Construction Materials Giant Enhances Security with Identity Management and MFA

> "Having a single tool to disable users and implement two-factor authentication without having to reinvent the wheel is a huge payoff."
>
> NETWORK ENGINEER

INDUSTRY

Construction Materials

USERS

5,000

TOP CLOUD APPS

G Suite, Cisco Cloudlock, AWS, Zscaler, Salesforce, Billtrust, PeopleSoft, PeopleFluent

CHALLENGES

User authentication not integrated across all apps

Need for accurate, rapid user offboarding for access security

Difficulty scaling infrastructure to support cloud apps and MFA

Phishing and ransomware risks

SOLUTION

SSO and MFA with OneLogin

Pre-integrated SAML app connectors with user provisioning

Zscaler and Cisco Cloudlock for threat protection

RESULTS

Reduced security risk from phishing and ransomware

Streamlined IT infrastructure from ADFS to the cloud

New SaaS apps can be added in minutes with SAML

A member of the Fortune 1000, this construction materials manufacturer is among the largest suppliers of building materials, which are used in nearly all forms of construction.

CHALLENGES

Multi-factor Authentication across SaaS Apps

The construction materials manufacturer has a number of apps, on-premise and in the cloud, for employee productivity. With increased pressure to roll out more apps, employees needed to connect remotely to the office to stay productive. With a VPN appliance in place for remote access to the office network, a Network Engineer set out to find a solution to implement multi-factor authentication (MFA) for some of the apps. Duo Security met that initial need, but he quickly realized it was limiting: the company needed to scale MFA for an increasing number of cloud-based SaaS apps, as well as a desire to use secure token-based authentication as much as possible.

Meanwhile, a System Integrator and colleague of the network engineer was also looking for a solution that would still allow secure user authentication across many apps with single sign-on (SSO), even for apps that did not support a standard integration such as SAML.

Hurdles Extending ADFS

Initially, the company used an internal Active Directory Federation Services (ADFS) setup to connect four cloud-based apps. However, connecting each new app took several hours for SAML integration, and with the need to roll out more apps with MFA integration, the team required a more agile solution. The adoption of the Salesforce

Community Portal to bring the company closer to its customers became the impetus to either extend ADFS themselves, or to select a cloud-based identity and access management (IAM) solution instead.

Phishing Risk

The network engineer speaks to another challenge: “When we moved to G Suite, people became very accustomed to putting their username and password into web pages as a normal thing they do every day, logging into Google. And because of that, the ability for users to get phished went exponentially higher.”

> “OneLogin had things that we could use right out the gate and a very good integration into the Juniper SSL VPN facility. That made OneLogin a perfect next step.”

Accurate User Deprovisioning

The company also wanted to simplify user deprovisioning.When a user is disabled, it is critical to make sure their accounts are disabled everywhere in the SaaS environment. So when they disable them in one place, they are no longer able to access anything related to the company.

Additional items on the IAM solution “shopping list” included the ability to use SSO and two factor authentication (2FA) as an administrator to access sensitive parts of the company infrastructure, such as its Juniper SSL VPN administration portal, while maintaining Sarbanes-Oxley compliance. Integration of Azure and PowerShell was also essential, and of the Zscaler and Cisco Cloudlock security solutions that were already in use.

SOLUTION

After reviewing three IAM providers, they found OneLogin attractive due to its comprehensive application integrations, as well as the ability for them to start small and expand services as needed. The network engineer explains, “OneLogin had things that we could use right out the gate and a very good integration into the Juniper SSL VPN facility. That made OneLogin a perfect next step.”

OneLogin Professional Services helped the company accelerate deployment while the IT team became more familiar with SAML, and handling roles and role mapping for integrating its first apps.

Implement SSO and MFA with OneLogin

The OneLogin SSO capabilities work for thousands of apps, whether SAML-enabled or not, allowing a simple experience for users and less work for IT.

Not only can the company implement MFA through OneLogin, but they can also provide different second factor options. For instance, the company primarily uses the SMS integration with Twilio as a user's second factor. Some employees may use the OneLogin OTP app, and a few workers who do not have smartphones use Yubico Yubikey. This is especially helpful as the company moves towards connecting more external partners and contractors to its IT resources.

Zscaler + Cisco Cloudlock + OneLogin for Threat Protection

Together, Zscaler, Cisco Cloudlock, and OneLogin protect the company against threats, preventing phishing attacks and stopping ransomware. The network engineer shares, "The combination of Cisco Cloudlock and OneLogin has really solved a lot of the phishing problem, which was a huge risk for us. There's still some spear phishing that happens, which is why we have our users participate in security awareness training."

To prevent someone from carrying a ransomware back into the office, they use the Zscaler app, and then allow the user to SAML authenticate. Whether on net or off net, they are in OneLogin.

Virtual Provisioning for AWS

In addition, the Amazon Web Services (AWS) Multi-Role connector from OneLogin lets application developers easily pick the role they need, logging into AWS as web developers, web production managers, or infrastructure masters.There is one account which is the local account. Everyone else is a virtual federated user using one of the role-based profiles created for various users.

RESULTS

The company benefits from OneLogin in four significant ways:

Reduced Security Risks

OneLogin reduces security risks at the company in a number of ways. Combined with Cisco CloudLock, OneLogin helps significantly reduce phishing attacks. Also, implementing MFA across all apps means the company can require two-factor in environments they were not able to before.

Centralized user management enables them to accurately deprovision users as well. The network engineer sums it up, "Having a single tool to disable users and implement two-factor authentication without having to reinvent the wheel is a huge payoff."

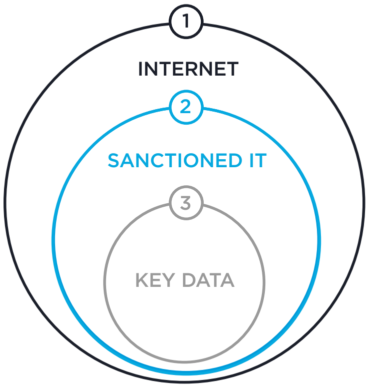
Streamlined IT Infrastructure

On the impact that choosing OneLogin over extending ADFS had on the team, the system integrator says, "A key attraction of OneLogin was that it was an alternative to expanding or scaling up our ADFS infrastructure.

THREE-TIER SECURITY PROTECTION

ONELOGIN + ZSCALER + CISCO CLOUDLOCK

A three-tier security approach consisting of OneLogin, Cisco Cloudlock and Zscaler enables multidimensional protection against corporate security threats including phishing attacks, network viruses, and password and data theft.



1 zscaler

Zscaler filters network traffic as the first line of defense against cloud security threats

2 onelogin by ONE IDENTITY

OneLogin protects access to sensitive corporate data residing in corporate applications

3 cisco Cisco Cloudlock

Cisco Cloudlock UEBA logic evaluates risk based on usage in key corporate applications. Integration with OneLogin enables automatic action to be taken (e.g. prompt MFA) based on risk and policy settings.

Bringing in OneLogin has been a big deal for systems integration. It's saved us a tremendous amount of time in reducing the risk, in pushing this out into the cloud where we believe it needed to be."

Not only did this reduce risk, it saved them time and money as well. He continues, "Putting the infrastructure of this function in the hands of people who do this for a living, that's where the savings are. It takes the risk off from our staff, to a certain extent."

SAML for Ease of App Integration

The IT team appreciates how easy it is to convince vendors to SAML-enable their product for greater access security, thanks to free OneLogin resources like the SAML Toolkit. "The help that OneLogin gives service providers is very good. It's very easy to just say, 'Here's a link, and the OneLogin folks will work with you to build a plugin for your product,'" explains the system integrator.

"The help that OneLogin gives service providers is very good. It's very easy to just say, 'Here's a link, and the OneLogin folks will work with you to build a plugin for your product.'"

"Some of the other things we were trying to integrate you already had, and the things you didn't, you went ahead and worked with our vendors to build connectors and get that done right up front," says the network engineer.

About OneLogin, Inc

OneLogin brings speed and integrity to the modern enterprise with an award-winning single sign-on and identity management platform. Our portfolio of solutions secure connections across all users, all devices and every application, helping enterprises drive new levels of business integrity and operational velocity across their entire app portfolios.