CLOUDFLARE

전자책

CISO의 SASE 채택 가이드

우선순위가 높은 사용 사례의 SASE 플랫폼 평가 방법

사이버 복원력을 달성하려는 사명

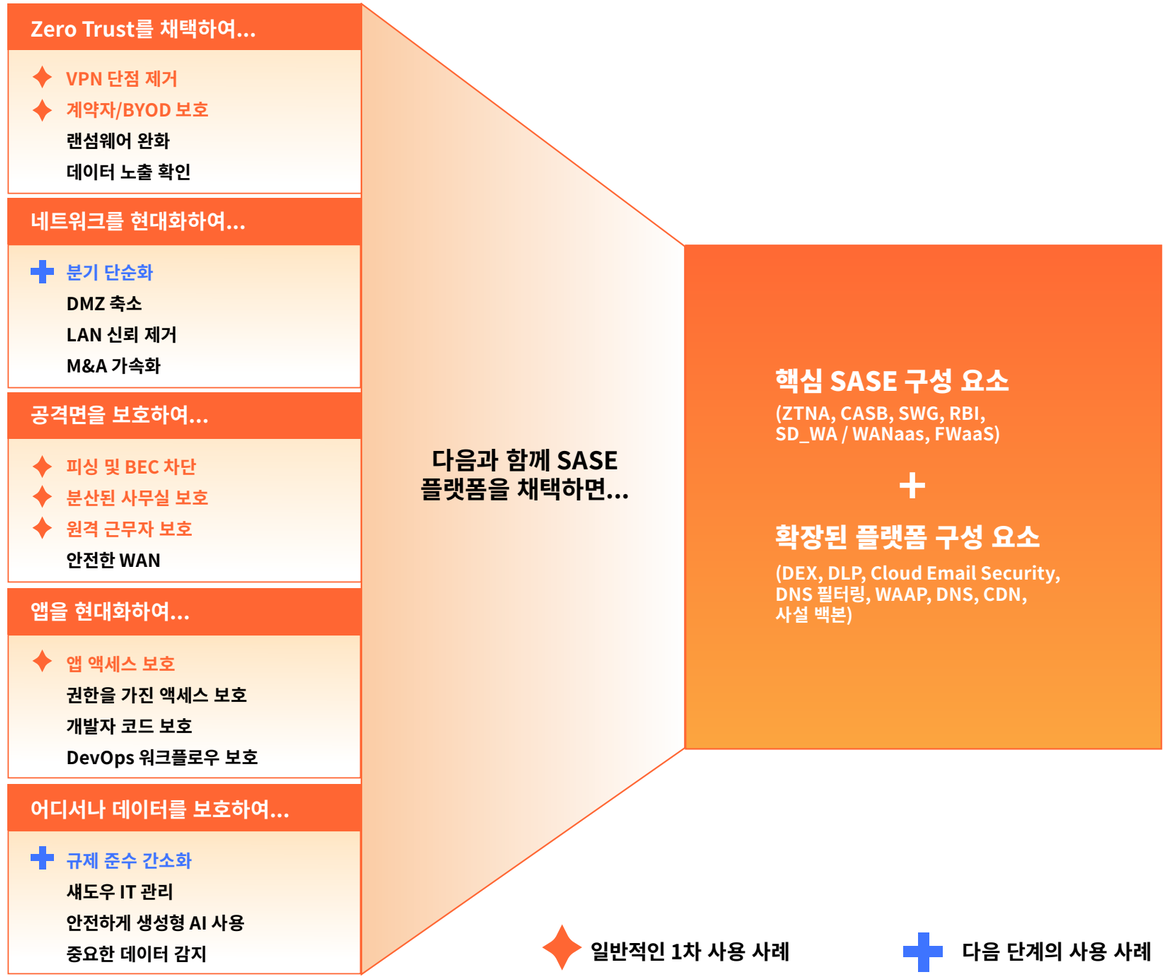
미국 국립표준기술원(NIST)에서 내린 사이버 복원력의 정의는 사이버 리소스를 사용하거나 사이버 리소스로 구동되는 시스템에서 불리한 조건, 스트레스, 공격 또는 손상을 예측하고, 견뎌내고, 이로부터 복구하고, 적응하는 능력입니다.

유출 완화 비용을 줄이면서도 사이버 복원력을 강화하는 과정에는 몇 가지 어려움도 있습니다.

- **계속 전술을 발전시키는 사이버 범죄자:** 공격자가 더 정교한 도구, 기술, 절차를 개발하고 있어 위협 환경은 조직에서 보호하기 훨씬 더 어려워지고 있습니다.
- **점점 더 복잡해지는 IT 환경:** 멀티클라우드 아키텍처를 통해 많은 장치와 애플리케이션이 연결되어 있어 환경을 보호하는 비용이 많이 들며 프로세스도 복잡합니다.
- **내부 팀 과부하:** 예산이 축소되고 내부 팀 업무가 과도해지면서 조직 리소스에 제약이 생길 수 있습니다.

이러한 문제를 극복하기 위해 보안 액세스 서비스 에지(SASE) 프레임워크로 전환하는 CISO가 많습니다. 이전의 네트워킹 접근 방식과 달리 SASE 아키텍처는 보안과 네트워킹을 하나의 클라우드 플랫폼에 통합하여 일관된 가시성과 제어를 제공합니다. SASE는 기업 데이터 센터가 아닌 클라우드 에지에 네트워크 제어 기능을 배치하므로, 기업에서는 위치와 관계없이 모든 사용자, 앱, 장치, 네트워크에 간편하고 안전한 액세스를 제공할 수 있게 됩니다.

이 가이드에서는 가장 일반적인 몇 가지 SASE 사용 사례를 소개하고 SASE 실행을 시작하기 위한 핵심 단계를 소개하여 사이버 복원력을 강화하고 빠른 성과를 달성할 수 있습니다.



사용 사례 1번:

Zero Trust 네트워크 액세스(ZTNA) 채택

하이브리드 근무 준비, 멀티클라우드 환경, 관리되지 않는 장치에 기존의 경계 기반 보안을 적용하는 조직의 가시성은 제한되고, 구성은 서로 충돌하며, 조직에 과도한 위험이 따르게 됩니다. 세분화된 접근 제어로 엔터티를 기본적으로 신뢰하지 않도록 하는 Zero Trust 접근 방식은 보안 전략을 현대화하는 데 다음과 같은 방식으로 도움을 줄 수 있습니다.

기존의 하드웨어 기반 보안 대체

가상 사설망(VPN)과 같은 기존의 네트워크 경계 제어는 확장하기 어렵고 가시성에 영향이 미칠 수 있으며 보안 팀에서 공격을 발견하고 해결하기 어려울 수 있습니다. SASE 모델에서는 Zero Trust 네트워크 액세스(ZTNA)를 구현하면서도 네트워크 트래픽을 전역 클라우드 네트워크에서 라우팅하고 처리함으로써 최종 사용자의 마찰과 내부망 이동을 모두 줄여 안전한 대안을 제시합니다.

장치 액세스 관리

계약자, 에이전시, 공급업체 등의 제3자 사용자에게 액세스 권한을 부여할 때, 조직에서 실수로 관리되지 않는 장치에 권한을 너무 많이 프로비저닝하거나 액세스 권한을 너무 많이 부여할 경우 위험이 생길 수 있습니다. 조직에서 SASE를 이용하면 제3자 사용자가 필요한 항목에만 액세스하게끔 클라이언트리스 Zero Trust 정책을 설정할 수 있습니다.

랜섬웨어 공격 방지

랜섬웨어는 전체 네트워크에서 빠르게 확산될 수 있고, 여러 네트워크와 조직 전체에 퍼지는 경우도 있습니다. SASE는 감염이 감지되자마자 네트워크와 애플리케이션 액세스를 취소하여 랜섬웨어 공격이 확산되지 않도록 방지하는 데 유용합니다. 이러한 방식은 '최소 권한 접근 제어'라는 Zero Trust 원칙에 기반하므로, 공격자가 권한을 상승시켜 네트워크 안에서 내부망을 이동하기가 어려워집니다.

데이터 노출 제한

사용자가 승인된 애플리케이션과 승인되지 않은 애플리케이션에서 중요한 정보를 업로드하거나 배포할 때, 데이터 노출 및 유출은 조직에 심각한 위협이 될 수 있습니다. SASE Zero Trust 정책을 통해 각 사용자가 액세스할 수 있는 애플리케이션을 제한하여 데이터 노출을 방지하는 동시에, 자주 사용되는 SaaS 제품군을 스캔하여 중요한 데이터와 잘못된 구성이 있는지 확인할 수 있습니다.

사례 연구

Zero Trust 채택

Fortune 500대 통신업체 중 한 공급업체에서는 Cloudflare의 SASE 플랫폼을 사용하여, AWS, Azure, 기타 클라우드 환경에서 호스팅되는 수백 개의 애플리케이션 전체에서 직원 10만 명 이상의 하이브리드 근무 환경을 보호했습니다. 이 기업은 ID 기반 Zero Trust 네트워크 아키텍처, 보안 웹 게이트웨이, 통합 접근 제어를 사용해 정책 구축 인터페이스, VPN, 인터넷 필터링 서비스 여러 개를 바꾸어가며 사용하지 않고도 위협에서 사용자를 보호할 수 있었습니다.

사용 사례 2번:
공격면 보호

디지털 변환과 원격 근무로 인해 공격면이 넓어지면서, 더 널리 흩어져 있는 사용자와 관리되지 않는 장치에 내부 리소스 액세스 권한이 필요해졌습니다. 그러나 온프레미스 방화벽을 클라우드로 넓히고 VPN을 통해 네트워크를 규모를 늘리면 외부 위협과 내부 위협 모두에 더 많이 노출되고 가시성까지 동시에 줄어들 수 있습니다. SASE 아키텍처를 사용하는 조직에서는 가시성과 제어 능력을 넓혀, 다음과 같은 방식으로 “무경계” 모델을 지원하고 일관된 보호 조치를 시행할 수 있습니다.

멀티 채널 피싱 방지

공격자는 사용자가 방심한 채로 클릭하기 쉬운 채널, 특히 이메일 보안 제어로 보호되지 않는 도구에 피싱 공격을 하는 경우가 많습니다. 통합 SASE 플랫폼은 모든 환경을 포괄적으로 보호하여 자격 증명 도용, 계정 탈취, 데이터 유출의 위험을 완화합니다.

원격 근무자 방어

원격으로 업무를 진행하려면 사용자들이 여러 위치와 장치에서 연결해야 하며, 이러한 위치와 장치는 원격 근무자를 고용한 조직의 권한 밖에 있는 경우가 많습니다. 조직에서는 핵심 환경 및 데이터에 대한 직원 액세스 권한과 제3자 액세스 권한을 보호하는 데 SASE 아키텍처를 사용하여, 보호되고 생산적인 하이브리드 근무 접근 방식을 보장할 수 있습니다.

사용자 경험 개선하기

사무실 트래픽을 스크러빙하는 기존 접근 방식은 트래픽을 중앙 집중식 기업 데이터 센터로 백홀링해야 하는 경우가 많으므로 대기 시간이 늘어나고 생산성이 떨어질 수 있습니다. 하지만 사용자에게 인터넷에 직접 액세스할 권한을 부여하는 대안을 사용하면 보안 위험이 초래되고 사용자 경험이 일관적이지 않게 됩니다. SASE는 모든 클라우드 또는 인터넷 대상에 대한 직접 연결을 지능적으로 관리하고 최적화하며, 최종 사용자와 최대한 가까운 곳에서 정책과 보호 조치를 시행합니다.

광역 네트워크(WAN) 보안

일부 WAN은 지사 간 트래픽에서 클라우드 보안을 우회합니다. 그래서 보안 서비스와 소프트웨어 정의 WAN을 통합한다는 주장은 처음에 생각했던 것과 다를 수 있습니다. 조직에서 SASE를 사용하면 사무실, 데이터 센터, 퍼블릭 클라우드, 광범위한 인터넷 내외부의 기타 위치 간의 트래픽을 필터링하고 검사함으로써 WAN 연결 방식을 단순화하고 보호할 수 있습니다.

사례 연구

늘어나는 공격면 보호

Werner Enterprises는 클라우드 마이그레이션 과정에서 중요한 비즈니스 또는 고객 서비스 중단 없이 SASE 서비스를 원활하게 배포했습니다. 이 회사는 배포 후 악성 이메일을 50% 이상 줄였고 수동 이메일 분류 작업 시간까지 하루에 몇 시간씩 최소화하여, 보안 팀에서 더 전략적인 비즈니스 목표에 집중할 수 있게 되었습니다.

사용 사례 3번:

어디에서든 데이터 보호

데이터가 더 많은 환경에 있게 되면서 조직에서 추적하는 데 어려움을 겪는 경우가 많습니다. 생성형 인공 지능과 섀도우 IT를 승인 없이 사용하면 중요한 데이터가 노출되어 손상 또는 유출로 이어질 수 있으며, 복구하는 데 많은 비용이 들 수 있습니다. SASE는 웹, SaaS, 사설 앱 환경 전반에서 데이터 가시성과 제어를 통합하여 조직에서 다음 사항을 달성하는 데 도움을 줍니다.

데이터 프라이버시 규제 준수 간소화

대규모 언어 모델(LLM) 및 기타 AI 도구가 등장했으니, 사용자 데이터를 보호하기 위한 규정 준수 표준 역시 진화해야 합니다. SASE는 데이터 제어를 통합하여 데이터를 비공개 상태로 안전하게 지켜주므로, 보안 팀에서 규제 대상 데이터 클래스를 막고 유출 위험을 줄이며 엄격한 데이터 요구 사항에 계속 따를 수 있습니다.

생성형 AI의 안전한 사용

AI를 채택하는 조직이 많아질수록 중요한 데이터의 노출 위험도 높아집니다. 보안 웹 게이트웨이 및 인라인 클라우드 액세스 보안 브로커라는 SASE 접근 방식을 통해 보안팀은 AI 애플리케이션 사용을 감지하고 승인하거나, 데이터 유출 위험이 있는 잘못된 구성을 스캔하거나, 격리된 웹 브라우저에서 AI 앱을 실행하여 데이터 입력 및 출력을 제한할 수 있습니다.

섀도우 IT 관리

섀도우 IT(조직에서 관리하거나 보호하지 않은 미승인 애플리케이션)의 경우, 중요한 데이터가 섀도우 IT로 이동할 위험이 생길 수 있습니다. SASE는 인라인 클라우드 액세스 보안 브로커(CASB)를 통해 트래픽에 프록시를 설정하여 이러한 위험을 최소화합니다. 클라우드 액세스 보안 브로커는 모든 연결과 요청을 기록하고 승인되지 않은 애플리케이션의 존재를 확인한 다음 조직에서 해당 앱의 액세스 및 사용을 제어할 수 있게 합니다.

중요한 데이터 보호

SASE 아키텍처를 사용하는 조직은 중요한 데이터가 IT 환경의 내부, 주변, 외부로 이동하는 방식을 감지하고 제어할 수 있습니다. 그 예로는 앱을 스캔하고 트래픽에서 규제 대상인 개인 데이터 및 지적 재산을 검사하는 것, 피싱 및 랜섬웨어 등의 인터넷 위협을 차단하는 것, 데이터 도난 및 의도치 않은 유출에 추가 보호 조치를 구현하는 것 등이 있습니다.

사례 연구

모든 곳에서 데이터 보호

Applied Systems에서는 직원 2,500명 이상의 자체 호스팅 애플리케이션 및 인프라 액세스를 보호하기 위해 SASE 서비스를 채택했습니다. 기업 보안 팀은 이 새로운 접근 방식에서 제공하는 유연성을 통해, AI 도구에 데이터를 공유하는 방식을 제어하는 동시에 다양한 사용자 요구 사항을 충족할 철저한 제어 조치를 적용할 수 있게 되었습니다.

SASE 솔루션 선택:

단일 벤더 통합 vs. 다수의 포인트 솔루션

단일 벤더 SASE 공급자는 네트워크 및 보안 기능을 하나의 클라우드 제공 서비스로 통합합니다. 덕분에 기업에서는 서로 다른 포인트 제품을 통합하고 장비를 덜어내며 일관적인 정책을 시행할 수 있습니다. 멀티 벤더 SASE를 구현할 때의 결과 역시 단일 벤더 접근 방식과 비슷하지만, 복잡성과 비용이 늘어나고 내부 가시성과 유연성이 떨어지는 경우가 많습니다.

단일화된 플랫폼에서 이러한 기능을 통합하면 '총 소유 비용을 절감하고 진화하는 비즈니스 요구 사항을 충족하기 위해 쉽게 조정할 수 있게 간소화되고 효율적인 네트워크 및 보안 인프라'라는 SASE의 진정한 약속을 이행할 수 있습니다.

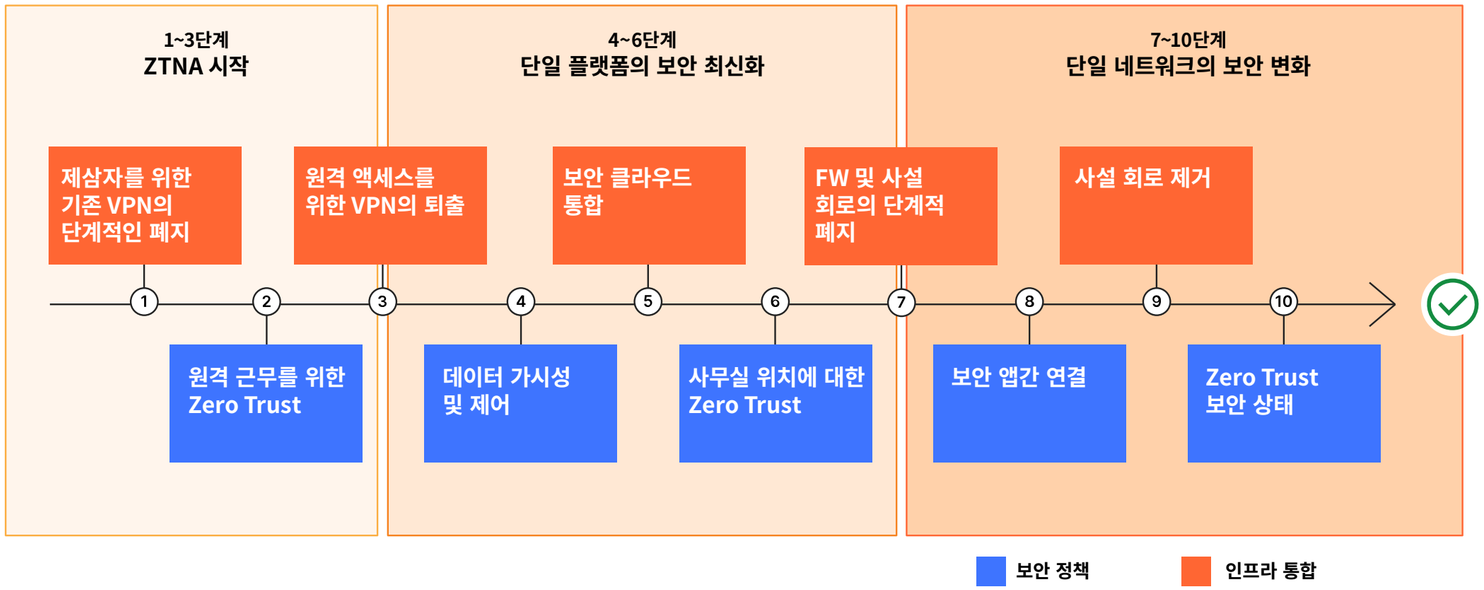
고려 중인 SASE 공급자를 평가할 때는 다음 질문을 유념하세요.

1. 위협 및 중요한 데이터 감지 엔진이 단일 경로로 애플리케이션 트래픽을 해독하고 검사하나요? 배포 시 주의 사항이 있나요?
2. SaaS 제품군을 통한 모든 데이터 흐름과 통신이 모든 채널(인라인 및 대역 외 웹 활동과 이메일 활동)에서 보호되나요?
3. 모든 사용자와 애플리케이션에 원격 브라우저 격리가 활성화되어 있나요? 이 부분은 생산성에 어떤 영향을 미칠까요? 추가 요금이 부과되나요?
4. 네트워크 온램프(on-ramp) 때문에 보안 기능이 우회되나요?
5. 다중 테넌트 클라우드 아키텍처에서 고객 트래픽을 격리하고 비공개로 유지할 수 있나요?
6. 어떤 데이터 현지화 기능을 사용할 수 있나요? 데이터 현지화를 활성화하면 현지화 지역 밖에서 연결하는 원격 사용자의 대기 시간이 늘어나나요?
7. 위협 인텔리전스 피드를 아키텍처에 통합할 수 있나요? 이 플랫폼은 위협 인텔리전스 피드의 오탐을 어떻게 줄일까요?
8. 어떤 종류의 사용자/장치 위험 점수 및 분석을 사용할 수 있나요? 위험 점수를 모든 애플리케이션에 균일하게 적용할 수 있나요?

Cloudflare의 SASE 제공 방법

많은 기업이 통합 SASE 플랫폼으로의 여정을 Cloudflare에 맡겨 완성하고 있습니다. 전체 플랫폼에 일관적으로 내장된 ID 및 컨텍스트 기반 연결을 갖춘 Zero Trust 네트워크 아키텍처로 시작할 수 있는 유일한 SASE 공급자가 바로 Cloudflare입니다.

완전한 SASE 아키텍처를 위한 장기 로드맵은 아래 예시와 유사한 흐름으로 이어질 수 있습니다.



전 세계 310여 개 도시에 걸쳐 있는 전역 네트워크를 갖춘 Cloudflare는 엔터프라이즈급 보안, 복원력, 성능을 달성하도록 CISO를 돕습니다. Cloudflare의 단일 제어판으로 여러 보안 도메인 전반의 포인트 솔루션을 통합할 수 있으므로, 조직에서는 보안 운영을 간소화하고 진화하는 위협에 일관된 보호를 보장할 수 있습니다.

웹 사이트를 방문하여 Cloudflare 및 Cloudflare SASE 플랫폼에 대해 자세히 알아보세요.

전화번호: 007-9814-2030-192
이메일: enterprise@cloudflare.com
방문: cloudflare.com/ko-kr