okta

Okta for Global, Distributed Organizations

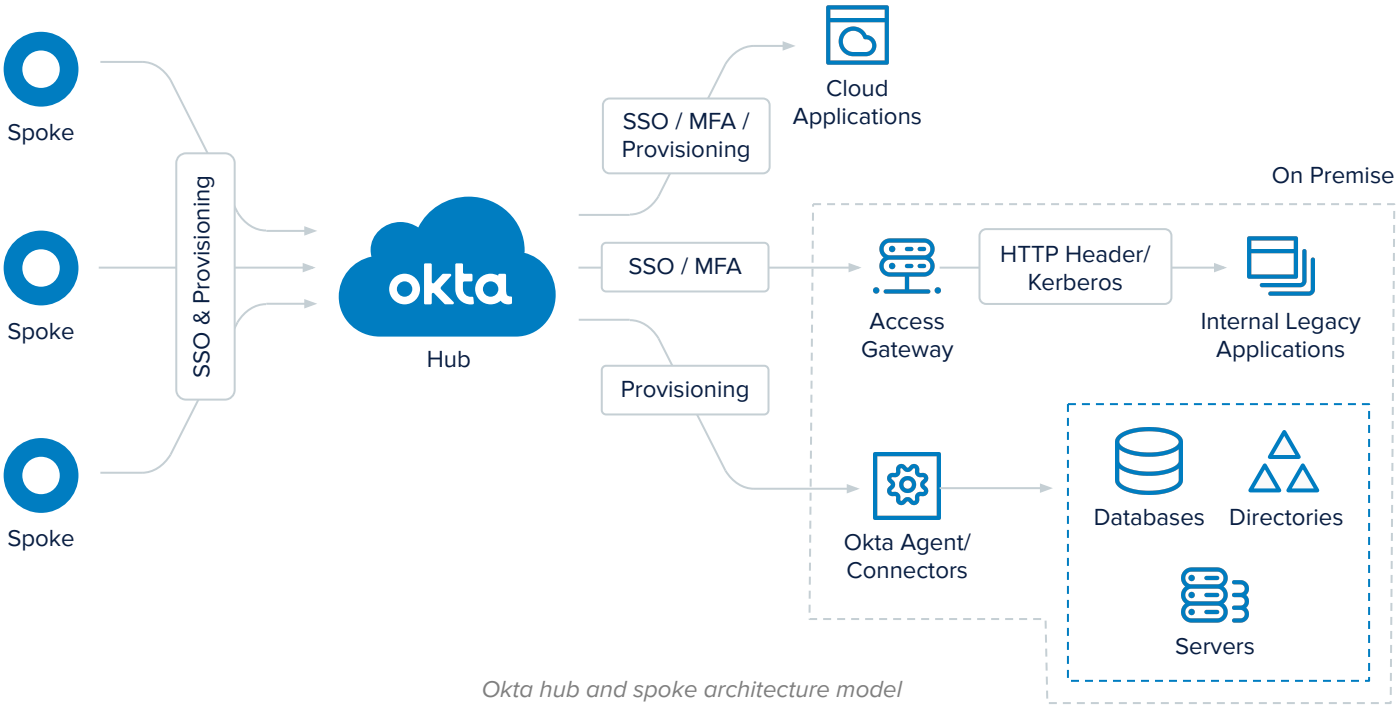
Managing Services Across a Global Organization or Diverse Business Units

For large organizations comprised of numerous independently managed business units, centralizing identity can be extremely challenging. Business units and regional offices often operate independently, making their own decisions and managing their own technology. Multinational organizations must adhere to regulatory requirements related to data residency, and the ambitious goal of a centralized identity can seem impossible given the need to store personally identifiable information (PII) within each respective country. Finally, organizations looking to augment their capabilities for either the short term (i.e. seasonally) or for the long term (including M&A) have challenges centralizing identities originating from outside of their organization.

In this paper, we'll break down how a 'hub and spoke' identity model can serve as the foundation for unified services across an entire organization, while allowing for specific application flexibility across distributed information technology (IT) organizations. We'll also review a few example use cases for how this hub and spoke model is leveraged for deployments in some of the world's largest organizations.

Okta's Hub and Spoke Architecture

The hub and spoke model enables organizations to physically and logically separate a collection of identities from one another through the use of multiple Okta tenants (also referred to as Okta Orgs). The flexibility that this model provides allows organizations to address complex use cases typically driven by business, technical, and/or compliance requirements. Through the use of the Okta Integration Network's (OIN) Org2Org connector, multiple Okta orgs can be integrated together to enable both single sign-on (SSO) and provisioning within a matter of minutes.



Okta hub and spoke architecture model

In this architecture, the hub and spoke functions as the following:

Hub

A single Okta Org, acting as a hub, operates as an independent service provider (SP) to the spoke(s), and is responsible for providing directory services, authentication, and authorization services in a centralized manner. The hub then uses common identity standards to act as an identity provider (IdP) and integrate with downstream applications to provide seamless and secure access from an SSO (e.g. using SAML, WS-Federation, and OpenID Connect) and provisioning (e.g. using SCIM) perspective.

Spoke

One or more Okta Orgs, acting as individual spokes, operate as independent identity providers (IdP) responsible for providing directory services, authentication and authorization services. While these responsibilities are identical to the hub, the spokes provide these capabilities in a decentralized manner for users within each spoke. Spokes utilize their own instance of Okta's Universal Directory and store user profile and group information which can be created directly in Okta (i.e. Okta as the source of truth) or sourced from other repositories such as Active Directory, LDAP, or even HR applications.

The spoke(s), leveraging the Okta Integration Network's (OIN) Org2Org connector, will provide seamless and secure access by provisioning user profiles into the hub as well as enabling SSO to any applications or services integrated with the hub. This model can then be used in a variety of scenarios for organizations that manage both internal employees as well as customer or partner identities.

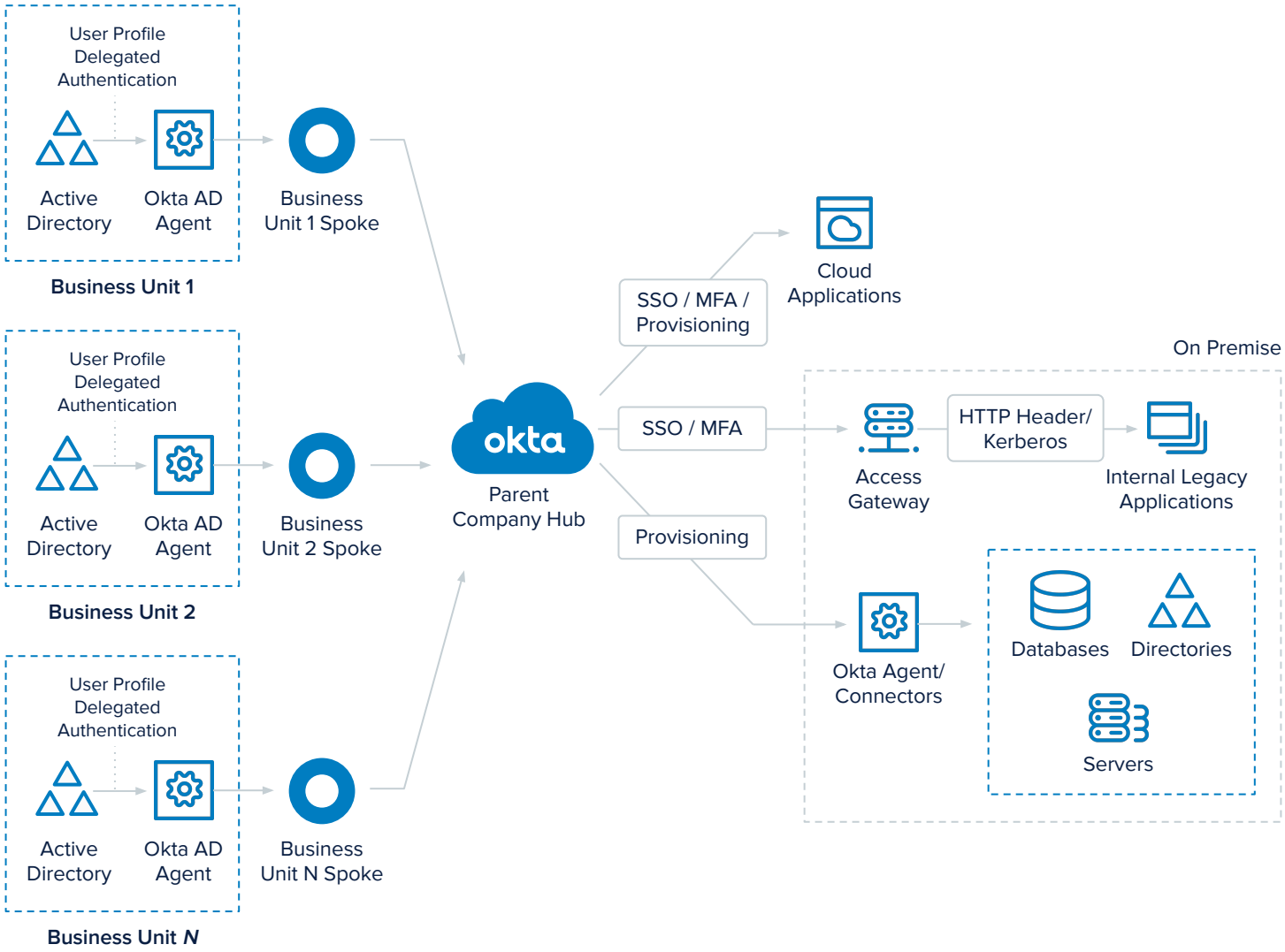
Deployment Models

Designing a hub and spoke architecture for your business can help to ease centralized management of resources while providing flexibility for distributed IT organizations. Businesses can leverage a hub and spoke model in a few different ways, and we'll walk through different deployment models in this section.

Deployment Model 1: Large Organizations with Multiple Business Units

Large organizations can be comprised of numerous independently managed business units which can make their own decisions around the selection of various technology solutions and may also have their own personnel responsible for managing these IT investments. While these business units operate independently, parent organizations looking to lower overall cost and improve efficiency across the entire organization may offer various technology services and platforms to all business units through a shared services model. Enabling these independent business units to participate in a shared services model for various applications and platforms while not requiring them to relinquish their independence can be a difficult challenge both organizationally and from a technology perspective.

As depicted in the following diagram, by leveraging the Okta Identity Cloud with a hub and spoke architecture, the Parent Company (i.e. hub) is able to deliver various applications and platform services, both on premise and cloud-based, without disrupting the individual business units or requiring them to relinquish any control of their existing user repositories and technology investments. Individual business units will utilize their existing Active Directory user repository, which they manage themselves, to not only provide access to their applications via the spoke, but to also enable access to applications provided by the hub in a shared services model. Business Unit users will access all applications, including applications provided by the hub, in a seamless and secure manner (i.e. SSO) and continue to authenticate using their existing Active Directory credentials. Finally, the hub can provision user access to downstream applications and user repositories where appropriate.



Deployment Model 1: Large Organizations with Multiple Business Units

Spotlight: NTT Data

A top priority for NTT has always been security. For large organizations like NTT, workforce turnover and role changes add to the pain of manual provisioning tasks that not only drain IT resources, but risk security vulnerabilities through orphaned accounts and credentials.

To address this, NTT Data's hub and spoke model manages its 125K+ employees - some of whom with the same names - to keep each person's information, logins and apps organized. NTT adopted the Okta Identity Cloud to automate provisioning tasks and allow each company to remain connected, yet operate autonomously. One of NTT's goals was for every employee to have the same NTT branding email. Behind the scenes, the central identity hub knows every identity ever created across the 900+ companies and has created a branding suffix to ensure that no one person can crash or collide with another identity across the different spokes.

Okta enables NTT to have one single provisioning point where it can provision everything in its central hub and then connect to every office — keeping all of NTT's organizations aligned, while still allowing them to operate as individual entities. Additionally, NTT's IT teams now have a clean graphical user interface to seamlessly combine custom actions across applications and within specific time frames to enhance security and efficiency within the enterprise.

Deployment Model 2: Multinational Organizations with Data Residency

Over the last several years, governments have become more involved in the protection of an individual's data privacy through the passage of various laws and regulations. These protections are afforded to citizens who may be employees, partners, and/or customers of an organization. In addition, many of these laws and regulations can vary by country and oftentimes require that the personally identifiable information (PII) of a citizen reside within their respective country (i.e. data residency requirements). Multinational organizations are having great difficulty delivering applications and services to their employees, partners, and customers in this highly complex regulatory environment.

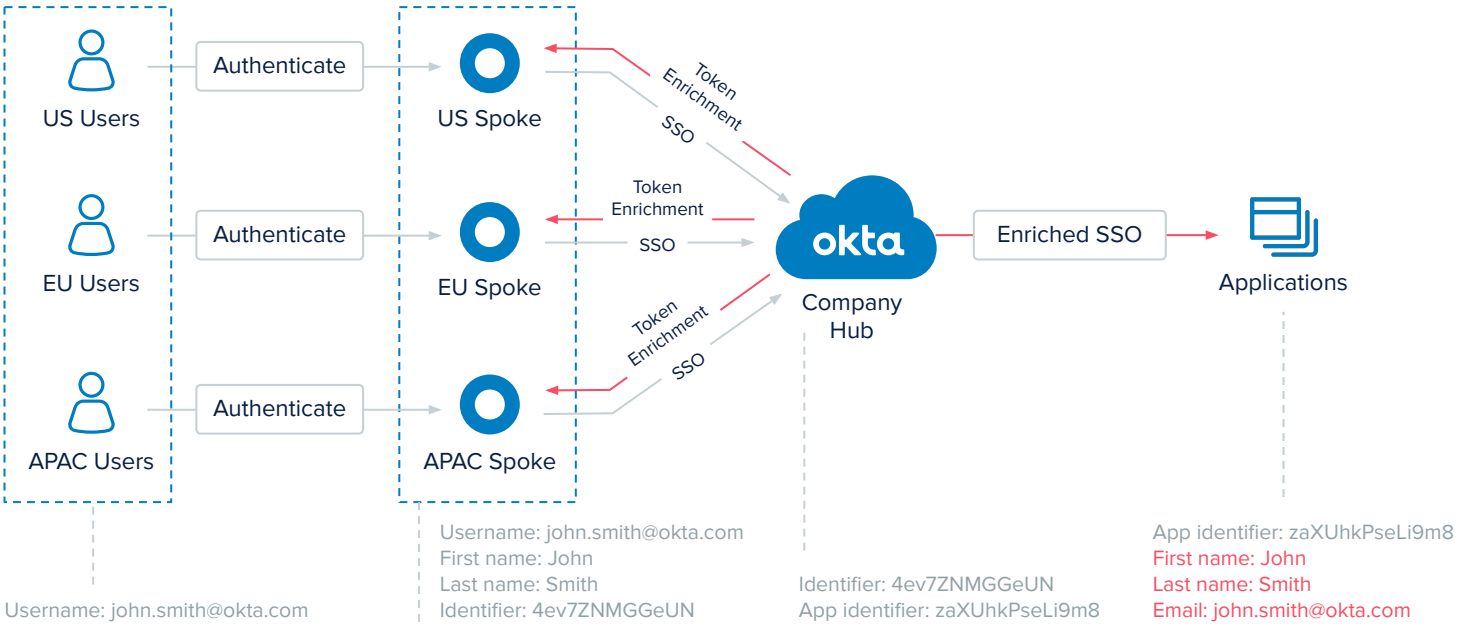
By leveraging the Okta Identity Cloud with a hub and spoke architecture, a hub is able to deliver various applications and platform services, while ensuring that PII remains persistently stored only within the users' appropriate region (i.e. spoke) and conforms to data residency requirements for employees, customers, and/or partners.

Each region (US, EU, and APAC) will employ their own spoke, located in their respective region, to persistently store user profile information including PII and adhere to data residency requirements. These regional spokes will store user profile information containing PII that was created either directly in their spoke (i.e. Okta Mastered) or sourced from other repositories such as Active Directory, LDAP, or even HR applications (depending on the type of user).

Maintaining Privacy

In addition to storing user profile information which contains PII, regional spokes will also store a unique identifier (e.g. Identifier) for each user profile. This unique identifier will be constructed without containing any PII and be used as a referenceable key when creating persistent identities outside of the region as well as during runtime when users access applications (i.e. SSO). Leveraging this unique identifier will ensure that both user privacy and adherence to data residency requirements are maintained. Additionally, if downstream applications integrated with the hub require PII at runtime (i.e. during user access via SSO), Okta's powerful Hooks capability, can be utilized at the hub to enrich identity tokens with PII stored at the spoke. These enriched tokens are then passed to the downstream applications.

It is important to note that use of the Okta Hooks functionality will not result in the persistent storage of PII at the hub and that the PII is purely transient in nature. That being said, applications that utilize the enriched token, which contains PII, must only utilize the information during the user's session at runtime. Applications must not persistently store the PII (e.g. database storage) as this would not conform to privacy and data residency requirements.



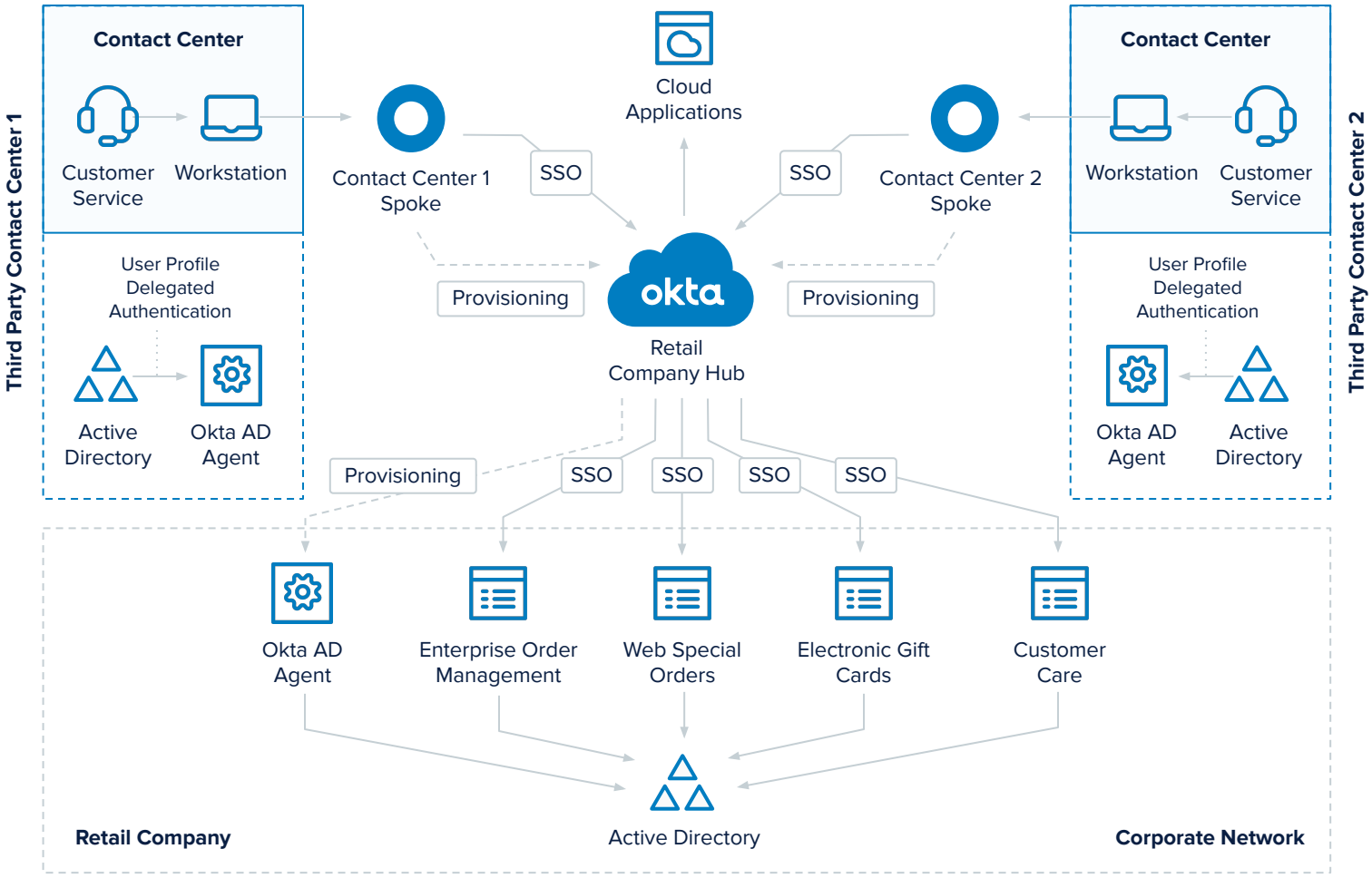
Deployment Model 2: Multinational Organizations with Data Residency

Deployment Model 3: Third-Party (Including Contractor) Outsourcing

Many organizations outsource business functions (e.g. call center outsourcing) for various reasons such as increased efficiency, lower cost, or to elastically scale their business during high demand (seasonal) peaks. Organizations looking to provide outsourced personnel with seamless and secure access to applications and services that have been traditionally architected for employee use only can pose unique technology and security challenges.

By leveraging the Okta Identity Cloud with a hub and spoke architecture, a Company (i.e. hub) is able to deliver various applications and platform services, both on premise and cloud-based, to outsourced personnel. Each third-party outsourcing organization will leverage their existing Active Directory user repository and Okta spoke, which they could either manage themselves or use their own IdP to federeate into the spoke. Third-party outsourcing organizations will access applications and platform services provided by the hub, in a seamless and secure manner, from both an SSO and provisioning perspective. In addition, outsourced personnel will continue to authenticate using their existing Active Directory credentials. Finally, the hub can provision user access to downstream applications and user repositories where appropriate.

It is important to note that while the company is relying on the third-party outsourcing organization to properly manage their personnel in Active Directory to ensure appropriate access, the company can still enforce its own security policies within the hub related to access through the use of Okta groups and group membership rules. The use of multi-factor authentication via Okta sign-on policies can also be implemented via the hub to add an additional level of security if required. In the event of an emergency situation where immediate termination of an individual's access is required, the company can suspend or deactivate the user access immediately within the hub without requiring any assistance from the third-party outsourcing organization, their Active Directory, or their spoke. Finally, if the outsourcing partnership is terminated, the company (i.e. hub) can disconnect a spoke and immediately terminate all access for users of that spoke.



Deployment Model 3: Third-Party (Including Contractor) Outsourcing

Spotlight: Dick's Sporting Goods

Dick's Sporting Goods—the largest omni-channel sporting goods retailer in the US—has a seasonal workforce that relies on outside contractors. During the winter holiday months, the organization grows from four customer call centers to nine. As a result, its IT team needs to onboard all new agents in less than a month, and deprovision them in half that time after the holidays. This manual onboarding required an additional 1.5 full-time employees, prompting the organization to look for a more efficient and affordable way to grant new teammates the tools they needed to succeed.

Okta's hub and spoke approach provided the solution they were looking for. Each of their Business Process Outsourcing (BPO) partners each manage their own Okta spoke, which then connects into the Dick's Sporting Goods hub. From there, the Dick's Sporting Goods team has the ability to provision the call center, internal applications, order management, web special orders, gift cards, et cetera. The Dick's Sporting Goods team also gives BPO partners access to external applications that require authentication, such as carriers, fulfillment partners, etc. -- and all via a repeatable process that can be used with multiple BPOs.

Since implementing Okta, the company has significantly reduced its licensing costs and sped 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. Our agent teammates have simplified access to our tools, as well as self-service password resets," said Eva Sciulli, IT Product Manager for Customer Interaction at Dick's Sporting Goods.

Hub and Spoke for Your Organization

A hub and spoke model enables organizations to provide centralized identity services across the organization while offering the flexibility required with distributed IT organizations. In doing so, organizations can deliver seamless, secure access to technologies for their entire extended workforce (e.g. employees, partners, and contractors) as well as customers that may be distributed either logically (via technology) or location (geographically).

Additional Resources

- For more specifics on M&A use cases, check out our Okta M&A podcast here.
- For more details on B2B federation with Okta, view our whitepaper here.
- Hear more from the Dick's Sporting Goods team on their Okta deployment in their Oktane session here.

For more help on architecting a hub and spoke model for your use case, reach out to Okta.com/contact.