okta

How Identity Integrates Office 365 with HR and Security Systems at Nexteer Automotive

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

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

A leader in intuitive motion control, Nexteer is a multibillion-dollar global steering and driveline business delivering electric and hydraulic steering systems, steering columns and driveline systems, advanced driver-assistance systems (ADAS) and automated driving technologies for OEMs around the world.

Locations: 42 locations worldwide, including manufacturing plants, customer support, and technical support centers

User Count: 7,000 knowledge workers, 14,000 total workforce

Industry: Automotive

Okta + Office 365 Benefits

- **Automated:** provision and deprovision user accounts
- **Seamless:** Assign and revoke licenses based on Active Directory changes
- **Flexible:** Anywhere, anytime access to Office 365
- **Secure:** Multi-Factor Authentication to Office 365 services like SharePoint
- **Scalable:** Integration support for additional Office 365 services and deployment to all users

Customer Profile

Nexteer Automotive is a US $4 billion Tier 1 supplier to Ford, GM, and other automotive manufacturers. Although Nexteer was formed from a 2007 divestiture from Delphi Steering, its origins date back to 1906. From its earliest innovations in mechanical power, assembly line production, to computer automation, Nexteer is now building internet-connected physical systems.

Risk Profile

Automobile component manufacturers face pressures of global competition and rising customer demand. These pressures can only be met through digital transformation—but only about five percent of manufacturing executives are satisfied with their digital strategies.[1] Nexteer is tackling a whole new level of security challenges—including more locations, suppliers, and an interdependent supply chain—all with connectors into Nexteer's network. Every point of entry into Nexteer needs to be secured, including access by employees, OEM business partners, suppliers, and contractors.

Goals and Proposed Solution

Nexteer's chief information security officer, Arun DeSouza, conducted an enterprise risk assessment shortly after joining the company. Some of the key areas of focus he identified included loss of intellectual property, cloud computing governance, secure employee onboarding and offboarding, and network security. DeSouza knew that connecting more devices and systems to the internet would raise the organization's risks of data breaches. With Europe's General Data Protection Regulation (GDPR)[2] now in effect, privacy is also a major concern for companies doing business in Europe. Depending on the severity, GDPR can penalize two to four percent of a company's revenue. Nexteer is taking these risks seriously with a measured and responsible approach toward digital transformation.

To increase productivity and innovation, Nexteer chose to adopt a common set of cloud applications across the organization, including Office 365, SAP SuccessFactors, Concur, DocuSign, and Salesforce. They needed to minimize risk by automating user lifecycle management, and reduce threats by integrating security elements across applications, services, and infrastructure. However, Nexteer was globally dispersed, and had a disjointed IT infrastructure with multiple software tools being used in different locations. To adopt a "One Nexteer" focus across their entire organization, DeSouza wanted to consolidate the technologies down to those that worked seamlessly together, and enabled cloud transformation.

[1] http://mktforms.gtnexus.com/rs/979-MCL-531/images/GTNexus-Digital-Transformation-Report-US-FINAL.pdf
[2] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

After its divestiture from Delphi Steering, part of Nexteer's IT assets included a carved-out portion of Delphi's old Active Directory, which needed to be stabilized. DeSouza worked with Microsoft to restructure their Active Directory for better performance and security. Then, he broke down Nexteer's strategy into three phases:

Phase 1: Embrace the cloud

The company's restructured Active Directory now serves as the foundation for identity across the entire organization. DeSouza and his team conducted a proof-of-concept evaluation of Okta's Enterprise Lifecycle Management and Single Sign-On integration with Active Directory. After Okta met the success criteria, Nexteer acquired the Okta Identity Cloud.

Now end users authenticate once (using their Active Directory credentials) and get federated Single Sign-On for about 15 enterprise cloud applications as well as some custom applications. Additionally, IT admins have privileged access to IT services and infrastructure. Okta manages it all based on Active Directory identity and group policy.

Multi-Factor Authentication

To protect against credential theft, Nexteer decided to enforce strong authentication to secure access to their services. The company deployed Okta Multi-Factor Authentication to secure access to their applications, networks, and devices.

Office 365

Office 365 was one of the first applications to be provisioned across the 7,000 knowledge workers at Nexteer. Compared to their earlier email and collaboration suite, Office 365 scales well to support adding new users through mergers and acquisitions. It also reduces costs by eliminating the need to purchase separate point products, like web conferencing. Choosing Okta, instead of a traditional identity federation solution, for Office 365 helped the company deploy faster and achieve security and privacy compliance for regulations like the GDPR.

Okta + Office 365 Deployment Timeline

Nexteer IT installed and connected Okta to Office 365 within minutes. They tested and deployed components of Office 365 to over 7,000 users in four stages—starting with Yammer, then Skype for Business, OneDrive, and finally email.

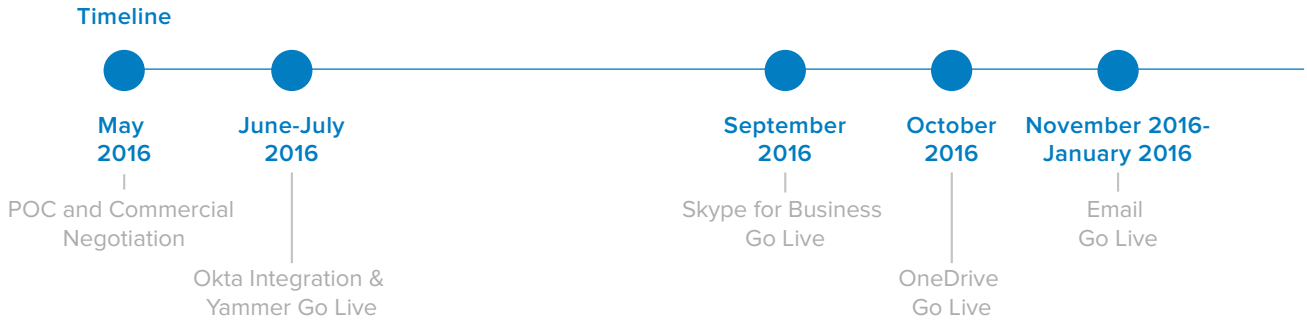

Figure 1. Office 365 Deployment Timeline

"With Okta's with automated provisioning, we were able to power through the Office 365 integration in a day or two."

Arun DeSouza, Nexteer CISO

Okta + Office 365 Benefits

- **Automated:** provision and deprovision user accounts
- **Seamless:** Assign and revoke licenses based on Active Directory changes
- **Flexible:** Anywhere, anytime access to Office 365
- **Secure:** Multi-Factor Authentication to Office 365 services like SharePoint
- **Scalable:** Integration support for additional Office 365 services and deployment to all users

Phase 2: Minimize Risk with Automated User Lifecycle Management

Nexteer onboards a large number of employees on a regular basis. With this in mind, they sought an automated user lifecycle management system to:

1. Uniformly grant privileges for a particular role
2. Manage the lifecycle of the employee as they transition between roles and responsibilities
3. Accurately deprovision users when they leave the organization

HR-Driven Identity: SAP SuccessFactors with Okta Lifecycle Management

Instead of relying on IT to manage the user lifecycle, Nexteer wanted to take advantage of SAP® SuccessFactors to start the onboarding process. SuccessFactors was already being used by the company's Human Resources department. Now it was time to take SuccessFactors to the next level—by integrating it into the IT workflow using Okta's Lifecycle Management.

But even with a powerful human capital management (HCM) tool, the onboarding process for new hires can still be painful—often requiring the IT department to manually respond to a ticket and create accounts in apps and systems for each new user. It has also been difficult for IT to synchronize HR user records between Active Directory and enterprise applications. This challenge increases as more people join the organization, change job roles over time, manually update their own information, and leave the company. Okta's integration with SuccessFactors ensures that Nexteer's HR department can drive the entire employee lifecycle from onboarding, to role change, to offboarding.

Less Time Spent Provisioning New Users

In the past, using native tools, Nexteer IT needed days or even weeks of effort to complete all the tasks required to onboard a new employee. Now, Okta is the hub for identity between Active Directory and SuccessFactors. Nexteer's IT teams can ensure the right people are automatically provisioned for the right set of applications and services. The only manual intervention is when Human Resources enters a new employee's information into SuccessFactors, and when IT receives the automatic workflow request to create their user account in Active Directory. All other attributes in Active Directory are populated automatically: Okta's pulls information from the employee's HR record in SuccessFactors and populates Active Directory group memberships and permission levels based on their organization and role.

Steps	Using Native Tools	Using Okta Lifecycle Management
Add employee to HR system	5 minutes	5 minutes
Send requests to IT, Facilities, etc.	10 minutes	Automatic through SuccessFactors automated workflows
Create user account in Active Directory	10 minutes	5 minutes—populate user information into Active Directory from SuccessFactors records
Add user to groups	10 minutes	Automatic—(provisioned with Okta Group Membership Rules)
Apply administrative permissions	5 minutes	Not necessary (managed units)
Create home directory	5 minutes	Automatic
Create mailbox	5 minutes	Automatic
Create user account in other applications	10 min per application	Automatic
Effort	60 minutes	10 minutes
Elapsed time	Days to weeks	10 minutes

Figure 2. Provisioning Users: Native Tools vs. Okta Lifecycle Management

Immediate Revocation of Access Rights When Employees Leave

Using Okta Lifecycle Management, Nexteer IT can automatically disable a departing user's account in Active Directory, immediately revoke all access to cloud applications and Office 365 email, and pull and reassign Office 365 licenses. Alternately, an HR manager may go into SuccessFactors and change the employee status to "Terminated" or "Inactive". Okta reads either action and synchronizes information so that Okta, SuccessFactors, and Active Directory all have the same information.

SuccessFactors + Okta Solution Benefits

- Automatic provisioning and deprovisioning between Success Factors, Active Directory, and enterprise applications
    - Create and deactivate Active Directory accounts, driven by changes in SuccessFactors
    - Schedule data synchronization hourly, daily, or on demand
    - Centralize reporting and audit access across all enterprise systems
- Comprehensive identity lifecycle management
    - Implement fully-automated Active Directory group management
    - Create Active Directory security group memberships
    - Match group these security group memberships to SuccessFactors provisioning groups
    - Automate application provisioning and deprovisioning based on the group's authorization level

Phase 3: Reduce Threat Vectors by Integrating Security from Proofpoint and Zscaler

Nexteer's security model is based on three broad layers: Application Security, Services Security, and Infrastructure Security. They rely on Okta to tie identity into every layer—from application security, authentication and identity management, and security monitoring. To strengthen email, web and infrastructure security, the company also utilizes services from Proofpoint and Zscaler.

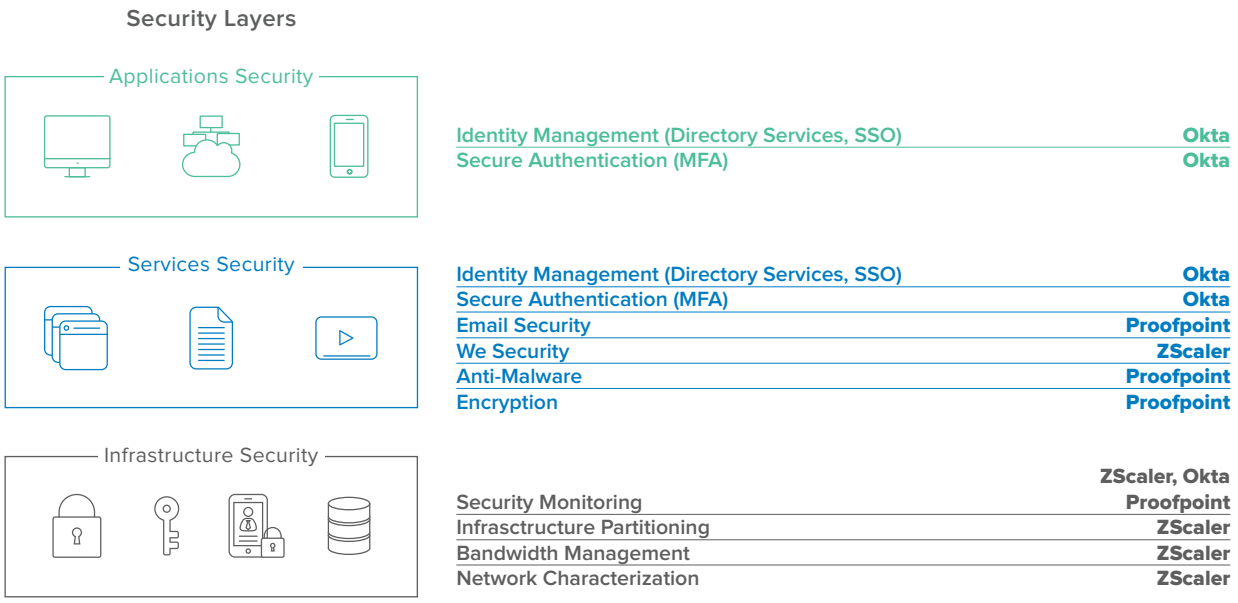

Figure 3. Tools Mapped to Nexteer's Layered Security Architecture

Email Security with Proofpoint + Okta

Proofpoint secures Office 365 email, and provides anti-malware and encryption services, while its threat intelligence prevents, detects and notifies Nexteer of threats spanning email, network, mobile apps, and social media. The security team gets the visibility and intelligent reporting they need to filter through the noise and respond quickly to real incidents.

Okta's ability to provision users into cloud-based Azure Active Directory improved Nexteer's Proofpoint deployment. Before implementing Okta, Nexteer IT had to populate Proofpoint with new or changed user records from Azure Active Directory every day or every week, depending on workforce fluctuations. Okta keeps users and groups synchronized between Active Directory and Azure Active Directory. Now Proofpoint's rules protect all user accounts.

Without Okta, synchronizing users and groups into Proofpoint required either manual updates, or a custom application built on the Microsoft Azure portal. Using Okta as the identity hub has increased the efficiency and automation for Proofpoint's email protection, while reducing the attack surface for the organization.

Benefits of Proofpoint + Okta

- **Transparent service provisioning:** Okta powers service provisioning directly to Proofpoint, increasing Proofpoint efficiency and automation
- **Automated synchronization:** Proofpoint compliance and threat protection now covers all user accounts without relying on manual updates to Azure Active Directory

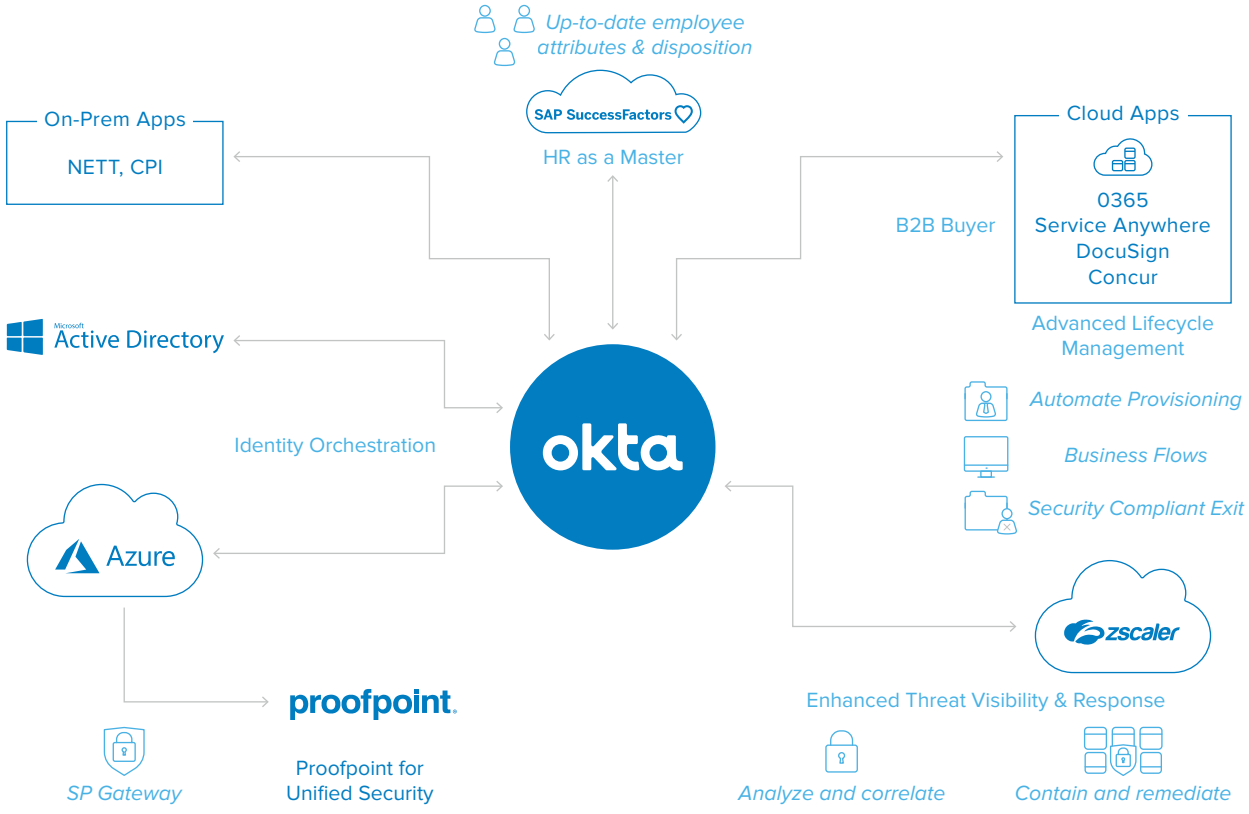

Figure 4. Okta is the Hub of Nexteer's Identity Architecture

Scaling Security for the Cloud with Zscaler + Okta

As Nexteer began to move to the cloud, they found their traditional hub and spoke architecture couldn't handle the sudden spike in cloud application traffic. Their on-premises internet gateways and security appliances were designed to provide real-time visibility, traffic inspection, threat protection, and URL filtering for all internet traffic—but could not support direct-to-cloud connections. Backhauling cloud traffic through on-premises device proxies was slowing everything down. DeSouza realized that he could no longer fix the problem by adding more hardware. Instead, he needed to find a security platform that was built for the cloud.

Nexteer deployed Zscaler Internet Access, a solution that offers two main components: a software defined wide area network (SD-WAN) for better, faster access to cloud applications like Office 365, and a security stack as a service for access control, data protection, and threat prevention.

Zscaler made it possible for Nexteer's knowledge workers, some who travel extensively, to access their cloud applications from any location without performance lags. Traffic is no longer forced through the company's on-premises internet gateways and security appliances. Zscaler helped Nexteer to add or remove branch offices with greater ease and speed than if they had been using device proxies in their data center.

Zscaler Improves the Office 365 User Experience

Slow performance in Office 365 is why Nexteer turned to Zscaler in the first place. The initial data migration from on-premises Exchange servers to Office 365 had been choking the network. Post-migration, the situation wasn't much better. Each user's Office 365 client software opens from 20 to 30 connections to the Office 365 platform, causing performance lags—especially when traffic isn't routed to the closest Microsoft data center. Since deploying Zscaler with Okta, end users get a fast and secure connection to Office 365. Okta manages end-user access to Office 365 through a combination of Single Sign-On and Multi-Factor Authentication. Zscaler manages the connections and dedicates 40 percent of Nexteer's bandwidth to handle Office 365 traffic.

Zscaler and Okta, Better Together

Okta's Security Assertion Markup Language (SAML)[3] integration with Zscaler enables just in time provisioning of users to the Zscaler database to enforce policies. Ongoing SAML assertions from Okta let Zscaler know that traffic has been authenticated. The System for Cross-domain Identity Management (SCIM)[4] integration with Okta helps Zscaler maintain user information including whether users have changed groups and job roles.

As part of the Okta Integration Network, Zscaler relies on Okta to provide information about users and how to enforce group level security policy—such as which groups of users should have access to which apps, or which groups are authorized to send sensitive customer information over the internet. While originating user records are created SuccessFactors, Zscaler relies on the centralized identity data from Okta to enforce security policies.

Benefits of Zscaler + Okta

- Rapid access to Office 365 from any location
- Eliminated need for on-premises device proxies
- Guaranteed 40% of network bandwidth reserved for Office 365
- Transparent, Okta-powered service provisioning directly to Zscaler
- Real-time visibility with a holistic view of enterprise internet and Office 365 traffic

[3] https://www.okta.com/blog/2016/12/what-is-saml/
[4] SCIM, or System for Cross-domain Identity Management, is an open standard that allows for the automation of user provisioning.

Outcomes

Nexteer's vision is to connect everything: users, digital factories, and Internet of Things (IoT) enabled devices. While adhering to their original investments in Active Directory, the company accomplished a complete cloud transformation across their entire organization. They chose Okta to enable this transformation—because it simply worked.

"After spending two weeks trying (and failing) to connect Active Directory to the cloud using 'traditional methods,' in the span of four hours, we connected everything to Okta," DeSouza said.

Blending strong security with high usability is key for Nexteer. Knowledge workers need the right tools and easy access to get their jobs done, no matter the location. The company needs to know that every point of entry into their organization is secured, and identifiable. For Nexteer, Okta is the lynchpin that holds all aspects of security together.


okta