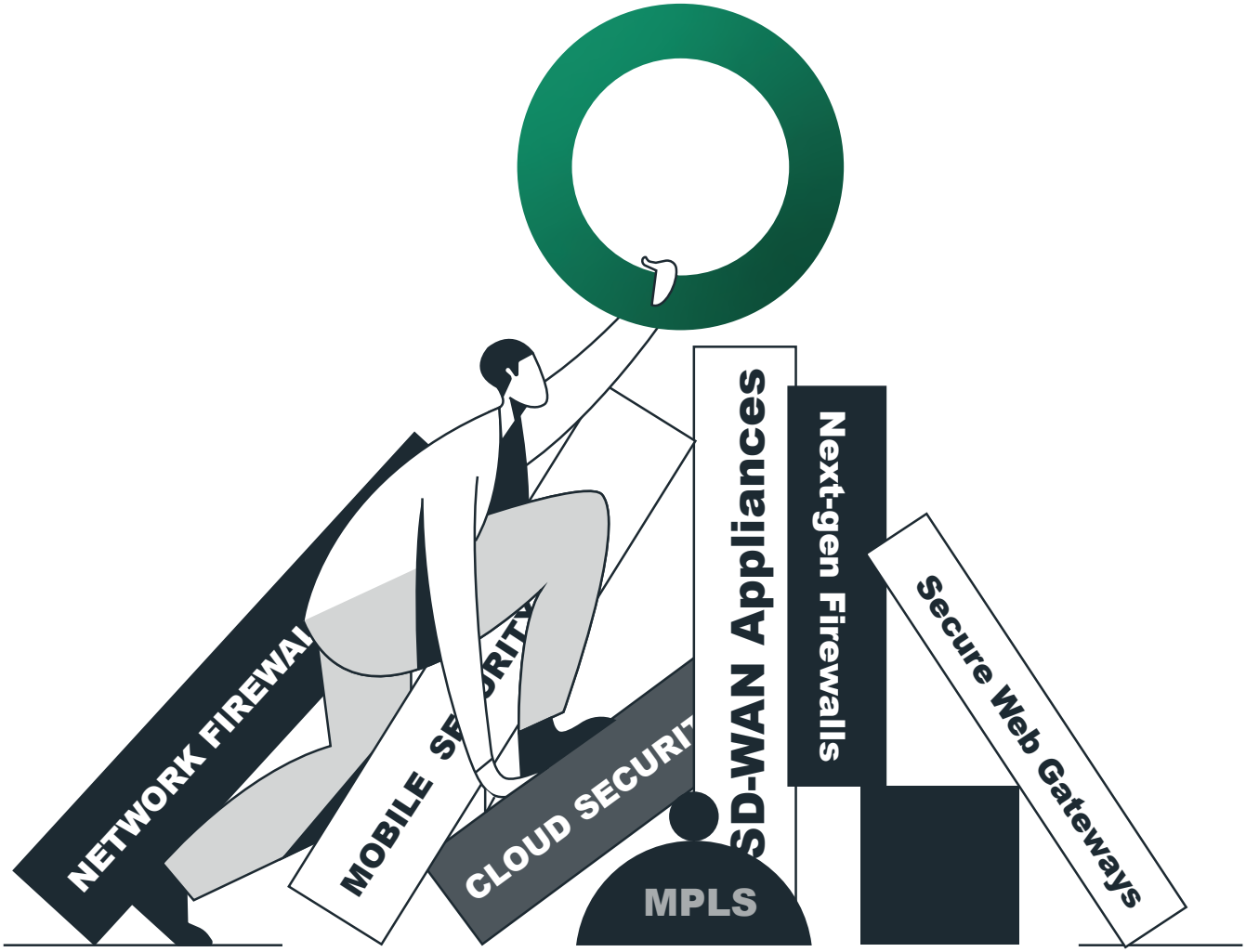
CATO
NETWORKS

디지털 비즈니스를 위한
Secure Access Service Edge (SASE)



지금은 속도전 시대 :
디지털 비즈니스와 속도의 관계

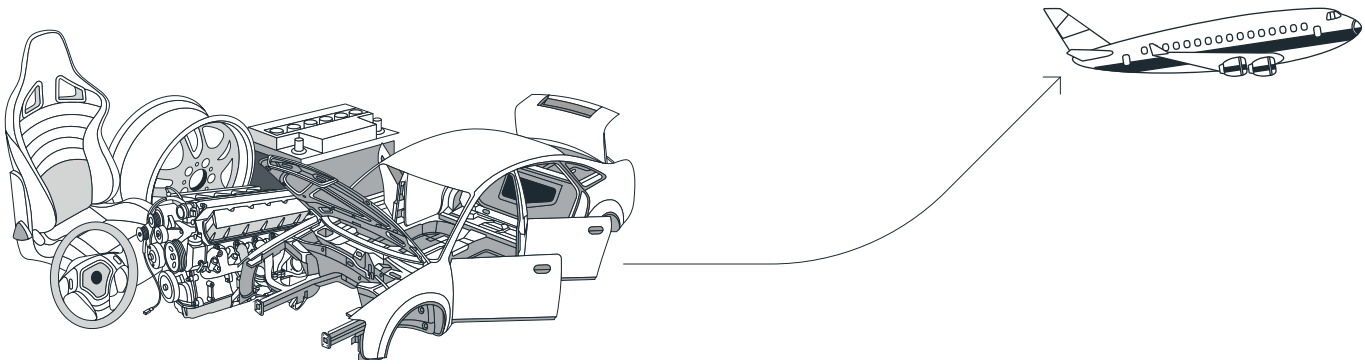
디지털 비즈니스의 관건은 속도입니다. 신제품 개발 시간, 제품의 시장 도달 시간, 사업환경 또는 경쟁구도의 변화에 대응하는 시간... 모두 속도의 문제입니다. 기술은 속도를 내는 수단이며, 이것을 가능케 하는 IT는 비즈니스 성공의 토대가 됩니다. 현대 IT 인프라는 자동화, 민첩성, 탄력성, 유연성이라는 특성을 갖습니다. 클라우드 컴퓨팅 사용이 증가하면서 우리는 이미 이러한 특성이 갖는 힘을 확인하고 있습니다.

클라우드 컴퓨팅과 달리 네트워크와 보안은 '클라우드 중심의 모바일 우선 비즈니스' 와는 고통스러울만큼 함께 가기 힘듭니다. 네트워크는 융통성이 없고 고정된 상태인데 보안 위치, 클라우드 자원, 모바일 사용자로 구성된 다수의 도메인 때문에 심각하게 파편화되어 있기 때문입니다. 네트워크와 보안은 수십년 전부터 분단된 상태가 지속되어 왔고, 그때 그때 발생하는 업무 요건에 짜깁기 방식으로 대응해왔기 때문에 사업 속도를 더디게 만들곤 했습니다.

디지털 비즈니스를 목적으로 한다면 네트워크과 보안은 IT 플랫폼에 포함되어야 합니다. 가트너는 최근 네트워크와 보안을 단일 클라우드 기반 서비스로 융합한 새로운 카테고리 SASE(Secure Access Service Edge 안전한 접속 서비스 에지)를 내놓았습니다. SASE는 비즈니스의 미래를 위한 안전한 네트워크입니다.

극복 과제 :
자동차 부품으로 제트기를 만들 수는 없다.

과거 IT 팀은 포인트 솔루션을 가지고 새로 등장하는 비즈니스 이슈를 해결했습니다.
예를 들면 용량 제약을 해소하기 위해 SD-WAN 박스를 추가하고, 인터넷 링크에 값비싼 MPLS 연결을 추가하는 식이었습니다. 또는 지점의 안전한 직접 인터넷 연결을 위해 방화벽을 설치했습니다. 이런 땜질식 처방은 포인트 솔루션들이 통합되지 못하도록 함으로써 결국 기술 사일로(silo)를 만들어 냈습니다. 궁극적으로 IT의 임무는 모든 글로벌 비즈니스 자원에게 일정한 성능과 강력한 보안을 비용효과적인 방식으로 제공하는 것입니다. 이것은 단순한 기능이 아니라, 아키텍처의 문제입니다. IT 사일로는 제거되어야 하며, 새로운 업무를 위해 도입했던 짜깁기식 '포인트 솔루션 패치' 도 없어져야 합니다. IT 아키텍처는 사일로와 포인트 솔루션을 극복하고 SASE 방식으로 진화해야 합니다.



SASE : 새로운 네트워킹 및 보안 아키텍처

SASE는 가트너의 보안 분석전문가 닐 맥도널드(Neil McDonald)와 네트워크 분석전문가 조 스코루파(Joe Skorupa)가 내놓은 새로운 카테고리입니다. SASE는 기업 네트워크와 보안 아키텍처의 전환에 관한 것으로, IT부서는 민첩하면서 디지털 비즈니스에 적용할 수 있는 총체적인 서비스를 제공할 수 있습니다. SASE 클라우드 서비스에는 4가지 주요 특성이 있습니다. 아이덴티티 드리븐(identity-driven), 클라우드 네이티브(cloud-native), 글로벌 분산 구조(globally distributed), 모든 에지 지원(supports all edges – WAN, 클라우드, 모바일, 에지 컴퓨팅)이 그것입니다.

신원 중심 : SASE 네트워킹과 보안 정책의 토대

SASE의 핵심은 신원(Identity)입니다. 모든 기업 자원에는 신원이 있습니다. 사람, 애플리케이션, 서비스, 장치는 모두 신원을 가지고 있습니다. 자원의 실체를 판단하는 기준은 물리적 위치가 아니라 바로 신원입니다. 포괄적이면서 다이내믹한 상황 인식 개념인 신원을 가지고 모든 플로우의 리스크와 네트워크 서비스 프로필을 파악할 수 있을 뿐만 아니라, 인증 방식, 보안위협 검사, 데이터 접근 인증을 결합한 결과를 의미있게 만들 수 있습니다. 신원 '파악불가' 는 순수 네트워크 벤더들의 특징이지만, 보안 업체에게는 '기본 판돈' 입니다. 보안과 네트워크가 융합되면, 접속하는 동안 신원을 중심으로 서비스 품질을 보장할 수 있고 리스크 기반 보안 통제기술을 적용할 수 있다는 장점이 있습니다.

클라우드 네이티브 (Cloud-native) : 클라우드기반 서비스 아키텍처

SASE는 클라우드에서 만들어진 서비스형 모델이라는 핵심 특성을 가집니다.
클라우드 네이티브의 아키텍처에는 탄력성, 적응성, 자가치료, 자가관리 등의 핵심 특성이 있습니다.

SASE를 사용하려면 클라우드를 구성하는 클라우드 가상 접속 포인트(PoPs) 망이 구축되어야 합니다. PoPs은 공급자 소프트웨어를 가지고 네트워크와 네트워크 보안을 서비스 형태로 공급합니다. 그리고 컴퓨터 노드를 추가해가면서 변화하는 트래픽 양에 적응하는 방식의 순조로운 확장이 가능해야 합니다. PoPs 소프트웨어는 IT의 개입 없이도 업그레이드를 통해 새로운 기능을 더할 수 있고 버그 수정도 할 수 있습니다. 또한 클라우드 아키텍처는 자동으로 장애가 발생한 노드와 PoPs에서 정상 노드로 전환할 수 있는 자가치료 기능을 반드시 포함해야 합니다.

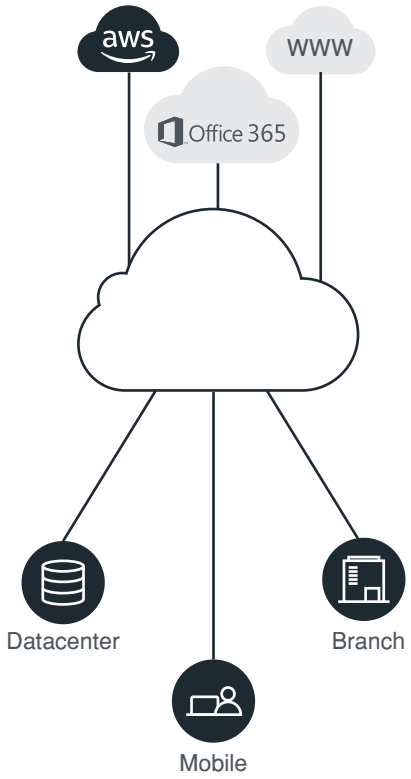
이러한 기능은 가상 어플라이언스를 클라우드에서 운영한다고 해서 가능한 것이 아닙니다. 어플라이언스란 단일 고객(싱글 테넌트)을 위해 설계되었기 때문에 탄력성과 자가치료 기능을 가지기에는 클라우드 조정 레이어가 충분하지 않습니다. 재래식 포인트 제품, 어플라언스 또는 클라우드 서비스를 엮는 방식은 서비스 품질과 성능에 영향을 줄 가능성이 큽니다.

글로벌 분산 구조

SASE 클라우드는 글로벌 분산 클라우드 플랫폼으로 구현됩니다. 고객의 에지가 어디에 있든 완전한 네트워크와 보안 기능이 제공되도록 설계되었습니다. SASE 공급자는 PoP을 전략적으로 배치하여 고객의 사업장, 클라우드 애플리케이션, 모바일 사용자 모두를 지원합니다. 가트너에 따르면 SASE PoPs는 공공 클라우드 서비스 공급자의 서비스 구역(AWS, 애저 등)을 넘어 기업 에지까지도 지연이 낮은(low-latency) 서비스를 제공해야 합니다.

글로벌 클라우드 플랫폼을 구축하려면 서비스 공급자는 PoP을 클라우드와 실제 데이터센터 모두에 신속하게 구축할 역량을 갖추어야 하고, WAN과 클라우드 접속을 지원할 수 있는 고가용성(High-capacity)과 리던던트 접속을 보장해야 하며, 에지 전체에 엔드-투-엔드 보안과 최적화 기술을 적용할 수 있어야 합니다.

에지 전체 : 실제 위치, 클라우드, 사용자, 에지 컴퓨팅



모든 기업 에지를 똑같이 지원하는 것은 SASE만의 특징입니다. 네트워크와 보안에 클라우드 우선 방식을 채택함으로써 네트워크 최적화, 보안위협 방지 등 수많은 공통의 기능을 에지에서 분리하여 클라우드 안에 배치합니다. 예를 들면, 기존 네트워크 보안 어플라이언스들은 특정 장소에 위치하기 때문에 클라우드 또는 모바일 에지 서비스에는 적합하지 않은데, SASE는 이런 문제를 해결합니다.

SASE에는 씬-에지(thin-edge) 컴포넌트가 포함되어 있어 여러 에지를 가장 가까운 SASE PoP과 연결합니다. 에지는 SASE 클라우드 서비스와 동시 작동하여 PoP 장애 또는 접속 문제를 우회하여 서비스가 지속될 수 있도록 합니다. 앞에서 언급했던 SASE 클라우드는 모든 PoP으로부터, 고객의 특정 컴포넌트에 대한 의존성 없이, 동일한 기능을 전달하도록 설계되어 있어 트래픽 전환이 단순합니다.

에지 구현은 다양하게 할 수 있습니다. 물리적 장소는 SD-WAN 장치와 다수의 인터넷 링크를 사용하여 대역폭을 최대로 늘려주고 QoS를 확보하며 접속 장애 또는 품질 저하를 극복합니다. 모바일 사용자는 엔터프라이즈급 보호를 받고 데이터센터 및 클라우드 내 애플리케이션에 최적화된 접속을 할 수 있도록 VPN 클라이언트 또는 VPN 클라이언트 없이 웹 접근을 합니다. 클라우드 데이터센터는 SASE 클라우드에 다수의 터널을 통해 연결되며, 모든 트래픽은 원천 에지와 상관없이 보안이 적용되며 최적화됩니다.

SASE의 주요 기능 : 플러그 앤 플레이, 가시성, 최적화, 제어

SASE 아키텍처에는 두 가지 핵심 구성요소가 있습니다. SASE 클라우드는 네크워크와 보안을 종합하는 기능을 합니다. SASE 에지 커넥터는 물리적 에지, 클라우드, 장치 에지에서 SASE 클라우드 프로세싱을 위해 트래픽을 이동시킵니다. SASE는 모든 트래픽을 대상으로 최적화와 리치 컨텍스트(rich context) 보안 검사기능을 효율적으로 적용하기 위해 싱글-패스(single pass), 트래픽 처리 엔진을 사용합니다. SASE 모델을 스태킹 포인트 제품들과 비교해 보십시오.
스태킹 포인트 제품은 특정 요건의 트래픽을 분석하고 복호화 등 액션을 위한 오버헤드를 더하기 때문에, 타 네트워크와 타 보안 포인트 제품에서 생성된 상황 컨텍스트 부족이 발생합니다.

주요 SASE 기능은 다음과 같습니다.

인증: 에지 연결 즉시 다이내믹 리스크 평가를 토대로 다단계 인증이 활성화됩니다.

접속: 주요 응용프로그램과 서비스 접속은 응용프로그램 인식 및 유저 인식 차세대 방화벽 정책으로 제어합니다. 또한 제로-트러스트(zero-trust) 네트워크 접속 모델 덕분에 사용자는 전체 네트워크에 접속할 필요없이 승인받은 응용프로그램에만 접속할 수 있습니다.

우선순위 설정: VoIP와 가상데스크탑접속(VDI) 등 연결장애에 예민한 응용프로그램을 최적화할 수 있도록 응용프로그램을 파악하여 예민하고 중요도가 높은 트래픽에 우선순위를 부여합니다.

복호화: 패킷 검사를 세밀하게 할 수 있도록 암호화된 트래픽은 일단 복호화를 거친 다음, 여러 위협방지 엔진들이 해당 트래픽을 처리합니다.

보안위협 방지: 여러 보안 엔진은 위험한 접속을 탐지하기 위해 트래픽을 파싱합니다.
악성 웹사이트를 찾아내는 보안 웹게이트웨이, 악성 파일 다운로드를 막는 안티 맬웨어, 봇 활동을 시사하는 인바운드/ 아웃바운드 이상 연결을 끊는 IPS 등이 포함됩니다.

데이터손실 방지: SASE에서는 네트워크 플로우 중 민감한 데이터를 탐지할 수 있는 특정 데이터 손실 방지 규칙이 적용되며,, 이러한 데이터의 유실을 방지합니다. 이와 유사하게 클라우드 접속 서비스 브로커(CASB)를 통해 클라우드의 애플리케이션 접속을 세밀하게 관리할 수 있습니다.

위에 열거한 기능은 SASE의 수많은 기능 중 일부입니다. SASE 아키텍처는 새로운 기능이 추가되어도 '싱글패스 트래픽 처리 엔진' 을 신속히 확장할 수 있도록 설계되어 있어, 네트워크의 미래 변화에 적응하며 지속적으로 사용할 수 있다(future-proofing)는 것이 고유의 특장점입니다. SASE 클라우드를 확장해서 새로운 기능들을 어디든, 누구에게든 확대 적용할 수 있습니다. SASE 클라우드 서비스를 새로운 보안 위협 또는 공격 벡터에 적응시키는 작업은 중앙에서 실시하는데, 모든 고객사와 전체 에지에 즉시 적용됩니다. 이때 IT 부서에서 기능을 추가 설치하거나 활성화하는 수고를 하지 않아도 됩니다.

디지털 비즈니스를 돕는 진정한 IT 기반

SASE의 장점

SASE는 모든 에지를 네트워크 및 필요한 보안 기능에 연결하는 종합 플랫폼입니다.
이 다이내믹한 환경 속에서 현업을 지원하는 비용, 복잡성, 리스크가 모두 낮아집니다.

다음은 SASE 플랫폼의 주요 장점입니다.

민첩성: IT는 SASE 아키텍처를 통해 최적화된 네트워크 성능과 강력한 보안 기능을 모든 사업장, 응용프로그램, 사용자에게 전달할 수 있습니다. 새로운 자원과 기능의 제공은 신속하고 간단합니다. 딱 맞는 에지 클라이언트를 설치하고 SASE 플랫폼에 플러그인 하면 회사 정책 그대로 네트워크와 보안을 관리할 수 있습니다.

협업: IT팀은 네트워크와 보안의 융합을 통해 단일 인터페이스로 모든 기능과 정책을 관리합니다. 공통 용어를 쓰며 네트워크와 보안 이벤트를 깊숙이 들여다 볼 수 있습니다. 여러 팀의 협업을 통해 가용성, 성능, 보안 요건이 모두 충족되어야 하는 현업의 서비스를 효과적으로 개선합니다.

효율성: SASE를 사용하는 IT팀은 on-premise 인프라 관리의 부담에서 벗어날 수 있습니다. 물리적 토폴로지, 리던던시, 확장, 사이징, 업그레이드 업무가 확실하게 감소합니다. IT는 이제 더 나은 서비스를 현업에 제공하는 한편, 귀중한 자원과 스킬을 통상적인 인프라 관리에 소모하지 않고 실질적인 현업 관련 문제에 집중할 수 있습니다.

비용절감: 네트워크와 보안 스택이 단순화되고 여러 포인트 제품이 통합되면 벤더와 고객들은 인프라 운영에 드는 총비용의 절감을 경험할 수 있습니다.

진짜 SASE 인가요?

저마다 SASE라는 주장을 하면서 대단한 마케팅 전쟁이 일어날 것입니다. 가트너는 일부 기존 벤더들이 기존 제품을 SASE로 포장해서 SASE와 유사한 솔루션을 제공하려 할 것이라고 경고한 바 있습니다. 사실 해당 기술들이 애초에 클라우드용으로 설계되지 않았기 때문에 시장 내 서비스 품질과 공급에 리스크가 발생할 것입니다. 기대하는 결과를 낼 수 있는지 판단하기 위해서는 기반이 되는 SASE 아키텍처를 신중하게 살펴야 합니다.

통신사업자의 대척점에 선 SASE

지난 10년간 통신사업자들은 고객사의 복잡한 네트워크와 보안 스택을 관리해 줄 수 있다면서, 자신들이 구매하고 설치하고 관리하는 포인트 솔루션들을 제시해왔습니다. 하지만 복잡성은 사라지지 않았고, 고객사는 제품과 관리인력을 위한 지출을 늘릴 수밖에 없었습니다. 또한 고객은 통신사업자에 전적으로 의존하게 되었고, IT 조직은 기어가는 듯한 속도로 업무를 해야 했습니다. SASE는 완전히 다릅니다. 재래식 어플라이언스, 가시성이 제한적이거나 전혀 없는 파편적 관리는 사라집니다. SASE 클라우드는 확장성이 있고, 자가 서비스가 가능하며, 민첩합니다. 통신사업자는 그렇지 못합니다.

클라우드 내 가상머신은 여전히 어플라이언스 스택

가상머신을 AWS, 애저 등 IaaS에서 인스턴스화하는 것은 대단한 일이하지만 SASE에서는 아닙니다. On-premise 어플라이언스를 '클라우드' 로 옮기기는 하지만, 여전히 제각각 포인트 솔루션들이고 SASE가 가지는 온전한 클라우드 통합(cloud-native integration), 싱글패스 프로세싱, 글로벌 규모의 범위, 탄력성을 제공하지는 못합니다. 고객사는 벤더 수에 따라 여전히 여러 개의 관리 콘솔을 사용해야 합니다.

서비스 체이닝, 그럴듯 하지만…

멀티벤더 환경에서 서비스 체이닝은 SD-WAN, 라우터, 방화벽, WAN 옵티마이저 등 다수의 포인트 솔루션을 엮어주는 테크닉입니다. 실제 어플라이언스를 얼마나 많이 사용하는지 또는 여러 가상머신을 호스팅하는 uCPE(댁내장치)의 사용 여부와 상관 없이, 솔루션은 제각기 움직이기 때문에 각각 사이징, 확장, 관리가 필요합니다. 궁극적으로 SASE는 핵심 속성 중심의 융합을 제시합니다. 서비스 체이닝은 융합이 아니라 여러 포인트 솔루션의 헐거운 묶음이라고 할 수 있습니다.

불완전한 SASE: 기존 클라우드와 에지 밴더의 부족한 점

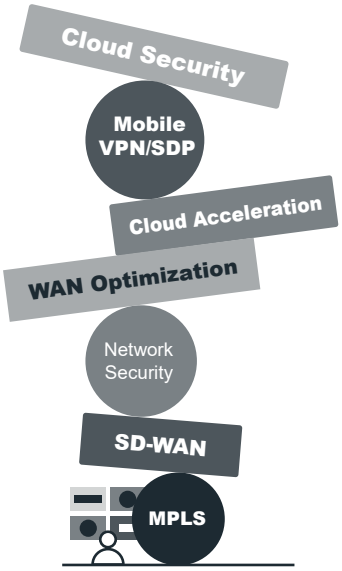
서비스형 보안 벤더는 SWGs (Secure Web Gateways) 와 CASBs (Cloud Access Security Brokers)를 가지고 다수의 보안 기능을 공급하기 위한 노력을 해왔습니다. 하지만 네트워크 플로우를 제어하면서 WAN 에지를 원천적으로 지원하는 핵심 SASE 요소가 아직 부족합니다. 모든 에지(사무실, 클라우드 데이터센터, 사용자, 장치)를 안정적으로 그리고 안전하게 SASE 클라우드에 연결할 수 있는 기술이 애초부터 통합되어 발전하지 않으면 SWGs와 CASBs는 또 다른 사일로가 되어버립니다. 이와 비슷하게 에지 어플라이언스 벤더들은 글로벌 분산형 클라우드 네이티브 서비스를 제공하는 CATO와 유사한 방식으로 클라우드 기능을 구축하는 프로젝트를 해야만 합니다.

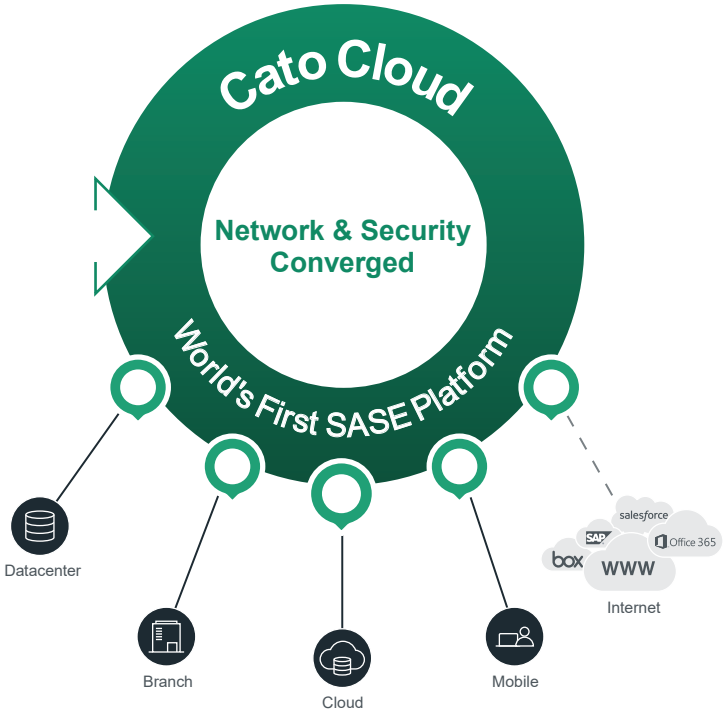
Cato Networks: 바로 배포 가능한 간단한 SASE 플랫폼

WAN 전환 또는 어플라이언스 리프레시를 통해 오늘 바로 SASE를 시작할 수 있습니다.
SASE 비용은 어떻게 지불할까요?

다행스럽게도 SASE 예산은 이미 책정된 범위 내에서 가능합니다. 귀사의 차기 보안 어플라이언스 리프레시, 다음 MPLS 계약 갱신, 또는 M&A 통합 프로젝트 등과 함께 SASE 프로젝트를 시작하시면 됩니다. 마이그레이션은 단번에 하지 않아도 되며, SASE 플랫폼은 점진적인 마이그레이션을 지원합니다. 마이그레이션이 진행되는 동안 SASE는 기존 네트워크 및 보안 솔루션이 종료될 시점까지 공존할 수 있습니다.

가트너는 **Gartner's Hype Cycle for Enterprise Networking 2019** 에서 최초로 SASE 카테고리를 정의했습니다만, 구현은 새로운 것이 아닙니다. Cato는 기업 네트워크와 보안 기능을 클라우드 서비스 방식으로 제공되는 싱글패스 소프트웨어 스택에 융합합니다.





Cato: 클라우드로 융합한 네트워킹과 보안

Cato 클라우드에 구현된 SASE 아키텍처의 주요 속성

신원 중심 주의: 위치가 어디든 Cato 클라우드로 들어오는 신원 또는 자원을 자동으로 파악합니다. 신원은 플로우와 함께 흐르고 사용되며, 다른 상황인지 요소들과 결합하여 다단계 인증을 개시하며, 각 응용프로그램 접속 정책을 구동하며, 네트워크 서비스 품질을 결정하고, 플로우의 데이터 리스크를 지속적으로 평가합니다.

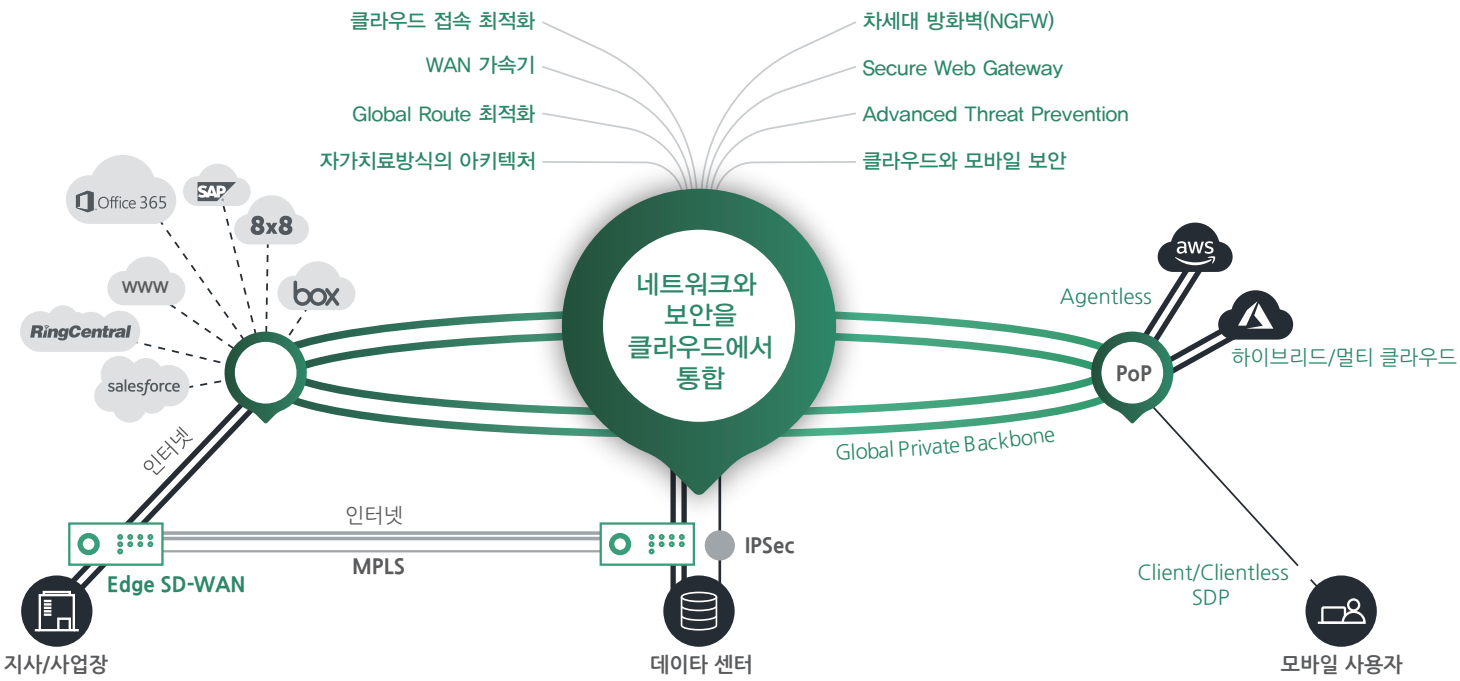
클라우드 네이티브 트래픽 처리: Cato 클라우드는 처음부터 클라우드 네이티브 서비스로 개발되었습니다. '싱글 패스 엔진' 을 이용해 모든 트래픽을 패킷 단위부터 처리하며, 최적화와 보안 기능을 적용합니다. 목적 중심 어플라이언스 또는 가상머신이 필요하지 않으며, 이로 인해 고객은 클라우드 공급자의 확장성, 자가 서비스 및 민첩성을 누릴 수 있습니다.

에지 지원: 물리적 장소, 모바일 사용자, 클라우드 데이터센터, 응용프로그램은 Cato 클라우드에 에지 솔루션으로 접속합니다. 물리적 장소는 에지 SD-WAN 장치(Cato Socket)을 사용하며, 모바일 장치는 VPN 클라이언트 애플리케이션 또는 웹 브라우저를 사용하고, IPsec 터널은 클라우드 자원을 Cato 클라우드에 연결합니다. 에지가 어떤 형태이며 어디에 위치하든 가장 가까운 Cato PoP에서 Cato의 네트워크와 보안 기능을 즉시 적용합니다.

글로벌 PoP 네트워크: Cato 클라우드는 47개 이상의 PoP을 통해 전체 서비스를 제공합니다. Cato의 PoPs은 티어 1 통신사업자들과 연결되어 있고, WAN과 클라우드 트래픽을 최적화하는 글로벌 프라이빗 백본 네트워크를 구성합니다. PoP 소프트웨어를 통해 세밀한 패킷 검사를 적용함으로써 Cato 클라우드를 통과하는 트래픽을 다수의 보안 위협으로부터 보호합니다.

Cato 클라우드

Cato 클라우드는 고객사의 네트워크를 연결하고 안전하게 보호하며 관리하는 융합 플랫폼입니다. 순차적으로 지점/지사, 클라우드 자원, 사용자에게 적용하면서 기존 네트워크 서비스와 보안 포인트 솔루션들을 대체해 가면 됩니다.



Cato 클라우드 사용 후기

많은 기업들이 Cato 클라우드라는 혁신적 방식의 혜택을 누리고 있습니다. Cato 클라우드로 MPLS를 강화하거나, 교체하거나, 지점 어플라이언스를 폐기하는 등 다양하게 활용하고 있습니다. 구현하는 방식은 다양하지만 고객들이 동의하는 한 가지가 있습니다. Cato 클라우드는 네트워크 민첩성을 증대시키고 비용을 기업이 경쟁력을 유지하기 위해서는 반드시 디지털 시대로 도약해야 하며, 이 과정에서 IT 인프라가 뒤쳐져서는 안됩니다. Cato는 고객의 디지털 사업의 새로운 기반이 될 안전한 글로벌 네트워크를 제공합니다.

UNIVERSAL

"Transitioning to Cato was so easy. I joke that it was like pressing the Staples' Easy Button."

Leslie W. Cothren,
IT Director

HUMPHREYS & PARTNERS ARCHITECTS, L.P.

"Cato gave us freedom, now we can use a socket, a VPN tunnel, or the mobile client, depending on location and user requirements."

Paul Burns,
IT Director

FISHER & COMPANY

"The loss and latency of the Cato Cloud is comparable to our MPLS service."

Kevin McDaid,
Systems Manager

Cato Networks 는
클라우드 태생의 서비스사업자

사업 환경이 빠르게 디지털로 변화하고 있는 지금, 성공의 필수 요건은 온프레미스 또는 클라우드상의 응용프로그램과 데이터에 최적화된 접속이 가능한가 그리고 급증하는 모바일 사용자를 어떻게 지원하는가 하는 점입니다. 지금까지의 네트워크는 디지털 환경의 변화 속도를 따라가지 못합니다. 포인트 솔루션을 짜깁기하는 방식은 힘들고 자원도 많이 소모합니다. 통신사업자의 서비스는 비용이 많이 들고 융통성도 떨어집니다. 이제 더 나은 방법을 찾아야 합니다.

Cato는 글로벌 환경의 클라우드 네이티브 서비스사업자입니다. 데이터센터, 지점/지사, 모바일 사용자, 클라우드 자원 등을 글로벌 환경의 안전한 최적화 관리형 SD-WAN 서비스 형태로 제공합니다. WAN과 인터넷 트래픽은 종합 보안 서비스 스위트를 통해서 보호하며 전담 보안 전문가가 업데이트와 관리 서비스를 제공합니다. 기업은 MPLS와 네트워킹 및 보안용 포인트 솔루션을 Cato 클라우드로 교체함으로써 네트워크의 민첩성과 효율성이 크게 개선되어, 현재는 물론이고 내일의 사업 환경이 요구하는 조건까지 충족할 수 있습니다.

Cato.
Network at the Speed of Now.

Cato Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Mobile Access Optimization

Managed Services

- Managed Threat Detection and Response (MDR)
- Intelligent Last-Mile Management
- Hands-Free Management

CATO
NETWORKS