Red Hat

# 클라우드 컴퓨팅이 보안을 지원하는 6가지 방식

클라우드 컴퓨팅이 도입되는 현재 상황에서, 조직은 클라우드 환경을 활용하며 비용 효율성, 확장성, 편의성을 얻을지 아니면 데이터와 애플리케이션을 자체 서버에서 안전하게 호스팅할지 결정해야 합니다. 그런데 온프레미스가 정말 클라우드 컴퓨팅보다 안전할까요? 전문가들의 의견에 따르면 그렇지 않습니다. 클라우드 컴퓨팅으로 전환하는 것이 좋은 6가지 이유를 함께 알아보겠습니다.

## 1 보안의 값비싼 비용

보안에는 돈이 듭니다. 귀하의 기업에서 얼마나 많은 비용을 감당할 수 있을까요? 온프레미스 데이터센터에 필요한 보안을 배포하는 비용은 중소기업에 매우 부담스럽습니다. 하이퍼스케일러가 고객에게 제공할 수 있는 것과 비슷한 수준의 보안을 달성하기란 거의 불가능합니다.

## 2 보안에 필요한 상당한 인적 자원

또한 보안에는 많은 인적 자원이 들어갑니다. 대규모 클라우드 제공업체는 1년 365일 가동되는 보안 팀과 전면적인 보안 운영 센터를 갖추어 IT 인프라스트럭쳐와 물리적 하드웨어를 지속적으로 모니터링합니다. 예를 들어 Microsoft Azure는 3,500명 이상의 사이버 보안 전문가로 구성된 팀이 보호하고 관리합니다. 그러나 대부분의 조직에는 하이퍼스케일러와 같은 수준의 보안을 제공할 만한 인력이 없습니다.

## 3 보안이 곧 비즈니스인 클라우드 제공업체

기업에서 보안을 아무리 신경 써도 비즈니스는 아니기 때문에 한계가 있습니다. 보안은 일반 기업에는 여러 고려 사항 중 하나이지만, 클라우드 제공업체에는 최고 우선순위 중 하나입니다. 경쟁력 유지를 위해서 고객에게 가능한 한 강력한 보안을 제공해야 하기 때문이죠. 예를 들어 Google Cloud는 보호 및 암호화가 기본적으로 제공되는 '보안을 고려하여 설계된 인프라'를 제공합니다.[1]

Microsoft Azure는 '180억 개의 Bing 웹 페이지, 4,000억 개의 이메일, 10억 개의 Windows 기기 업데이트, 머신 러닝을 활용한 4,500억 개의 월간 인증, 행동 분석, Microsoft Intelligent Security Graph의 일부분인 애플리케이션 기반 인텔리전스를 포함한 폭넓은 소스를 분석'하여 위협을 식별합니다.[2]

클라우드 제공업체는 여러 가지 엄격한 프로그램을 통해 보안 인력, 프로세스, 기술을 독립적이고 세계적으로 인정받은 방식으로 인증하고 감사하여 최고 수준의 표준도 충족해야 합니다. 예를 들어 AWS(Amazon Web Services)는 정기적으로 수천 개의 글로벌 컴플라이언스 요구 사항에 대해 제3사 검증을 수행합니다. 대부분의 조직에는 이 정도의 보안 검증을 수행할 만한 시간, 리소스, 예산이 없습니다.[3]

1 *"Trust and security."* Google, 2022년 4월 29일 액세스.

2 *"Strengthen your security posture with Azure."* Azure, 2022년 4월 29일 액세스.

3 *"AWS cloud security."* Amazon, 2022년 4월 29일 액세스.

## 4 고급 보안 툴

클라우드 제공업체는 고객 애플리케이션과 데이터를 보호하기 위해 다양한 고급 보안 툴을 배포합니다. AWS는 정교한 Identity 및 액세스 관리, 지속적인 모니터링, 위협 탐지, 네트워크 및 애플리케이션 보호, 다중 암호화 계층, 자동 인시던트 대응 및 복구 등을 제공합니다. 하이퍼스케일러는 파트너 마켓플레이스에 있는 수백 개의 추가적인 보안 솔루션에 대한 액세스를 제공합니다. 자체 네트워크 및 데이터센터에 이처럼 방대한 고급 보안 툴을 복제하는 것은 사실상 불가능합니다. 보안에 특화되지 않은 기업에는 여기에 필요한 비용, 인력, 시간, 노력이 너무 과하기 때문입니다.

## 5 네트워크 분리

클라우드 환경에 내재된 보안 관련 이점은 사용자 워크스테이션으로부터의 분리입니다. 사이버 공격의 일반적인 방법은 이메일 및 웹사이트를 통해 시스템상 특정 사용자를 표적으로 하는 것인데, 이 경우 사용자 워크스테이션을 통해 시스템으로의 진입이 이루어집니다. 하지만 클라우드 환경에서는 사용자 워크스테이션이 사용자가 작업을 수행하는 데 필요한 정도로만 연결해 줍니다. 워크스테이션이 기업 네트워크에 직접 액세스할 수 없다는 뜻입니다. 따라서 워크스테이션이 침해되더라도 공격자는 기업과 그 애플리케이션 및 데이터에 액세스할 수 없습니다.

## 6 물리적 보안

물리적 보안은 언제나 중요한 요인입니다. 하드웨어에 물리적으로 직접 액세스할 수 있다면 잠재적으로 심각한 보안 위험이 될 수 있습니다. 그러나 데이터와 애플리케이션이 클라우드 환경에 있다면, 회사에 불만을 가진 직원이나 우발적인 피해를 유발할 수 있는 현장 작업자가 더 이상 이러한 자산에 액세스할 수 없습니다. 클라우드 환경에 있는 데이터를 찾는 것은 훨씬 어렵기 때문입니다.

추가로 하이퍼스케일러는 보안 요원, 서버 케이지, 그리고 대부분의 조직에 없는 최첨단 물리적 보안 제어를 포함하여 물리적 데이터 도난을 방지할 수 있는 리소스를 보유하고 있습니다.

**자세히 보기**

"Empowering developers through cloud services(클라우드 서비스를 통한 개발자 역량 강화)"를 읽고 Red Hat® Cloud Services를 통해 클라우드 네이티브 애플리케이션 여정을 헤쳐 나갈 수 있는 방법에 대한 다양한 인사이트를 확인하세요.

한국레드햇 홈페이지 https://www.redhat.com/ko

**Red Hat 소개**

Red Hat은 권위 있는 어워드를 수상한 지원, 교육, 컨설팅 서비스로 고객이 여러 환경에서 표준화를 진행하고, 클라우드 네이티브 애플리케이션을 개발하고, 복잡한 환경을 통합, 자동화, 보안, 관리할 수 있도록 지원합니다.

www.facebook.com/redhatkorea
구매문의 02-6105-4390
buy-kr@redhat.com

www.redhat.com/ko
#F31540_0522