CATO NETWORKS

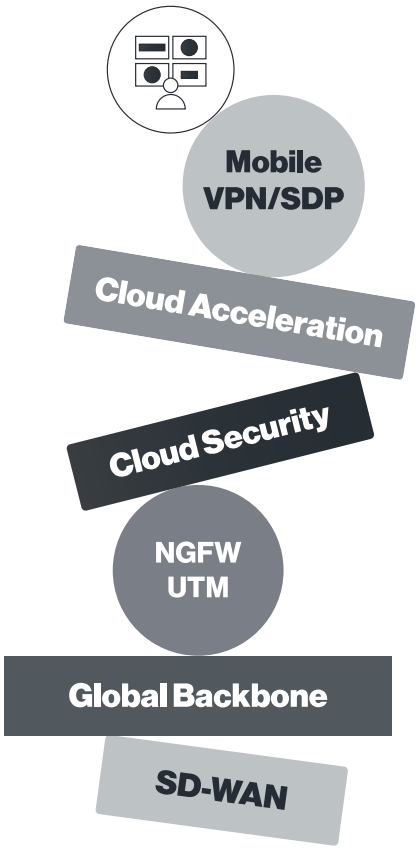
Cato 클라우드

세계 최초
SASE 플랫폼

—

솔루션 요약

디지털 환경 전환의 네트워크 및 보안 과제



사업환경이 빠르게 디지털로 변화하고 있습니다. 온프레미스 또는 클라우드상의 응용 프로그램과 데이터에 최적화된 접속이 가능해야 하고, 급증하는 모바일 사용자 지원 역량에 사업성패가 달려있습니다. MPLS와 보안 장비들로 구성된 기존 네트워크는 새로운 비즈니스, 기술적 요구사항 그리고 진화하는 보안위협 환경에 제대로 대응하지 못합니다.

그 결과 여러 곳에서 발생하는 문제점을 포인트 솔루션을 늘려가는 방식으로 처리할 수밖에 없었습니다. 고객은 이와 같이 복잡한 네트워크를 운영하기 어렵고 자원도 많이 요구됩니다. 이 복잡한 환경을 통신사에 맡긴다 하더라도 비용이 많이들 뿐만 아니라 디지털 업무에 필요한 속도와 민첩성을 제공할 수 없습니다. 변화하는 디지털 환경에 걸 맞는 더 나은 방식을 찾아야 합니다.

디지털 사업의 핵심은 클라우드 우선의, 신속하고 민첩한 환경이기에 기존의 통신사와 네트워크 서비스 공급자가 제공하기는 어렵습니다.

디지털 전환이 기존 네트워크 아키텍처에 부담이 되는 이유:

- MPLS는 클라우드 접속이 안되는 WAN 접속을 목적으로 구축되어 있으며, 비용이 많이 들고 융통성도 떨어집니다.
- 지점/지사의 보안 인터넷 접속은 MPLS를 통한 데이터센터로 연결된 백홀을 통해 통신되며, 지점/지사는 인터넷 보안 위협으로부터 사용자를 보호하기 위한 더 엄격한 네트워크 보안이 필요합니다.
- 기존 WAN은 설치된 물리적 장소를 벗어나면 클라우드와 모빌리티 요건을 지원하지 못합니다. 증가하는 여러 네트워크 요건과 보안위협을 처리하고 해결하기 위해 더 많은 솔루션이 필요합니다.
- 이러한 모든 장비를 관리하는 것은 어렵습니다. 각 구성요소의 콘솔 및 솔루션 유지보수 주기가 다르기 때문입니다 (크기, 구매, 설치, 설정, 확장, 업그레이드, 패치, 폐기).

기존 통신사가 파트너로 역부족인 이유:

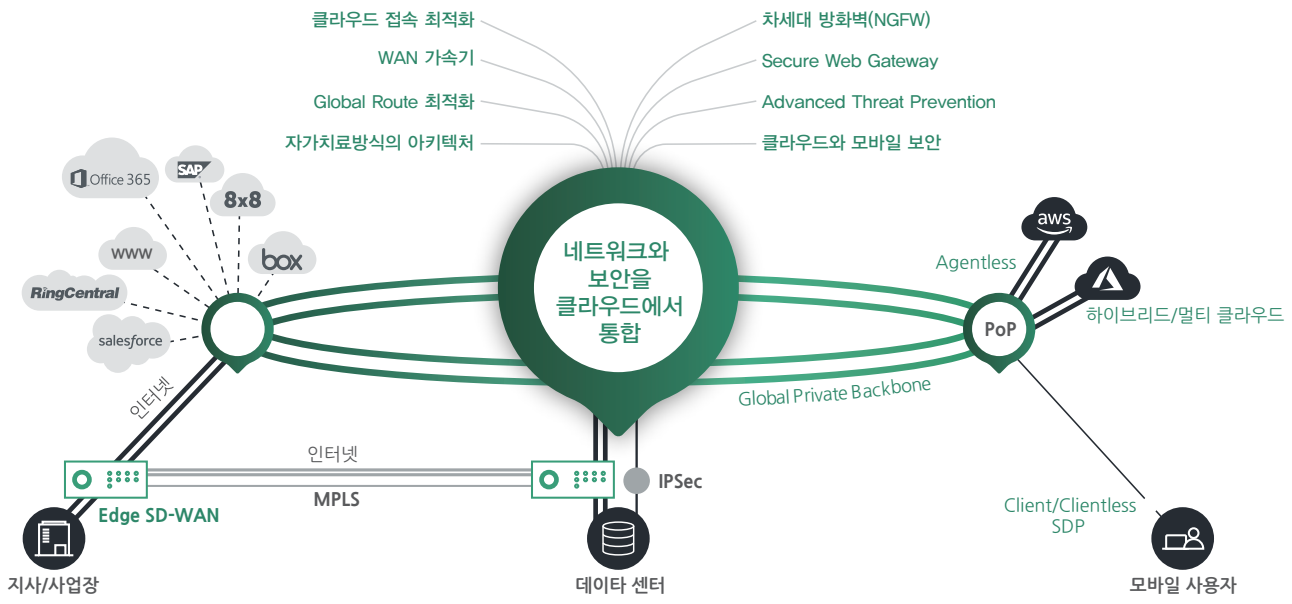
- 고가의 전용 인프라, 외부 포인트 솔루션들, 복잡한 관리 활동이 필요합니다.
- 유연성이 없으며 현장 설치까지 시간이 많이 걸립니다.
- 연계된 보안 및 네트워크 서비스의 기술지원은 타사 지원에 의존해야 하며 전문성도 떨어집니다.
- 정체된 기본 기술과 제품 로드맵을 가지고 있지 못하기 때문에 통신사는 변경 실행을 거의 할 수 없습니다.
- 가시성이 떨어지기 때문에 고객에게 가시성과 네트워크 제어 역량을 제공하는 데 한계가 있습니다.

세계 최초 SASE 플랫폼

SD-WAN과 네트워크 보안을 글로벌 클라우드 서비스로 융합한 세계 최초 SASE 플랫폼입니다.

Cato는 가트너에서 제시한 SASE(Secure Access Service Edge) 프레임워크를 최초로 구현한 회사이며, 글로벌 백본 인프라 및 클라우드 네이티브 아키텍처를 통해 모든 사용자와 애플리케이션에 안전하고 최적화된 액세스를 제공합니다. Cato를 통해 기업은 포인트 솔루션 및 고가의 MPLS 서비스로 구축된 오래된 네트워크에서 글로벌하고, 안전하고, 민첩하고, 경제적인 최신 네트워크로 교체할 수 있습니다.

Cato Cloud는 지점/지사에 위치한 모바일 사용자, 물리적, 클라우드 데이터 센터와 같은 모든 기업의 네트워크 리소스를 글로벌하고 안전한 관리형 SD-WAN 서비스에 연결합니다. Cato는 WAN과 인터넷 트래픽을 클라우드로 통합하고, 이 모든 트래픽을 항상 보호할 수 있도록 일체의 보안 서비스를 적용합니다.



글로벌 프라이빗 백본네트워크

Cato의 글로벌 프라이빗 백본망은 전세계 50개 이상의 PoP로 구성되어 있으며, 이 PoP은 SLA지원 받는 Tier-1 서비스 공급자 다수를 통해 상호 연결되어 있습니다. 모든 PoP은 Cato의 클라우드 소프트웨어 스택을 가지고, 완벽한 멀티테넌트(multitenant), 확장성, 유비쿼터스 방식으로 Global Route 최적화, 동적 경로선정(Dynamic Path Selection), 트래픽 최적화, 엔드 투 엔드 암호화 등 모든 네트워크 기능을 수행하며, Cato 보안 서비스에 필요한 검사 및 시행 기능도 실행합니다.

WAN 최적화

WAN 최적화는 네트워크 소프트웨어 스택의 필수적인 부분으로, 파일 전송과 같은 주요 작업에서 처리량을 극대화하기 위해 TCP 프록시 및 고급 혼잡 관리(advanced congestion management algorithms) 알고리즘을 활용합니다.

글로벌 경로 최적화

Cato의 라우팅 알고리즘은 지연(latency), 패킷손실, 지터(jitter) 등을 고려합니다. 인터넷 라우팅과 달리 Cato 라우팅은 항상 모든 네트워크 패킷에 대해 최적의 경로를 선택하여 제공합니다.

암호화

가장 강력한 업계표준 암호화 기술을 사용하는 엔드 투 엔드 암호화 방식은 데이터 기밀성, 개인정보, 멀티테넌시를 철저히 보호합니다.

자가치료방식 아키텍처

Cato는 백본 네트워크를 지속적으로 모니터링하고 측정합니다. 자가치료기능이 있기 때문에 99.999% 서비스 가용성을 보장합니다. 탄력적인 스케일업 클라우드 소프트웨어 설계 원칙을 통해 서비스 다운 타임이나 중단 없이 원활한 서비스 인프라 성장을 보장합니다.

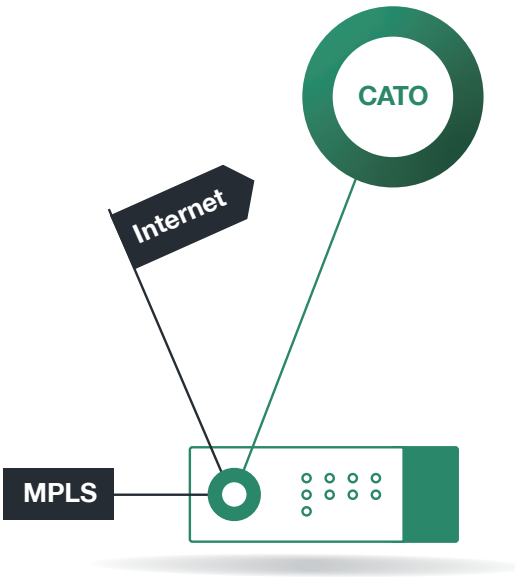
각 지역은 Cato의 제로 터치 에지 SD-WAN 어플라이언스인 Cato 소켓 또는 IPsec 터널을 지원하는 장치에서 암호화된 터널을 설정하여 Cato 글로벌 프라이빗 백본에 연결합니다. 클라우드 데이터센터는 에이전트 사용 또는 에이전트를 사용하지 않는 설정을 통해 연결됩니다.

모바일 사용자는 Cato Client를 통해 내부 애플리케이션에 접근할 수 있고 또한 SDP를 통해 사용자 식별 후 인가 받은 애플리케이션에 접속이 가능합니다.

에지 SD-WAN

Cato 에지 SD-WAN은 다양한 인터넷 회선을 거쳐 Cato의 글로벌 프라이빗 백본 네트워크에 안정적으로 접속하여 고성능 엑세스를 제공합니다. MPLS를 통한 트래픽은(Cato PoP를 통하지 않고) 사업장간 직접 라우팅 되어 연결되고, 뿐만 아니라 IPsec 터널을 통해 외부 장치와도 연결됩니다.

Cato의 에지 SD-WAN 장치인 Cato Socket은 제로 터치 방식으로 전원과 인터넷만 연결되면 수분 만에 활성화됩니다. Socket은 X1500은 지점/지사용, X1700은 데이터센터용으로 두 가지 모델이 있습니다. Cato의 NOC (network operations center)에서 두 제품 모두 지속 모니터링되고 업데이트 합니다.



Cato Sockets 기능

- **링크 애그리게이션(Link Aggregation)** 기능은 MPLS와 여러 인터넷 회선(광, DSL, 케이블, 4G/LTE, 5G 등)을 통과하는 인바운드/아웃바운드 트래픽 균형을 조절하면서 대역폭 용량(Active/active)과 가용성을 극대화합니다.

- **동적 경로 선정**으로 응용프로그램, 사용자, 실시간 연결 품질(지터, 지연, 패킷손실)을 감안하여 최적의 이동경로를 찾아 트래픽을 라우팅합니다.

- **응용프로그램 인식** 기능은 Cato의 고급 DPI (Deep Packet Inspection) 엔진을 사용하여 첫 번째 패킷에서 수천 개의 애플리케이션과 수백만 개의 도메인을 자동으로 식별합니다.

- **대역폭 관리 규칙**은 더 중요한 애플리케이션이 항상 필요한 업 스트림 및 다운 스트림 용량을 제공받도록 보장하며, 다른 애플리케이션은 상황에 맞는 최선의 용량을 활용하도록 되어 있습니다.

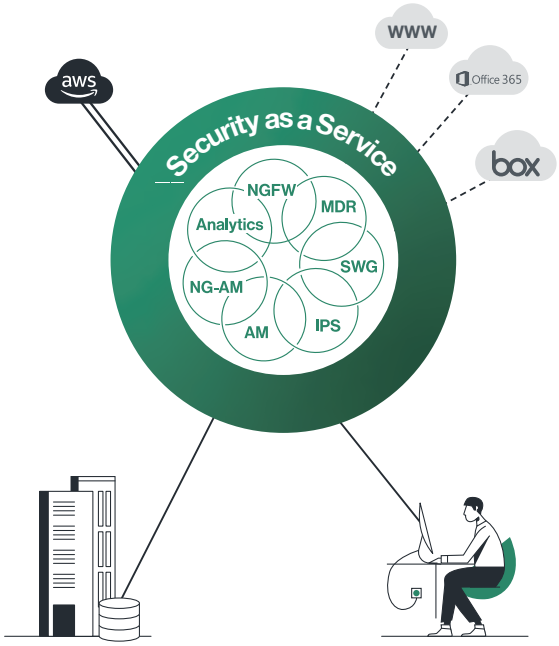
- **패킷 손실 완화 기술**은 트래픽을 동적으로 더 좋은 경로로 전환하며 응용프로그램 별로 패킷을 사전에 복제합니다. Cato의 아키텍처는 middle-mile 패킷 손실을 제거합니다.

- **라우팅 프로토콜 통합**을 위해 BGP 정보를 활용한 실시간 라우팅 결정을 내리던 인프라를 Cato Edge SD-WAN과 쉽게 쉽게 통합합니다.

- **고가용성(HA)**은 추가비용이 부가되지 않으며 설치는 수 분 안에 완료될 만큼 간단합니다. Sockets은 자동으로 최적의 Cato PoP에 연결되나 접속 품질이 나빠지거나 장애가 발생하게 되면, 다른 최적의 PoP를 찾아 자동 연결합니다.

서비스형 보안(Security as a Service)

Cato보안엔진이 Cato 글로벌 프라이빗 백본 네트워크에 구축되어 있어 서비스형 보안을 제공합니다. 따로 구매 또는 설치해야 하는 어플라이언스가 필요하지 않습니다. 보안 엔진은 응용프로그램을 인지하는 차세대 방화벽 (NGFW), URL 필터링이 되는 보안 웹게이트웨이 (SWG), 표준 및 차세대 안티-멀웨어와 Cato SOC (Security Operation Center)에서 관리하는 IPS 등을 포함합니다.



이 보안엔진들은 Cato의 관리 서비스에 포함하여 제공되는 종합 MDR (위협감지 및 대응 관리) 서비스의 기반입니다. 모든 엔진은 완벽한 확장성을 가지고 있어, 어플라이언스와 포인트 솔루션을 확장, 패치, 업그레이드하는 번거로움 없이 암호화 또는 암호화되지 않은 모든 고객 트래픽 확장을 지원합니다. Cato는 사용자 개인정보를 보호하며 GDPR을 준수합니다. Cato 서버는 검사 데이터를 저장하지 않으며 외부와 공유하지 않습니다. 고객은 금융정보와 건강정보와 같은 개인정보와 관련된 응용프로그램을 검사에서 제외할 수 있습니다. 또한 Cato는 SOC2와 ISO27001을 준수합니다.

차세대 방화벽

모든 Cato PoP에 차세대 방화벽(NGFW)이 작동합니다. 조직 전체를 대상으로 응용프로그램 인식 및 사용자 인식 보안 정책을 단일하게 통합적용하여 보호합니다. 추가 비용이 들지 않으며 개별 방화벽 어플라이언스를 업그레이드하거나 유지 보수하는 등의 복잡한 과정도 필요하지 않습니다. Cato의 차세대방화벽만의 기능은 다음과 같습니다.

- **완벽한 가시성** 모바일 사용자와 비 모바일 사용자가 사용하는 WAN 트래픽과 인터넷 트래픽 일체를 검사할 수 있습니다. 사각지대가 없어 다수의 보안 어플라이언스나 툴을 설치할 필요가 없습니다.

- **무한 확장성** 보안정책을 적용 및 어떠한 트래픽이 혼재되어도 (암호화 또는 비암호화) 회선 속도로 검사할 수 있습니다. 처리속도와 네트워크 성능은 계약한 서비스 수준을 보장합니다.

- **통합 보안 정책** 단일 사용자에서 회사 전체로 확장가능한 하나의 세분화된 정책과 규칙기반을 적용합니다. 규칙기반은 모든 보안 기능과 트래픽 유형에 공통 적용되며, 특정 어플라이언스 또는 포인트 제품과 이들 정책을 연동할 필요도 없습니다.

- **단순한 사용주기관리** 방화벽을 사이징, 업그레이드, 패치, 교체 할 필요가 없습니다. 고객은 새로운 위협과 변화하는 비즈니스 요구에 대비하여 네트워크 보안을 최신 상태로 유지하는 지속적인 작업이 필요하지 않으며, 통신사에게 이러한 업무를 맡기느라 비용을 더 들일 필요도 없습니다.

보안 웹 게이트웨이(Secure Web Gateway)

보안 웹 게이트웨이(SWGs)는 피싱, 멀웨어 및 기타 인터넷에서 들어오는 위협으로 부터 고객을 보호합니다. Cato는 보안 웹 게이트웨이와 차세대 방화벽을 통합하여 다수의 포인트 솔루션과 어플라이언스 사용주기마다 정책을 적용할 필요가 없습니다. Cato의 통합 SWG는 피싱 위협, 악성 프로그램 전달, 봇넷 및 기타 악성 콘텐츠에 대한 많은 정보와, 항상 최신 URL 데이터베이스가 포함된 동적 사이트 분류 기능을 제공합니다. 고객은 사용자 활동 가시성을 기반으로 모바일 및 비모바일 사용자의 웹 접속 정책을 한 세트로 정하고 실행함으로써 조직 리스크를 낮출 수 있습니다.

지능형 위협 예방(Advanced Threat Prevention)

지능형 위협 예방은 현재 존재하는 위협과 새로 등장한 위협요인을 처리할 수 있도록 배포된 네트워크 보안 및 관련된 방어수단의 모음입니다. IT조직은 네트워크로 침투하는 지능형 위협 인자를 파악하고 차단하는 등 복잡한 조직의 인프라를 유지해야 하는 어려운 과제에 직면해 있습니다. Cato의 지능형 위협 예방기능은 회선 속도로 암호화되거나 암호화되지 않은 트래픽에 대해 악성 프로그램 및 네트워크 기반 위협을 검사하여 이러한 문제를 해결합니다.

TLS 검사

대부분의 인터넷 트래픽은 암호화되어 있기 때문에 SSL/TLS 트래픽 내에서 전달되는 위협을 탐지하고 차단하는 일은 매우 중요합니다. 하지만 인라인 SSL/TLS 트래픽 검사는 상당한 자원을 소모합니다. 어플라이언스 기반의 보안 솔루션의 문제는 하드웨어 성능 이슈로 리소스 한계에 부딪히는 경우가 잦고, 그 결과 예산 주기를 벗어난 하드웨어 업그레이드를 강행하는 경우가 많습니다. Cato 보안 서비스는 무한한 컴퓨팅 성능의 클라우드를 활용합니다. Cato는 TLS 암호 트래픽 흐름 전부를 검사하되 사용자 또는 응용 프로그램 성능에는 전혀 영향을 주지 않습니다.

멀웨어로부터 보호

Cato의 네트워크 기반 멀웨어 보호기능은 Cato PoP 전체에 설치 운영되는 다수의 멀티레이어 구조로 완벽히 통합된 멀웨어 방지 엔진을 통해 이루어집니다. 첫 번째 계층에서는 글로벌 위협 인텔리전스 데이터베이스를 기반으로 항상 최신 상태로 유지되는 시그니처 (signature) 및 휴리스틱 기반(heuristics-based) 검사 엔진이 포함되어 있으며 Cato 백본에서 전송중인 파일을 검색하여 알려진 멀웨어로부터 보호합니다. 두 번째 계층에서는 SentinalOne의 머신 러닝 알고리즘을 적용하여 제로데이 공격 이나 시그니처 (signature) 기반의 검사 엔진을 회피하도록 설계된 이미 알려진 위협의 변종과 알려지지 않은 멀웨어를 파악하고 차단합니다.

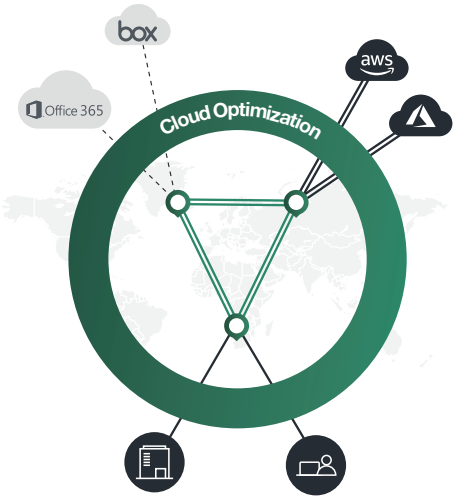
침입방지

Cato의 IPS는 여러 계층과 기술을 통해 네트워크 공격을 차단합니다. **네트워크 프로토콜 검증**으로 프로토콜 조작 및 비정상 패킷을 탐지합니다. **컨텍스트 이해 시그니처 (Context-aware signatures)** 및 규칙은 알려진 취약점(CVE)에 기반한 공격, 네트워크 트래픽 동작에 기반한 알 수 없는 공격 및 네트워크 스캔을 차단합니다. **내외부 평판자료(reputation feeds)**는 IPS인텔리전스에 질을 높입니다. **지리적 기반 제한 (Geographic-based Restrictions)**으로 위협 환경을 최소화합니다.

기존 IPS 기술을 활용하려면 상당한 스킬과 관리가 필요합니다. IT 팀은 새로운 시그니처 (signatures)을 평가하고, 활성화 할 시그니처 (signatures)을 판단해야 하며, 업무 혼란을 야기하지 않도록 검증하고, IPS 어플라이언스와 네트워크에 미칠 성능영향을 고려해야 합니다. Cato IPS에는 이런 우려가 없습니다. 다른 Cato 보안 서비스와 마찬가지로 Cato 보안 리서치랩과 SOC는 고객을 대신하여 Cato IPS를 관리하며, 적절한 검증과 용량 분석을 통해 새로운 보안위협 방지에 적절한 규칙을 적용합니다. 활성화도 간단합니다. Cato 고객은 관리 콘솔에서 IPS 만 활성화하여 예방 기능을 활용할 수 있습니다.

클라우드 & 모바일 접속 최적화

클라우드 데이터센터 통합

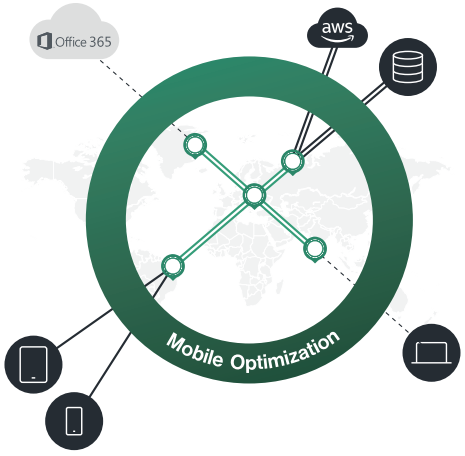


Cato는 클라우드 데이터센터를 SD-WAN으로 쉽게 연결합니다. Amazon AWS, Microsoft Azure, Google Cloud 등 모든 클라우드 제공자는 일반적으로 Cato PoP과 공유되는 물리적 데이터 센터만 통과하면 되는 이중화된 IPsec 터널을 통해 Cato 글로벌 백본에 연결되어 있습니다. 이러한 방식으로 Cato는 최적의 클라우드 환경을 제공합니다. 클라우드 데이터센터 트래픽은 Cato 글로벌 프라이빗 백본 네트워크를 거쳐 Cata PoP로 들어가는 최적의 경로로 라우팅 됩니다. Cato PoP에서 트래픽은 보통 데이터센터 네트워크를 거쳐 클라우드 데이터센터로 보내집니다. 이러한 아키텍처는 AWS DirectConnect 또는 Microsoft Azure Express Route와 같은 프리미엄 클라우드 연결 서비스가 필요하지 않습니다.

에이전트를 사용하지 않는 (Agentless) 통합 방식이므로 **가상 어플라이언스는 필요하지 않습니다.** 가상 어플라이언스를 선호하는 경우 Cato에서 vSocket을 제공할 수 있습니다. 에이전트없는 구성은 모든 클라우드 공급자가 제공하는 IPsec 게이트웨이 연결을 활용하여 추가적인 VM 비용이 들지 않으며 서버 네트워크 설정을 변경하는 위험 부담도 할 필요 없습니다. 다른 모든 트래픽과 마찬가지로 클라우드 데이터센터 트래픽은 Cato 보안 서비스가 제공하는 모든 보안 검사를 거칩니다.

클라우드 애플리케이션 가속화

Cato는 Office 365, Cloud ERP, UCaaS, Cloud Storage 같은 퍼블릭 클라우드 애플리케이션 성능을 향상시킵니다. 클라우드 애플리케이션 트래픽을 Cato의 글로벌 프라이빗 백본 네트워크를 통과시켜 클라우드 애플리케이션 공급자의 데이터센터가 가장 가까운 Cate PoP로 최적화된 라우팅을 제공함으로써 지연 시간을 줄입니다. Cato에 내장된 WAN 최적화 기능으로 엔드 투 엔드 처리량을 극대화하여 특히 파일 전송 같이 대역폭을 많이 요구하는 작업을 중심으로 응용 프로그램 성능을 개선합니다. 클라우드 애플리케이션과 주고받는 모든 트래픽과 파일은 Cato 클라우드 내에서 모든 보안검사를 거칩니다.



보안 원격접속

Cato는 모든 네트워크 및 보안 기능을 원격 및 모바일 사용자까지 확장합니다. Cato Client를 사용하거나 Cato Client 없이 브라우저를 통해 가장 가까운 Cato PoP으로 접속하면 트래픽은 Cato 글로벌 프라이빗 백본 네트워크를 통해 최적 경로로 라우팅되어 on-premise 또는 클라우드 상의 응용프로그램까지 도달합니다.
Cato의 제로-트러스트 SDP (Software Defined Perimeter) 접속모델로 사용자 접속 제어를 특정 응용프로그램까지 매우 미세하게 제어를 할 수 있습니다. 반면, 기존 VPN 솔루션은 전체 서브넷 접속을 제한합니다. 모든 사용자 활동은 Cato에 내장된 네트워크 보안 스택으로 보호받으며, 모든 사용자는 어디에 있든 엔터프라이즈급 보호를 받습니다.

Cato 관리 애플리케이션

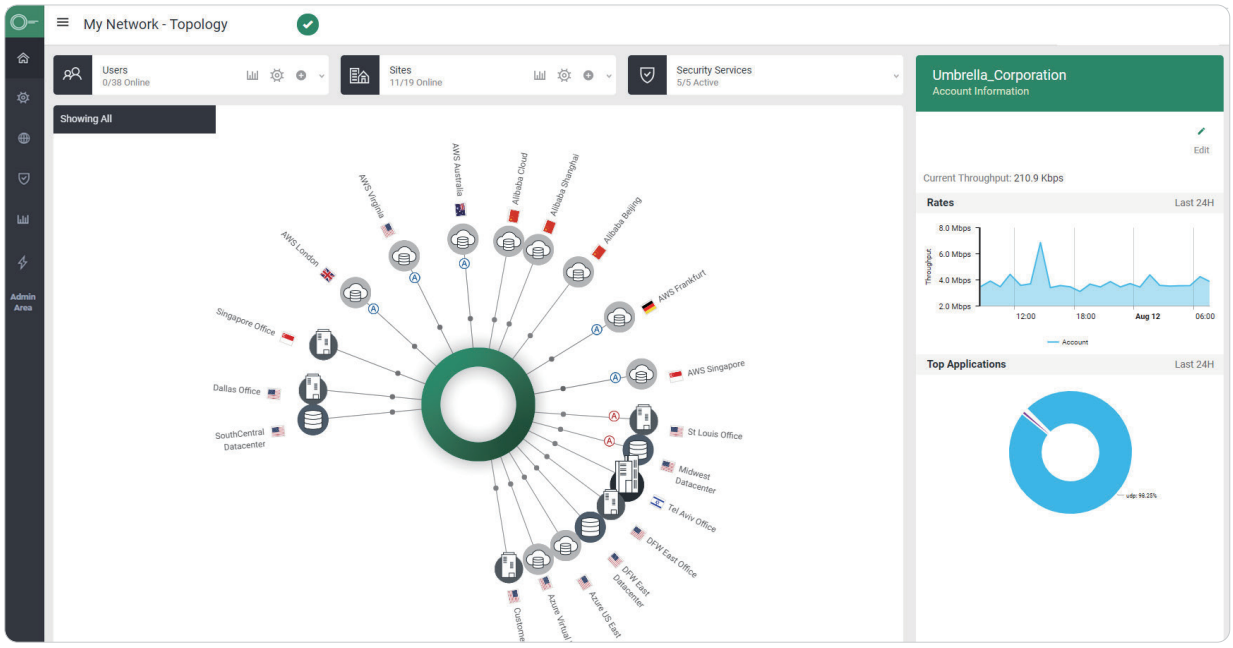
Cato는 클라우드 기반의 관리 애플리케이션을 통해 고객은 회사 네트워크 (사이트, 클라우드 리소스, 네트워킹 및 보안을 위한 모바일 사용자) 전체를 단일 통합 관리 콘솔(single-pane-of-glass)로 볼 수 있습니다. 고객과 서비스 공급자는 이 응용 프로그램을 통해 네트워크 및 보안 정책 구성, 상세한 네트워크 분석 및 보안 이벤트 리포팅 등 전체 서비스를 제어할 수 있습니다.

- **Cato 관리 콘솔은 강력하고 간단하게 구성되어 있습니다.** 관리자는 오랜 학습이나 반복적인 수동 작업없이 인텐트-드리븐(intent-driven) 유저 인터페이스로 세분화된 네트워크 및 보안 정책을 정의합니다.

- **시간 분석과 과거 기록 분석 및 보고 기능**을 통해 포괄적인 네트워크 가시성을 제공하므로 접속 제어, 사용자 경험, 문제해결, 쉐도우 IT 등 주요한 문제해결이 가능해집니다.

- SIEM과 같은 **외부 분석 솔루션에 전체 네트워크 및 보안 이벤트 로그를 수집 및 제공**할 수 있기 때문에 다수의 어플라이언스와 자원에서 가져온 데이터를 일일이 모으는 수고를 하지 않고도, 모든 이벤트를 볼 수 있는 단일 인터페이스의 우수한 장점을 누릴 수 있습니다.

관리 애플리케이션은 웹 기반이며 인터넷을 통해 멀티 인증을 거쳐 접속합니다.
접속과 설정 변경사항은 모두 중앙(audit log)에 기록됩니다.



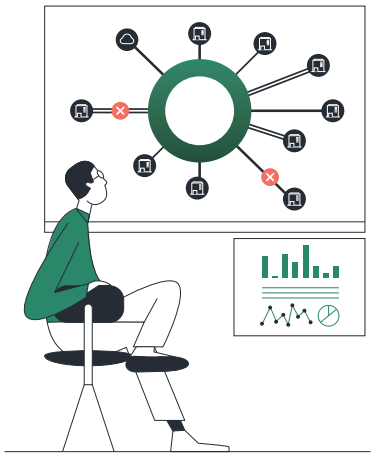
Cato의 관리 콘솔은 단일 창 방식으로 연결된 모든 사업장, 클라우드 자원, 사용자 현황을 보여줍니다.

관리 서비스

Cato는 고객 요구 사항에 가장 잘 맞는 관리 모델에 따라 관리 서비스 제품군을 제공합니다. Cato에서 기본 플랫폼을 유지 관리하기 때문에 고객은 자체 유지보수 비용의 부담과 네트워크 및 보안 인프라자원의 확장, 업그레이드하는 관련 비용과 복잡성에서 벗어날 수 있습니다.

셀프 서비스 관리를 통해 고객은 자신의 네트워크의 모든 측면을 관리합니다. 공동 관리를 통해서 고객은 설정과 단순 문제해결 업무를 Cato NOC 또는 지역 파트너에게 위임할 수 있습니다. 전체관리 방식으로는 고객사의 네트워크 모니터링과 관리의 책임을 지역 파트너에게 넘길 수 있습니다.

네트워크 변경 시 티켓 오픈방식으로 처리하는 전통적인 통신회사와 관리형 네트워크 서비스 공급자는 제공할 수 없는 Cato만의 장점은 여러 형태의 관리 서비스가 가능하다는데 있습니다. Cato와 Cato의 파트너사는 현장 설치 지원뿐만 아니라 다음과 같은 여러 관리 서비스를 제공합니다.



인텔리전트 라스트-마일 관리

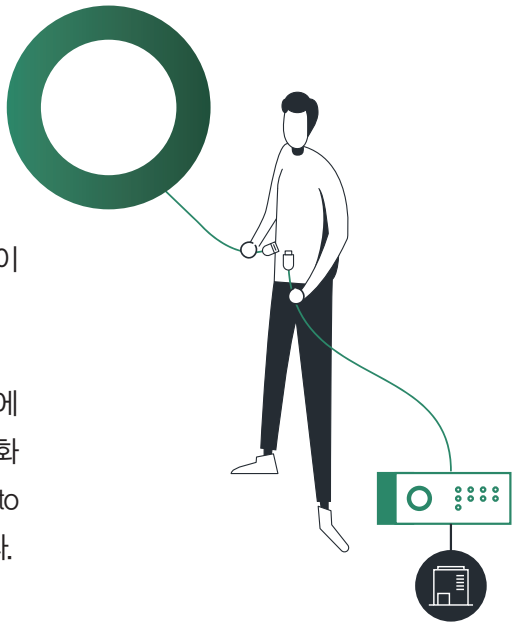
Cato는 라스트 마일 ISP를 지속적으로 모니터하는 프리미엄 서비스를 제공합니다. 장애 (blackout) 또는 성능저하 (brownout) 상황이 발생하면 Cato는 해당 ISP와 협력하여 사고와 관련하여 적절한 상세 네트워크 정보를 제공하여 문제를 해결합니다. MPLS 네트워크에서 전환한 고객인 경우, 내부 IT 자원을 사용하지 않고도 신속하게 글로벌 ISP들의 네트워크 문제를 해결할 수 있는 방법이 됩니다.

위협 탐지 및 대응 관리

Cato는 프리미엄 서비스를 통해 지속적으로 고객의 네트워크를 모니터링하면서 문제가 되는 엔드포인트를 찾아냅니다. 예방만으로 기업 네트워크를 충분히 보호할 수는 없습니다. 지능적 공격에 대한 완벽한 방어를 위해서는 탐지가 중요합니다. 그러나 이러한 위협 탐지 및 대응 관리 (MDR) 서비스는 비용이 많이 들고 구매 설치가 필요한 복합한 작업입니다. Cato MDR은 Cato 네트워크를 심층적으로 볼 수 있는 네트워크 가시성을 활용하여, 네트워크 트래픽을 마이닝하고, 탐지된 이상 징후에 대한 사람의 인증을 마이닝하는 머신러닝 알고리즘 조합을 사용하여 상주하는 보안위협을 zero-footprint 방식으로 탐지해낼 수 있습니다.

손 쉬운 관리

고객은 Cato 또는 Cato의 파트너를 선정하여 고객사 네트워크를 손쉽게 관리할 수 있습니다. 변경요청이 제출되면 티켓팅 포털을 거쳐 Cato의 서비스 SLA에 따라 처리됩니다. 전문 인력이 비즈니스 및 기술 요구 사항을 수용하기 위해 필요한 경우 네트워킹 및 보안 정책에 대한 변경을 수행하게 됩니다.



현장 설치 / 구성

Cato의 현장 설치/구성 서비스를 활용하면 Cato의 전문 서비스팀(PS)이 초기 현장 설치와 설정을 수행합니다.

초기 설치 이후 PS팀은 네트워크와 보안 정책을 고객의 요구사항에 맞추어 세밀하게 조정합니다. 추가 교육을 통해 현지 자원이 현장 활성화 작업을 마무리 할 수 있도록 필요한 것들을 제공하고 지원합니다. Cato의 PS와 지원팀은 설치/구현이 진행되는 동안 지원을 받을 수 있습니다.

전담 지원 엔지니어 (DSE)

전담 지원을 원하는 고객을 위해 지원 문제에 대한 단일 연락처를 제공하는 DSE 서비스를 제공합니다. DSE는 고객 환경에 대한 이해가 깊은 티어-3 지원 엔지니어가 지명됩니다.

이를 통해 고객 특정 정보를 전달할 필요가 없어지며 이슈를 신속하게 해결할 수 있습니다.

Use Cases

MPLS의 SD-WAN 전환

Cato는 고객이 비용이 많이 들고 융통성이 떨어지며 용량이 제한된 MPLS 네트워크를 여러 고용량 인터넷 링크로 대체하고 Cato의 라스트 마일 및 미들 마일 최적화를 활용할 수 있도록 합니다. 고객은 Cato의 에지 SD-WAN을 통해 메가 비트 당 더 저렴한 비용으로 가용 용량과 신축성을 개선시킵니다. 글로벌 규모의 사업을 영위하는 고객은 Cato의 경제적인 글로벌 프라이빗 백본 네트워크로 글로벌 MPLS와 예측성이 떨어지는 인터넷을 대체하여 성능을 최적화하면서 on-premise 와 클라우드 상의 자원 처리량을 극대화합니다.

최적화된 글로벌 연결

Cato는 WAN 및 클라우드 최적화가 내장된 글로벌 프라이빗 백본을 사용하여 어디에서나 SLA 보장되고 예측 가능한 고성능 네트워크 환경을 제공합니다. 글로벌한 활동 중 심각한 지연과 네트워크 불안정을 겪어본 고객은 온프레미스 나 클라우드 애플리케이션에 접속할 때 Cato를 통해 놀라운 유저경험을 합니다.

안전한 지점/지사 인터넷 접속

Cato는 Cato Cloud에 내장된 전체 네트워크 보안 스택을 제공합니다. 전 사업장을 에지 SD-WAN을 통해 Cato 글로벌 프라이빗 백본 네트워크로 연결하면 인터넷과 WAN의 모든 트래픽은 Cato의 Security as a Service로 완벽하게 보호됩니다. 포인트 보안 솔루션, 어플라이언스 또는 클라우드 서비스의 비용과 복잡성을 추가할 필요가 없습니다.

클라우드 가속화와 제어

Cato는 모든 클라우드 트래픽을 클라우드 대상과 가장 가까운 Cato PoP로 라우팅하여 클라우드 액세스를 가속화합니다. Cato의 PoP들이 주요 클라우드 서비스 공급자의 데이터센터를 코로케이션 하기 때문에 Cato와 서비스공급자들 사이 구간에서의 지연은 거의 0에 가깝습니다. 클라우드 액세스 최적화를 위해서는 Cato Cloud에서 클라우드 애플리케이션 트래픽이 어디로 내보낼 것인가를 정하는 단일 애플리케이션 레벨 규칙만 필요합니다. 클라우드 어플라이언스를 설치하거나, 클라우드까지 가는 지연을 감소하기 위한 별도의 허브를 구성할 필요가 없습니다.

모바일 보안 및 최적화

모바일 사용자의 랩탑, 스마트폰, 태블릿까지 Cato의 글로벌 네트워킹 및 보안 기술이 적용됩니다. 모바일 사용자를 네트워크와 보안 인프라에서 차별 취급할 이유가 없습니다. Cato Client 또는 클라이언트 없는 브라우저 액세스를 사용하여 사용자는 가장 가까운 Cato PoP에 동적으로 연결되며, 트래픽은 Cato 글로벌 프라이빗 백본을 통해 온프레미스나 클라우드의 애플리케이션으로 최적화되어 라우팅 합니다. Cato Security as a Service는 모바일 사용자를 모든 위협으로부터 보호하고 애플리케이션 액세스 제어를 시행합니다.

재택근무

Cato는 직원의 재택근무 환경을 항상 완벽하게 지원합니다. 고객은 온프레미스와 클라우드 데이터센터를 Cato 클라우드로 신속하게 연결하고, 재택 근무 또는 원격으로 접속이 필요한 모든 사용자에게 Cato Client 서비스를 활성화합니다. 기존 VPN과 SDP 제품들은 업무를 지원하는데 필요한 확장이 어려웠지만 Cato의 글로벌 클라우드 기반 플랫폼은 글로벌 프라이빗 백본 네트워크를 통해 응용 프로그램으로 가는 트래픽을 최적화할 수 있도록 구성되어 있으며, Cato의 융합 보안 스택은 보안위협 탐지와 접속 제어를 위한 트래픽 검사를 지속적으로 실시합니다.

Cato 클라우드
완벽한 WAN의 변신

MPLS와 기존 WAN을 교체하는 일은 단순히 우리 사무실을 신속하고 경제적으로 연결하는 기회가 아닙니다. 전 세계 어디에서든 모든 사용자를 모든 리소스에 연결함으로써 전체 조직을 변화 시킬 수 있는 기회입니다. 단순한 업그레이드가 아닌 혁신을 통해 기업은 WAN 비용을 절감하는 한편 처리량을 2배로 늘리면서 더 많은 장소를 네트워크에 추가하고, 설치 시간은 수 개월에서 불과 30분으로 단축하고, 기존 보안 어플라이언스에서 놓친 조직내 위협요인을 파악합니다.

급진적인 비전입니다만, 동시에 현실이기도 합니다. 수 백 곳에 달하는 고객들이 이미 Cato의 파워를 경험하고 있습니다. 오늘 저희와 함께 PoC를 통해 직접 경험해 보지 않으시겠습니까?

Cato. 미래를 위한 네트워크

Cato Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Secure Remote Access
- Cato Management Application

Managed Services

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

ISO 27001 Certified

SOC2 Approved

GDPR Compliant