cisco The bridge to possible

# 2022 글로벌 네트워킹 트렌드 보고서

## 특별 보고서: SASE 솔루션 트렌드와 업계 현황 – NaaS(Network as a Service)의 부상

# 특별 보고서: SASE 솔루션 트렌드와 업계 현황

# 목차

# 보안 액세스 서비스 에지(SASE) 전략 수용

## 하이브리드 업무 환경에는 어디서나 일관성 있고 탁월한 사용자 경험을 제공하기 위한 통합 SASE 전략이 필요합니다.

시장에서 SASE(보안 액세스 서비스 에지)를 둘러싸고 커지는 관심을 반영하고자, 시스코는 2022 글로벌 네트워킹 트렌드 보고서: NaaS(Network as a Service)의 부상에 추가로 SASE를 위한 내용을 업데이트 했습니다.

원격 근무 및 하이브리드 클라우드 도입이 가파르게 증가하는 가운데 더욱 주목받고 있는 SASE는 모든 위치나 디바이스에서, 모든 네트워크를 통해, 모든 애플리케이션에 끊김 없이 안전한 연결을 지원합니다.

SASE는 네트워킹 및 보안 기능을 하나의 클라우드 네이티브 솔루션 또는 서비스로 통합하여 제공합니다.

기존 보안 솔루션과 달리, 갈수록 분산화되는 최종 사용자 및 애플리케이션에 더 가까운 곳에서 보안 정책을 설정하고 실행합니다. 제로 트러스트 개념을 확장하는 이 기술을 적용하면, 데이터를 데이터 센터로 계속 백홀링할 필요가 없습니다. 따라서 네트워크 로드 및 병목 현상이 크게 줄고, 더 우수한 사용자 경험이 제공됩니다.

기본 보안 스택을 대체하면서 엣지부터 엣지까지, 데이터 센터, 원격 사무실, 로밍 사용자 및 기타 영역을 포괄하는 범위에서 보안 액세스를 제공합니다.

이번 추가 특별 보고서에서는 SASE와 관련한 최신 트렌드 및 인사이트를 집중 조명합니다. 이를 위해 여러 시장 조사에서 수집한 데이터, 그리고 업계를 대표하는 애널리스트 및 전문가의 시각을 기반으로 했습니다. 네트워킹, 보안, 클라우드 전략을 수립하는 과정에서 SASE의 이점 및 효과를 올바르게 이해하는 데 이 정보가 도움이 되기를 바랍니다.

— Omri Guelfand, 시스코, 네트워크 서비스 부문 VP

---

"시장에서 SASE의 정의를 둘러싼 혼란이 여전히 사그라지지 않고 있습니다. 그러나 새로운 합의는 우리의 관점, 즉 SASE가 완전히 새로운 기술이 아니라 소프트웨어 정의 WAN(SD-WAN)과 같은 기존 네트워킹과 보안 웹 게이트웨이(SWG)와 같은 보안 기술을 하나의 클라우드 기반 보안 연결 솔루션으로 통합한 것이라는 인식과 일치합니다."

— Dell'Oro Group[1]

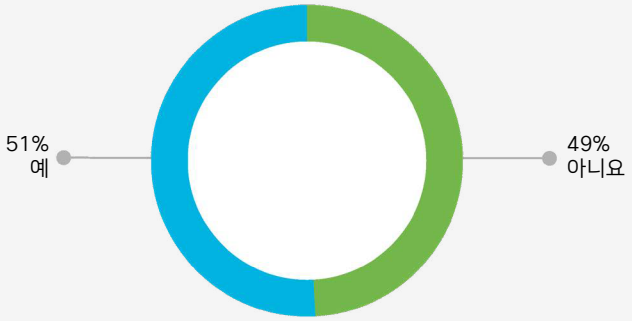
# IT의 과제: 안전한 클라우드 퍼스트 하이브리드 업무 경험 제공

오늘날 IT 팀에서 직면한 2가지 중요 트렌드는 멀티 클라우드 애플리케이션 전략으로의 지속적인 전환과 하이브리드 업무 모델의 도입일 것입니다. 사용자와 애플리케이션이 그 어느 때보다 분산화된 상황에서 이들을 연결하고 보호하는 일의 복잡성이 크게 증가했습니다.

여러 프라이빗 클라우드 및 퍼블릭 클라우드에 애플리케이션이 분산될 뿐만 아니라, 하이브리드 업무 모델에 의해 사용자 및 업무 공간도 더욱 분산화되었습니다. 이처럼 고도로 분산된 환경에서 우수한 품질의 포용적인 사용자 경험을 유지하려면, 강력한 통제가 가능했던 온프레미스 엔터프라이즈 환경과 전혀 다른 접근이 필요합니다.

**최근 설문조사에서 IT 팀의 76%는 원격 근무자를 보호하는 것이 더 어렵다고 답했으며,[2] 51%의 회사에서 지난 18개월간 직원을 회사의 리소스와 연결하는 데 각종 문제를 겪고 있다고 밝혔습니다.[3]**

귀하/귀사는 지난 18개월간 직원을 중단 없이 연결하는 데 어려움을 겪으셨습니까?




오늘날 데이터 센터 중심의 애플리케이션 모델을 인터넷 기반 클라우드 중심 모델로 전환하는 과정에서 IT 팀은 기존 네트워킹 전략을 획기적으로 개편해야 했습니다. 보안 팀 역시 사용자와 애플리케이션이 온프레미스에서 벗어나 사고에 의한 노출 또는 고의적 공격에 더 취약해지면서 안전하고 만족스러운 사용자 경험을 제공하는 데 어려움을 겪고 있습니다.

이에 클라우드 네이티브 SASE 모델이 주목받고 있습니다. 즉, SD-WAN과 같은 네트워킹 솔루션을 보안 서비스 엣지(SSE) 및 제로 트러스트 네트워크 액세스(ZTNA)와 같은 클라우드 보안 솔루션과 연계하는 방식입니다.

SASE는 사용자와 애플리케이션이 어디에 위치하고 호스팅되더라도 상관없이 확실히 연결함으로써 궁극적으로 더 유익하고 일관적이며 안전한 사용자 경험을 제공하는 것을 목적으로 합니다. 아울러 IT 비용 및 복잡성을 줄이고 네트워크 유연성 및 성능을 강화함으로써 더 발전된 애플리케이션 경험을 제공할 것을 약속합니다.

> "팬데믹이 2020년에 정점에 이르렀을 때, 미국의 직원 중에서 풀타임으로 또는 가끔씩 원격 근무하는 직원의 수가 팬데믹 이전 대비 450% 증가했습니다. 그 비율이 줄고 있으나, 장기적으로는 원격 근무 비율이 팬데믹 이전 대비 200% 수준에 안착하리라 전망합니다."
>
> — Dell'Oro Group[4]

## 결론:

인력의 분산화 및 다양화는 계속될 것입니다. 올바르게 구현된 SASE는 분산된 사용자와 애플리케이션을 연결하고 보호합니다. 네트워크 및 보안 정책을 연계하고, 네트워크 및 보안 관리의 부담과 위험을 덜어줍니다.

# SD-WAN과 SASE의 관계

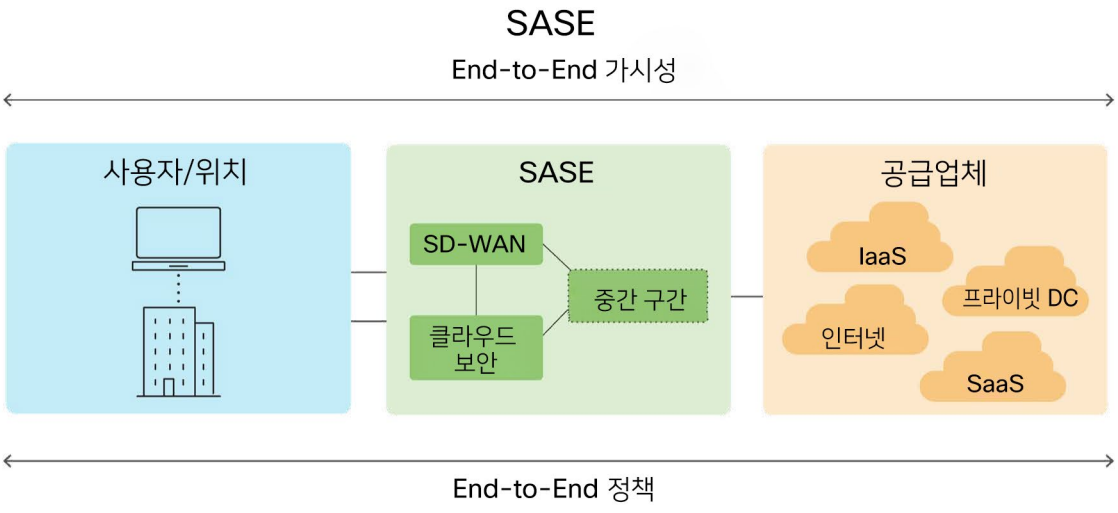
시장에서 SASE를 둘러싼 혼란이 커지면서 기존 SD-WAN 솔루션에 관해 여러 가지 의문이 제기되었습니다. SASE가 SD-WAN을 대체합니까? 이 둘은 상호 보완 관계입니까? 아니면 각기 다른 니즈를 해결하는 전혀 다른 솔루션입니까?

## 답은 간단합니다. SD-WAN은 SASE의 기초입니다.

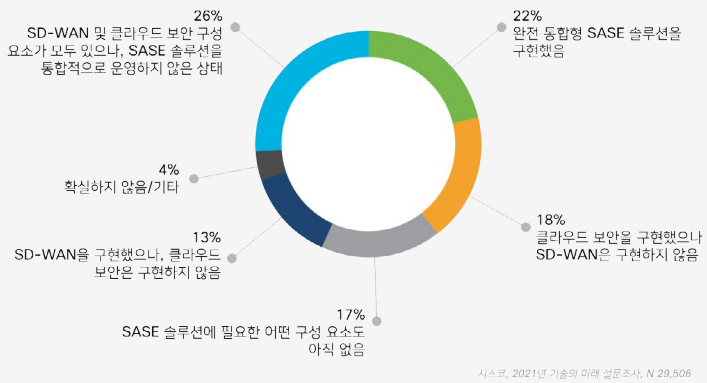
SASE는 SD-WAN의 기본 보안 기능을 클라우드 중심 보안에 접목함으로써 사용자와 애플리케이션이 어디에 위치하고 호스팅되더라도 상관없이 모두 연결하고 보호합니다. 오버레이 아키텍처인 SASE는 다음과 같은 SD-WAN의 안전 보장 기능 없이 보편적 보안을 실현할 수 없습니다.

- NAT(Network Address Translation) 활성화
- 네트워크를 여러 서브네트워크로 분할
- 악성코드/악성 트래픽 모니터링 및 차단
- 허가받지 않은 사용자 제한
- 불필요한 콘텐츠 또는 애플리케이션 차단
- 방화벽을 통해 불필요한 수신 트래픽 및 VLAN-VLAN 트래픽 차단
- Site-to-Site/터널 내 VPN 보호
- 위치 기반 액세스 제어를 위한 지오펜싱

> "SASE가 SD-WAN을 대체하지 않습니다. 오히려 SD-WAN은 SASE의 기초가 되는 구성 요소입니다. SASE 솔루션은 aaS(as-a-service) 형태로 제공되는 여러 네트워크 및 보안 기능, 즉 SD-WAN, 보안 웹 게이트웨이(SWG), 클라우드 액세스 보안 브로커(CASB), 차세대 방화벽(NGFW), 제로 트러스트 네트워크 액세스(ZTNA) 등을 통합하여 제공합니다."
>
> — 2021 Gartner®, Quick Answer: Does SASE Replace SD-WAN?[5]



귀사의 SASE 도입 과정은 현재 어느 단계입니까?




IT 조직은 SD-WAN 또는 클라우드 보안에서 시작해야 할까요? 단계적으로 SASE를 구현하는 곳이 많습니다. 대부분 SASE 여정이 진행 중입니다. 즉, SD-WAN과 클라우드 보안 구성 요소의 조합이 아직 완전한 통합 또는 운영 상태에 이르지 못했습니다.

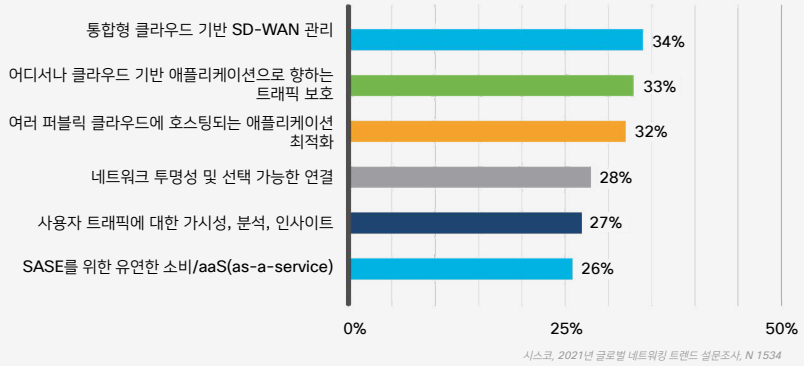
**기업의 18%가 클라우드 보안을 구현했지만 SD-WAN은 구현하지 못했습니다. 그리고 13%는 SD-WAN을 구현했지만 클라우드 보안은 구현하지 못했습니다.[6]**

결론:
SD-WAN은 SASE의 기초를 이루는 요소로서 클라우드 중심 보안 솔루션/서비스와 연계하여 온프레미스, 클라우드, 엣지 도메인 어디서나 사용자와 데이터를 보호합니다.

# 모범적인 SASE 기능

SASE가 네트워크 기능과 보안 기능의 통합을 의미하는 바, 기업의 34%는 통합형 클라우드 기반 SD-WAN 관리를 지원하는 솔루션 및 서비스에 우선순위를 두고 있습니다. 클라우드 기반 애플리케이션으로 향하는 트래픽을 보호하고(33%), 여러 퍼블릭 클라우드에 호스팅되는 애플리케이션을 최적화하고(32%), 네트워크 투명성 및 유연성을 강화하는 것 (28%)도 최우선순위로 꼽혔습니다.

귀사에서는 어떤 SASE 기능이 우선순위에 있다고 보십니까?




*시스코, 2021년 글로벌 네트워킹 트렌드 설문조사, N 1534*

## 원격 근무자를 연결하기 위해


43%는 서비스 형태의 VPN을 사용할 계획입니다.


36%는 제로 트러스트 네트워크 액세스 및 다단계 인증 기능 도입을 고려하고 있습니다.


35%는 호스트 기반 통합 클라이언트에 관심이 있습니다.


35%는 SD-WAN을 모바일 사용자 및 재택 사용자에게 확장할 방법을 모색하는 중입니다.

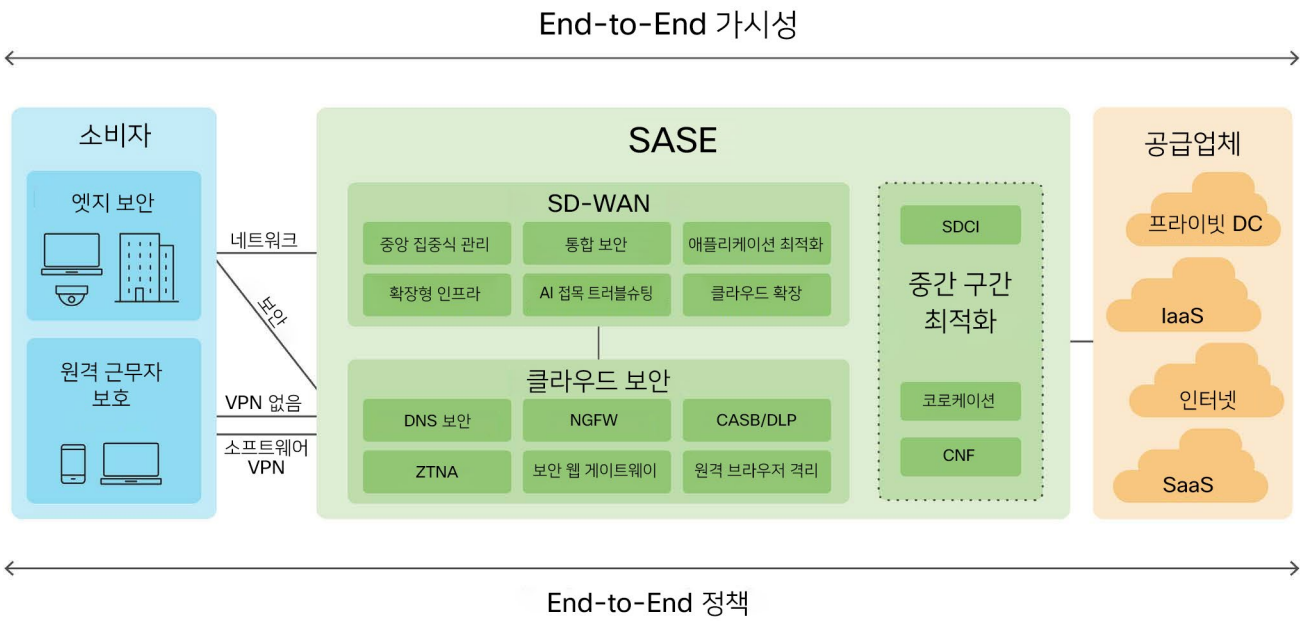
SASE 아키텍처, 솔루션, 서비스가 계속 발전하고 있으나, 그 근본적인 목적은 SD-WAN 및 클라우드 보안의 핵심 기능 일부 또는 전체를 통합하여 제공하는 데 있습니다.

| SD-WAN | 클라우드 보안 |
|---|---|
| **중앙 집중식 관리**<br>고도로 시각적인 중앙 집중식 대시보드에서 디바이스 구성, 네트워크 관리, 모니터링, 자동화를 지원합니다. 네트워크 엣지에서의 제로 터치 프로비저닝을 포함합니다. | **제로 트러스트 네트워크 액세스(ZTNA)**<br>무단 액세스를 방지하고 보안 위반을 억제하고 공격자의 네트워크 전반 측면 이동을 최소화하는 보안 프레임워크입니다. ZTNA를 강력한 ID 및 액세스 관리(IAM)와 연계하여 사용자의 ID를 검증하고 디바이스에 대한 트러스트를 설정한 다음 승인된 애플리케이션에 대한 액세스 권한을 부여해야 합니다. |
| **클라우드 네트워크 확장 및 중간 구간 최적화**<br>포괄적인 클라우드 온램프(on-ramp) 통합으로 어떤 사이트-클라우드 및 사이트-사이트 구성에서도 원활한 자동 연결을 실현합니다. 소프트웨어 정의 클라우드 인터커넥트(SDCI) 및 코로케이션 통합을 통한 최적화된 중간 구간 연결을 포함합니다. | **보안 웹 게이트웨이(SWG)**<br>웹 트래픽을 기록하고 검사하여 완전한 가시성과 URL 필터링을 제공할 뿐만 아니라 애플리케이션을 제어하고 악성코드로부터 보호하는 게이트웨이입니다. |
| **애플리케이션 경험**<br>웹 애플리케이션의 사용 편의성 및 성능을 모니터링하고 검증하는 기능입니다. 세부적인 메트릭 및 워터폴 화면에서 웹 구성 요소의 순차적 가져오기 및 로딩 프로세스를 보여주면서 오류 및 병목 현상을 식별하고 애플리케이션 성능에 미칠 영향을 파악합니다. | **침입 방지 시스템(IPS)을 갖춘 클라우드 기반 방화벽**<br>네트워크 트래픽 관리 및 검사를 지원하는 소프트웨어 기반, 클라우드 구축형 서비스 |
| **유연한 확장형 인프라**<br>다양한 물리적 플랫폼 및 가상 플랫폼에서 우수한 가용성과 처리량, 기가비트 단위의 포트 옵션, 5G 셀룰러 링크, 강력한 암호화 기능까지 제공합니다. 서비스 레벨 요구 사항에 부합하는 가장 효율적인 WAN 링크를 탄력적으로 선택하면서 WAN 트래픽을 최적화합니다. | **클라우드 액세스 보안 브로커(CASB)**<br>네트워크의 전 범위에서 사용 중인 클라우드 애플리케이션을 감지하여 보고하고, 섀도우 IT를 찾아내고, 게시물 및 업로드와 같은 위험한 SaaS 앱 및 특정 작업의 차단을 가능하게 하는 소프트웨어입니다. |
| **AI 접목 트러블슈팅**<br>강력한 AI/ML을 활용하여 네트워크 성능을 최적화하고, 일상적인 수작업을 자동화하고, 트러블슈팅의 속도를 높입니다. 지능형 알림, 셀프 문제 해결, 예측 기반 인터넷 재라우팅 기능을 제공합니다. | **데이터 손실 방지(DLP)**<br>인라인에서 데이터를 분석하는 소프트웨어를 통해 회사의 네트워크 또는 클라우드 이상의 범위로 송수신되는 민감한 데이터를 모니터링하고 제어합니다. |
| **통합 보안**<br>강력한 보안 기능을 클라우드 보안과 연계하면서 브랜치, 재택 사용자, 클라우드 기반 애플리케이션을 침투 위험으로부터 보호합니다. | **원격 브라우저 격리(RBI)**<br>웹 트래픽을 사용자 디바이스와 격리하는 소프트웨어가 브라우저를 통해 유입되는 위협으로 인한 위험을 최소화합니다. |
| **ID 기반 정책 관리**<br>여러 위치와 도메인을 포괄하는 마이크로세그멘테이션 및 ID 기반 정책 관리를 수행합니다. | **DNS 레이어 보안**<br>IP 주소와 연결되기 전에 악의적인 DNS 요청을 차단하여 인터넷 위협으로부터 보호하는 1차 방어선의 역할을 하는 소프트웨어입니다. 강력한 DNS 보안으로 보안 팀이 매일 분류해야 하는 위협 건수를 대폭 줄일 수 있습니다. |
| **차원 높은 인사이트**<br>포괄적인 홉(hop) 단위 분석으로 애플리케이션, 인터넷, 클라우드, SaaS 환경에 대한 가시성을 강화합니다. 오류가 생긴 도메인의 격리를 가능하게 하고, 실행 가능한 인사이트를 제공하여 트러블슈팅에 속도를 내고 사용자에 미칠 영향을 최소화하거나 차단합니다. | **위협 인텔리전스**<br>위협 연구진, 엔지니어, 데이터 사이언티스트 팀에서 텔레메트리 및 첨단 시스템을 사용하여 정화하고 신속하게 실행 가능한 위협 인텔리전스를 생성합니다. 이를 바탕으로 보안 스택에 포함된 툴을 지원하는 규칙 세트를 적용하여 최신 위협을 식별하고, 새로운 취약점을 발견하고, 통제되지 않는 위협의 확산을 방지합니다. |

SASE 모델은 SD-WAN 기능과 클라우드 보안 기능을 통합할 뿐만 아니라 운영 사일로화를 해소하고 네트워크 팀과 보안 팀의 더 큰 시너지를 실현하는 데에도 기여합니다. 모든 보안 구성 요소와 네트워킹 구성 요소를 포괄하여 표준화된 정책, 공유 텔레메트리, 통합 알림 기능을 적용하는 SASE 덕분에 네트워크 운영 팀과 보안 운영 팀이 IT의 효율성 및 가시성을 제고하고 더 효과적으로 보호할 수 있습니다.

이러한 관점에서 각 기업은 포괄적인 SASE 전략, 즉 네트워크 운영 목표와 보안 운영 목표를 모두 수용하고, 운영의 협업을 확대하고, 가까운 미래의 니즈를 뒷받침할 전략을 수립해야 합니다.

## SASE: 정밀 탐구




"(2020년 기준 5% 미만에 불과했던) 클라우드 기반 보안 웹 게이트웨이(SWG), 클라우드 액세스 보안 브로커(CASB), 제로 트러스트 네트워크 액세스(ZTNA), 브랜치 오피스 FWaaS(firewall-as-a-service) 기능을 같은 벤더에서 도입하는 기업의 비율이 2024년에는 30%에 이를 것입니다."

— Gartner[7]

### 결론:

SASE 전략 및 솔루션을 평가하는 기업에서는 현재와 미래의 변화하는 니즈를 해결하고자 SD-WAN □ 클라우드 보안의 기초 기능을 제공하는 솔루션/서비스를 찾고 있습니다.

# 통합의 중요성

현대의 기업은 다양한 네트워크 환경(데이터 센터 네트워크, LAN, WAN)과 보안 솔루션(온프레미스/클라우드 기반 시스템을 위한 방화벽, 게이트웨이, 액세스 제어)을 사용합니다. SASE는 기술 및 서비스 통합으로 이 모든 영역을 포괄하는 가시성, 정책 오케스트레이션, 보호를 제공할 수 있습니다.

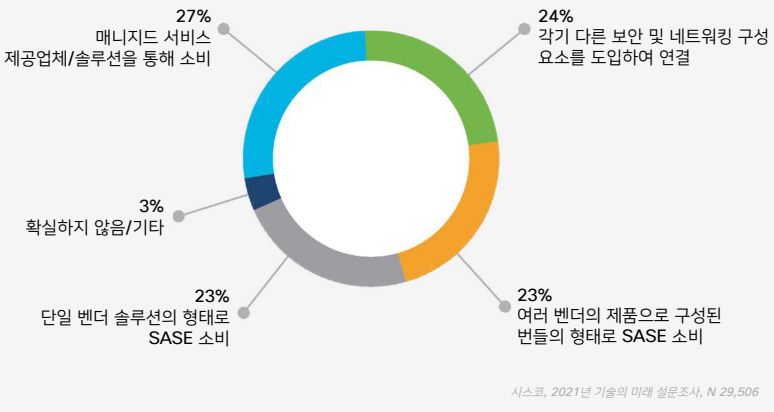
사용자와 애플리케이션이 어디에 위치하고 호스팅되더라도 상관없이 안전하게 연결한다는 궁극적인 목표를 가진 이러한 통합은 다음과 같은 이점도 제공합니다.

- 보안 사고의 규모 감축
- 트러블슈팅 및 문제 해결 속도 향상
- 시스템 모니터링 및 관리 간소화
- 정책 표준화 및 시행 강화
- 지역별 컴플라이언스 및 데이터 요건 이행
- CapEx 및 OpEx 절감

"상용화된 SASE 구현 방식은 크게 2가지로 나눌 수 있습니다. 통합형(unified)과 세분화형(disaggregated)입니다. 통합형 구현은 단일 벤더가 제공하는, 강력하게 통합된 SASE 플랫폼으로 구성됩니다. 세분화형 구현은 다양한 벤더 또는 다양한 제품을 구현하는 방식으로, 통합형보다 통합의 정도가 더 낮습니다."

— Dell'Oro Group[9]

귀사의 SASE 솔루션은 어떻게 구축하고 운영하시겠습니까?



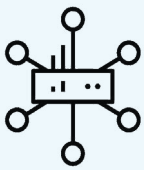

*시스코, 2021년 기술의 미래 설문조사, N 29,506*

단일 벤더 및 멀티 벤더 솔루션/서비스가 등장하고 다수의 포인트 솔루션을 조합하는 맞춤형 아키텍처도 가능해진 만큼, SASE 구축 및 운영 방식에는 다양한 옵션이 있습니다.

맞춤형 솔루션을 구현하고 통합하거나 멀티 벤더 SASE 번들을 운영하는 과정에서 불필요한 복잡성, 운영 관련 과제, 보안 취약점을 수반할 수 있으므로, 단일 벤더의 단일 통합형 및/또는 관리형 솔루션을 찾는 곳이 많습니다(50%).

- 70%는 멀티 벤더 네트워킹 및 보안 스택을 효과적으로 관리하는 것이 갈수록 복잡해지고 있다는 데 동의하거나 크게 동의합니다.
- 26%는 클라우드 보안 및 SD-WAN 기능을 모두 갖추었지만, 완전한 SASE 모델로 통합하고 운영하는 수준에는 이르지 못했습니다.[10]

맞춤형 아키텍처, 멀티 벤더 번들, 단일 벤더의 완전 관리형 서비스 또는 그 변형된 형태 등 무엇이든 간에 모든 SASE 솔루션은 다음 요소를 더 긴밀히 연계하고 통합해야 합니다.



### SD-WAN과 클라우드 보안

- SD-WAN 디바이스와 클라우드 보안 PoP(point of presence) 간의 트래픽 라우팅 자동화
- 성능 문제가 있을 경우, 대체 PoP로 트래픽을 자동 재라우팅하여 탄력성 확보
- AI를 활용하는 예측 분석으로, 사용자 경험에 영향을 미치기 전에 대체 PoP로 트래픽 자동 재라우팅

### 네트워크 운영(NetOps) 및 보안 운영(SecOps) 팀

- SD-WAN 구현과 클라우드 보안 구현 간에 보안 정책(예: 액세스 승인 및 세그멘테이션) 상시 공유 가능
- SD-WAN 플랫폼과 클라우드 보안 관리 플랫폼 간의 데이터 교환을 가능하게 하여 정책 및 이벤트에 관한 일관성 있는 가시성 제공
- 엔터프라이즈 네트워크 구성 요소(예: VPN, 보안 그룹 태그)와 정책을 클라우드 보안 플랫폼으로 확장 및 전환
- SD-WAN 및 클라우드 보안 관리 플랫폼의 전 범위에 SSO(Single Sign-On) 관리 인증 적용

### 최종 사용자와 애플리케이션

- SD-WAN, 중간 구간(예: SDCI), 멀티 클라우드, SaaS 서비스 간의 직접 연결 활성화
- SD-WAN, 클라우드 보안 PoP, IaaS/SaaS 연결을 포괄하는 통합 가시성 및 분석 기능으로 사용자 경험 모니터링 및 최적화

"보안을 통합하지 않고는 네트워킹을 제대로 구현할 수 없습니다. 엔드포인트부터 네트워크 및 애플리케이션에 이르는 전 범위에서 거시적 관점으로 보안에 접근해야 합니다. NaaS(network-as-a-service)에서는 네트워크와 보안을 책임지고 해결하는 제공업체가 필요합니다. 만약 NaaS 벤더가 네트워크만 책임진다면, 완전한 보호 및 신속한 위협 제거에 필요한 가시성 및 제어 기능을 확보해야 합니다. 제공업체가 네트워킹과 보안을 모두 맡는 것이 이상적입니다."

— 글로벌 소비재 회사, IT 인프라 책임자

## 결론:

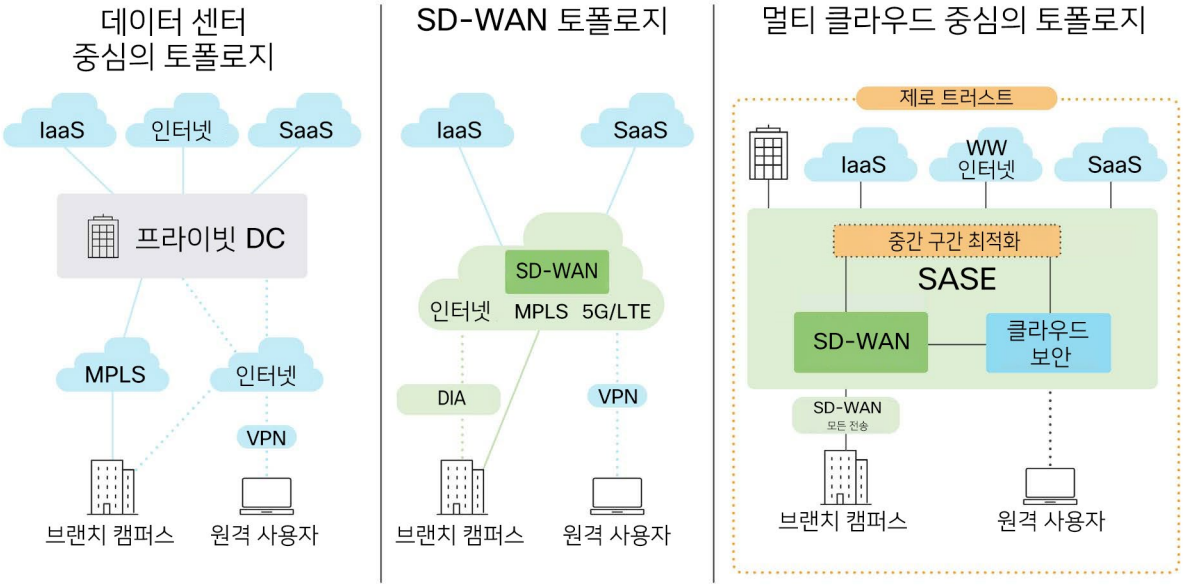
맞춤형이든 하나 이상의 벤더가 제공하는 형태이든 간에, SASE 솔루션 및 서비스는 SD-WAN과 클라우드 보안 시스템 간의 긴밀한 통합으로 안전한 사용자 경험을 최적화하고 NetOps/SecOps 협업의 시너지를 높여야 합니다.

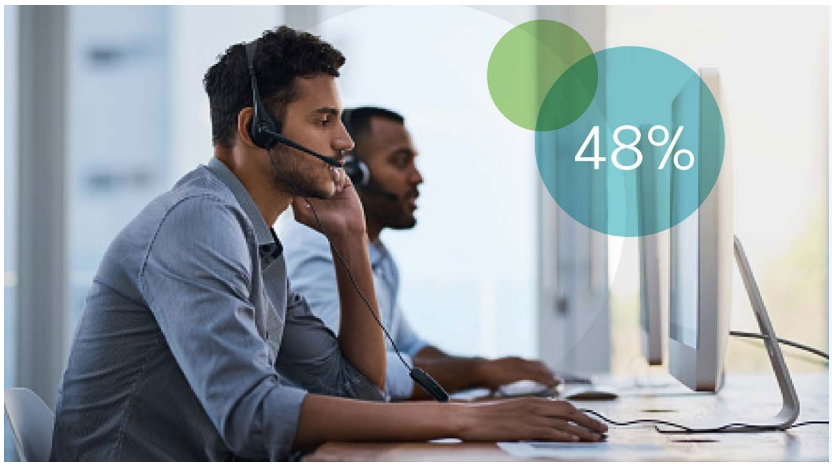
# SASE 도입 트렌드

여느 기술 결정과 마찬가지로, 각 조직에 적합한 SASE 모델 및 구축 방식은 저마다 다릅니다. 어떤 SASE 결정에서든, 기존 네트워크 및 보안 솔루션, 그리고 종합적인 운영 전략 및 비즈니스 우선순위를 염두에 두어야 합니다. 주요 이니셔티브, 규제 관련 요건, 인수 합병, 공급망 운영, 비즈니스 탄력성 요구 사항도 고려해야 합니다.

데이터 센터 중심의 애플리케이션 모델에서 클라우드 또는 멀티 클라우드 중심의 모델로 바꾸는 조직의 경우, 이를테면 SD-WAN으로 시작한 다음 중간 구간 최적화 및 클라우드 보안 통합을 전개하는 방식으로 SASE 여정을 진행할 수도 있습니다.

## DC 중심이 아닌 멀티 클라우드 중심의 토폴로지

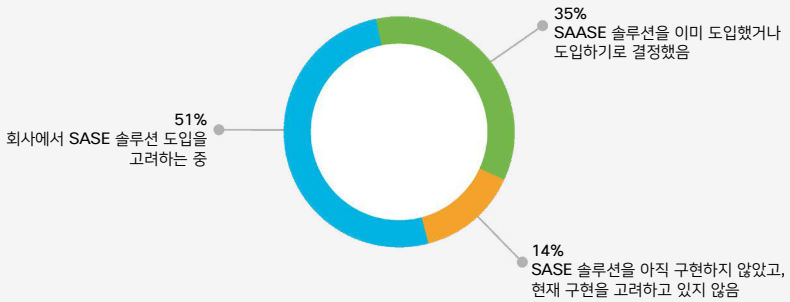



SASE에 관심 있는 기업의 48%는 보안으로, 31%는 네트워크로 시작할 것입니다. 그리고 21%는 보안과 네트워킹을 동시에 다룰 계획입니다.[8]

구체적 모델 또는 구축 방식이 무엇이든 간에, 많은 기업은 SASE 도입이 순조롭게 진행 중이라고 밝힙니다. 86%는 SASE 도입을 고려하는 중이거나 이미 도입한 상태입니다.[11]

귀사는 SASE 솔루션을 도입했거나, 도입하기로 결정했거나, 도입을 고려하는 중입니까?




*시스코, 2021년 기술의 미래 설문조사, N 34,351*

"(2020년에는 10%에 불과한) 사용자, 브랜치, 엣지 액세스까지 포괄하는 SASE 도입을 위해 명시적 전략과 일정을 수립하는 기업이 2025년에는 60%를 넘어설 것입니다."

— Gartner[12]

## 결론:

SASE 구축 방식은 기존 인프라의 라이프사이클, 운영 우선순위, 비즈니스 이니셔티브의 영향을 받습니다. IT 팀은 완전한 SASE 아키텍처를 목표로 점진적으로 구현하는 전략적 계획 접근 방식을 채택해야 합니다.

# SASE 소비 모델

SASE 솔루션 및 서비스에는 3가지 기본 소비 모델이 있습니다. 이 소비 모델이 내부 팀 및 운영에 미치는 영향은 저마다 다르지만, 모두 기존 네트워킹 및 보안 사일로를 해체한다는 공통점이 있습니다. 그에 따라, SASE는 운영의 협업 및 효율을 높이는 기폭제가 될 수 있습니다.

## aaS(as-a-service)

빠르게 구축하고 운영 및 직원에 미칠 영향을 최소화하고 SLA 관련 위험을 줄이고자 한다면, aaS(as-a-service) 형태의 SASE에서 단일 대시보드를 통해 다양한 완전 통합형 클라우드 기반 기능을 이용하고 라이프사이클 전 범위의 지원도 누릴 수 있습니다. 26%의 기업이 aaS(as-a-service) 형태의 SASE를 선호하는 소비 모델로 꼽습니다.

## 하이브리드 또는 공동 관리형

아직 본격적인 aaS(as-a-service) 모델에 준비되지 않았거나 이러한 서비스보다 더 높은 수준의 맞춤 구성을 원하는 곳이라면, 하이브리드 접근 방식을 적용할 수 있습니다. 이는 클라우드 기반 보안 기능을 기존 SD-WAN 솔루션과 통합하거나, 매니지드 서비스 제공업체와 네트워 및 보안 책임을 공유하는 것을 의미합니다. 이러한 하이브리드 방식으로 보안 및 지원을 한층 더 강화할 수 있습니다. 그리고 IT 팀에서 상시 모니터링하고 제어하면서 전반적인 라이프사이클 관리의 요구 사항을 줄이는 것이 가능해집니다.

## 고도의 맞춤 구성 또는 DIY

네트워크 및 보안 환경을 완전히 맞춤 구성하고 제어하길 원하는 곳이라면, 직접 SASE 기능을 구현, 통합, 관리할 수 있습니다. 이처럼 고도의 맞춤 구성 및 제어가 이루어지려면, 속도 및 민첩성이 떨어지는 것이 일반적입니다. 게다가 하드웨어, 소프트웨어, 라이센스에 대한 추가적인 라이프사이클 관리가 필요합니다. 보안 및 컴플라이언스 전문가도 따로 두어야 합니다. 매우 전문적인 요구 사항을 해결해야 하고 SASE의 아키텍처/운영 요구 사항을 해결할 만한 네트워크 및 인력이 있는 곳이라면, 좋은 선택이 될 것입니다.

실제 경험에서 얻은 교훈을 시스코 보안 액세스 서비스 에지(SASE) 구축 고객 사례에서 확인하십시오.

## 결론:

다양한 SASE 소비 모델이 있고, 각 모델이 운영에 미치는 영향은 저마다 다릅니다. 각 조직에 적합한 모델은 다양한 요인, 이를테면 내부 IT 팀의 규모, 기술력, 가용 시간/재원 그리고 전문적인 니즈, 속도, 민첩성, 가시성, 통제의 우선순위에 의해 결정됩니다.

# SASE 결론

SASE 아키텍처, 솔루션, 서비스는 사용자와 애플리케이션이 어디에 위치하거나 호스팅되는지에 상관없이 모두 안전하게 연결합니다. 그러나 SASE를 향한 여정은 조직에 따라 각기 다르게 전개될 것입니다. 적합한 모델 및 접근 방식은 기존 기술 투자, 그리고 IT 및 비즈니스 우선순위에 좌우됩니다.

시스코와 시스코 파트너 에코시스템은 업계 최고의 완성도, 유연성, 탄력성을 자랑하는 SASE 솔루션으로 고객의 특별한 네트워크 및 보안 요구 사항 해결을 지원합니다.

동급 최고의 네트워킹, 클라이언트 연결, 보안, 고유한 인터넷 가시성을 결합하여 폭넓은 선택지로 제공하는 시스코 SASE 포트폴리오를 통해 필요한 성과를 달성하실 수 있습니다. 아울러 각종 상황 및 요구 사항에 부합하는, 간단하면서도 유연한 여러 SASE 구축 및 소비 모델 중에서 선택할 수 있습니다.

가용성이 뛰어난 시스코의 글로벌 클라우드 보안 인프라는 사용자 및 애플리케이션이 어디에 있더라도 안전한 액세스를 제공합니다. 그리고 업계 최고 수준의 시스코 SD-WAN 솔루션은 사용자에게 우수한 품질의 경험을 안정적으로 선사하는 데 필요한 민첩성과 기능을 제공합니다. 시스코 클라우드 보안 솔루션과 SD-WAN 솔루션의 시너지로, 업계에서 가장 완전하고 특별한 통합 SASE 기능이 구현됩니다.

앞으로도 시스코는 지속적인 통합 및 기능 향상을 통해 SASE 중심의 혁신에 더욱 속도를 낼 것입니다. 날로 발전하는 시스코 솔루션과 함께, 가장 유연하고 간편한 SASE 서비스를 필요한 조건에 맞게 이용하십시오.

Cisco SASE 리소스 센터에서 더 자세히 알아보시기 바랍니다.

시스코는 Gartner Magic Quadrant™, WAN 엣지 인프라 부문에서 실행 능력과 비전의 완전성을 인정받아 리더 그룹에 선정되었습니다.[13]

## 추가 리소스 및 지원

SASE 로드맵 링크 >

시스코 파트너 찾기 >

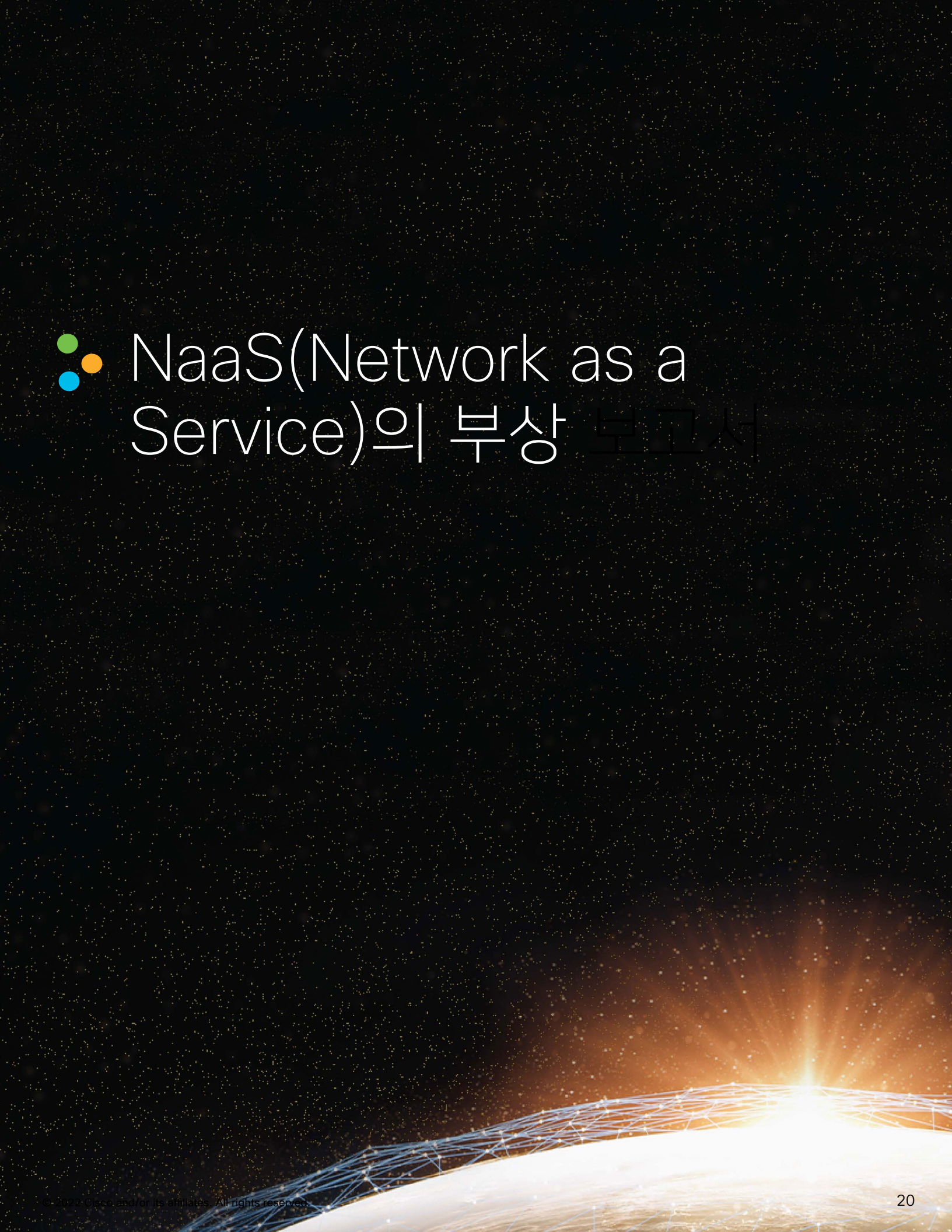
시스코 세일즈 팀에 문의 >



### SASE 자료 출처

1. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, 2021년 9월.
2. The State of Security 2021, Splunk, 2021년 2월.
3. Future of Technology, Cisco, 2021년 11월.
4. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, 2021년 9월.
5. Gartner Quick Answer: Does SASE Replace SD-WAN?, Andrew Lerner, Neil MacDonald, 2021년 12월.
6. 2022 Cisco Global Networking Trends Report: The Rise of Network as a Service, Cisco, 2021년 10월.
7. Gartner 2021 Strategic Roadmap for SASE Convergence, 2021년 3월.
8. SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG Research Report, 2021년 12월.
9. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, 2021년 9월.
10. 2022 Cisco Global Networking Trends Report: The Rise of Network as a Service, Cisco, 2021년 10월.
11. Future of Technology, Cisco, 2021년 11월.
12. 2021 Strategic Roadmap for SASE Convergence, Gartner, 2021년 3월.
13. Gartner Magic Quadrant for WAN Edge Infrastructure, 2021년 9월.

# NaaS(Network as a Service)의 부상 보고서



# 목차

# 환영

## *2022년 글로벌 네트워킹 트렌드 보고서: NaaS(Network as a Service)의 부상*에 오신 것을 환영합니다.

우리는 현재 평범한 자연인으로서도, 그리고 네트워크 전문가로서도 놀라운 시기를 경험하고 있습니다. 지난 한 해 동안 IT 리더와 네트워크 전문가는 원격 근무자를 지원하고, 더욱 분산된 컴퓨팅 환경 전체의 데이터를 보호하며, 사용자, 고객, 파트너를 위한 새로운 서비스를 제공하는 임무를 맡아왔습니다. 많은 기업에서는 이러한 새로운 요구 사항을 충족하기 위해 유연성, 민첩성, 속도 향상을 지원하는 클라우드 및 SaaS(Software as a service)를 활용하여 디지털 혁신을 서두르고 있습니다.

2021년 글로벌 네트워킹 트렌드 보고서에서는 네트워크 기술을 사용하여 상황에 상관없이 비즈니스 탄력성을 개선하는 방법에 중점을 두었습니다.

올해의 보고서에서는 미래에 큰 영향을 미칠 새로운 트렌드인 NaaS(Network as a Service)에 초점을 맞춥니다.

SaaS 및 IaaS(Infrastructure as a Service) 등 점점 더 인기가 높아지고 있는 aaS(as-a-service) 모델에 이어, NaaS는 많은 기업이 네트워킹 기능을 습득하고, 제공하고, 관리하는 방법을 변화시킬 것입니다. 이를 자세히 알아보기 위해 IT 리더 20명과 대화를 나눈 후 13개국의 IT 전문가 1,534명을 대상으로 NaaS에 대한 인식은 어떤지, NaaS의 강점 및 제약은 무엇인지, 새로운 네트워크 사용량 기반 모델을 도입할 계획이 있는지에 대한 설문을 실시했습니다.

이 보고서의 데이터, 견해, 조언이 여러분이 네트워킹 전략을 발전시키는 과정에서 NaaS의 이점과 영향을 보다 잘 이해하는 데 도움이 되기를 바랍니다.

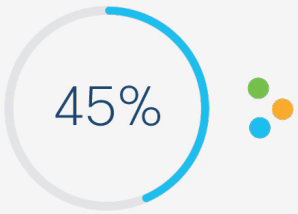
— 시스코 SVP 네트워크 서비스, James Mobley

# 주요 조사 결과

네트워크를 사용하고 운영하는 방식을 완전히 전환하는 것은 사소한 일이 아닙니다. 이를 as-a-service 모델로 전환하려면 합당한 비즈니스상의 근거와 기술적인 근거가 있어야 합니다. 또한 조직을 원활한 상태로 유지하려면 안심하고 신뢰할 수 있는 파트너가 필요합니다. 그럼에도 불구하고 많은 조직에서는 혁신을 실현하는 데 매우 의욕적인 상태입니다. 다음은 2022년 NaaS 조사를 통해 얻은 몇 가지 주요 조사 결과입니다.

## 주요 조사 결과 1: 당면 과제

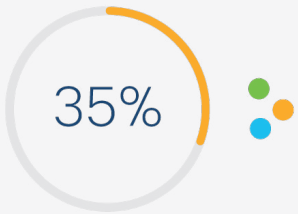
탄력성 및 민첩성이 문제라면 대부분의 경우 NaaS가 답입니다.




- 중단에 대한 대응(45%) 및 새로운 비즈니스 요구 사항 수용(40%)이 2021년의 가장 큰 네트워크 당면 과제로 꼽혔습니다.
- 그와 동시에, IT 팀은 NaaS의 중요한 이점을 IT 팀의 업무 부담을 줄여 혁신 및 비즈니스 가치를 제공할 수 있도록 지원하는 것으로 생각하고 있습니다(46%). 응답자의 나머지 40%는 NaaS가 중단에 대한 대응을 개선하며, 34%는 네트워크 민첩성을 향상하는 것으로 생각하고 있습니다.

## 주요 조사 결과 2: 이점

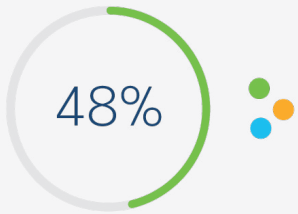
최신 기술을 빠르게 사용할 수 있다는 점이 가장 큰 기대 사항이자 이점입니다.




- 기술은 조직이 이를 도입할 수 있는 속도보다 훨씬 더 빠르게 발전하고 있습니다. 응답자의 35%는 Wi-Fi 6, SD-WAN(Software-Defined WAN), 보안 액세스 서비스 에지(SASE), 5G, AI 및 기타 최신 네트워킹 기술을 지속적으로 구축해야 하는 요구 사항을 NaaS에 대한 가장 주요한 동인으로 생각하고 있습니다.

## 주요 조사 결과 3: 운영

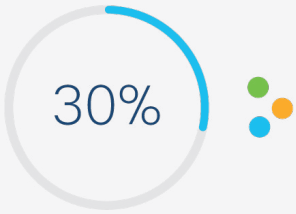
NaaS는 우수한 모델이지만, 이는 네트워킹 팀이 SLA(Service-Level Agreement)를 준수해야만 효과를 발휘합니다.




- NaaS 사업자를 통해 제공받아야 하는 주요 서비스는 네트워크 라이프사이클 관리(48%), 네트워크 탄력성(42%), SLA 준수를 위한 모니터링 및 문제 해결(38%)인 것으로 나타났습니다.

## 주요 조사 결과 4: 우려 사항

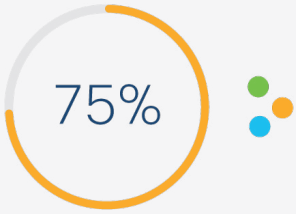
하지만 이 모든 과정이 매사 순조로운 건 아닙니다. 제어 위임 및 비용과 관련한 몇 가지 우려 사항이 있기 때문입니다.




- 그러한 우려 사항으로는 NaaS가 이전에 볼 수 없었던 새로운 수요(30%)를 지원할 수 있는지 여부, 그리고 보안 제어력 상실(26%) 문제가 있었습니다.
- 전환 비용 및 업무 중단도 높은 순위를 차지했습니다(28%).

## 주요 조사 결과 5: 역할

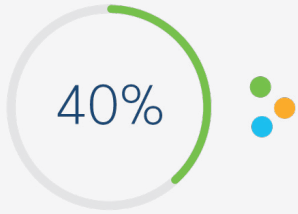
NaaS는 IT 전문가를 위한 새로운 지평을 열고 있으나, 게임의 레벨을 높여야 할 필요가 있습니다.




- 75% 이상의 조직이 NaaS가 IT 팀의 기술을 향상할 수 있는 기회를 제공한다는 데 동의합니다.
- 그러나 현재 비즈니스 요구 사항을 기술적인 정책으로 전환할 때 자사의 IT 직원을 시스템 통합업체, 매니지드 서비스 사업자 또는 NaaS 벤더보다 더 신뢰하여 그들에게 맡길 조직은 4곳 중 한 곳 정도에 불과합니다.

## 주요 조사 결과 6: 도입

NaaS를 시작하는 방법은 여러 가지이며, 그중 하나가 바로 SASE입니다.



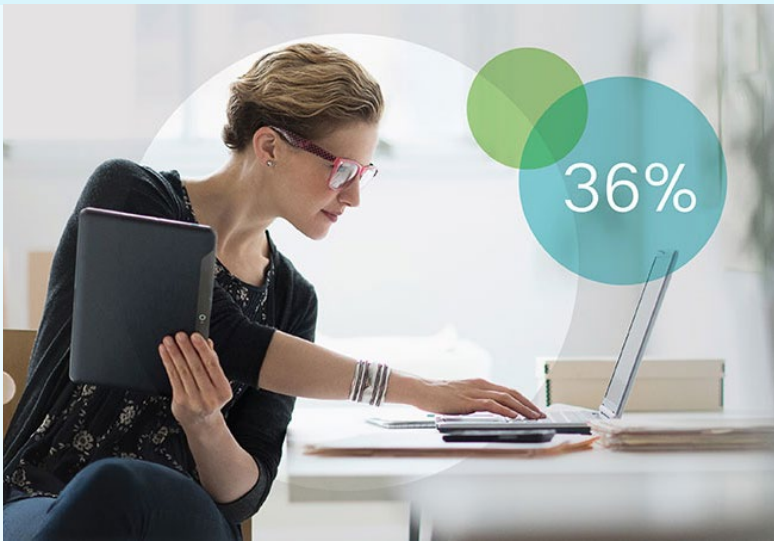

- SASE는 NaaS의 진입점일 가능성이 높은데 그 이유는 조직의 40%가 멀티 클라우드 액세스를, 그리고 34%가 보안을 NaaS에 적합하다고 꼽았기 때문입니다.
- 조직의 49%는 교체 또는 업그레이드 주기 동안 NaaS를 시작할 계획이 있으며, 34%는 기존 사이트를 조정하는 단계부터 시작할 것 같다고 답했습니다.

# 색다른 네트워킹 모델

18개월 이상의 업무 중단 및 적응기를 거친 후, 네트워크 기술이 기업의 생존과 성공에서 차지하는 역할은 그 어느 때보다 명확해졌고 어떻게 보면 더욱 필수적인 요소가 되었습니다. 이미 원격 근무를 실현하는 핵심 요소가 된 네트워크는 이제 더 안전한 업무 환경, 하이브리드 근무 모델, 발전하는 비즈니스 운영을 지원해야 할 임무를 부여받았습니다. 이렇게 하려면 온프레미스, 멀티 클라우드, 엣지 환경 전체에서 네트워크가 원활하게 작동해야 합니다. 네트워크는 위치, 디바이스 또는 연결성 제공 방법에 상관없이 모든 사용자를 위한 안전하고 일관된 경험을 제공해야 합니다. 그리고 네트워크는 기존 애플리케이션과 최신 마이크로서비스 기반 애플리케이션을 모두 지원해야 합니다.

리소스와 대역폭이 한정된 경우가 많으므로, 많은 IT 및 네트워크 리더는 이러한 당면 과제를 해결하기 위한 대안적 방법으로 NaaS를 살펴보고 있습니다. 하지만 NaaS란 정확히 무엇일까요?

IT 전문가에게 NaaS의 정의에 대해 물어본 결과, 이는 여러 사람마다 다른 의미로 해석될 수 있다는 점이 금세 명확해졌습니다. 실제로 시스코 설문에 따르면 놀랍게도 응답자의 36%가 이미 NaaS를 보유하고 있다고 주장했습니다. 이는 신생 기술치고는 높은 수치로 보일 수 있으나, 인터뷰를 실시한 결과 자사의 네트워크 중 일부라도 서드파티 사업자가 관리하는 경우라면 NaaS를 보유 중인 것으로 간주하는 응답자가 많다는 걸 알 수 있었습니다. 이러한 정의는 너무 광범위하며 더 구체적으로 좁혀야 할 필요가 있다고 생각합니다.



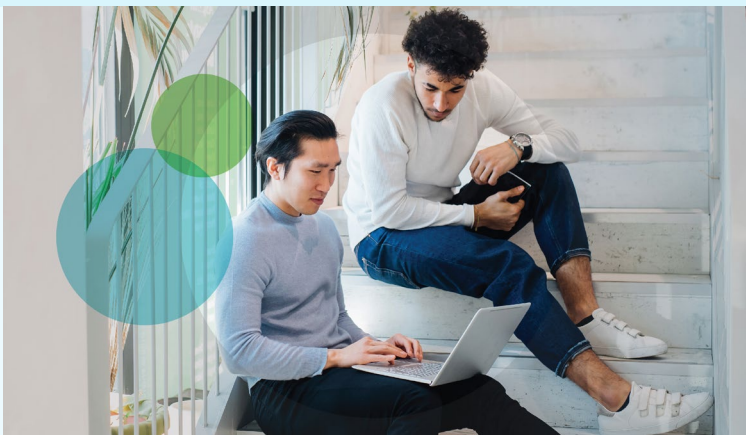

**NaaS는 인프라를 소유하거나, 구축하거나, 유지 관리하지 않아도 사용자가 네트워크 기능을 구매하고 오케스트레이션할 수 있는 클라우드 방식의 사용량 기반 소비 모델입니다.**

"조직은 내부 리소스와 파트너가 제공하는 리소스의 적절한 조합을 찾고자 노력하고 있습니다. 많은 조직에서는 인력, 애널리틱스, 관측 가능성, 자동화에 투자하는 방식을 선택하고 있으며 전략적인 벤더를 활용하여 인프라 관리 및 유지 관리 업무를 경감할 방법을 열심히 고심하고 있습니다."
— IDC,리서치 부문 부사장, Mary Turner

NaaS는 유선 및 무선 LAN, WAN, VPN은 물론 브랜치, 데이터 센터, 엣지, 멀티 클라우드, 하이브리드 클라우드 환경을 비롯한 폭넓은 네트워크 요소에 대한 대안적인 소비 모델을 제공합니다. NaaS는 SASE 같은 새로운 네트워크 모델을 제공하는 데 사용할 수 있습니다. 이를 통해 조직의 모델을 전환할 수 있으며, 일례로 하이브리드 근무로 전환하는 경우를 들 수 있습니다. 그리고 IT 팀은 온디맨드 서비스인 NaaS를 통해 더욱 쉽게 스케일업 또는 스케일다운하고 새로운 서비스를 신속하게 구축하며 자본 지출(CapEx) 및 운영 지출(OpEx) 간의 균형을 최적화할 수 있습니다.

우리가 이야기를 나눴던 일부 IT 리더들의 말에 따르면, NaaS는 현재 절실히 필요한 새롭고 더욱 개선된 네트워킹 형식을 제시합니다.

이러한 IT 리더는 자신들이 뒤처지고 있으며 사용자의 신뢰를 잃어가고 있다는 점을 인식하고 있습니다. 그리고 이들은 NaaS가 최신 기술을 실현하고, 늘어나는 요구 사항을 충족하고, 가속화 중인 비즈니스 속도를 따라가는 데 도움이 될 것이라 생각합니다.



"네트워킹 복잡성의 수준이 너무나 높아지고, 기업이 시장 변화에 대응해야 하는 속도가 급격히 빨라지는 동시에 최신 네트워크의 범위가 방대해지면서 많은 이들이 '우리 힘만으로는 더 이상 이 일을 할 수 없으며, 도움이 필요하다'라는 점을 깨닫고 있습니다."

— IDC네트워크 분석, 리서치 책임자, Mark Leary

결론:

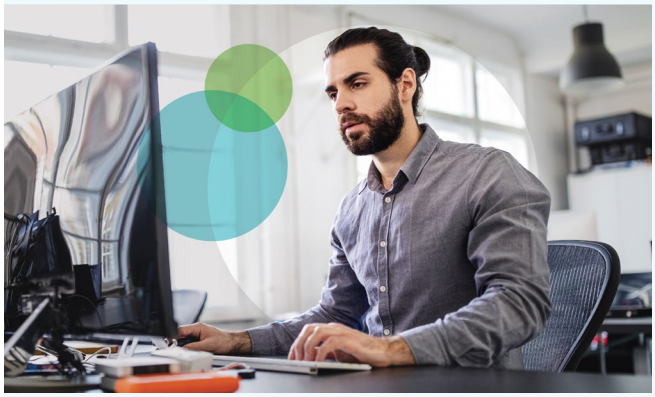
NaaS 도입률은 2021년부터 2027년까지 연평균 성장률 40.7% 규모로 성장할 것으로 예상됩니다.[1]

# 당면 과제 해결, 이점 제공

NaaS 모델을 도입할 것인지 선택하는 과정은 결국 NaaS가 해결하는 비즈니스 및 기술 당면 과제, 그리고 NaaS가 제공하는 이점으로 귀결됩니다.

설문조사에 참여한 조직의 경우, 민첩성을 가장 염두에 두는 것으로 나타났습니다. 네트워크가 해결해야 할 가장 큰 비즈니스 당면 과제를 질문한 결과, IT 전문가의 약 50%가 업무 중단에 대응하는 것이라 답변했으며, 40%는 새로운 비즈니스 애플리케이션 및 비즈니스 프로젝트를 수용하는 것이라 답변했습니다. 응답자의 1/3 이상이 네트워크 민첩성에 대한 필요성을 NaaS의 주요 동인으로 생각하고 있으며, 응답자의 절반은 NaaS를 사용하여 증대된 혁신 및 비즈니스 가치를 제공할 수 있을 것으로 기대한다고 답했습니다.

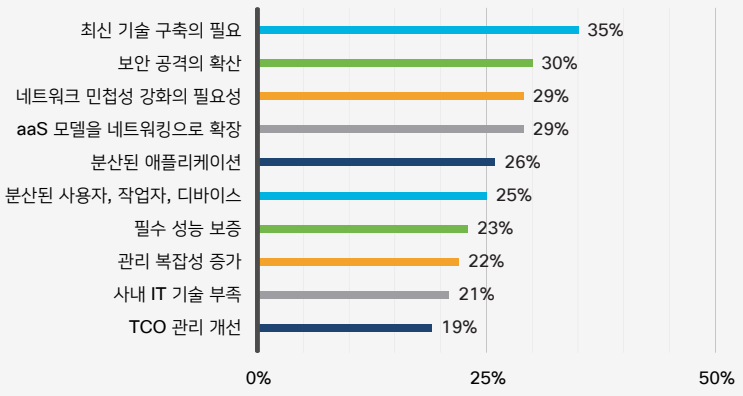
민첩성 강화를 위한 노력의 일환으로, 많은 IT 조직은 애플리케이션 및 서비스를 클라우드로 전환하고 있는데 이로 인해 새로운 보안, 거버넌스, 컴플라이언스 문제가 발생할 수 있습니다.



본 설문조사에 참여한 IT 전문가들의 의견에 따르면, 현재 네트워크를 관리하는 과정에서 당면하고 있는 가장 큰 기술 문제는 여러 클라우드 연결(36%), 네트워크, 사용자, 애플리케이션 보호(34%), 보안 또는 성능 문제의 근본 원인 파악 및 신속한 복구(31%)입니다.

그와 동시에 응답자의 1/3은 최신 네트워킹 기술(예: Wi-Fi 6, SD-WAN, SASE, 5G, AI 등)을 지속적으로 구축해야 할 필요성을 NaaS로 전환하는 주요 동기로 꼽았으며, 나머지 1/3은 최근 들어 점점 더 빈번해지고 정교해진 보안 위협에 방어할 수 있는 기능을 꼽았습니다.

귀사가 NaaS 모델로 전환하는 가장 큰 원인은 무엇입니까?



"경영진은 직원들이 디바이스를 설정하거나 인프라를 운영하는 일은 생산적인 가치가 없다고 생각합니다. 그들은 IT 조직이 비즈니스 목표 측면에서 고민하길 원합니다. 기본적인 운영 업무에 외부 서비스를 이용하면 직원들이 비즈니스 성과에 더 가깝게 다가갈 수 있습니다."

— 글로벌 소비재 회사, IT 인프라 책임자

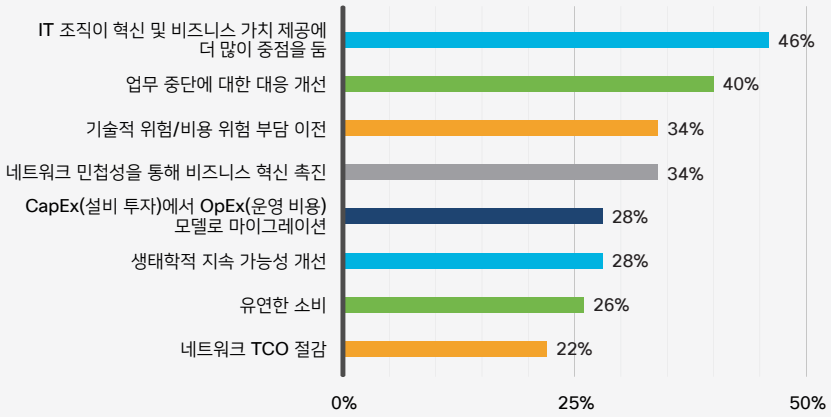
IT 전문가가 NaaS에서 기대하는 주요 이점을 질문한 결과, 주요 의사 결정권자는 일상적인 인프라 관리 대신 비즈니스 가치를 제공하는 데 중점을 둘 수 있는 기능을 꼽았습니다.

네트워크 및 보안 중단에 대한 대응 개선은 또 다른 높은 평가를 받은 NaaS의 이점으로, 네트워크 실무자의 45% 그리고 주요 의사결정권자의 40%가 이를 언급했습니다. 보안 개선에 우선순위를 두는 것은 자연스러운 일이었지만, 네트워크 실무자의 25% 이상 그리고 주요 의사결정권자의 33%가 생태학적 지속 가능성 개선을 NaaS의 중요한 이점으로 생각한다는 사실을 알게 된 점이 흥미로웠습니다.

## NaaS의 재정적 이점이 낮은 순위를 차지한 것은 더욱 놀라웠습니다.

유연한 소비 모델 및 구독 기반 가격을 갖춘 NaaS를 통해 IT 팀은 자본 지출(CapEx)을 운영비용(OpEx)으로 전환하고, 네트워크 인프라에 대해 반복되는 대규모 투자를 방지할 수 있습니다. 대신, 지출의 일관성과 예측 가능성이 더 증가하게 되므로 기업은 사용하는 리소스에만 비용을 지불할 수 있습니다. 하지만 그럼에도 불구하고 IT 리더 및 네트워크 전문가는 NaaS의 이러한 회계상의 이점보다는 민첩성, 혁신, 관리 업무 완화 이점을 더 높이 평가했습니다.

NaaS 모델 사용 시 발생할 수 있는 3가지 주요 비즈니스 이점은 무엇이라고 생각하십니까?




## 결론:

기업은 비즈니스 가치를 제공하고 업무 중단에 신속히 대응하는 데 훨씬 더 촉각을 곤두세우고 있으므로, NaaS의 경우 TCO는 우선순위 목록에서 낮은 순위를 차지하는 것으로 나타났습니다. IT 리더의 68%는 NaaS로 인해 IT 팀이 일상적인 관리 업무에서 해방되어 혁신 및 비즈니스 가치를 제공하는 일에 집중하는 데 더 많은 시간을 할애할 수 있을 것이라는 점에 동의하거나 매우 동의한다고 답했습니다.

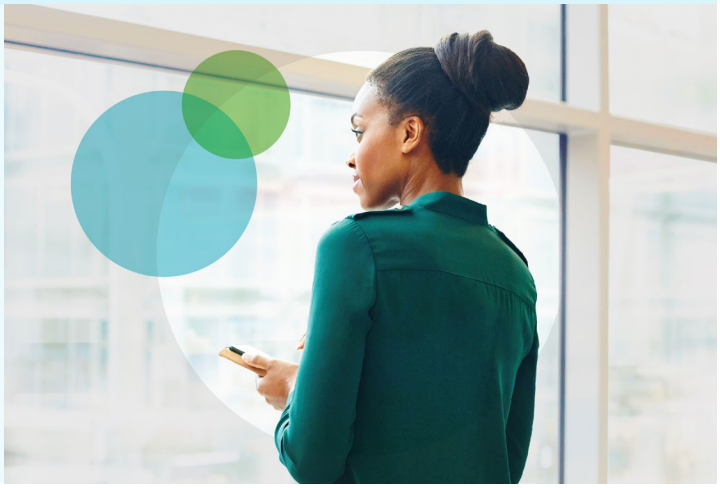
# NaaS를 통한 네트워크 운영(NetOps) 방식의 변화

NaaS에 대한 일반적인 한 가지 우려 사항은 네트워크 운영에서 완전히 손을 떼야 하므로, NaaS 사업자에게 모든 책임을 위임하게 되고 조직의 NetOps 팀은 아무런 할 일이 남지 않게 된다는 데 있습니다. 그러나 현실적으로 보았을 때, 운영 책임에 관한 한 NaaS는 양자택일해야 하는 문제가 아닙니다.

NaaS 모델의 경우, 해당 사업자는 네트워크 라이프사이클 관리의 모든 측면에 대한 책임을 집니다. 여기에는 계약상의 성과를 제공하는 데 필요한 네트워크 인프라(고객의 모든 온프레미스 장비 포함)의 모든 요소를 구축, 통합, 제어, 업데이트, 모니터링, 복구하는 일이 포함됩니다. 성과에는 연결된 사용자, 사이트, 클라우드 사업자, 애플리케이션의 수는 물론 합의된 서비스 레벨, 대역폭, 애플리케이션 성능, 보안 조항, 컴플라이언스 및 기타 요구 사항이 포함될 수 있습니다.

그렇다면 남은 관리 항목은 무엇일까요? NaaS 고객의 네트워크 운영 팀은 핵심 업무 또는 부가가치를 생산하는 업무에 더 많은 시간을 집중할 수 있게 됩니다.

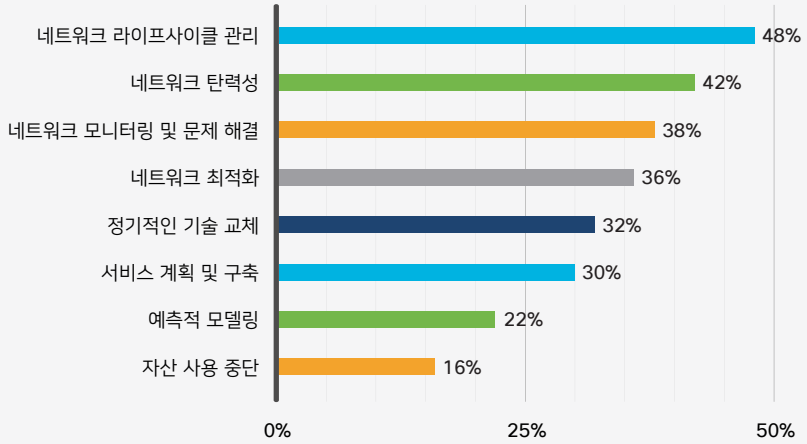
예를 들어 이러한 업무에는 원하는 네트워크 성과(예: 사용자 및 애플리케이션 액세스 정책, 애플리케이션 성능 레벨)를 규정하고 모니터링하는 일이 해당될 수 있습니다. 고객의 네트워크 운영 팀은 네트워크 성능 및 인사이트를 모니터링하여 도메인 전체의 네트워크 정책 및 동작을 지속적으로 조정하고 최적화할 수 있습니다.



또한, 고객의 네트워크 운영 팀은 API를 사용하여 NaaS와 기존 시스템 간의 통합을 관리하여 IT 워크플로우 및 프로세스를 간소화할 수 있습니다. 그리고 네트워크 운영 팀은 NaaS 사업자와 긴밀히 협업하여 SLA 및 SLO(Service-level Objective)를 충족하고자 할 가능성이 높습니다. 운영 책임 및 위임에 상관없이, IT 전문가들은 인프라 관리의 부담을 절실히 줄이고자 한다는 것을 명확히 알 수 있었습니다.

설문조사에 참여한 IT 전문가의 48%가 NaaS 모델에 포함할 가장 중요한 서비스는 네트워크 라이프사이클 관리라고 답했습니다. 상위 3가지 서비스 중 그 뒤를 이은 건 네트워크 탄력성(42%), 네트워크 모니터링 및 문제 해결(38%)이었습니다. 이는 점점 더 분산되고 복잡하게 뒤섞인 위치, 사용자, 디바이스, 애플리케이션, 클라우드 리소스를 관리하는 일 때문에 부가가치를 창출하는 활동 및 혁신에 할애할 시간이 거의 없다는 견해를 더욱 확고하게 뒷받침합니다.

다음 중 NaaS 모델에 포함할 가장 중요한 서비스는 무엇입니까?




"사업자가 자잘한 일상 업무를 처리하므로 내부 팀은 새로운 요구 사항을 해결하여 네트워크를 통해 더 많은 가치를 더하는 데 주력할 수 있습니다. 우리 회사의 엔지니어와 기술자는 문제를 해결하느라 업무를 중단하지 않아도 되며, 새로운 프로젝트에 집중할 수 있습니다."

— 글로벌 컨설팅 회사, 선임 네트워크 엔지니어

## 결론:

NaaS 모델에서는 운영 책임을 공유합니다. 네트워크 라이프사이클 관리의 부담이 사업자에게 옮겨지므로, 고객의 IT 팀은 비즈니스 가치에 기여하는 운영 활동에 더 많이 주력할 수 있습니다.

# 역할, 책임, 기술

인프라 유지 관리 및 라이프사이클 관리 책임이 사업자에게 이전되므로, NaaS는 상당한 시간을 얻게 해주는 효과가 있습니다. 그리고 이로 인해 고객의 네트워크 운영 팀은 인프라 유지 관리의 기술 및 운영적인 측면 대신 원하는 네트워크 성과에 주력할 수 있습니다.

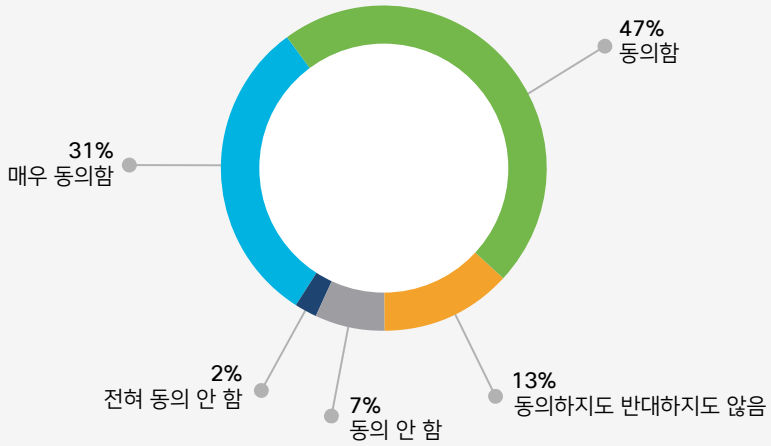
즉, 네트워크 엔지니어는 "비행기를 조종"하는 일에서 "관제탑에서 관리 감독"하는 일로 전환하게 됩니다. 하지만 이들은 어떤 유형의 관리 감독을 예상하고 있을까요?

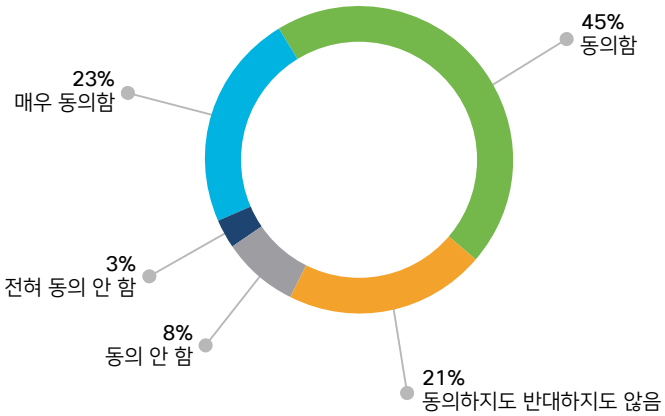
응답자들의 답변에 따르면, IT 직원이 기술 전문 지식 및 NaaS 대시보드를 활용하여 비즈니스 요구 사항을 네트워크 정책으로 전환할 것이라 생각하는 응답자는 27%였습니다. 그리고 놀랍게도 응답자의 73%는 서드파티 사업자가 이러한 비즈니스 크리티컬한 역할을 수행하는 걸 선호할 것 같다고 답변했습니다. 이는 내부 기술 역량이 부족하거나 확신이 부족함을 나타내는 것일 수 있습니다.


"일상 업무의 가장 큰 부분을 NaaS 사업자에게 넘기게 되면 고객의 네트워크 운영 팀은 일반적인 네트워킹 및 네트워크 보안 기술, 그리고 비즈니스 인텐트를 세부적인 네트워킹 개념으로 전환하는 설계 기술 쪽으로 자연스럽게 향하게 됩니다. 이들은 NaaS 사업자와 긴밀하게 협업하여 네트워크 설계, 정책, 성능, SLA를 최적화해야 할 것입니다. 그리고 이러한 변화를 파악하고 오케스트레이션하려면 탄탄한 데이터 과학 기술이 필요합니다."

— 시스코 수석 엔지니어(Distinguished Engineer), Joe Clarke

NaaS 모델을 도입하면 네트워크 팀원들이 새로운 기술을 익히고 조직에 더 많은 가치를 제공할 수 있는 기회가 주어질 것이다.




NaaS는 네트워킹 팀이 일상적인 네트워크 관리 대신 IT 혁신 및 비즈니스 가치를 제공하는 업무에 주력할 수 있는 시간을 확보하게 해줄 것이다.

결론:

75% 이상의 조직이 NaaS 모델이 IT 팀의 기술을 향상하고 더 많은 가치를 제공할 수 있는 기회를 선사하게 될 것이라는 점에 동의 또는 매우 동의합니다.

# 우려와 망설임

NaaS는 IT 조직의 여러 부문에 영향을 미치므로 새로운 운영 모델, 기존 프로세스 및 기술과의 새로운 통합, 역할 및 기술 변화, 자본 지출(CapEx)에서 운영 지출(OpEx)로 재정적 변화가 필요합니다. 이러한 광범위한 영향을 염두에 둔 IT 전문가들은 NaaS에 대해 복합적인 반응을 보였습니다. 그리고 NaaS 도입과 관련해서는 좋은 쪽이든 나쁜 쪽이든 대부분 극과 극의 관점을 가진 것으로 나타났습니다.

NaaS에 대한 IT 리더의 관점은 자신이 가진 매우 중요한 네트워킹 철학을 반영하는 것 같았습니다. 그리고 이러한 철학은 크게 두 가지 진영인 "제어형 IT" 및 "린(lean) IT"로 나뉘었습니다. 전자의 철학을 가진 리더들은 고급 기술을 갖춘 직원을 보유하고 있을 뿐만 아니라, 팀이 네트워킹 스택을 소유하고 완전히 제어해야 한다고 확고히 생각하는 쪽입니다. 이와 반대로, 후자 그룹은 IT를 통합하고, 일상 업무와 부가가치가 있는 업무를 비교하여 재평가하고, 인프라 유지 관리의 부담을 덜 수 있는 방법을 찾고자 노력합니다. 이미 IT 리소스의 일부를 클라우드로 전환한 "린 IT" 철학에 기반한 조직은 당연히 NaaS 솔루션에 매우 열린 사고를 갖고 있습니다.

> "네트워크에 필요한 관리 및 우선적인 처리가 이루어지지 않을 것 같으며, 우리 조직의 환경에 완벽히 맞을 것 같지 않아 NaaS 도입을 늦추고 있습니다."
>
> — 미국 군사 기관, 네트워킹, IT 관리자

본 조사를 통해 대화를 나눠본 일부 IT 리더는 자사의 네트워크 및 프로세스가 매우 특별하며, NaaS가 이와 같은 독특한 복잡성 및 당면 과제를 해결할 수 있을 것이라 생각하지 않는다고 밝혔습니다.

한편, NaaS가 IT 조직 내에 격변을 일으킬 것이 현실적인 우려 사항이라고 밝힌 다른 리더들도 있었습니다.

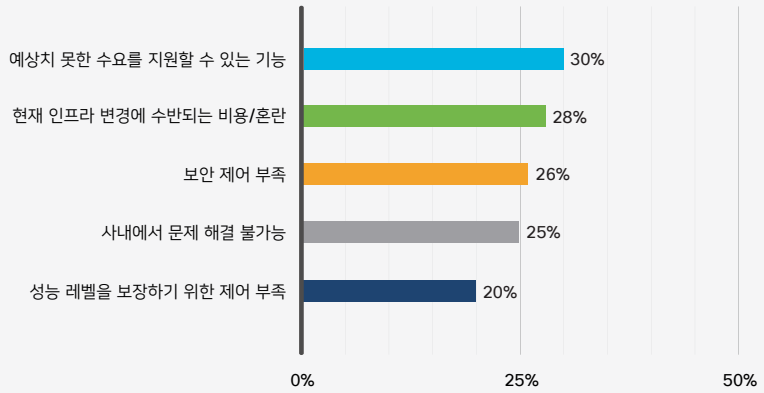
IT 리더들은 다양한 우려 사항을 이야기했으나, 그중에서도 제어력 상실을 가장 우려하는 것으로 나타났습니다. 응답자의 30%가 NaaS를 도입할 경우 미래의 요구 사항에 부응할 수 있을지 의문스럽다고 답했습니다. 다른 응답자들은 보안 제어력 상실(26%) 및 성능(20%)이 우려된다고 답했습니다. 사실 NaaS는 더 큰 규모의 온디맨드 확장성 및 최신 기술의 신속한 지원을 위해 설계되었습니다. 그리고 보안, 성능 및 그 밖의 중요한 제어 결정권은 NaaS 벤더가 아니라 여전히 IT 팀에게 있습니다.

"NaaS 사업자는 기업의 보안 지침에 적응하고 기업의 지시 사항을 따라야 합니다. 이것이 NaaS의 중요한 차별점입니다."

— 글로벌 기술 회사, 리드 아키텍트

응답자의 28%가 기존 인프라 및 운영 변경과 관련된 비용과 업무 중단이 저해 요소라고 답했습니다. 그도 그럴 것이, 조직은 다양한 기술을 보유하고 있고 여러 가지 투자를 감행해왔으므로 이러한 자산의 감가상각 시기는 저마다 다릅니다. 다른 조직은 레거시 기술 및 애플리케이션이 NaaS에 적합하지 않을 것 같다는 우려를 나타냈습니다. 그리고 일상적인 인프라 관리 업무를 딱히 경감하고 싶지 않다는 의견도 있었습니다.

## NaaS 모델 구축에 대한 주요 우려 사항은 무엇입니까?




이러한 우려와 망설임을 해결하려는 경우, 조직은 한 가지 도메인에서 작은 규모로 시작하여 NaaS 모델을 테스트해볼 수 있습니다. 이렇게 하면 네트워크 인프라 또는 운영을 대대적으로 변경하지 않고도 NaaS 기능 및 제어 지점을 보다 잘 이해할 수 있습니다. 사업자와 내부 팀 간의 책임 분배를 체험해본 후 이를 최적화하고, 협업을 통해 최상의 결과를 실현하기 위한 방법을 배울 수 있습니다. 역할, 책임, 제어 지점을 완전히 이해하고 이러한 개념에 익숙해지면 지금까지 얻은 인사이트와 모범 사례를 활용하여, 서서히 다른 도메인으로 규모를 늘리고 확장할 수 있습니다.

## 결론:

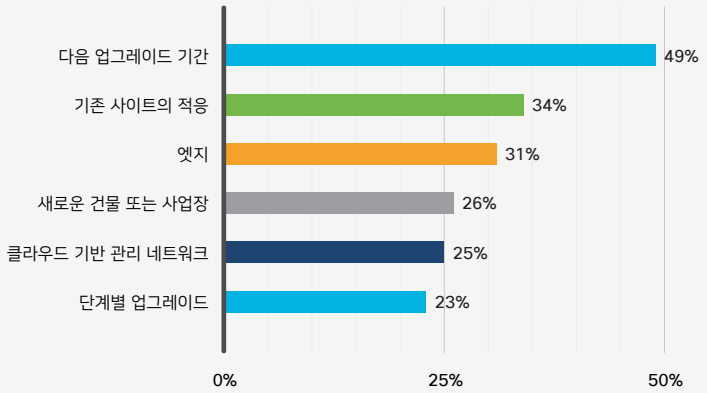
어떤 전환 모델이든 우려가 예상되는 것은 당연한 일입니다. IT 리더는 작은 규모로 시작하여 NaaS와 관련된 위험과 보상을 평가하여 이 모델이 조직에 적합한지 확인할 수 있습니다.

# 도입 추세

네트워크 운영에 미치는 영향 및 활용 가능한 방법의 다양성으로 인해 NaaS 도입은 모든 조직마다 다릅니다. NaaS 준비도 평가 및 구축 로드맵은 복잡성을 최소화하고 성공률을 극대화할 수 있습니다.

응답자에 따르면, IT 리더의 49% 및 네트워크 실무자의 57%는 NaaS를 도입하기에 가장 좋은 시기와 상황은 네트워크 인프라를 업그레이드하거나 교체할 때, 그리고 최신 기술(자동화, 100기가비트 이더넷, Wi-Fi 6, 5G, SD-WAN, SASE 등)을 이용할 방법을 모색할 때라고 생각하는 것으로 나타났습니다. 응답자의 34%는 네트워킹 기술이 이미 구축된 기존(브라운필드) 사이트가 NaaS를 도입하기에 적합한 시나리오라고 답했습니다. 흥미롭게도, NaaS를 도입하기에 가장 알맞은 경우가 그린필드라고 답한 응답자는 26%에 불과했습니다. 그리고 도메인을 NaaS와 함께 하나씩 업그레이드하는 단계별 방식이 조직에 가장 알맞은 시나리오라고 답한 응답자는 23%뿐이었습니다.

다음 시나리오 중 귀사에 NaaS가 가장 알맞을 것 같은 경우는 무엇입니까?




## 결론:

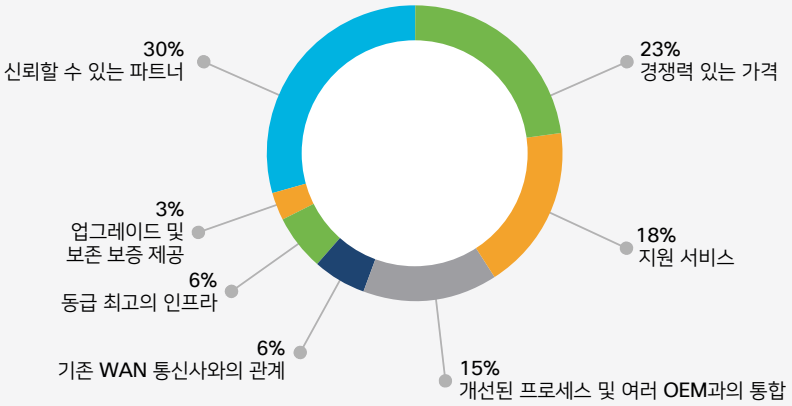
NaaS를 구축하는 방법, 시기, 이유는 모든 조직마다 다릅니다.

# NaaS 사업자 선정

네트워크는 직원 생산성, 고객 참여, 비즈니스 운영을 지원하는 중요한 요소이므로, 올바른 NaaS 사업자를 선정하는 일은 그리 간단하지 않습니다. 본 조사에 참여한 일부 IT 리더는 제어력을 상실하게 되는 것이 두렵다고 말하기도 했습니다. 그럼에도 이들은 신뢰할 수 있는 파트너라면, 그리고 그러한 경우에 한하여 제어 수단을 위임할 의향이 있다고 답했습니다. 협업하는 대상이 시스템 통합업체, 매니지드 서비스 사업자 또는 부가 가치 리셀러(Value-added Reseller)인지 여부와 관계없이, IT 리더는 네트워크 환경, 비즈니스 목표, 지원 요구 사항에 대해 이미 높은 이해도를 가진 탄탄한 파트너와 일할 때 가장 마음을 놓을 수 있습니다.

NaaS 구축의 경우, 본 설문조사에 참여한 IT 전문가의 약 1/3은 네트워크 벤더보다 시스템 통합업체가 더 신뢰도가 높으며 가격 경쟁력이 있다고 여기는 것으로 나타났습니다. 그리고 "신뢰할 수 있는 전문 지식"이 "동급 최고의 인프라"보다 훨씬 더 중요하다고 밝혔습니다.

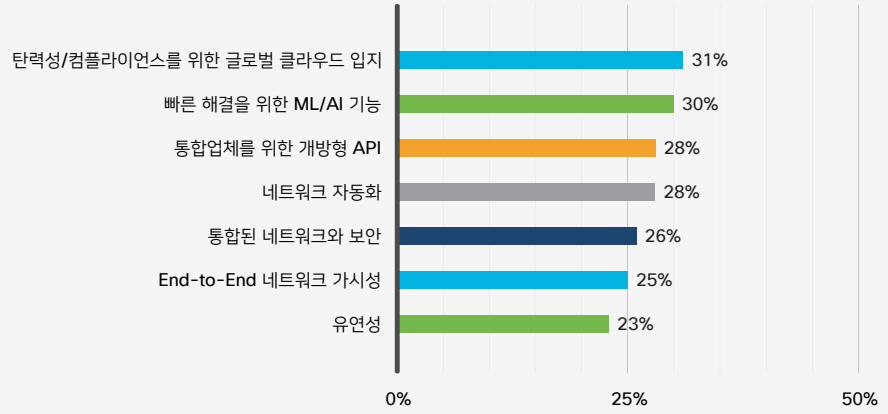
NaaS 구축 시 네트워크 벤더와 직접 일하는 것보다 파트너와 협업하는 걸 선호하는 주된 이유는 무엇입니까?




그리고 비즈니스 요구 사항을 기술 정책으로 전환하는 문제의 경우, IT 전문가는 NaaS 벤더보다 시스템 통합업체나 내부 IT 직원을 더 신뢰할 가능성이 2~3배 높은 것으로 나타났습니다. 이는 조직이 NaaS와 관련하여 단순히 솔루션을 찾는 게 아니라, 자사에 대해 잘 아는 신뢰할 수 있는 어드바이저의 안내와 지원을 받고자 한다는 사실을 분명히 보여줍니다.

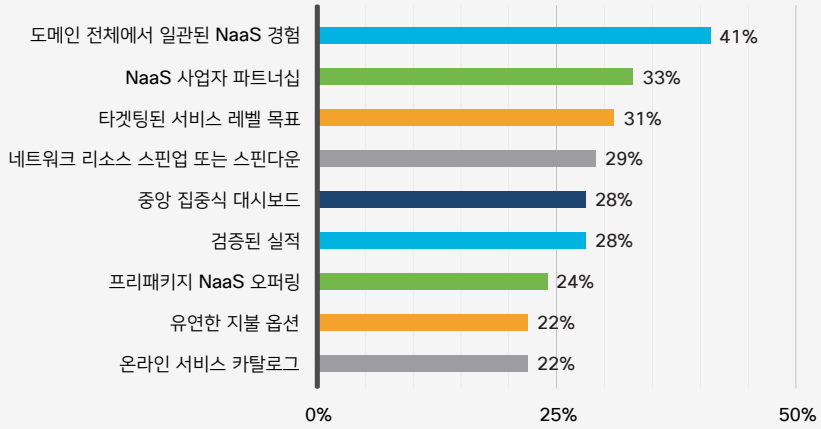
NaaS 사업자 및 솔루션의 기술적 속성을 고려할 경우, 본 설문의 응답자는 신뢰성, 성능, 지역별 컴플라이언스(31%)를 지원하는 글로벌 클라우드 입지는 물론, NaaS 서비스의 지속적인 최적화를 실현할 수 있는 머신러닝(ML) 및 인공 지능 기능(30%)을 우선시하는 것으로 나타났습니다. API, 자동화, 통합 보안, 네트워크 가시성, 네트워크 유연성도 높은 순위를 차지했습니다.

## NaaS 오퍼링의 가장 중요한 기술적 속성 2가지는 무엇이라고 생각하십니까?




응답자의 41%가 NaaS 사업자의 중요한 역량은 네트워크 도메인(액세스, WAN, 데이터 센터, 클라우드 등) 전반에 걸친 일관된 NaaS 플랫폼을 제공하는 것이라고 답했습니다. 수많은 IT 팀이 여러 가지 환경, 툴셋, 운영 모델을 관리하느라 고충을 겪고 있는 상황에서 NaaS는 네트워크 리소스, 정책, 운영을 통합할 수 있는 기회를 제공합니다.

## 다음 중 NaaS 사업자 오퍼링을 고려한다고 가정할 경우 가장 중요한 점은 무엇입니까?




"제가 절실히 찾고 있는 건 우리 회사의 네트워크와 시스템 전체에서 펌웨어 업데이트, 설정, 변경 같은 일상적인 관리 업무를 처리할 수 있는 사람입니다. 그렇게 되면 우리 팀은 개선 사항, 빌드, 전략 구현에 주력할 수 있습니다. 그리고 유연성도 늘어날지 모릅니다. 이번 달에 저 혼자 꽤 과중한 업무를 처리해야 하는데, 두 달 정도 도움을 요청하여 이러한 사용량을 확대하고 업무 지원을 받고자 합니다."

— U.S. $100 M(비영리단체) 기술 및 보안 VP

## 결론:

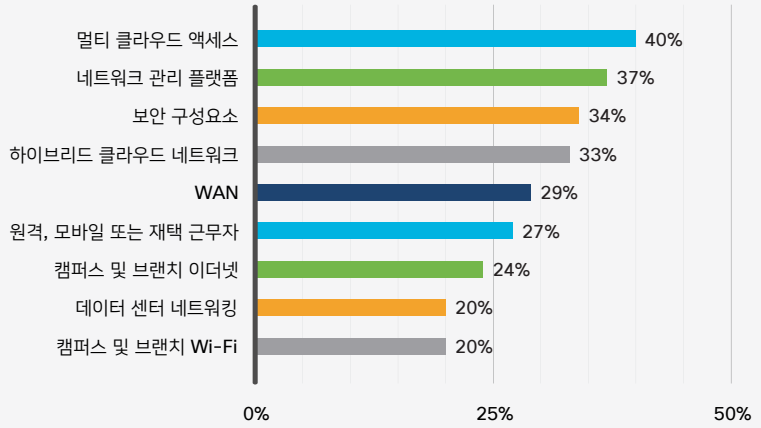
NaaS 벤더보다 시스템 통합업체가 더 신뢰성이 높고, 가격 경쟁력이 있으며, 서비스 중심적이라고 생각합니다. 사업자에 상관없이, 고객은 모든 네트워크 도메인 전체를 다루는 서비스 및 운영 경험을 모색하고 있습니다.

# SASE, 그리고 NaaS의 다른 점

유선 및 무선 LAN, VPN, WAN, 네트워크 보안, 원격 또는 재택 근무 액세스, 데이터 센터 네트워크, 클라우드 네트워크를 비롯하여 NaaS 오퍼링의 수가 증가하고 있습니다. 시스코의 조사에 따르면, 멀티 클라우드 액세스 및 보안이 포함된 NaaS 모델이 가장 수요가 높은 것으로 나타났습니다. 이는 어디서든 안전한 멀티 클라우드 액세스를 제공하는 SASE가 여러 IT 조직에서 수요가 많은 aaS(as-a-service) 오퍼링이 될 것임을 뜻합니다.

여러 개의 서로 다른 클라우드에 연결하는 것이 쉬운 일이 아니라는 점을 감안하면, 멀티 클라우드 액세스가 NaaS의 주요 우선순위(40%)로 꼽힌 건 당연한 일입니다. NaaS 벤더는 SD-WAN 서비스를 제공하여 광범위한 클라우드 기반(IaaS 및 SaaS) 애플리케이션에 연결하는 일관되고 최적화된 방법을 제공할 수 있습니다.

네트워크 장비 및 관리의 어떤 측면이 NaaS에 적합할 것 같습니까?

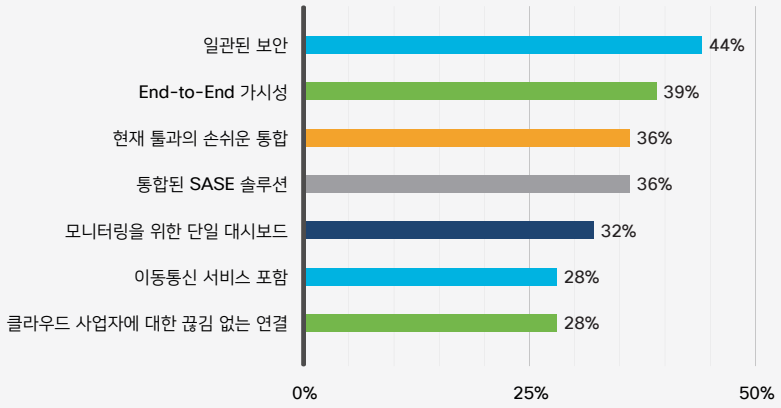



응답자의 34%가 VPN, 보안 정보 및 이벤트 관리(SIEM), 보안 웹 게이트웨이, 방화벽, 침입 방지 및 탐지 서비스(IPS/IDS)를 비롯하여 보안에 중점을 둔 NaaS 솔루션을 우선시하는 것으로 나타났습니다. 이러한 솔루션은 여러 클라우드 및 컴퓨팅 환경 전체에서 사용자, 디바이스, 애플리케이션을 일관성 있게 보호할 수 있습니다.

엣지에서 멀티 클라우드 액세스 및 보안을 함께 조합하여 제공하는 NaaS 벤더는 SASE 솔루션에 대한 증가하는 수요를 충족하기에 적합한 입지를 갖추고 있습니다.

응답자의 약 절반(44%)이 액세스하는 위치에 상관없이 "모든 사용자 및 디바이스에 대한 일관된 보안(위협 탐지 및 해결 기능 포함)"을 SASE의 중요한 측면으로 꼽았습니다. 클라우드 기반 애플리케이션에 액세스하기 위해 인터넷 의존도가 증가함에 따라, 응답자의 1/3 이상(39%)이 "인터넷 및 클라우드 인프라 전체의 네트워크 트래픽에 대한 가시성 및 인사이트"를 원하는 것으로 나타났습니다. 그리고 응답자의 36%는 현재 툴과 쉽게 통합되는 SASE 솔루션을 찾고 있다고 답했습니다.

## 귀사에서 SASE를 aaS (as-a-service)로 구축하기로 선택한 경우, 다음 중 귀하가 가장 중요한 것으로 고려할 기능은 무엇입니까?




## 결론:

멀티 클라우드 액세스 및 보안은 NaaS의 주요 우선순위입니다. SASE 옵션을 NaaS 포트폴리오에 함께 구성하는 벤더는 온프레미스 및 클라우드 리소스를 조율하고 보호하는 기능에 대한 증가하는 요구를 충족할 수 있습니다.

# 결론

수많은 IT 조직이 네트워크 복잡성을 관리하고, 업무 중단에 대응하고, 사용자와 데이터를 보호하고, 가속화되는 비즈니스 속도를 따라잡기 위해 고군분투하고 있습니다. 이러한 당면 과제를 해결하기 위해 많은 조직에서는 NaaS 같은 새로운 네트워킹 모델을 조사하고 있습니다.

NaaS는 온디맨드 또는 구독 기반 모델을 통해 최신 네트워킹 기술에 지속적으로 액세스할 수 있도록 합니다. 일상적인 네트워크 관리의 부담을 서드파티 제공자가 지게 됩니다. 따라서 IT 팀은 NaaS를 이용하여 민첩성, 탄력성, 혁신을 제공하는 부가 가치 활동에 집중할 수 있습니다.

여느 혁신 모델과 마찬가지로 NaaS를 둘러싼 우려와 망설임이 존재합니다. 그러나 이는 양자택일을 해야 한다는 제안이 아닙니다. IT 팀은 신뢰할 수 있는 파트너와 협력하여 소규모로 NaaS를 사용해 보고 위험과 리워드를 평가하며 가장 중요한 비즈니스와 기술 전략과 맞는지 확인할 수 있습니다.

## 추가 리소스 및 지원

NaaS(Network as a Service)란? >

Cisco+ 솔루션 >

시스코 파트너 찾기 >

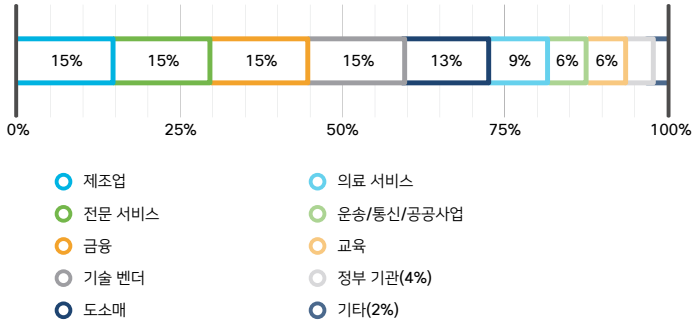
시스코 영업 팀에 문의 >

## 이 보고서 정보

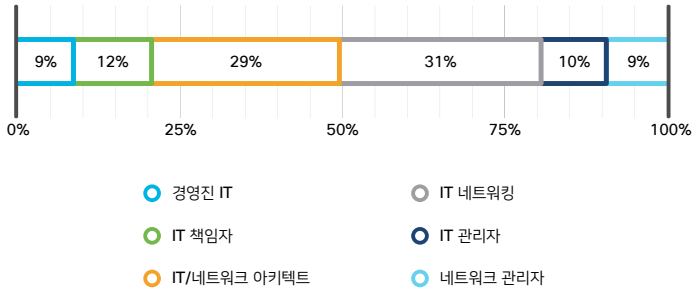
2019년에 처음 발간된 글로벌 네트워킹 트렌드 보고서는 엔터프라이즈 네트워킹 및 클라우드 산업 내의 최신 전략과 기술을 중점적으로 다룹니다. 이 보고서는 업계 리서치를 활용하며 IT 조직이 현재의 기술 트렌드를 이해하고 네트워킹 모델을 발전시키며 역동적인 비즈니스 요구 사항을 지원할 수 있는 관점, 인사이트, 조언을 제공합니다.

2022년 보고서 작성을 위해 시스코에서는 IT 리더 20명을 대상으로 인터뷰를 실시했으며 13개국의 IT 전문가 1,534명으로부터 NaaS에 대한 견해와 향후 2년간 NaaS가 네트워킹 전략에 어떻게 부합되고 강화될 것인지 의견을 들었습니다. 응답자는 최대 세 개의 답변을 선택할 수 있었습니다.

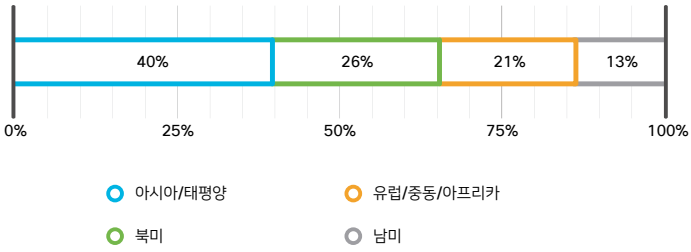
### 응답자 업종




### 응답자 직무




### 응답자 지역



## 이 보고서를 사용할 권한

시스코에서는 언론, 애널리스트, 블로거, 서비스 제공자, 규제 기관 및 기타 이해 당사자들이 본 조사 자료를 활용하고 참조할 수 있도록 지원합니다. 시스코 2022 글로벌 네트워킹 트렌드 보고서 데이터를 비공개적 또는 공개적으로, 서면 또는 전자 형식으로 게시하거나 공유하는 모든 경우에는 "출처: 시스코 2022 글로벌 네트워킹 트렌드 보고서"와 같은 방식으로 출처를 명시해야 합니다. 시스코의 공개 백서, 보고서, 웹 기반 툴을 참조하는 데 추가적인 서명과 동의 절차는 필요 없습니다.

시스코에서는 항상 시스코의 데이터가 사용되는 상황에 관심을 두고 있습니다. 시스코의 콘텐츠를 활용하시는 경우 시스코 2022 글로벌 네트워킹 트렌드 보고서 삽입을 포함하여 완성된 작업 사본을 시스코와 공유해 주시면 대단히 감사하겠습니다. 시스코 2022 글로벌 네트워킹 트렌드 보고서의 참조 자료를 포함한 문서를 networkingtrends-inquiries@cisco.com으로 전달하실 수도 있습니다.



**2022 글로벌 네트워킹 트렌드 자료 출처**

1. Global Network-as-a-Service (NaaS) Market Industry Dynamics, Market Size, and Opportunity Forecast to 2027, Report Ocean, 2021년 3월.