okta

IT 부서가 벤더와 파트너에게 안전한 액세스를 제공하기 위해 해결해야 할 5가지 문제

Okta Inc.
서울 강남구 테헤란로 152
강남파이낸스센터 41층

support.okta.com
050-6626-1877

목차

전통적으로 기업은 모든 직원이 한 울타리 안에서 각 부서로 분산되는 구조를 유지해왔습니다. 하지만 이러한 기업 구조는 지난 15년에 걸쳐 점차 모호해졌고, 내/외부 직원을 비롯해 타사 벤더와 파트너까지 아우르면서 확장 기업의 형태를 띄기 시작했습니다.

기업의 사용자 기반이 정규 직원으로만 구성되던 시대는 이제 지났습니다. 이제는 애플리케이션과 데이터를 계약자, 벤더, 파트너, 임시 인력 등의 새로운 사용자와 주기적으로 공유하는 등 변화하는 요건에 그 어느 때보다 빠르게 적응해야 합니다. 마치 지문처럼, 사용하는 디바이스와 애플리케이션 및 시스템도 사용자마다 다릅니다. 이로 인해 각자의 직무를 효과적으로 처리하기 위해 시스템에 선별적으로 안전하게 액세스할 수 있는 방법이 필요해졌습니다.

외부 공급업체부터 파트너에 이르기까지 수많은 사용자에게 적합한 액세스 권한을 제공하고 이후 상황에 따라 액세스 권한을 취소하는 일은 매우 복잡합니다. 온프레미스 인프라의 비중이 높은 하이브리드 환경을 운영 중인 대기업의 경우 특히 그렇습니다.

안전한 벤더 액세스 관리의 어려움

타사 액세스 관리 제어라고 하면 IT 부서가 회사 안팎에서 점차 증가하는 아이덴티티를 관리해야 한다는 것을 의미합니다. 하지만 안타깝게도, 이는 말처럼 그렇게 쉽지 않습니다. 기업이 계약자에게 안전하고 원활한 액세스 환경을 제공하려고 하는 과정에서 중요한 문제들이 다수 발생합니다.

IT 부서의 지원: 특히 대부분의 작업을 수동으로 처리하는 IT 부서의 경우, 직원들을 내부 시스템과 애플리케이션에 프로비저닝/디프로비저닝하는 데 상당한 부담을 안고 있습니다. 여기에 각종 시스템과 기존/신규 테크놀로지, 고유한 정책과 프로세스 등 근무 환경이 서로 다른 파트너와 벤더까지 추가되면서 복잡성이 가중되어 IT 부서의 지원이 기대에서 점차 멀어지고 있습니다.

통합: 타사 공급업체와 파트너를 애플리케이션과 리소스에 연결하는 것은 각종 테크놀로지 구현의 어려움으로 인해 힘든 작업이 될 수 있습니다. 파트너마다 사용하는 시스템과 애플리케이션이 다를 수 있으며, 새로운 테크놀로지가 기존 테크놀로지를 보완하지 못할 경우에는 또 다른 문제가 발생하게 됩니다. 또한 라이프사이클 관리 시스템을 이미 구축한 대형 B2B 파트너가 있다 하더라도 일부 소규모 파트너사들은 시스템에 원활하게 통합되지 않는 기존 테크놀로지를 사용하고 있을 가능성이 있습니다. 따라서 이 두 가지 시나리오를 모두 관리할 수 있는 방법을 찾아야 합니다.

보안 위험: 새 공급업체를 이용하는 신규 사용자들로 인해 불가피하게 새로운 보안 위험이 발생하는데, 예를 들면 벤더 액세스 수준에 대한 가시성이 떨어지거나, 모든 파트너십 단계에서 기밀 데이터를 보호하지 못하는 것 등의 문제가 있습니다. 이러한 보안 위험을 항상 쉽게 정의할 수 있는 것은 아니지만 확장 기업을 주제로 대화를 나눌 수 있는 토대를 마련한다는 점에서 안전한 벤더 액세스 방식을 찾는 데 도움이 될 것입니다.

벤더 액세스와 관련해 기업이 해결해야 할 5가지 주요 문제

Okta는 기업이 안전한 벤더 액세스 환경을 구축하는 과정에서 다양한 문제에 끊임없이 부딪히고 있다는 사실을 잘 알고 있습니다. Okta에서는 문제의 본질을 파악하기 위해 고객을 참여시켜 이 과정에서 발생하는 각종 해결 과제에 대한 인사이트를 확보했습니다.

1 벤더 또는 파트너 아이덴티티 소스에 연결하려면 어떻게 해야 하는가?

내부 직원에게 액세스 권한을 부여하는 일은 어렵지 않습니다. 자사 디렉터리에 모든 직원의 정보가 저장되어 있기 때문입니다. 하지만 벤더/파트너 아이덴티티의 경우 문제가 다른데, 테크놀로지 성숙도와 이해 및 지원 수준이 회사마다 다르기 때문입니다.

IT 부서는 타사 액세스 관리 환경에서 발생하는 각종 시나리오를 처리하여 파트너 및 벤더 사용자 액세스에 대한 가시성을 확보해야 합니다. 이를 위해 기업은 다음과 같은 방법들을 도입할 수 있습니다.

파트너 디렉터리: 파트너가 Microsoft의 Active Directory(AD)나 Lightweight Directory Access Protocol(LDAP) 서버와 같은 기존 사용자 디렉터리를 가지고 있는 경우도 있습니다. 이러한 디렉터리에는 파트너가 공유 리소스에 액세스하기 위해 사용하고자 하는 사용자 계정과 자격 증명이 포함되어 있습니다.

아이덴티티 페더레이션: 규모가 큰 기업들은 공유 리소스를 페더레이션할 수 있는 아이덴티티 공급자(IdP)가 이미 있는 경우가 많습니다. 이러한 기업들은 테크놀로지에 정통할 가능성이 높기 때문에 사용자 관리를 처리할 수 있어야 합니다(입사자 및 퇴사자 계정 관리).

아이덴티티 테크놀로지이 없는 경우: 테크놀로지 성숙도가 비교적 낮아서 IdP나 디렉터리가 없는 파트너라면 기업 IdP에 이 파트너를 위한 로컬 계정을 만들면 됩니다. 이는 벤더나 파트너를 적극 지원하는 측면에서 더욱 까다로운데, 그 이유는 기업이 파트너의 사용자 라이프사이클까지 관리해야 하기 때문입니다.

2 벤더와 계약자에게 안전하고 선별적인 액세스를 제공하려면 어떻게 해야 하는가?

오늘날 기업들은 일반적으로 계약자 및 벤더 사용자의 액세스 수준에 대한 가시성이 떨어지기 때문에 기밀 데이터를 보호하거나 사용자를 자사 애플리케이션에 안전하게 연결하는 데 어려움을 겪고 있습니다. 타사 사용자가 필요한 툴과 시스템에 손쉽게 액세스할 수 있게 해주는 도구를 도입하지 않아 결국 도입률이 떨어지고 파트너 충성도가 낮아지게 되는 것입니다.

중요한 점은 벤더와 계약자가 기업의 시스템과 파일 및 폴더에 모두 액세스해야 할 필요는 없다는 사실입니다. 오히려 선별적으로 액세스해야 하기 때문에 필요한 것만 열람하거나 조작할 수 있으며, 이러한 선별적 액세스를 제공할 수 있는 방법은 다음과 같습니다.

SSO(Single Sign-On): 액세스 권한은 최대한 쉽고 간단하게 부여해야 하며 이와 동시에 보안도 강력해야 합니다. SSO(Single Sign-On)는 어떤 디바이스에서도 사용할 수 있는, 소비자 친화적인 웹 포털을 통해 애플리케이션에 대한 사용자 액세스를 중앙화합니다. 이로써 리소스 액세스가 간소화되며, 내/외부 사용자는 액세스 권한이 부여된 정보만 확인할 수 있습니다.

패스워드리스 인증: 확장 기업에서는 비밀번호를 관리할 수 없습니다. 비밀번호는 근본적으로 불안전하여 잊거나 분실하는 경우가 많으며, 사용자가 자신이 액세스할 수 없는 정보까지 액세스하게 될 가능성이 커집니다. SSO(Single Sign-On) 외에도 SAML이나 OIDC 같은 페더레이션 접근 방식을 이용하면 벤더 액세스 관리를 완전히 제어할 수 있습니다. 또한 더 안전할뿐더러 관리하기 쉽기 때문에 IT 부서가 아이덴티티 공급자에 대한 사용자 액세스를 즉시 취소할 수 있습니다.

아이덴티티 프루핑: 기업은 자사가 협력하는 타사 공급자가 늘어날수록 사용자 아이덴티티, 즉 신원 확인에 대해 보다 심층적인 인사이트를 확보해야 합니다. 각종 아이덴티티 프루핑 기능과 함께 다중 요소 인증(MFA) 기법을 제공하면 예방 조치가 추가되어 보안 위험을 최소화할 수 있습니다. 예를 들어 Okta의 아이덴티티 프루핑 통합은 사용자가 문서, 사진, 보안 질문 등 고객이 선택하는 방식으로 자신의 아이덴티티를 안전하게 인증할 수 있는 기능입니다.

Okta 고객은 파트너와 벤더에게 안전한 액세스를 어떻게 제공할까요?

21ST CENTURY FOX

21st Century Fox가 수십 년 동안 성공 가도를 달릴 수 있었던 이유는 바로 협업을 기반으로 했기 때문입니다. 이 회사의 글로벌 CISO인 Melody Hildebrandt에 따르면, "기본적으로 당사의 사용자들은 타사 벤더와 늘 협업하고 있습니다" 이에 따라, 자사의 직원과 콘텐츠를 보호하는 동시에 빠르게 변화하는 파트너 에코시스템에 적응할 수 있는 액세스 및 아이덴티티 솔루션이 필요해졌습니다.

21st Century Fox는 현재 직원과 계약자 및 파트너로 구성된 광범위하고 복잡한 네트워크에서 Okta Identity Cloud를 사용해 사용자들에게 총체적인 보안과 사용자 친화적인 프로비저닝/디프로비저닝 서비스를 제공하고 있습니다.

> *Okta MFA 덕분에 우리가 설계한 대로 정책을 적용하여 보안 목표를 달성할 수 있었습니다. 또한 사용자에게 만족도 높은 테크놀로지를 제공하여 기업의 테크놀로지 목표까지 달성했습니다.*
>
> —Melody Hildebrandt, 21st Century Fox의 글로벌 CISO

사용자 행동 검사: 아이덴티티 프루핑으로 심층적인 인사이트를 확보하는 것 외에도 사용자 행동에서 신호를 찾는 것이 중요합니다. 여기에는 사용자가 액세스하는 애플리케이션, 사용자가 속한 그룹, 사용자의 위치, 그리고 사용자가 사용하는 디바이스 등 관련 정보에 대한 검사가 포함됩니다. 이러한 정보들은 잠재적 위험에 대해 경고하여 타사 액세스를 최대한 안전하게 관리할 수 있다는 점에서 매우 중요합니다.

3 벤더 등록 및 등록 해제 시 사용자 권한을 자동화하려면 어떻게 해야 하는가?

직원을 새로 채용하게 되면 IT 부서와 HR 부서가 긴밀히 협력하여 입사자 계정 관리에서부터 업무 변경과 퇴사자 계정 관리에 이르는 전 과정을 관리합니다. 하지만 새 계약자나 벤더의 계정을 관리하려면 다른 팀, 특히 해당 벤더와 협력 중인 부서(마케팅, 엔지니어링 등)의 도움이 필요한 경우가 많습니다. 이러한 시나리오에서는 기존의 라이프사이클 관리 프로세스를 간과하여 보안 위험과 초과 지출이 증가할 가능성이 커지게 됩니다.

많은 기업이 스프레드시트나 이메일을 통해 파트너 및 벤더 사용자에게 액세스 권한을 일일이 부여하느라 엄청난 시간과 자원을 낭비하고 있습니다. 이는 취약한 보안, 계약자의 애플리케이션 액세스 지연, 파트너 이탈 등 여러 가지 문제를 야기합니다. 이러한 문제점을 막기 위해서는 프로젝트가 시작되었을 때 애플리케이션에 대한 액세스 권한을 쉽고 빠르게 부여하고, 프로젝트가 종료되었을 때 권한을 취소할 수 있어야 합니다. Okta 자동화는 관리자가 이러한 작업을 자동화하여 시간을 절약하고 인적 오류의 위험을 제거할 수 있는 기능입니다. 다음은 자동화 기능의 실제 사용 예시입니다.

예정된 계정 정지: 기업은 특정 그룹이나 프로젝트에 할당된 사용자 권한을 예정된 시점에 자동으로 취소할 수 있습니다. 예를 들어 계약자에게 부여된 액세스 권한을 연말에 취소해야 한다고 가정하겠습니다. Okta의 Lifecycle Management 제품은 예약을 통해 12월 31일에 특정 그룹(계약자 등)에 사용자가 남아 있는지 확인하고, 사용자가 남아 있을 경우 해당 사용자의 계정을 정지시키고 액세스 권한을 제거할 수 있습니다.

휴면에 따른 계정 정지: 그룹 내 휴면 사용자 유무를 점검한 후 해당 사용자의 액세스 권한을 주기적으로 정지시키도록 조건을 설정하여 일정 기간 동안 아무런 활동이 없는 사용자의 계정을 자동으로 정지시킬 수 있습니다.

위와 같은 접근 방식으로 애플리케이션에 대한 액세스를 보다 면밀히 제어할 수 있으며, 이는 파트너와 계약자가 자사의 사용자 계정을 선제적으로 관리하지 않는 경우에 특히 효과적입니다.

Okta 고객은 파트너와 벤더에게 안전한 액세스를 어떻게 제공할까요?

DICK'S SPORTING GOODS

Dick's Sporting Goods는 겨울 휴가 시즌이 되면 고객 콜 센터를 4곳에서 9곳으로 늘리는데, 약 1개월 동안 신규 상담원의 계정을 모두 관리한 후 휴가 시즌이 지나면 15일 내로 상담원의 계정을 디프로비저닝해야 합니다.

이전에는 이러한 프로세스를 수동으로 처리하느라 정규 직원 1.5명을 추가로 고용해야 했습니다. 하지만 Okta의 허브-앤-스포크(hub-and-spoke) 방식을 도입한 덕분에 라이선스 비용을 대폭 절감하고 휴가 시즌을 보다 신속하게 준비할 수 있게 되었습니다.

> *Okta 통합 기능을 통해 고객 서비스 운영의 가치를 끌어올렸습니다. 또한 기존 BPO 파트너에 신규 파트너까지 합류하면서 이제 파트너들이 아이덴티티 소유권을 책임지고 있습니다. Okta는 당사 IT 지원 팀과 비즈니스 운영 팀에게 게임 체인저 역할을 하고 있습니다.*
>
> —Eva Sciulli, Dick's Sporting Goods의 제품 관리자

4 벤더 액세스 관리에 대한 컴플라이언스를 검증하려면 어떻게 해야 하는가?

오늘날 기업들은 기밀 데이터를 보호하는 동시에 파트너가 애플리케이션에 안전하게 연결할 수 있도록 지원하는 데 어려움을 겪을 때가 많습니다. 이를 위해서는 다음과 같이 신뢰할 수 있는 보고와 더불어 벤더 및 파트너 액세스 수준에 대한 가시성이 필요하기 때문입니다.

할당 현황 보고서: 어떤 사용자가 어떤 애플리케이션에 액세스하고(그 반대의 경우 포함), 어떻게 액세스 권한을 얻었는지를 보여줍니다.

할당 해제 현황 보고서: 지정된 기간 동안 어떤 사용자가 앱에서 할당 해제되었는지를 보여줍니다. 예를 들어 회사가 11월부터 3개월 동안 계약직 근로자를 고용할 경우, 이 보고서를 통해 11월에 액세스 권한이 부여되고, 1월 말에 액세스 권한이 취소된 것을 확인할 수 있습니다.

5 파트너 및 벤더 사용자에 대한 관리 부담을 덜어주려면 어떻게 해야 하는가?

IT 팀의 업무 부담을 줄이려면 타사 사용자에 대한 관리를 없애면 됩니다.

셀프서비스: 기업은 벤더 및 파트너 사용자가 간단한 계정 문제를 스스로 관리하도록 셀프서비스 기능을 제공할 수 있습니다. 이렇게 되면 IT 지원 요청 전화가 줄어들어 IT 팀이 기업 가치를 창출할 수 있는 작업에 더욱 집중할 수 있게 됩니다.

관리 위임: 또한 관리자 역할을 실행하여 파트너 및 벤더 액세스 관리에서 일정 부분을 없앨 수도 있습니다. 예를 들어 지원 관리자 업무 중에는 비밀번호 리셋이나 계정 잠금 등이 있지만 이러한 업무는 계약자에게 위임할 수 있습니다. 이러한 유형의 관리자 업무를 살펴서 특정 사용자 그룹만 관리할 수 있도록 설정할 수도 있습니다.

Okta 고객은 파트너와 벤더에게 안전한 액세스를 어떻게 제공할까요?

HENDRICK AUTOMOTIVE GROUP

이전에는 Hendrick의 직원들이 여러 곳의 자동차 딜러십에서 근무하다 보니 직원 추적 시스템이 100여 개의 독립 HR 시스템으로 구성되어 매우 복잡했습니다. 이러한 시스템을 통합하기로 결정하고 라이프사이클 관리 업무의 99%를 자동화할 수 있도록 Okta에게 도움을 요청했습니다.

그 결과 Okta 덕분에 입사자 계정 관리에서부터 퇴사자 계정 관리에 이르기까지 전 과정이 자동화되었고, 임원들은 이제 새로운 솔루션과 아이디어를 도입할 때 Okta를 빼놓지 않습니다.

> *Okta는 오랜 시간이 걸리는 수동 프로세스로 인해 정보를 제때 얻지 못하고 부정확한 문제에 빠져있던 우리에게 해답을 제시했습니다. 이제는 매주 처리하는 프로비저닝 및 디프로비저닝 이벤트만 약 150건에 이릅니다. 이전이라면 불가능했을 일입니다.*
>
> —Amy Frost, Hendrick Auto의 IT 엔지니어링 부문 이사

Okta의 지원 방식

Okta는 기업이 자사의 애플리케이션과 시스템에 안전하게 액세스할 수 있는 권한을 타사에게 제공할 수 있도록 도와주는 아이덴티티 솔루션을 다양하게 제공하고 있습니다.

LIFECYCLE MANAGEMENT

라이프사이클 관리란 입사자 계정 관리에서부터 업무 변경과 퇴사자 계정 관리에 이르기까지 사용자 계정의 라이프사이클을 유지 관리하는 프로세스를 말합니다. Okta의 Lifecycle Management는 수동 프로비저닝에서 벗어나 정책 중심의 컨텍스트 기반 방식으로 자동화함으로써 이러한 작업을 간소화합니다. 따라서 IT 부서가 중앙에서 어떤 사용자가 어떤 시스템과 파일에 액세스하는지 모니터링하여 액세스 권한과 라이선스를 할당하거나 취소하는 데 효과적입니다.

SSO(SINGLE SIGN-ON)

Okta의 SSO(Single Sign-On)는 어떤 디바이스에서도 사용할 수 있는 소비자 친화적인 웹 포털을 통해 애플리케이션에 대한 사용자 액세스를 중앙화합니다. 사용자가 포털에 로그인하면 Okta가 인증을 관리하여 사용자 업무에 따라 권한이 할당된 애플리케이션에 액세스할 수 있도록 허용합니다. 이로써 계약자와 벤더가 허용된 정보에만 액세스할 수 있기 때문에 안심할 수 있습니다.

UNIVERSAL DIRECTORY

Okta의 Universal Directory는 기업이 사용자와 그룹 및 디바이스를 한 곳에서 관리할 수 있는 솔루션이며, 이러한 정보들은 모두 Okta 또는 각종 소스로 마스터링 됩니다. 기업은 사용자와 비밀번호를 비롯해 링크 객체, 중요한 속성, 사전 설정된 목록 등 사용자와 속성을 원하는 만큼 안전하게 저장할 수 있습니다.

ADAPTIVE MFA

지능적인 데이터 유출이 점차 늘어나면서 고객과 직원의 데이터를 보호해야 하는 중요성도 더욱 커지고 있습니다. Okta의 Adaptive Multi-factor Authentication을 이용하면 번거롭고 불안한 비밀번호 입력 로그인 방식에서 벗어날 수 있습니다. 이에 따라 보안을 강화하고, IT 부서의 관리 업무를 간소화하며, 모든 고객과 직원에게 손쉽게 로그인할 수 있는 환경을 제공할 수 있습니다.

모두에게 안전한 액세스 관리

기업의 네트워크가 보안 경계이던 시대는 이제 지났습니다. 휴대용 디바이스와 클라우드 컴퓨팅의 등장으로 사용자 등록 및 등록 해제가 반복되면서 기업 경계가 확장과 수축을 끈임없이 반복하고 있습니다. 이에 따라 Zero Trust 환경에 맞게 높은 보안 수준을 유지하려면 기업도 그에 맞게 변화해야 합니다.

기업이 직원과 확장 기업의 형태에 맞춰 라이프사이클 및 액세스 관리의 최신화를 추진하고 있다면 앞서 살펴본 질문들을 검토하는 것도 당연합니다. 대부분의 경우, 비즈니스 성장과 민첩성을 고려하여 개발된 올인원 솔루션에서 그 해답을 찾을 수 있습니다.

지원, 계약자, 파트너를 보다 확실하게 보호하고 지원할 수 있는 방법을 찾고 있다면 지금 Okta의 협업 솔루션에 대해 자세히 알아보세요.