일관성과 협업으로 업계 최고의 네트워크 보안을 유지하는 방법

클라이언트 에지에서부터 데이터센터 애플리케이션까지 강력한 보안 보장

목차

에지에서 시작되는 보안

주니퍼는 취약점을 획기적으로 줄이는 동시에 네트워크 및 보안 관리를 간소화합니다.

자세한 내용 →

기본적으로 보안 유효성은 보안이 위협을 얼마나 잘 방지하고, 탐지하며, 대응하는지에 따라 간단히 측정됩니다.

일반적인 환경에서 보안은 클라이언트 에지의 최종 사용자로부터 시작되며, 클라이언트 에지는 직원들이 디바이스와 상호 작용하고 회사의 리소스에 접근하는 지점을 의미합니다. 이 계층의 보안이 약하면 그 영향이 연쇄적으로 발생하여 데이터센터의 가장 민감한 IP를 위험에 처하게 할 수 있습니다.

따라서 "보안은 에지에서 시작된다"는 원칙은 아무리 강조해도 지나치지 않습니다.

직원이 악성 첨부 파일이 포함된 겉보기에는 무해한 이메일을 여는 경우를 생각해 볼 수 있습니다. 만약 엔드포인트에 적절한 보안 제어가 부족하다면, 이는 사용자의 디바이스뿐 아니라 잠재적으로 전체 네트워크를 위협하는 침해로 이어질 수 있습니다. 순간적인 판단 오류가 비즈니스에 지속적인 영향을 미칠 수 있습니다.

이것이 바로 현대 조직이 보안에 대한 포괄적인 접근 방식을 채택하여 클라이언트 에지에서부터 데이터센터 애플리케이션에 이르기까지 모든 구성 요소가 위협으로부터 사전에 강력히 보호되도록 보장해야 하는 이유입니다. 위협을 완화하는 가장 좋은 방법은 위협이 시작되기 전에 차단시키는 것입니다.

핵심 보안 트렌드

조직은 갈수록 정교해지는 사이버 위협에 대응하여 네트워크 성능을 저하시키지 않으면서도 최신 보안 기술을 활용하여 포괄적인 보호를 제공하는 솔루션이 필요합니다.

01 AI를 활용한 사이버 보안 강화

오늘날의 디지털 세계에는 전통적인 보안 조치로는 대응하기 어려울 정도로 빠르게 움직이는 지능형 위협이 존재합니다. 인공 지능(AI)은 방대한 양의 데이터를 실행 가능한 인사이트로 변환하여 비정상적인 동작과 잠재적인 위험이 네트워크에 영향을 미치기 전에 신속하고 정확하게 사전에 식별합니다.

02 SASE(Secure Access Service Edge)

엔터프라이즈들이 모바일 엔드포인트에서 클라우드와 원격 근무자를 수용함에 따라 전통적인 네트워크 경계는 모호해졌습니다. SASE는 네트워크 연결성과 보안 기능을 하나의 클라우드 기반 서비스로 결합한 네트워크 아키텍처입니다.

03 제로 트러스트 보안

상호 연결된 디지털 시대에 전통적인 보안 경계는 사라졌습니다.
제로 트러스트는 침해를 가정하고 어디에서 발생하든 관계없이 모든 액세스 요청을 검증함으로써, 승인된 사용자와 장치만 네트워크에 접근할 수 있도록 보장합니다.

03 갈수록 복잡해지는 상황

계속되는 지연으로 인한 문제

급속한 네트워크 아키텍처의 발전으로 인해 인력 분산, 클라우드 호스팅 애플리케이션, 다양한 디바이스 간의 연결성 강화 시대가 열렸습니다.

이러한 새로운 환경은 공격접점(Attack Surface)의 확장으로 이어졌으며, 이에 따라 보다 탄력적이고 지능적이며 적응 가능한 보안 조치가 필요하게 되었습니다.

그렇다면 오늘날 거의 모든 네트워크 팀이 거대한 벽을 마주한 듯한 막막함을 느끼는 이유는 무엇일까요?

문제는 이러한 추가 보안 조치가 네트워크 인프라에 지연 문제를 야기한다는 것입니다. 네트워크 자체가 사용자들에게 불편을 주는 원인이 되고 있는 것입니다. 또한 문제 해결은 시간이 많이 소요되고 수동 작업이 필요하며, 팀은 사일로화된 시스템과 단편화된 데이터를 탐색하면서 문제를 효율적으로 정확하게 찾아 해결하는 데 어려움을 겪고 있습니다.

설상가상으로 네트워크 팀과 보안 팀 간에 서로를 비난하고 책임을 전가하는 문화가 만연하여 갈등을 초래하고 협업을 방해하고 있습니다.

이러한 현실들은 사용자가 요구하는 빠르고 원활한 경험을 제공하는 데 큰 어려움을 초래합니다. 네트워크가 더 안전하고 복잡해질수록 성능은 더욱 저하될 수 있으며, 이는 결국 사용자와 사업자 모두에게 불만과 의심을 불러일으킬 수 있습니다.

73%

네트워크 환경이 불과 2년 전보다 다소 또는 훨씬 더 복잡해졌다고 밝힌 조직의 비율[1]

Enterprise Strategy Group

04 혼란을 극복하고 협업으로

혼란을 극복하는 협업의 압도적인 이점

역사적으로 네트워크 팀과 보안 팀은 단합된 힘으로 협력하기보다는 단편화되고 고립된 각자의 영역에서 역할을 수행하는 경우가 많았습니다.

네트워크 팀의 주요 관심사는 항상 최적의 연결성과 성능을 유지하는 것이지만 보안 팀의 주요 관심사는 이러한 연결, 애플리케이션 및 이를 통과하는 민감한 데이터를 보호하는 것입니다.

이러한 현실은 쉽게 혼란과 책임 전가, 그리고 결과적으로 취약점으로 이어질 수 있습니다. 보안 인시던트가 발생하면 빠르게 책임 전가로 변질될 수 있습니다. 네트워크 팀은 보안 팀이 충분한 조치를 취하지 않았다고 생각하고, 반대로 보안 팀은 네트워크 팀이 빌미를 제공했다고 생각합니다.

이러한 집중의 단편화는 사용자의 보안 태세에 매우 해로울 수 있습니다.

네트워크 팀과 보안 팀이 통합된 선제적인 위협 탐지 및 인시던트 대응 절차를 구축함으로써 네트워크나 보안 관련 문제가 발생할 때 실시간 공동 커뮤니케이션과 협력적이고 정보에 입각한 의사 결정을 보장할 수 있습니다.

네트워크 팀과 보안 팀 간의 협업을 촉진함으로써 얻을 수 있는 운영상의 이점은 헤아릴 수 없이 큽니다. 통합 접근 방식을 통해 보안 유효성을 향상시킬 수 있을 뿐 아니라, 운영을 간소화하고 네트워크가 최적의 수준에서 계속 성능을 발휘하도록 보장할 수 있습니다. 중복 프로세스 실행이나 의사소통 오류로 인해 네트워크 중단이나 보안 문제가 발생하는 대신 두 팀이 보다 효율적이고 효과적으로 협력할 수 있습니다. 이것이 바로 윈-윈입니다.

64%

자신의 조직이 향후 24개월 동안 네트워크 팀과 보안 팀의 통합을 적극적으로 추진하는 방향으로 나아갈 것이라고 말하는 응답자의 비율[2]

Enterprise Strategy Group

05 일관된 정책의 강력한 힘

사이버 범죄를 막기 위한 정책 경로

네트워크 및 애플리케이션 계층 전반에서 보안 정책의 일관성을 유지하는 것이 가장 중요합니다.

일관된 정책이 없으면 조직은 사이버 범죄자들이 적극적으로 악용하는 보안 공백으로 인해 어려움을 겪을 수 있습니다.

모든 디바이스가 암호화 및 강력한 인증 프로토콜과 같은 특정 보안 기능을 갖추어야 한다는 정책이 있다고 가정해 보십시오. 이 정책을 일관되게 시행하면 모든 수준의 데이터를 보호할 뿐 아니라 네트워크 팀과 보안 팀 모두에게 기대 사항을 명확히 하는 강력한 프레임워크가 생성됩니다.

모두가 같은 생각을 가지고 있으면 오해나 불일치 발생의 소지가 줄어들고 보다 안전한 환경이 조성됩니다.

필요한 것은 네트워크 벤더의 전체 포트폴리오에 걸쳐 네트워크 보안을 강화하는 보안 정책 엔진입니다. 이는 이전의 구성 및 보안 표준이 클라이언트 에지에서부터 데이터센터에 이르기까지 모든 플랫폼과 모든 위치에 걸쳐 적용된다는 것을 의미합니다.

모두가 같은 생각을 가지고 있으면 오해나 **불일치 발생의 소지가 줄어들고 보다 안전한 환경이** 조성됩니다.

06 새로운 방식

네트워크를 보호하는 새로운 방식

통합된 제로 트러스트 보안 원칙과 첨단 AI 기능은 보안을 약화시키지 않으면서 뛰어난 네트워크 성능을 보장합니다.

AI 네이티브 보안을 통해 주니퍼는 네트워킹과 보안 모두에 대해 경험 최우선 접근 방식을 취합니다. 이는 한 지점에서 다른 지점(라우팅, 스위칭, 액세스 포인트)으로 데이터를 이동하는 역할을 하는 네트워크 인프라를 사용하여 지연이나 다른 성능 문제를 일으킬 위험 없이 동시에 데이터 보안을 유지하는 것을 의미합니다.

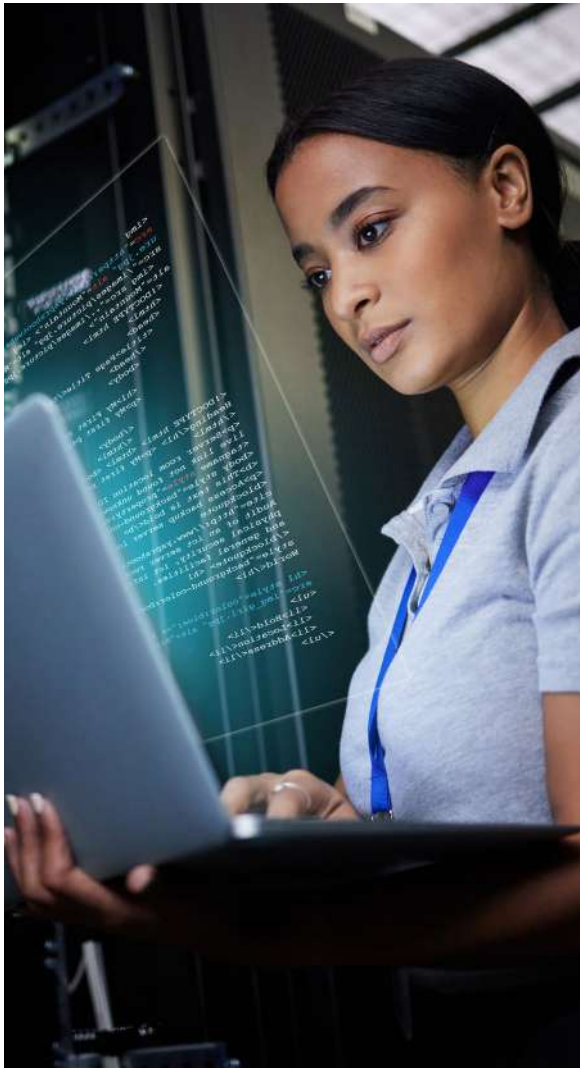
생산성이 문제가 될까요?

네트워크 보안 팀은 네트워크 AI와 자동화를 활용하여 운영 효율성 향상을 경험하고 있습니다. Enterprise Strategy Group에 따르면 62%의 조직에서 위협 탐지 속도가 향상되었으며, 52%는 위협 탐지 정확도가 향상되었다고 합니다[3]. 이를 통해 네트워크 보안 팀의 업무가 더욱 편리해지고 전체적인 생산성이 향상됩니다.

주니퍼 AI 네이티브 보안은 공통 Mist AI 콘솔에서 모두 액세스할 수 있는 네트워킹, 보안, AIOps의 통합 제품군을 통해 생산성 최적화를 지원합니다. 탁월한 가시성과 이에 따른 고급 AI 인사이트를 통해 위협을 더 빠르게 선제적으로 식별하고 대응할 수 있습니다.

일관성과 단순함의 만남

Mist UI에 통합된 AI 기반 네트워크 및 보안 텔레메트리를 통해 주니퍼의 시큐어 AI 네이티브 에지 및 보안 데이터센터 솔루션이 함께 작동하여 통합되고 자동화된 보안 및 네트워크 관리를 제공합니다. WAN 에지에서 원격 사용자까지 그리고 클라우드에서 데이터센터까지, 네트워킹과 보안 모두에 일관된 정책이 적용되어 탁월한 운영 효율성과 보호 기능을 제공합니다.



47%

네트워크 팀과 보안 팀 모두가 액세스할 수 있는 기술을 보유하고 있거나 구축할 예정이라고 답한 응답자의 비율[4]

Enterprise Strategy Group

07 시큐어 AI 네이티브 에지

주니퍼 시큐어 AI 네이티브 에지를 통해 책임 전가에서 협업으로 전환

단일 공통 클라우드 및 UI에서 AIOps, 네트워킹 및 보안을 통합하는 최초이자 유일한 보안 에지 솔루션입니다.

주니퍼 시큐어 AI 네이티브 에지는 네트워크 보안 제공 방식을 향상시키 완전한 SASE(Secure Access Service Edge) 아키텍처를 제공하여 높은 이동성을 가진 직원들을 어디에서나 보호합니다. 이는 통합된 가시성, 운영 민첩성, 강력한 위협 보호 기능을 제공하여 운영 팀이 네트워크 성능에 영향을 미치지 않고 보다 빠르게 보안 결정을 내릴 수 있도록 돕습니다.

협업 강화, 생산성 증대

업계 최고의 AIOps를 통해 공통 운영 포털에서 네트워킹 및 보안을 통합하는 유일한 시큐어 AI 네이티브 에지 솔루션을 제공합니다. 이는 협업 및 네트워크 가시성을 개선하고, 보다 효율적으로 문제를 해결하며, 보안 인시던트에 더 빠르게 대응할 수 있도록 해줍니다.

풀스택, 포괄적인 보호

시큐어 AI 네이티브 에지는 웹, SaaS 및 온프레미스 애플리케이션에 대한 포괄적인 보안을 제공합니다. 사용자가 어디에 있든, 어떤 디바이스를 사용하든 상관없이 일관되고 안전한 액세스를 보장하여 광범위한 디지털 위협으로부터 효과적으로 보호합니다.

AI 기반 SD-WAN으로 연결성 향상

시큐어 AI 네이티브 에지는 주니퍼의 AI 기반 SD-WAN과 통합되어 최고의 SASE 접근 방식을 제공합니다. 이러한 통합은 WAN 운영을 간소화하고, 클라우드 애플리케이션의 성능을 개선하며, 위치에 관계없이 안전하고 최적화된 연결을 보장하는 데 도움이 됩니다.

관리 및 구축 용이성

시큐어 AI 네이티브 에지는 다양한 플랫폼과 위치 전반에서 보안 프로토콜을 간소화하고, 일관성을 보장하며, 복잡성을 줄이는 통합 정책 관리를 통해 IT 운영을 간소화합니다. 보안 결정이 더욱 빨라진다는 것은 네트워크가 의도한 대로 FAST를 실행할 수 있다는 것을 의미합니다.

"가시성은 보안 우선 접근 방식의 일부라고 할 만큼 중요합니다. 시스템과 네트워크에 어떤 일이 일어나고 있는지 알 수 없다면 통제하고 보호할 수 없습니다."

Seth Tabor CTO, Syntrio

08 보안 데이터센터

주니퍼의 보안 데이터센터로 모든 곳에서 보안 서비스 운영화

오늘날 많은 애플리케이션과 워크로드가 여러 프라이빗 및 퍼블릭 클라우드 환경에 걸쳐 분산되어 있어 복잡성이 가중되고 공격접점(Attack Surface)이 커짐에 따라 데이터센터는 빠르게 "데이터의 중심"이 되고 있습니다.

주니퍼의 보안 데이터센터는 데이터센터 보안의 중요한 발전을 의미하며 기존 보안 방식과 현대 디지털 환경의 요구 사항 간의 격차를 해소합니다. 주니퍼의 AI 기반 보안의 일부인 보안 데이터센터는 통합 관리 경험, 단일 정책 프레임워크, 업계에서 가장 효과적인 위협 보호 기능을 제공합니다.

제로 트러스트 자동화

하이브리드 환경 전반에 걸쳐 제로 트러스트 보안을 확장하고 승인된 액세스와 마이크로세그먼테이션을 적용합니다.
또한 애플리케이션이 새로운 클라우드 환경으로 마이그레이션할 때 수동으로 재구성하지 않아도 어디든 적용할 수 있는 보다 효과적인 보안 정책도 만들 수 있습니다.

탁월한 확장성

이 아키텍처는 섀시 크기 및 폼 팩터와 관련된 기존 제한을 제거하여 제약 없이 보안 서비스와 성능을 확장할 수 있도록 해줍니다. 이러한 개방형 확장성을 통해 새로운 하드웨어에 지속적으로 재투자할 필요 없이 데이터센터가 조직의 요구에 맞춰 발전할 수 있습니다.

기존 하드웨어 활용

기존 투자를 활용함으로써 추가적인 큰 비용 없이
확장 가능한 고성능 아키텍처를 활용하여 포워딩 디바이스의 용도를 변경할 수 있습니다.

주니퍼의 보안 데이터센터 솔루션은 새로운 위협으로부터 데이터센터를 보호하는 동시에 확장성, 안정성, 고성능을 보장하려는 현대 조직을 위한 강력하고 확장 가능한 솔루션입니다.

"주니퍼 덕분에 원하는 방식으로 네트워크를 마이크로세그먼트화할 수 있는 뛰어난 유연성을 갖춘 동급 최고의 방화벽을 보유할 수 있게 되었습니다."

Seth Tabor CTO, Syntrio

09 외부 테스트

검증을 통한 장기적인 보안 강화

주니퍼는 솔루션의 유효성을 독립적으로 검증하기 위한 외부 테스트를 강력히 지지합니다.

CyberRatings.org와 같은 신뢰할 수 있는 테스트 기관에서 지난 5년 동안 업계 최고의 유효성 결과를 기록한 솔루션을 통해 모든 구성에서 99% 이상의 유효성을 제공하는 것으로 입증된 주니퍼 제품을 안심하고 구매하고 구축할 수 있습니다.

주니퍼는 보안 인프라에 대한 투자가 사후 대응이 아닌 선제적 조치로 조직에 실질적 이익을 제공하도록 약속합니다. 설치된 보안 도구가 압박 속에서도 잘 작동할 것이라고 빠르게 확신할 수 있으므로 기업은 취약성보다는 성장에 집중할 수 있습니다.

주니퍼의 신뢰성을 입증하는 추가 증거인 실제 고객 사례는 AI 네이티브 보안 솔루션의 혁신적인 잠재력을 강조합니다.

99.7%

주니퍼 vSRX 가상 방화벽의 보안 효과성.[5]

CyberRatings.org

10 결론

탁월한 필수적 보안 유효성을 제공하는 주니퍼

오늘날의 사이버 위협 환경에서 클라이언트 에지에서부터 데이터센터 애플리케이션에 이르기까지 보안 유효성을 달성하는 것은 필수적인 과제입니다.

일관된 정책에 투자하고 네트워킹 팀과 보안 팀 간의 협업을 촉진함으로써 사용자는 보안 태세를 강화할 수 있을 뿐 아니라, 통합된 조직을 통해 운영 효율성도 높일 수 있습니다.

주니퍼 네트웍스는 엄격한 테스트를 통해 입증된 보안 유효성을 제공하는 데 주력하고 있습니다. 테스트를 거듭할수록 최고의 점수를 받고 지속적으로 가장 낮은 오탐률을 기록하는 것은 팀을 안심시킬 수 있는 요소입니다.

기업들은 진화하는 위협에 대응하기 위해 올바른 도구, 효과적인 커뮤니케이션, 그리고 협업 문화를 비롯한 통합 전략을 우선순위에 두어야 합니다. 고객들은 클라이언트 에지에서부터 데이터센터, 클라우드에 이르기까지 네트워크의 모든 위치에서 효과적인 보안을 제공하는 주니퍼의 AI 네이티브 보안 솔루션을 사용할 수 있습니다.

주니퍼는 **지난 5년 동안 외부 독립기관 유효성 테스트에서 빠짐없이 1위를 차지했으며** 모든 사용 사례에서 99% 이상의 효과성을 보였습니다.

11 사례 연구

AmeriTrust

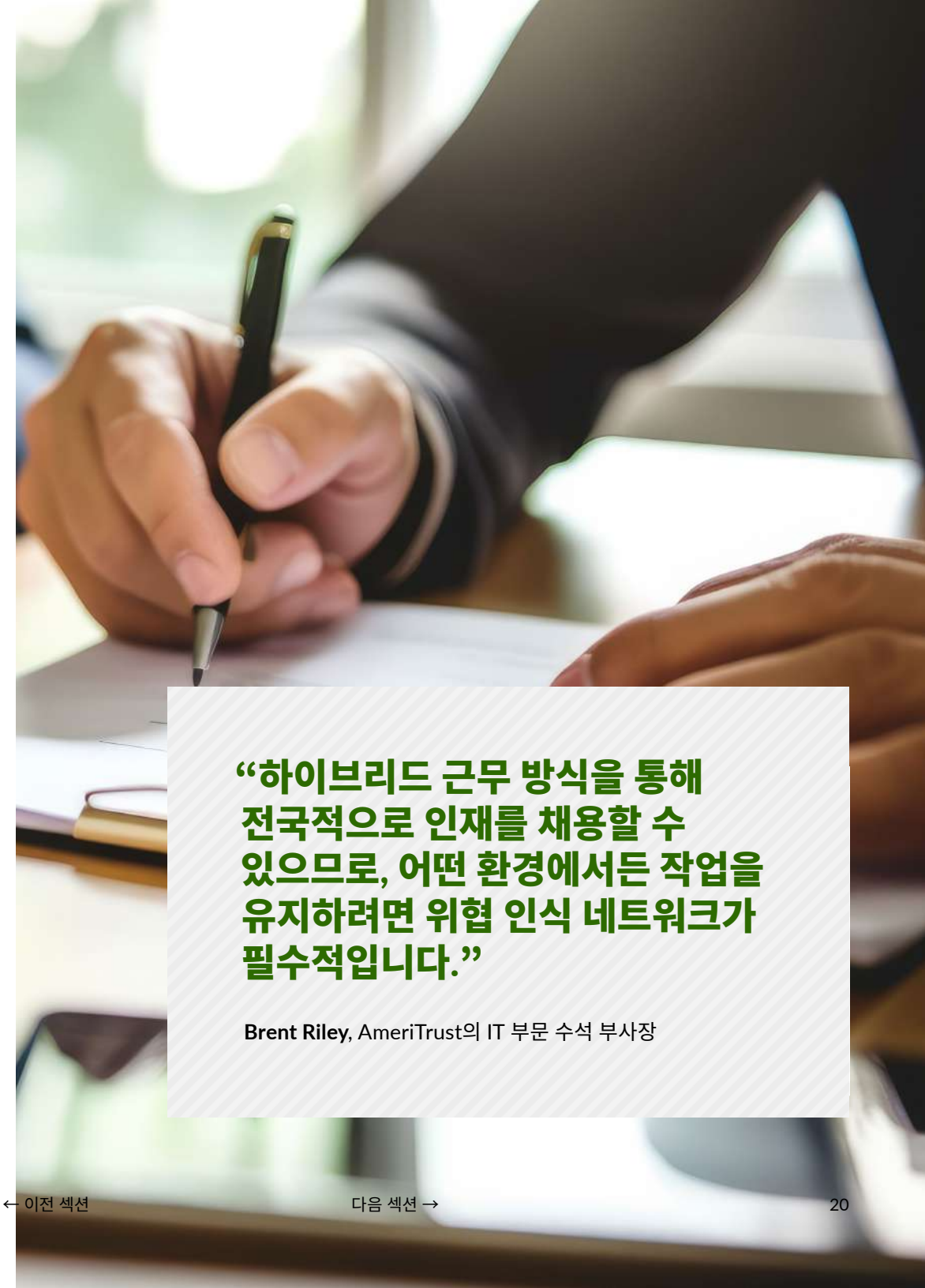
주니퍼의 위협 인식 네트워크는 복원력과 고객 경험을 향상시킵니다.

과제: 고객 및 데이터 보호

전문 상업 보험 인수 및 관리 서비스 회사인 AmeriTrust는 운영을 단순화하고 보안을 최우선으로 생각했습니다. 뉴욕과 캘리포니아를 비롯한 다양한 산업 및 주 차원의 보안 규정으로 인해, 이 회사는 사이버 공격으로부터 보호하고 데이터 개인정보 보호 의무를 지키기 위해 할 수 있는 모든 조치를 취하고 있는지 확인해야 했습니다.

결과: 최적화되고 안전한 사용자 경험

AmeriTrust는 제로 트러스트 액세스 제어 및 세그먼테이션을 통해 최적화되고 안전한 사용자 경험을 제공하는 애플리케이션 인식 네트워크 패브릭을 위한 주니퍼 세션 스마트 라우터를 통해 엔터프라이즈 WAN을 한 단계 더 발전시켰습니다. 아울러 주니퍼의 차세대 방화벽(NGFW)은 네트워크 에지에서 가시성, 제어 및 차단 기능을 제공합니다. 동작 및 실시간 위협 탐지 기능과 결합하여 AmeriTrust의 사용자, 애플리케이션 및 디바이스를 보호합니다.



"하이브리드 근무 방식을 통해 전국적으로 인재를 채용할 수 있으므로, 어떤 환경에서든 작업을 유지하려면 위협 인식 네트워크가 필수적입니다."

Brent Riley, AmeriTrust의 IT 부문 수석 부사장

보안을 한 단계 더 발전시키기 위한 액션 가이드

해당 e-book을 통해 보안 유효성에 대해 표면적으로 다룰 수 밖에 없었으나, 적어도 조직 내에서 같은 생각을 가진 다른 사람들과 소통할 때 훌륭한 대화의 시작점이 될 수 있기를 바랍니다. 추가적으로 보안 유효성에 관한 지식을 확장하기 위해 지금 바로 실행할 수 있는 네 가지 방법을 소개해 드립니다.

01

AI 네이티브 보안 수용

이제 사용자가 요구하는 탁월한 경험을 희생하지 않고도 부서 간 사일로를 제거하고, 생산성을 향상시키며, 위험을 완화할 수 있다는 아이디어를 받아들이십시오.

02

비용상의 이점 고려

네트워크와 보안 가시성을 하나의 AI 기반 플랫폼으로 통합함으로써 중복 도구를 제거하고, 워크플로우를 간소화하며, 전반적인 복잡성을 줄이는 데 도움이 된다는 사실을 잊지 마십시오.

03

보안 데이터센터에 대한 이해

이 인포그래픽을 통해 “보이지 않는 부분에 대한 가시성”, “반드시 자동화가 필요한 영역” 등 진정한 제로 트러스트 데이터센터의 10가지 요소를 보다 정확하게 이해해 보시는 것을 추천드립니다.

04

외부 테스트 보고서 참조

클라우드 네트워크 방화벽 및 엔터프라이즈 방화벽에 대한 2024년 보고서를 최근 게시한 CyberRatings.org와 같은 외부 테스팅 조직에서 얻은 업계 최고의 유효성 결과를 살펴보십시오.

다음 단계

전문가와 연결

주니퍼 네트웍스가 클라이언트 에지에서부터 데이터센터 애플리케이션에 이르기까지 강력한 보안을 보장하는 여정을 어떻게 안내할 수 있는지 알아볼 준비가 되셨습니까? 무료 상담을 예약하십시오.

문의 →

고객 사례 알아보기

주니퍼 AI 네이티브 보안이 어떻게 고객의 과제를 다양한 산업과 상황에서 성과를 창출하는 기회로 바꾸었는지 알아보십시오.

필라델피아 →

Syntrio →

Scripps →

자세히 알아보기

주니퍼 AI 네이티브 보안에 대해 더 많은 내용을 알아보고, 공통 클라우드를 통해 모두 통합된 네트워킹, 보안, AIOps의 통합 제품군으로 생산성을 향상시키는 방법에 대해 알아보십시오.

사이트 방문하기 →

평가판 사용

주니퍼의 AI 네이티브 네트워킹 플랫폼을 더욱 경제적으로, 쉽게 사용할 절호의 기회입니다. 다양한 동영상, 데모, 기간 한정 혜택을 통해 이를 경험해 보십시오.

확인 →

저자 소개

Jeff Aaron

제품 마케팅 담당 GVP,
주니퍼 네트웍스

Jeff는 AI 네이티브 네트워킹 포트폴리오 전반에서 전 세계 주니퍼 전체 제품군 홍보를 담당합니다. Jeff는 다양한 소프트웨어, 네트워킹, 통신 회사에서 근무하며 하이테크 분야에서 24년이 넘는 시간 동안 마케팅 관련 경력을 쌓았습니다. Jeff는 듀크대학교에서 컴퓨터 과학과 경제학을 전공하고 학사 학위를 받았습니다.

주니퍼 네트웍스에 대하여

주니퍼 네트웍스는 우수한 연결과 우수한 연결 상태는 전혀 다른 개념이라고 생각합니다. 주니퍼의 AI 네이티브 네트워킹 플랫폼은 처음부터 AI를 활용하여 에지에서부터 데이터센터와 클라우드에 이르기까지 탁월하고 보안이 뛰어나며 지속가능한 사용자 경험을 제공하기 위해 구축됩니다. 자세한 정보는 www.juniper.net/kr/ko에서 확인하시거나 X(Twitter), LinkedIn, Facebook에서 주니퍼를 찾아보십시오.

자세한 정보

주니퍼 AI 네이티브 보안에 대해 자세히 알아보려면 주니퍼 담당자나 파트너에게 문의하거나 juniper.net/kr/ko/security.html을 방문하십시오.

참고 자료

01 최신 네트워크를 위한 AI 네이티브 요구 사항, Enterprise Strategy Group, 2024년 1월. https://www.juniper.net/us/en/forms/2024/ai-native-networking-platform-requirements-for-modern-networks.html

02 네트워크 및 보안 융합에 대한 네트워크 관점, Enterprise Strategy Group, 2024년 1월. https://research.esg-global.com/reportaction/515201726/Marketing?SearchTerms=network%20security%20collaborate%29

03 설문조사 결과 완료: 네트워크 인프라 운영에서 AIOps의 역할,
Enterprise Strategy Group, 2024년 4월.
https://research.esg-global.com/reportaction/515201780/Marketing?SearchTerms=The%20role%20of%20AIOps

04 네트워크 및 보안 융합에 대한 네트워크 관점, Enterprise Strategy Group, 2024년 1월. https://research.esg-global.com/reportaction/515201726/Marketing?SearchTerms=network%20security%20collaborate%29

05 2024 클라우드 네트워크 방화벽 보고서, CyberRatings.org, 2024년 4월. https://www.juniper.net/us/en/forms/2024/2024-cyberratings-cloud-network-firewall-report.html

juniper.net

Juniper Networks Inc.
1133 Innovation Way
Sunnyvale, CA 94089

7400200-001-KO, 2024년 10월