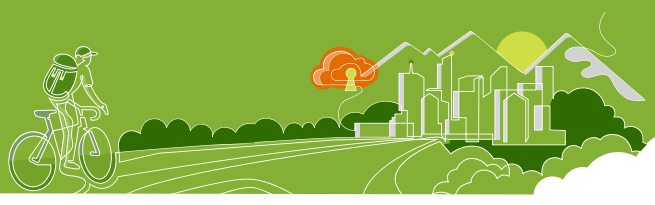

파트너
로고 공간

TOP 10 SASE 공급업체에서 확인해야 할 10가지 주요 기능

버튼 하나만 누르면 전체 네트워크 아키텍처가 SASE 아키텍처로 쉽게 전환되어 안전한 클라우드 환경이 바로 구현된다면 얼마나 좋을까요? 아쉽게도 이것은 현실적으로 어렵지만, 그렇다고 해서 전환이 꼭 복잡하거나 힘들기만 한 것은 아닙니다.

SASE 아키텍처로의 원활한 전환은 여정을 도와줄 적합한 공급업체를 찾는 것에서 시작됩니다. SASE 공급업체는 기존 투자를 활용할 수 있도록 지원하고, 경험을 바탕으로 고객이 비즈니스에 가장 적합한 속도로 원활하고 안전하게 클라우드 기반 보안으로 전환할 수 있도록 도움을 주어야 합니다.

1 통합 정책 관리

온프레미스, 내부/외부 클라우드 등 언제 어디서나 단일 UI로 보안 관리.

통합 정책 관리는 사용자, 디바이스, 애플리케이션이 어디로 이동하든 따라다니는 정책을 통해 안전한 사용자 환경을 보장해야 합니다.

2 지능형 위협에 대한 빠르고 효과적인 방어

암호화되어 보이지 않고 알려지지 않은 위협까지 모두 방어.

정적, 동적 멀웨어 탐지를 수행하여 아무리 정교하고 고도화된 위협도 탐지하여 즉시 식별하고 거의 실시간으로 차단할 수 있는 클라우드 기반 서비스를 찾으십시오.

3 복원력과 확장성

물리적, 가상, 클라우드 기반 보안 환경에 맞게 쉽고 효과적으로 확장.

최종 사용자에게 보이지 않고 사용자 경험에 부정적인 영향을 미치지 않는 광범위한 운영 간소화 및 보안이 필요합니다.

4 단일 정책 프레임워크를 갖춘 단일 스택 아키텍처

기존 투자를 비즈니스 크리티컬 클라우드 보안 서비스의 발판으로 활용.

정책을 일괄 작성하여 사용자/애플리케이션 기반 액세스, IPS, 멀웨어 방지, 보안 웹 액세스를 포함한 통합 정책 관리를 언제 어디서나 적용할 수 있습니다.

5 분산된 인력을 위한 일관된 보안

원격 근무자가 업무를 효과적으로 수행하는 데 필요한 애플리케이션과 리소스에 안전하게 액세스할 수 있도록 지원.

규칙 세트를 복제하거나 다시 만들 필요 없이 일관된 보안 정책이 사용자, 디바이스, 애플리케이션을 따라가야 합니다.

6 하이브리드 환경 지원

고객 인프라가 온프레미스인지, 클라우드인지, 아니면 두 가지를 결합한 형태인지 여부에 관계 없이 SASE 공급업체가 모든 환경을 지원할 것.

SASE 공급업체는 고객이 자사 비즈니스에 적합한 속도로 원활하고 안전하게 SASE 아키텍처로 전환할 수 있도록 지원해야 합니다.

7 신원 확인을 위한 단일 소스

시중에 나와 있는 모든 신원 확인 솔루션과 원활하게 통합.

SASE 공급업체는 고객이 자사 비즈니스 요구에 가장 적합한 신원 확인 솔루션을 선택할 수 있도록 지원해야 합니다.

8 다이나믹 유저 세그멘테이션 (DYNAMIC USER SEGMENTATION)

사용자가 어디에 있든 안전하게 보호.

사용자 추적 정책을 통합하고 세분화된 정책을 통해 위험도에 따라 자동화된 액세스 제어 기능을 제공하고 써드파티 액세스를 공격 벡터로 간주하여 차단합니다. 써드파티 액세스를 처리하여 에지의 공격 노출면을 더욱 줄입니다.

9 검증된 보안 성능

조사를 통해 보안 효과가 입증된 SASE 공급업체를 찾을 것.

SASE 공급업체는 클라이언트/서버 익스플로잇, 랜섬웨어, 봇넷, DNS 터널링 등을 포함한 위협에 대한 효과적인 방어 기능을 제공해야 합니다. 당면 위협 과제를 해결하고, 온프레미스 및 클라우드 환경의 공격을 차단하며, 서비스 형태(as-a-service)로 제공되어야 합니다.

10 고객에게 적합한 속도로 클라우드 기반 보안으로 원활하게 전환.

SASE 아키텍처 전환 시점을 결정하는 주체는 고객.

통합 정책과 직관적인 배포 마법사를 사용하여 동일한 관리 UI 내에서 고객이 원하는 속도에 맞춰 클라우드 기반 보안 아키텍처로 원활하게 전환할 수 있어야 합니다. 서비스 위치에 관계 없이 정책 서비스를 쉽고 효과적으로 오케스트레이션, 프로비저닝하고 관리하세요.

11 보너스 포인트: 보안 보장

정책 규칙을 안심하고 변경하고 정책 변경 사항이 효과적으로 적용되도록 보장합니다.

기존 방화벽 정책에 대한 규칙이든 서비스로 제공되는 정책에 대한 규칙이든 적절한 순서로 배치되어야 효과를 발휘할 수 있습니다. SASE 공급업체는 IT 팀이 이러한 규칙 세트를 파악하고 커밋 전에 중복 및 새도우 규칙을 자동으로 표시할 수 있도록 지원해야 합니다.

모든 SASE 여정은 조직에 따라 다르겠지만, 궁극적으로 이 새로운 아키텍처를 설계, 구축 및 유지 관리하여 필요할 때 필요한 사용자 경험, 서비스 및 데이터를 최적화하는 방법은 고객의 선택에 달려 있습니다. 어떤 길을 선택하든 고객이 있는 곳에서 SASE를 구현하도록 도와주고 여정의 모든 단계에 함께할 수 있는 공급업체를 찾는 것이 중요합니다.

본사 및 영업 본부

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

전화: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

팩스: +1.408.745.2100

www.juniper.net

한국주니퍼네트웍스

서울 강남구 테헤란로 142

아크플레이스 19층

(역삼동 736-1)

www.kr.juniper.net

전화: 02-3483-3400

팩스: 02-3483-3488

JUNIPER NETWORKS | Driven by Experience™

파트 번호: 3050168

TOP 10 SASE 공급업체에서 확인해야 할 10가지 주요 기능

버튼 하나만 누르면 전체 네트워크 아키텍처가 SASE 아키텍처로 쉽게 전환되어 안전한 클라우드 환경이 바로 구현된다면 얼마나 좋을까요? 아쉽게도 이것은 현실적으로 어렵지만, 그렇다고 해서 전환이 꼭 복잡하거나 힘들기만 한 것은 아닙니다.

SASE 아키텍처로의 원활한 전환은 여정을 도와줄 적합한 공급업체를 찾는 것에서 시작됩니다. SASE 공급업체는 기존 투자를 활용할 수 있도록 지원하고, 경험을 바탕으로 고객이 비즈니스에 가장 적합한 속도로 원활하고 안전하게 클라우드 기반 보안으로 전환할 수 있도록 도움을 주어야 합니다.

1 통합 정책 관리

온프레미스, 내부/외부 클라우드 등 언제 어디서나 단일 UI로 보안 관리.

통합 정책 관리는 사용자, 디바이스, 애플리케이션이 어디로 이동하든 따라다니는 정책을 통해 안전한 사용자 환경을 보장해야 합니다.

2 지능형 위협에 대한 빠르고 효과적인 방어

암호화되어 보이지 않고 알려지지 않은 위협까지 모두 방어.

정적, 동적 멀웨어 탐지를 수행하여 아무리 정교하고 고도화된 위협도 탐지하여 즉시 식별하고 거의 실시간으로 차단할 수 있는 클라우드 기반 서비스를 찾으십시오.

3 복원력과 확장성

물리적, 가상, 클라우드 기반 보안 환경에 맞게 쉽고 효과적으로 확장.

최종 사용자에게 보이지 않고 사용자 경험에 부정적인 영향을 미치지 않는 광범위한 운영 간소화 및 보안이 필요합니다.

4 단일 정책 프레임워크를 갖춘 단일 스택 아키텍처

기존 투자를 비즈니스 크리티컬 클라우드 보안 서비스의 발판으로 활용.

정책을 일괄 작성하여 사용자/애플리케이션 기반 액세스, IPS, 멀웨어 방지, 보안 웹 액세스를 포함한 통합 정책 관리를 언제 어디서나 적용할 수 있습니다.

5 분산된 인력을 위한 일관된 보안

원격 근무자가 업무를 효과적으로 수행하는 데 필요한 애플리케이션과 리소스에 안전하게 액세스할 수 있도록 지원.

규칙 세트를 복제하거나 다시 만들 필요 없이 일관된 보안 정책이 사용자, 디바이스, 애플리케이션을 따라가야 합니다.

6 하이브리드 환경 지원

고객 인프라가 온프레미스인지, 클라우드인지, 아니면 두 가지를 결합한 형태인지 여부에 관계 없이 SASE 공급업체가 모든 환경을 지원할 것.

SASE 공급업체는 고객이 자사 비즈니스에 적합한 속도로 원활하고 안전하게 SASE 아키텍처로 전환할 수 있도록 지원해야 합니다.

7 신원 확인을 위한 단일 소스

시중에 나와 있는 모든 신원 확인 솔루션과 원활하게 통합.

SASE 공급업체는 고객이 자사 비즈니스 요구에 가장 적합한 신원 확인 솔루션을 선택할 수 있도록 지원해야 합니다.

8 다이나믹 유저 세그멘테이션 (DYNAMIC USER SEGMENTATION)

사용자가 어디에 있든 안전하게 보호.

사용자 추적 정책을 통합하고 세분화된 정책을 통해 위험도에 따라 자동화된 액세스 제어 기능을 제공하고 써드파티 액세스를 공격 벡터로 간주하여 차단합니다. 써드파티 액세스를 처리하여 에지의 공격 노출면을 더욱 줄입니다.

9 검증된 보안 성능

조사를 통해 보안 효과가 입증된 SASE 공급업체를 찾을 것.

SASE 공급업체는 클라이언트/서버 익스플로잇, 랜섬웨어, 봇넷, DNS 터널링 등을 포함한 위협에 대한 효과적인 방어 기능을 제공해야 합니다. 당면 위협 과제를 해결하고, 온프레미스 및 클라우드 환경의 공격을 차단하며, 서비스 형태(as-a-service)로 제공되어야 합니다.

10 고객에게 적합한 속도로 클라우드 기반 보안으로 원활하게 전환.

SASE 아키텍처 전환 시점을 결정하는 주체는 고객.

통합 정책과 직관적인 배포 마법사를 사용하여 동일한 관리 UI 내에서 고객이 원하는 속도에 맞춰 클라우드 기반 보안 아키텍처로 원활하게 전환할 수 있어야 합니다. 서비스 위치에 관계 없이 정책 서비스를 쉽고 효과적으로 오케스트레이션, 프로비저닝하고 관리하세요.

11 보너스 포인트: 보안 보장

정책 규칙을 안심하고 변경하고 정책 변경 사항이 효과적으로 적용되도록 보장합니다.

기존 방화벽 정책에 대한 규칙이든 서비스로 제공되는 정책에 대한 규칙이든 적절한 순서로 배치되어야 효과를 발휘할 수 있습니다. SASE 공급업체는 IT 팀이 이러한 규칙 세트를 파악하고 커밋 전에 중복 및 새도우 규칙을 자동으로 표시할 수 있도록 지원해야 합니다.

모든 SASE 여정은 조직에 따라 다르겠지만, 궁극적으로 이 새로운 아키텍처를 설계, 구축 및 유지 관리하여 필요할 때 필요한 사용자 경험, 서비스 및 데이터를 최적화하는 방법은 고객의 선택에 달려 있습니다. 어떤 길을 선택하든 고객이 있는 곳에서 SASE를 구현하도록 도와주고 여정의 모든 단계에 함께할 수 있는 공급업체를 찾는 것이 중요합니다.

본사 및 영업 본부

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

전화: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

팩스: +1.408.745.2100

www.juniper.net

한국주니퍼네트웍스

서울 강남구 테헤란로 142

아크플레이스 19층

(역삼동 736-1)

www.kr.juniper.net

전화: 02-3483-3400

팩스: 02-3483-3488

Driven by Experience™

3050168-001-KO 2023년 8월