OdoAccess

기업을 위한 제로트러스트 네트워크 액세스 솔루션

OdoAcess는 IT와 DevOps팀이 VPN 없이도 멀티클라우드와 온프레미스 인프라에 걸쳐 원격 접근을 관리할 수 있게 하는 간단하고 안전한 중앙 집중식 플랫폼입니다.
제로 트러스트 아키텍처는 관리자에게 모든 사용자 활동에 대한 가시성을 제공함과 동시에 기업 리소스에 대한 최소한의 접근 권한을 부여할 수 있게 합니다.
다른 접근법과는 달리, OdoAccess는 완전한 에이전트리스이며 웹, SSH, RDP와 DB 프로토콜 지원을 통해 조직 전체에 걸쳐 그 가치를 전달합니다.

문제점

업무 환경은 다양한 변화를 겪고 있지만, 네트워크 액세스 솔루션은 그렇지 않습니다. IT와 DevOps 엔지니어들의 새로운 업무환경은 클라우드, 모빌리티, 증가하는 애자일 방식의 환경을 지원해야 합니다. 새로운 업무환경에도 불구하고, 기업들은 여전히 VPN과 같은 레거시 액세스 솔루션을 사용하고 있습니다.
문제는 이를 통해서는 대규모 관리가 불가능하며 계속해서 변화하는 공격 방식에 대한 대응이나, 실제 진행되고 있는 작업에 대한 가시성을 확보할 수 없습니다.

OdoAccess의 장점

기업 리소스에 대한 최소 권한 기반의 접근제어

기업의 리소스들과 리소스 내의 접근에 대해 상황별로 동적이고 세분화된 접속을 제공합니다. Odo의 클라우드 네이티브 액세스 솔루션을 통해 멀티 클라우드, 멀티 사이트, 멀티 리전 환경을 대상으로 손쉽게 애플리케이션, 데이터센터, 직원 및 파트너 인력을 추가 또는 삭제할 수 있습니다.

사용자 행위에 대한 전체적인 감사 내용 확보

실행된 SSH 명령 및 세션 기록을 포함한 사용자 작업에 대해 전체 감사 추적이 가능합니다. 각 계정에서 실행된 중요한 작업을 확인할 수 있습니다.
또한, 감사 로그 범위를 좁혀 구체적인 이벤트 혹은 유저를 확인할 수 있으며 추가적인 상황 자료를 위해 SIEM으로 로그를 내보낼 수 있습니다.

보안 위험의 감소

애플리케이션 계층에서 세분화된 접속을 제공해 네트워크 레벨 접근을 제거하고 네트워크 레벨 공격에 대한 리스크를 경감시킬 수 있습니다. 쉽게 접근 정책을 수정하고 강화해 실시간으로 의심스러운 이벤트를 차단할 수 있습니다.

사용자 경험 향상

복잡한 구성과 클라이언트 프로그램 설치가 필요한 VPN을 사용할 필요가 없으며, 에이전트리스 방식으로 터미널을 통해 모든 리소스에 빠르고 안전하게 연결할 수 있습니다.

이용 사례

VPN 대체

오늘날 일하는 방식은 모바일화 되었으며 모든 기기를 통해 어디서나 호스팅 되는 애플리케이션에 대한 접속을 필요로 합니다. Odo의 제로 트러스트 아키텍처는 중요한 회사 데이터에 접근하기 전에 방화벽 같은 경계를 두고, 기존에 검증된 사람은 접속시키고 검증되지 않은 사람은 차단시키는 전통적인 네트워크 접근제어 방식의 보안 모델을 대체합니다.

써드파티 액세스

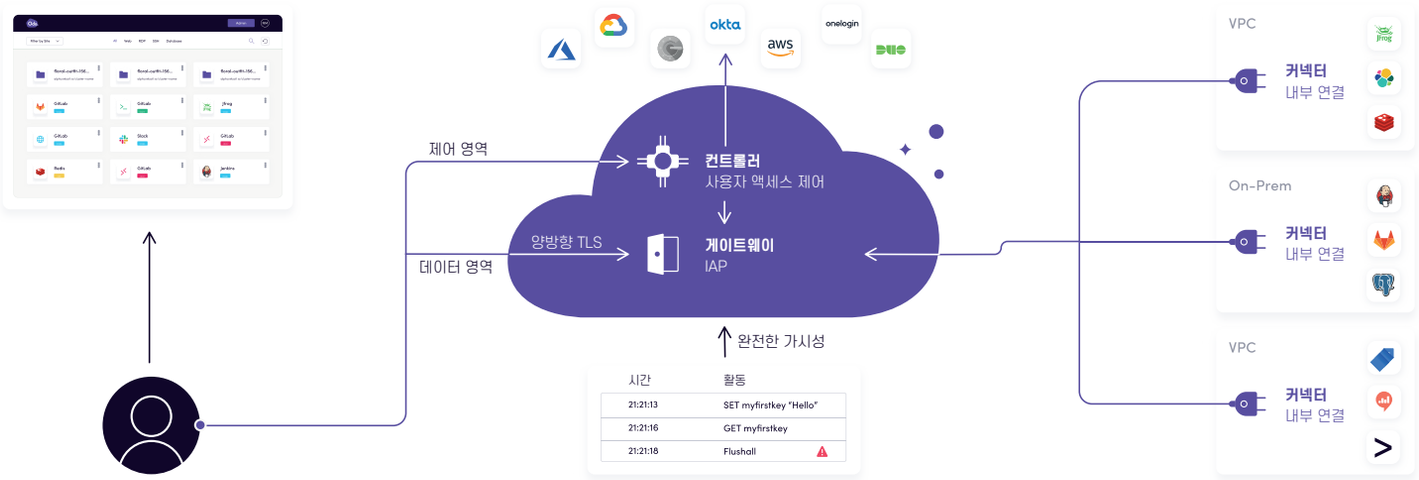
프리랜서 및 파트너들은 중요한 역할을 하지만 민감한 데이터에 대한 그들의 접근 관리 또한 처리하기 힘든 업무가 되었고 이로 인해 잠재적인 보안 리스크에 노출되어 있습니다. Odo를 통해 모든 애플리케이션, 서버, 데이터베이스와 환경에 대한 서드파티 액세스 및 접근을 시간과 범위를 기준으로 구분하고 제한할 수 있습니다.

DevOps 액세스

엔지니어 팀은 보안의 위험 없이 클라우드 기반 개발 및 생산환경의 민첩성과 유연성을 활용할 수 있어야 합니다. OdoAccess는 모든 사용자에게 최소한의 권한을 제공하는 방식으로 모든 작업에 대한 감사 정보를 동적 환경, 하이브리드 환경에서 제공합니다. 관리자는 가상 머신, 애플리케이션 및 서비스에 대한 접근을 손쉽게 구성 및 해제할 수 있는 클라우드 네이티브 플랫폼을 활용할 수 있게 됩니다.

MEGAZONE CLOUD
메가존클라우드(주) 서울시 강남구 논현로 85길 46 메가존빌딩
Contact Us. 1644.2243 | E-mail. contact@megazone.com | Website. www.megazone.com

작동 방법



- Odo는 접근 결정 권한을 네트워크 계층에서 애플리케이션 계층으로 이동시켜, 공격자가 네트워크 내에서 자유롭게 접근하지 못하도록 합니다.
- 모든 사용자는 자신의 위치, 장치 및 행동 패턴과 같은 상황별 데이터를 기준으로 인증되며, 기업의 정책을 기준으로 접근 권한을 부여받습니다.
- 인증된 사용자는 작업을 수행하는 데 필요한 접근 권한만 부여받게 됩니다. 다른 리소스들에는 접근할 수 없으며 존재조차 알 수 없습니다.
- IT 및 DevOps 엔지니어는 의심스러운 활동에 대한 실시간 알람을 통해 사용자 작업의 전체 감사 추적이 가능합니다.
- SaaS 플랫폼으로, 쉽고 빠르게 사용이 가능합니다.

주요 특징

손쉬운 사용과 적용

네이티브 API를 활용하여 수 초 이내에 새로운 가상머신, 애플리케이션에 대한 접속 설정이 가능합니다. 사용자에게 에이전트리스, SaaS의 경험을 제공합니다. - 사용자의 환경에 에이전트를 설치하거나 어플라이언스를 설치 및 관리할 필요가 없습니다.

SSH Key 관리 기능 내장

안전한 중앙 집중 관리 방식으로 SSH 키를 통합 관리하여 키 분실 및 손상 위험을 감소시킵니다. SSH 계정과 실제 작업을 진행하는 사용자와 매핑하고 그 내역을 감사 정보로 제공합니다.

중앙 집중형 관리

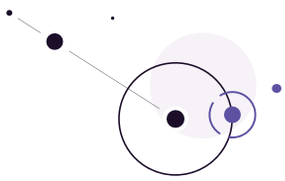
사용자 속성 및 디바이스 상태를 파악하여 리소스 및 리소스 내 환경에 대한 세부적인 접근을 제어합니다. 사용자의 데이터베이스 쿼리 및 명령어 사용내역과 서버, 기업의 데이터 저장소에 다양한 정책을 적용할 수 있습니다.

SSH 명령 및 쉘 로그

실행된 SSH 명령을 포함한 사용자 활동에 대해 전체 추적 감사가 가능합니다. 모든 감사 로그는 사용자의 계정과 디바이스를 기준으로 제공하며, 추가적인 분석을 위해 SIEM과 연동할 수 있습니다. 실시간으로 SSH 세션에 대한 관리가 가능합니다.

기존 IDP와의 연동

OdoAcess를 통해 사용자, 그룹 및 접근 정책을 생성하고 관리합니다. 또한 OdoAccess는 기존 IDP와 연동될 수 있습니다.



"Odo Security는 기존 인프라 위에서 쉽게 적용이 가능하고 사용자에게 원활하고 직관적인 접근 방식을 제공합니다."

Steve Brasen
Research Director at EMA.

"접근 제어를 적용하면서 개발 및 실제 운영환경에 대한 가시성을 제공하는 것은 복잡한 과제입니다. 이러한 접근 제어 방식은 다른 플랫폼에서는 제공하지 못했던 기능입니다."

Eyal Sasson
CISO of Gett

MEGAZONE CLOUD
메가존클라우드(주) 서울시 강남구 논현로 85길 46 메가존빌딩
Contact Us. 1644.2243 | E-mail. contact@megazone.com | Website. www.megazone.com