5 QUESTIONS IT Must Address to Provide Secure Access for Vendors and Partners

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

Table of Contents

Traditionally, companies were structured as localized entities with all of their employees under the same roof. Over the last 15 years, modern enterprises have become more nebulous, made up of in-house and remote employees and orbited by a large network of third-parties, otherwise known as the extended enterprise.

Gone are the days when a company's user-base consisted solely of full-time employees—now more than ever, companies must adapt quickly to shifting needs, which means regularly sharing applications and data with new users including contractors, vendors, partners, and temporary workers. Like fingerprints, each user has their own unique set of devices, applications, and systems. Each requires secure and selective access to your systems in order to do their jobs effectively.

Providing the right level of access to hundreds of users, from external suppliers to partners—and then ensuring access is revoked accordingly—can be a complex task. For large organizations operating in hybrid environments that are weighed down by on-premise infrastructure, this is especially true.

The turbulent ride towards secure vendor access management

Taking control of third-party access management means IT teams have to manage an increasing number of identities, both internally and externally. Unfortunately, this is easier said than done. As enterprises try to provide secure and seamless access to their contractors, a number of critical challenges present themselves.

IT SUPPORT: Being fully responsible for provisioning and deprovisioning employees to all internal systems and applications is already a significant strain on your IT team—especially if a lot of the work is still done manually. Adding partners and vendors that work with different systems, new and old technologies, and their own policies and processes adds another layer of complexity that takes IT staff away from doing what they do best.

INTEGRATION: Connecting third-party suppliers and partners to applications and resources can be a tough task, with various technical aspects that are difficult to implement. Partner organizations likely operate on different systems and applications, and there's an added challenge when newer technologies don't complement older tools. While you might have larger B2B partners that already have lifecycle management systems in place, some of the smaller businesses you work with might still be reliant on legacy technology that doesn't seamlessly integrate with your systems. The key is finding a way to manage both scenarios.

SECURITY RISKS: New users from new suppliers inevitably lead to new security risks. There are issues associated with poor visibility into vendor access levels, for instance, and an inability to protect confidential data at every stage of the partnership. While they're not always easy to define, these security risks offer a way to frame the conversation around the extended enterprise, helping organizations navigate secure vendor access.

The 5 main questions businesses have about vendor access

At Okta, we understand that enterprises are constantly facing challenges on their path to secure vendor access. To understand the crux of the problem, we engaged our customers to gain insight into the questions and challenges that arise during this process.

1 HOW DO I CONNECT TO VENDOR OR PARTNER IDENTITY SOURCES?

Providing access to internal employees is fairly straightforward, given they're all housed in a directory that's owned by the business. However, when it comes to vendor and partner identities, each company will have varying levels of technical maturity, understanding, and support.

The IT team needs to be able to handle various scenarios across the third-party access management landscape, and have visibility into partner and vendor user access. To accomplish this, there are a number of methodologies that businesses can adopt.

PARTNER DIRECTORY: Partners might have existing user directories such as Microsoft's Active Directory (AD), or a Lightweight Directory Access Protocol (LDAP) server. These directories contain user accounts and credentials that partners wish to use to access shared resources.

IDENTITY FEDERATION: Large organizations will often have an existing identity provider (IdP) which can federate your shared resources. These organizations will likely be technically savvy, so they should be able to take on user management (onboarding and offboarding of users).

NO IDENTITY TECHNOLOGY: For partners that are less technically mature and don't have an IdP or directory, you can create local accounts in your IdP for them. This is more demanding in terms of actively supporting your vendors or partners, as you will have to manage the partner's user lifecycles.

2 HOW DO I PROVIDE SECURE AND SELECTIVE ACCESS TO MY VENDORS AND CONTRACTORS?

Businesses typically have poor visibility into contractor and vendor user access levels, making it difficult to protect confidential data and securely connect users to their applications. By not adopting streamlined tools that make it easy for third-party users to access the tools and systems they need, businesses are seeing low rates of adoption and reduced partner loyalty.

It's important to understand that vendors and contractors don't require access to all systems, files, and folders across the organization. Instead, they need selective access, so they can only see and touch what they need to—which can be done with the following tools.

SINGLE SIGN-ON: Providing access needs to be as simple and straightforward as possible, yet highly secure. Single sign-on centralizes user access to applications through a consumer-friendly web portal that can be used on any device. It simplifies resource access and only allows users—both internal and external—to see the information they have been granted access to.

PASSWORDLESS AUTHENTICATION: Passwords are unmanageable within the extended enterprise. Not only are they inherently insecure and routinely forgotten or lost, they also increase the chances of users accessing information beyond their access level. Alongside single sign-on (SSO), a federated approach, such as SAML or OIDC, helps businesses to seize control of vendor access management. It's more secure, easier to manage, and enables IT to immediately revoke user access to their identity provider.

IDENTITY PROOFING: As businesses work with more third-party providers, they need to gain a deeper insight into the identity of users—namely, ensuring people are who they say they are. Providing multi-factor authentication (MFA) alongside other identity proofing features will put extra precautionary steps in place to minimize security risks. For example, Okta's identity proofing integrations enable users to securely verify their identities in the way the customer chooses — through documents, photographs, or security questions.

EXAMINE USER BEHAVIORS: In addition to gaining deeper proof of identity, it's also important to look at signals

How Okta customers provide secure access for partners and vendors

21ST CENTURY FOX

Collaboration is foundational to 21st Century Fox's decades-long success. In fact, according to the company's Global CISO, Melody Hildebrandt, "By design, our users are collaborating with third parties all the time." As a result, they needed an access and identity solution that could protect their employees and content, as well as adapt to a rapidly shifting partner ecosystem.

21st Century Fox uses Okta Identity Cloud to provide end-to-end protection and user-friendly provisioning and deprovisioning to users across its broad, complex network of employees, contractors, and partners.

> *Okta MFA accomplished a security goal, which was to make sure that the policy was enforced in the way that we had designed it. It also accomplished an enterprise technology goal, which was to give our users technology that delights them.*
>
> —Melody Hildebrandt, Global CISO at 21st Century Fox

around user behavior. This includes examining pertinent information, including the applications users are accessing, groups they are part of, their location, and the devices they are using. This is vital information that can provide red flags around potential risks to make third-party access management as secure as possible.

3 HOW DO I AUTOMATE USER PRIVILEGES AS MY VENDORS COME AND GO?

When you hire an employee, your IT and HR teams work closely to manage that user through their onboarding, any role changes, and offboarding. Onboarding contractors and vendors, however, often requires the involvement of other teams—particularly the department that the vendor is working with (e.g. marketing or engineering). In this scenario, the established process for lifecycle management might be ignored, and the possibility of security risks and overspending increases.

Many businesses waste significant time and resources on manually providing access to partner and vendor users via spreadsheets or email. This presents a number of issues, not the least of which are compromised security, delays in contractors getting access to the applications they need, and partner churn. To counter this, application access must be granted quickly and easily when a project begins, and then revoked as soon as it comes to an end. Okta Automations empower admins to automate these tasks, thereby saving time and eliminating the risk of human error. Here are a few examples of Automations in action.

SCHEDULED SUSPENSIONS: Businesses can automatically revoke user privileges that have been assigned to a specific group or project on a scheduled basis. For example, assume your contractors should have their access revoked at the end of the year. Okta's Lifecycle Management product can be scheduled to check if any users still exist within a specific group (e.g. Contractors) on Dec 31 and, if so, suspend their account and remove their access.

INACTIVITY-BASED SUSPENSIONS: It's also possible to automatically suspend users that have been inactive for a defined timeframe by setting up a condition that checks for inactive users within groups and routinely suspends their access to applications.

These approaches will ensure you have tighter control over access to your applications, especially if partners and contractors aren't proactive in managing their user accounts.

How Okta customers provide secure access for partners and vendors

DICK'S SPORTING GOODS

During the winter holiday months, Dick's Sporting Goods grows from four customer call centers to nine, which means all new agents must be onboarded in less than a month and deprovisioned in half that time after the holidays.

Manually, this process required an additional 1.5 full-time employees, however, Okta's hub and spoke approach allowed the company to significantly reduce their licensing costs and speed up their holiday ramp-up time.

> *Our Okta integrations have driven value into our customer service operations. With our existing and any new BPO partners, the ownership of identity becomes our partner's responsibility. This is a game changer for our IT support, and business operations teams.*
>
> —Eva Sciulli, Product Manager at Dick's Sporting Goods

4 HOW DO I VALIDATE PROPER COMPLIANCE IN VENDOR ACCESS MANAGEMENT?

It's often a struggle for businesses to protect confidential data and enable partners to securely connect to their applications. Achieving this requires good visibility into vendor and partner access levels alongside solid reporting, such as:

CURRENT ASSIGNMENTS REPORT: This demonstrates which users have access to which applications (and vice versa) and how they gained access.

RECENT UNASSIGNMENTS REPORT: This report details which users were unassigned from an app over a specified period. For example, if a company hires seasonal workers for three months, this report will prove they were given access in November and their access was effectively revoked at the end of January.

5 HOW DO I OFFLOAD MANAGEMENT OF PARTNER AND VENDOR USERS?

To prevent your IT team from being overwhelmed, you can offload the management of your third-party users.

SELF-SERVICE: Your business can provide self-service features that enable vendor and partner users to manage minor account issues themselves. This will reduce IT helpdesk calls, allowing your IT team to focus on more impactful tasks that add value to the organization.

DELEGATED ADMINISTRATION: You can also implement admin roles to offload certain areas of partner and vendor access management. For example, a helpdesk admin role allows admins to reset passwords and account lockout, and it can be outsourced to contractors. These types of admin roles can be scoped to ensure they can only manage certain groups of users.

How Okta customers provide secure access for partners and vendors

HENDRICK AUTOMOTIVE GROUP

Previously, Hendrick's employees worked across multiple auto dealerships requiring an intricate employee tracking system made up of over 100 independent HR systems. When they made the decision to consolidate, they turned to Okta to help them automate 99% of their lifecycle management.

Now, everything from onboarding to termination is automated using Okta, and senior execs insist any new solution or idea integrates with Okta.

> *Okta was the answer for getting us out of the manual processes that we were firmly in—which took a lot of time, didn't get the right information fast enough and wasn't accurate. We now churn through about 150 provisioning and deprovisioning events a week, which isn't something we could keep up with before.*
>
> —Amy Frost, Director of IT Engineering, Hendrick Auto

How Okta can help

Okta provides a suite of identity solutions that help enterprises provide secure third-party access to their applications and systems.

LIFECYCLE MANAGEMENT

Lifecycle management is the process of maintaining the lifecycle of a user account from onboarding, through role changes, and on to termination. Okta's Lifecycle Management simplifies this task by taking businesses away from manual provisioning in favor of an automated, policy-driven, and contextual approach. This provides IT with a centralized view into which users have access to which systems and files and helps the business assign and revoke access and licenses.

SINGLE SIGN-ON

Okta's Single Sign-On centralizes user access to applications through a consumer-friendly web portal, which can be used on any device. Users sign into the portal and Okta manages authentication to the applications they are assigned access to based on their role. This way, you can have peace of mind that your contractors and vendors only have access to the information they are authorized to see.

UNIVERSAL DIRECTORY

Okta's Universal Directory provides one place for businesses to manage their users, groups, and devices, all of which are mastered in Okta or various sources. It enables businesses to securely store an unlimited number of users and attributes, such as linked-objects, sensitive attributes, and predefined lists, as well as users and passwords.

ADAPTIVE MFA

As data breaches become more sophisticated, it is increasingly important for businesses to protect their customer and employee data. Okta's Adaptive Multi-factor Authentication frees businesses from cumbersome, insecure password entry logins. The approach improves company security, simplifies management for IT, and provides simple logins for all customers and employees.

Secure access management for all

In the past, an organization's network was their perimeter, but that's simply not the case anymore. Thanks to portable devices and cloud computing, the perimeter is constantly expanding and contracting as users come and go, and organizations must adapt in order to maintain the high level of security required to operate in a zero-trust environment.

If your organization is moving toward modernizing your lifecycle and access management for employees and your extended enterprise, it's understandable you'll have questions. For many, the answers can be found in an all-in-one solution designed to drive business growth and agility.

If you're looking to better protect and enable your employees, contractors, and partners, learn more about Okta's collaboration solutions today.