CUSTOMER STORY

Leading Food Manufacturer Strengthens Its Security Posture in Line with Its Growing Business and Global Presence

Since its founding in 1919, this company has established itself as a reputable developer of ingredients and solutions for bakers, pâtissiers and chocolatiers worldwide. Its overarching goal is to be a reliable partner in innovation, helping its customers around the world deliver nutritious and tasty food to their local communities. Over 9,000 employees and a network of local subsidiaries enable the company to maintain its leadership position in the more than 100 countries where its products and services are available.

Evolved security posture

Made it possible to easily track users and app access

Gained foundation for unified app access environment

CHALLENGE

Approximately 30% of the company's employee base work in factories while the other 70% are in offices around the world. As the company increasingly digitizes business operations, it is moving more services and applications to the cloud. One of the biggest initiatives in this area was deploying Office 365 for existing employees and those joining through the one or two acquisitions the company averages each year.

Hand in hand with this shift came a need for enhanced security around application access. Like many businesses, the company experienced phishing attempts where hackers targeted its finance department, among others. While the security team implemented procedures to prevent these attacks from succeeding, the company was vulnerable when employees ignored the procedures or shared their access credentials.

In response, it implemented scalable infrastructure and numerous access security solutions, including a certificate-based VPN, two-factor authentication for all web-based applications, and an SMS-based MFA solution on an external VPN. However, according to its Manager Network & Security, "We were missing a security solution for the cloud and want to ultimately manage all identity and access management in a single portal."

SOLUTION

To address its needs, the company launched a search for a Multi-factor Authentication (MFA) solution. After conducting its due diligence and narrowing its options to OneLogin and another major identity and access management (IAM) vendor, it chose OneLogin.

"In addition to the price, we appreciated the flexibility of configuring and rolling out the solution via a portal. Plus, we like the SmartFactor Authentication option that allows us to prompt users for MFA based on a risk score," says says the company's Group Infra Network & Security Specialist.

INDUSTRY

Engineering and Manufacturing

USERS

5,500 users

INTEGRATIONS

Office 365

Once the company decided to partner with OneLogin, its security team benefitted from OneLogin's hands-on involvement and strategic advice. With a mandate to roll out the MFA solution as quickly as possible across multiple regions and managers, the team worked closely with OneLogin to make this happen. "OneLogin helped us organize meetings and communications and synced with our regional IT leaders," explains the Group Infra Network & Security Specialist .

OneLogin's experts were also instrumental in the solution setup and rollout. "They thought out-of-the-box and expertly guided us to address our technical needs, particularly when it came to Active Directory and Azure AD. In fact, the rollout happened quickly once it was underway," he continues.

Within weeks, MFA was deployed across multiple lines of business with a focus on office workers. Once the migration to Office 365 is complete for the company's factory workers, they, too, will be activated on OneLogin. "It's very easy activating users through the OneLogin portal, and very clear to users what they need to do to use MFA," the Group Infra Network & Security Specialist adds.

RESULTS

With advanced, context-aware MFA in place for employees, the company feels confident about preventing users from falling victim to phishing attacks. As it rolls out OneLogin in phases to enable factory workers, regional managers can access reports via the OneLogin portal to understand which users are being triggered for MFA. "The portal is intuitive to use and because we can grant user-based privileges, there is no danger that regional managers will interfere with the MFA configuration," says the Group Infra Network & Security Specialist.

Eventually, the company will use OneLogin to replace its existing automated password reset tool and onboard more applications for use with OneLogin. "We need to protect all business-critical applications and information and must be more vigilant about tracking users and application access. With OneLogin, we can address these needs," the Manager Network & Security adds.

According to him, OneLogin MFA is one of the company's most important security measures. In fact, it's a mandatory security tool across the company, and an important element in its digital transformation.

"We need to control user access to cloud apps, especially with a mix of employees working in the office and at home. OneLogin is the solution that helps ensure a smooth, productive, secure transition to the cloud. Ultimately, we can use it to centralize all our identity and access management measures," the Manager Network & Security concludes.

> "With SmartFactor Authentication from OneLogin, our company can confidently continue its digital transformation and migration to the cloud as we empower our employees to work in powerful new ways."
>
> Manager
> Manager Network & Security