ASTI MARKET INSIGHT 2024-291

ASTI MARKET INSIGHT

보안 아키텍처 SASE

데이터분석본부 산업시장분석연구팀 책임연구원 **이 중 연** Tel: 02-3299-6043 e-mail: jylee@kisti.re.kr

KEY FINDING

1. SASE는 광역 네트워크와 보안 서비스를 하나의 클라우드 기반 서비스로 결합한 것을 지칭하며, 기존 보안 솔루션을 사용해 사용자, 시스템, 엔드 포인트 등을 안전하게 연결하도록 한다.
2. SASE의 주요 기술로는 SD-WAN, 클라우드 접근 보안 중개, 서비스형 방화벽, 보안 웹 게이트웨이, 제로 트러스트 네트워크 접근, 데이터 유출 방지 등이 있다.
3. SASE의 세계 시장 규모는 2021년 1,288백만 달러에서 CAGR 26.4 %로 성장해 2026년 4,148백만 달러에 이를 전망이다. 국내 시장 규모는 2021년 141억 원에서 CAGR 27.8 %로 성장해 2026년 481억 원에 이를 것이다.
4. 세계 SASE 시장은 미국의 시스코, 브이엠웨어, 팔로알토네트웍스, 포티넷 등의 글로벌 IT 업체가 선점하고 있으며, 국내에서는 CMT정보통신, 모니터랩, 에스에스앤씨, 포티넷시큐리티코리아, 지니언스, 안랩 등 전문 기업이나 외국계 기업의 자회사 등이 시장에 참여하고 있다.
5. COVID-19 팬데믹 이후 변화하는 근무 환경에 따라 바뀌는 보안 요구 사항을 빠르게 반영하기 위해 SASE의 수요가 늘어나고 있으며, 이에 대응하기 위한 기술의 연구개발은 물론이고 관련 기술의 표준화 및 고도화의 필요성이 증가하고 있다.
6. 국내 SASE 업체는 작은 내수 시장 규모, 군소 업체의 난립과 외국 업체의 국내 시장 진출로 수익률이 많이 떨어지고 있으므로, 경제성과 수익성 확보를 위한 사업 영역의 다각화 및 적극적인 해외 시장 진출을 통한 시장성 확보가 필요하다.

1) 시장의 개요

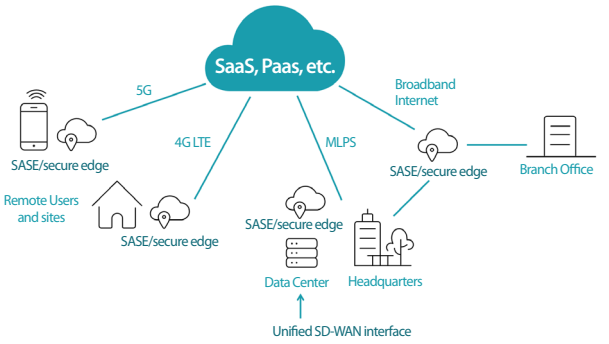
SASE(Secure Access Service Edge)는 클라우드 기반의 보안 서비스를 제공하는 새로운 보안 아키텍처로서 광역망(WAN)과 네트워크 보안 서비스를 하나의 클라우드 기반 서비스 모델로 결합한 것을 지칭한다. 2019년 마케팅 전문 기관인 가트너가 최초로 SASE란 용어를 사용했으며, 데이터 센터가 아닌 네트워크 엣지의 연결 소스에서 직접 서비스를 제공하는 것이 특징인데, 여기서 연결 소스는 사용자, 장치, 사물 인터넷(IoT), 엣지 컴퓨팅 지역 등이다.

SASE는 신기술은 아니지만 기존의 보안 솔루션을 활용해

증가하는 사용자, 시스템, 엔드 포인트, 서비스형 소프트웨어(Software-as-a-Service, SaaS) 등을 복잡도 저하나 성능 저하 없이 안전하게 활성화하는 방법과 프레임워크로서 이해할 수 있다. 사용 장소나 장치에 상관없이 악성 코드 감염, 명령 및 제어 콜백, 피싱, 무단 접근 및 허용되지 않는 사용 등 다양한 위협으로부터 사용자를 보호하기 위한 보안 전략을 포함한다.

SASE의 주요 기술로는 소프트웨어 정의 광대역망(Software-Defined Wide-Area Network), 클라우드 접근 보안 중개(Cloud Access Secure Broker), 서비스형 방화벽(Firewall-as-a-Service), 보안 웹 게이트웨이(Secure Web Gateway), 제로 트러스트 네트워크 접근(Zero Trust Network Access), 데이터 유출 방지(Data Loss Prevention) 등을 들 수 있다.

그림 1 SASE의 개념도



출처 : futuriom.com

표 1 SASE의 주요 기술

기 술	내 용
소프트웨어 정의 광대역 네트워크 (SD-WAN)	• 소프트웨어 정의 네트워크(Software-Defined Network, SDN)를 WAN까지 확장한 개념을 의미함(SDN이란 소프트웨어 프로그래밍을 통해 네트워크 경로 설정과 제어 및 복잡한 운용 관리를 편리하게 처리할 수 있는 차세대 네트워크 기술임.).
클라우드 접근 보안 중개 (CASB)	• 2012년 가트너 의해 소개된 개념으로서 사용자가 이용하는 클라우드 및 애플리케이션에 대해 가시화, 데이터 보호 및 거버넌스를 실현하는 서비스를 의미함. 클라우드 내 데이터에 대한 가시성을 확보하고, 사용자 접근 통제를 적용함으로써 사용자의 자산을 보호함.
서비스형 방화벽 (FWaaS)	• 기업의 IT 인프라를 단순화할 수 있도록 하는 클라우드 기반 방화벽 서비스임. 기업 내 하드웨어 방화벽과 유사하지만, 클라우드에 기반하므로 네트워크 크기, 구성, 수요 및 보안 요구 사항에 맞추어 즉각적인 확장이 가능하고 새로운 서비스의 제공이 용이함.
보안 웹 게이트웨이 (SWG)	• 조직의 웹 접근 관련 정책을 설정하여 외부의 웹 기반 위협으로부터 내부 시스템과 사용자를 보호하는 솔루션을 의미함. 가트너가 정의한 SWG는 최소한 URL 필터링, 악성 코드 탐지 및 필터링, 인스턴트 메시징 등 웹 기반 응용에 대한 제어를 포함함.
제로 트러스트 네트워크 접근 (ZTNA)	• 명확하게 정의된 접근 제어 정책을 기반으로 조직의 응용, 데이터, 서비스에 대한 보안 원격 접근 서비스를 제공하는 보안 솔루션임.
데이터 유출 방지 (DLP)	• 민감하거나 중요한 데이터를 인가된 사용자에게 제공하면서 승인되지 않은 무단 사용자에게는 유출되지 않도록 하는 일련의 활동 또는 솔루션을 지칭함.

출처 : 한국과학기술정보연구원 작성

2) 정책 및 규제 현황

SASE(Secure Access Service Edge)는 클라우드 기반의 보안 서비스를 제공하는 새로운 보안 아키텍처로서 기업의 주 전산 환경이 온프레미스 서버에서 클라우드로 전환되면서 새롭게 출현하였다. 기업에서 클라우드의 구축과 도입을 추진할 때 가장 큰 장애 요인은 보안 문제인데, 정보를 외부에 위탁하는 클라우드의 특성 때문에 보안에 대한 우려의 시각은 상존하고 해당 문제를 극복하기 위해 주요국은 클라우드 보안과 관련된 다양한 정책 및 규제를 시행하고 있다.

미국은 클라우드 환경의 가장 큰 장애 요인 중 하나인 보안 문제를 해결하기 위해 2012년부터 매우 까다로운 보안 인증 제도

인 FedRAMP(Federal Risk and Authorization Management Program)를 운영해 인증을 취득한 기업의 경쟁력을 높이고 있다. FedRAMP는 미 연방정부의 '정보시스템 및 개인정보 보안지침(NIST SP 800-53)'을 기반으로 인증 체계가 설계되었으며, 인증 후 지속적인 모니터링 등 사후 관리를 통해 클라우드 서비스의 보안 수준을 일정하게 유지하도록 한다. 다만, 통제 항목수가 많고 인증 절차가 복잡한 단점이 있지만, 인증을 취득할 때 높은 보안 수준을 인정받아 세계적인 경쟁력을 확보할 수 있는 장점이 있다.

영국은 정부 기관에서 이용하는 클라우드 서비스인 'G-클라우드'에 대한 안전성 확보를 위해 '클라우드 서비스 보안원칙'의 준수 여부를 인증하는 제도를 운영하는데, 해당 제도는 정보 보호 관리 체계에 대 한 국제 표준인 ISO-2700을 기반으로 클라우드 특성을 고려해 개발되었으며, 국가정보보증기술국(CESG)에서 인증을 실시한다.

일본은 정부에서 클라우드 정보 보안 관리 지침을 수립해 발표하고 민간 단체인 일본정보감사협회(JASA)에서 퍼블릭 클라우드 서비스를 대상으로 정보 보안 감사를 실시한다. 정보 보안 관리 지침은 일본 정보 보호 표준(JISQ 27001) 및 국제 표준(ISO 27001:2013)을 기반으로 클라우드 특성을 반영해 개발되었다. 또한 재단법인 멀티미디어진흥센터(FMCC)는 2008년 'ASP-SaaS 서비스 정보 공개 인증', 2012년 'IaaS-PaaS 서비스 공개 인증'과 '데이터 센터 서비스 정보 공개 인증'을 시행 중인데, 이러한 3 개 서비스 영역 인증 제도를 '클라우드 서비스 안전·신뢰성에 관한 정보 공개 인증 제도'라고 총칭해 운영하고 있다.

싱가포르는 민간 클라우드 서비스 제공자에 대한 안전성 확보를 위해 MTCS(Multi-Tier Cloud Secuirty) 인증을 도입해 운영하고 있다. MTCS는 자율 인증이지만 공공 클라우드 입찰 시 필수 요건이며, 총 취득 비용의 70 %를 정부에서 지원하고 있다. MTCS는 국제 표준 ISO 27001:27005를 바탕으로 개발되었으며, 항목별 보안 등급을 보안 수준이 낮은 서비스, 일반적으로 기업에서 요구하는 서비스, 특정 기업에서 요구하는 보안 수준이 높은 서비스 등 3 단계로 구분하고 있다.

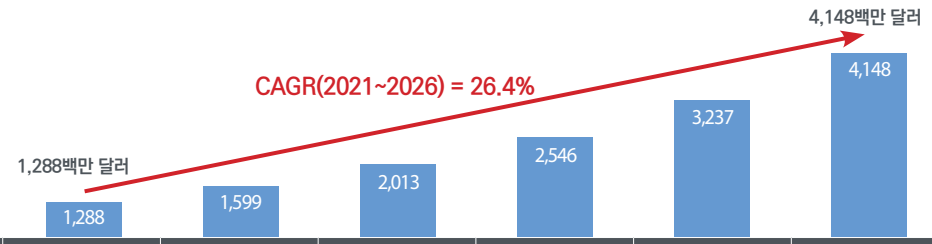
우리나라는 민간 기업이 공공 부문에 클라우드 서비스를 공급하기 위해 필요한 인증으로 '클라우드 서비스 보안인증(CSAP)'을 운영하고 있다. '클라우드 컴퓨팅 발전·이용자 보호에 관한 법률'에 따라 정보 보호 기준 준수 여부를 인증 기관인 한국인터넷진흥원(KISA)이 평가·인증한다. 공공 기관에 안전성과 신뢰성이 검증된 민간 클라우드 서비스를 공급해 이용자의 우려를 해소하고 클라우드 경쟁력을 확보한다는 취지로 2016년에 도입되었다. CSAP는 클라우드 데이터의 물리적 위치를 국내로 한정해 그동안 해외 클라우드 사업자의 국내 시장 진입을 어렵게 했다. 그러나 2023년에 CSAP를 일부 개정, 공공 클라우드의 보안 인증 체계를 시스템 중요도에 따라 상·중·하 등급으로 나누고, '하'등급의 경우 물리적 망 분리 이외에 논리적 망 분리를 허용해 해외 클라우드 사업자의 국내 시장 진출을 가능하게 하였다.

3) 시장 동향

시장 규모 및 전망

SASE의 세계 시장 규모는 2021년 1,288백만 달러에서 연평균 26.4 %로 성장해 2026년 4,148백만 달러가 될 것으로 전망된다.

표 2 SASE의 세계 시장 규모 및 전망 (단위 : 백만 달러)

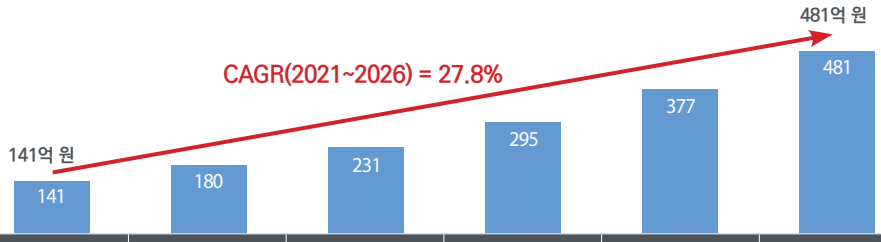


구 분	2021년	2022년(E)	2023년(E)	2024년(E)	2025년(E)	2026년(E)	CAGR(%) (2021~2026)
시장 규모	1,288	1,599	2,013	2,546	3,237	4,148	26.4
성장률(YoY)	-	24.1%	25.9%	26.5%	27.1%	28.1%	-

출처 : "Secure Access Service Edge (SASE) Market - Global Forecast to 2026", MarketsandMarkets, 2021

국내 SASE 시장은 2021년 141억 원에서 2026년까지 연평균 27.8 %로 성장해 2026년 481억 원으로 될 것으로 전망된다. 코로나를 계기로 기업의 클라우드 이전이 증가하자 안전한 원격 근무와 재택 근무의 환경을 지원하는 SASE에 대한 수요가 높아지고 있으며, 기존 보안 시장을 대체하면서 SASE 기반 클라우드 보안 시장이 지속적으로 높은 성장을 이어갈 것으로 전망된다.

표 3 SASE의 국내 시장 규모 및 전망 (단위 : 억 원)



구 분	2021년	2022년(E)	2023년(E)	2024년(E)	2025년(E)	2026년(E)	CAGR(%) (2021~2026)
시장 규모	141	180	231	295	377	481	27.8
성장률(YoY)	-	27.8%	27.8%	27.8%	27.8%	27.8%	-

출처 : "Secure Access Service Edge (SASE) Market - Global Forecast to 2026", MarketsandMarkets, 2021, "2020년 클라우드산업 실태조사 결과보고서", 과학기술정보통신부, 2020, "2021년 클라우드산업 실태조사 결과보고서", 과학기술정보통신부, 2021

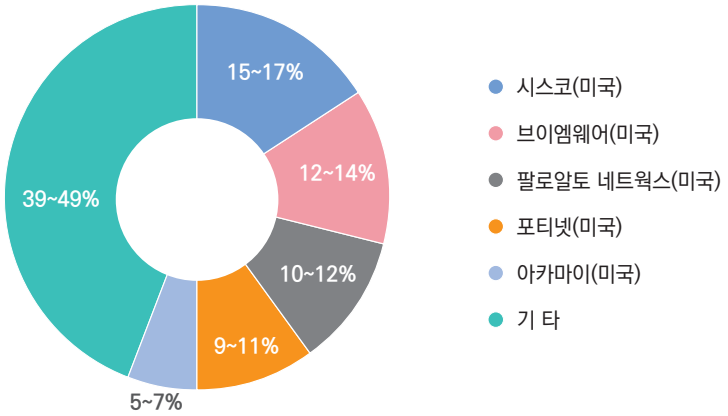
* 환율(KRW/USD): 1,144.42

경쟁 현황

해외의 주요 SASE 업체로는 시스코(Cisco), 브이엠웨어(VMware), 팔로알토네트웍스(Palo Alto Networks), 포티넷(Fortinet), 아카마이(Akamai) 등이 있다. 전 세계 SASE 시장점유율은 2020년 기준 시스코가 15~17 %로 가장 높고, 브이엠웨어 12~14 %, 팔로알토네트웍크 10~12 %, 포티넷 9~11 %, 아카마이 5~7 %, 기타 39~49 % 순으로 나타났다. 기타 업체에는 지스케일러(Zscaler), 클라우드플레어(Cloudflare), 카토네트웍스(Cato Networks), 베르사네트웍스(Versa Networks), 포스포인트(Forcepoint), 맥아피(McAfee), 브로드컴(Broadcom), 체크포인트(Check Point) 등을 들 수 있다.

국내 SASE 시장의 주요 업체로는 CMT정보통신, 모니터랩, 에스에스앤씨, 포티넷시큐리티코리아, 지니언스, 안랩 등이 있다.

그림 2 전 세계 SASE(Secure Access Service Edge) 시장의 주요 기업 시장점유율 현황(2020)



출처: "Secure Access Service Edge(SASE) Market-Global Forecast to 2026", MarketsandMarkets, 2021

표 4 해외 SASE 업체

업 체	현 황
시스코 (Cisco) (미국)	• 1984년12월에 설립된 글로벌 네트워킹 장비 제공업체임. • 동사의 SASE는 네트워킹 기능과 보안 기능을 클라우드에서 결합해 작업 위치에 관계없이 애플리케이션에 안전하게 액세스할 수 있도록 보장하는 클라우드 기반의 네트워크 인프라임. • SASE 시장에서 머라키(Meraki) 기반 시스코 SD-WAN, 시스코엄브렐라(Umbrella), 시큐어 액세스 바이 듀오(Secure Access by Duo) 등을 통합 번들로 제공하는 데 차별점을 두고 있음.
브이엠웨어 (VMware) (미국)	• 1998년에 설립된 클라우드 컴퓨팅 및 가상화 SW 제공 업체임. • 클라우드 네트워킹 및 클라우드 보안 서비스를 통합해 모든 규모의 기업을 위한 유연성, 민첩성 및 확장성을 제공하는 SASE 플랫폼을 제공함. • SASE의 구성 요소에는 소프트웨어 정의 광역 네트워크(SD-WAN), 제로 트러스트 네트워크 액세스(ZTNA), 클라우드 웹 보안(CWS), IT 운영을 위한 인공 지능(AIOps)이 포함됨.
팔로알토 네트웍스 (Palo Alto Networks) (미국)	• 2005년에 설립된 다국적 사이버 보안회사로 네트워크, 엔드포인트 보안 및 클라우드 서비스에 걸친 보안을 제공함. • 2021년 자사의 Prisma Access와 Prisma SD-WAN을 통합형 클라우드 서비스로 제공하는 신규 오퍼링 Prisma® SASE를 전 세계적으로 출시하였음.
포티넷 (Fortinet) (미국)	• 2000년에 설립된 다국적 기업으로 물리적 방화벽, 바이러스 백신 소프트웨어, 침입 방지 시스템 및 사이버 보안 솔루션을 개발 및 판매함. • 포티넷 보안 패브릭의 확장 기능으로 SASE 서비스를 제공하여 포티넷 보안 솔루션의 전체 포트폴리오를 연결하는 공통 운영 체제인 FortiOS의 성능을 어디서든 확장하고 활용함.
아카마이 (Akamai) (미국)	• 1998년8월에 설립된 분산 컴퓨팅 및 클라우드 컴퓨팅을 전문으로 하는 기업으로 세계적인 CDN(콘텐츠 전송 네트워크)을 기반으로 미디어 및 소프트웨어 전송 솔루션과 클라우드 보안 솔루션을 제공하고 있음. • 아카마이 SASE는 전 세계적으로 분산된 클라우드 네이티브 단일 플랫폼에서 통합 네트워크 및 보안 서비스를 제공함.

출처 : 한국과학기술정보연구원 작성

표 5 국내 업체 현황

업 체	현 황
CMT정보통신	• 2019년에 케이토네트웍스(Cato Networks)와 파트너 계약을 체결하고, 국내 시장에 SASE 솔루션을 공급하고 있음. • 2021년 4월 클라우드 기반 SASE 서비스를 종합건설회사이자 해외 토목 사업 분야 전문 기업 LT삼보에 공급하였으며, 이번 레퍼런스를 바탕으로 국내 시장에 SASE 솔루션 공급을 본격화한다는 계획임.
모니터랩	• 2005년에 설립된 보안 솔루션 벤더로 프록시 기술을 기반으로 한 웹 방화벽과 시큐어 웹 게이트웨이 분야에서 국내 선두 업체로 입지를 다져 왔으며, 자체 개발한 SECaaS인 AIONCLOUD 서비스를 SASE 플랫폼을 통해 글로벌 딜리버리가 가능하도록 AISASE 플랫폼을 구축하여 서비스하고 있음. • 현재 제공하고 있는 보안 서비스는 서버 사이드 보안 서비스인 WAF(Web Application Firewall)[1], WMD(Web Malware Detection)[2]와 클라이언트 사이드 보안 서비스인 SWG(Secure Web Gateway)가 있음.

1) 웹 방화벽(Web Application Firewall, WAF) : 일반적인 네트워크 방화벽(Firewall)과는 달리 웹 애플리케이션 보안에 특화되어 개발된 솔루션임.

2) 웹 멀웨어 탐지(Web Malware Detection, WMD) : 웹사이트의 악성 코드를 분석, 탐지해 주는 솔루션임.

업 체	현 황
에스에스앤씨	• 2018년3월에 설립된 정보 보호 전문 기업으로 2020년7월 글로벌 보안 전문 기업인 포스포인트(Forcepoint)의 한국지사로 선정되었음. • 포스포인트 SASE '다이내믹 엣지 프로텍션(DEP)'는 임직원의 안전한 인터넷 이용을 지원하는 '클라우드 시큐리티 게이트웨이(CSG)'와 임직원이 안전하게 업무에 접속할 수 있도록 하는 ZTNA '프라이빗 액세스(PA)'로 구성됨.
포티넷 시큐리티코리아	• 포티넷의 SASE는 시큐어 SD-WAN, SD-Branch, 제로트러스트 네트워크 액세스(ZTNA)와 함께 하이브리드 형태로 구축할 수 있음. • 시중에 나와 있는 대부분 물리적 보안 솔루션과 클라우드 기반 보안 솔루션과 완전히 통합된 서비스형 방화벽(FWaaS), ZTNA, 시큐어웹게이트웨이(SWG), 클라우드 액세스 보안 브로커(CASB) 등의 SASE 솔루션을 제공함.
지니언스	• 2005년에 설립된 통합 보안 플랫폼 기업으로 네트워크 접근 제어(NAC)[3] 기술을 기반으로, 위협 인텔리전스/클라우드 보안 시장을 개척하고 있음. • 2005년 국내 최초로 NAC를 개발하였으며, 2022년 글로벌 IT 컨설팅 및 시장 조사 기관 가트너가 최근 발표한 전 세계 엔터프라이즈 네트워크 장비 분야 TOP 5 NAC 기업에 랭크되었음. • NAC의 확장 기술인 ZTNA(Zero Trust Network Access)를 기반으로 SASE 등 차세대 정보 보안 솔루션 개발에 박차를 가하고 있음.
안랩	• 안랩은 국내 대표 보안 업체로서 V3를 비롯한 엔드포인트 보안, 네트워크 보안, 모바일 보안, 보안 관제, 보안 컨설팅, 보안 SI 사업 등 보안 제품 개발 및 서비스를 제공함. • 2022년 3월에는 클라우드 보안 전문기업 모니터랩과 투자 계약 및 MOU를 체결하며 ZTNA(Zero Trust Network Access)와 SASE(Secure Access Service Edge) 등 신사업 영역을 확장하고 있음.

출처 : 각사 사업보고서 및 홈페이지 참조, 한국과학기술정보연구원 재구성

4) 분석자 인사이트

최근 새로운 요구 사항을 충족하는 네트워크 및 보안 아키텍처의 필요성이 더욱 커지고 있다. 네트워킹 및 보안 환경은 다수의 서로 다른 포인트 솔루션에서 완전히 통합된 다기능 클라우드 제공 네트워킹 및 보안 플랫폼으로 진화하고 있는데, 특히 COVID-19 팬데믹 이후 근무 환경 및 네트워크 구조가 급변하면서 변화된 보안 요구사항을 빠르게 반영하기 위한 SASE의 수요가 늘어나고 있다. 또한 다양한 네트워크 및 보안 정책을 적용하기 위한 시나리오 학습 및 대응 방안에 대한 연구개발의 필요성 역시 높아지고 있다.

그러나 국내 SASE 솔루션 개발 수준은 매우 미흡한 상태이다. 기능적인 요구 사항만을 충족시키는 개별 솔루션보다 향후에 조금 더 보완이 필요한 상황이더라도 조직 및 개인의 안전을 보장하면서 효율적인 서비스를 제공할 수 있는 통합 솔루션의 개발이 필요하다. 또한 지능형 통합 보안 서비스 엣지 기술에 대한 연구개발을 통해 해외 시장에서 경쟁 우위를 확보하며 시장 경쟁력을 높이는 전략이 요구된다. 특히, 국내 SASE 업체는 작은 내수 시장 규모, 군소 업체의 난립과 외국 업체의 국내 시장 진출로 수익률이 많이 떨어지고 있으므로 경제성과 수익성 확보를 위한 사업 영역의 다각화 및 적극적인 해외 진출을 통한 시장성 확보가 필요하다.

한편 SASE 관련 기술의 표준화 및 고도화 필요성 역시 더욱 높아지고 있다. SASE는 신기술의 도입 보다 독립적으로 존재하는 네트워킹 및 보안 기술을 통합해 유연한 보안 기술 적용과 부하 감소를 목표로 하고 있지만, 현재는 각 벤더가 독자적인 솔루션을 제공하고 있는 상황이다. 기존의 레거시 시스템과의 상호 운용성이 부족하며, 더 나은 기능을 제공하기 위한 산업, 학계, 연구 기관의 협업 및 표준화 개발의 시급하다고 할 수 있다. ASTI

3) 네트워크 접근 제어(Network Access Control, NAC) : 단말기(PC 등)가 네트워크에 접근하기 전 보안 정책 준수 여부를 검사해 네트워크 사용을 제어하는 것

비매품/무료
95500
9 788929 416904
ISBN 978-89-294-1690-4 (PDF)