okta

최신 인프라 액세스에 대한 8가지 원칙

Okta Inc.
서울 강남구 테헤란로 152
강남파이낸스센터 41층

info@okta.com
050-6626-1877

서론 3
기존 방식으로 해결할 수 없는 문제 3
키 대신 Zero Trust 모델을 도입하세요 4
최신 인프라 액세스에 대한 8가지 원칙 5
수동 조작 대신 자동화로 5
정적 키 대신 임시 자격 증명으로 6
공유 계정 대신 사용자 아이덴티티로 6
권한 에스컬레이션 대신 역할 기반 액세스로 7
디렉토리 인터페이스 대신 로컬 계정으로 7
VPN 대신 배스천으로 8
체크아웃 프로세스 대신 SSO로 8
세션 기록 대신 구조화된 로그로 9
결론 10

서론

인프라 자원은 기업 네트워크 전체에서 가장 중요하고 가치 있는 자산 중 하나입니다. 서버와 데이터베이스가 클라우드에 있든 온프레미스에 있든 이에 대한 액세스를 제어하는 것은 IT 팀과 보안 부서의 최우선 과제입니다. 기존 방식은 '비밀번호 키 보호'에 초점이 맞춰져 있지만 매년 관리자의 자격 증명이 유출되면서 기업들이 큰 피해를 입고 있습니다. 이제는 달라져야합니다.

본 백서에서는 인프라 액세스 보호라는 핵심 과제와 더불어, 현재까지 업계에서 사용해온 접근법을 왜 재고해야 하는지 그 이유를 살펴봅니다. 우리는 포레스터의 Zero Trust 모델에 기반해 인프라에 액세스하는 새로운 방법론을 마련했습니다. 이 방법은 최신 클라우드 시대에 맞게 보다 안전한 환경을 구축하기 위한 8가지 원칙을 토대로 개발되었습니다.

기존 방식으로 해결할 수 없는 문제

정적인 자격 증명의 경우, 자격 증명 소유자가 권한을 100% 갖게 되며 사용자의 아이덴티티와는 직접적인 관련이 없습니다.

이로 인해 자격 증명 문제가 발생하게 됩니다. 대다수 기업들이 사용하고 있는 비밀번호나 키 기반 시스템은 심각한 문제를 일으킬 수 있습니다. 인프라 보호의 가장 큰 문제는 서버에 로그인할 때 사용되는 자격 증명 메커니즘입니다. 로그인 키나 비밀번호만 알면 해당 자격 증명을 확보한 경위와 관계없이 누구나 시스템에 액세스 할 수 있기 때문입니다. 도용된 자격 증명은 해커들에게 마치 전권 위임장처럼 사용됩니다. 이 자격 증명 문제를 해결하기 위해 다수의 제품과 방침이 마련되었습니다. 이 해결책들은 주로 자격 증명에 한 단계의 관리 절차를 추가해 자격 증명이 분실, 도난, 오용되지 않도록 관리하는 데 초점을 두고 있습니다. 자체 관리 방식에서 한 단계 발전한 방법이긴 하지만 이러한 해결책들도 사용자가 아닌 자격 증명이 시스템 액세스에 중요한 역할을 한다는 개념에 기반합니다.

기존 해결책의 문제점

- 정적인 자격 증명 자격 증명을 보호하는 추가적인 관리 절차가 있다 하더라도 본래의 속성은 바뀌지 않습니다. 여러 명의 사용자가 동일한 자격 증명을 보유할 수 있으며 아이덴티티을 보장하거나 추적할 방법이 없습니다.
- 까다로운 운용성 자격 증명과 관련 제품들은 운용하기 어려운 것으로 알려져 있습니다. 특히 고도로 자동화되고 탄력적인 클라우드 환경일수록 사용하기가 더 까다롭습니다. 이 문제는 자동화 속도를 지연시켜 클라우드 인프라 도입에 방해가 될 수 있습니다.
- 미흡한 엔드 유저 경험 자격 증명을 확인하기 위해 대역 외 프로세스를 사용하는 것은 시스템 관리자에게 매우 어려운 일일뿐만 아니라 꽤 많은 시간이 소요되는 일입니다. 기술 직원들이 업무를 할 수 없게 될 경우 그 대안책을 찾아낼 것이고 그렇게 되면 사내 보안 체계가 제 역할을 할 수 없게 됩니다.

서버 자격 증명의 문제점

정적인 특성: 키는 한번 생성되면 절대 변경할 수 없습니다. 이런 암호화 속성이 안전성을 반드시 강화하는 것도 아닙니다. 자격 증명은 분실, 도난, 또는 오용되는 경우가 많습니다.

프로비저닝 매뉴얼: 직원이 퇴사하거나 다른 팀으로 이동할 경우 해당 직원이 사용하던 키는 수동으로 제거됩니다. 관리자는 어느 서버에서 어느 사용자가 어느 키를 사용했는지를 확인해야 합니다. 하지만 해당 직원의 액세스를 완전히 취소했는지 어떻게 확인할 수 있을까요?

아이덴티티와 관련 없음: 앨리스와 밥의 예시를 통해 PKI(개인키 기반구조)에 대해 알게 됐지만, 개인 키는 특정인의 아이덴티티 프로필과 관련이 없습니다. 자격 증명 소유자가 100% 권한을 갖게 되며 개인 키만 알면 누구나 액세스 할 수 있습니다.

시스템 전반에 공유: 자격 증명이 무분별하게 확산하면 비밀번호가 확산하는 것과 다를 바가 없지만 위험성은 더 높습니다. 시스템에 키를 추가하면 시간이 지나면서 그 권한이 누적됩니다. 그렇다면 시스템에 액세스할 수 있는 키는 몇개나 될까요?

키 대신 Zero Trust 모델을 도입하세요

Zero Trust 보안 모델은 기업 네트워크 보안을 바라보는 우리의 관점을 바꿉니다. Zero Trust 보안 모델에서 액세스는 오로지 네트워크에 기반한 이진법 방식의 결정이 아니라 동적인 사용자, 디바이스, 네트워크 및 위치 정보를 감안하여 그 상황에 맞는 결정을 내리는 것입니다. 이 프레임워크는 간단합니다. 매번 시스템을 검증하는 것입니다.

Google의 BeyondCorp 이니셔티브는 Zero Trust를 잘 수행한 대표적인 사례로, 다음과 같은 전제로 설계되었습니다.

- 특정 네트워크를 통해 연결되었더라도 이것이 액세스 할 수 있는 서비스를 결정해서는 안 된다.
- 서비스에 대한 액세스는 사용자와 사용자 디바이스 정보를 바탕으로 부여된다.
- 서비스에 대한 모든 액세스는 인증, 승인 및 암호화되어야 한다.

BeyondCorp는 Google 조직 전체에 영향을 끼친 획기적인 프로젝트였습니다. 이렇게 극적인 변화를 수용할 수 있는 회사는 많지 않기에 Okta에서는 점진적인 전환을 권장하고 있습니다. 인프라 액세스는 Zero Trust를 도입하는 첫번째 사례가 되어야 합니다. Zero Trust는 아키텍처 및 절차상의 변경을 처리할 수 있는 기술팀에 적용되는 것이기 때문에 Okta 고객들은 이 이니셔티브에 집중하여 큰 성공을 거둘 수 있었습니다.

최신 인프라 액세스에 대한 8가지 원칙

이제 조직의 규모를 막론하고 모든 기업들이 아이덴티티에 기반한 아키텍처를 도입해야 할 때입니다. Okta Identity Cloud는 Advanced Server Access 제품을 해결책으로 내세워 아이덴티티 기반 아키텍처를 지원하는 기반 플랫폼입니다.

인프라 액세스를 혁신하기 위해서는 종래의 방식과 제품에서 탈피해야 합니다. Okta에서는 고객들과 협력하여 다수의 대규모 인프라에 이러한 새 방식을 도입하였고, 추적 가능한 방식으로 큰 성공을 거두었습니다. 이와 같은 사례를 통해 Okta는 현대의 모든 조직에 적합한 하나의 통합된 아키텍처를 구성하는 8가지 원칙을 도출했습니다. 각각의 원칙은 결과 중심적이며 기업들이 자사의 아이덴티티 및 액세스 솔루션에 진정으로 필요한 것이자 원하는 요소들에 중점을 두고 있습니다.

1 수동 조작 대신 자동화로

액세스 제어를 자동 프로비저닝하는 구성 관리

기존의 액세스 관리 방법에는 상당량의 복잡한 작업이 수반됩니다. 클라우드 도입률이 높아짐에 따라 이러한 방식은 점차 구식으로 치부되고 있습니다. 서버 관리자가 퇴사했다고 가정해봅시다. 서버 관리자들의 자격 증명과 계정의 비활성화 여부를 확인하는 것은 매우 복잡한 일입니다. 기업들은 그 규모나 유연성과 관계없이 자동화를 적극 도입할 때 클라우드 인프라를 십분 활용할 수 있습니다. 하지만 일반적으로 보안 제품들이 자동화를 지원하지 않기 때문에 클라우드 도입을 지연시키는 요인이 될 수 있습니다.

DevOps 툴과 프로세스의 등장으로 '코드형 인프라(infrastructure as code)'를 구축, 설치하는 개발자 및 운영팀과 동기화하기 위해서는 보안 제어 방식의 '근본적인 문제부터 해결'해야 합니다. 이 문제가 제대로 해결되면 팀이 환경을 한번 구성한 후 자동화가 수행됩니다. 제대로 구성하는것이 매우 중요한데, 가장 좋은 방법은 테스트 환경을 이용하는 것입니다. 초기 작업이 완료되면 효율적, 효과적으로 확대 적용할 수 있습니다.

액세스 제어와 관련해서는 시스템상의 사용자와 그룹 계정이 자동화됩니다. 그 후 자동화가 진행되는 과정에서 각각의 액세스 정책이 시행됩니다. 사용자 상태, 그룹 멤버십, 상세 정책이 변경될 때마다 실시간으로 포착되어야 합니다. 따라서 모든 요청은 최신 정보를 기반으로 평가됩니다. 서버 관리자가 퇴사하는 경우 기록 시스템에서 취해지는 조치가 모든 액세스를 즉시 비활성화하는 일련의 워크플로를 트리거하게 됩니다.

핵심 요점

Okta에 관한 모든 정보는 API 형태로 노출됩니다. 등록, 프로비저닝, 구성은 모두 완전 자동화 될 수 있으며 이를 통해 사용성을 크게 높일 수 있습니다.

2 정적 키 대신 임시 자격 증명으로

로그인 자격 증명은 일회용으로만 사용할 수 있도록 그 범위와 사용 시간이 제한됩니다.

Zero Trust의 핵심 원리는 액세스 제어를 네트워크 계층에서 보다 스마트한 의사결정을 내릴 수 있는 동적인 환경의 애플리케이션 계층으로 이동하는 것입니다. 이로써 순수 이진법에 의한 액세스 결정(예: 네트워크에 있음/없음)은 사용하지 않게 됩니다. 맥락을 수집하고 이를 실시간으로 실행하는데 모든 노력을 기울였지만 결국 사용자에게 공유형의 정적인 자격 증명을 제공된다고 상상해 보세요. 결국 쓸데없는 일을 한 셈입니다. 기존에 내린 액세스 결정을 유지하기 위해서는 자격 증명 메커니즘이 정확히 일치해야 합니다.

자격 증명과 관련된 리스크를 완화하는 것은 관리 영역을 통해 자격 증명을 보호하는 것보다는 자격 증명의 가치를 제한하는 것에 더 가깝습니다. 사용 시간과 범위가 제한된 자격 증명에는 주어진 시간과 범위 외에 그 어떤 내재적 가치도 주어지지 않습니다.

최신 기술을 통해 범위와 시간을 제어할 수 있는 좀 더 유연한 자격 증명 메커니즘을 구현할 수 있습니다. 클라이언트 인증서 아키텍처를 활용하여 액세스 결정과 정확히 일치하도록 로그인 자격 증명을 주문형으로 발행할 수 있습니다. 범위는 주변 맥락, 즉 디바이스를 통해 서버에 액세스 중인 사용자입니다. 인증서는 완전히 인증 및 승인될 경우에 단 한번만 발행됩니다. 그리고 개별 인증서는 유효기간이 짧으며 한 번만 사용할 수 있습니다.

핵심 요점

클라이언트 인증서를 지원하기 위해 엔드투엔드 PKI를 운영하는 것은 간단한 일이 아닙니다. Okta는 Advanced Server Access를 통해 프로그래밍 가능한 Certificate Authority를 내부에서 구동하는 방법으로 이러한 복잡한 문제를 해결합니다. Okta 지원 서버는 사용자에게 주문형으로 발행되는 서명된 인증서를 신뢰하도록 구성됐습니다.

3 공유 계정 대신 사용자 아이덴티티로

시스템 계정은 ID 공급자를 통한 사용자 소스가 직접적인 원인입니다.

기존의 액세스 관리 제품에서는 시스템 관리자가 고유한 권한을 갖습니다. 일반적으로는 각각 잠겨 있는 별도의 공유 계정을 활용합니다. 최소 권한의 원칙을 따르고 각 시스템에서 사용자가 수행할 수 있는 활동을 제한하는 것입니다. 최소 권한을 통해 얻길 바라는 결과가 Zero Trust 모델과 일치하긴 하지만 별도의 계정을 사용하는 것은 사람을 보안 경계로 삼는다는 개념과 상충됩니다.

맥락에 기반한 액세스 정책은 액세스 권한을 받아야 하는 대상과 그렇지 않는 대상을 명확히 구분합니다. 이 정책을 효과적으로 준수하기 위해서는 액세스 제어를 사내 기록 시스템의 아이덴티티와 직접 연계하여 공유 계정의 사용을 없애야 합니다.

이 모델은 오직 강력한 기반 아이덴티티 계층을 통해서만 구현되며, 자동화를 통해 다운스트림 시스템에 반영됩니다. 시스템상의 계정들은 ID 공급자가 보유한 계정에 직접 연결되며 수정 사항이 있을 경우 자동으로 포착됩니다.

핵심 요점

Okta는 아이덴티티에 기반한 액세스 제어를 원칙으로, 모든 인증 워크플로를 사용자 계정에서 직접 확장합니다. 이렇게 확장된 인증 워크플로는 사용자의 서버로 프로비저닝됩니다. 모든 활동은 사용자에게 귀속되어 감사 로그를 깨끗하고 일관되게 유지할 수 있습니다.

4 권한 에스컬레이션 대신 역할 기반 액세스로

시스템 차원의 권한은 사용자 역할의 기능으로, 초기 권한 부여 시 적용됩니다.

공유 계정은 시스템상의 특정 활동에 권한을 위임해 시스템 경로와 명령에 대한 일종의 '가드레일' 역할을 합니다. 이 에스컬레이션 모델은 최소 권한을 시행하는 또 다른 형태로, 흔히 사용되는 모델입니다. 이 방식의 문제는 바로 여기에 적용되는 정책입니다. 관리 영역은 시스템의 로컬 기능이기 때문에 특정 기기에서 어느 사용자에게 어떤 권한을 부여해야 할지 확인하기가 매우 어렵습니다. 화이트리스트와 블랙리스트를 관리하는 것도 굉장히 어려운 일이며 그 규모가 커지거나 작아지더라도 변경 사항을 일일이 확인하기가 쉽지 않습니다.

로컬 시스템에서 정책과 실행을 더 많이 추출할수록 중앙 제어판을 통해 그러한 정책들을 보다 효과적으로 준수할 수 있게 됩니다. 아이덴티티 기반 액세스 제어 매커니즘으로 전환하는 것은 변경될 수 있는 사용자의 역할에서 권한이 비롯된다는 것을 의미합니다. 예를 들어, TechOps팀 일원 중 한명에 Linux 서버에 대한 'sudo'권한이 부여되고 DataScience팀 일원 중 한명에게는 데이터베이스 서버에 대해 읽기 전용 SQL 쿼리만 실행할 수 있는 권한이 부여된다고 가정해 봅시다.

이 예시에서 역할은 사용자와 ID 공급자의 그룹 멤버십의 기능입니다. 시스템은 사용자가 로그인하면 사용자의 역할을 인지해서 그에 맞게 로컬 권한을 부여할 수 있어야 합니다. 이것은 자동화 기능일 뿐만 아니라 로컬 시스템 권한 모델의 기능이기도 합니다.

핵심 요점

Okta는 그룹 멤버십을 다운스트림 서버에 적용할 수 있는 중앙 제어판을 제공함으로써 정책 준수 절차를 간소화합니다. 명령 시 화이트리스트 또는 블랙리스트를 도입하는 것은 사용자 역할의 직접적인 기능이 되고 정책은 액세스 계층에서 관리됩니다.

5 디렉토리 인터페이스 대신 로컬 계정으로

기기에 직접 프로비저닝 및 디프로비저닝 되는 시스템 계정

서버에는 자체 로컬 계정과 파일 시스템이 있으며 이를 기록 시스템에 연결하는 것은 쉽지 않습니다. 일반적으로, 기기에서 디렉토리 인터페이스를 실행한 다음 이것을 백업 ID 공급자와 동기화 하는 방법이 사용됩니다. Linux에서는 이 작업을 LDAP PAM 모듈을 통해 수행할 수 있습니다. 이 인터페이스들을 구축하고 운영하는 과정은 매우 복잡하며, 확장 시 문제가 쉽게 발생합니다. 이는 일관성을 보장하기 어려운 분산 시스템 문제로 변질되기 쉽습니다.

좀 더 효과적인 접근법은 ID 공급자가 로컬 계정을 직접 프로비저닝 하는 것입니다. 이 방법을 사용하면 기기에서 디렉토리 인터페이스를 실행할 필요가 없어 시스템 권한이 로컬 계정과 연계되는 역할 기반 액세스 원칙에 좀 더 직접적으로 연결됩니다.

디렉토리 인터페이스는 로컬 계정을 제어하고 기록 시스템에 다시 직접 연결되는 로컬 에이전트로 대체됩니다. 이 에니전트는 사용자의 상태나 그룹 멤버십의 변동사항을 파악하고 이에 따라 로컬 계정을 생성, 업데이트, 삭제할 수 있습니다.

핵심 요점

Okta는 Server Agent를 통해 기기의 로컬 사용자와 그룹 계정을 관리하며 총체적인 자동 수명주기 관리를 제공합니다. 사용자가 Okta에서 비활성화되면 로컬 사용자 계정이 즉시 비활성화되기 때문에 해당 사용자가 어느 서버에 액세스할 수 있는지를 걱정할 필요가 없습니다.

6 VPN 대신 배스천으로

개인 시스템은 7 계층 액세스 제어 체계가 있는 배스천 아키텍처를 통해 보호됩니다.

본래 인프라 환경 보호는 네트워크 보호를 의미했습니다. 하지만 클라우드 시대가 도래하면서 Zero Trust 모델에 유리한 쪽으로 네트워크 경계가 허물어지고 있습니다. 대표적인 예로 Google BeyondCorp가 있습니다. BeyondCorp는 Google의 전 세계 직원들을 대상으로 VPN 사용을 없앴습니다.

망 분리는 가장 많이 권장되는 심층 방어책이지만 액세스 제어 메커니즘과는 독립적으로 구동되어야 합니다. 개인 인프라 리소스를 보호하기 위한 좀 더 효과적인 클라우드 네이티브 접근법은 손쉬운 배스천 호스트를 사용하는 것입니다. 사용자들은 목표 시스템에 접근하기 위해 이 호스트에 인증하거나 이 호스트를 건너뛰기도 합니다. 적절히 구성된 배스천 아키텍처는 VPN이 필요 없기 때문에 인증 워크플로를 어디서든 원활하게 확장할 수 있습니다.

가장 좋은 방법은 배스천 호스트를 통해 인바운드 연결에 액세스할 수 있도록 네트워크 계층에서 개인 시스템을 구성하는 것입니다. 그런 다음 배스천을 공용 인터넷에 실행합니다. 일반적으로는 가용성을 높이기 위해 인스턴스 그룹으로 실행하게 됩니다. 일단 인증이 완료되면 여러 가지 방법을 통해 목표 시스템으로 이동할 수 있습니다. 여기서 포트포워딩 방식이 주로 사용되는데, 트래픽이 해독되기 때문에 위험한 방법입니다. Okta는 배스천을 통한 프록시 트래픽을 사용할 것을 권장합니다. 이렇게 하면 목표 시스템에 도달할 때까지 암호화된 채널을 사용할 수 있습니다.

핵심 요점

Okta는 배스천을 최우선시합니다. 따라서 사용자는 인증과 전송이 투명하게 이뤄지는 배스천 호스트를 통해 대상 기기를 구성할 수 있습니다.

7 체크아웃 프로세스 대신 SSO로

기반 전송 프로토콜 네이티브 아이덴티티 기반 로그인 워크플로

정적 자격 증명에 기반한 공유 계정 모델에서 가장 흔히 사용되는 워크플로는 증명 후 사용 가능한 공유 자격 증명을 확인한 다음 이를 사용해 시스템에 로그인하는 것입니다. 시스템 관리자 입장에서 이 대역 외 프로세스는 사용하기 어렵고 더딘 방식이 될 수 있는데, 인시던트 발생 시 특히 그렇습니다. 시스템 관리자들은 숙련된 기술자들이기 때문에 업무 수행을 방해하는 모든 보안 제어를 우회하려고 할 것입니다.

SSO(Single sign-on, 1회성 로그인)은 흔히 사용되는 기업용 앱 액세스 방식으로 자리잡았습니다. 이와 같이 동일한 원칙과 원활한 경험이 인프라 계층에도 적용됩니다.

인프라 리소스의 경우, 기반 전송 프로토콜에 인라인으로 인증 워크플로우를 주입하여 이 작업을 수행할 수 있습니다. 사용자가 SSH를 통해 Linux 박스에 로그인하면 시스템은 ID 공급자가 지원하는 인증 워크플로우를 실행합니다. 다중 요소 인증 정책이 있을 경우 이는 워크플로우의 일부로 도입됩니다.

핵심 요점

Okta는 Advanced Server Access 제품을 사용자의 로컬 툴과 직접 인터페이스되고 Linux나 Windows 서버의 SSH 및 RDP 프로토콜과 인라인으로 구동되도록 설계했습니다. 모든 인증 및 권한 인증 작업이 배후에서 이뤄지기 때문에 엔드 유저 경험을 저해하지 않으면서 보다 안전한 액세스 제어 방식을 구현할 수 있습니다.

8 세션 기록 대신 구조화된 로그로

검색 및 경고 알림이 가능한 구조화된 로그로 기록되는 이벤트 감사

법의학 분석은 모든 컴플라이언스 기준의 공통 항목으로, 시스템상의 모든 관리자 활동은 추후 확인할 수 있도록 기록되어야 합니다. 이 데이터를 기록, 보관, 전달하는 데 투입되는 노력 대비 이 정보를 쉽게 사용하여 얻을 수 있는 보안상의 이점이 훨씬 큽니다.

보안 관점에서, 조직은 누가 어느 디바이스에서 언제 시스템에 액세스 했고 시스템에 로그인한 후 무엇을 했는지 명확히 검사해야 합니다. 해당 데이터에서 실행 가능한 정보를 구축하기 위해서는 세션 기록을 통해 구조화된 로그를 사용하는 것이 좋습니다. 이렇게 하면 이 정보를 빠르게 색인화하고 검색하며 경고 알림을 받을 수 있습니다.

이런 수준의 감사 능력을 확보할 수 있는 방법에는 크게 두가지가 있는데, 하나는 모든 트래픽을 프록시화하는 게이트 웨이를 사용하는 방법이고, 또 하나는 캡쳐 프로세스를 실행하는 에이전트를 사용하는 방법입니다. 두 방법 모두 추가 검사를 위해 로그인 서비스 또는 SIEM에 전송될 수 있는 구조화된 로그를 도출하게 됩니다. 두 방법 모두 사용자 세션에 방해되지 않도록 비동기식 프로세스가 적용됩니다.

핵심 요점

Okta는 각 기기에 손쉬운 Server Agent를 실행하여 대시보드나 제3의 SIEM 서비스를 통해 추가 분석이 가능한 로그 항목 형태로 로그인 활동을 포착합니다.

결론

최신 클라우드 시대가 인프라 환경을 근본적으로 혁신함에 따라 액세스 제어 방식도 바뀌어야 합니다. 앞서 설명한 8가지 아이덴티티 기반 원칙을 따르면 높은 보안성과 확장 가능한 자동화된 환경을 운영하는데 접합한 조직으로 거듭날 수 있을 것입니다. 클라우드 마이그레이션의 일환이든, 그린필드 구축 방식이든, 아키텍처를 조기에 잘 구축하면 시간과 비용을 절감할 수 있고 수작업에 따른 문제를 방지할 수 있습니다.

사내 인프라 전체에 각 8개 원칙을 적용해 IAM 시스템을 구축하는 것은 쉬운 일이 아닙니다. Okta Advanced Server Access는 Okta Identity Cloud 기반의 단일 제어 영역으로 이러한 복잡성을 해소합니다.

여기를 클릭해 Okta Advanced Server Access에 대한 상세 정보를 확인하세요.
https://www.okta.com/kr/products/advanced-server-access/

Okta 소개

Okta는 수천 개의 고객사와 수백만 명의 사용자 아이덴티티를 관리, 보호하는데 앞장서고 있습니다. Okta는 채용, Okta를 구동하는 소프트웨어 아키텍처와 개발, 기업들이 세계적인 수준의 서비스를 제공할 수 있게 해주는 데이터 센터 전략과 운영 방식을 아우르는 종합 보안 서비스를 제공하고 있습니다. 제품 혁신과 수상 경력에 빛나는 고객 지원 서비스 외에도 사용자와 사용자의 정보를 보호할 가장 안전한 보안 플랫폼을 구현하기 위해 쉬지 않고 일하는 세계적인 수준의 사이버 보안 팀이 Okta의 솔루션을 만들고 있습니다. Okta는 고객의 데이터를 안전하게 보호하기 위해 최첨단 암호화 키 관리 시스템을 사용하고 있습니다. Okta의 고객 데이터 보호 기술은 GDPR, FedRAMP 및 NIST 800-53, HIPAA, ISO 27001의 조건에 따라 감사됩니다. Okta는 ENGIE, Eurostar, Scottish Gas Networks, News Corp 등 글로벌 기업뿐만 아니라 American Express, U.S. Department of Justice, Nasdaq 등 가장 엄격한 규제를 도입한 기업들의 사용자 정보를 보호하고 있습니다.

자세한 정보는 Okta 홈페이지(www.okta.com/education)에서 확인하실 수 있습니다.