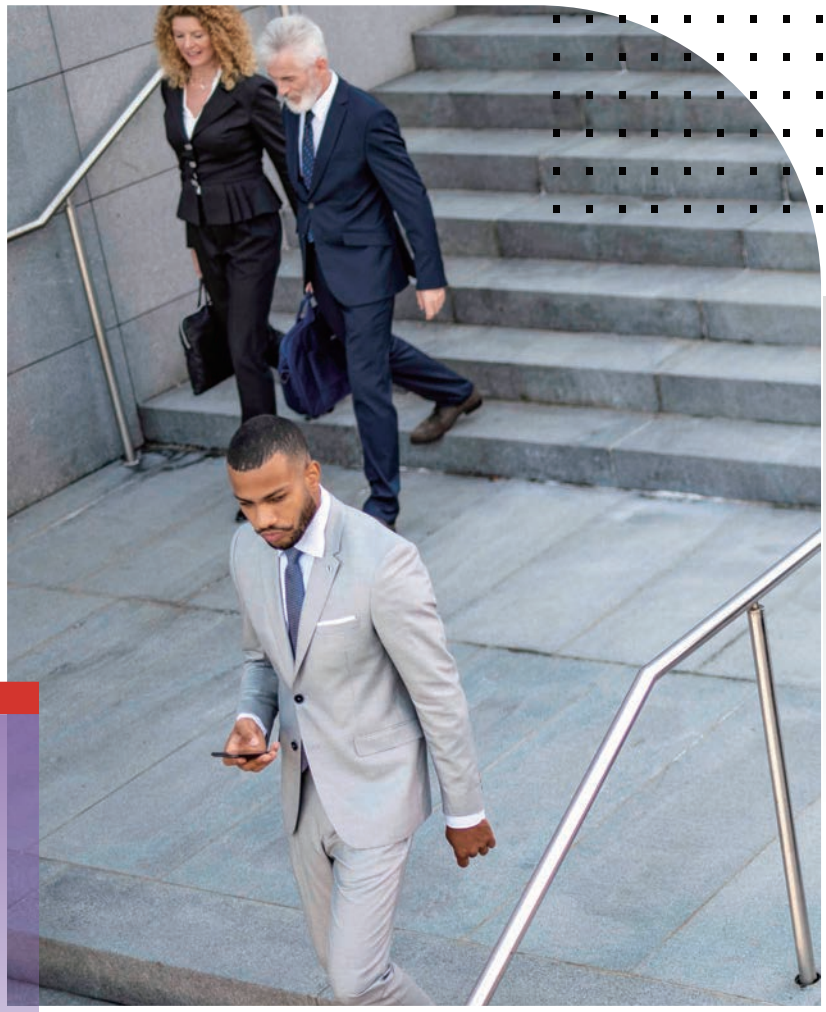
백서

SASE—모든 곳에서 어디서나 사용자에게 클라우드 기반 보안 제공



종합 요약

엔터프라이즈 네트워크에서 클라우드 기반 애플리케이션을 활용하는 사례가 늘어나고 있습니다. 클라우드 기반 애플리케이션으로 비즈니스를 운영하고, 원격 및 모바일 사용자에게 분산된 워크플로를 지원합니다. 기존 코어 네트워크나, 소규모 원격 사무실, 지점 사무실 또는 재택 근무와 같은 다른 원격 위치 엣지에서 클라우드 서비스에 액세스하고자 하는 사용자들이 빠르게 늘어나고 있어 기업에서 이를 지원하려면 기존 엔터프라이즈 네트워크를 빠르게 확장해야 했습니다.

다양한 기기와 여러 장소에서 중요한 리소스에 액세스하는 이런 하이브리드 인력으로 인해 네트워크를 새롭게 정의하였고 그 결과로 인프라팀에서는 이렇게 확장된 공격면을 관리하고 보호하기 어렵게 되었습니다. 보안 액세스 서비스 엣지(SASE) 솔루션은 네트워크 및 클라우드 기반 보안 서비스를 하나의 통합 패키지로 융합하도록 설계되어, 언제 어디서나 모든 원격 사용자가 모든 네트워크 엣지에 유연하고 안전하게 액세스하도록 지원합니다.

그러나 SASE 솔루션이 확장된 네트워크의 일부가 될 수 있어야 합니다. 클라우드 전용 솔루션은 기업이 직면한 문제의 일부만 해결할 뿐이기 때문입니다.. 즉, SASE는 융합된 대규모 통합 보안 프레임워크의 일부로 설계되어 제공되어야 합니다.

"고객들이 단순성, 확장성, 유연성, 낮은 지연, 보편적 보안을 요구하면서 하이브리드 근무 환경을 위한 보안 도구에 융합이 일어나게 되었습니다."[1]

"디지털 혁신을 지원하는 강화된 비즈니스 민첩성과 보안 원격 액세스에 대한 요구는 시큐어 액세스 서비스 엣지, 즉 SASE 모델 도입으로 이어졌습니다."[2]

SASE의 정의

SASE는 비즈니스 애플리케이션, 특히 네트워크 외부에서 일하는 경우가 많은 직원에게 클라우드 중심 업무환경을 지원하도록 설계되었습니다. SASE 솔루션은 지속해서 변환하는 환경에서 비즈니스 지속성을 보장하면서도 분산된 네트워크와 인력에게 일관적인 보안 기능을 제공함으로써 디지털 혁신을 지원합니다. 그 결과, 비즈니스 연속성이 개선되었으며 클라우드 애플리케이션에 일관적으로 안전하게 액세스하고, 사용자 경험이 향상되었습니다.

SASE는 안전하고 유연한 연결을 제공하는 것 외에도 기업이 자본 지출을 관리하고 디지털 혁신에서 발생하는 보안 인프라의 복잡성을 낮추도록 설계되었습니다. 또한, 기존의 소프트웨어 정의 광역 네트워크(SD-WAN) 솔루션으로 인해 발생한 연결성과 보안의 틈새를 WAN과 클라우드 엣지에 검증된 통합 보안을 제공함으로써 해결할 수 있습니다.

적절한 SASE 솔루션이라면 인프라 리더가 클라우드와 동일한 보안 솔루션을 제공하여 보안 인프라에 대한 기존의 투자 가치를 확장하도록 지원해야 합니다. 이를 위해서 SASE 솔루션은 모든 엣지에서 배포할 수 있는 공통적인 보안 솔루션과 광범위한 아키텍처를 기반으로 구축하고, 기존 환경을 보호하던 보안을 원격 사용자에게까지 확장하여 네트워크의 씬 엣지를 보호해야 합니다. 클라우드 기반 액세스 제어도 광범위한 액세스 전략 내에서 일관적으로 통합해야 합니다.

사람들이 일하는 환경은 네트워크 전체로 퍼져 있고, 클라우드 기반 솔루션만으로는 충분하기 어렵습니다. 일반적으로 SASE는 클라우드 기반 서비스를 용어로 설명합니다. 그러나 SASE가 실제로 효과를 발휘하려면 클라우드 기반 솔루션과 물리적 네트워크 사이의 통합을 활용하는 네트워크 환경을 지원해야 합니다. 전체적으로 일관적이고 유연한 기능을 제공하고 정책을 적용하기 위해서는 SASE 클라우드 연결 기능을 네트워크 액세스 제어, 무선 로컬 영역 네트워크(LAN) 컨트롤러, 지사 사무실의 Wi-Fi 액세스 포인트 및 네트워크의 변화하는 엣지에 배포한 다양한 보안 도구를 결합해야 합니다.

즉, 효과적인 SASE 솔루션은 기본적인 클라우드 기반 보호를 제공해야 할 뿐만 아니라, 범용 액세스, 네트워크 망분리, 규정 준수 요구사항 등과도 상호운용되어야 합니다. 클라우드 기반 보안 솔루션만으로는 물리적 네트워크에서 로컬 트래픽을 클라우드로 보내 검사하지 않고 이런 문제를 해결할 수 없기 때문입니다.

SASE 솔루션의 주요 요소

대부분 네트워크 솔루션이 원격 사용자, 사무실, 엔드포인트의 워크플로를 지원할 만큼 빠르게 발전하고 있지만, 대부분 보안 도구와 솔루션은 그 속도를 따라갈 수 없어 일관적인 보안을 제공할 수 없고 온프레미스와 원격 사용자에게 최적의 사용자 환경을 보장하지 못합니다.

일반적인 엔터프라이즈는 분산된 환경 전반에 평균 45개의 보안 솔루션을 적용하고 있습니다.[3]

예를 들어, 가상 사설 네트워크(VPN) 전용 솔루션은 사용자 인증이라는 최소한의 보호만을 제공하므로, 만약, 해킹된 사용자와 기기가 네트워크에 액세스하면 기업에서 위협 행위자의 내부망 이동과 멀웨어 위험에 노출됩니다. 마찬가지로, 해킹될 가능성이 있는 사용자가 클라우드 기반 애플리케이션에 직접 액세스하려고 시도할 때도 심각한 문제가 됩니다. 안타깝게도 엔터프라이즈 보안 관계자는 네트워크는 물론이고, 서로 완전히 분리되어 느슨하게 분산된 도구들을 사용하는 분산형 네트워크를 보호해야 합니다. 공급업체와 솔루션은 급격한 디지털 혁신으로 인해 무분별하게 확산되고, 이는 사일로화된 포인트 보안 제품을 도입하는 것으로 이어지게 됩니다.. 이로써 관리와 제어 복잡성이 한층 더해집니다.

이렇게 분산되고 분리된 솔루션을 관리하고 서로 연결하는 작업은 이미 큰 부담을 지고 있는 보안팀에게는 감당하기 어려운 일이고, 하이브리드 인력(네트워크 안팎으로 분산된 사용자)에 대해 일관적인 보안 정책을 적용하기가 불가능에 가깝습니다. 기업에서 경쟁력을 유지하려면 변화하는 위협 동향을 해결하면서도 위치와 관계없이 모든 네트워크 사용자에게 적용할 수 있는 일관적인 통합 보안 및 네트워크 정책을 사용하여 모든 엔드포인트를 보호하고 관리해야 합니다.

자격을 갖춘 공급업체 부족

개념적으로 SASE는 네트워크 안팎의 씬 엣지 사용자에게 일관적인 보안을 적용하지 못해서 발생하는 보안 문제를 해결하도록 설계되었습니다. 문제는 SASE가 온프레미스 또는 원격에서 분산된 동적 네트워크의 제어 및 보안 요구 사항을 해결하는 것을 목표로 한다는 것입니다. 그러나 SASE 공급업체 중에서 실제로 기업에 필요한 수준의 보안과 WAN 통합을 제공하기 위한 종합적 솔루션을 제공할 자격을 갖춘 곳이 거의 없습니다.

예를 들어 SASE 전용 공급업체를 사용하여 포괄적 보안 전략을 구축하려다 보면 여러 보안 공급업체에서 제공하는 이질적인 도구들을 합친 솔루션이 구축되는 경우가 많습니다. 심각한 경우에는 나머지 네트워크에 배포된 것과 다른 경우도 대부분입니다. 이런 전략은 비용이 많이 들 뿐만 아니라 어디에나 일관적인 보안을 제공하고 배포와 관리를 단순화한다는 SASE의 핵심적 의도를 부정하기까지 합니다.

이런 문제를 피하려면 SASE 솔루션을 클라우드를 통해 제공하더라도 기존 WAN 보안 기능을 확장하듯이 작동하도록 해야 합니다. WAN 엣지에 배포되고, 기본적으로 기업의 나머지 보안 프레임워크와 상호운용되도록 설계되었으며, 검증과 인증을 받은 보안 솔루션이 필요합니다. 그렇지 않으면 SASE는 오늘날 하이브리드 인력이 직면한 문제의 절반만 해결할 뿐입니다. 액세스를 제공하면서도 사용자와 서비스를 분리하고, 네트워크 전체에 보편적 가시성과 제어 기능을 제공할 수 없게 됩니다.

[1] Frank Marsala, "The Future of Network Security Is in the Cloud," Gartner, 2019년 9월 13일.
[2] Geetha Nandikotkur, "The SASE Model: What's Driving Adoption?" Data Breach Today, 2020년 8월 31일.
[3] Charlie Osborne, "The more cybersecurity tools an enterprise deploys, the less effective their defense is," ZDNet, 2020년 6월 30일.

FORTINET

www.fortinet.com/kr

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