시스코 공개 보고서

The bridge to possible

2023 글로벌 네트워킹 트렌드 보고서

분산된 인력을 위한 안전한 멀티 클라우드 연결 간소화

The bridge to possible

2023 글로벌 네트워킹 트렌드 보고서

분산된 인력을 위한 안전한 멀티 클라우드 연결 간소화

목차

서론

시스코 글로벌 네트워킹 트렌드 보고서는 엔터프라이즈 네트워킹 및 클라우드 산업 내 중요한 전략과 기술에 초점을 맞춰 매년 발행되고 있습니다. 본 보고서는 경영진의 관점 및 인사이트를 통한 주요 연구 및 업계 조사 결과를 취합하여 최신 기술 동향을 파악하고 IT 조직이 역동적인 비즈니스 요구 사항을 지원하여 네트워킹 모델을 혁신할 수 있도록 도움이 되는 가이드를 제공합니다.

2023 보고서에서는 기업과 조직이 네트워크를 구축하고 혁신하여 분산된 애플리케이션, 사람, 장소, 사물을 위한 안전한 연결을 지원하는 방법에 대해 소개합니다. 북미, 남미, 아시아 태평양, 서유럽 13개국에서 2,500명이 넘는 IT 리더들을 대상으로 설문조사를 실시했습니다.

주요 결과: 여러 클라우드를 연결하는 네트워킹 현황

하이브리드 업무는 계속해서 보안 연결 문제를 야기하고 있습니다.

하이브리드 워크 시대가 도래하면서 멀티 클라우드 환경에 분산된 기업 데이터 및 자산에 원격 근무자를 안전하게 연결할 수 있는 새로운 접근 방식이 필요해지고 있습니다.

- 직원들에게 사무실 복귀를 권장하고 있지만, **40%** 이상의 직원들은 풀타임 또는 일주일에 며칠씩 원격 근무를 계속하고 있습니다.
- 애플리케이션이 여러 클라우드에 배포되고 인력이 고도로 분산됨에 따라 기존의 보안 모델이 제 역할을 하지 못해 IT 전문가들의 골칫거리가 되고 있습니다. IT 전문가 절반 이상(**51%**)이 주요 과제로 클라우드 보안 위험 파악을, **39%**가 원격 근무자의 증가를 꼽았습니다.

클라우드 및 멀티 클라우드로의 전환이 가속화되고 있습니다.

비즈니스 민첩성에 대한 해답으로 많은 응답자들이 클라우드라고 답했습니다.

- 조직은 계속해서 클라우드 플랫폼을 도입하고 있습니다. 현재 **63%**의 조직에서 워크로드의 **40%** 이상을 호스팅하고 있으며, 설문 응답자의 **78%**가 해당 조직에서 2025년까지 워크로드의 **40%** 이상을 호스팅할 계획이라고 답했습니다.
- 멀티 클라우드 도입도 증가하고 있습니다. 클라우드 및 네트워킹 전문가의 **42%**가 여러 클라우드 사용의 주요 동기로 더욱 민첩하고 확장 가능한 애플리케이션 개발을 꼽았습니다.

클라우드 애플리케이션에 대한 사용자 액세스 보안이 2023년 가장 중요한 네트워킹 과제로 떠올랐습니다.

디지털 서비스 제공 공급망(예: 사용자와 클라우드 간)을 유지하여 일관된 애플리케이션 경험을 제공하는 것 또한 엔터프라이즈 IT 전문가들의 주요 관심사입니다.

- 네트워크 전문가의 **41%**가 여러 클라우드에 분산되어 있는 애플리케이션에 대한 보안 액세스를 제공하는 것을 최우선 과제로 꼽았습니다.
- 응답자의 **37%**는 기업 네트워크의 경계 바깥에서 생성되거나 종료되는 트래픽이 증가함에 따라, 네트워크 성능 및 보안에 대한 포괄적인 가시성을 확보하는 것이 두 번째로 큰 과제라고 답했습니다.

필수 가이드: 클라우드 기반 애플리케이션에 안전하게 액세스하기 위한 성공적인 네트워킹 전략

네트워킹 및 보안 통합 추구

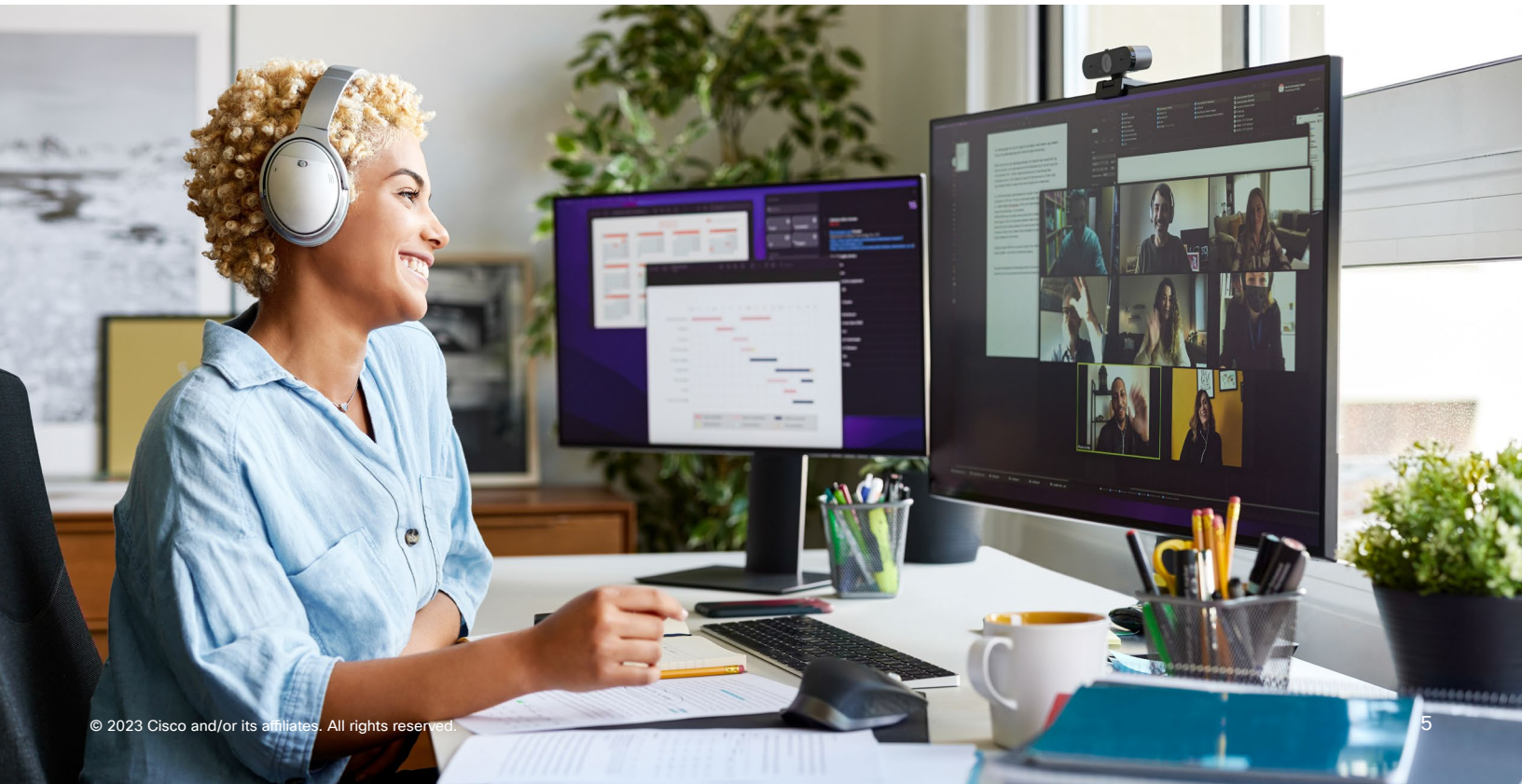
IT 팀 간 협업을 활성화하여 액세스 네트워킹부터 클라우드까지 운영을 간소화합니다.

사일로화된 조직과 기존 연결 제공 모델로는 고도로 분산된 애플리케이션, 사람, 장소, 사물의 동적 네트워크 성능과 보안 니즈를 충족하기 어렵습니다.

- 보안, 네트워킹, 클라우드 운영 전체에서 정책 표준화, 텔레메트리 공유, 워크플로우 간소화를 통해 기술 사일로 상태에서 운영되는 환경보다 효과적이고 빠른 IT 및 비즈니스 성과를 달성할 수 있습니다.
- 응답자의 40%가 분산된 위치에서 여러 클라우드 기반 애플리케이션으로의 보안 액세스를 제공하는 데 핵심적인 과제 중 하나로 사일로화된 운영을 꼽았습니다.
- 클라우드 전문가들은 네트워크 운영과 클라우드 운영의 일관성을 향상시켜야 한다고 생각합니다. 38%가 네트워킹 팀과의 협업 증진을 원하고 있으며 34%가 운영 일관성을 핵심 목표로 삼고 있습니다.

SASE 아키텍처를 통해 통합 네트워킹 및 보안 모델로 전환하십시오.

SASE(Secure Access Service Edge)는 멀티 클라우드 액세스 및 하이브리드 인력에 필요한 운영 간소화와 일관된 보안 및 성능을 제공합니다.



- 조직들은 SD-WAN(Software-Defined WAN)과 클라우드 보안을 통합하여 SASE 아키텍처를 구현하고 있습니다.
- 응답자의 47%가 2년 이내에 SD-WAN 환경을 전체적인 SASE 아키텍처로 확장하여 브랜치와 원격 클라이언트를 연결할 계획이라고 답했습니다.

클라우드 우선 네트워킹 및 보안 도입

SD-WAN 연결을 지속적으로 여러 클라우드에 확장하여 IT 관리를 간소화하고 애플리케이션 경험을 개선할 수 있습니다.

모든 클라우드에 정책을 일관적으로 적용하여 클라우드에 구애받지 않은 연결을 자동화함으로써 애플리케이션 경험을 최적화하고 보호하십시오.

- 클라우드, SaaS, 중간 협력업체에 가시성, 제어, 제로 트러스트 액세스를 확장하면 IT에서 더욱 안전하고 개선된 사용자 경험을 제공할 수 있습니다.
- 응답자의 절반 이상(53%)이 향후 2년에 걸쳐 모든 위치에서 클라우드 기반 애플리케이션에 대한 연결을 개선하기 위해 클라우드 서비스 제공업체와의 통합을 우선과제로 삼고 있다고 답했습니다.

클라우드 중심 보안을 혁신하여 일관된 운영 및 정책을 구현하십시오.

여러 보안 기능을 클라우드 플랫폼에서 결합하면 가시성, 정책 관리, 제어가 간소화될 뿐 아니라 범위가 확장되고 효과가 강화됩니다.

- 응답자의 59%가 여러 위치에 분산된 사용자와 디바이스에 일관된 정책을 적용하는 것이 중요하므로 향후 2년 간 클라우드 액세스 네트워킹의 최우선 과제는 클라우드에서 보안을 중앙 집중화하는 것이라고 답했습니다.

선제적 운영으로의 전환

포괄적인 네트워크 가시성을 통해 점점 복잡해지는 디지털 서비스 제공 공급망 전체에 일관된 사용자 경험을 제공할 수 있습니다.

자체 네트워크를 넘어 인터넷과 클라우드 환경으로 가시성을 확장하지 않으면 IT 팀이 클라우드 기반 애플리케이션 및 서비스를 위한 높은 품질의 일관된 사용자 경험을 제공할 수 없습니다.

- 응답자의 51%가 사전 예방적인 문제 탐지 및 해결을 위한 우선과제로 포괄적인 네트워크 텔레메트리 및 가시성을 꼽았습니다.
- 사용자와 디바이스 트랜잭션의 대부분이 기업의 경계 너머에서 이루어지는 지금, 인터넷과 클라우드 트래픽에 대한 가시성이 특히 중요합니다.

사후 대응적 운영에서 예측적 운영으로 전환하여 가동 시간을 개선하고 성능 수준을 향상하십시오.

예측적 애널리틱스는 전반적인 IT 운영 간소화, 가속화, 효과 증진을 위한 AIOps(Artificial Intelligence for IT Operations) 툴킷의 중요한 부분 중 하나로 인식되고 있습니다.

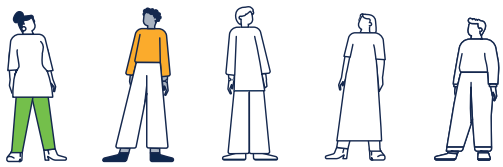
- 중단이 발생한 후 문제를 해결하는 대신 네트워크 성능 저하를 방지하기 위해, 응답자의 47%가 향후 2년 동안 예측형 네트워크 애널리틱스 도입에 주력할 계획이라고 밝혔습니다.

The bridge to possible

소개: 멀티 클라우드 액세스 트렌드

"전화 시스템이 공공 유틸리티인 것처럼, 언젠가는 컴퓨팅도 공공 유틸리티로 제공되어 구독자가 실제로 사용하는 용량에 대한 요금만을 지불하게 될 것입니다."[1] John McCarthy 교수가 1961년 MIT 강의에서 미래를 예측한 말입니다.

그로부터 60년 넘게 지난 지금, 온디맨드 컴퓨팅 유틸리티 공유에 대한 McCarthy 교수의 비전은 아직 완전히 실현되지는 않았지만 글로벌 디지털 혁신을 이끄는 주요 동인 중 하나가 되었습니다.



직원 5명 중 2명이 하이브리드 또는 풀타임 원격 근무를 하고 있습니다.

계속되는 멀티 클라우드로의 전환

오늘날 대부분의 조직에서 여러 클라우드를 사용하고 있습니다. 시스코 2023 글로벌 네트워킹 트렌드 연구 결과, 조직의 3분의 2가 이미 워크로드의 40% 이상을 여러 클라우드에서 운영하고 있습니다. 또한 대부분의 조직이 2개 이상의 클라우드 공급업체를 이용하고 있으며 대다수의 조직이 5개 이상의 SaaS 공급업체를 이용하고 있습니다(그림 1 참조).

하이브리드 업무는 계속됩니다

고도로 분산화되는 것은 애플리케이션 뿐만이 아닙니다. 하이브리드 업무가 널리 도입됨에 따라 사람과 사물도 그 어느 때보다 분산되고 있습니다.

최근 연구에 따르면, 59%의 직원들이 사무실로 복귀했지만, 28%는 하이브리드 방식으로, 나머지(13%)는 완전히 원격으로 근무하는 등 상당수의 직원들이 원격 근무를 계속하고 있습니다.[2] 이 수치는 업계와 역할에 따라 크게 다릅니다.

이와 동시에 IoT 기술과 엣지 컴퓨팅의 도입이 가속화됨에 따라 매일 관리 및 보안이 필요한 연결과 엄청난 양의 데이터 흐름이 계속 증가하고 있습니다.

인력이 분산화되고 IoT 및 엣지 컴퓨팅이 확산되면서, 확장 가능한 보안 연결과 멀티 클라우드 애플리케이션에 대한 액세스, 네트워크 전체에 대한 글로벌 호스팅 서비스의 필요성이 대두되고 있습니다(그림 2). 많은 네트워킹 전문가들이 이를 2023년 최우선 과제로 꼽았습니다.

인터넷을 통한 연결은 네트워킹 및 보안 전문가의 가시성과 제어 범위를 벗어난 인프라로 인해 이 문제를 더욱 복잡하게 만들고 있습니다. 그럼에도 불구하고 네트워킹 및 보안 담당자들은 여전히 직원, 고객, 파트너의 디지털 경험과 보호에 대한 책임이 있습니다.

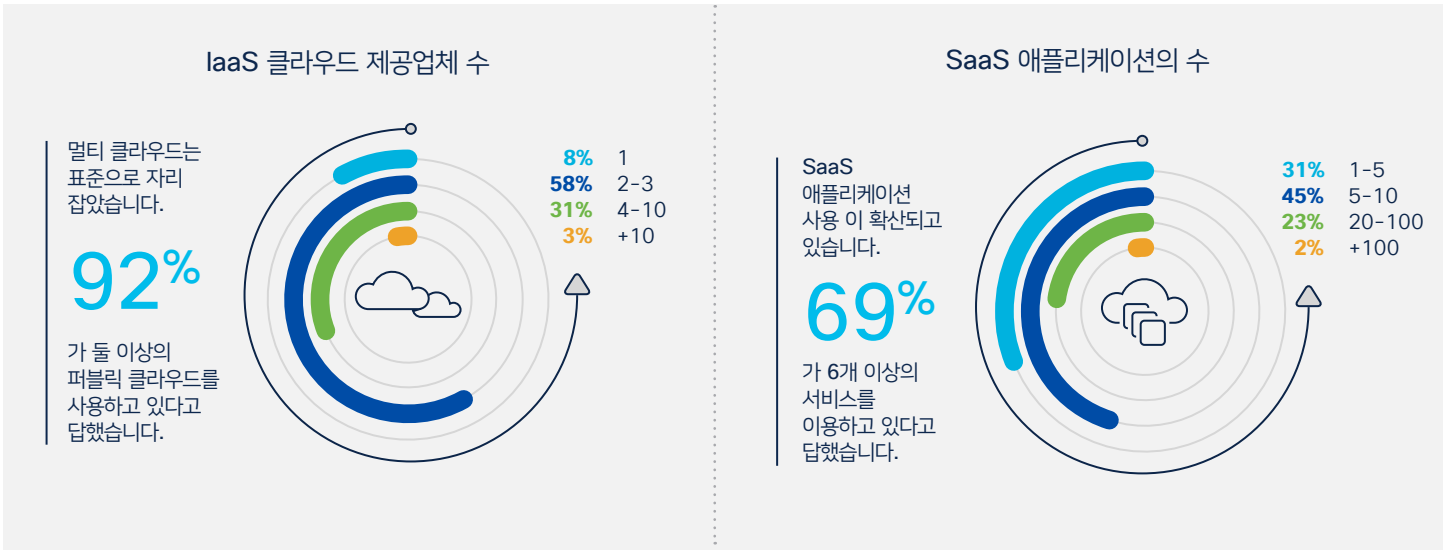


그림 1. 여러 클라우드 및 SaaS 제공업체 이용이 표준으로 자리 잡았습니다.

The bridge to possible

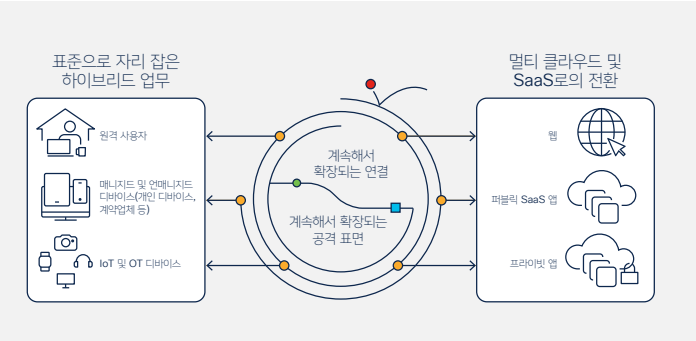


그림 2. 하이브리드 업무와 클라우드 및 SaaS로의 전환은 네트워크 보안의 과제가 인간의 역량을 넘어섰다는 것을 의미합니다.

"사람들은 비즈니스 우선순위를 위해 몇 주나 몇 개월을 기다리고 싶어하지 않습니다. 따라서 사람들은 모든 비즈니스 이니셔티브에 있어 과거에 존재했던 병목현상 대신 더욱 즉각적인 만족을 기대합니다."

— 소매업계 IT 디렉터

속도와 민첩성의 중요성 대두

오늘날 민첩성은 대부분의 조직에서 필수 요소로 떠올랐습니다. 설문조사 결과에 따르면 여러 클라우드로 전환하게 되는 가장 큰 이유는 비용이 아니라, McCarthy 교수가 예측했듯이 비즈니스 민첩성과 혁신의 필요성, 그리고 높은 품질의 새로운 애플리케이션과 서비스를 신속하게 제공해야 할 필요성 때문인 것으로 나타났습니다. 전 세계를 뒤흔든 팬데믹과 지정학적, 경제적 혼란, 공급망 문제를 경험한 지금, 시장 트렌드를 활용하기 위한 발빠른 태세 전환이 우선과제 중 하나가 되었습니다.

조직들은 오늘날의 환경에서 사일로화된 기술 및 운영 모델에는 너무 많은 제약이 따르고, 효과적이지 않으며, 새로운 툴과 프로세스가 필요하다는 사실을 인식하고 있습니다. 연결 및 보안 과제를 해결하려면 더욱 단순하고 안전하며 유연한 네트워크 인프라 및 운영 모델을 제공할 수 있는 보다 포괄적인 접근 방식이 필요합니다.

본 보고서의 다음 부분에서는 이러한 과제에 대해 알아보고 유연하면서도 안전한 연결을 확보하기 위한 모범 사례 가이드를 소개합니다. 또한 어디서든 직원, 파트너, 고객에게 안정적이고, 안전하며, 강력한 클라우드 기반 경험을 제공하기 위해 네트워크 팀과 보안 팀이 협업해야 하는 방식과 그 이유를 알아봅니다.

1 https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative

2 https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf

The bridge to possible

필수 가이드: 멀티 클라우드에 대한 보안 액세스를 제공하기 위한 6가지 모범 사례

필수 가이드 1: IT 팀 간 협업을 활성화하여 액세스부터 클라우드까지 IT 운영을 간소화합니다.

사일로화된 조직과 기존의 연결 제공 모델로는 고도로 분산된 애플리케이션, 사람, 장소, 사물의 동적 네트워크 성능과 보안 니즈를 충족하기가 어렵습니다.

복잡성이 증가하고 위협 표면이 확장됨에 따라 IT 리더들은 빠르게 변화하는 비즈니스 니즈에 빠르고 효율적이며 안전하게 대응할 수 있도록 팀 간 협업을 개선해야 합니다.

분산된 위치에서 여러 클라우드 기반 애플리케이션(예: IaaS(Infrastructure as a service), SaaS(Software as a service))에 대한 사용자 액세스를 제공할 경우 가장 큰 5가지 과제 중 4개가 보안 관련 문제입니다. 응답자의 40%가 분산된 위치에서 여러 클라우드 기반 애플리케이션으로의 보안 액세스를 제공하는 데 핵심적인 과제 중 하나로 사일로화된 클라우드, 네트워크, 보안 운영을 꼽았습니다.

수많은 IT 조직의 네트워크 팀과 보안 팀에서는 개별적인 계획 및 운영이 이루어지고 있지만, 기술 및 운영 사일로를 제거하고 포인트 통합 시스템의 수를 줄여야만 IT 리더들이 오늘날의 보안 과제를 해결할 수 있습니다.

팀, 툴, 프로세스를 조율하여 운영을 간소화하려면 운영 모델의 일관성을 향상시켜야 합니다. 시스코 조사 결과에 따르면 86%의 CIO와 IT 리더들은 온프레미스, 프라이빗 클라우드, 퍼블릭 클라우드, SaaS 시스템에서 더욱 일관된 운영 모델 개발의 필요성을 인식하고 있습니다.[3] 클라우드 운영 모델 원칙을 통해

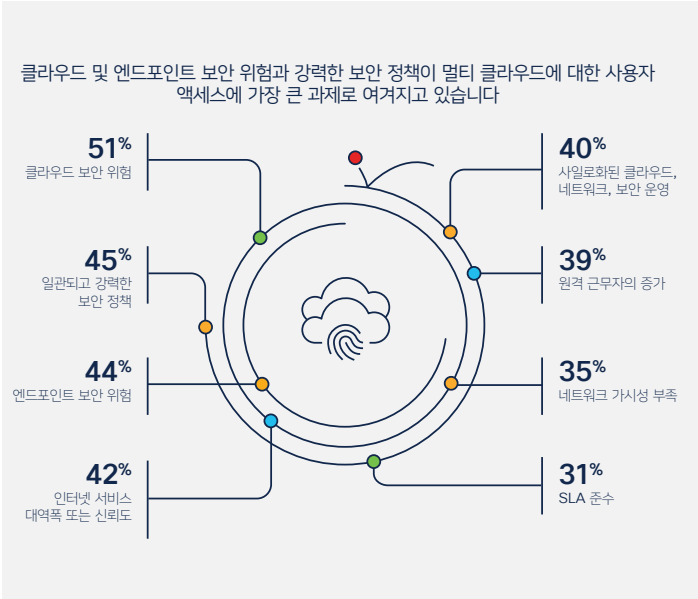


그림 3. 원격 위치에서 여러 클라우드 기반 애플리케이션에 대한 보안 액세스 제공에 따르는 과제

개발 운영 팀과 클라우드 운영 팀이 효과적으로 운영을 간소화하고 민첩성을 제공한다는 사실은 널리 알려져 있습니다. 클라우드 운영 모델 원칙을 도입하면 IT 팀에게도 이러한 효과가 있을 수 있습니다. 설문조사 결과도 이를 잘 보여줍니다. 클라우드 담당자 중 38%가 가장 큰 운영 과제는 네트워크와의 효과적인 통합이라고 답했으며, 34%는 클라우드와 네트워크 간 운영 일관성을 유지하는 것이라고 답했습니다.

The bridge to possible

38%의 클라우드 담당자들이 네트워크와의 긴밀한 통합을 큰 운영 과제 중 하나로 꼽았습니다.

네트워크와 전체 클라우드/네트워크 IT 스택에서 클라우드 운영 모델 원칙을 적용하면 IT 팀이 혁신을 가속하고, 보안을 강화하며, 클라우드 운영의 위험성을 방지할 수 있습니다. 네트워크, 보안, 클라우드 운영 간의 협업을 방해할 수 있는 복잡성과 파편화를 줄이고 궁극적으로 조직의 역동적인 니즈를 지원할 수 있습니다.

결론

클라우드 중심 모델을 바탕으로 네트워킹과 보안 정책, 기술, 툴, 운영 워크플로우를 통합함으로써 조직은 공동 툴을 사용하여 지속적인 보안 연결을 강화하면서 효율성을 증진하고 위험을 최소화할 수 있습니다.

3 https://ebooks.cisco.com/story/accelerating-digital-agility-2021/page/7/1

전문가 의견

강력한 팀 조정을 통해 보안, 단순성, 성과를 향상할 수 있습니다.

"먼 과거에는, 운영 팀이 케이블 연결부터 애플리케이션까지 모든 레이어와 모든 시스템을 파악하고 이 모두를 전체적으로 관리했습니다. 이러한 모델로 돌아가야 합니다.

클라우드의 네트워킹은 온프레미스의 네트워킹과 다르고, 이제 조직이 더 이상 에코시스템의 모든 디바이스와 소프트웨어를 제어하지 않지만 보안은 여전히 필요합니다. 특히 클라우드 애플리케이션에 대한 액세스를 보호하려면 사용자의 위치와 디바이스에 상관없이 일관된 정책을 적용해야 합니다. 이러한 정책에 따라 설계, 운영, 아키텍처를 통합할 수 있습니다.

앞으로는 운영 성능뿐 아니라 보안과 단순성이라는 원칙에 따라 엔드투엔드 인프라에서 협업하는 네트워킹 팀과 보안 팀이 늘어날 것이며, 이는 두 팀 모두 동일한 목표를 지향하기 때문입니다."

Wendy Nather
시스코 CISO 자문
위원장

The bridge to possible

필수 가이드 2: SASE 아키텍처를 통해 통합 네트워킹 및 보안 모델로 전환하십시오.

SASE는 멀티 클라우드 액세스 및 하이브리드 인력에 필요한 운영 간소화와 일관된 보안 및 성능을 제공합니다.

SASE는 네트워크 도메인과 보안 도메인을 통합하여 복잡하고 고도로 분산된 환경에서 사용자를 애플리케이션에 안전하고 원활하게 연결하는 데 필수적인 프레임워크를 제공합니다.

SASE는 안전한 멀티 클라우드 액세스를 위한 통합 아키텍처로 빠르게 자리 잡고 있습니다. 응답자의 47%가 2년 이내에 SASE 모델을 주로 사용하여 브랜치와 원격 클라이언트를 연결할 계획이라고 밝혔습니다.

그러나 많은 조직에서는 솔루션이 특정 기능을 갖추고 있지 않거나 완전히 통합된 네트워크 및 보안 솔루션을 제공하지 않아 SASE를 제대로 활용하지 못하고 있습니다.

SASE를 통합하려면 강력한 SD-WAN 기반과 다양한 기능을 갖춘 클라우드 보안 또는 SSE(Security Service Edge) 솔루션이 필요합니다(그림 4). 이러한 아키텍처가 완전히 통합되어야만 IT 조직이 SASE의 이점을 제대로 활용할 수 있습니다. 즉, 간소화된 운영 모델을 통해 어디에서든 사용자를 최대한 쉽고 일관되며 안전하게 연결하는 가시성을 확보하고, 관리 및 제어를 제공할 수 있습니다.

모든 보안 구성 요소와 네트워킹 구성 요소를 포괄하여 표준화된 정책, 공유 텔레메트리, 통합 알림 기능을 적용하는 통합 SASE 솔루션 덕분에 네트워크 운영 팀과 보안 운영 팀이 IT의 효율성, 성능, 보안을 강화할 수 있습니다. 네트워크 운영 팀과 보안 운영 팀이 보다 효율적이고 일관된 운영 모델과 워크플로우를 사용하면 확실히 더 나은 사용자 경험을 얻을 수 있습니다.

포괄적인 SASE 구현을 통해 운영 효율성, 사용자 경험, 보안을 개선할 수 있습니다. 이러한 이점의 예는 다음과 같습니다.

"SASE(Secure Access Service Edge)는 SD-WAN, SWG, CASB, NGFW, ZTNA(Zero Trust Network Access)를 포함한 서비스형 통합 네트워크 및 보안 기능을 제공합니다. SASE는 브랜치 오피스, 원격 근무자, 온프레미스 보안 액세스 활용 사례를 지원합니다. SASE는 주로 서비스 형태로 제공되며 디바이스 또는 개체의 ID에 기반한 제로 트러스트 액세스와 함께 실시간 컨텍스트와 보안 및 컴플라이언스 정책을 지원합니다."

— Gartner IT 용어, SASE(Secure Access Service Edge), 2023년 5월 2일 현재.

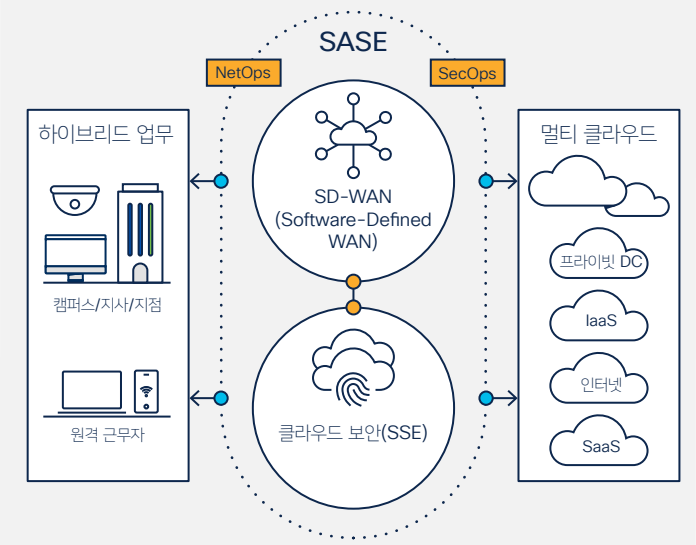


그림 4. 네트워크 및 보안 기술과 운영은 새로운 보안 연결 모델인 SASE(Secure Access Service Edge)를 제공합니다.

The bridge to possible

2021년에는 단일 벤더 SASE 제품에 SD-WAN 구매가 포함된 경우가 10% 미만에 불과했지만, Gartner®의 예측에 따르면 2025년까지 SD-WAN 구매의 50%가 단일 벤더 SASE 제품에 포함될 것으로 보입니다.[4]

- 시스코의 내부 IT 팀에서는 SASE 사용으로 운영 비용이 **40%** 절감되었습니다.
- 독립 테스트 기관의 엄격한 성능 평가 결과, 보안 정책이 적용된 Umbrella(Cisco SASE의 핵심 구성 요소)는 보안이 없는 인터넷을 통해 SaaS 애플리케이션에 액세스하는 경우보다 더 나은 성능을 발휘하는 것으로 나타났습니다.
- TechValidate 고객 조사에 따르면 Cisco 고객의 **85%**가 SASE 아키텍처를 도입하여 악성코드 감염을 **50%** 줄였습니다.

이러한 긍정적인 결과를 달성할 수 있는 두 가지 기본적인 접근 방식이 있습니다.

첫 번째는 보통 단일 벤더 또는 두 개의 벤더에서 제공하는 개별 네트워킹 및 보안/SSE 제품을 완전한 SASE 솔루션으로 통합하는 것입니다. 이 방식은 이미 SSE 또는 SD-WAN을 구축했으며 더 큰 사용자 지정 및 유연성이 필요한 조직에 적합합니다.

두 번째는 통합 관리를 통해 모든 네트워킹 및 보안 구성 요소를 단일 턴키 클라우드 서비스로 제공하는 통합 접근 방식입니다. 적절한 설계가 이루어진 통합 SASE 솔루션은 속도, 단순성, 가치 실현 시간을 단축합니다.

4 Gartner, 2022 Strategic Roadmap for SASE Convergence, Neil MacDonald, Andrew Lerner, John Watts, 2022년 6월, GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

전문가 의견

SASE 솔루션이 SASE 솔루션의 가치를 발휘하지 못하는 경우

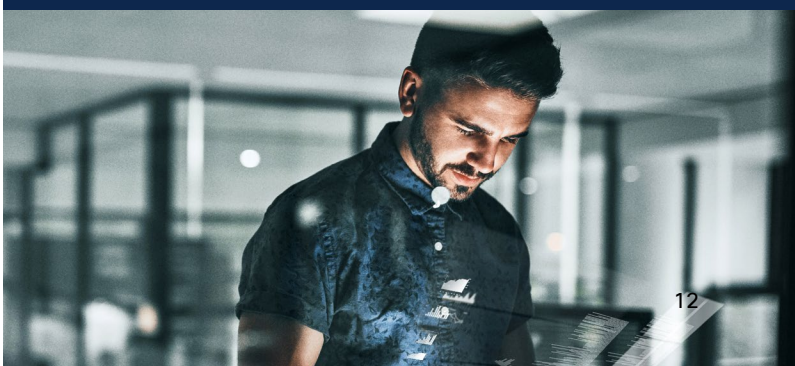
"모든 조직이 기존의 기반 기술을 보유하고 있기 때문에 이미 보유한 것에서 제외된 SASE 기능만 추가하는 방법이 매력적으로 보일 수 있습니다. 하지만 SASE는 장기적인 전략이며 고도의 통합 없이 단순히 SASE 모델의 모든 구성요소를 구축하는 것만으로는 SASE 솔루션을 제대로 활용할 수 없으며 원하는 결과를 얻을 수도 없습니다.

네트워킹 리더와 보안 리더는 자체적인 우선순위에 따라 고도로 통합된 SASE 솔루션을 이용하거나 턴키 통합 서비스를 이용해야 합니다.

통합 턴키 클라우드 서비스를 이용하면 네트워크 운영 팀과 보안 운영 팀이 엔드포인트, 엔터프라이즈 엣지, 클라우드 엣지에 걸친 분산된 지능형 시행, 보안, 가시성을 갖춘 중앙 집중식 관리를 통해 더 안전한 엔드투엔드 솔루션을 제공하여 최종 사용자 경험을 개선할 수 있습니다.

고객의 니즈를 더욱 효과적으로 충족하기 위해 어떤 기술 및 아키텍처를 선택하든, 벤더가 모든 구성요소를 제대로 통합된 하나의 시스템으로 결합하는지 확인하는 것이 중요합니다."

Omri Guelfand
Cisco Meraki NaaS/SASE
제품 관리 부문 VP



결론

기존 보안 솔루션과 달리, 클라우드 중심의 통합 SASE 아키텍처는 중앙 집중식으로 관리되는 보안 정책 및 시행을 최종 사용자와 애플리케이션에 더 가깝게 적용하여 유연하고 원활하며 안전한 연결성을 제공합니다.

SASE 자세히 알아보기

필수 가이드 3: SD-WAN 연결을 지속적으로 여러 클라우드에 확장하여 IT 경험을 간소화하고 애플리케이션 경험을 개선합니다.

모든 클라우드에 일관된 정책을 적용하여 클라우드에 구애 받지 않는 연결을 자동화함으로써 애플리케이션 경험을 최적화하고 보호하십시오.

클라우드가 엔터프라이즈 네트워크의 확장이 되었습니다. 많은 기업에서 SD-WAN은 완전한 SASE 구현의 디딤돌로 활용됩니다. 주요 IaaS, SaaS, 중간 협력업체를 통해 SD-WAN 패브릭 확장을 자동화하면 IT의 제어 범위가 확대되어 개선된 사용자 경험을 제공할 수 있습니다.

네트워킹 팀에서는 사용자 경험에 대한 제어 범위 확대를 매우 중요하게 생각합니다. 응답자의 53%가 분산된 위치에서 클라우드 기반 애플리케이션에 대한 연결을 개선하기 위해 클라우드 서비스 제공업체와의 통합에 중점을 두고 있다고 답했습니다. 응답자의 49%는 향후 24개월 간 SD-WAN과 멀티클라우드 통합을 최우선 이니셔티브로 삼겠다고 답하는 등 네트워킹 팀이 조치를 취하고 있습니다.

SD-WAN 멀티 클라우드 통합을 통해 네트워킹 팀과 클라우드 팀이 인터넷, 인터커넥트, 코로케이션, 클라우드 제공업체 네트워크를 통해 엔터프라이즈 현장에서 다양한 클라우드 제공업체 및 다른 엔터프라이즈 사이트로의 확장을 가속하고 자동화할 수 있습니다(그림 5). 이러한 통합이 이루어지면 시스템 관리자가 애플리케이션 경험을 최적화하고 모든 클라우드 및 온프레미스 위치에서 운영 경험의 일관성을 확보할 수 있습니다. 또한 IT는 Equinix, Megaport와 같은 글로벌 네트워크 인터커넥트 제공업체와 통합하여 클라우드 애플리케이션과 PoP(Point of Presence)에 안전하고 확장 가능한 액세스를 제공할 수 있습니다. 이러한 통합을 통해 IT 부서는 몇 분 만에 간소화되고 완전 자동화된 방식으로 글로벌 네트워크를 구축할 수 있습니다.

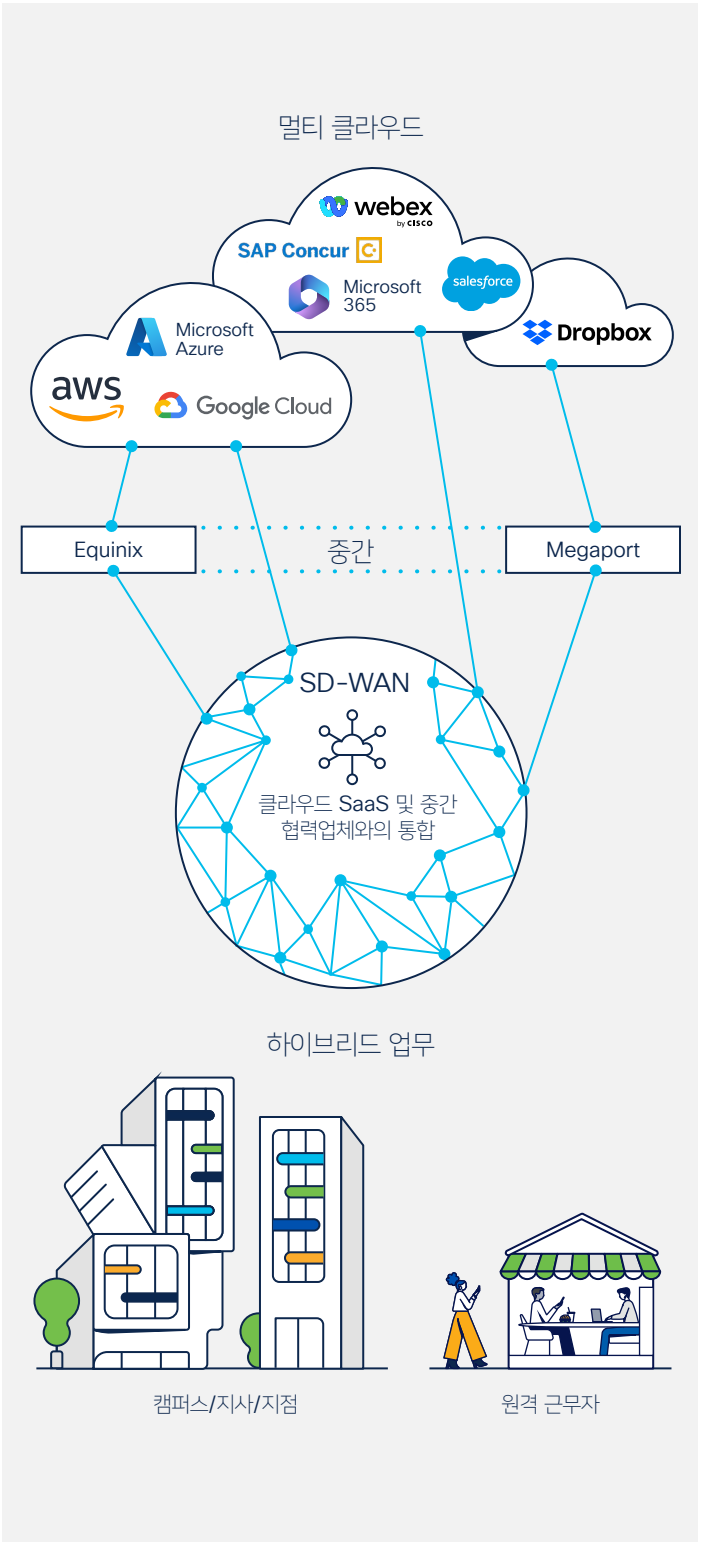


그림 5. IaaS, SaaS, 중간 협력업체와의 SD-WAN 통합은 IT 및 사용자 경험 개선에 필수적입니다.

The bridge to possible

결론

기업에서 1개 이상의 클라우드로의 확장을 가속화 및 간소화하고, 사용자 애플리케이션 경험을 최적화하고, 제로 트러스트 액세스를 통해 클라우드 애플리케이션 보안을 강화해야 하는 IT 팀에는 SD-WAN 멀티 클라우드 통합이 매우 중요합니다.

SD-WAN 자세히 알아보기

전문가 의견

멀티 클라우드 연결의 복잡성과 위험성을 간과해서는 안 됩니다.

" 오늘날 클라우드 중심 환경에서는 대표적인 클라우드, SaaS, 중간 협력업체와의 긴밀히 통합되지 않은 SD-WAN 솔루션을 제공하는 것은 상상조차 할 수 없습니다. 고객은 글로벌 사이트와 클라우드 워크로드 간 SD-WAN 패브릭 확장을 자동화하여 클라우드 여정을 가속하고 간소화된 네트워크 운영, 엔드투엔드 암호화 보장, 발빠른 비즈니스 혁신을 위한 유연성을 활용할 수 있습니다.

또한 분산된 클라우드 및 SaaS 애플리케이션 사용으로 인해 위협 환경이 확대되고 계속 진화함에 따라 네트워크에 '제로 트러스트' 방식과 '절대 신뢰성을 가정하지 말고 항상 확인하고 최소 권한을 시행한다'는 핵심 원칙을 적용해야 합니다. 제로 트러스트 방식에 SD-WAN을 통합하면 조직이 누가 어떤 클라우드 서비스에 액세스할 수 있는지 제어하는 보안 태세를 구축하고, 허용된 트래픽에 대한 자동화된 보안 제어를 제공하며, 지속적인 시행을 제공하고, 보안 태세 변화에 따라 즉각적으로 대응할 수 있습니다."

JL Valente
시스코 SD-WAN 및 클라우드 네트워킹 제품 관리, 엔터프라이즈 라우팅 부문
VP

필수 가이드 4: 클라우드 중심 보안을 혁신하여 일관된 운영 및 정책을 구현합니다.

여러 보안 기능을 클라우드 플랫폼에서 결합하면 가시성, 정책 관리, 제어가 간소화될 뿐 아니라 범위가 확장되고 효과가 향상됩니다.

하이브리드 업무가 확산됨에 따라 사람들은 회사 소유의 디바이스와 개인 디바이스를 모두 사용하며 기업 네트워크 안팎의 매니지드 및 언매니지드 네트워크에서 점점 더 많은 애플리케이션을 소비하고 있습니다. 기존의 경계 보안으로는 더 이상 충분하지 않습니다. 따라서 IT는 모든 엔드포인트, 애플리케이션, 데이터를 보호하는 것을 최우선순위로 두고 있습니다.

전통적으로 원격 근무자에 대한 보안 정책은 온프레미스에 대한 정책과 다릅니다. 원격 보안 정책은 신뢰도 수준이 다르며 별도의 보안 툴로 관리됩니다. 개별적으로 정책을 지원하면 IT 오버헤드가 증가하고 최종 사용자에 혼란을 줄 수 있습니다. 본 연구에서 보안 정책에 대한 질문에 응답자의 **45%**는 분산된 위치에서 안전한 멀티클라우드 액세스를 제공하는 데 있어 일관되고 강력한 보안 정책이 가장 큰 과제라고 답했습니다.

보안 팀은 끊임없이 이어지는 사이버 위협에 대응할 뿐만 아니라 주기적으로 보안 정책을 업데이트해야 합니다. 분산된 인력 전체에 걸쳐 일관된 애플리케이션 보안 정책 업데이트의 필요성은 보안을 중앙 집중화해야 하는 강력한 동인입니다. 응답자의 **59%**가 향후 **24**개월 동안 최우선 클라우드 액세스 네트워킹 이니셔티브로 클라우드 보안 중앙 집중화에 주력하고 있다고 답했습니다(그림 6).

전통적인 경계 방어만으로는 부족합니다. 중앙 집중식 클라우드 보안 솔루션에 대규모로 애플리케이션 및 워크로드에 대한 액세스를 보호하는 더 효과적인 방법을 사용해야 합니다. 바로 여기에서 SASE의 핵심 요소인 SSE가 필요합니다.

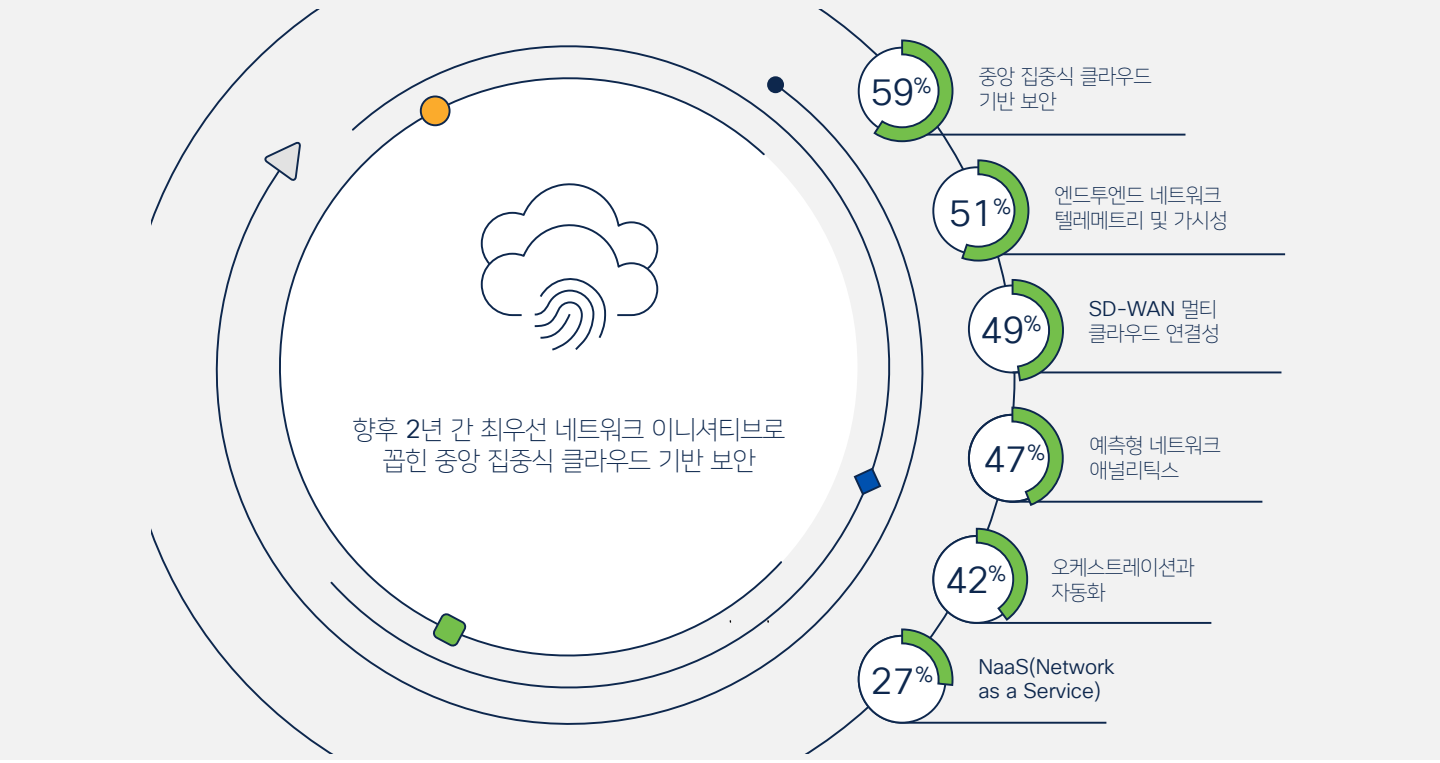


그림 6. 향후 24개월 간 최우선 클라우드 액세스 네트워크 이니셔티브

결론

원격 근무(WFA), BYOD, 클라우드 서비스의 확산으로 인해 명확하게 정해져 있던 보안 경계가 흐려졌습니다. 매일 사용되는 수많은 애플리케이션이 클라우드에 있기 때문에, 조직은 여러 보안 기능을 결합하고 이러한 기능을 클라우드에서 효과적으로 제공하는 포괄적인 SSE 전략을 설계해야 합니다.

전문가 의견

클라우드 보안 통합은 중앙 집중식 통합 모델의 핵심입니다.

" 수년 동안, 조직들은 계속해서 확장되는 위협에 대응하기 위해 포인트 보안 제품을 추가하는 방법을 선택했습니다. 그 결과 보안이 강화되기는 했지만, 운영 복잡성이 크게 증가하여 보안상 이점이 상쇄되고 있습니다. SSE 솔루션으로 전환하면 확장 가능한 클라우드 네이티브 보안 기능(Secure Web Gateway, Cloud Access Security Broker, Zero Trust Network Access, Firewall as a Service)을 통합하여 최종 사용자를 위한 경험을 개선하고, 보안을 강화하며, IT 팀의 업무 부담을 줄일 수 있습니다.

이러한 중앙 집중식 통합 방식을 선택하면 관리 업무를 간소화하고, 손쉽게 성능을 확장하며, 높은 가시성을 확보하고, 조직 전체에서 보안을 강화할 수 있습니다. 통합 SSE 솔루션은 완전한 SASE 아키텍처에 필수적입니다."

Jeff Scheaffer
시스코 보안/SSE 제품 관리 부문
VP

필수 가이드 5: 엔드투엔드 네트워크 가시성을 통해 점점 복잡해지는 디지털 서비스 제공 공급망 전체에 일관된 사용자 경험을 제공합니다.

자체 네트워크를 넘어 인터넷과 클라우드 환경으로 가시성을 확장하지 않으면 IT 팀이 클라우드 기반 애플리케이션 및 서비스를 위한 높은 품질의 일관된 사용자 경험을 제공할 수 없습니다.

사용자 경험을 향상하는 것은 IT 부서의 중요한 목표입니다. 네트워킹 팀은 원활한 경험을 제공하기 위해 기존 툴을 넘어 자체 네트워크 안팎의 상황에 대한 실시간 가시성을 확대하는 솔루션을 도입하고 있습니다. 이렇게 확장된 측정항목과 애플리케이션 성능 간의 상관관계를 파악함으로써 IT 부서는 이러한 인사이트 데이터를 활용하여 모든 직원과 고객을 위한 디지털 경험을 최적화할 수 있습니다.

조직들이 SaaS 및 클라우드 솔루션 도입을 가속하고 이러한 애플리케이션에 대한 액세스를 제공하기 위해 인터넷과 같은 공용 네트워크 사용을 확대하며, 이러한 멀티홉 네트워크가 점점 더 복잡해짐에 따라 고급 가시성 솔루션에 대한 투자가 매우 중요해졌습니다. 응답자의 절반 이상(51%)이 포괄적인 네트워크 텔레메트리 및 가시성을 주요 네트워크 이니셔티브의 최우선과제로 여기고 있습니다.

애플리케이션 트랜잭션은 여러 네트워크, 네트워크 세그먼트, 서비스를 거칠 수 있습니다(그림 7). 따라서 특정 애플리케이션의 성능과 가용성을 추적하기가 어렵습니다. 응답자의 약 절반(48%)이 연결을 향상하기 위해 인터넷 가시성 및 인사이트에 주력해야 한다고 답했습니다. 이는 IT 부서가 담당하거나 제어하지 않는 외부 네트워크와 환경을 포함한 전체 트랜잭션 경로를 파악하고 시각화할 수 있는 툴의 필요성을 더욱 강조합니다.

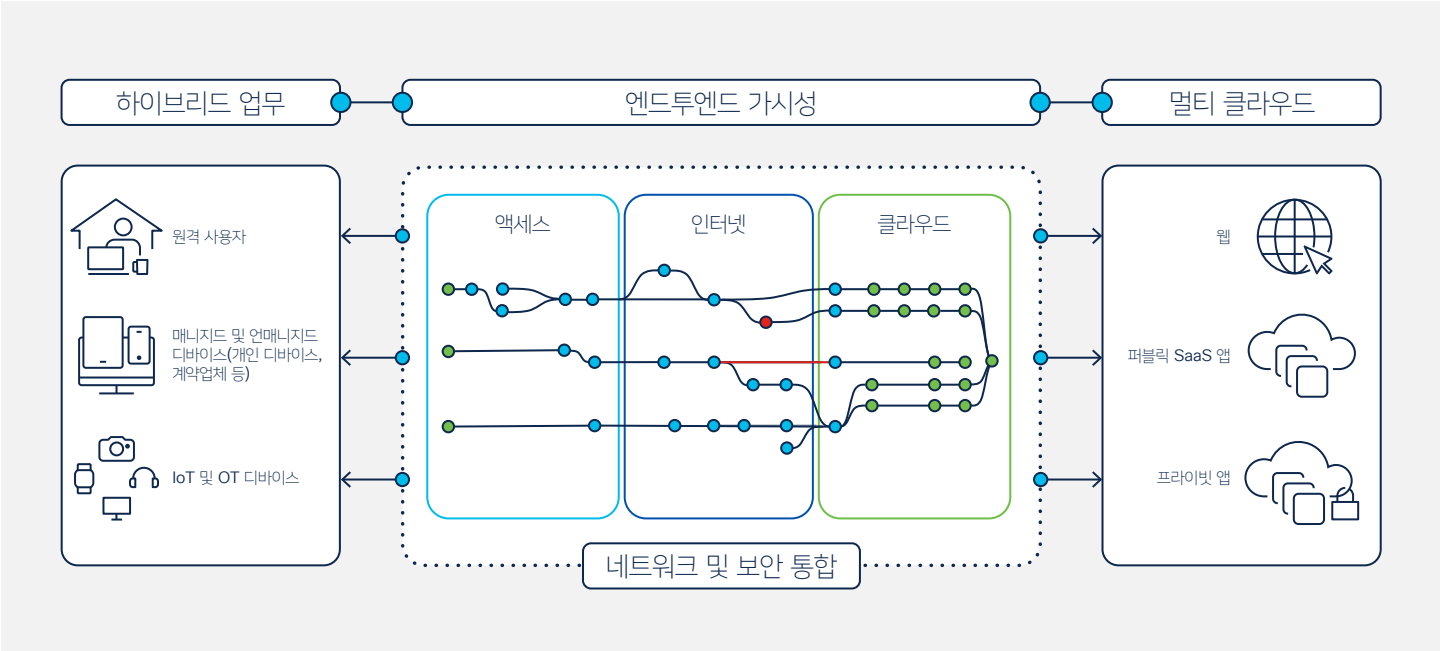


그림 7. 인터넷을 통해 분산된 환경을 연결하는 작업의 복잡성이 증가함에 따라 더욱 효과적이고 포괄적인 가시성이 필요합니다.

The bridge to possible

결론

클라우드는 새로운 데이터 센터이고, 인터넷은 새로운 네트워크이며, 클라우드 제품이 애플리케이션을 장악하고 있습니다. IT 팀은 전체적인 인터넷 상태와 주요 SaaS 애플리케이션의 성능을 파악함으로써 예기치 않은 주요 네트워크 또는 애플리케이션 문제를 사전에 감지하고 문제가 발생하는 즉시 해결할 수 있습니다.

전문가 의견

인터넷은 인프라의 새로운 중추입니다.

" 디지털 경험 공급망이 단일 도메인에서 다자간 협업 시스템 및 네트워크로 전환되었습니다. 사용자는 어디에나 존재할 수 있습니다. 애플리케이션은 API와 분산된 마이크로 서비스를 기반으로 민첩성을 제공합니다. 조직은 더욱 줄어든 제어 권한으로 다양한 애플리케이션, 서비스, 클라우드, 네트워크 전반에서 원활한 경험을 제공해야 합니다.

따라서 최신 디지털 경험에는 가시성 및 어슈어런스에 대한 새로운 접근 방식, 즉 팀이 집, 사무실, 클라우드, 인터넷 등 도메인에 상관없이 중단을 빠르게 탐지하고 진단하며 인프라와 네트워크 문제와의 상관관계를 파악할 수 있도록 지원하는 접근 방식이 필요합니다. 이를 위해서는 외부 제공업체와 함께 연결된 에코시스템 내에서 적시에 적절한 데이터에 액세스하고 애플리케이션, 네트워크, 인프라 운영에서 내부적으로 이러한 데이터를 손쉽게 수집하고 상관관계를 분석할 수 있어야 합니다."

Joe Vaccaro
Cisco ThousandEyes
제품 관리 부문 VP

필수 가이드 6: 사후 대응적 운영에서 예측적 운영으로 전환하여 가동 시간을 개선하고 성능 수준을 향상하십시오.

예측적 애널리틱스는 전반적인 IT 운영 간소화, 가속화, 효과 증진을 위한 AIOps(Artificial Intelligence for IT Operations) 툴킷의 중요한 부분 중 하나로 인식되고 있습니다.

확장된 네트워크는 조직의 비즈니스 운영에 필수적이므로, 서비스 품질이 저하되거나 다운타임이 늘어나면 큰 타격이 됩니다. IT 리더들은 문제가 발생하여 사용자 경험에 영향을 주기 전에 사전 예방적으로 문제를 파악하고 해결할 방안을 모색하고 있습니다.

다양한 클라우드 기반 관리 플랫폼이 등장함에 따라 기업은 더 많은 소스의 실시간 및 과거 텔레메트리에 광범위하게 액세스할 수 있습니다. AI/ML(Artificial Intelligence/Machine Learning) 기술을 사용한 예측적 애널리틱스가 발전함에 따라 모든 과거 및 실시간 데이터에 기반하여 실제 활용 가능한 인텔리전스를 확보할 수 있습니다. 따라서 조직이 데이터 패턴을 파악하고 문제가 네트워크에 영향을 주기 전에 정확히 예측하고 해결할 수 있습니다. 이러한 모델은 지속적인 피드백 루프를 통해 수집되는 데이터를 학습함으로써 시간이 갈수록 스마트해집니다.

응답자의 47%가 향후 2년 간 클라우드 연결 개선을 위해 예측형 네트워크 애널리틱스 도입에 주력하고 있다고 답했습니다.

사전 예방적 IT 운영은 분산된 클라우드 애플리케이션에 액세스하는 분산된 사용자에게 일관된 고성능 서비스를 제공하는 데 특히 중요해지고 있습니다. 설문 응답자들은 이를 중요한 향후 방향으로 생각하고 있습니다. 47%가 향후 2년 간 클라우드 연결 개선을 위해 예측형 네트워크 애널리틱스 도입에 주력하고 있다고 답했습니다.

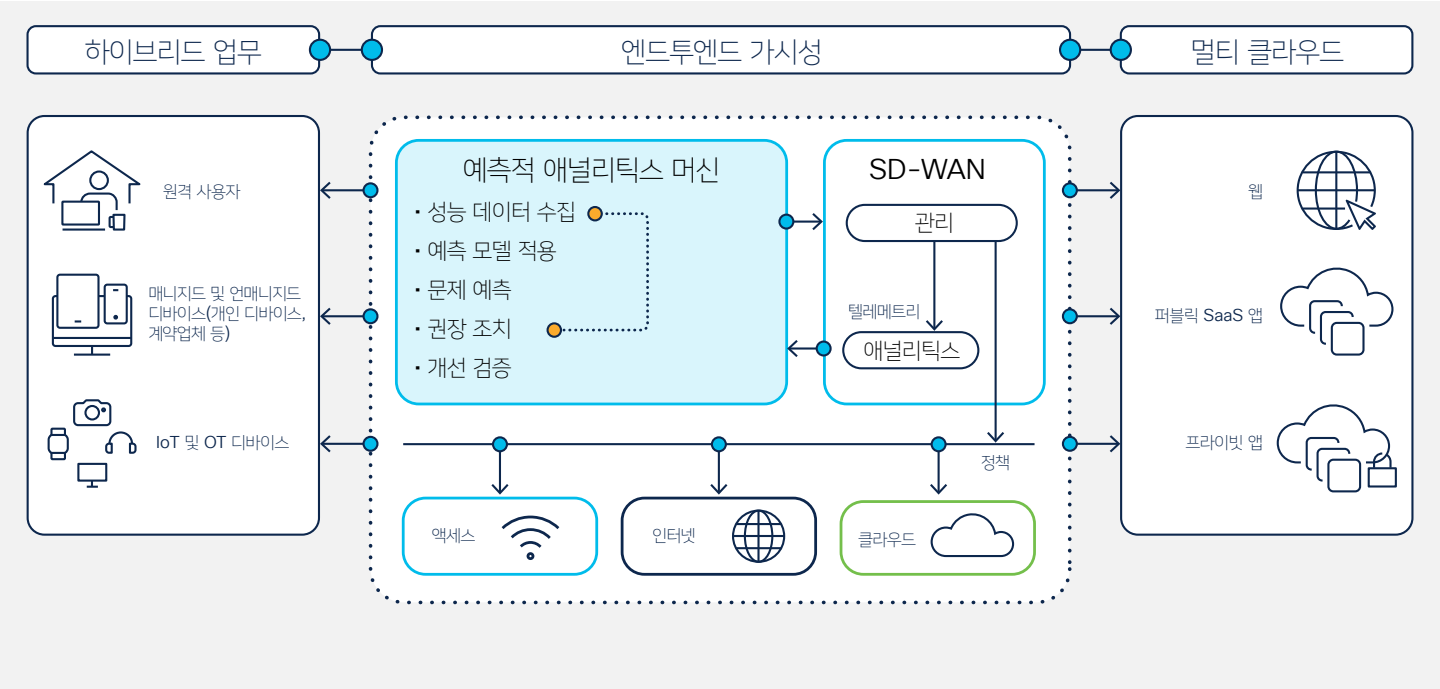


그림 8. SD-WAN 관리에 예측적 애널리틱스를 통합하여 네트워크 성능 저하가 사용자 경험에 영향을 주기 전에 파악하고 예방합니다.

The bridge to possible

결론

인터넷이 변화하고 진화함에 따라 디지털 경험의 속도, 비용, 품질은 불안정한 상태에 있습니다. 조직은 지속적인 데이터 피드백 루프를 통해 시간이 지남에 따라 최적화되는 예측 모드와 사전 예방적 운영 워크플로우를 도입하여 인프라 탄력성과 회복성을 향상시켜야 합니다.

전문가 의견

IT 팀의 필요로 인해 예측적 애널리틱스가 구현되었고, 이 기술을 활용할 수 있게 되었습니다.

" 기존의 사후 대응적 운영 모드에서는 주로 연결 문제 또는 서비스 품질 저하로 인해 발생하는 문제를 탐지한 후에야 트래픽을 다른 경로로 다시 라우팅합니다. 예측적 애널리틱스의 흥미로운 장점은 원격 분석, 통계 데이터, AI/ML 기반 컴퓨팅 모델을 사용하여 잠재적인 문제가 발생하기 전에 예측할 수 있다는 점입니다. 클라우드 중심 환경은 그 특성상 예측이 불가능합니다. 자동으로 조치를 권장하거나 트래픽을 사전 예방적으로 다시 라우팅하는 기능은 성능을 최적화하고 시스템 다운타임의 위험을 완화하는 데 매우 중요합니다. 이를 통해 사용자 경험을 개선하고 IT 부서가 사후 대응적인 분류가 아닌 전략적 이니셔티브에 집중할 수 있도록 지원함으로써 조직에 도움이 됩니다."

Murtaza Doctor
Cisco ThousandEyes
엔지니어링 부문 VP

The bridge to possible

결론

원격 근무와 하이브리드 업무는 앞으로도 계속될 것입니다. 여러 클라우드 도입이 가속화되고 있습니다. 그러나 고도로 분산된 작업자, 디바이스, 애플리케이션에 안전하고 일관된 연결을 제공하는 것은 위협 환경의 확대와 네트워킹 팀, 클라우드 팀, 보안 팀 전반의 툴 및 기술의 복잡성으로 인해 여전히 어려운 과제입니다.

이러한 팀들이 개별적으로는 연결 및 보안 과제를 해결할 수 있고 조직의 경쟁력에 필요한 디지털 경험 및 민첩성을 제공할 수도 없습니다. 대부분의 IT 리더들은 이 사실을 잘 알고 있습니다. 이들은 적극적으로 네트워킹, 클라우드, 보안 기술을 통합하고 역동적으로 변화하는 니즈를 충족하기 위한 혁신적인 운영 모델을 테스트하고 있습니다.

확실한 방법 중 하나는 SASE로 전환하는 것입니다. 설문조사 응답자의 약 절반이 2년 이내에 브랜치와 원격 클라이언트를 연결하는 긴밀히 통합한 SASE 아키텍처를 구축할 계획이라고 답했습니다. SASE가 약속하는 것은, 클라우드 애플리케이션에 대규모로 분산된 직원과 고객을 안전하게 연결하는 보다 간편하고 유연한 방식을 통해 IT 경험을 간소화하고 보호한다는 점입니다. 클라우드 기반 자동화 및 네트워크 인사이트를 지원하는 네트워킹 플랫폼과 보안 플랫폼을 결합하여 워크플로우를 통합하고 네트워크 운영 팀과 보안 운영 팀 간 협업을 증진합니다.

클라우드 중심 SASE 모델은 데이터를 활용하여 포괄적인 가시성과 예측적 애널리틱스와 같이 일관된 사용자 경험을 제공하는 데 중요한 기능을 제공합니다.

비즈니스 및 기술 우선순위에 따라 SASE 여정을 시작하는 방식은 다양합니다.

SASE에 대해 자세히 알아보고 시스코에서 SASE 여정을 어떻게 지원하는지 살펴보십시오.

보고서 정보

글로벌 네트워킹 트렌드 보고서는 북미, 남미, 아시아 태평양, 서유럽 등 13개국에서 실시한 설문조사 결과를 바탕으로 2023년 2월에 작성되었습니다.

올해 보고서에는 클라우드 서비스를 사용하는 조직 내 네트워크 운영 담당자들의 설문조사 데이터가 포함되어 있습니다. 본 보고서에서는 설문조사 데이터를 통해 멀티 클라우드 환경이 네트워크 기술 및 운영 우선순위, 선호도, 선택에 미치는 영향에 대한 인사이트를 제공합니다.

본 보고서에 참조된 설문조사 데이터는 시스코의 의뢰로 S&P Global Market Intelligence의 451 Research에서 수집하여 시스코에서 분석했습니다. 클라우드 컴퓨팅, 개발 운영, 엔터프라이즈 네트워킹을 담당하는 전 세계 IT 의사결정권자와 전문가 2,500명 이상을 대상으로 진행된 독립적인 웹 설문조사의 일환으로 진행되었습니다.

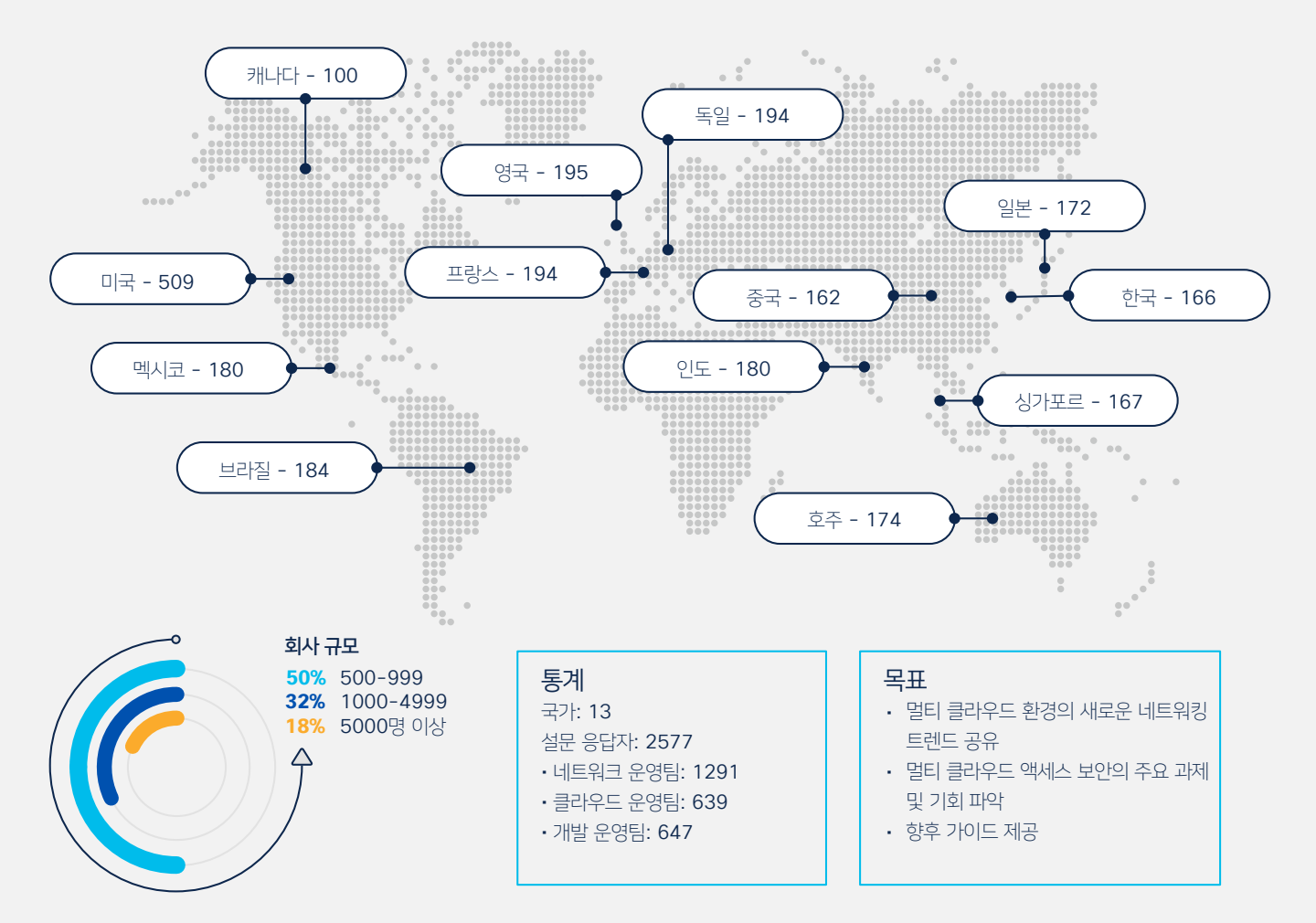


그림 9. 시스코 2023 글로벌 네트워킹 트렌드 설문조사 방법론 및 목적.