La-Z-Boy

DUO CUSTOMER SUCCESS STORY: **RETAIL**

The Challenge

Protecting a Complex Environment

La-Z-Boy is a producer of reclining chairs and the manufacturer/distributor of residential furniture in the United States. Founded in 1927, La-Z-Boy employs over 10,000 people and has 900 retail La-Z-Boy Furniture Galleries and Comfort Studio locations. La-Z-Boy had $1.7B in sales in 2020.

La-Z-Boy wanted to protect corporate, manufacturing, and retail employees against breaches through a Zero Trust framework and by onboarding multi-factor authentication (MFA).

“Implementing multi-factor authentication for retail was new for us. We have boots on the ground and in corporate. When COVID first hit and people were sent home to work remotely, we started seeing more hacking activity that started with our rollout of Office 365. We were looking for opportunities to secure our environment with a second factor. We knew we wanted to secure our VPN and O365, as well as other applications, including HR. Our first use case was when we saw activity on O365 and wanted to address it. Our second use case was our work-from-home VPN perspective. We knew that even post-pandemic we would need a hybrid solution. We created a 5-year plan around our VPN and applications that the hybrid plan was based on,” said Craig Vincent, Director of IT Infrastructure and Operations at La-Z-Boy.

La-Z-Boy built cybersecurity into their planning, so that if they had to move an application or change a platform in the future, they could with cybersecurity at the forefront of the planning cycle. La-Z-Boy discussed internally how these changes might work from a security perspective, and their understanding of how to apply Zero Trust. They needed a solution that worked agnostically that they could grow with and that would be easy to roll out and implement.

Managing Devices

Like other retailers whose financial data and revenue represent a prime target for ransomware, malware, spear-phishing and other attacks, defending against these top threats to reduce the risk of a data breach is top-of-mind for La-Z-Boy.

“Many of our retail (and plant) floor workers do not have dedicated machines, and often share a machine (like a PC, tablet, POS device or a cell phone). Many do not have company-issued devices and use their personal device (BYOD—bring your own device). It is important that our security solution can protect and identify credentials of managed and unmanaged devices and check the health of devices that access our network and databases. Corporate employees using company-issued devices also need highly secured identity protection and access management,” said Vincent.

Vincent continued “More than half the La-Z-Boy retail employees have a networked account or access to our systems, but more than half of them don’t have a dedicated piece of machinery or a smartphone to log onto.” La-Z-Boy needed to look at all of those devices and secure authentication to the network from any kind of device an employee might use.

Meeting Compliance Regulations

The Executive Order from the White House, and compliance laws including CCPA, GDPR, and PCC DSS, require multi-factor authentication because it can prevent unauthorized breaches. Having strong security as a defense while protecting private and personal data of customers is crucial to securing the business.

“Because La-Z-Boy manages customers’ personal identifiable information (PII), it is very important that we stay up to date and inline with compliance regulations like GDPR (General Data Protection Regulation - EU), CCPA (California Consumer Privacy Act), and other important privacy regulations including PCI DSS (Payment Card Industry Data Security Standard). PCI and the other privacy regulations require implementation of MFA to mitigate risk and implement a layer of Zero Trust security around network access managed by granular policies for teams, locations, and roles,” said Vincent.

The Solution

Implement Zero Trust with an Easy MFA Roll Out

Duo’s Trusted Access platform was La-Z-Boy’s first step to using a Zero Trust framework. To secure the workforce, La-Z-Boy needed to validate the identity of the users and ensure the security of their devices before granting access to only the applications and data they need, and not to the ones they do not by setting user-specific policies by role, location, group and more. Duo’s MFA helps block unauthorized access attempts and establishes user trust.

A Zero Trust security model helps La-Z-Boy secure against threats such as phishing, stolen credentials, and out-of-date devices that may be vulnerable to known exploits and malware.

“Duo was easy to implement. Our rollout of Duo was very successful for us. It was great on the admin side and the user side. Our company is spread out around the country and it was easy for us to focus on locations and to install from plant to plant and work with our retail team and stores. Implementing by location was our strategy and geography was an easy way to roll out Duo,” said Vincent.

Secure Retail and Remote Workers

“Securing our retail workers was the top priority. We started looking ahead to see what we thought the future requirements down the road might be. It was very quick and easy to see where Duo fit into our environment quite well, and worked with any application or legacy app, while deploying quickly. Duo was an easy choice for us,” said Vincent.

Vincent added, “The level of detail Duo provided into what devices that were connecting to our networks, managed or unmanaged, was helpful. We could see things we could never see before—like the number of attempts on a credential on O365 or someplace else, the number of lockouts that have happened. We have been able to use Duo’s Device Trust to train our people and give them better avenues to resolve. Duo’s Trusted Access platform gives us another deeper layer of insight on how our users are functioning out there.”

With Duo’s Device Health app, La-Z-Boy is able to continuously monitor the devices connecting to its networks, checks for updates, reminds users to update, or eventually blocks the device entirely if the device hasn’t been updated. Hackers use known exploits to get in when security patches are not current. Enforcing updates helps La-Z-Boy mitigate those risks.

Duo Helps Protect from Ransomware, Malware and Phishing in Three Ways:

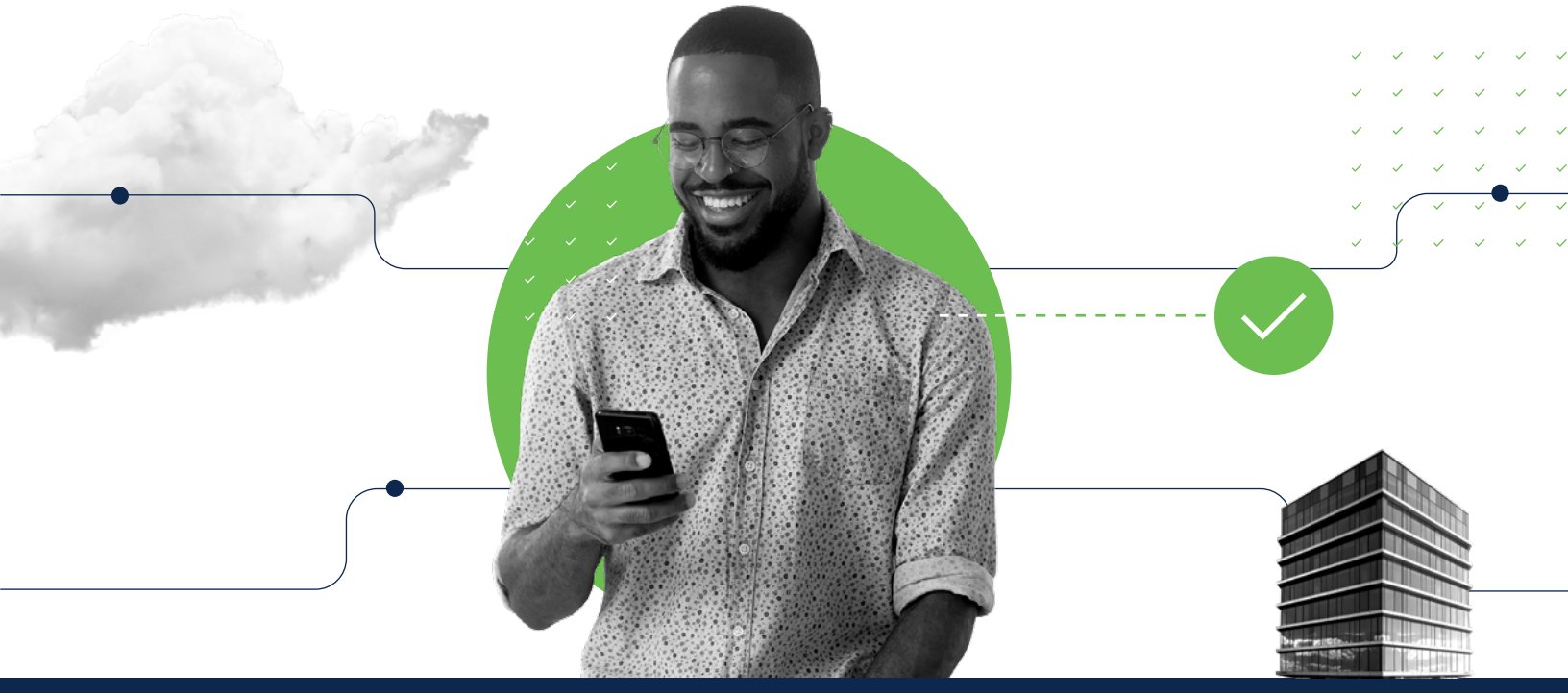
- Preventing ransomware, malware, and phishing from getting an initial foothold in an environment by addressing the risks of weak or stolen user credentials and out-of-date devices.
- Preventing or slowing down the propagation of a successful ransomware attack within an organization by defending uncompromised users from pivot attacks.
- Protecting the critical data and assets of the organization and allowing admins to quickly lock down access by possibly compromised credentials while a remediation investigation is conducted.

Stay Compliant

Staying compliant and on top of compliance regulations while protecting its retail consumers' PII (personally identifiable information) data was important. La-Z-Boy uses POS (point of service) devices that need to protect user data. They need to be able to prove they have implemented MFA and have an easy to access audit trail. Duo meets the PCI DSS requirements for 7.1–7.2 and 8.2–8.3 for MFA requirements.

Duo's MFA helps La-Z-Boy meet compliance requirements by securing endpoints with multi-factor authentication. PCI extends MFA as a required control for all remote access (console and non-console) into the cardholder environment. Remote access application examples include virtual private network (VPN), virtual desktop infrastructure (VDI), remote desktop (RDP), and Secure Shell (SSH). Duo offers comprehensive logging and reporting, and flags suspicious behavior with alerts. Duo's Trust Monitor helps compliance by building machine learning models to learn about common authentication patterns within the environment of each customer and continuously scans the environment looking for authentication anomalies and highlights them for visibility. Further, Duo's Access Policies can be tailored to user, geography, security level, group, device hygiene and more.

As La-Z-Boy continues to grow, they were looking for a solution they could grow with that would help protect all of their workers from on-the-floor retail and manufacturing to corporate employees. They noticed more attacks after implementing O365 and knew they wanted to add more factors to authentication. They chose Duo's MFA solution because it meets their needs today and will meet their needs tomorrow. Duo helps La-Z-Boy maintain a Zero Trust framework, stay compliant, and get clear visibility into what is connecting to their network and VPN as they manage all devices, whether corporate or employee owned.



“It was very quick and easy to see where Duo fit into our retail environment quite well, and worked with any application or legacy app, while deploying quickly. Duo was an easy choice for us.”

Craig Vincent
Director of IT infrastructure and operations
La-Z-Boy

Start your free 30-day trial and quickly protect all users, devices, and applications at duo.com.

The bridge to possible

Duo Security, now part of Cisco®, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of the Cisco Zero Trust offering, the most comprehensive approach to securing access across IT applications and environments, from any user, device, and location. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Founded in Ann Arbor, Michigan, Duo also has offices in Austin, Texas; San Francisco, California; and London.