CLOUDFLARE

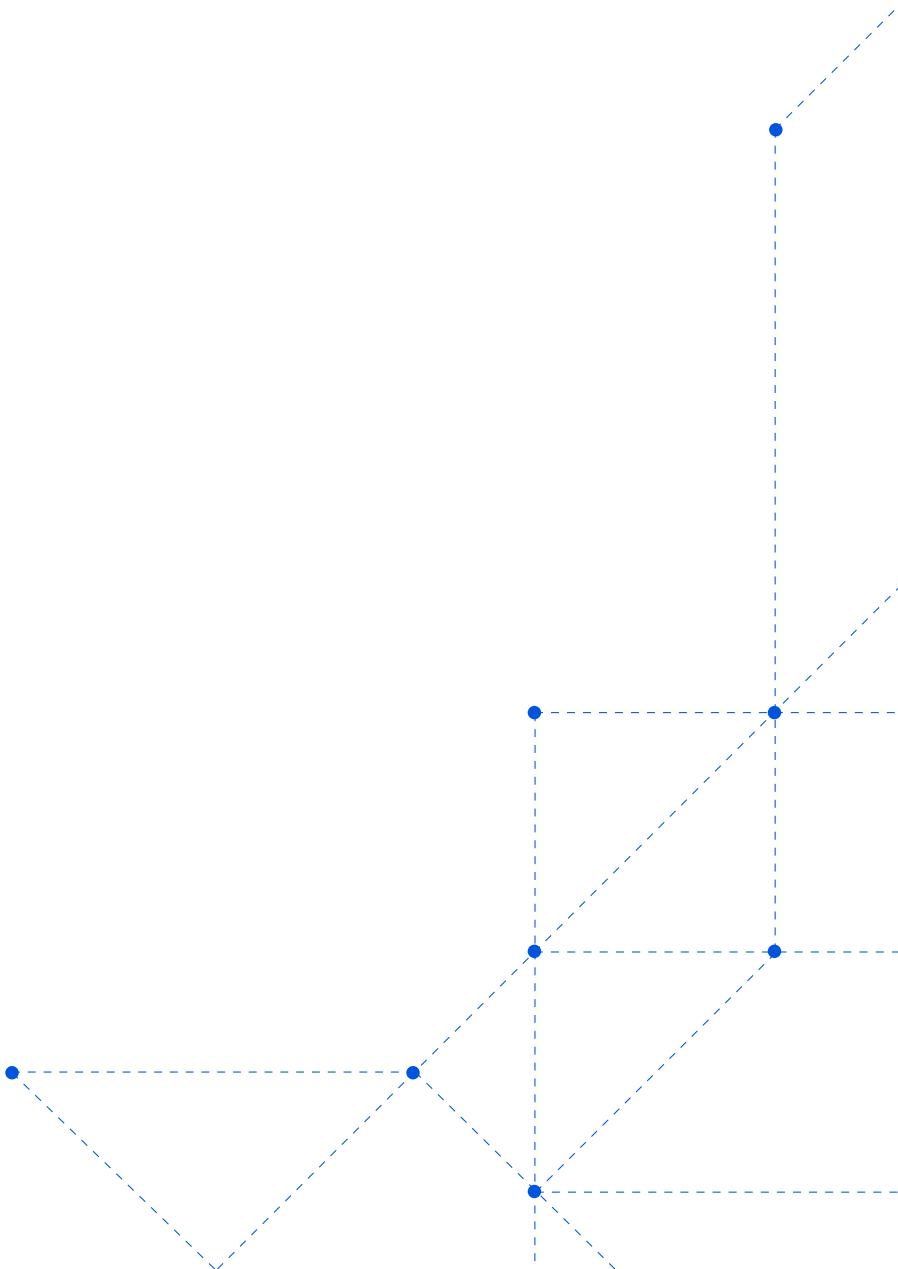
백서

네트워크 하드웨어 장치의 종말

지금 네트워크 하드웨어를 업그레이드 해야하는 이유

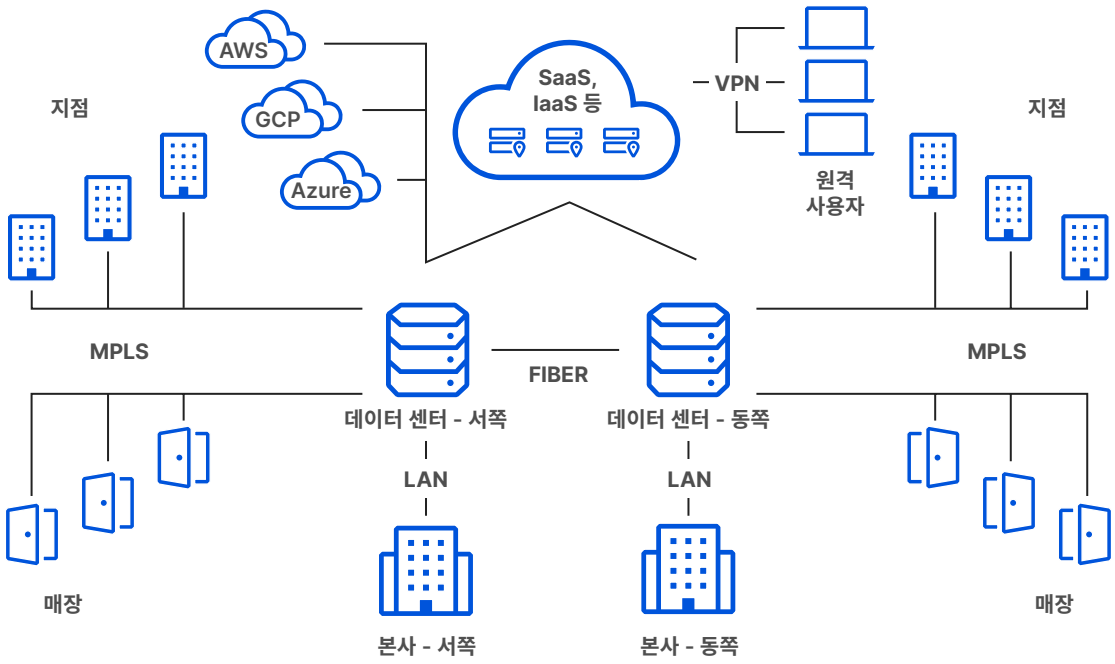
핵심 요약

스토리지와 컴퓨팅이 클라우드로 옮겨졌지만 여전히 다수의 네트워킹 기능이 온프레미스에 남아 용량 제한, 높은 총소유 비용, 지원 문제, 보안 격차를 유발하고 있습니다. 하이브리드 작업이 이미 표준으로 자리잡았지만 조직들은 지금도 적절한 용량과 효과적인 보안을 확보하는 데 어려움을 겪고 있죠. 하드웨어 백로그가 1년 넘게 이어지면서 많은 전환 프로젝트도 정체되고 있습니다. 본 문서에서는 이러한 문제를 살펴보고, 그에 따른 결과를 정량화하며, 하이브리드 클라우드 인프라의 속도, 경제성, 보안을 개선하기 위한 클라우드 기반 솔루션을 제안합니다.



소개

클라우드 마이그레이션이 인프라 비용을 절감하고, 데이터 및 애플리케이션의 가용성을 향상시키고, 운영 민첩성을 증가시키는 데 효과적인 전략이라는 것은 이미 입증됐습니다. 하지만, 마이그레이션이 한 번에 이루어지는 경우는 드뭅니다. 많은 대형 조직에는 멀티 클라우드와 온프레미스 인프라가 복잡하게 섞여 있습니다.



이러한 하이브리드 인프라가 꼭 나쁜 것은 아니지만, 복잡성을 초래하는 것만은 분명합니다. 특히 DDoS 완화, 로드 밸런싱, 방화벽, VPN 등의 다양한 네트워크 기능이 온프레미스에 유지되는 상황이 발생합니다.

레거시 네트워크 하드웨어 장비들은 클라우드 중심 환경에서 중요한 인프라를 보호하고 가속화하는 역할을 해낼 수 없습니다. 이 장비들은 비싸고 거미줄처럼 얽힌 케이블을 통해 손쓸 수 없을 만큼 복잡하게 연결되어 있어, 늘 골칫거리였습니다. 이 상황에 클라우드까지 추가되면 곧바로 보안 격차, 성능 저하, 추가 지원 문제까지 뒤따를 것이 분명합니다.

이 문서에서는 클라우드로 옮겨가는 지금 세계에서 네트워크 하드웨어를 유지하는 데 따르는 위험과 문제를 설명하고 더욱 안전하고 효과적으로 네트워크를 구축하는 전략에 대해 설명합니다.

클라우드 세계에서 하드웨어의 위험

네트워크 하드웨어는 다양한 특정 기능을 위한 것이며, 조직마다 조금씩 다르게 사용니다.

일반적인 사례는 다음과 같습니다.

보안

- DDoS 방어
- 방화벽
- VPN(Virtual Private Network)
- 구성 가능한 정책

성능 및 신뢰성

- 부하 분산
- 트래픽 가속/WAN 최적화
- 패킷 필터링
- 트래픽 분석

이 하드웨어가 온프레미스에 배포되는 경우, 아키텍처는 일반적으로**공급망 부담, 용량 제한, 높은 총 소유 비용, 지원 문제, 보안 격차**의 다섯 가지 위험을 겪게 됩니다.

가장 수준 높은 네트워크 및 보안 팀이라도 처음 세 가지 범주에서는 항상 문제를 겪습니다. 나머지 두 범주는 클라우드 마이그레이션으로 완화할 수 있습니다.

공급망 부담

다른 물리적 제품과 마찬가지로 네트워킹 하드웨어도 다양한 공급망 문제에 취약합니다. 재료비가 오르거나, 특정 재료와 구성요소를 구하기가 더 어려워지거나, 배송업체의 부담이 커질 때 네트워킹 하드웨어를 구매하여 재배치하는 일은 더욱 어려워지죠.

안타깝게도 코로나19 팬데믹이 막대한 영향을 미치면서 최근에는 이러한 문제들이 더욱 보편화되었습니다. Gartner Research에 따르면, "팬데믹 이전에는 납품소요시간이 4~6주 정도였다면 지금은 보통 200~300일에 달하며, 고객에게 430일 이상의 납기로 견적을 내는 경우도 목격됩니다."

이러한 지연은 여러 요인으로 발생합니다.

- **물류 문제:** 물류 문제: 지금까지의 공급망 모델에는 여러 장애 지점이 존재하고, 최소 인력이 부족하며, 그 안전성 여부가 확인되지도 않은 기술들에 지나치게 의존했는데, 결국 그런 점들이 최근에 와서는 문제의 원인이 되었습니다. 팬데믹 동안 많은 공장이 문을 닫았고 배송업체들은 배송이 지연되고 있으며, 다양한 유형의 공급망 근로자를 고용하고 유지하기가 더욱 어려워지고 있습니다. 이러한 모든 어려움으로 인해 하드웨어를 제조하고 배송하는 데 시간이 더욱 오래 걸립니다. 모든 물류 과정에서 기억해야 할 가장 어려운 측면은 릴레이 경주와 비슷하다는 점일 수도 있습니다. 각각의 조직에서는 문제를 겪지 않더라도, 공급망 연결이 끊어지는 바람에 그 영향을 받을 수도 있기 때문이죠.
- **재료비 상승:** 네트워크 하드웨어 장비에는 다양한 원자재가 필요합니다. 수요는 많지만 공급이 제한되어 재료비가 급등했고, 이에 따라 네트워크에 필요한 장비를 구하기 위해 기업에서 더 오래 기다려야 할 뿐만 아니라 훨씬 더 많은 비용을 지불하게 되었습니다. 안타깝지만, Gartner에서는 이런 문제 때문에 2023년 초반까지 하드웨어 장비의 납기 지연이 이어질 것으로 예상합니다(출처).

이와 같은 문제점은 또다른 결과로 이어집니다. 하드웨어 박스를 조달, 유지, 교체하는 데 계속 초점을 맞출 경우 간접비가 더 많이 들고, 실행하기 보다는 계획하는 데 시간이 더 소요되며, 기약 없이 물리적 공급망을 보호해야 하기 때문에 보안 우려 사항 역시 늘어납니다. 조직에서는 물류, 납기, 조달, 하드웨어 박스 보관 등에 집중하는 대신, 고객의 니즈를 충족하는 데 집중해야 합니다.

용량 한계

네트워크 하드웨어는 특성상 트래픽의 합법성 여부에 관계없이, 예상치 못한 트래픽 급증 시 과부하를 받을 수 있습니다. 하지만 최근 추세를 보면 이러한 한계에 도달하는 일이 더욱 흔히 발생하고 있습니다.

분산 서비스 거부(DDoS) 마이그레이션을 생각해 보겠습니다. Microsoft에 따르면 사상 최대 규모의 DDoS 공격은 2021년 11월에 발생했으며 그 규모가 3.47Tbps에 도달한 것으로 알려졌습니다(출처). DDoS 공격은 시중에서 가장 성능이 좋은 DDoS 완화 하드웨어 박스가 처리할 수 있는 용량의 몇 배까지 과부하를 일으킬 수도 있습니다. 일반적으로 하드웨어 박스는 이와 같은 공격을 완화하는 데 필요한 용량의 일부만을 제공합니다.

2021년 11월, 사상 최대의 DDoS 공격이 발생했으며, 최대 3.47Tbps의 규모에 도달한 것으로 알려져 있습니다.

모든 조직이 이러한 규모의 공격을 받지는 않겠지만, 모든 조직이 최첨단 DDoS 완화 하드웨어를 실행할 수 있거나 실행하는 것도 아닙니다. Cloudflare 보고서에 따르면 2022년 1분기에 볼류메트릭 공격이 증가했습니다. 실제로, 10Mpps(초당 100만 패킷)를 넘는 공격이 전분기 대비 300% 이상 늘어났으며 100Gbps를 넘는 공격은 전분기 대비 645% 늘었습니다(출처). DDoS 공격이 급속하게 증가하는 것은 물론 걱정스러운 상황이며, 이러한 공격 유형 때문에 고용량이라고 알려진 하드웨어 기반 완화 솔루션까지도 과부하가 걸릴 수 있습니다.

게다가, 공격하는 동안 데이터 센터에 도달했을 수도 있는 합법적인 트래픽은 공격 규모에 고려되지 않습니다.

블랙 프라이데이 쇼핑 주말처럼, 전자상거래 일일 페이지 조회수가 하룻밤 사이에 평균 두 배로 증가할 수 있는 고트래픽 기간(출처)에는 트래픽이 급증하므로 소규모 공격으로도 보안 하드웨어 운영을 충분히 중단시킬 수 있죠.

DDoS 완화는 온프레미스 하드웨어의 용량 한계를 보여주는 하나의 예에 불과합니다.

다음과 같은 다른 예도 있습니다.

로드 밸런서: 개별 온프레미스 로드 밸런서는 합법적인 트래픽이 갑자기 증가하면 쉽게 과부하를 받을 수 있습니다. 이러한 상황이 발생하면, 추가 하드웨어를 프로비저닝하고 설치하는 데 많은 시간이 걸릴 수 있죠. 최악의 상황에도 대비할 수 있을 만큼 용량을 유지할 수도 있지만, 이 방법을 쓰려면 높은 비용으로 여러 하드웨어를 계속 가동해야 합니다.

가상 사설 네트워크(VPN): VPN 사용량을 미리 예측하는 일은 더욱 어려워졌습니다. 완전 재택 및 하이브리드 근무를 새로운 표준으로 삼은 조직이 많지만, 기존 VPN 접근 방식에서는 신중한 계획과 유지보수 및 관리가 필요합니다. 대부분의 VPN은 조직 전체가 지속적으로 이용하는 것을 염두에 두고 설계된 것이 아니기 때문입니다. 너무 많은 직원이 VPN을 사용하면 연결성과 안정성이 저하됩니다. 게다가 제로 트러스트 관리 없이 설계되는 VPN의 방식 특성에 따라 보안 문제가 발생할 수도 있죠. 또한 VPN에 과부하가 발생할 경우 조직에서는 웹으로 향하는 트래픽이 VPN을 거치지 않도록 트래픽을 "분할 터널링"할 수도 있는데, 그러면 직원의 웹 활동을 추적하고 관리하는 일이 어려워집니다.

이에 대한 대응으로 최신 고용량 하드웨어를 더 많이 구매할 수도 있습니다. 하지만 이러한 접근법은 다른 많은 문제를 일으킵니다.

소유 비용

용량 제한을 생각해보면 데이터 센터 하드웨어 비용이 비싼 것도 당연합니다. 예를 들어 약 100Gbps의 DDoS 완화 용량을 갖추기 위한 하드웨어 비용은 선불로 400,000~500,000달러가 필요할 수 있습니다.

게다가, 이 비용은 하드웨어 총 소유 비용의 일부에 불과합니다.

다음의 비용도 고려해야 합니다.

- 팀 비용: OSI 모델의 모든 계층을 위협으로부터 보호하고, 최신 웹 사이트 및 인터넷 응용 프로그램에서 기대되는 수준의 성능 및 안정성을 제공하기 위한 하드웨어를 구매하고, 운영하며, 유지하려면 모든 네트워킹 기능을 전문가 수준으로 이해하고 있는 팀원이 필요합니다. 특히 세계의 인력 시장이 사상 최대로 제한된 이 시기에는, 이러한 폭과 깊이의 전문성을 갖춘 팀을 구성하는 데는 아주 많은 비용이 듭니다. 2022년 ISACA 조사에 따르면 연간 조사에 참여한 2,000명의 사이버보안 전문가 중 63%가 사이버보안 직책에 결원이 있다고 응답했으며 이는 전년 대비 8% 증가한 수치입니다(출처).
- 유지 비용: 네트워크 하드웨어의 평균적인 온프레미스 부분의 평균 수명은 겨우 3년에서 5년이지만,이 전체 기간을 보증하는 데 추가 지출이 필요한 경우도 많습니다. 기술 혁신의 속도를 고려할 때 이러한 온프레미스 박스의 수명은 계속 줄어들 수밖에 없습니다. 보증을 이용하지 않는 경우에 미리 예산을 책정해 두지 않은 수리 작업이 필요하다면 원 제조업체나 제3자에게 의뢰해야 합니다. 하드웨어가 오작동하면 데이터 센터가 멈추면서 분당 평균 8,800달러 이상의 기회 비용이 발생할 수도 있습니다(출처).
- 교체 비용: 조직에서 3년마다 하드웨어 장비를 교체하려면 초기 투자 비용을 다시 지출해야 할 뿐만 아니라, 새 하드웨어를 배송하고 설치하는 데 자원을 투입해야 합니다. 교체가 늦어지면 오작동이 더 자주 발생하여 유지 비용까지 추가되죠.

이 모델과 클라우드 기반 네트워킹 서비스를 비교해 보겠습니다. 클라우드 서비스를 운영하는 팀은 복잡하지 않으며, 이 서비스는 유지 및 배송 비용이 발생하지 않고, 조직이 값비싼 업그레이드와 오작동 증가 사이에 무엇을 선택할지 고민하지 않아도 됩니다.

하드웨어가 오작동하면, 데이터 센터가 멈추면서 기회 비용이 분당 평균 8,800달러 이상 발생할 수 있습니다.

지원 문제

네트워크 하드웨어 지원은 비용이 많이 필요할 뿐만 아니라, 물류 문제도 해결해야 합니다. 최신 취약성과 공격 전술을 따라잡기 위해 하드웨어를 자주 패치해야 합니다. 이 과정은 수동 실행이 필요한 경우가 많기 때문에 인간 오류가 발생할 수 있습니다.

조직에서 사용하는 하드웨어 장비가 많을수록 중요 시스템에 미칠 영향에 유의하지 않거나, 오히려 중요 시스템에 미칠 영향을 우려하여 결국 패치를 등한시할 가능성이 높아집니다. 미국 국가안전보장국(NSA), 미국 사이버보안 및 기반시설 보안국(CISA), 미국 연방수사국(FBI)은 최근의 공동 사이버보안 권고를 통해 패치되지 않은 네트워크에 발생하는 공개적으로 알려진 결함 16가지가 광범위한 캠페인에서 악용되었다고 보고했습니다(출처). 이와 같이 결함을 악용하여 소규모 사업체의 라우터부터 기업 VPN에 이르기까지 다양한 온프레미스 디바이스가 영향을 받았으며, 공격자가 네트워크 트래픽을 조작하고 대상 네트워크에서 데이터를 유출시킬 능력을 갖출 가능성이 생겼습니다.

제시된 결함 16개가 대부분 치명적인 결함으로 분류되었음에도, 패치와 복원은 간단한 작업이 아닙니다. 사실 회사가 하드웨어를 최신 상태로 유지하기 위해 하드웨어 패치를 진행하는 일은 온갖 종류의 소프트웨어가 존재하는 만큼 매우 복잡할 수 있습니다(출처).

패치를 한 번만 게을리해도 심각한 결과로 이어질 수 있습니다. 하드웨어가 취약해질 뿐만 아니라, 패치가 배포되면 기회를 노리는 공격자는 그 패치와 관련된 취약성을 주요 표적으로 삼습니다. 이런 단점과 대조적으로, 클라우드 기반 보안 서비스에서는 취약성 해결과 업데이트 설치가 기본적으로 자동적으로 이루어지고, 클라우드 공급자의 네트워크 속도에 따라 달라질 수는 있지만 업데이트 전파에 30초 정도밖에 걸리지 않습니다.

기타 하드웨어 유지 문제에는 다음과 같은 것이 있습니다.

- **문제 해결:** 하드웨어 전용 시나리오에서는 문제 해결을 위해 IT 팀이 로드 밸런서, 방화벽, 기타 온프레미스 장치를 한 번에 하나씩 끄면서 문제를 파악하는 고된 과정을 거쳐야 할 때가 많습니다.

  이 과정은 클라우드 서비스를 동시에 사용할 때 더욱 복잡해집니다. 하드웨어를 주로 이용하는 조직은 주로 중앙 데이터 센터와 개별 장치로 해당 서비스에 대한 액세스를 관리합니다. 직원이 특정 서비스에 액세스할 수 없을 때 IT 팀이 문제를 진단하려면 확인할 추가 공간이 필요합니다. Productiv의 최신 보고서에 따르면 모든 SaaS 응용 프로그램 중 56%가 섀도우 IT의 분류에 속하거나, IT 지식 없이 조달되어 승인도, 관리도 받지 못하는 응용 프로그램에 속한다고 합니다. 그리고 이 문제는 그 범위와 규모면에서 모두 빠르게 증가하고 있죠(출처).
- **물리적 유지 보수:** 하드웨어에 장애가 발생하면 IT 팀은 물리적으로 하드웨어를 차단하고, 교체용 하드웨어를 주문하며, 테스트하고, 다시 설치해야 하는 고된 과정을 다시 겪어야 합니다. 여러 글로벌 기업의 규모를 고려하면 이렇게 주의가 필요한 장비는 전 세계 장비의 절반에 이를 수도 있습니다.

보안 간극

조직에서 최신 고용량 온프레미스 하드웨어를 지속해서 제공하고 유지하는 데 필요한 자원을 보유하고 있더라도, 그렇게 구성된 인프라는 특히 클라우드로 전환이 이루어지는 환경에서 심각한 보안 결함을 겪을 수 있습니다.

직원 액세스 관리를 생각해보겠습니다. VPN 하드웨어는 내부 데이터 센터에 호스팅된 애플리케이션과 원격 근무 중인 직원의 장치 사이에 암호화된 터널을 수립할 수는 있지만, 터널을 구축한 후 사용자 활동을 모니터링하고 보호할 수 없습니다.

직원의 장치가 맬웨어의 공격을 받거나, 피싱 공격으로 직원의 VPN 자격 증명이 유출된 경우, 공격자는 VPN 권한을 사용하여 여러 중요한 정보에 액세스할 수 있습니다. 피싱과 맬웨어는 앞으로도 심각한 위협이 될 것입니다. 피싱과 맬웨어 둘 다 심각한 위험 요소에 계속 해당되고 있으며, 위협 행위자는 상당한 금전적 이득을 얻습니다. FBI에 따르면 사이버 범죄로 인해 2021년에 69억 달러의 손실이 발생했습니다. 특히 비즈니스 이메일 손상(BEC)으로 24억 달러의 손실이 발생했죠(출처).

직원의 장치가 맬웨어의 공격을 받거나, 피싱 공격으로 직원의 VPN 자격 증명이 유출된 경우 공격자는 VPN 권한을 사용하여, 다양한, 민감한 정보를 액세스할 수 있습니다.

클라우드 서비스와 SaaS 응용 프로그램 때문에 하드웨어 중심 인프라의 보안은 더욱 복잡해집니다. 예를 들어 하이브리드 클라우드 모델을 이용하는 조직은 온프레미스 및 클라우드 인프라를 조합하여 운영합니다. 조직에서 보안 하드웨어를 클라우드 공급자에게 보낼 수는 없습니다. 이 조직이 자체 데이터 센터에서 온프레미스 하드웨어를 계속 사용한다고 하면 인프라의 각 부분을 서로 다른 방식으로 보호해야 하므로 유입되는 공격을 보안 팀에서 확인하고 통제하기 어려워집니다.

클라우드 기반 서비스는 데이터 센터와 클라우드 서비스를 단일 소프트웨어 정의 계층 아래에 통합하여, 이러한 문제를 모두 극복할 수 있습니다.

이 접근법에 대한 상세 내용은 본 문서의 범위를 벗어나므로 다음 문서에서 자세히 알아보시기 바랍니다.

- 제로 트러스트 네트워크란?
- 보안 액세스 서비스 에지란?

클라우드 기반 보안 및 성능 서비스: 장점 및 과제

클라우드를 통해 네트워크 서비스를 제공하면 공급망 부담, 용량 제한, 비용, 지원 문제, 보안 격차 등의 많은 하드웨어 관련 문제를 겪지 않을 수 있습니다.

- **공급망:** 여러 클라우드 기반 네트워킹 공급자는 최신 글로벌 아키텍처로 확장할 수 있도록 설계되므로 공급망 문제를 완화할 수 있습니다.
- **용량:** 클라우드의 분산 특성과 소프트웨어 정의 특성 덕분에, 비즈니스 규모가 커지면 간편하게 추가 용량을 준비할 수 있죠.
- **비용:** 하드웨어 추가 비용이 없거나, 미리 계획하기가 더 쉽습니다. 또한, 클라우드 서비스는 일반적으로 자본 지출이 아닌 운영 지출로 분류되기 때문에 여러 기업에 세무 및 회계상 이점이 생깁니다.
- **지원:** 서비스 공급자가 물류 및 자원 소요를 담당합니다. 또한, 자동 업데이트되므로 패치를 누락할 가능성이 없습니다.
- **보안:** 소프트웨어 정의 네트워킹 서비스로 단일 보호 계층 아래 다양한 인프라를 통합할 수 있습니다.

하지만 클라우드 네트워킹 서비스는 철저히 배포하지 않으면 그에 따른 위험이 있습니다.

위험	설명
대기 시간	일부 클라우드 기반 네트워크 기능은 스크러빙 센터 같은 특수 클라우드 기반 데이터 센터를 이용하여 DDoS를 완화합니다. 이러한 데이터 센터로 트래픽을 백홀하면 데이터 센터와 대상 서버 간 거리에 따라 대기 시간이 크게 증가할 수 있습니다. 조직에서 다양한 네트워크 기능을 사용하려고 다수의 공급자를 이용할 때 이 문제는 더 심각해집니다. 공급자와 공급자 사이에서 트래픽을 호핑해야 할 때 수백 밀리초의 대기 시간이 발생할 수 있는 것이죠.
지원	조직이 다양한 기능에 각기 다른 공급자를 사용하면 문제 해결이 어렵습니다. 정체나 중단의 원인이 어느 공급자에게 있는지 파악하기 힘들기 때문입니다.
비용	조직이 다양한 기능에 각기 다른 공급자를 사용할 때는 공급자 관리 시간(및 그로 인한 비용)이 매우 많이 필요할 수 있습니다.

이 문제를 피하기 위해서 다음과 같은 전략을 고려하세요.

- **클라우드 및 온프레미스 인프라 모두를 지원할 수 있는 공급자가 필요합니다.**
  이러한 역량이 있으면 IT팀과 보안팀이 일관된 제어 규칙을 설정하고, 한 곳에서 글로벌 트래픽을 모니터링할 수 있습니다. 더욱 복원력 강한 아키텍처를 구축하는 데도 도움이 됩니다.
  이러한 아키텍처에서는 시장 상황의 변동에 대응해 팀이 신속하게 방향을 바꿀 수 있죠.
- **서로 연동되는 다양한 네트워킹 기능을 제공하는 클라우드 공급자가 필요합니다.**
  그러면 트래픽이 네트워크 간 호핑할 횟수가 줄어 대기 시간이 감소되므로, 최종 사용자 경험이 개선됩니다. 네트워크 문제를 해결할 때는 여러 회사가 아니라 한 회사에만 연락하면 되므로 더욱 수월합니다. 물론 여러 기능을 통합하면 비용이 줄어들기도 합니다.
- **클라우드 공급자의 자체 네트워크 내 모든 위치에서 네트워크 기능을 다양하게 실행할 수 있는 공급자가 필요합니다.**
  공급자가 인수와 합병으로 서비스 포트폴리오를 확대하는 경우에도 항상 새 서비스 전체를 통합하는 것은 아니기 때문에, 특정 기능은 특정 데이터 센터를 통해서만 제공되기도 합니다. 이런 문제가 없도록 자체 네트워크 전체에서 기능을 제공하는 공급자를 고려해보세요.
- **글로벌 기반이 폭넓은 클라우드 공급자가 필요합니다.**
  이 역량은 앞서 언급한 역량을 뒷받침해주고, 그 위치와 관계없이 언제나 네트워크 가까이 최종 사용자를 배치해줍니다. 또한 넓은 네트워크 기반을 형성하여, DDoS 트래픽을 흡수하고 대용량이 필요한 기타 네트워킹 기능들도 수행할 수 있습니다.

Cloudflare가 도움을 드리는 방법

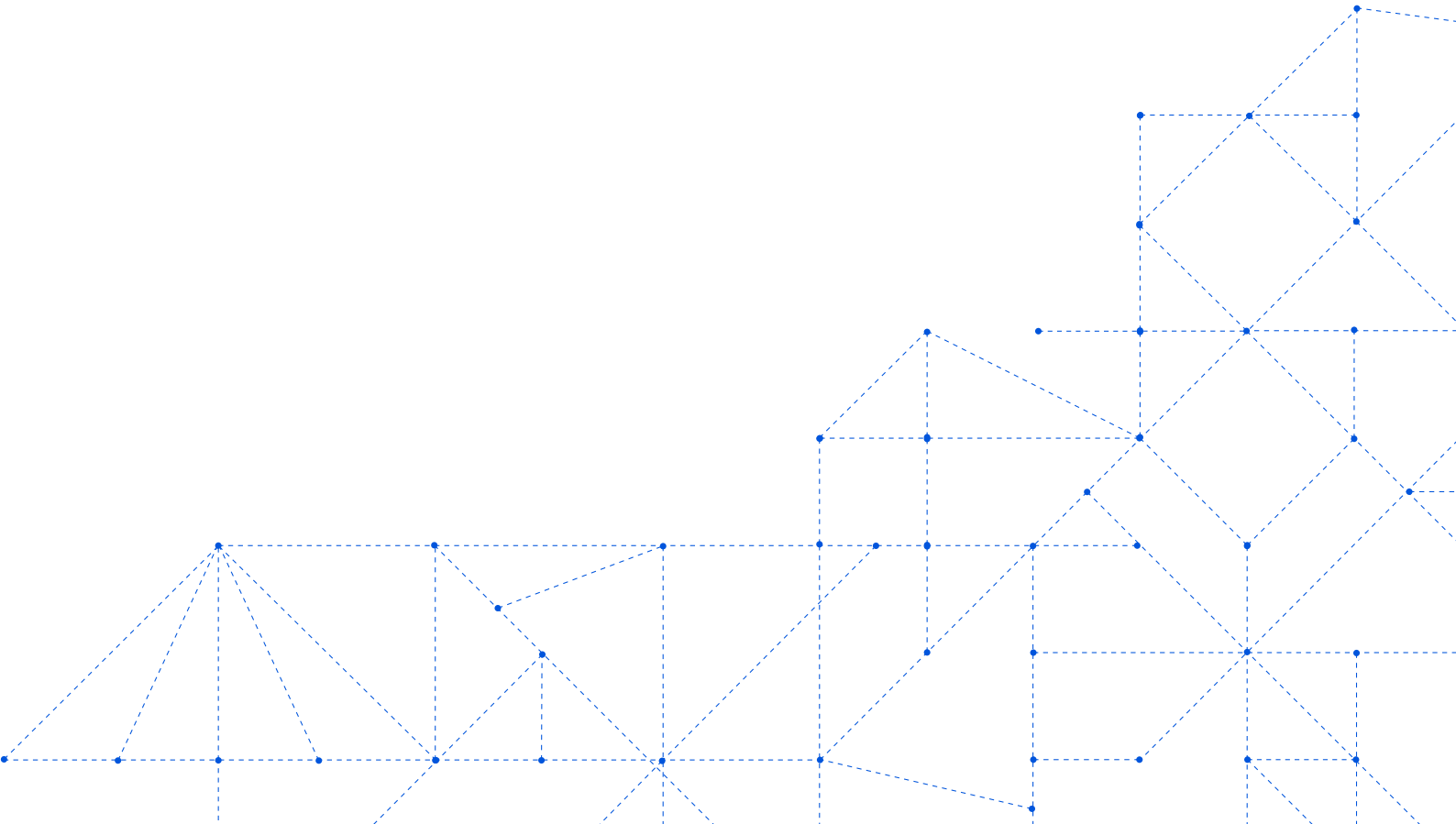
하드웨어가 도착하기를 기다릴 필요가 없고, 고작 몇 년만 이용할 수 있는 박스에 많은 비용을 쏟아붓지 않고도, 조직에서 네트워크 전환을 가속할 수 있는 방법은 무엇일까요?Cloudflare를 이용하는 것입니다.

Cloudflare는 다양한 서비스를 제공하는 글로벌 클라우드 플랫폼을 구축하여, 조직을 더욱 안전하게 보호하고, 애플리케이션 성능을 강화하고, 개별 네트워크 하드웨어 관리에 필요한 비용과 복잡성을 제거합니다. 이 플랫폼은 확장 가능하고, 사용이 쉽고, 통합된 제어판 역할을 하여 온프레미스, 하이브리드, 클라우드, SaaS(Software-as-a-Service) 애플리케이션 전반에서 보안, 성능, 안성성을 제공합니다.

결정적으로, 전 세계 270여 개 도시의 전역 네트워크에 위치한 Cloudflare의 모든 데이터 센터에서 모든 서비스를 제공할 수 있으므로, 대기 시간을 줄여 클라우드 실행이 복잡해지지 않습니다. 네트워크 스택을 간소화하고 변환을 가속하며, 이후 상황에 맞게 네트워크를 준비하세요.

자세한 내용을 알아보려면 www.cloudflare.com을 방문하세요.

> “Dropbox는 최근 '가상 우선' 조직이 되었습니다. 우리는 이 비즈니스 전략이 보안 접근법과 네트워크 아키텍처에 어떠한 영향을 미쳤는지 분석했습니다. 우리와, 우리처럼 원격을 우선시하는 다른 조직에서 이러한 '뉴노멀'을 적용할 방법을 배울 수 있게 해준 Cloudflare의 지원에 감사드립니다."
>
> Konstantin Sinichkin
> **Dropbox 엔지니어링 관리자**



CLOUDFLARE

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3313.2022JUN10