AKAMAI 솔루션 설명서

세그멘테이션을 통한 사용자 ID 접속 관리

최신 하이브리드 데이터 센터를 위한 추가적인 중요 통제 레이어

오늘날 IT 환경의 공격표면을 줄이는 작업은 단순히 특정 애플리케이션에 대한 강력한 제어를 구축해 링펜싱하는 것 이상의 의미를 갖습니다. 공격표면의 축소는 훌륭한 첫 단계이며, 유출 격리 또는 컴플라이언스와 같은 일부 사용 사례에 확실히 큰 도움이 됩니다. 그러나 사용자 ID 접속 관리를 지원하는 세그멘테이션 솔루션이 없으면, 네트워크를 사용하거나 네트워크에 들어오는 모든 사용자를 포함한 기업의 보안 사각지대가 생깁니다.

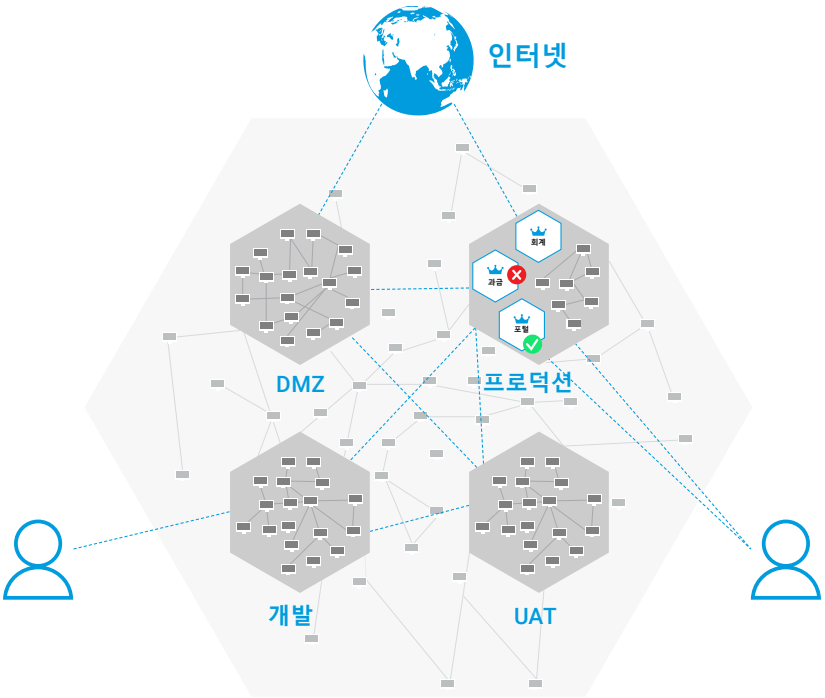
애플리케이션 세그멘테이션이 구축되면 다음으로 수행할 필수 단계는 세그멘테이션 솔루션을 활용해 이러한 애플리케이션에 접속할 수 있는 사용자를 위한 정책을 수립함으로써 네트워크 전반의 모든 아키텍처에서 보안을 유지하는 것입니다.

사용 사례: 사용자 ID 접속을 위한 세그멘테이션

사용자 접속 관리

Akamai Guardicore Segmentation은 Active Directory 사용자 그룹을 사용해 모든 환경에서 모든 애플리케이션 또는 워크로드에 대한 사용자 접속을 제어할 수 있습니다. 특정 사용자 그룹은 특정 포트 또는 프로세스를 통해 특정 서버에 접속할 수 있는 반면, 다른 그룹은 접속할 수 없습니다. 사용자 그룹에는 고유한 권한이 있지만 다른 모든 접속은 차단될 수 있습니다. 중앙 집중식 방화벽을 구축하지 않고도 네트워크의 특정 세그먼트에 있는 워크로드 간에 정밀한 접속 제어를 적용할 수 있습니다.

사용자 접속 제어



사용자 접속 제어를 위해 세그멘테이션이 필요한 이유

어디서나 사용자 접속 제어
노트북, 데스크톱, VDI, 가상 또는 베어 메탈 서버, 클라우드 인프라 전반에서 정책 적용

소프트웨어 정의 세그멘테이션
네트워크 또는 아키텍처 변경, 케이블, 서버 가동 중단, 시스템 재부팅이 필요하지 않음

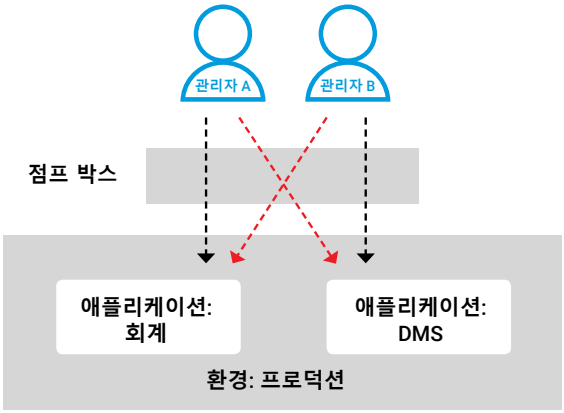
빠르고 강력한 정책
정책은 간단하고 직관적으로 만들 수 있으며, 새 세션과 활성 세션 모두에 즉시 적용됨

비용 효율성
기존의 점프 박스 인프라를 이용하던 유사한 사용 사례와 비교했을 때 비용 효율적임, 최대 60% 비용이 절감됨

Akamai

동시 사용자 접속 처리

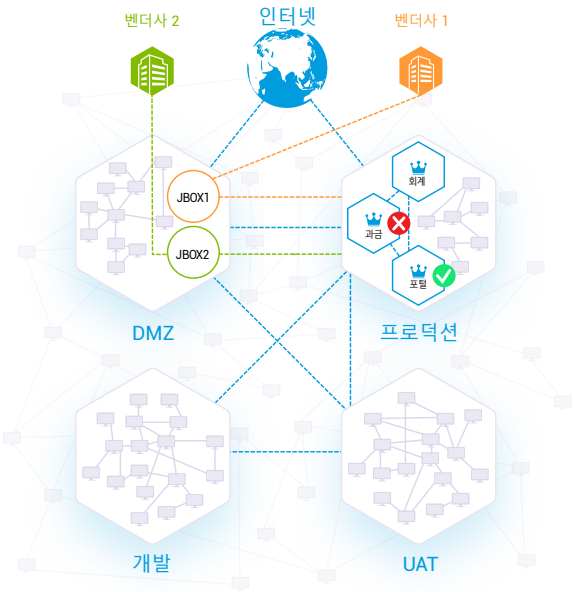
관리자는 동시에 로그온한 경우에도 동일한 점프 박스 또는 터미널 서버를 통해 여러 애플리케이션에 접속할 수 있습니다. 이와 동시에 개별 정책들이 원활하게 작동하므로 해당 접속 권한이 있는 항목에는 접속을 허용하면서 사용자의 서비스나 접속 권한에 아무런 지장을 주지 않고 다른 사용자의 접속은 계속 차단할 수 있습니다.



써드파티 접속 제어

Akamai Guardicore Segmentation은 사용자 ID를 기반으로 외부 벤더사 또는 SaaS 공급업체 등의 써드파티 접속 관리를 제어할 수 있습니다. 사용자 그룹을 이용해 각 써드파티 연결은 데이터 센터와 특정 애플리케이션 모두에 대해 고유한 접속 정책을 정의할 수 있으므로 사용자에게 업무 수행에 필요한 권한만 부여할 수 있습니다.

써드파티 접속 제어



애플리케이션 세그멘테이션 및 사용자 ID 접속 관리를 함께 사용하면 최신 기업 데이터 센터를 보호할 수 있는 가장 강력한 수단을 갖출 수 있습니다.

함께 사용하는 방식에 대해 알고 싶으신가요? Akamai 전문가에게 문의하세요.