상 선택 사항이 아니라 필수 사항입니다.

올바른 구매 결정을 위해
HPE 프리세일즈 담당자와 상의하십시오.

문의하기

ArubaNetworks.com 방문하기

© Copyright 2024 Hewlett Packard Enterprise Development LP. 본 문서의 내용은 사전 통지 없이 변경될 수 있습니다. Hewlett Packard Enterprise 제품 및 서비스에 대한 보증의 경우, 해당 제품 및 서비스와 함께 제공된 보증서에 명시된 내용만이 적용됩니다. 본 문서에는 어떠한 추가 보증 내용도 들어 있지 않습니다. Hewlett Packard Enterprise는 본 문서에 포함된 기술상 또는 편집상의 오류나 누락에 대해 책임지지 않습니다.

모든 타사 마크는 해당하는 소유자의 재산입니다.

SO_hpeanwClientsInsights_OH_041224 a00069032KOP

Hewlett Packard Enterprise