

SASE 프로젝트를 계획하는 방법

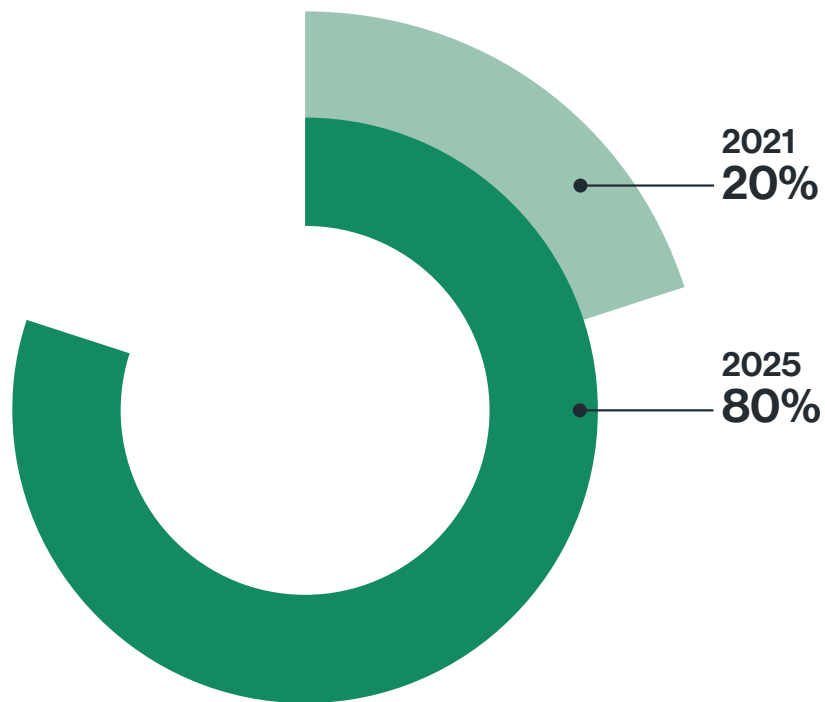


요약

지난 수십 년 동안 기업들은 복잡하고 경직된 구조에 갇혀 디지털 전환을 제대로 실행하지 못했고 비즈니스 민첩성도 확보하지 못했습니다. 하지만 이제 훨씬 더 유연한 대안이 있습니다. **SASE(보안 액세스 서비스 에지)**는 2019년 Gartner가 정의한 개념으로, 기업 네트워킹과 보안 포인트 솔루션을 단일 아키텍처로 통합하는 것을 말합니다. 이 클라우드 네이티브 아키텍처는 전 세계적으로 분산되며 원격 사용자, 사이트, 클라우드 리소스 등 모든 기업 에지를 보호합니다.

Gartner는 2025년까지 80%의 기업이 SASE를 사용하여 웹, 클라우드 서비스, 개인 애플리케이션 액세스를 통합하는 전략을 채택할 것으로 추정합니다. 이는 2021년의 20%보다 증가한 수치입니다. SASE 아키텍처를 구현하면 운영 효율성 증가, 사용자 경험 일관성 향상, 애플리케이션 및 네트워크 성능 개선, 보안 향상 등 많은 이점을 얻을 수 있습니다.

Gartner: SASE 융합 전략 채택 상황



대부분의 기업은 레거시 보안 경계를 가진 전통적인 허브 앤 스포크 방식의 광역 네트워크를 새롭고 유연한 SASE 아키텍처로 전환하기 위한 마이그레이션 계획이 필요합니다. 이러한 전환을 위해서는 좋은 계획을 세워야 합니다. Cato Networks는 이 여정을 막 시작한 기업에 현실적인 SASE 도입 프로젝트 로드맵 수립을 위한 실행 계획을 제공합니다.

팀 구축

여러 고객사들은 여전히 보안 팀과 네트워크 운영 팀이 분리된 레거시 아키텍처로 운영되고 있을 수 있습니다 . 이론적으로는 단일한 팀이 SASE 마이그레이션을 주도할 수 있습니다 . 특정 문제를 해결하기 위해 하나의 팀이 Cato 솔루션을 배포할 수도 있지만 , 이상적으로는 네트워크 팀과 보안 팀이 협력하여 미래 지향적인 네트워크를 함께 설계하는 것이 바람직합니다 . 오늘날 보안은 네트워크 운영에 있어 너무나 필수적인 요소이기 때문에 부서별로 단절되어 의사결정이 이루어지는 것은 적절하지 않습니다 . 또한 네트워크 운영 및 성능은 사용자 경험에 매우 중요하므로 무시될 수 없습니다 .

고객사의 조직 문화에 따라 필요하다면 보안 또는 네트워크 아키텍처에 직접 관여하지 않는 중립적인 인물 (프로그램 매니저 , 프로젝트 매니저 , 디지털 전환 책임자 등) 을 프로젝트 팀 리더로 지정하는 것이 도움이 될 수 있습니다 . 이 리더의 역할은 모든 요구 사항이 고려되고 팀의 나머지 구성원에게 잘 전달되도록 하는 것입니다 .

고객사의 핵심 전략 애플리케이션을 담당하는 책임자들도 팀에 포함될 수 있습니다 . 이러한 책임자들은 데이터 자산과 애플리케이션의 성능 및 보안은 물론 해당 애플리케이션을 사용하는 사용자 경험도 면밀히 확인해야 합니다 . 이는 SASE 아키텍처의 중요한 고려 사항입니다 .

또한 Gartner 는 프로젝트 팀에 인력 전환 및 지사 사무소 전환과 관련된 담당자도 포함할 것을 권장합니다 . SASE 프로젝트가 전사적인 디지털 전환 전략에 포함되어 있고 , 이 과정에서 비즈니스 프로세스와 업무 방식이 크게 달라질 것으로 예상된다면 , 이러한 요소는 특히 중요하게 고려되어야 합니다 .

왜 SASE 를 원하십니까 ?

목표 정하기

이 문서는 SASE 구축을 위한 전환 과정에 초점을 맞추며 , 그 범위는 본사 , 지사 , 원격 근무자 , 클라우드 리소스를 포함합니다 . 물론 , 고객사의 특정 요구 사항은 다른 기업들과 다를 수 있습니다 .

기업은 SASE 구현을 위한 계획을 세울 때 다음과 같은 목표를 설정하는 경우가 많습니다 .



어디서나 근무할 수 있는 작업 환경 (WFA) 및 원격 액세스 지원

팬데믹 봉쇄 조치로 인해 많은 직원이 지사 근무 대신 원격 근무를 선택했습니다 . 오늘날 대부분의 제한이 해제된 상황에서도 원격 근무 방식은 여전히 많은 이들이 선호하고 있으며 , 이러한 추세는 장기화될 가능성이 높습니다 .

앞으로도 다양한 작업 환경에서 근무하는 인력이 늘어날 것을 고려하여 안전한 액세스 요건을 관리하기 위한 계획을 마련해야 합니다 .

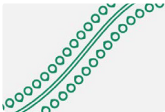


팬데믹 이후 장기적으로 원격 근무를 준비하는 방법
[더 알아보기 >](#)



전 세계 비즈니스 거점 지원하기

기업은 물리적 연결 및 클라우드 데이터 센터에 연결하기 위해 비용 효율적이고 일관된 전송 수단이 필요하며 , 이는 공용 인터넷보다 더 신뢰할 수 있고 안전해야 합니다 .



백본이라고 다 같은 백본이 아닙니다
[더 알아보기 >](#)



안전한 다이렉트 인터넷 액세스 (DIA) 구현하기

레거시 아키텍처에서는 지점 사무실에서 안전하게 인터넷을 사용하려면 모든 곳에 보안 어플라이언스를 따로 배치하는 방법과 인터넷 트래픽을 중앙 보안 거점으로 우회시키는 방법 중에서 하나를 어렵게 선택해야 합니다 . 지점 보안 어플라이언스는 운영이 상당히 복잡하기 때문에 IT 팀이 트래픽 증가에 대응하거나 CPU 집약적인 작업을 지원하기 위해 원치 않는 시점에 하드웨어를 업그레이드해야 할 수 있습니다 . 게다가 트래픽을 본사로 우회시키는 방식은 대기 시간을 늘립니다 . 효율적인 SASE 아키텍처는 가장 가까운 접속 지점 (PoP) 을 통해 안전한 DIA 를 가능하게 하므로 , 보안 어플라이언스를 따로 배치하거나 트래픽을 멀리 떨어진 보안 거점으로 우회시킬 필요가 없어집니다 .



안전한 다이렉트 인터넷 액세스
[더 알아보기 >](#)



클라우드 리소스 및 애플리케이션에 대한 액세스 제공하기

기업은 사용자가 어디에 있든 전 세계 어느 지점에서든 클라우드에 최적의 방식으로 연결할 수 있어야 합니다 . 본사 데이터 센터의 빠른 연결만으로는 충분하지 않습니다 .



AWS, Azure, 클라우드 액세스를 위한 WAN 을 최적으로 설계하는 방법
[더 알아보기 >](#)

요구 사항 수집

어떤 SASE 솔루션을 도입할지 계획하기 전에 , 연결하고 보호해야 할 사이트 , 사람 / 사용자 , 클라우드 리소스 측면에서 어떤 요구 사항이 있는지 파악해야 합니다 . 향후 새로운 요구 사항이 발생할 경우의 혼란이나 재작업을 최소화하기 위해 미래를 고려한 설계를 미리 해두는 것도 좋습니다 .



사이트

근무지 또는 지점 사무실은 소규모에서 대규모에 이르기까지 규모가 다양하고 핵심 작업 수행, 단순한 재택근무 등 목적도 여러 가지입니다 . 모든 규모와 목적에 대응할 수 있고 각 유형의 업무 요구 사항을 충족할 수 있는 네트워크가 필요합니다 .SASE 의 SD-WAN 연결 기능은 케이블 , DSL, 광케이블 , 4G 등 다양한 인터넷 회선을 통합하여 모든 회선 위에 가상 오버레이 네트워크를 구성함으로써 유연성을 제공합니다 . 부하 분산 , 각 회선의 실시간 품질 측정과 같은 기능이 있는 SD-WAN 은 다양한 인터넷 회선을 조합하여 비즈니스에 필요한 높은 서비스 가용성을 보장합니다 .

각 사이트를 중요도에 따라 분류하고 , 해당 중요도에 맞게 라스트마일 연결의 가용성과 성능 기준을 조정하는 것이 좋습니다 . 회선의 종류와 수량을 자유롭게 조합할 수 있으면 , 불필요한 과잉 투자 없이 지점별로 요구되는 구체적인 가용성 요건을 만족시킬 수 있습니다 . 과도한 비용 지출 없이 요구 사항을 충족할 수 있는 연결 방식의 예는 다음과 같습니다 .

- **본사 또는 중요한 지점** - 지역 SLA 가 적용된 이중 광회선
- **지역 지점** - DIA 와 브로드밴드의 혼합
- **소규모 지점 또는 홈 오피스** - 이중 브로드밴드 회선

애플리케이션의 최적화된 성능을 보장하기 위해 특별한 전송 방식을 고려해야 할 수도 있습니다 . 예를 들어 , 음성 및 영상과 같은 실시간 애플리케이션은 대기 시간이 증가하거나 지터 또는 패킷 손실이 발생하면 품질이 저하됩니다 . 실시간 애플리케이션을 위한 빠른 세션 장애 전환 , 패킷 중복과 같은 고성능 회선 및 기술을 계획하기 위해서는 현재 어떤 애플리케이션이 실행되고 있는지를 파악하는 것이 중요합니다 .

일부 지점의 경우 , 네트워크 및 보안 계층 차원에서고가용성 (HA) 을 고려한 인프라 설계가 필요할 수 있습니다 .SASE 는 클라우드 기반으로 제공되므로 HA 를 구축하는 일차적 부담은 서비스 업체 측에 있습니다 . 네트워크 및 보안 로직이 클라우드 서비스에서 제공되므로 사용자는 HA 를 쉽게 설계할 수 있습니다 . 그럼에도 불구하고 기업은 몇 가지 방안 중에서 선택하여 에지 연결 장비와 같은 사이트 기반 구성요소의 복원력을 확보할 수 있습니다 .

관련 글



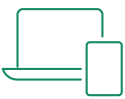
팬데믹 이후 장기적인 원격 근무를 준비하는 방법

[더 알아보기 >](#)



백본이라고 다 같은 백본이 아닙니다

[더 알아보기 >](#)



사용자

어디서나 근무하는 (WFA) 원격 및 모바일 사용자는 사용성 , 성능 , 보안과 관련된 다양한 요구를 가집니다 .SASE 개념에서는 이런 사용자 역시 지사에서 근무하는 사용자와 동일한 수준의 기능이 필요한 하나의 예지로 취급됩니다 .

SASE 솔루션을 사용하면 일반적으로 사용자의 장치에 소프트웨어 에이전트를 설치해야 네트워크에 연결할 수 있는 경우가 많습니다 . 일부 제공업체는 단순히 브라우저에서 특정 URL 에 접속하는 것만으로도 연결이 가능하도록 허용할 수도 있습니다 . WFA 사용자들이 최대한 원활하게 작업할 수 있도록 사용의 간편성을 우선적으로 고려하십시오 .



사용자들이 주로 어디에 위치해 있는지 확인하고 SASE 공급업체의 PoP 이 얼마나 가까운지 비교해 보십시오 . 대기 시간을 줄이고 애플리케이션 성능을 높이려면 PoP 과 사용자가 최대한 가까이 있는 것이 좋습니다 . 가장 가까운 PoP 에 대한 왕복 대기 시간은 일반적으로 25ms 이하여야 합니다 . 그 이상일 경우 사용자 불만이 생길 수 있습니다 .

WFA 사용자는 지사 근무자와 동일한 수준의 보안 서비스가 필요합니다 . 이로 인해 보안 스택을 어디에 둘 것인지에 대한 문제가 생깁니다 . 레거시 네트워크는 중앙 데이터 센터에 보안 스택이 집중됩니다 . 이에 따라 원격 위치와 모바일 사용자의 트래픽은 모두 본사 데이터 센터에 강제로 우회된 후 기업 보안 어플라이언스 스택을 거쳐 인터넷으로 나갑니다 . 네트워크 응답도 동일한 스택을 거쳐 데이터 센터에서 원격 사용자에게 전달됩니다 . 트롬본의 흰 파이프처럼 뒤틀린 이런 경로는 대기 시간을 증가시켜 사용자 경험에 부정적인 영향을 미칩니다 .

일부 SASE 솔루션은 미니 데이터 센터 역할을 하는 지역 허브에 보안 기능을 호스팅할 것을 권장합니다 . 이 방식은 가장 가까운 허브로 트래픽을 우회시켜 사용자 측 성능 저하를 완화할 수 있습니다 . 하지만 보안 스택의 여러 인스턴스를 관리해야 하는 근본적인 문제뿐 아니라 분산된 데이터 센터를 구축하고 성능 및 가용성 요건을 충족해야 하는 과제는 여전히 남게 됩니다 .

WFA 사용자가 네트워크에 접속하는 위치에 있는 PoP 의 보안 스택을 통합하는 SASE 솔루션을 고려해 보십시오 . 보안 기능이 PoP 에 통합되어 있으므로 별도의 보안 어플라이언스를 유지 및 관리할 필요가 없습니다 . 또한 PoP 에 접속하는 모든 사용자와 예지에 단일한 보안 정책을 적용할 수 있습니다 .

[보안 기능을 호스팅하는 위치에 대해 더 알아보려면 ‘트롬본의 소리 \(The Sound of the Trombone\)’ 를 읽어 보십시오 >](#)

사용자 요구 사항에 대한 추가 리소스 :

제로 트러스트 구축 시 흔히 발생하는 실수를 피하기 위한 CISO 가이드

[읽어보기 >](#)

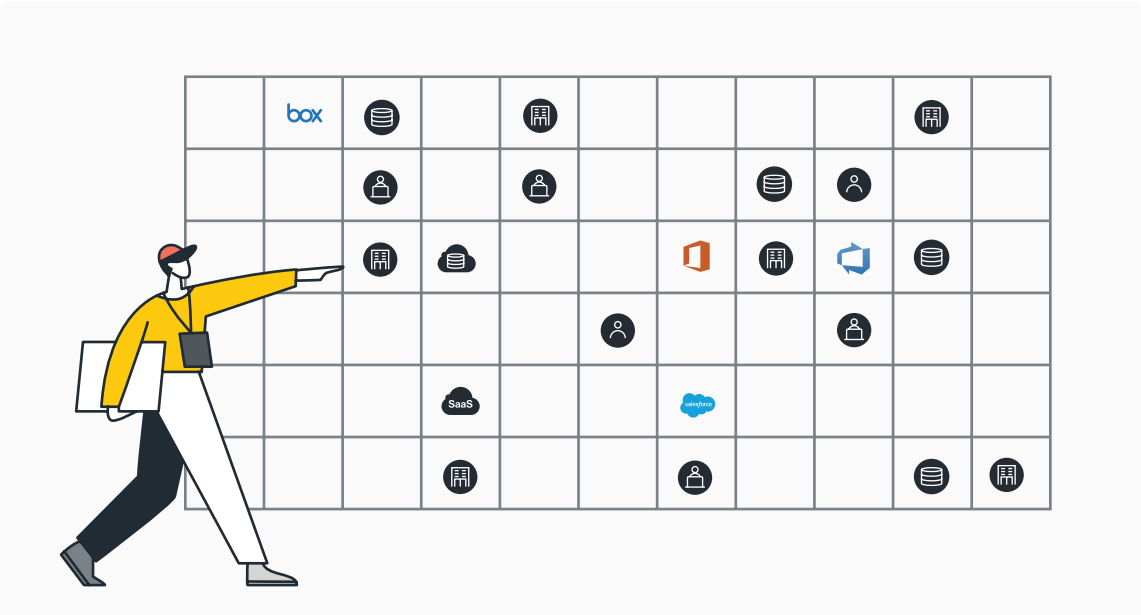


클라우드 리소스

리소스나 애플리케이션이 ‘클라우드에 있다’라고 이야기할 때 , 실제로 이것이 전 세계 어딘가의 물리적인 데이터 센터에 저장되어 있다는 사실을 떠올리는 사람은 드뭅니다 . 이러한 데이터 센터의 위치는 애플리케이션의 성능과 대기 시간에 매우 중요합니다 .

데이터 센터가 사용자에게서 멀리 떨어져 있을수록 애플리케이션과 데이터 센터 사이를 오가는 트래픽의 왕복 시간이 길어지고 사용자가 경험하는 애플리케이션의 성능은 저하됩니다 .Equinix, Rackspace, Verizon 과 같은 최상위 호스팅 기업뿐 아니라 Amazon, Microsoft, Google 과 같은 클라우드 플랫폼 기업은 수많은 지역 데이터 센터를 보유하고 있어 해당 플랫폼의 고객사는 사용자와 가까운 곳에서 애플리케이션을 호스팅할 수 있습니다 .

SASE 구현 계획 시 중요한 부분은 Microsoft 365, SAP, Salesforce 와 같은 다양한 SaaS 애플리케이션을 비롯하여 기업이 클라우드에 보유하고 있는 모든 리소스를 파악하는 것입니다 . 일부 애플리케이션은 실제로 전 세계의 여러 클라우드 호스팅 데이터 센터에 분산되어 있을 수 있습니다 . 예를 들어 , Microsoft 는 다양한 분산형 데이터 센터에 마이크로서비스를 호스팅하고 있습니다 . 이러한 호스팅 위치와 사용자 위치를 파악하면 애플리케이션 대기 시간을 예측하는 데 도움이 되며 , 이는 애플리케이션 성능에 직접적인 영향을 미칩니다 .

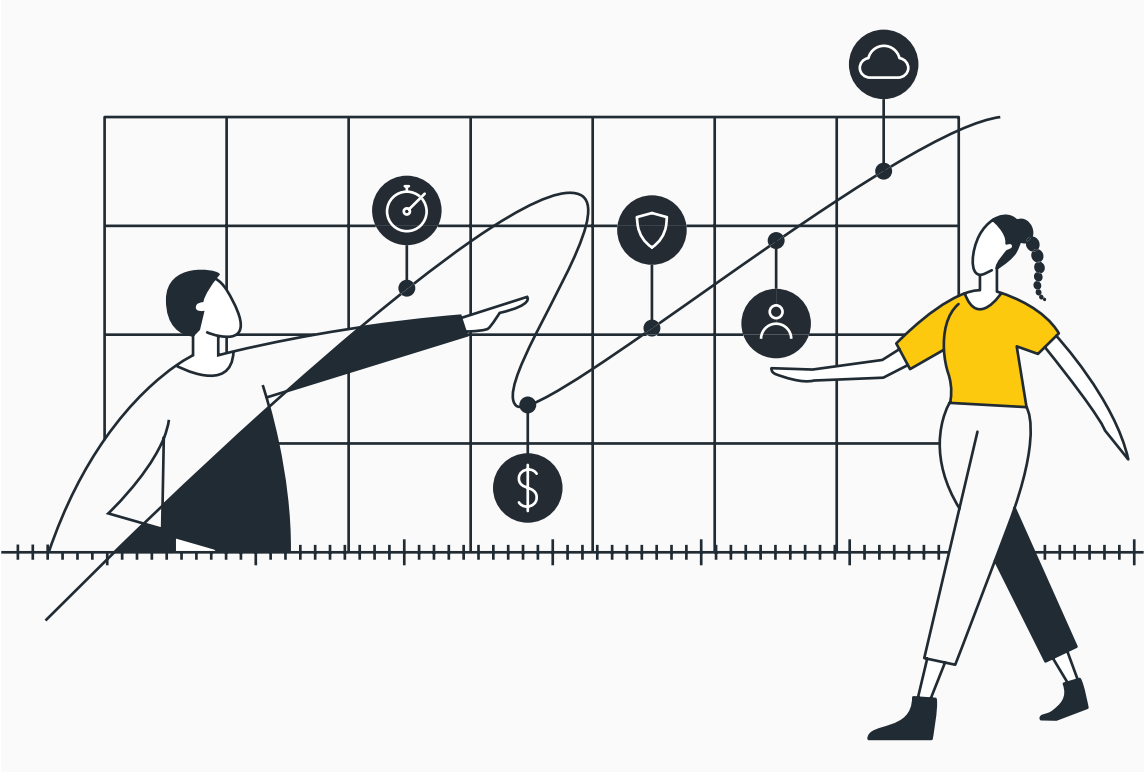


SASE 솔루션은 클라우드에 SaaS 및 기타 클라우드 서비스에 대한 온램프 역할을 하는 PoP 를 갖추게 됩니다 . 그중 일부 PoP 은 주요 SaaS 애플리케이션과 동일한 코로케이션 데이터 센터 (예 : 피어링 지점) 에 위치할 수도 있습니다 . 이 경우 애플리케이션 성능과 사용자 경험 측면에서 큰 이점이 있습니다 . 다만 , 항상 그렇게 되는 것은 아닙니다 .

따라서 클라우드 리소스가 위치한 지역을 철저히 파악하여 이러한 위치를 SASE 솔루션의 지역 간 연결 능력과 맞춰보는 작업을 수행해야 합니다 . 사용자가 지역 PoP 을 통해 애플리케이션의 가장 가까운 인스턴스에 연결될 수 있다면 트래픽이 멀리 떨어진 호스트 데이터 센터까지 이동하는 경우와 비교하여 애플리케이션 성능이 크게 향상될 수 있습니다 .

향후 고려 사항

계획 수립 팀은 아직 알 수 없는 미래의 비즈니스 요구 사항까지 수용할 수 있도록 네트워크를 ‘미래 지향적’으로 설계해야 합니다. 이는 향후에 발생하고 변화할 비즈니스 요구에 쉽게 대응하지 못하는 경직된 솔루션을 구축하는 실수를 방지하기 위한 중요한 과정입니다.



대부분의 기업과 마찬가지로 귀사 또한 경쟁사에 뒤처지거나 시장에서 도태되지 않기 위해 성장을 전략적 비즈니스 목표로 삼고 있을 것입니다. 이러한 목표를 위해 기술 플랫폼은 비즈니스 변화에 빠르게 적응하며 성장을 뒷받침할 수 있어야 합니다.

이러한 변화는 새로운 위치로의 확장을 동반할 수 있으며, 이 경우 당연히 보안 네트워크 기능이 필요합니다. 클라우드 기반 SASE 솔루션은 며칠 만에 구축이 가능하지만, 전통적인 네트워크를 위한 MPLS 회선을 확보하려면 수개월 이상이 걸릴 수 있으며, 경우에 따라 확장하려는 지역에서 회선 자체를 구하기 어려울 수도 있습니다. 예를 들어 중국에 새 시설을 여는 경우, 직접 회선을 설치해야 하거나 특정 SASE 솔루션이 해당 지역에 PoP 을 보유하고 있지 않다면 어려움이 생길 수 있습니다.

기업은 인수합병을 통해 성장할 수 있습니다. 계약이 성사된 이후에는 양사의 IT 시스템을 최대한 빨리 통합하는 것이 아주 중요합니다. 레거시 네트워크를 사용할 경우 시스템 통합에 수년이 걸릴 수 있지만, SASE 플랫폼을 활용하면 인수한 기업에 대한 신규 서비스를 며칠 내지 수주일 내에 구축할 수 있습니다.

귀사는 시간이 지남에 따라 점진적으로 더 많은 애플리케이션을 클라우드로 이전할 것입니다. 앞서 언급했듯이, SASE 솔루션의 PoP 과 클라우드 내 애플리케이션이 호스팅된 위치 사이의 거리는 애플리케이션 성능에 결정적인 영향을 미칩니다. PoP 이 전 세계적으로 분산되어 있는 SASE 솔루션을 선택하십시오.

요약하면, SASE 플랫폼은 현재와 미래에 필요한 모든 기능을 하나로 통합합니다. 대조적으로, SASE 가 아닌 기존 방식을 사용하면 각 요구 사항을 충족하기 위해 여러 제품을 직접 찾아보고, 평가하고, 구매하고, 통합하고, 관리해야 합니다. 이러한 수고를 할 필요 없이 준비되었을 때 스위치만 켜면 새로운 기능을 사용할 수 있다고 생각해 보십시오. 얼마나 많은 시간을 절약할 수 있을지 짐작할 수 있을 것입니다.

RFI 작성

SASE 솔루션에 대한 요구 사항을 수집했고 귀사가 원하고 필요로 하는 것을 파악했다면 , 여러 공급업체에 정보 요청서 (RFI) 를 보내 그들이 귀사의 요구를 충족하기 위해 어떤 제안을 할지 확인할 차례입니다 . 이를 통해 개념 검증 (PoC) 단계로 나아가기 전에 시장 상황과 다양한 선택 사항을 확인할 수 있습니다 . 귀사의 RFI 에는 다음 내용이 포함되어야 합니다 .



비즈니스 및 IT 개요

공급업체가 귀사의 환경을 충분히 이해한 후 그에 맞춰진 제안을 하고 자사 솔루션이 귀사에 구체적으로 어떤 가치를 제공하는지를 설명할 수 있도록 해야 합니다 . 이 섹션에서는 귀사의 비즈니스 , SASE 프로젝트의 목표 , 비즈니스 대상 지역 , 네트워크 리소스 범위 등을 다루어야 합니다 . 또한 네트워크 토폴로지 , 네트워크 및 보안 스택 구성 , 다양한 네트워크 연결 대상 간의 연결 및 보안 방식에 대한 자세한 설명도 포함해야 합니다 .



솔루션 아키텍처

많은 SASE 솔루션이 유사한 기능을 가지지만 , 해당 기능이 제공되는 방식은 비용 , 복잡성 , 그리고 전체 프로젝트의 성공에 영향을 미칩니다 . 따라서 기능이 어떤 아키텍처 요소로 구성되어 있는지 , 그 역할은 무엇인지 , 어디에 배치되는지 (지사 , 장치 , 클라우드) , 어떻게 확장되는지 , 장애 발생 시 어떻게 대응하고 복원력을 제공하는지 등을 명확히 이해하는 것이 중요합니다 .



솔루션 기능

이 섹션의 목표는 솔루션이 SD-WAN, 클라우드 , 보안 , 모바일 등 다양한 영역에서 제공하는 기능을 이해하는 데 있습니다 . 귀사 네트워크의 요구 사항을 선택하십시오 .



지원 및 서비스

공급업체의 고객 지원 체계와 관리형 서비스 종류를 파악해 두십시오 . 글로벌 조직의 경우 , 24 시간 글로벌 순환 지원 모델이 필수적입니다 . 또한 기존에 통신사 계약을 통해 완전 관리형 서비스를 이용해 왔다면 , 이번 프로젝트는 셀프서비스 또는 공동 관리 모델로 전환할 수 있는 기회가 될 수 있습니다 .



RFI 작성

[SASE-RFP-Template 받기 >](#)



SASE 제공업체에 물어볼 5 가지 질문

[전자책 받기 >](#)

점진적 배포 계획 (사이트 / 기능)

점진적인 구축 계획을 수립하면 , 몇 개의 사이트부터 시작해 전체 구조에 대한 감을 잡은 후 점진적으로 확장할 수 있습니다 .

다음은 이러한 점진적 전환을 가능하게 하는 대표적인 SASE 사용 사례들입니다 .



MPLS 를 SD-WAN 으로 전환

SASE 아키텍처를 사용하면 MPLS 에서 SD-WAN 으로 간단하게 전환할 수 있습니다 . SASE 는 MPLS 와 SD-WAN 을 병행하여 운영할 수 있도록 지원하기 때문입니다 . 이는 특정 사이트만 전환하고 , 자체 일정에 따라 점진적으로 MPLS 를 종료하거나 신규 사이트부터 SD-WAN 으로 시작할 수도 있다는 의미입니다 . 레거시 보안 및 원격 액세스 솔루션은 그대로 유지되고 , SASE 의 SD-WAN 기능만 활용됩니다 . 이를 통해 라스트마일 구간에 대한 유연성을 확보할 수는 있지만 , SASE 를 통한 보안 간소화의 이점은 누리지 못합니다 .



MPLS 계약 조기 해지 방법

[블로그 글 읽기 >](#)



글로벌 연결 최적화

글로벌 사이트와 애플리케이션의 성능을 높이기 위해 SASE 아키텍처로 전환하는 경우가 많습니다 . 이 사용 사례에서는 중요한 WAN 애플리케이션을 위해 MPLS 연결을 유지하면서 모든 트래픽 백홀링은 제거할 수 있습니다 . 어떤 방식을 선택하든 SASE 는 인터넷 및 WAN 애플리케이션 또는 위치에 대한 연결성을 개선하는 데 사용될 수 있으며 , 특히 MPLS 적용이 어려운 곳에서 활용하기 좋습니다 .



지점 인터넷 액세스 보안

지점 인터넷 액세스 보안은 SASE 도입을 고려하는 또 다른 주요 이유입니다 . MPLS 기반 환경에서 인터넷 브레이크아웃을 사용하거나 MPLS 없이 다이렉트 인터넷 액세스를 하는 경우 , 에지 보안이 필요합니다 . SASE 를 도입하면 모든 트래픽을 클라우드 보안 스택으로 우회시킴으로써 NGFW, SWG, IPS, AM 같은 별도의 에지 보안 장비를 둘 필요가 없어집니다 .



클라우드 가속 및 제어

클라우드 데이터 센터 및 애플리케이션의 성능과 제어를 개선하는 것이 SASE 도입의 주요 동기가 되는 경우도 있습니다 . SASE 는 글로벌 PoP 네트워크를 통해 클라우드 데이터 센터에 대해 최적화된 사설 네트워크 액세스를 제공합니다 . SaaS 애플리케이션은 고급 라우팅 정책 덕분에 예측 불가능한 인터넷이 아닌 최적화된 네트워크를 통해 트래픽이 처리됩니다 .



원격 액세스

어디서나 근무할 수 있는 작업 환경에 대한 오늘날의 요구 사항으로 인해 기존 VPN 만으로는 비즈니스 요구를 충족하기 어렵습니다 . 이러한 상황에서는 VPN 서버 추가 없이 보안도 유지하면서 원격 근무자의 접속을 신속히 확장할 수 있는 SASE 가 대안이 될 수 있습니다 . SASE 는 글로벌 PoP 네트워크를 통해 원격 근무자의 트래픽을 안전하게 보호하고 최적화해 줍니다 .



ZTNA 배포 시 발생하는 어려움을 올바른 솔루션으로 극복하기

[블로그 글 읽기 >](#)



SASE 를 단계적으로 배포하기

[이러한 사용 사례에 대한 추가 정보 >](#)

비즈니스 타당성 분석

네트워크 전환은 비즈니스 성장을 촉진하고 시장 점유율 확대를 돕는 게임 체인저 전략입니다 . 따라서 SASE 로의 마이그레이션은 이사회가 결정해야 할 사안입니다 . 이사회 승인을 받는 일은 장기적으로 비즈니스 목표를 실행하고 추진할 수 있는 역량을 확보하는 데 중요합니다 .

CIO 는 이사회에 보고할 때 기술 전략을 이사회가 중시하는 핵심 사안들과 연계하여 제시하고 다음과 같은 관점에서 설명해야 합니다 .

- 이 전략이 기업의 IT 대응 속도를 높이고 비즈니스 성장을 지원하는 역량을 강화하는 데 어떻게 도움이 되는지
- 이 이니셔티브를 통해 기업이 얻을 수 있는 비즈니스 가치
- 이 전략이 보안 측면에서 핵심 애플리케이션에 미치는 긍정적 효과
- 증가하는 보안 위협에 대한 IT 조직의 대응 역량을 높이는 방법
- 이 이니셔티브의 단기 및 장기 재무적 영향
- 기업의 현재 및 차세대 IT 인재에게 미치는 영향

이러한 전략을 논의할 때 , 네트워크 전환을 통해 비즈니스 성과를 달성하기 위해서는 단순화 , 최적화 , 리스크 완화가 필수적이라는 점을 명확히 전달하는 것이 핵심입니다 . 그리고 바로 이 과정에서 보안 액세스 서비스 에지 (SASE) 는 이사회와의 전략적 논의를 이끌어가는 핵심 개념이 됩니다 .

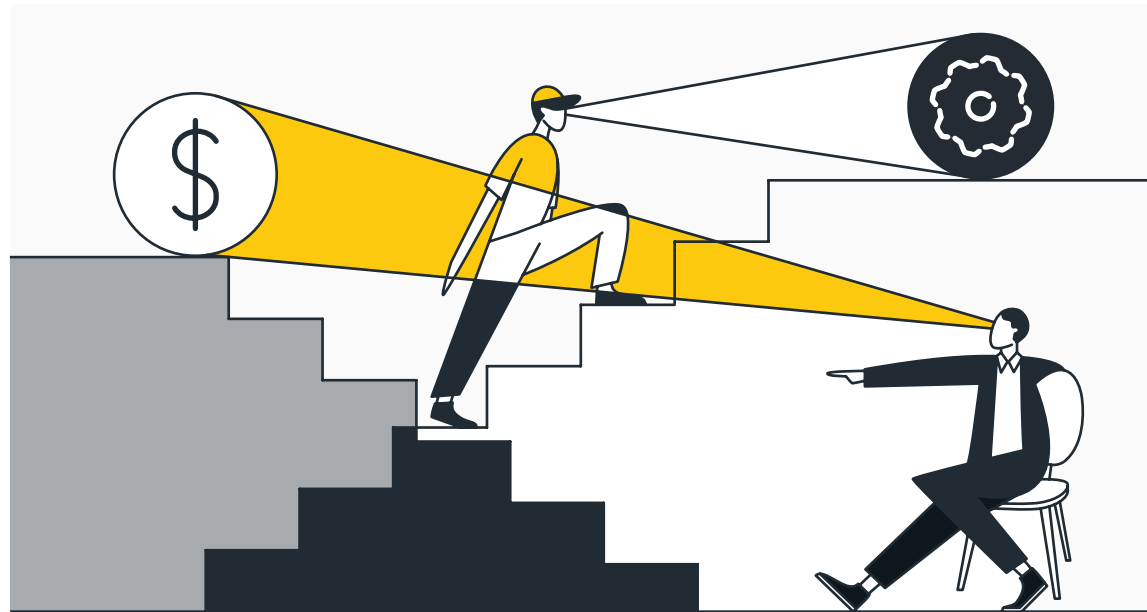
SASE 는 리스크 관리 , 성장 , 재무적 유연성과 같이 이사회에서 주로 우려하는 문제를 해결할 수 있는 네트워크 전환 수단입니다 . SASE 는 네트워킹과 보안 기능을 단일한 고성능 클라우드 네이티브 아키텍처로 통합합니다 . 이를 통해 기업은 효율성과 성능을 높이면서 핵심 비즈니스 운영을 확장하고 , 일관된 정책 및 보안 기능을 유지할 수 있습니다 .



**이사회에서 SASE 에 대해 설명하기 :
CIO 가 ‘승인’을 이끌어내는 방법**

[비즈니스 타당성 분석을 위한 조언 얻기 >](#)

이사회는 비즈니스의 장기적인 재무 성과 목표에 집중합니다 . 이사회는 네트워크 전환이 재무제표와 고객 유지에 어떻게 도움이 되는지를 이해해야 합니다 . 많은 CIO 들은 기술 투자와 재무 지표를 직접 연결 짓는 것을 꺼립니다 . 하지만 SASE 가 재무 개선에 기여하는 구체적 효과를 설득력 있게 설명한다면 SASE 를 명확한 ROI 창출 수단으로 인식시킬 수 있습니다 .



SASE 로의 전환이 재무에 미치는 영향은 솔루션 공급업체마다 크게 다를 수 있습니다 . 경쟁사의 사례에 대해서는 언급하지 않겠습니다 . 하지만 Cato Networks 솔루션의 총 경제 효과 (Total Economic Impact) 는 Forrester 가 실제 고객과의 심층 인터뷰를 바탕으로 분석한 자료를 통해 확인할 수 있습니다 . Forrester 는 인터뷰에 응한 고객의 경험을 종합해 하나의 대표 조직 (Composite Organization) 을 구성했습니다 . 그 결과 대표 조직의 투자 수익률은 246% , 순현재가치 (Net Present Value) 는 433 만 달러 , 투자 회수 기간은 6 개월 미만인 것으로 분석되었습니다 . 이 Forrester 보고서는 SASE 솔루션 도입 시 재무적 타당성을 입증하고 제시하는 데 유용한 자료입니다 .



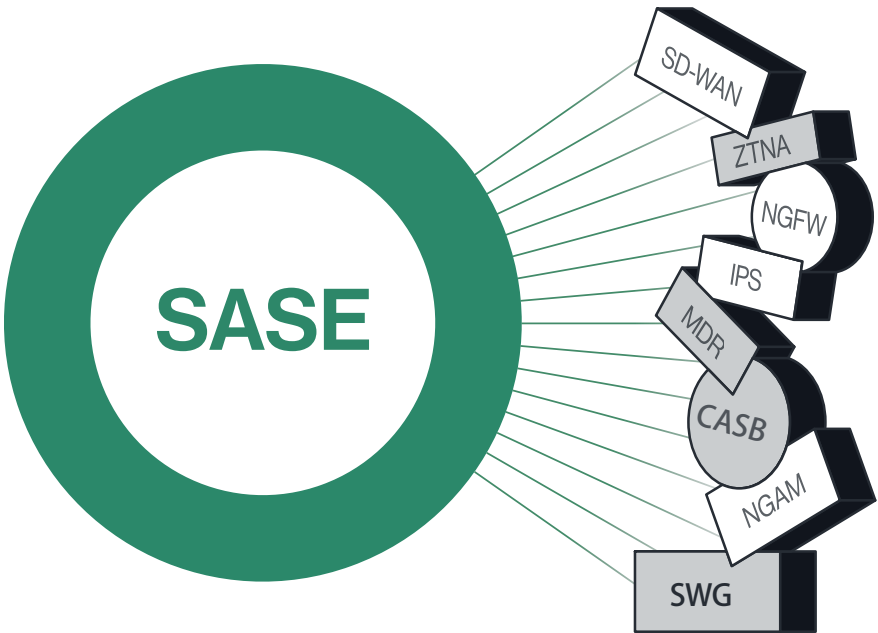
**Forrester Research: Cato SASE 클라우드
의 총 경제적 영향 ™ 보고서**

[읽어보기 >](#)

네트워킹 및 보안 팀 내에서 합의 이끌어내기

SASE의 일부라도 도입하기로 결정되면 다음 과제는 네트워크 팀과 보안 팀 사이에 공감대를 형성하는 것입니다. 이들의 동의를 얻는 일은 매우 중요합니다. 현재 자신들이 지원하고 있는 기술이 변화하거나 사라질 경우, 일자리가 위협받는다고 느낄 수 있기 때문입니다.

합의를 이끌어내기 위해 반드시 해야 하는 일은 SASE가 전사적으로 전략적 가치를 발휘하는 사용 사례들을 강조하는 것입니다. SASE를 성공적으로 구현하면 클라우드 마이그레이션, 재택근무 정책, 서비스형 통합 커뮤니케이션 (UCaaS), 글로벌 확장 프로젝트 등 많은 것들을 보다 수월하게 추진할 수 있습니다. 여러 사용 사례에 따르면 SASE는 복잡성을 완화하여 네트워크 및 보안 문제를 줄이는 데 그치지 않고, IT 업무를 간소화하여 IT 팀이 비즈니스 목표 달성을 위한 전략적인 노력에 집중할 수 있도록 합니다.



SASE는 보안 전문가에게 핵심 업무인 환경 내 리스크 완화의 기회를 제공합니다. 오랜 기간 동안 개별적인 문제를 해결하기 위해 포인트 솔루션을 도입하면 기술 환경이 과도하게 복잡해집니다. 이로 인해 보안 사각지대가 발생하고 복잡성이 증가하며 리스크 관리가 어려워집니다. SASE는 보호 체계를 단순화하고 가시성을 높이며 위협 탐지 및 대응을 개선하고 보안 정책을 통합하며 감사 과정을 용이하게 함으로써 실질적으로 리스크를 완화할 수 있습니다. 또한 SASE는 핵심 애플리케이션에 대해 단순한 제로 트러스트 접근 방식을 적용하여 네트워크 전반에 걸쳐 일관된 정책을 시행합니다.



원격 액세스가 네트워크 및 보안 팀의 협업
프로젝트가 되어야 하는 이유

[다운로드 >](#)

개념 검증 프로젝트 실행

SASE 솔루션은 기존의 레거시 네트워크 및 보안 구성과는 전혀 다른 방식을 사용합니다. 게다가 다양한 SASE 공급업체의 솔루션도 서로 다릅니다. 따라서 특정 솔루션 도입을 결정하기 전에 귀사의 사용 사례 중 하나에 기반한 개념 검증 (PoC) 프로젝트로 시험 운영을 해보는 것이 가장 좋습니다. PoC 를 통해 확신을 가지고 솔루션 도입에 대한 결정을 내리는 데 필요한 경험을 얻을 수 있습니다. PoC 계획은 간단하게 구성하고 공급업체는 2-3 곳 이내로 제한하여 각 업체당 약 30-60 일간 평가하는 것이 좋습니다.

SASE 전면 도입 시 달성하고자 하는 목표와 가까운 한두 가지의 사용 사례를 선택하십시오. 다양한 지리적 위치에 있는 지점과 사용자가 PoP 연결 상태, 애플리케이션 성능, 사용 경험 등을 실제로 체감할 수 있도록 하십시오. 최종적으로 전체 프로젝트에 배포될 다양한 유형의 회선도 테스트해야 합니다. 실제 운영 환경에 최대한 가까운 방식으로 테스트를 진행하십시오. 또한 SASE 솔루션을 완전히 구현한 이후에도 레거시 장비를 그대로 사용할 계획이라면, 새로운 구성요소 및 장비와의 통합 시 호환되는지 여부도 반드시 점검해야 합니다.



PoC 를 시작하기 전에 여러 시나리오가 포함된 테스트 계획을 수립하고 성공을 측정할 방법을 결정하십시오. 두 가지 이상의 공급업체 솔루션을 테스트할 계획이라면 두 솔루션을 비교하는데 사용할 지표도 명확히 정의해야 합니다. 가능하다면 완전히 구현했을 때 기대되는 절감 효과를 추정하기 위한 비용 - 편익 분석도 포함하십시오.

발생한 문제나 실패 사례는 문서화하고, 그 원인에 대한 판단도 기록해 두어야 합니다. 이러한 문제나 실패는 해당 솔루션에 내재적 한계가 있어 전사적으로 도입하기에는 부적절하다는 신호일 수 있습니다.

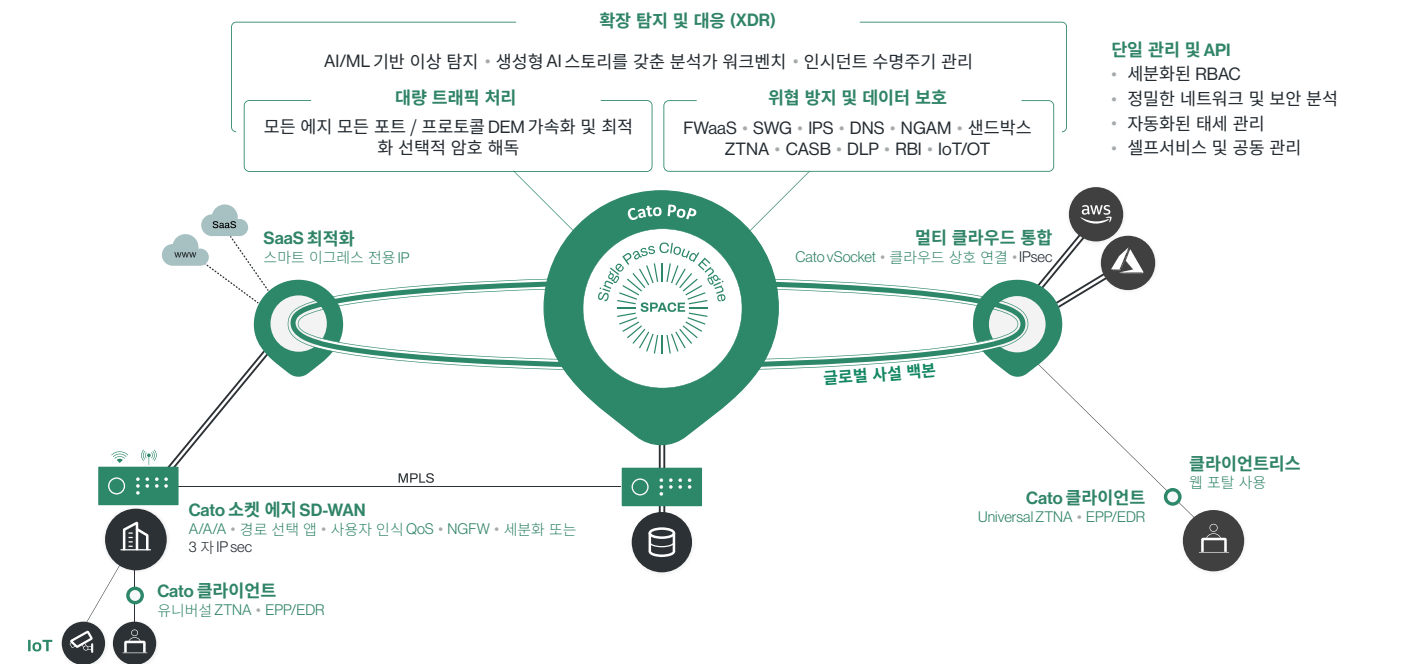
결정 내리기

SASE 아키텍처로의 전환을 통해 달성하려는 목표를 알고 있습니다. 사용 사례를 명확하게 구상하고 있습니다. 이사회는 SASE 기술을 통해 비즈니스를 지원하고 더욱 활성화하려는 귀하의 접근 방식과 제안을 지지합니다. 네트워크 및 보안 팀이 솔루션을 조속히 도입하기를 원합니다. 한 가지 또는 두 가지의 모델을 이미 테스트하여 그 성능을 알고 있습니다. 비용 - 편익 분석을 통해 기대할 수 있는 절감 효과를 어느 정도 예상합니다. 이제 모든 준비가 갖춰졌으므로 충분한 검토를 마쳤다는 확신을 가지고 SASE 솔루션을 선택할 수 있습니다.

Cato Networks 소개

Cato 는 세계 최고의 단일 공급업체 SASE 플랫폼을 제공합니다 . Cato 는 위협 방지 , 데이터 보호 , 신속한 사고 탐지 및 대응을 손쉽게 구현하는 매끄럽고 세련된 고객 경험을 창출합니다 . Cato 를 사용하면 기업은 비용이 많이 들고 경직된 레거시 인프라를 SD-WAN, 목적에 맞게 설계된 글로벌 클라우드 네트워크 , 내장된 클라우드 네이티브 보안 스택에 기반한 개방적이고 모듈화된 SASE 아키텍처로 쉽게 교체할 수 있습니다 .

Cato SASE 클라우드 플랫폼



Cato. 저희는 SASE 그 자체입니다 .

Cato SASE 클라우드 플랫폼

사용 사례

연결 클라우드 네트워크 클라우드 온램프	네트워크 전환 MPLS 에서 SD-WAN 으로 의 전환 글로벌 액세스 최적화 하이브리드 클라우드 및 멀티 클라우드	보안 혁신 안전한 하이브리드 근무 안전한 다이렉트 인터넷 액세스 안전한 애플리케이션 및 데이터 액세스 인시던트 탐지 및 대응
네트워크 보안 엔드포인트 보안	비즈니스 혁신 공급업체 통합 지출 최적화 M&A 및 지역 확장	
탐지 인시던트 수명주기 관리		
실행 통합 관리 및 API		

문의하기