

Hillstone Networks CloudHive 솔루션으로 클라우드 기반 캠퍼스를 보호하는 베이징대학

고객

베이징대학(Peking University)은 중국 베이징에 위치한 중국 최고의 교육 및 연구 대학입니다. 1898년에 북경 제국 대학(Imperial University of Peking)으로 설립된 중국 최초의 현대적인 국립 대학교인 이 대학은 30개 단과대학과 12개 학부에 걸쳐 약 35,950명의 학생과 6,441명의 교직원을 보유하고 있습니다.

해결 과제

급증하는 네트워크 트래픽을 유연한 방식으로 지원하기 위해 베이징대학은 물리적 네트워크 인프라를 클라우드 플랫폼으로 변환하는 VMware v5.5 기반의 프라이빗 클라우드를 구축하여 대학교의 직원 및 학생에게 서비스를 제공하고 있습니다. 약 500개의 가상 머신을 실행하는 30개의 물리적 호스트가 각 학과에 클라우드 컴퓨팅 서비스를 제공하며, 각 학과에는 가상 머신, 스토리지 및 네트워킹을 포함한 자체 가상 리소스가 할당됩니다. 웹 메일, 온라인 수강 신청 시스템, 온라인 강의 등 대부분의 애플리케이션이 이 클라우드 플랫폼으로 마이그레이션되었습니다. 경계에 강력한 방어 시스템을 구현했음에도 불구하고 IT 팀은 클라우드 내부 트래픽(횡방향 트래픽)에 대한 가시성과 보안 제어가 없다는 점에 대해 우려했습니다.

보안 영역은 기존 네트워크 환경의 물리적 장치로 분할되지만 가상화된 환경에서는 네트워크 경계가 없으며, 기존 보안 솔루션으로는 클라우드 내부의 세그먼테이션이 불가능합니다. 따라서 한 가상 머신이 악성 코드에 감염되면 측면 이동을 통해 다른 가상 머신도 감염됩니다.

Hillstone Networks CloudHive 솔루션으로 클라우드 기반 캠퍼스를 보호하는 베이징대학

솔루션

Hillstone은 CloudHive를 제공하여 보안 팀이 클라우드 내부에 대한 가시성을 확보하고 악성 코드의 측면 이동을 방지할 수 있도록 했습니다. CloudHive는 기존의 네트워크 배치를 변경하지 않고 Layer 2에 구현할 수 있는 매우 간단한 방법을 제공했습니다. CloudHive를 통해 베이징대학의 IT 팀은 다음과 같은 이점을 누릴 수 있었습니다.

- 가상 머신 간 트래픽에 대한 가시성을 제공하고 트래픽으로부터 애플리케이션을 식별하는 CloudHive 애플리케이션 식별 엔진을 사용합니다. CloudHive의 통찰력 있는 기능을 통해 애플리케이션과 보안 위협, 시간 및 가상 머신 간의 관계를 분석하여 토폴로지 형식으로 표현합니다.
- CloudHive 마이크로 세그먼테이션 기술을 통해 IT 팀은 가상 머신 간 다차원의 세분화된 액세스 제어를 실행하여 가상 머신을 보호하고 가상 머신에서 시작되는 공격을 차단합니다.
- CloudHive IPS 엔진을 사용하여 가상 머신이 감염된 이후 가상 머신 간 악성 코드의 확산을 효과적으로 방지합니다.

결론

베이징대학의 IT 팀은 Hillstone Networks의 보안 솔루션을 사용하여 클라우드 내부의 모든 보안 요구사항을 해결할 수 있었으며, 그 결과 대학은 안심하고 우수한 학업 환경을 조성하는 데 집중할 수 있었습니다.

