

직원 및 벤더 원격 액세스를 관리 및 감사하세요.

Privileged Remote Access가 함께합니다.

오늘날의 기업들은 IT 환경의 무한한 경계 확장으로 인해 점점 더 복잡해지는 네트워크에 대한 액세스를 관리해야 합니다. IaaS(Infrastructure-as-a-Service), 내부 클라우드 리소스, 웹 기반 관리 콘솔 등을 포함한 최근의 IT 환경은 여러 타사 벤더 및 원격 직원의 액세스가 필요합니다. 부적절하게 관리된 원격 액세스 권한, 특히 '양자택일' 식의 VPN은 악의적인 공격자에게 매우 매력적인 위협 요소입니다.

BeyondTrust의 Privileged Remote Access는 적절한 시기에 적합한 사람에게 적합한 시스템에 대한 권한을 제공하고, IT 관리자, 타사 벤더, 개발자, CloudOps 엔지니어를 포함한 모든 원격 액세스의 가시성 및 제어를 제공합니다. 조직은 Privilege Remote Access를 활용하여 엄격한 보안 및 컴플라이언스 표준을 충족시키면서 중요한 IT 자산에 대한 액세스를 원활하게 확장할 수 있습니다.

"이전에는 VPN을 설정하는 것이 벤더의 원격 접속을 가능하게 하는 유일한 방법이었습니다. 그런데 이제는 BeyondTrust 덕분에 내부 환경에 대해 제한된 액세스를 제공할 수 있고, 벤더들의 세션을 기록함으로써 완료된 항목에 대한 정확한 감사 기록을 확보하게 되었습니다. 덕분에 훨씬 더 안전해진 거죠."

- Brian Bard, 노스캐롤라이나 대학교 살렛 캠퍼스,
테크놀로지 애널리스트

주요 기능:

권한 있는 액세스 제어

정의된 세션 Parameters를 통해 세분화된 역할 기반의 액세스 권한을 적용함으로써 '양자택일' 식의 원격 액세스를 제거하고, 직원 및 외부 업체가 Windows 서버에서 Kubernetes 클러스터까지 어디서든 안전하고 원활하게 접속할 수 있도록 합니다.

코드형 인프라(IaC)

Terraform과 같이 쉽게 사용할 수 있는 API 및 도구를 통해 자동화의 장점을 활용함으로써 클라우드 인프라를 스펠업 및 스펠다운하고 액세스를 프로비저닝 및 디프로비저닝합니다.

BYOT(Bring Your Own Things)

VPN 없이도 기술 직원이 Putty, Azure Data Studio 등의 친숙한 툴을 사용할 수 있게 하여 안전한 워크플로를 유지할 수 있습니다.

간단한 통합

기존의 SIEM 솔루션에 권한 있는 안전한 원격 액세스를 구축하여 이미 적응하여 편하게 느끼는 워크플로 내에서 애널리스트, 테크니션들을 위한 올인원 환경을 갖출 수 있습니다.

효율성 향상

컴플라이언스 또는 보안을 저해하지 않는 강력한 통합으로 안전한 액세스를 제공하고 워크플로를 유지합니다.

컴플라이언스 요구사항 충족

중앙 집중식으로 모든 원격 지원 활동에 대한 세션을 기록하여 감사를 간소화합니다.

비용 절감

VPN이 필요성이 없어지므로 가치가 극대화되고 네트워크 보안이 강화됩니다.

