체크리스트

# SASE 필수 요소

## 하이브리드 근무 환경을 위한 클라우드 기반 보안

**최근 몇 년 들어서 기업에서는 멀티 엣지 네트워크 전략을 지속해서 확장하면서 새로운 재택근무 문화를 지원하고, 근로자가 클라우드 애플리케이션과 환경에서 점점 더 많은 작업을 할 수 있도록 지원하게 되었습니다. 그러나 이런 네트워크가 새로운 비즈니스 수요에 맞춰 확장되면 공격면도 증가합니다. 안타깝게도 기존 보안 솔루션 대부분은 클라우드 기반 네트워크의 혁신 속도를 따라갈 수 없습니다.**

**그로 인해 네트워크와 보안 범위 사이에 격차가 커져서 더 많은 해킹 지점에 노출되었으며, 기존 가상 사설 네트워크(VPN) 전용 솔루션을 사용해서 네트워크에 액세스하는 원격 사용자의 환경까지 영향이 미치게 됩니다. 이는 대체로 모든 애플리케이션 트래픽을 네트워크를 통해 다시 보내져 보안과 액세스 제어를 적용하기 때문입니다.**

**보안 액세스 서비스 엣지(SASE)는 이러한 문제를 해결하도록 개발되었으며, 보안과 네트워크 전략을 빠르게 융합하고 확장하도록 지원합니다. SASE를 사용하면 확장되고 있는 새로운 동적 네트워크 엣지를 안전하게 제공할 수 있으며, 네트워크 안팎의 사용자 사이에 분산된 하이브리드 근무 환경의 새로운 수요를 충족할 수 있습니다.**

**이렇게 성능을 중시하는 새로운 분산형 전략을 지원해야 오늘날 디지털 시장에서 성공할 수 있기 때문에, 파트너로 삼을 수 있는 적절한 SASE 공급업체를 선택한다면 모든 기본적 요소를 함께 운영하는 어려움을 해결하면서도 성공적으로 운영할 수 있습니다. 이론적으로 SASE는 모든 사용자에게 어디서나 안전한 클라우드 액세스를 제공합니다. 그러나 일부 SASE 솔루션은 확장성, 보안, 오케스트레이션에 저마다 차이가 있어서 구현해야 할 기술과 통합 시스템으로 운영하는 데 필요한 IT 인력 측면에서 간접비용이나 업무부하 등이 증가하게 됩니다.**

## SASE 솔루션의 가장 중요한 요구 사항 4가지

이런 문제와 이와 유사한 문제가 발생하지 않도록 하기 위해서는 SASE 솔루션을 도입할 때 4가지를 필수적으로 지켜야 합니다.

### ☑ SASE는 통합 보안 플랫폼의 일부여야 합니다.

SASE는 안전한 클라우드 기반 연결을 제공하도록 설계되었습니다. 그러나 클라우드에서만 운영되는 엔터프라이즈 네트워크는 거의 없습니다. 기업의 93% 이상이 멀티 클라우드 전략을 추구하지만,[1] 대다수가 여전히 물리적 네트워크를 보유하고 있습니다. 즉, 클라우드 전용 보안은 그 성격 자체가 불완전합니다. 데이터 센터와 다른 온프레미스 리소스를 보호해야 할 뿐만 아니라 통합 보안 전략의 일부로 정책을 배포하고 오케스트레이션해야 합니다. SASE에서 제공하는 보안 제품과 서비스는 물론이고 다른 곳에 적용한 것과 동일한 제품과 서비스를 사용해야 합니다. 그 이유로 SASE만 제공하는 공급업체 대부분은 클라우드 액세스 보안만 해결할 수 있으므로 전체적인 보안 문제를 해결하는 능력이 제한적입니다.

대신 기업에서는 광역 네트워크(WAN) 보안을 포함한 확장된 네트워크와 통합하거나, 매끄럽게 확장하여 배포할 수 있는 SASE 서비스를 강조해야 합니다. 그 결과로 구축한 통합 보안 프레임워크는 총소유비용(TCO)을 낮추고 SASE의 실질적 사용률을 개선할 수 있습니다.

## ☑ 엔터프라이즈급 보안

SASE 서비스를 평가할 때 보안 요소의 기능과 성능이 효과적이어야 합니다. 서비스형 방화벽(FWaaS) 솔루션이 상태 저장 및 프록시 프로토콜을 모두 지원할 수 있을까요? 애플리케이션과 동시에 SSL 검사를 지원하나요? 고객이 저급 기술에 만족하도록 강요하지 않고 검증과 테스트를 거친 솔루션 일체를 제공하나요? 이런 질문과 이와 유사한 질문에 답하면 SASE를 선택할 때 기업에서 요구하는 규모로 보안을 제공할 수 있습니다.

진정으로 안전한 SASE 솔루션에는 다음과 같은 보안 기능과 도구의 스택이 포함되어야 합니다.

- **서비스형 방화벽(FWaaS).** SASE 솔루션은 다음과 같은 차세대 방화벽(NGFW)을 포함해야 합니다.
  - 클라우드를 통해 우수한 성능의 SSL 검사 및 지능적 위협 탐지 기술 제공
  - 분산된 사용자를 위한 보안 연결 설정 및 유지
  - 사용자 환경에 영향을 미치지 않고 인바운드 및 아웃바운드 트래픽 분석
- **도메인 이름 시스템(DNS).** DNS는 악성 도메인을 식별하여 격리함으로써 악의적 위협이 네트워크로 들어오지 못하게 차단합니다.
- **침입 방지 시스템(IPS).** IPS를 사용하여 네트워크를 능동적으로 모니터링하고, 알려진 취약성을 익스플로잇하려는 악의적 활동을 찾아내야 합니다.
- **데이터 손실 방지(DLP).** DLP 기능은 최종 사용자가 중요한 정보를 네트워크 밖으로 옮기지 못하게 차단하고 네트워크와 데이터를 모두 보호하는 데 필요합니다.
- **보안 웹 게이트웨이(SWG).** SWG 솔루션은 내부 및 외부 위험으로부터 웹 액세스를 보호합니다. 또한, TLS 1.3을 비롯한 암호화된 트래픽에 포함된 위협까지 모든 위협을 고성능 SSL 검사로 자동 차단해야 합니다.
- **제로 트러스트 네트워크 액세스(ZTNA) 및 가상 사설 네트워크(VPN).** 엔터프라이즈급 보안을 VPN에 더하고, ZTNA를 원격 사용자에게까지 확장해야 합니다. 그러면 SASE 솔루션을 기존 VPN 솔루션과 기본적으로 통합하고 제로 트러스트 애플리케이션 액세스를 네트워크 밖의 원격 사용자에게까지 확장할 수 있습니다.
- **샌드박스.** 샌드박스를 클라우드에서 실행하든 애플리케이션에서 실행하든 지금껏 알려지지 않은 위협을 차단하는 데 중요한 보호 기능을 제공합니다.

## ☑ 타사 검증을 받은 연구 및 서비스

SASE 서비스는 통합 보안 프레임워크가 필요할 뿐만 아니라, 이를 지원하는 위협 인텔리전스가 잘 갖춰져 있어야 효과적입니다. 네트워크에 대한 경험 뿐만 아니라, 지능적인 보안 연구와 혁신을 선보인 적이 있는 SASE 공급업체를 고려해야 합니다. 이를 통해 최신 위협 방식과 기술에 맞서 지속해서 업데이트되는 세계적인 수준의 SASE 솔루션을 통해 보안을 배포하고 적용할 수 있습니다.

서비스형 기술(TaaS)을 제공하는 SASE 공급업체는 위협 인텔리전스에서부터 보호 기능에 이르는 SASE 서비스와 기능에 대해 안정적인 솔루션 유지 관리와 업그레이드를 기본으로 제공해야 합니다. 하지만 이는 시작에 불과합니다. 우수한 TaaS 서비스라면 알려진 위협과 제로 데이 위협에 대해 지능적 위협 탐지까지 포함해야 합니다. 그러므로 기업에서는 SASE 여정을 시작하기 전에 도입을 고려하는 공급업체가 위협 연구에 투자하고 있고, SASE 보안 서비스를 지속해서 개선하는지 확인해야 합니다.

## SASE 보안을 전체적 보안 전략에 통합

보안은 SASE 솔루션의 근본적이면서도 기본적인 기능입니다. 각 요소는 엔터프라이즈급 솔루션으로 운영해야 합니다. 타사 테스트 및 검증, 세계적 수준의 보안 솔루션을 제공한 경험 등을 통해 이러한 결과를 확인할 수 있습니다. 또한, 이런 요소들이 통합 SASE 솔루션과 분산된 네트워크 전체를 커버하도록 설계된 전체적 통합 보안 패브릭에서 매끄럽게 통합된 보안 전략으로 상호운용되는 것도 중요합니다.

[1] Janakiram MSV, "10 Key Takeaways From RightScale 2020 State Of The Cloud Report From Flexera," Forbes, 2020년 5월 2일.



서울특별시 강남구 영동대로 325 에스타워 14 /15층 전화: 080-559-8989 Email: kr-callcenter@fortinet.com