CASE STUDY

Steelcase Gains Unprecedented Visibility into Cloud Applications and Services

Steelcase

Customer Profile
Headquartered in Grand Rapids, Michigan, Steelcase is the world's largest office furniture manufacturer with more than 80 locations and 11,000 employees worldwide, including facilities in Europe, the Middle East, and Asia.

Industry
Consumer goods

As a Fortune 1000 organization with 6,500 remote access workers across the globe, maintaining an open, collaborative environment is key to getting work done at Steelcase. Adoption of cloud services has helped create a productive digital environment by increasing collaboration and providing anytime access to information on any device. But it has also put sensitive company information at risk of unauthorized access.

Connect With Us

Getting a Handle on Shadow IT

Two years prior, the Steelcase Board of Directors' Audit Committee had expressed concern over the vast number of cloud applications and services in use at the company and requested an audit, which required finding, vetting, and approval of all cloud services.

As a result, Randy Moon, senior manager of IT security at Steelcase, decided to bring in McAfee to assess cloud usage and provide the granular visibility he and his team needed to perform the audit. After deploying McAfee® MVISION Cloud in their environment, Moon and his team discovered 3,500 cloud services in use within the company, with only a handful of them sanctioned by IT.

In utilizing the Cloud Registry, which includes comprehensive McAfee Skyhigh Cloud Trust Ratings for more than 20,000 cloud services across 50 attributes, Moon and his team were able to quickly identify the risk associated with each service and had actionable information they needed to be able to enforce governance policies. "We immediately started blocking all applications with a risk score of seven or higher," says Moon. "That is high enough risk that we knew we didn't want anyone to use those services."

In leveraging the MVISION Cloud just-in-time coaching tools, Moon and his team were able to start an open dialogue with their users and gain acceptance of the new cloud governance policies, all while directing their users to safer, sanctioned services. "We have blocked about 600 high-risk cloud services," says Senior Security Analyst Ed Kryda. "With the help of McAfee, we can now offer our users alternative cloud services that are safer and low risk."

The added visibility has also provided other benefits for the team at Steelcase, including the consolidation of services and a reduction in cost and labor hours to vet services, allowing Steelcase to onboard cloud services more quickly. "We have other business units approaching us and asking about new cloud services. Since we have the risk ratings literally at our fingertips, we have been able to help procurement teams understand the risk we could be incurring if we brought them into our environment," says Steelcase Security Architect Stu Berman.

Protecting Identity with OneLogin

With more 37,000 users worldwide, including external partners, Moon and his team chose OneLogin as their identity management tool to quickly and securely unify their four Active Directories for employees in the US, EMEA, and APAC, as well as for their external users, and provide secure login authentication for their cloud services.

In leveraging OneLogin's Identity Management as a Service (IDaaS) solution, which enables SAML 2.0, the open source standard for single sign-on (SSO), Steelcase is able to deploy new applications—an average of 30 per year—to their users in days instead of weeks. Additional IT savings derive from users' ability to lean on OneLogin to complete self-service password resets instead of having to open a ticket every time they need password assistance related to their various applications.

Challenges

- Rapid adoption of cloud services led to multiple accounts, passwords, and login procedures
- Growth of Shadow IT cloud services unmanaged by the IT department resulted in risk
- Wanted to enable cloud services like Microsoft Office 365 while ensuring sensitive data is protected

Solution

- McAfee MVISION Cloud for Office 365
- McAfee MVISION Cloud or Shadow IT
- OneLogin for Identity Management

"The login process has been very streamlined with OneLogin. I sign in once in the morning, and then I don't have to enter my login credentials again, regardless of whether I am accessing Office 365 or ServiceNow," says Moon. "It is very transparent, and our users don't even realize that OneLogin is working behind the scenes, authenticating all of their logins."

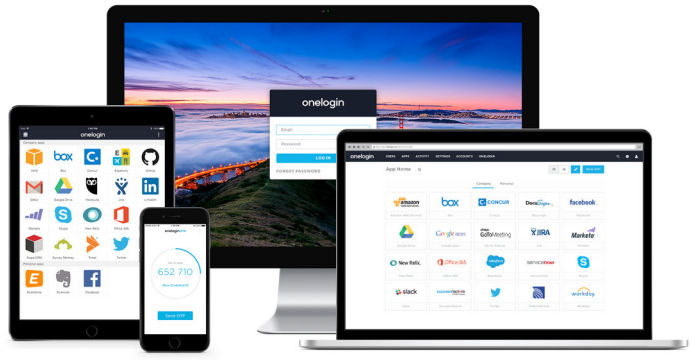

Figure 1. OneLogin enables single sign-on (SSO) and multifactor authentication for application access based on location, application, and user privilege level, ensuring that only authorized users get access to sensitive data.

In addition to Skyhigh, Steelcase has integrated close to 100 applications with OneLogin, giving employees and external partners the ability to safely access any cloud application or service from any location across the globe, while ensuring that necessary security and access controls, such as multifactor authentication or session time restrictions, are being applied.

Securing Office 365 with McAfee and OneLogin

When Steelcase rolled out Office 365 across the organization to take advantage of its productivity and collaboration features, Moon and his team were concerned about employees uploading sensitive data like intellectual property or their personally identifiable information (PII) to the cloud. To help tackle this, they added McAfee MVISION Cloud for Office 365 via API integration and leveraged OneLogin's identity and access management (IAM) capabilities as additional layers of control over Office 365.

OneLogin centralizes access management to Steelcase's cloud workloads. Managing employee access to the cloud through an application portal greatly reduces their risk of Shadow IT applications and the unauthorized use of access privileges by terminated users. OneLogin makes it easier to integrate adaptive and two-factor authentication into Steelcase's applications. With OneLogin, it's administratively easier to see who has access to specific applications, reducing the security risk.

While OneLogin is used to authenticate logins for Office 365, Skyhigh is used to enforce data loss prevention (DLP) policies and threat protection. Using MVISION Cloud's API integration with Office 365, Moon and his team are able to enforce existing DLP policies to detect PII and other sensitive data such as credit card numbers. They also use MVISION Cloud to enforce collaboration controls that alert the IT teams to files that were shared publicly.

Results

- Reduced the use of high-risk, unsanctioned services and coached users to Microsoft OneDrive
- Enforced DLP policies to prevent exfiltration of data from the cloud
- Increased user productivity by enabling single sign-on to cloud-based applications

"We need to be able to see what is going on in Office 365 with DLP and analytics tools to check for bad file permissions or people sharing data that they shouldn't," says Kryda. "The borders for data are changing and eroding. You can't just protect your core networks any more—you have to go out to your data."

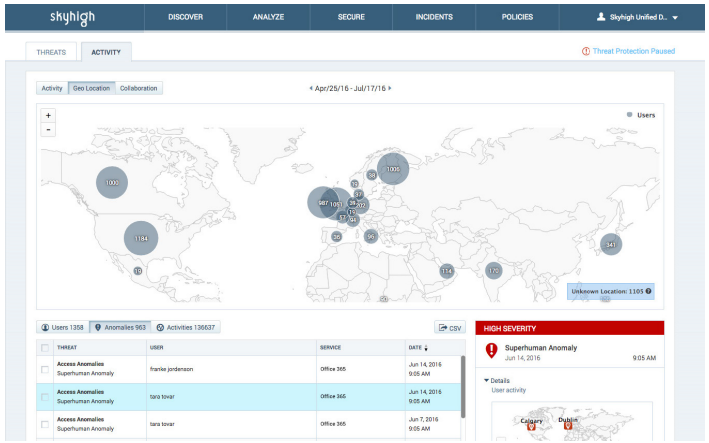

Figure 2. Unified dashboard to review and remediate cloud–based threats.

In utilizing MVISION Cloud's threat protection capabilities and geolocation analytics, the team at Steelcase has been able to detect anomalous usage within Office 365 which is often indicative of threats and compromised accounts. "We have seen six compromised accounts with superhuman logins," says Moon, referring to login activity that would be otherwise impossible, given timeframes and login locations across the globe.

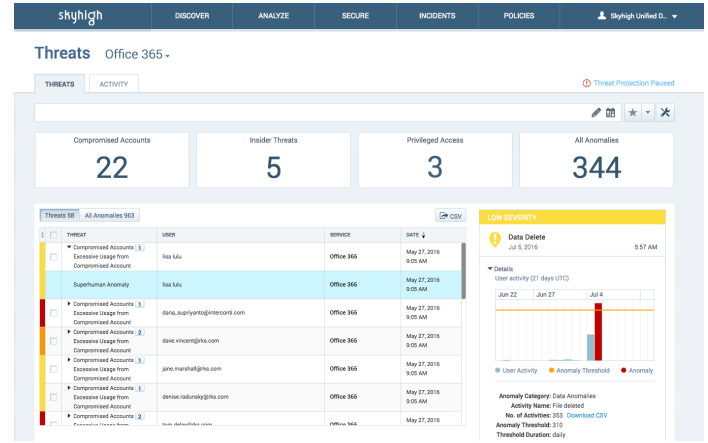

Figure 3. Account access analytics identify activity indicative of compromised accounts.

MVISION Cloud's threat protection was also used in instances where users downloaded sensitive data from Office 365 and uploaded it to unsanctioned, Shadow IT file-sharing services. "Massive data exfiltration was one of our main concerns," says Moon. "Our risk profile has greatly improved since bringing in McAfee. We have been able to remove vulnerabilities that could have done a lot of damage."

"Our risk profile has greatly improved since bringing in McAfee. We have been able to remove vulnerabilities that could have done a lot of damage."

—Randy Moon, Senior Manager of IT Security, Steelcase

The Vision Going Forward

As Steelcase continues to evolve its technology infrastructure to meet employee needs, the company is looking to expand its offering of secure cloud services, including applying real-time DLP and encryption controls to Office 365 through a reverse proxy to further enable collaboration for their global users. In this architecture, OneLogin will authenticate access credentials and redirect all Office 365 traffic to MVISION Cloud, which will enforce security controls.

"We are still pretty early in our cloud journey," says Kryda. "But we are taking the right steps to forge our own destiny. McAfee MVISION Cloud gives us real, actionable data, and now we know what we are using the cloud for—not just guessing."

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com