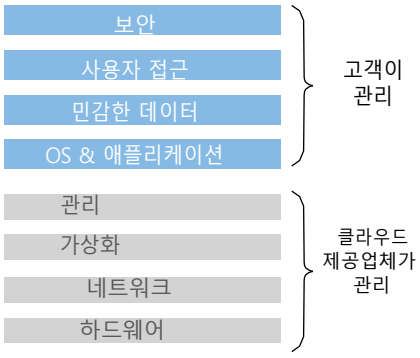
Kaspersky®
Cloud Security

Kaspersky Cloud Security 솔루션으로 더욱 안전한 Amazon 클라우드

하이브리드 클라우드 보호를 위해 Kaspersky Lab을 선택해야 하는 이유:

- **수상 경력이 가장 많은 보안 솔루션**으로 하이브리드 클라우드에 최적화되어 있습니다.
- **시스템 효율성을 유지하는 동시에** 클라우드의 보안 상황을 완벽하게 파악하고 관리할 수 있습니다.
- **향상된 기능을 제공합니다.** 애플리케이션, 웹 및 기기 제어를 비롯하여 고급 사이버 위협 및 랜섬웨어 공격을 방지하는 기능 등 다양한 고급 기능이 포함됩니다
- **기업 인프라와 긴밀하게 연동하는** 솔루션입니다.
- **리소스는 물론 운영 비용이 크게 절감**되어 하이브리드 클라우드 환경의 효율성을 높일 수 있습니다.

퍼블릭 클라우드 환경의 보안 책임 공유



Amazon과 Kaspersky Lab을 통한 하이브리드 클라우드 보안 구현

데이터 관리 및 스토리지에 하이브리드 클라우드 방식을 채택하면 자체 가상 환경과 하나 이상의 퍼블릭 클라우드 간에 워크로드가 자유롭게 이동하기 때문에 새로운 보안 문제가 대두하게 됩니다. 그러나 데이터가 사내 환경 또는 외부 환경 등 어디서 실행되든 기업과 디지털 자산, 비즈니스 연속성, 소속 직원을 효과적으로 안전하게 보호한다는 전반적 목표는 항상 동일할 것입니다.

프라이빗 클라우드 방식에서 하이브리드 클라우드 방식으로 전환하면 책임 모델도 달라집니다. 인프라, 하드웨어, 네트워크, 가상 레이어 등의 퍼블릭 클라우드 보안은 서비스 공급업체에서 관리하고 사용자는 클라우드에 담긴 내용, 즉 워크로드, 운영 시스템, 데이터, 애플리케이션 등의 보안을 담당합니다. 또한 직원의 사이버 안전을 비롯하여 보안 솔루션이 기업의 사이버 보안 목표에 부합하도록 하는 것도 사용자가 책임져야 합니다.

아마존 웹 서비스(AWS)는 안정적이고 확장 가능하며 경제적인 퍼블릭 클라우드 환경을 제공합니다. 가상 컴퓨터(VM)와 워크로드는 Kaspersky Cloud Security를 통해 보호되고, 가상 인프라의 운영 기반에 관계없이 동일한 보안 수준과 정책이 적용됩니다. 또한 단일 운영 콘솔을 통해 전체를 완벽하게 파악하고 한꺼번에 관리할 수 있습니다.

이 문서에서는 Kaspersky Cloud Security를 AWS 클라우드 리소스로 확장하여 하이브리드 클라우드 전체에 걸쳐 손쉽게 고급 보안 기능과 완벽한 VM 가시성, 통합 운영 기능을 활용하는 방법을 설명합니다.

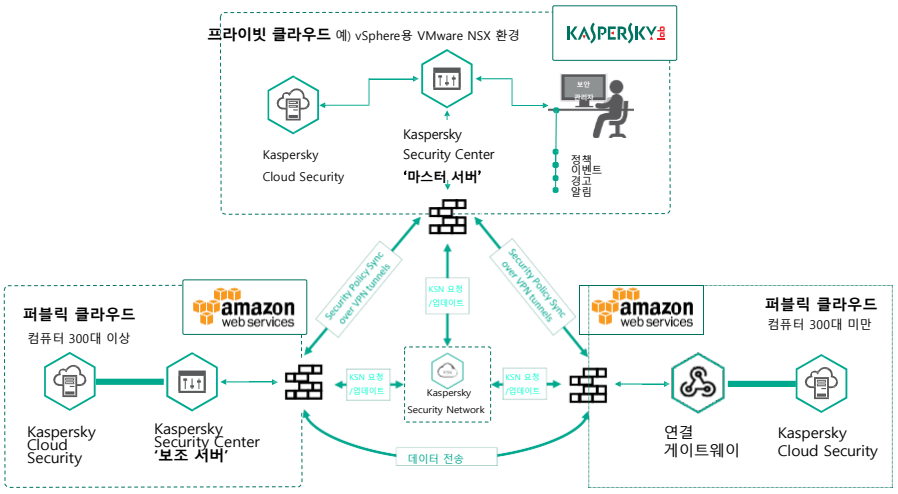


그림 1. Amazon 웹 서비스와 Kaspersky Cloud Security를 연동한 하이브리드 클라우드 환경 보호

일반적으로 권장되는 모범 사례는 공용 인터넷을 통해 표준 방식으로 클라우드 간 통신을 수행하는 것입니다. Kaspersky Lab에서는 프라이빗 클라우드 인프라와 퍼블릭 클라우드 인프라 간에 **안전한 암호화 채널**(VPN 터널)을 배포하여 가장 높은 수준의 보안 및 프라이버시 보호 기능을 확보할 것을 적극 권장하고 있으며, 이러한 용도로 Amazon Virtual Private Cloud Network 및 Amazon Virtual Private Gateway가 적합합니다.

Kaspersky Security Center 10 버전 이상에서 지원합니다.

또한 위 다이어그램과 같이 **네트워크 인프라**가 인프라 구성 요소 간 통신이 가능하도록 올바르게 구성되어 있는지도 확인해야 합니다. 네트워크 포트 및 방화벽 규칙 설정 방법에 대해 자세한 내용은 Kaspersky Security Center 구현 설명서를 참조하십시오.

AWS 클라우드 기반 운영 규모에 따라 Kaspersky Cloud Security 솔루션을 배포하는 방법은 2가지로 나눌 수 있습니다. 두 방법 모두 매우 간단합니다.

하이브리드 클라우드 보안: AWS 클라우드 + 프라이빗 클라우드

AWS 클라우드 내 VM이 300대 미만

퍼블릭 클라우드 규모가 VM 300대 미만일 경우 Kaspersky Cloud Security를 하이브리드 클라우드에 적용하는 데 필요한 작업은 연결 게이트웨이의 배포뿐입니다. 이를 통해 퍼블릭 클라우드 내의 보호되는 VM이 일반적인 프라이빗 클라우드 기반의 '마스터' Kaspersky Security Center에 직접 연결되므로 모든 VM이 보안 정책, 업데이트, 라이센스 정보를 수신할 수 있습니다.

연결 게이트웨이를 사용하면 AWS 퍼블릭 클라우드 내의 보호되는 여러 VM이 '마스터' Kaspersky Security Center 서버에 직접 연결되어 보안 정책, 업데이트, 라이센스 정보를 수신합니다. 필요한 경우 안티 맬웨어 업데이트를 비롯하여 통계 및 판정 검사 기능도 클라우드 기반 글로벌 서비스인 Kaspersky Security Network (KSN)에서 다운로드할 수 있습니다.

AWS 클라우드 기반 VM 한 대에 Kaspersky Network Agent를 설치하여 프라이빗 클라우드의 '마스터' Kaspersky Security Center IP 주소를 지정하기만 하면 됩니다. 그 VM은 이제 '연결 게이트웨이'가 되어, 토폴로지 수집 프로세스 중에 발견된 AWS 클라우드의 다른 모든 VM을 '마스터' Kaspersky Security Center에 연결할 수 있습니다.

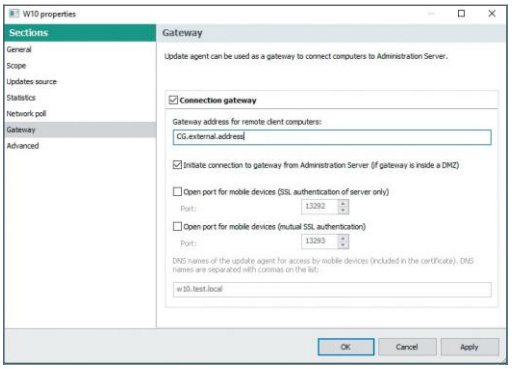


그림 2. 연결 게이트웨이 구성 설정

AWS 클라우드 내 VM이 300대 이상

'보조' Kaspersky Security Center 서버를 사용하는 경우 해당 '보조' 서버는 '마스터' 서버에서 모든 정보를 수신한 후에 AWS 퍼블릭 클라우드 내의 보호되는 VM에 모든 보안 정책과 업데이트, 라이센스 정보를 중앙집중식으로 배포합니다. 이렇게 하면 대규모 작업 환경에서 클라우드 간 네트워크 사용량이 크게 줄어듭니다.

퍼블릭 클라우드에 VM이 300대 이상인 경우에는 연결 게이트웨이보다는 '보조' Kaspersky Security Center 서버를 추가로 배포하여 모든 VM이 항상 안전하게 작동할 수 있도록 이중화 구조를 충분히 확보해야 합니다. 배포 마법사를 사용하여 손쉽게 '보조' Kaspersky Security Center 서버를 AWS 클라우드 기반 VM에 배포할 수 있습니다.

이제 양쪽 클라우드의 VM에 대한 보안은 '보조' Kaspersky Security Center 서버 또는 연결 게이트웨이를 통해 관리할 수 있습니다. 모든 운영은 프라이빗 클라우드 내의 '마스터' Kaspersky Security Center 서버를 통해 이루어집니다.

프라이빗 클라우드 외에 2개 이상의 퍼블릭 클라우드를 사용하는 경우 별도의 연결 게이트웨이와 '보조' Kaspersky Security Center 서버(필요한 경우)를 각 퍼블릭 클라우드의 VM에 설치해야 합니다.

이제 준비 작업은 끝입니다. 프라이빗 클라우드와 퍼블릭 클라우드 모두에서 VM을 바로 관리할 수 있습니다. 보호하려는 VM에 Kaspersky Cloud Security 에이전트를 배포하기만 하면 됩니다. 그러면 Kaspersky Security Center 통합 운영 콘솔을 통해 하이브리드 클라우드 전체에서 고급 보안 기능과 제어 기능을 적용하고 관리할 수 있습니다.

그림 3. KSC에서 '보조' 서버 역할 구성 설정

결과:

- 프라이빗 클라우드에서 퍼블릭 클라우드로 보안 정책을 설정하거나 배포하는 작업, 안티 맬웨어 데이터베이스 업데이트 구성, 보안 모니터링, 모든 VM에 대한 운영 리포트 작성 등의 작업을 모두 중앙집중식으로 한꺼번에 수행할 수 있습니다.
- AWS 퍼블릭 클라우드의 가상 자산도 프라이빗 클라우드 환경 수준으로 안전하게 보호되며 하이브리드 클라우드 인프라는 시스템 성능에 영향을 미치지 않으면서도 최적의 효율성으로 작동됩니다.
- 하이브리드 클라우드 전체에 대한 운영은 프라이빗 클라우드와 마찬가지로 단일 인터페이스를 통해 수행됩니다.

하이브리드 클라우드 보안: 퍼블릭 클라우드만 여러 개인 경우

퍼블릭 클라우드만 여러 개 있고 프라이빗 클라우드는 포함하지 않도록 하이브리드 클라우드를 구성하여 퍼블릭 인프라를 나머지 IT 부문으로부터 격리할 수 있습니다. 이 경우 VM은 AWS는 물론 Microsoft Azure 또는 Managed Hybrid Cloud Hosting 등 하나 이상의 다른 퍼블릭 클라우드에도 상주할 수 있습니다.

여기서도 **Kaspersky Cloud Security**를 사용할 수 있습니다. 최적의 보호 기능과 함께 엔터프라이즈급 관리 기능과 가시성을 모두 활용할 수 있으므로 퍼블릭 클라우드 위치에 관계없이 각각의 VM이 모두 완벽하게 보호됩니다.

프라이빗 클라우드 기반의 '마스터' Kaspersky Security Center 서버를 사용하고 있지 않으므로 이번 배포 프로세스에는 한 단계가 더 추가됩니다. 어느 한 퍼블릭 클라우드의 VM에 '마스터' Kaspersky Security Center 서버를 설치해야 합니다.

그런 다음 위에서 위에서 언급한 '퍼블릭 + 프라이빗' 하이브리드 클라우드의 경우와 마찬가지로 사용하는 다른 퍼블릭 클라우드에 각기 연결 게이트웨이를 설치합니다. 해당 클라우드에 VM이 300대 이상인 경우 '보조' Kaspersky Security Center 서버를 설치합니다. 마지막으로 모든 위치의 보호해야 할 VM 전체에 Kaspersky Cloud Security를 다시 한 번 설치합니다.

이제 '보조' Kaspersky Security Center 서버 또는 연결 게이트웨이를 통해 모든 퍼블릭 클라우드의 VM을 한꺼번에 관리할 수 있으며, 동시에 '마스터' Kaspersky Security Center 서버에서 제공하는 단일 인터페이스를 통해 모든 주요 보안 작업을 운영할 수 있습니다.

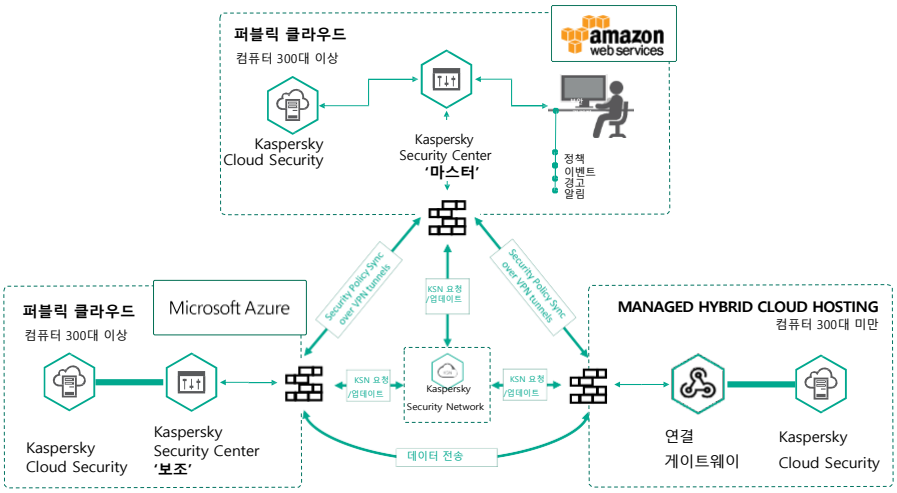


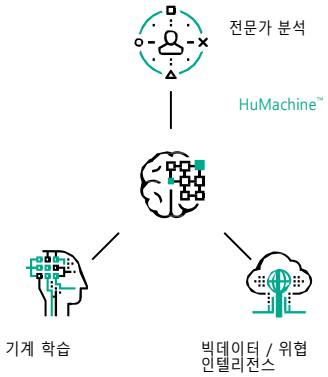
그림 4. 퍼블릭 클라우드로만 구성된 하이브리드 클라우드

하이브리드 클라우드 보안 요약

Kaspersky Cloud Security 솔루션은 하이브리드 클라우드가 제공하는 기술적 장점을 최대한 활용하도록 설계되어 인프라 변화에 동적으로 대응하고 강력한 보안 기능을 제공하며 최적의 속도와 리소스 효율성을 갖추고 있습니다. 운영 방식과 관계없이 모든 물리적 엔드포인트 및 가상 엔드포인트에 대한 통합 보안 관리 기능과 함께 탁월한 보호 기능을 제공하므로 하이브리드 클라우드 프로젝트를 각자에게 맞는 속도로 원활하고 안전하게 진행하면서도 IT 리소스에 대한 부담은 덜 수 있습니다.

Kaspersky Cloud Security에 대해 자세한 내용은 웹사이트를 참고하십시오.

www.kaspersky.com/cloud-security



카스퍼스키 랩
기업 사이버 보안: **www.kaspersky.com/enterprise**
사이버 위협 뉴스: **www.securelist.com**
IT 보안 뉴스: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.co.kr