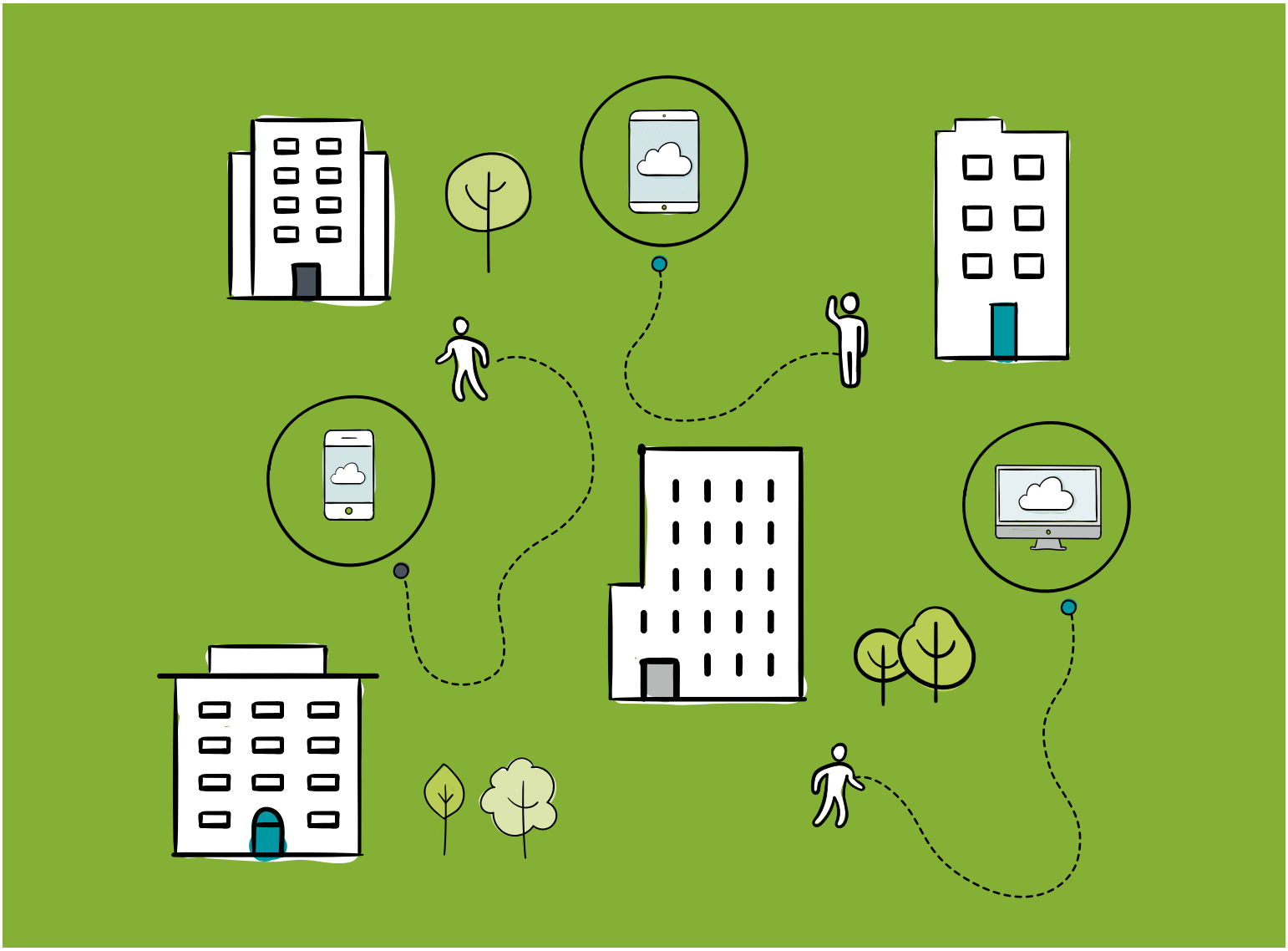
JUNIPER NETWORKS | Engineering Simplicity

eGuide

AI 기반 엔터프라이즈 구축에 필요한 모든 것

유무선 네트워크 최적화를 위한 구매자 가이드



2020년 3월

내용

소개

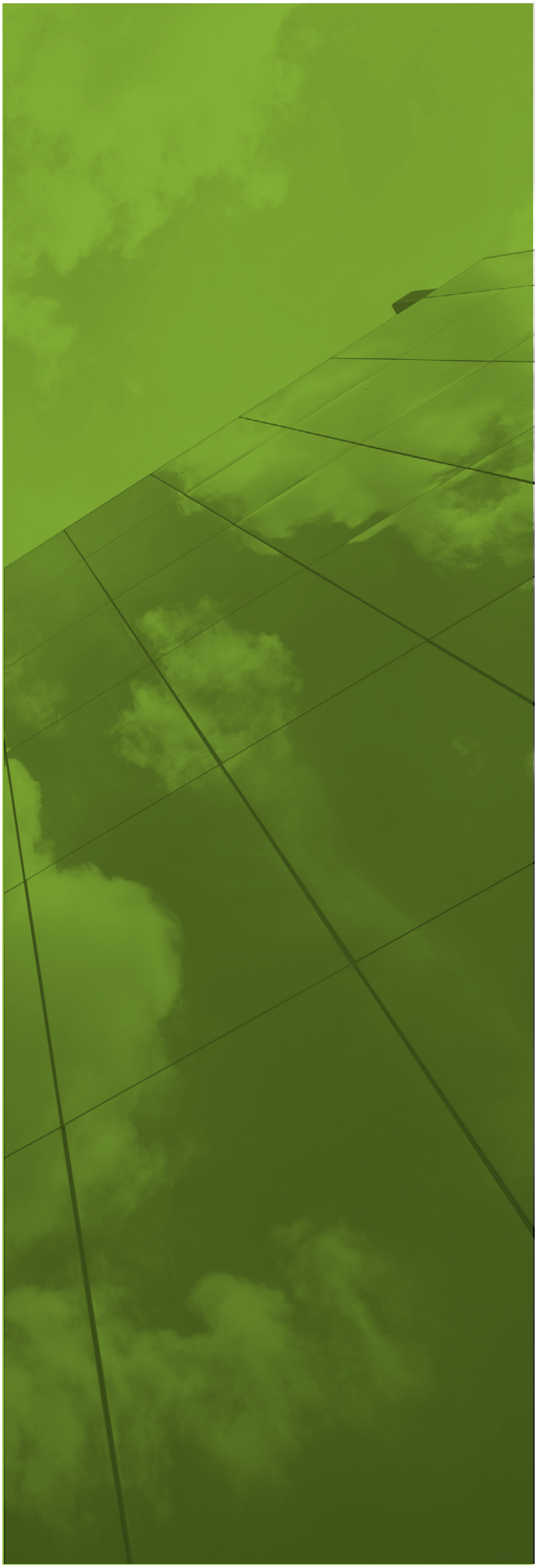
AI 기반 엔터프라이즈의 척도는 업타임이 아니라 경험입니다. AI 기반 엔터프라이즈는 운영 경험을 향상시키기 위해 툴, 인터페이스, 데이터를 활용하여 수작업 의존도를 줄입니다. 이를 위해 중요한 것이 캠퍼스 네트워크입니다.

주니퍼 네트웍스 캠퍼스 솔루션은 네트워크 구성과 구축에서부터 모니터링 및 관리에 이르기까지 일상적인 운영 업무를 단순화할 뿐만 아니라 안전하고 자동화된 멀티클라우드 엔터프라이즈의 이점을 실현하는 데 한 걸음 더 다가설 수 있도록 지원합니다.

주니퍼 미스트(Mist Systems)는 Gartner가 발표한 2019 유무선 LAN 액세스 인프라 핵심 기능 보고서(Critical Capabilities for Wired and Wireless LAN Access Infrastructure)와 매직 쿼드런트에 이름을 올렸으며, 주니퍼는 글로벌 고객이 모든 유무선 액세스 레이어와 관련된 전략을 추진함에 있어 주니퍼 Mist를 고려해 볼 필요가 있다고 생각합니다. 주니퍼는 6가지 사용 사례에서 모두 최고 점수로 3위 안에 들었으며, 또한 매직 쿼드런트에서 비저너리(Visionary)로 선정되었습니다.*

자세한 내용은 매직 쿼드런트 보고서와 핵심 기능 보고서를 확인해 보십시오.

인프라 리프레시와 확장 시점을 멀티클라우드 전환의 기회로 활용 하십시오.



Gartner 매직 쿼드런트 유무선 LAN 액세스 인프라 부문 보고서, Bill Menezes, Christian Canales, Tim Zimmerman, Mike Toussaint, 2019년 9월 24일.

Gartner 유무선 LAN 액세스 인프라 부문 주요 기능 보고서, Christian Canales, Tim Zimmerman, Bill Menezes, Mike Toussaint, 2019년 9월 26일.

Gartner는 연구 간행물에 소개된 특정한 벤더, 제품 또는 서비스를 추천하지 않으며, 기술 사용자들에게 최고 또는 기타 등급으로 지정된 벤더만을 선택하도록 권고하지도 않습니다. Gartner 연구 간행물은 해당 연구 조직의 의견을 담고 있으며 사실에 대한 진술로 해석해서는 안 됩니다. Gartner는 본 리서치와 관련해 상품화 또는 특정 목적에 대한 적합성을 비롯한 모든 명시적, 암시적 보증을 부인합니다.

캠퍼스 시장 동향

사용자 경험의 이해와 정의

캠퍼스 생산성, 효율성, 협업을 위해서는 반드시 우수한 사용자 경험이 보장되어야 합니다. 캠퍼스 네트워크에서 사용자의 서비스 경험은 액세스 에지에서부터 시작되며, 여러 관련 요소들이 있습니다. 예전에는 기본적인 모니터링과 업타임만으로 사용자 경험을 가늠했습니다. 그러나 이제는 강화된 SLE(Service Level Expectations)를 통해 정의된 경험의 품질이 기준이 됩니다. 이러한 기대에 부응하려면 IT 운영이 사후 대응적인 문제 해결에서 벗어나 선제적인 조치로 전환되어야 합니다. 사후 대응적 운영에서 선제적 운영으로의 전환은 이미 진행 중입니다. 운영 팀이 약속된 서비스를 보장할 수 있도록 해주는 AI가 이러한 전환을 가속화하고 있습니다.

AI for IT는 캠퍼스 전반에서 조직의 네트워크 특성에 따라 이벤트를 관찰하고, 학습하고, 관련성을 파악합니다. 이를 통해 의미 있는 SLE를 설정하고 기대 이상으로 만족시킵니다. AI for IT는 유무선 텔레메트리를 지속적으로 스트리밍하고 수집하여 엔드유저 경험에 대한 향상된 가시성을 확보하고, MTTR(Mean Time To Repair)을 단축합니다. 그리고 사용자가 문제를 인식하기도 전에 구성 오류를 알리고 수정합니다.

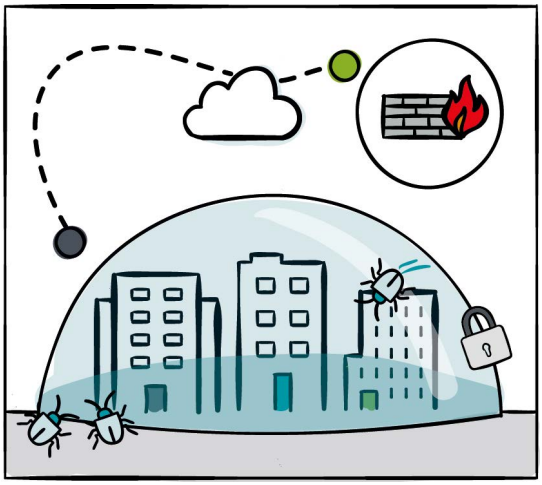
캠퍼스 사용자는 애플리케이션, 디바이스 유형에 관계없이 항상 안전하고 유연하며 안정적인 연결을 기대합니다. AI 기반 엔터프라이즈는 선제적인 이상 탐지, 셀프 드라이빙 운영, AI 엔진과 IT 비용 절감을 지원하는 유무선 보장(Wired and Wireless Assurance)을 제공합니다.

AI for IT

AI for IT로의 전환은 캠퍼스 네트워크에서 시작됩니다. 지속적이고 가치가 없는 수동적이면서 반복적인 작업은 고역이 아닐 수 없습니다. 이는 오버헤드 비용으로 간주되며 IT 설치 공간이 커질수록 같이 늘어 나는 경우가 많습니다. 운영은 운영 플레이북과 표준작업 절차서(SOP)에서 대부분 수작업 단계로 분류되는 트러블슈팅과 같은 반복적인 작업으로 인해 고되고 힘들어 집니다. 이러한 노동은 번아웃을 야기하고 사기를 떨어뜨립니다. 일단 AI와 자동화로 인해 불필요한 노동이 줄어들면, 혁신과 창의적인 문제 해결과 같은 보다 흥미로운 고객 및 엔지니어링 과제에 집중할 수 있도록 시간을 투자할 수 있습니다.

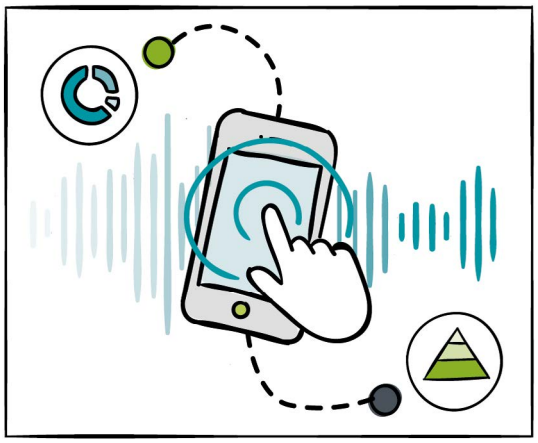
유능한 운영팀은 최신 플랫폼과 툴을 활용하여 업무 효율을 증대시킵니다. 네트워크를 유지보수하는 데 보내는 시간이 줄어들수록, 미래 지향적이고 전략적으로 행동할 수 있는 시간과 에너지, 동기가 증가한다는 것을 의미합니다.

민주화되고 분산된 운영



IT뿐만 아니라 일반 운영 팀도 기술에 발맞추기 위해 애쓰고 있습니다. AI 기술을 활용함 으로써, 모든 팀이 자연어 질문을 사용하여 네트워크 상태를 보다 쉽게 이해할 수 있습니다. 이러한 시스템은 지속적으로 근본 원인을 파악하고 수정 조치를 가능하게 합니다.

문제를 식별하고 쉽게 트러블슈팅할 수 있는 이 기능은 서비스 복원을 가속화하고 팀 전체의 신뢰를 높이는 데 도움이 됩니다. 또한 문제가 있는 디바이스에서 패킷 캡처를 선제적으로 자동 수행할 수 있는 AI 기반 플랫폼 기능을 사용하면 지원 인력이 실시간으로 참여하거나 개입할 필요가 없어집니다.

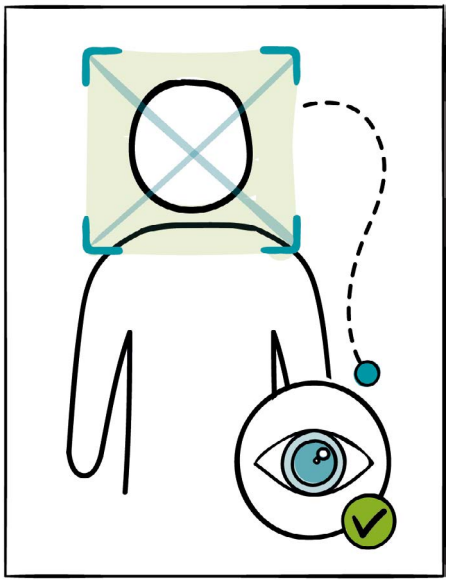


자동화된 보안으로의 진화

캠퍼스 네트워크와 캠퍼스 IT 리소스에 대한 보안의 중요성이 갈수록 커지고 있습니다. 네트워크의 규모와 복잡성이 증가하면서 공격 노출(attack surface)과 악의적인 공격의 양도 증가했습니다. 모바일, 클라우드 서비스, IoT 디바이스 사용이 확대되면서 캠퍼스 네트워크의 공격 노출 또한 폭발적으로 증가하고 있습니다.

경계 방화벽 뒤에 숨는 것은 애초부터 권장되는 보안 태세가 아니었지만, 경계 방화벽을 두고 로그 파일을 살펴보는 것만으로도 무방하다고 주장할 수 있던 시대는 오래 전에 끝났습니다. 이제 고급 위협 방어, 위협 인텔리전스의 실시간 글로벌 공유, AI 기반 자동 대응 솔루션이 새로운 표준이 되었습니다.

모바일 현실



실시간 위치 기반 데이터와 결합된 모빌리티(WLAN) 애플리케이션이 모바일 환경의 확대를 가속화하고 무선 처리량 요구를 끝없이 증대시키고 있습니다.

모바일 및 IoT 디바이스의 급증이 무선 인프라 업그레이드 주기를 가속화함에 따라 802.11n에서 802.11ac로의 전환이 이루어지고, 이제 802.11ax(Wi-Fi 6으로 명명됨)로의 전환이 시작되고 있습니다.

이러한 업그레이드의 파급 효과로 새로운 802.3bz 표준(2.5/5Gbps)을 비롯해 업링크를 기가비 트 이더넷에서 멀티 기가비트 이더넷으로 전환하고 있습니다. 최신 무선 액세스 포인트는 802.3af(15.4W)에서 802.3at(25.5W)로 전력 증가를 요구하며, 곧 802.3bt(>30W)로 마이그레이션할 것입니다. 이에 PoE(Power over Ethernet) 연결 또한 업그레이드 요구에 직면하게 될 것입니다.

캠퍼스 고객 과제

KLO 작업

KLO(Keeping the Lights On)는 사업이 성장하고 변화함에 따라 그 범위가 확대되어 왔습니다. 이러한 관리자 워크로드의 폭증과 책임 범위의 확대로 인해 IT 팀은 막대한 부담에 시달리고 있습니다.

오늘날 IT 팀은 효율성과 민첩성 측면에서 경쟁업체들과 대적하기 위해 IoT나 AI와 같은 최신 기술을 도입해야 하는 압박을 받고 있습니다. 그 결과 IT 팀은 주기적으로 난관에 봉착하고 있으며, 이를 해결하기 위해서는 끊임없는 혁신에 주력하는 동시에 KLO 작업 수행을 위한 시간을 확보해야 합니다.

KLO 작업은 세 가지 기본 범주로 나눌 수 있습니다.

1) **Day 0/Day 1 :** 이러한 작업에는 신규 디바이스 설치, 신규 애플리케이션 또는 서비스 추가, 신규 사이트 개설이 포함됩니다.

2) **지속적이고 일상적인 관리 및 모니터링 :** 네트워크 상태 모니터링 및 필요 시 정책 업데이트를 통한 네트워크 구성이 포함됩니다.

3) **문제 해결 :** 예기치 못한 정전, 네트워크 성능 저하 또는 보안 침해에 대한 대응이 포함됩니다.

일반적인 Day 0/Day 1 과제 :

- 새로운 장비의 설치, 문제 해결 또는 구성을 위한 로컬 전문 인력이 부족합니다.
- 새로 설치된 디바이스를 파악하고 관리하는 데 어려움이 있습니다.
- 조직의 멀티클라우드를 구성하는 모든 인프라 전반에서 신규 사용자/디바이스에 대한 보안 기본값을 적용하는 데 어려움이 있습니다.

지속적이고 일상적인 관리 및 모니터링 :

- 여러 인프라 전반에서 정책을 관리하는 작업이 점점 복잡해지면서 정책이 비일관되게 적용되고 오류가 발생할 가능성이 높습니다.
- 운영 체제, 애플리케이션 및 디바이스가 구버전으로 유지되는 경우가 많아 패치가 필요합니다. 스위치 및 라우터와 같은 네트워크 장비는 종종 최악의 문제를 가져오는 원인입니다.
- ACL(Access Control List) 충돌 : "ACL은 바퀴벌레와 같습니다. 일단 나타나면 사라지지 않습니다!"

문제 해결, 문제가 발생하는 경우 :

- 문제 해결은 지루하고 많은 시간을 허비하게 만듭니다.
- 분할된 데이터 소스 : “근본적인 문제 원인을 찾기 위해 여러 소스에서 여러 로그를 탐색해야 합니다.”
- 정보 과부하 : “무의미한 경고가 넘쳐납니다.”
- 노후 장비 고장

KLO 부담을 줄임으로써 IT 부서는 혁신에 더 많은 투자를 할 수 있으며 이는 경쟁에서 살아남을 수 있는 민첩한 조직을 유지하는 데 필수적입니다.

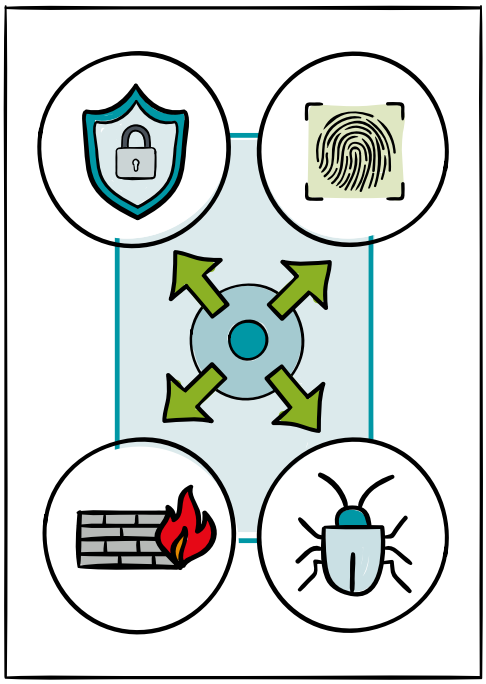
캠퍼스의 핵심 고려사항

클라우드 기반 중앙 관리

캠퍼스 네트워크 관리를 중앙화해 KLO 작업을 줄이거나, 제거해야 합니다.

네트워크가 다수의 캠퍼스 사이트, 분산된 리모트 사이트 또는 이둘의 조합이든 관계없이 전문적인 보호를 제공하는 클라우드 기반 관리 솔루션을 활용함으로써 일상적인 관리 업무를 위한 현장 IT 전문 인력 배치 필요성을 없앨 수 있습니다.

네트워킹 디바이스에서 제로 터치 프로비저닝 기술을 사용하면 어디서든 브라우저에 액세스하여 원격으로 손쉽게 신규 사이트를 구축할 수 있습니다.



고급 커넥티드 시큐리티(Connected Security)

전통적인 보안 접근 방식으로는 폭증하는 위협을 따라잡을 수 없습니다. 네트워크를 성공적으로 보호하려면 오늘날의 조직은 네트워크 전반에 걸쳐 심층적인 네트워크 가시성과 다수의 정책 적용 지점(points of enforcement)을 확보해야 합니다. 한 조직에서 발견된 위협 인텔리전스를 모든 조직이 공유함으로써 고급 위협 보호 기능을 제공하는 것도 여기에 포함됩니다.

모든 것이 네트워크를 통해 움직입니다. 위협도 마찬가지입니다. 따라서 전체 네트워크가 조직 보안 솔루션의 일부가 될 수 있습니다.

자동화된 최신 네트워크 보안을 사용하면 중앙 보안 솔루션에서 네트워크 전체 여러 지점으로부터 정보를 수집할 수 있을 뿐만 아니라 액세스 스위칭 레이어에 있는 모든 네트워크 디바이스에서 정책을 적용할 수 있습니다. ACL과 기타 네트워크 구성 기능은 네트워크 전 레이어에서 자동화된 정책 실행의 일부로 작동하게 됩니다.

오늘날 네트워크는 다양한 벤더의 이기종 제품과 서비스로 혼재돼 있으며, 여러 인프라에 걸쳐 자주 확장되는 멀티클라우드 환경으로 구성돼 있습니다.

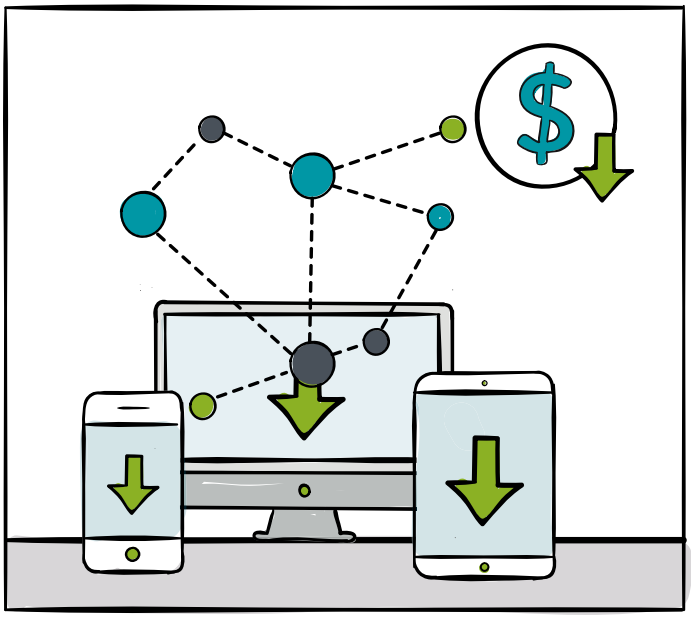
조직에서는 워크로드 또는 데이터가 조직의 인프라 내에서 어디에 있든 상관없이 위협을 감지하고 정책을 일관된 방법으로 적용할 수 있는 기능이 필요합니다.

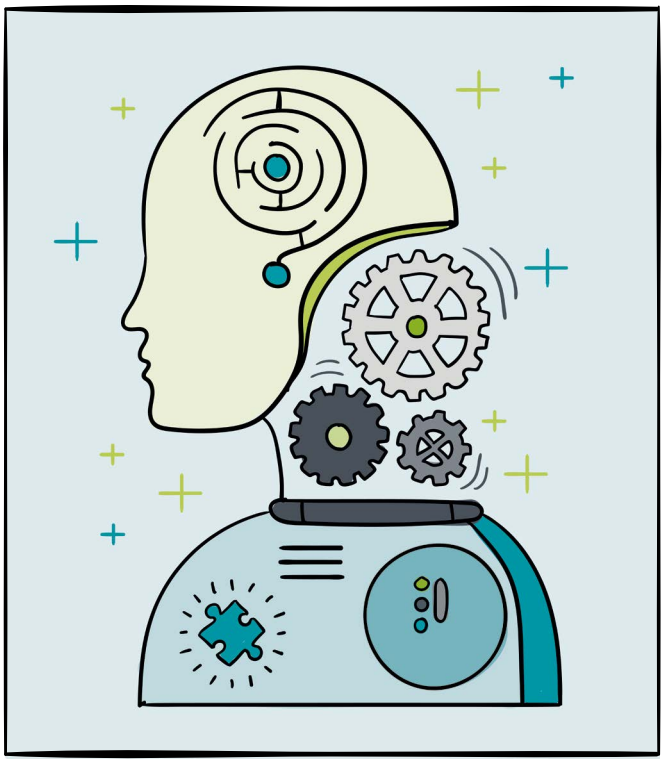
셀프 포밍(Self-Forming) 캠퍼스 패브릭

셀프 포밍(Self-Forming) 캠퍼스 패브릭은 효율성을 높이고 IT 운영을 단순화합니다. 캠퍼스 패브릭을 사용하면 캠퍼스 스위칭 인프라의 매니지드 디바이스 수를 줄이는 데 도움이 되며 그 결과 KLO 비용을 줄이고 OpEx를 크게 개선할 수 있습니다.

최신 패브릭 기술을 사용하면 처리량을 저하시키는 스패닝 트리 프로토콜(STP)이 필요 없으며 네트워크 레이어 축소 및 제거에도 도움이 됩니다. 이러한 패브릭은 간편한 플러그 앤 플레이(plug-and-play) 솔루션으로 구축을 단순화하고 설치 오류로 인한 중단을 줄이며 Day 0/1 작업을 간소화합니다.

개방형 표준 기반 자동화 및 관리 아키텍처는 네트워크 패브릭에 유용합니다. 따라서 관리 및 자동화 솔루션을 공유하는 단일 NOC(Network Operations Center)를 통한 운영이 가능합니다. 개방형 표준 기반 기술을 활용하면 또한 비용이 많이 드는 전면 교체(rip and replace)를 피할 수 있으므로 개별 캠퍼스에서 전체 멀티클라우드까지 네트워크 전체에 걸쳐 일관된 보안 정책을 적용할 수 있습니다.





AI 도구, 분석 및 어시스턴트

사용자가 일반적인 스마트폰 및 컴퓨팅 디바이스(PC, Macbook 등)를 넘어 더욱 다양한 디바이스를 사용함에 따라 캠퍼스 환경에서는 점점 더 많은 데이터가 생성됩니다. 개인 웨어러블 디바이스, 업무용 IoT 디바이스 여부에 관계없이 이러한 디바이스들은 캠퍼스 환경 특유의 다양성과 복잡성을 가중시킵니다. 이러한 디바이스가 유선인지 또는 무선인지 여부와 상관없이 캠퍼스 네트워크 환경에는 새로운 수준의 예측 불가능한 가변성이 발생합니다.

인공지능(AI) 도구와 기술을 통해 이러한 새로운 캠퍼스 환경을 이해할 수 있습니다. 타사 툴과 어시스턴트를 적용하여 네트워크에서 생성된 방대한 데이터를 쉽게 수집, 구조화 및 처리할 수 있습니다. 이를 통해 대응 및 의사결정을 자동화하거나 네트워크를 간단히 관리할 수 있습니다. AI나 AI 어시스턴트는 캠퍼스에서 뛰어난 사용자 경험을 손쉽게 제공할 수 있도록 해줍니다.

필수적인 캠퍼스 기능

AI 기반 운영 : 경험이 새로운 업타임이 되면 캠퍼스 네트워크의 역할이 더욱 중요해집니다. 셀프 드라이빙 네트워크는 데이터를 활용하여 AI와 자동화를 지원함으로써 이상을 신속하고 효과적으로 파악하고 근본원인을 식별합니다.

하지만 그외에도, 주니퍼는 복잡한 시스템에 관여하기 위해 난해한 명령보다 자연어 질문으로 궁극적인 사용자 환경을 위한 “오피스에서 만족하지 못하는 클라이언트는 누구인가” 또는 “AP ap-1은 어떤가” 같은 기본적인 질문을 사용할 수 있기를 기대합니다.

PoE(Power over Ethernet): 수십 년 된 기술이 그러하듯이 PoE에는 여러 버전이 있습니다. 다양한 표준으로 15W부터 새로운 PoE++에서 허용되는 100W까지의 전력 공급이 가능합니다.

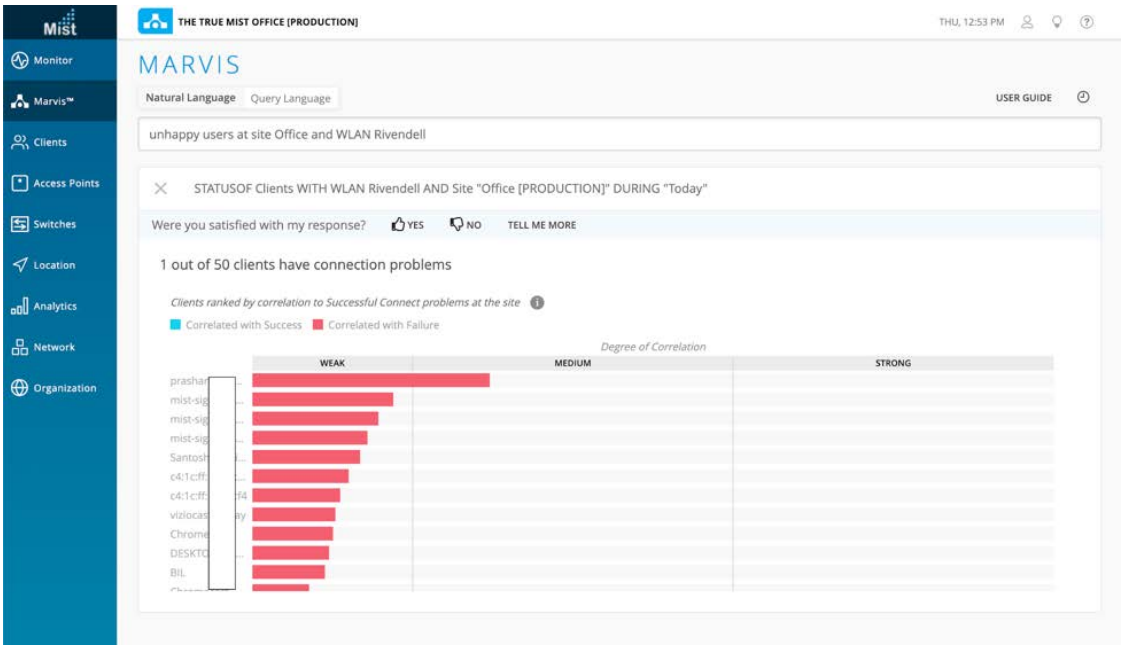
PoE는 케이블 수를 절반까지 줄이므로 캠퍼스의 물리적 배선이 대폭 간소화됩니다. 애플리케이션 및 디바이스에 따라 적절한 PoE 포트 수, 총 PoE 예산 및 PoE 포트당 전력량을 고려하여 캠퍼스 액세스 스위칭을 선택해야 합니다.

멀티기가비트 이더넷: 기존의 802.11n Wi-Fi 네트워크에서 새로운 WiFi 6 표준으로 전환하면 Wi-Fi 액세스 포인트에 1GbE 액세스 속도보다 높은 처리량이 필요합니다. 멀티기가비트 이더넷으로 업그레이드하면 기존의 케이블링 인프라를 사용하여 보다 높은 처리량의 액세스 포인트를 지원할 수 있습니다.

최신 캠퍼스 스위치는 1GbE 및 2.5GbE 액세스가 가능한 포트를 제공하며, 그중 다수가 1GbE, 22.5GbE, 5GbE 및 10GbE 포트를 제공합니다. 차기 네트워크 리프레시 시점에서 멀티기가비트 이더넷 포트 추가를 고려하십시오.

MACsec: 많은 정부 기관들이 캠퍼스 환경에서 액세스 스위치와 다양한 컴퓨팅 디바이스 간에 MACsec 암호화를 사용하도록 규정하고 있습니다. 해커가 비즈니스 데이터를 도용하는 것을 방지하기 위해 많은 기타 업계 및 관련 산업 전문가 또한 이 추가적인 보안을 채택하고 있습니다. 이제 MACsec 암호화는 액세스, 어그리게이션 및 코어 스위칭 디바이스에서 사용되고 있으며, 1GbE ~ 10GbE 및 훨씬 더 빠른 속도에서 코퍼 및 파이버 기반 링크를 보호합니다.

소형 및 팬리스 액세스 디바이스: 이제 집적 회로의 발전으로 조직은 캠퍼스 환경 전반에 걸쳐 무소음 팬리스 스위치를 구축할 수 있게 되었습니다. 이러한 스위치는 개방형 사무실 작업 공간, 교실, 심지어 호텔 객실까지 낮은 소음 수준을 필수적으로 유지해야하는 모든 곳에 구축될 수 있습니다. 소음이 없는 팬리스 스위치는 컴팩트하며 다양한 장착 옵션을 제공하여 다양한 구성으로 구축될 수 있습니다. 이러한 스위치는 네트워크에 안전하게 유선 연결할 수 있는 디바이스의 수를 늘리는 동시에 각 디바이스에 완전히 자동화되고 보안 네트워크 액세스가 가능한 포트를 제공합니다.



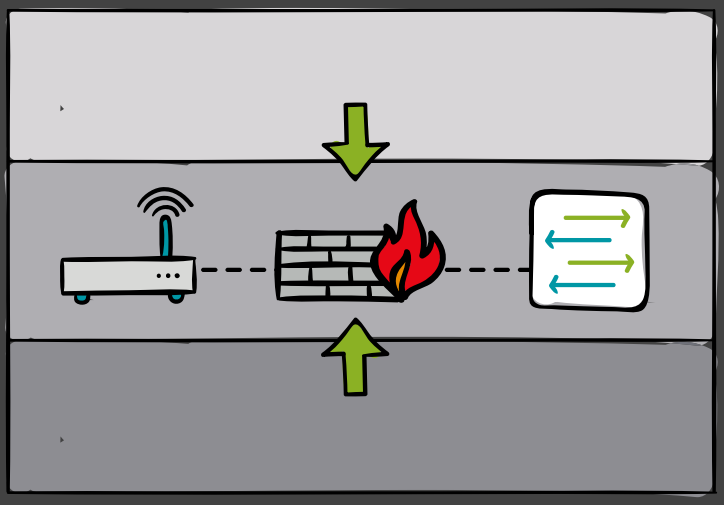
주니퍼 캠퍼스 네트워크를 **선택해야 하는 5가지 이유**

1 AI 기반 캠퍼스와 그 너머

주니퍼의 Mist AI 기반 플랫폼은 AI, 머신 러닝, 데이터 과학을 유연한 최신 마이크로서비스 클라우드를 통해 제공하는 강력한 유무선 솔루션으로, 네트워크에 대한 탁월한 분석 정보와 자동화 기능을 활용하여 고객의 사용자 경험을 최적화할 수 있도록 지원합니다.

Mist 플랫폼은 Wi-Fi 보장(Wi-Fi Assurance), Marvis 버츄얼 네트워크 어시스턴트, BLE 사용자 인게이지먼트(User Engagement), BLE 자산 가시성(Asset Visibility)을 위한 서비스를 제공합니다.

Mist Assurance는 유무선 포트폴리오를 통합하여 사용자 환경과 네트워크 운영에 대한 완벽한 가시성을 제공합니다.



2 간소화된 운영

네트워크의 각 개별 스위치에서 운영 및 구성 작업을 실행하는 것은 큰 부담이 될 수 있습니다. 주니퍼는 스위치 관리를 간소화하기 위해 고객의 확장 요구에 따른 다양한 패브릭 아키텍처를 지원합니다.

Virtual Chassis와 MC-LAG 및 EVPN-VXLAN과 같은 표준화된 기술은 다수의 분산된 주니퍼 스위치를 단일 논리적 디바이스로 상호 연결하고 관리할 수 있도록 함으로써 네트워크 복잡성 및 운영 비용을 줄여줍니다.

CSO(Contrail Service Orchestration)는 소프트웨어 정의 LAN, WAN, Wi-Fi를 위한 중앙 집중식 클라우드 기반 관리를 제공합니다. 제로 터치 구축을 지원하므로 네트워크를 즉시 가동할 수 있습니다. CSO는 EX 시리즈 이더넷 스위치, SRX 시리즈 차세대 방화벽 및 NFX 시리즈 버추얼 서비스 디바이스를 포함한 모든 주니퍼 디바이스를 지원합니다. 유무선 운영을 위한 통합 WAN 및 LAN의 가시성까지 제공할 수 있습니다.

3 커넥티드 시큐리티(Connected Security)

주니퍼 커넥티드 시큐리티(Connected Security)는 조직의 전체 멀티 클라우드 인프라를 모니터, 자동화 및 보호하기 위해 top to bottom, end-to-end 네트워크 보안을 제공합니다. 주니퍼 커넥티드 시큐리티(Connected Security)는 네트워크 전체에 심층적인 네트워크 보안과 여러 적용 지점을 제공합니다.

주니퍼 커넥티드 시큐리티(Connected Security)는 자동화된 동적 정책 적용과 함께 ATP(Advanced Threat Protection), 통합 ID 관리, 차세대 사용자 기반 방화벽 및 고급 분석 기능을 제공합니다. EX 시리즈 스위치를 포함한 모든 네트워크 요소가 네트워크 보안에 관여합니다.

주니퍼 커넥티드 시큐리티(Connected Security)는 경계 보호를 넘어서 네트워크 세그멘테이션(Network segmentation)을 포함함으로써 조직의 전체 인프라를 실행 도메인으로 전환합니다.

간단하고 직관적인 연결 보안 기능의 한 예는 MACsec입니다. MACSec은 두 네트워크 노드 간 전송을 도청하는 공격자로부터 네트워크를 보호하는 암호화 메커니즘입니다. 액세스 레이어 스위치에서 코어 및 어그레이게이션 스위치에 이르기까지 EX 시리즈 이더넷 스위치 제품군은 MACsec을 지원하여 네트워크를 통해 전송할 때 데이터가 어디에 있든 데이터의 보안을 보장할 수 있습니다.

4 투자 보호를 위한 공통 구성요소

처리량과 용량에 대한 요구가 높아지면 조직은 대체로 캠퍼스 네트워크를 확장합니다. 주니퍼의 Virtual Chassis 기술을 사용하면 최대 10개의 스위치를 지원하도록 구성을 확장할 수 있습니다. 또한 동일한 구축 환경에서 여러 EX 시리즈 스위치를 결합하여 1GbE, 10GbE, 40GbE 및 100GbE 인터페이스를 혼합 사용함으로써 보다 높은 처리량으로 간편하게 업그레이드할 수 있습니다.

확장성을 높이려면 EVPN-VXLAN 패브릭 아키텍처를 살펴보십시오. 이 기술을 사용하면 네트워크를 재설계하거나 대대적인 업그레이드를 수행할 필요 없이 비즈니스 요구에 맞게 코어, 어그리게이션, 액세스 레이어 디바이스를 쉽게 추가할 수 있습니다.

5 단순한 캠퍼스 포트폴리오

코어 및 어그리게이션부터 캠퍼스 에지에 이르기까지, 주니퍼 네트웍스는 모든 캠퍼스 인프라 요구를 만족시키는 간단하고 프로그래밍 가능한 솔루션을 제공합니다. Wi-Fi, Bluetooth LE 및 IoT 기술을 실내 및 실외 구축 모델과 통합할 수 있는 단순하고 다양한 엔터프라이즈 액세스 포인트 포트폴리오입니다. 액세스에서의 PoE++ 및 멀티기가비트는 최신 WLAN 표준 및 가장 높은 전력 공급을 요구하는 IoT 디바이스를 지원합니다. 고정 및 모듈식 10, 40 및 100GbE 코어 및 어그리게이션 디바이스는 고가용성을 제공하여 모든 규모의 캠퍼스 구축을 지원합니다. 또한 풍부한 기능의 WAN 에지 디바이스 포트폴리오는 차세대 방화벽 기능, 보안 라우팅, SD-WAN 및 강력한 검증된 라우팅 스택을 제공합니다.

> **"사용자의 기대치를 뛰어넘습니다. Junos와 Mist는 클라이언트 SLE(Service Level Expectations)를 보장합니다."**

주니퍼 네트웍스를 선택해야 하는 이유

주니퍼 네트웍스는 안전하고 자동화된 캠퍼스 네트워크를 제공합니다. 주니퍼 라우터, 스위치 및 방화벽은 상용 및 맞춤형 실리콘 기반의 공통 구성요소를 사용함으로써 다양한 확장성 및 비용 요구 사항을 지원할 수 있습니다.

주니퍼 네트웍스 Junos® 운영 체제를 바탕으로 설계된 캠퍼스 네트워크와 보안 디바이스는 프로그래밍 인터페이스 기능, 실시간 텔레메트리, 통합 기능 및 관리 도구를 갖춘 공통으로 자동화 된 프레임워크를 공유합니다.

통합된 Juniper Mist 솔루션은 유무선 네트워크에 분산된 인텔리전스를 통해 유연하고 단순화된 아키텍처를 제공합니다. 이를 통해 더 높은 수준의 성능, 보안, 안정성을 제공하여 궁극적으로 최종 사용자 환경을 개선합니다.

주니퍼 캠퍼스 포트폴리오

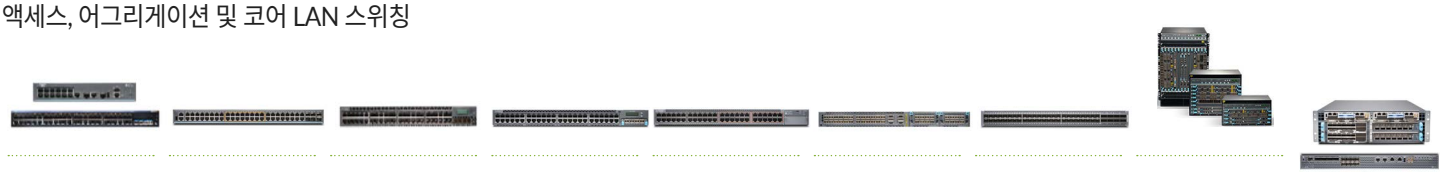
주니퍼 멀티클라우드 레디 캠퍼스 및 브랜치 포트폴리오

	엔트리 레벨	미드레인지	프리미엄	
에지	 SRX/NFX 시리즈	 SRX 시리즈	 MX 시리즈	
코어/ 어그리게이션	 EX4600/4650	 EX9250	 EX9200	 Juniper Sky Enterprise
액세스	 EX2300	 EX3400	 EX4300	

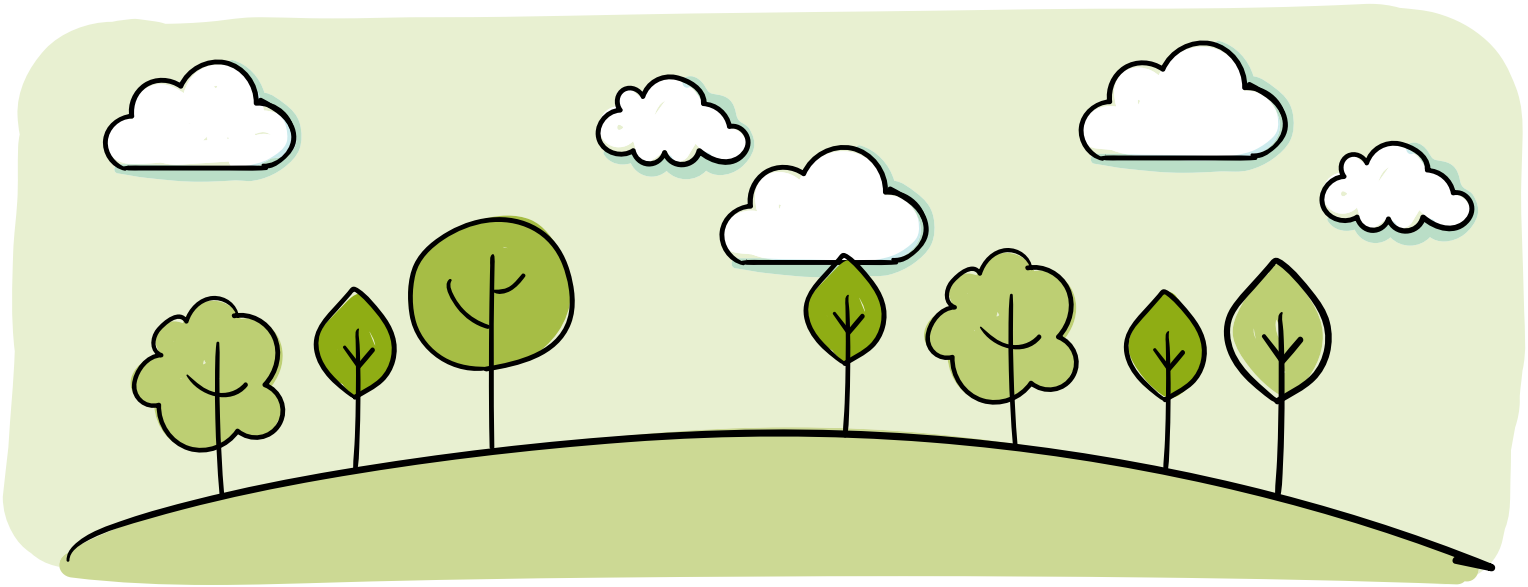
주니퍼 캠퍼스 포트폴리오

EX 시리즈 이더넷 스위치 포트폴리오

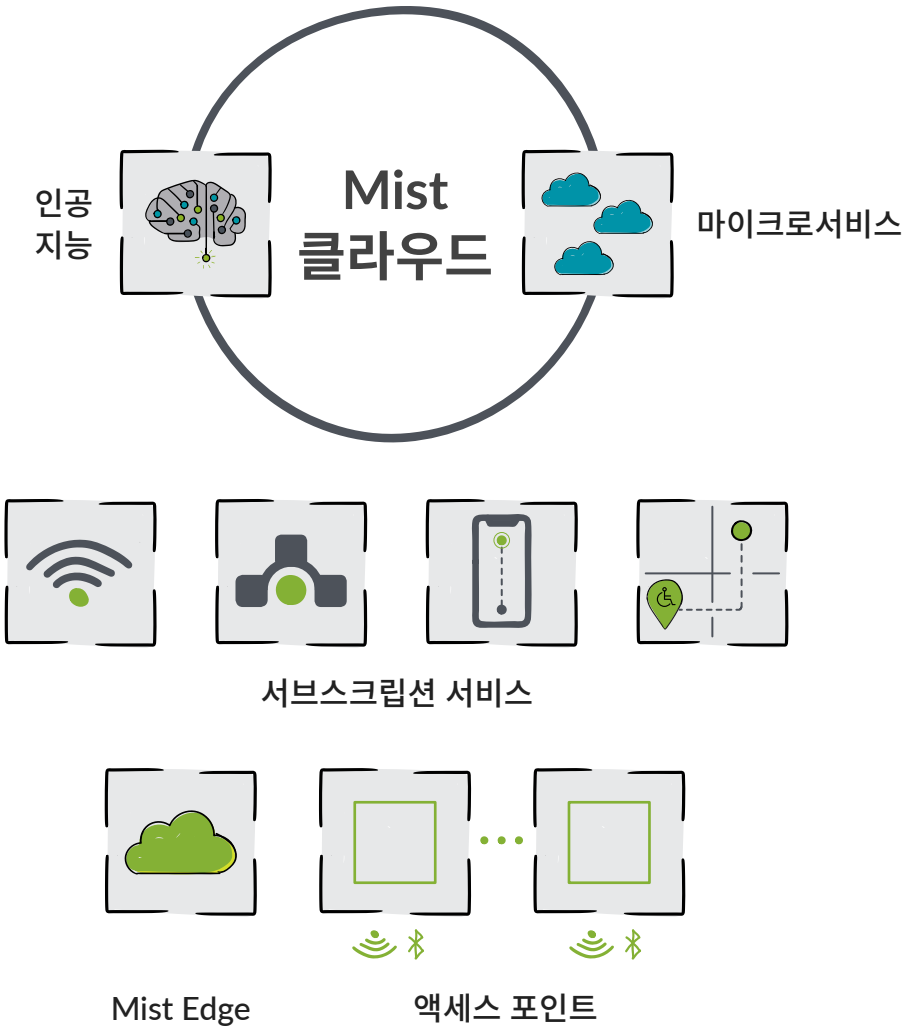
액세스, 어그리게이션 및 코어 LAN 스위칭



EX2300-C/EX2300	EX2300 멀티기가비트	EX3400	EX4300	EX4300 멀티기가비트	EX4600	EX4650	EX9200	EX9250
액세스	멀티기가 액세스	액세스	액세스 및 어그리게이션	멀티기가 액세스 및 어그리게이션	어그리게이션	코어 및 어그리게이션	코어 및 어그리게이션	소형 코어 및 어그리게이션
12-24-28 x GE 2-4 x 10GE SFP+		24-48 x GE 4 x 10GE SFP+ 2 X 40GE QSFP+	24-48 x GE 4 x 10GE SFP+ 2 X 40GE QSFP+		72 x 10GE SFP+ 12 x 40GE QSFP+	48 x 10GbE 8 x 100GbE	최대 320 x 10GE 최대 60 x 40GE 최대 20 x 100GE	최대 144 x 10GE 최대 36 x 40GE 최대 24 x 100GE
PoE/PoE+	PoE/PoE+	PoE/PoE+	PoE/PoE+	PoE/PoE+/PoE++	N/A	N/A	N/A	N/A
VC(Virtual Chassis) 기능					VC 및 MC-LAG	MC-LAG 및 EVPN-VXLAN	MC-LAG	



Mist 무선 LAN 플랫폼



AP43: 최고 성능의 802.11ax Wi-Fi, Bluetooth® LE, IoT

AP61: 실외 Wi-Fi 및 Bluetooth®

AP41: 최고 성능의 802.11ac Wi-Fi, Bluetooth® LE 및 IoT

AP21: 최고 성능의 802.11ac Wi-Fi 및 Bluetooth® LE

BT11: 엔터프라이즈급 Bluetooth® LE

Toolkit Tuesdays 웨비나에 등록하여 Mist Wired Assurance의 라이브 데모를 확인해 보십시오.
지금 juniper.net/wired-assurance-tuesdays에서 등록하기

본사

Juniper Networks, Inc.

1133 Innovation Way
Sunnyvale, CA 94089 USA

전화: 888-JUNIPER
(888-586-4737) 또는 +1.408.745.2000

팩스: +1.408.745.2100

한국주니퍼네트웍스

서울 강남구 테헤란로 142
아크플레이스 19층

우편번호 06236

전화: 02-3483-3400

팩스: 02-3483-3488

PN 7400100-004-KR

참고 :

이 가이드에는 법적 문제에 대한 일반적인 정보가 포함되어 있습니다. 법률 정보는 조언이 아니므로 조언으로 간주해서는 안 됩니다.

이 가이드의 모든 법률 정보는 명시적이거나 묵시적인 어떠한 진술이나 보증도 없이 “있는 그대로” 제공됩니다. 주니퍼 네트웍스는 이 가이드의 정보와 관련하여 어떠한 진술이나 보증도 하지 않습니다.

변호사 또는 기타 전문 법률 서비스 제공업체의 법률 조언을 대신하여 이 가이드의 정보에 의존해서는 안 됩니다. 이 가이드의 정보로 인해 법적 조언을 구하는 것을 지연하거나 법률 조언을 무시하거나 법적 조치를 시작하거나 중단해서는 안 됩니다.

출판 당시에 정확한 정보(2020년 3월).

JUNIPER NETWORKS | Engineering Simplicity