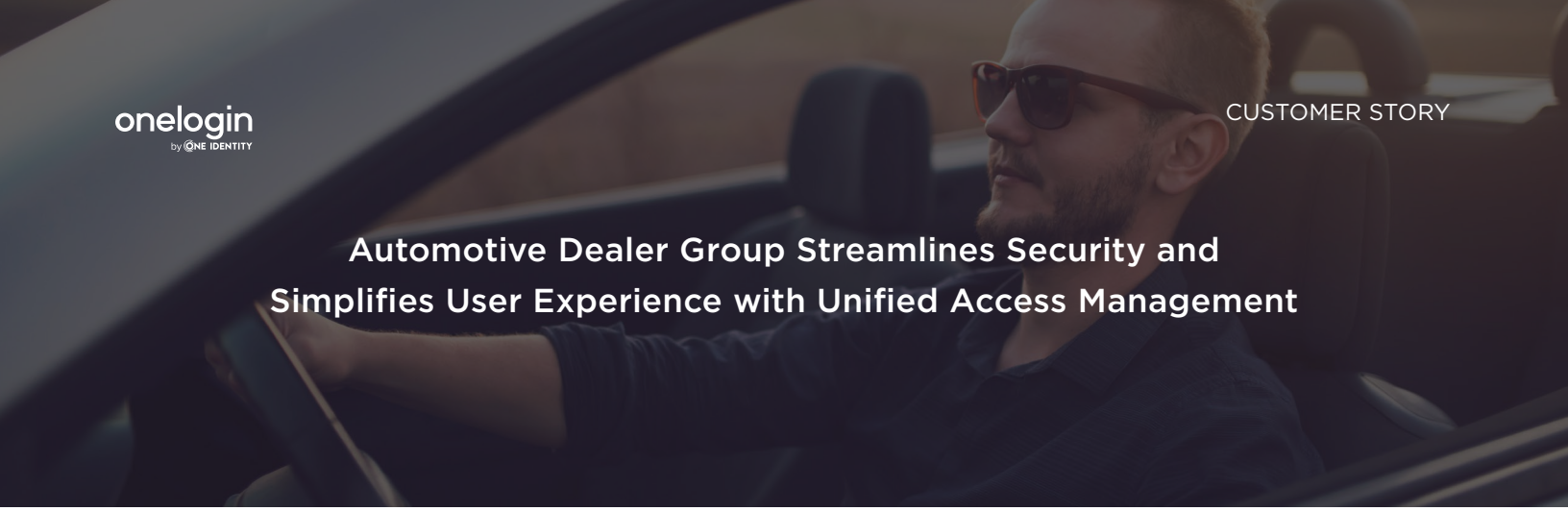

onelogin by ONE IDENTITY

CUSTOMER STORY

Automotive Dealer Group Streamlines Security and Simplifies User Experience with Unified Access Management

"OneLogin is the perfect way to centralize security management, and to provide users with a very clean and controlled experience."

DIRECTOR OF IT

Comprising a large dealer group of luxury automotive brands, including Audi, BMW, McLaren, and Porsche, this automotive dealer franchise has retail locations in three major metropolitan areas, as well as a vehicle design operation.

CHALLENGES

In the luxury automotive world, where managing high volumes of retail transactions involving customer data, multiple dealer locations, and remote employees accessing dealer management systems is a daily task, security is a huge deal.

"As we doubled in size over the past two years, we began building a brand-new IT infrastructure that embodied enterprise-level security components. With over 1,200 employees, the importance of ensuring identity, that everyone is properly authenticated, with controlled access in a unified manner, became very apparent," says the Director of IT for the dealer group.

Many users from various departments, such as Finance, IT, and some dealership staff, needed remote network access to applications using the Cisco Meraki VPN. They would be prompted for their username and password, and then a separate login for their computer. Common apps included RingCentral's cloud phone system, Office 365, and Box, as well as Zendesk and Oomnitza for helpdesk and asset management, respectively.

"For a dealership employee, you need to log in to dealer management software, then a quoting system, and maybe a CRM. All employees have email and a company intranet. Each of these have their own logins and passwords. This growing set of events created the need and the business

INDUSTRY

Automotive Retail

SIZE

1,200 employees

INTEGRATIONS

Apps: Box, Zendesk, RingCentral, Oomnitza; Dealer management systems
Networks: Cisco Meraki VPN

CHALLENGES

Confusion and inefficiency from multiple logins and passwords

Tighten VPN & cloud app access

Need to protect security of customer data and transactions

SOLUTION

IAM with unified portal for cloud apps and VPN network access

Real-time AD sync, MFA

Auto form fill for non-SAML apps

RESULTS

Simplified user experience increases adoption

Greater efficiency for end users and IT drive productivity gains

Centralized security maintains real-time access

case to look into identity platforms to secure access in a unified way. At the same time, we were building out a brand-new infrastructure, and looking ahead, we knew that Active Directory was the foundation, and then we wanted to further secure other things within an IAM provider," say the IT director.

SOLUTION

"We did evaluate a number of vendors, Okta in particular. At the time, OneLogin didn't have a push token for MFA, which in our eyes, was kind of a negative. Okta came in and said, 'we have that, and have for a really long time.' So it was tempting. But what helped us make a decision was your sales team--your pre-sales team, in particular. They helped us understand it was coming in the road map--in fact, the push token released when they said it would. But the reality was, we didn't need it for the initial rollout anyway," recalls the IT director.

What did make a difference was the Active Directory integration. He explains, "OneLogin didn't require us to set up ADFS, which as a federated service, adds complexity to your environment. So if we went with Okta, we'd need more Windows server components to integrate AD and even things like Office 365. So we could see that OneLogin would be an easier implementation and setup. And it's really proved that way."

Another key difference was the ability to manage access beyond just apps. "With OneLogin, not only can we connect our cloud-based software through SAML authentication, it has enabled us to secure our VPN access using the same platform as well. So it's really helped us with identity and access management," says the director.

The company's solution is made up of Cisco Meraki security appliances, with Active Directory on the back end of the security integration, joined through OneLogin as the identity provider. Sign-in is set up for trusted IPs and non-trusted IPs, so if a user signs in from a remote location like a Starbucks, they will be prompted for multi-factor authentication (MFA) from OneLogin Protect.

"With OneLogin, not only can we connect our cloud-based software through SAML authentication, it has enabled us to secure our VPN access using the same platform as well. So it's really helped us with identity and access management."

RESULTS

"In our branded portal, there are tons of automotive retail dealership software that use form-based authentication; they don't support SAML. Nor does our current HR management system. So you need to use the OneLogin browser extension for the auto form fill. That's been incredibly useful, especially for our help desk," states the IT director.

He continues, "When you're setting up a user, we can pre-fill that information for them, so when they login for the first time on day one, using their AD credentials to access OneLogin, they never have to know all of the other passwords. Similarly, if that person is terminated or they leave the company, we have a single kill switch. We just disable the AD account, and it's done. The AD sync is another advantage over Okta, since OneLogin does the AD sync in real time, versus certain intervals. It reduces your exposure to a window of opportunity where someone can do something malicious on their way out."

Experience Ease of Use

"As a traditional retail business, our employees were accustomed to doing things a certain way, but with OneLogin, our sales people see that it saves them time, not having to login to multiple systems and remember all the passwords. That is a real benefit to them," says the IT director.

He continues, "OneLogin is the perfect way to centralize security management, and to provide users with a very clean and controlled experience. That's what I find most attractive about this product—a single portal for SSO is everyone's launch pad to start their day and to use the applications they need to be productive."

"OneLogin is the perfect way to centralize security management, and to provide users with a very clean and controlled experience. That's what I find most attractive about this product—a single portal for SSO is everyone's launch pad to start their day and to use the applications they need to be productive."

Security at Scale

The infrastructure transformation through identity management has improved security through centralized password management and authentication, MFA, real-time on- and off-boarding and application provisioning. With only one support person for every 200-plus users, tools like OneLogin have enabled the IT group to really concentrate on other projects adding value to the company.

"Managing security with a growing landscape of custom and cloud-based software is difficult to do without unified access management. It's far less scalable, from a management perspective. If you're looking for an identity management platform, there are a number of different providers, and particularly when it comes to reducing employee effort while maintaining centralized security and control, OneLogin stacks up very well," concludes the IT director.

About OneLogin, Inc

OneLogin is the leader in Unified Access Management, Enabling Organizations to Access the World™. OneLogin makes it simpler and safer for organizations to access the apps and data they need anytime, everywhere. The OneLogin Unified Access Management Platform secures millions of identities for thousands of companies around the globe, spans both cloud and on-prem environments, and unifies all users, devices, and applications to transform enterprises. We are headquartered in San Francisco, California. For more information, visit www.onelogin.com, our blog, Facebook, Twitter, or LinkedIn.