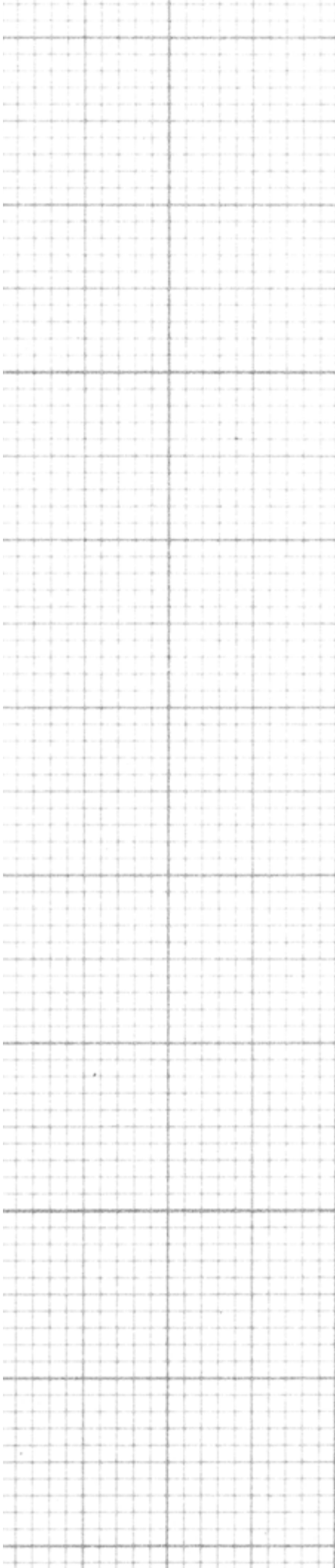
Retail Cybersecurity:

THE JOURNEY TO ZERO TRUST



Retail Cybersecurity:

THE JOURNEY TO ZERO TRUST

Table of Contents

01. The Retail Cybersecurity Landscape

There is a lot to protect.

The retail industry has been riding a wave of major changes from the decline of traditional brick-and-mortar stores to the rise of e-commerce with Amazon and online shopping. Coupled with the Great Resignation of frontline workers and supply chain issues, It has been a challenging time for retailers. The importance of the retail industry not only surviving but thriving is key to economic growth in America.

- With an annual U.S. gross domestic product (GDP) totaling $3.9 trillion, the retail industry comprises 4.2 million retail establishments.
- The retail industry also ranks as the top employer in the nation, holding one in every four jobs. Retail supports over 52 million American jobs.

+ $4.4 Trillion Total U.S. Retails Sales
+ $11 Billion Credit Card Fraud Loss in the U.S.
+ 33% of U.S. Retailers Were Victims of Credential Theft

There has always been an element of fraud in retail, but cyberattacks have taken losses to a new level. The steady stream of retail data security breaches have caused alarm, resulting in massive leaks of personal identifiable information (PII) and credit card numbers of consumers making their rounds on the dark web.

- The U.S. alone represents one-third of the world's credit card fraud loss at $11 billion in 2020 and is the most card fraud prone country globally.
- In 2020, the Federal Trade Commission (FTC) reported that consumers lost $3.3 billion to fraud, which is $1.5 billion more than what was reported in 2019. It also disclosed that 4.72 million identity theft and fraud reports were filed in 2020.

Because retail is the nation's largest employing industry, remote attacks compromising the security of retail organizations could significantly affect the nation's economy and workforce, as more attackers attempt to steal financial information, sell data dumps and make a profit off of fraud. The prevalence and rapid increase of breaches due to Covid-19 calls for stronger, more effective security measures in a fast evolving IT environment.

Omnichannel Supply Chain Complexity

The pandemic sped up the merger of ecommerce and in-store systems. According to a Digital Commerce 360 analysis of U.S. Department of Commerce data, online U.S. retail sales grew 32% in 2020. Delivery methods like curbside pickup grew in popularity, with 43.7% of the 245 top retailers offering it in 2020 compared to just 6.9% in 2019. This merger of ecommerce and in-store systems adds new areas to the attack surface and links technical debt from all environments.

This makes access management (authentication, authorization, privileged policies) more difficult, but also more important as security measures. With more employees and contractors working remotely, access to applications that may contain customer data poses a risk. With such valuable customer information, it is increasingly more urgent to place security at the forefront without sacrificing efficiency.

The Remote Access and Cloud Hybrid Model

A major challenge is that the fundamental way retailers conduct business has changed. Some corporate employees now access enterprise data (like Microsoft and Workday) directly in the cloud from their mobile devices — most of the time without being on an "enterprise network" or connecting via a VPN. With data now located both in the cloud and on-premises, older security solutions have become less effective. Many retailers have legacy systems they still rely on, even as they move more applications to the cloud. Migrating to this new model must be done without disrupting business, but managing a secure hybrid cloud environment is not a trivial exercise.

As security attacks targeting retailers and their suppliers grow in frequency and intensity, funding security initiatives has become paramount. The dollars earmarked for digital transformation have now become tied to zero-trust initiatives or other security maturity programs. Gartner reports that 46% of retailers plan to increase their cybersecurity spending and 36% will increase cloud solutions spending.

More retailers are realizing the increased risks they face and are protecting themselves with cyber liability insurance. Like health and car insurance, cyber insurance is a line of coverage designed to mitigate losses from cyber incidents. Retailers may suffer data breaches, network damage, stolen backups, reputational damage and the disruption of daily operations. Multi-factor authentication (MFA), endpoint visibility and access controls like those Duo Security provides are often required by cyber liability insurance providers and can help fortify against risks and lower insurance rates.

Unknown devices:
As more retailers allow personal devices or BYOD (bring your own device) they need visibility into the state of devices connecting to the network. Are they trustworthy? Are they updated? Are they secure? Whether from an employee, vendor or contractor, BYOD devices can pose new security risks. Retailers need to limit access to sensitive applications and data by having controls in place and policies.

"Always on" portals:
The new perimeter-less model of "always on" access requires a hybrid approach between cloud-hosted and on-premises data and applications. Consequently, remote access to these systems via web-based logins is an easy way for attackers to exploit internal company networks.

Supplier risk:
Within the retail industry, there are many threats to cardholder data and corporate networks, with third-parties, vendors, cloud applications and other points of access that open up companies to a potential incident. Finding a hybrid solution that can support all levels of access (including third-parties) at all times from anywhere is essential. Your security should take a layered approach so that even if your vendor is hacked, your data is not at risk.

Point-of-Sale (POS) intrusions:
POS malware, malicious web apps and ransomware are the top weapons wielded by retail cyber criminals.[1] Certain types of attacks are specific to the retail industry, including exploits specialized for POS systems, particularly software that system admins use to remotely access and manage POS technologies. There's also the threat of exploiting default or weak passwords.

Unfortunately, all it takes is one exploited opportunity. Intrusions can start with the compromise of a single device or set of credentials. After initial entry, attackers install malware to collect personal information and data from credit and debit cards and then transmit the data back to their own servers.

Dark Reading reports the top three threats to retail right now are stress on payments and control systems, denial-of-service (DDoS) attacks (flooding traffic to crash a site), and phishing or spoofing sites. Centralizing the use of credentials through single sign-on (SSO), MFA, and password managers have all helped to decrease the number of phishing attacks by half over the past two years according to Verizon. When users can access applications securely without much effort, it's only natural that phishing attacks would drop on this factor alone, simply based on improved and informed user behavior. SSO and password managers increase security and convenience at the same time, while MFA significantly reduces the risk of credential theft and re-use.

The 2021 Verizon Data Breach Investigations Report states that passwords caused 89% of web application breaches, either through stolen credentials or brute force attacks. MFA can be 99.9% effective at preventing stolen credentials. A zero trust layered VPN and firewall approach that includes MFA can prevent 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks, according to Google research.

"Security Magazine reports the number of stolen and exposed credentials has risen 300% since 2018.

1. A POS device is the system in a store used to accept payment in cash and credit cards.

Underfunding in Declining Companies

The retail industry is going through a digital transformation at the same time that brick-and-mortar stores face declining sales, low margins and increased competition from online retailers like Amazon and discount retailers like Walmart. During the pandemic 29 major brands have filed for bankruptcy, closing down 2,368 apparel stores, 1,433 home furnishing stores, and 907 department stores. Simon Property Group purchased J.C. Penny, Forever 21 and Brooks Brothers after they filed for bankruptcy signaling the decline of the brick-and-mortar retail chains that dominated the retail landscape for generations.

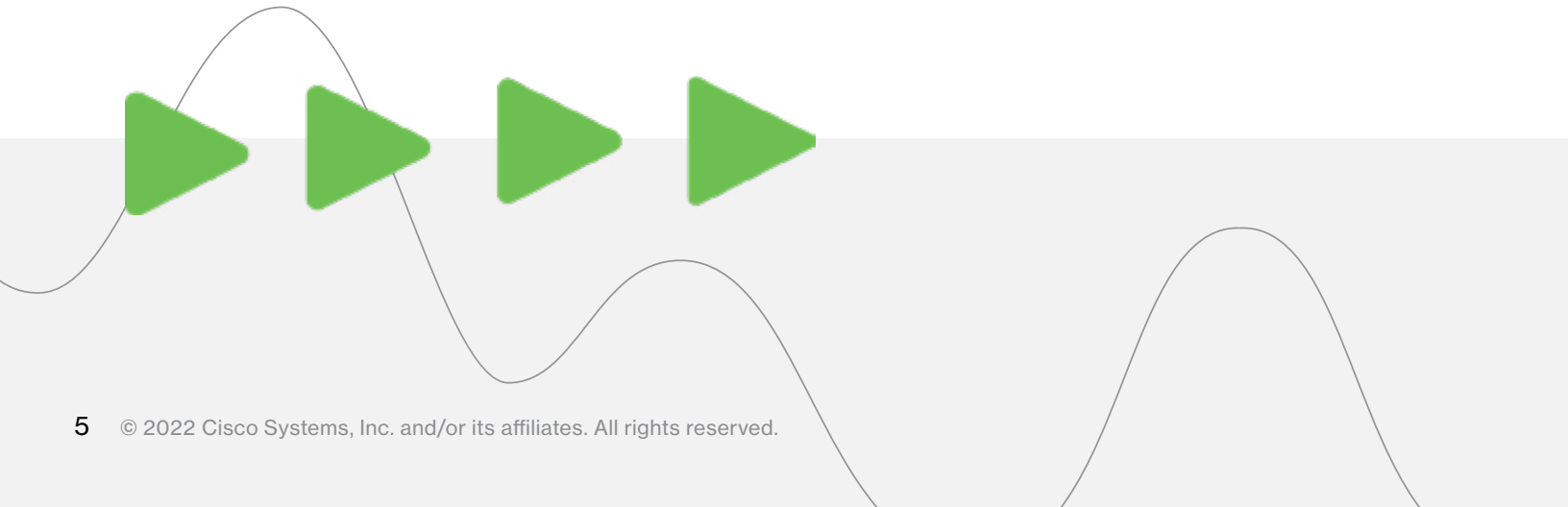
Low Margins, Increased Competition

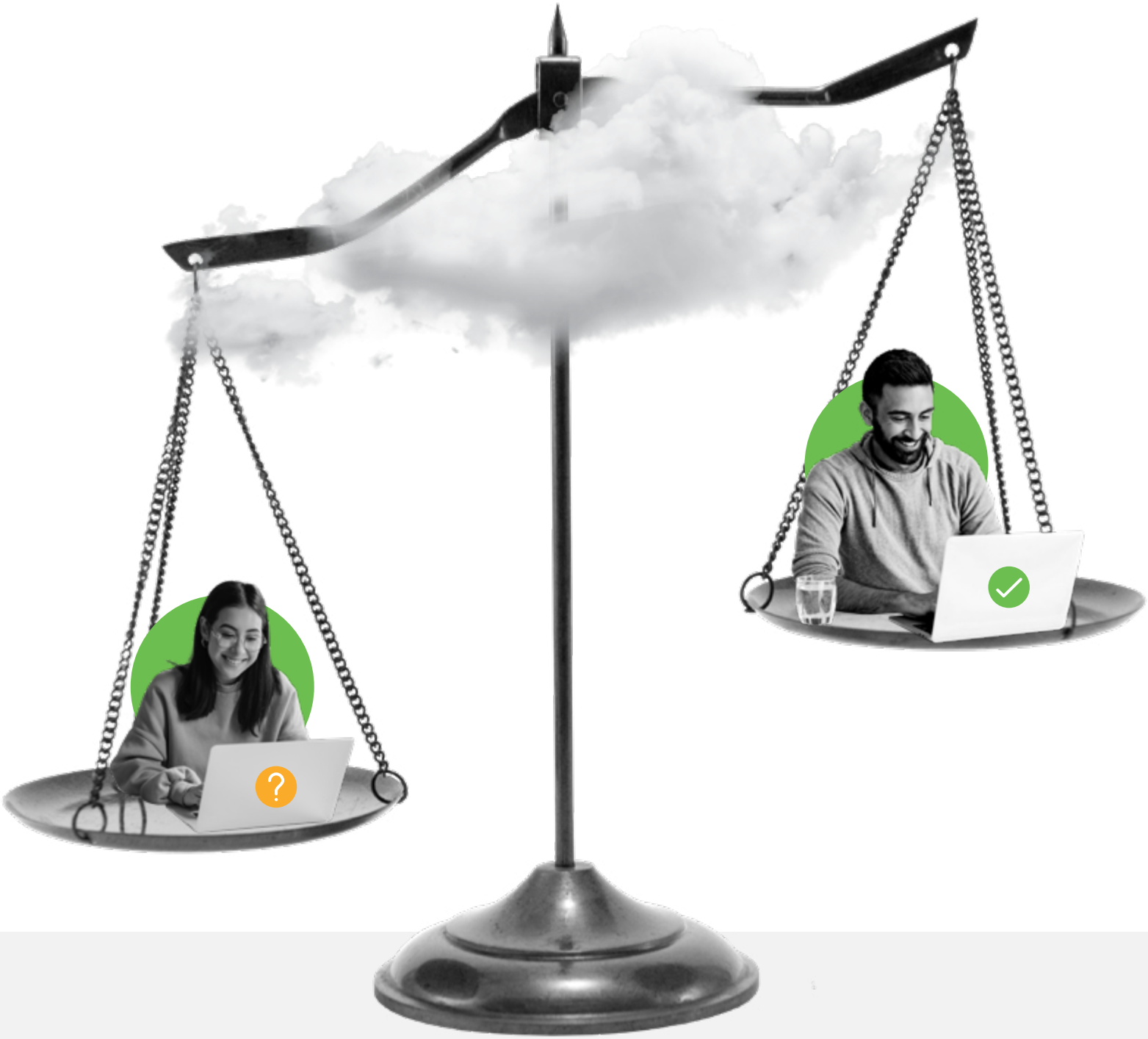
As traditional retailers struggled to implement online shopping experiences and move to a remote workforce, finding resources to re-platform and re-secure systems has been difficult. It has been a challenge to source and retain cybersecurity talent due to more demand than supply for cybersecurity professionals. Retailers are looking for ways to save money, meet compliance regulations and stay secure from malware attacks. They also want low-cost but high-value security solutions to protect credentials and their systems.

Workforce Risks

The need for managed and unmanaged device access in conjunction with shared devices, shared credentials and a heavy use of kiosks has made securing front-line employees problematic. Varying degrees of technical prowess means that cybersecurity measures need to be simple, flexible and easy to use.

Another challenge for retailers is the lack of cybersecurity education among workers. Cybersecurity education for all employees regardless of their technical knowledge is very important to help protect systems. A strong cybersecurity education program can be a requirement for cyber liability insurance, as is MFA.





02. Compliance and Assurance

Payment Card Industry Data Security Standards (PCI DSS)

A main driver for most retail organizations that deal with credit cardholder data, specifically, online transactions, is the PCI DSS framework that dictates data security guidelines for corporate networks and point of sale systems.

If you store, process, transmit or accept credit cardholder payments, or if you support the retail industry in any way, you likely fall within scope of the PCI DSS guidelines. That includes any software-as-a-service (SaaS) company that may provide e-commerce software applications to the retail industry.

PCI DSS Standards

The PCI DSS requirement 8.0 mandates that retail organizations identify and use multi-factor authentication access to system components.

The authentication standards hold true for all accounts within the retail organization, including point of sale, administrative, and any accounts used to view/access cardholder data. This includes vendor and third-party accounts for support or maintenance.

PCI DSS Requirements Mandate:

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 Multi-factor authentication is implemented to secure access into the cardholder data environment (CDE).

8.5 Multi-factor authentication systems are configured to prevent misuse.

PCI DSS 4.0 In-Depth

8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:

- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.
- Something you are, such as a biometric element.

8.3.2.a Examine vendor documentation and system configuration settings to verify that authentication factors are rendered unreadable with strong cryptography during transmission and storage.

8.3.2.b Examine repositories of authentication factors to verify that they are unreadable during storage.

8.3.2.c Examine data transmissions to verify that authentication factors are unreadable during transmission.

8.3.4 Invalid authentication attempts are limited by: Locking out the user ID after not more than 10 attempts. Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.

8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

8.4.2 indicates MFA will need to be in place for all kinds of system components including:

- Endpoints
- Servers
- Cloud environments
- Hosted systems
- On-premises applications
- Network security devices
- Workstations

In **8.4.1** Administrative access to the CDE cannot be obtained by the use of a single authentication factor and if a user has been idle for more than 15 minutes the user is required to re-authenticate and to re-activate the terminal or session as outlined in **8.2.8.**

- **8.4.3** MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows:
- All remote access by all personnel, both users and administrators, originating from outside the entity's network.
- All remote access by third parties and vendors.

8.5.1 MFA systems are implemented as follows:

- The MFA system is not susceptible to replay attacks.
- MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.
- At least two different types of authentication factors are used.
- Success of all authentication factors is required before access is granted.

Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With MFA, an attacker would need to compromise multiple authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

While the DSS requires MFA, it provides flexibility to determine at which level it is applied. For example, the standard indicates that MFA will need to be in place for a number of specific system components. However, it allows us to apply MFA either at the system/application level for a given component, or at a network level, which can greatly simplify and streamline the overhead of such a requirement.

Examples of multi-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate multi-factor authentication.

There are some significant updates to multi-factor in PCI DSS 4.0. Previously it required MFA to connect to VPN to pass with auditors. Today with the remote workforce MFA is to be implemented for all access into the cardholder data environment (CDE). Whereas previously MFA was required for individual non-console administrative access and remote access to the cardholder data and network access.

MFA recommendations now closely align with the NIST National Institute of Standards and Technology (NIST) requirements, including a requirement to re-authenticate after being idle for more than 15 minutes. This means users may be challenged for MFA more often. Also, all the apps that employees log in to will need to be protected with MFA which will make implementing SSO a priority. With SSO, users only need to login once to access all applications - reducing the risk of multiple passwords and increasing efficiency with fewer authentications.

Duo SSO is a cloud-hosted identity provider that secures access to cloud applications with existing directory credentials like Microsoft Active Directory or Google App. It provides SAML connections for applications like Amazon Web Services (AWS), Salesforce and Workday and offers a generic connector that can connect to just about any app supported by SAML the 2.0 standard.

Duo MFA Can Help With Compliance

Retail organizations should work with vendors who have compliance infrastructure that has achieved compliance according to multiple compliance standards, like Duo. Duo meets the compliance requirements of PCI DSS, NIST, DEA EPCS, GDPR, FFIEC, HIPAA, SOC 2, FIPS 140-2, CITC, ISO 27000, C5, and is AgID qualified.

Duo's MFA can help prevent attackers from gaining access in the first place and can limit access if they did get in by protecting critical systems. MFA requires a user to present a combination of two or more credentials to verify identity for login. For example, in addition to a username and password, Duo MFA asks for something you have — like a trusted device or a software or hardware token — before granting access to resources and can add a third factor like a biometric as outlined in PCI DSS 4.0. Thanks to this additional requirement, Duo MFA makes it a lot more challenging for attackers to get that initial foothold.

Bad actors are keen on using remote services, such as RDP and VPNs, to gain access to a network. Darkside, the alleged perpetrator of the Colonial Pipeline attack, is suspected to have used corporate VPN access not protected with MFA to gain entry to the victim's environment. Duo can protect your VPN and can also work without a VPN. More than just MFA, Duo MFA, Duo Device Trust (contextual policies), Duo Network Gateway (DNG) (connects to apps without a VPN) and Duo Trust Monitor (monitors for anomalies) combine into one trusted access solution and can secure remote access to on-premises and cloud infrastructure and prevent ransomware. Duo is platform agnostic and works with legacy systems.

03. Use of Identity Controls

Identity Controls Support All Security Program Functions

It is common in the retail industry to have a few different sets of users that need to authenticate, from remote access for corporate employees and contractors, to access to a few specific applications for store workers and contact center agents. Implementing a multi-factor authentication solution that meets the needs of all types of workers that is as easy to use as it is to roll out is critical to quick user adoption.

Duo Is Easy, Convenient, and Flexible For Users

Duo's solution makes it easy to get set-up quickly. Users can self-enroll by simply downloading an app and signing in. Duo's multi-factor authentication solution gives your users many different authentication options to fit their different needs in any given scenario, including ones in which they may not have cell service or an Internet connection.

Some authentication methods retail uses include SMS, phone calls, hardware token-based authentication like YubiKeys, passcodes and mobile push authentication technology. In the future retail might support passwordless authentication (biometrics). Duo supports all of these methods of authentication.

In addition to usability, Duo comes with a self-service portal that lets users manage their own devices, enroll and remove devices, reactivate mobile services, remediate out-of-date software, and more. This puts less strain on administrators, reducing the number of help desk tickets related to your multi-factor authentication solution. Duo can scale with you and support you along the way.

Device Trust

With Duo Device Trust you can identify risky devices (managed or unmanaged), enforce contextual access policies, and report on device health using an agentless approach or by integrating with your device management tools. Gaining visibility into devices is the first step in establishing device trust, and it's an essential aspect of a strong zero-trust strategy. Duo provides visibility into every device connecting to your network and enforces health checks at every login attempt.

Remote Access

In the past access was controlled at the network layer like a moat around a castle. Once connected to the VPN you could get onto the network and access all applications, whether you should or not. With Duo's access policies, control happens at the application layer making it easy to safely connect to on-premises or cloud applications remotely and limit access to only those that need it.

Duo's security solutions complement any technical environment, and they're engineered to verify identity and establish device trust no matter how, where, or when your users choose to log in. Duo provides secure remote access with or without a VPN, offers easy to set up application policies and provides simple and secure web application, SSH, and RDP access.

The Duo Network Gateway (DNG) is a remote access proxy security solution that helps employees, remote workers, and contractors access the applications they need to do their job by increasing productivity and reducing friction. It gives you granular access control per web application, SSH or RDP servers and user groups. You can specify different policies to make sure only trusted users and endpoints can access your internal services. DNG helps with on-premises and homegrown applications. This can protect users including contractors and third parties.

Passwordless

Passwords have become the weakest link in security today. Helping solve authentication at scale, Duo Passwordless eliminates the need for multiple passwords. Biometrics, security keys, and specialized mobile applications are all considered "passwordless" or "modern" authentication methods. Passwordless provides secure access for every enterprise use case (hybrid, cloud, on-premises and legacy apps). Duo Passwordless gives users a frictionless login experience, while reducing administrative burden and overall security risks for the enterprise.

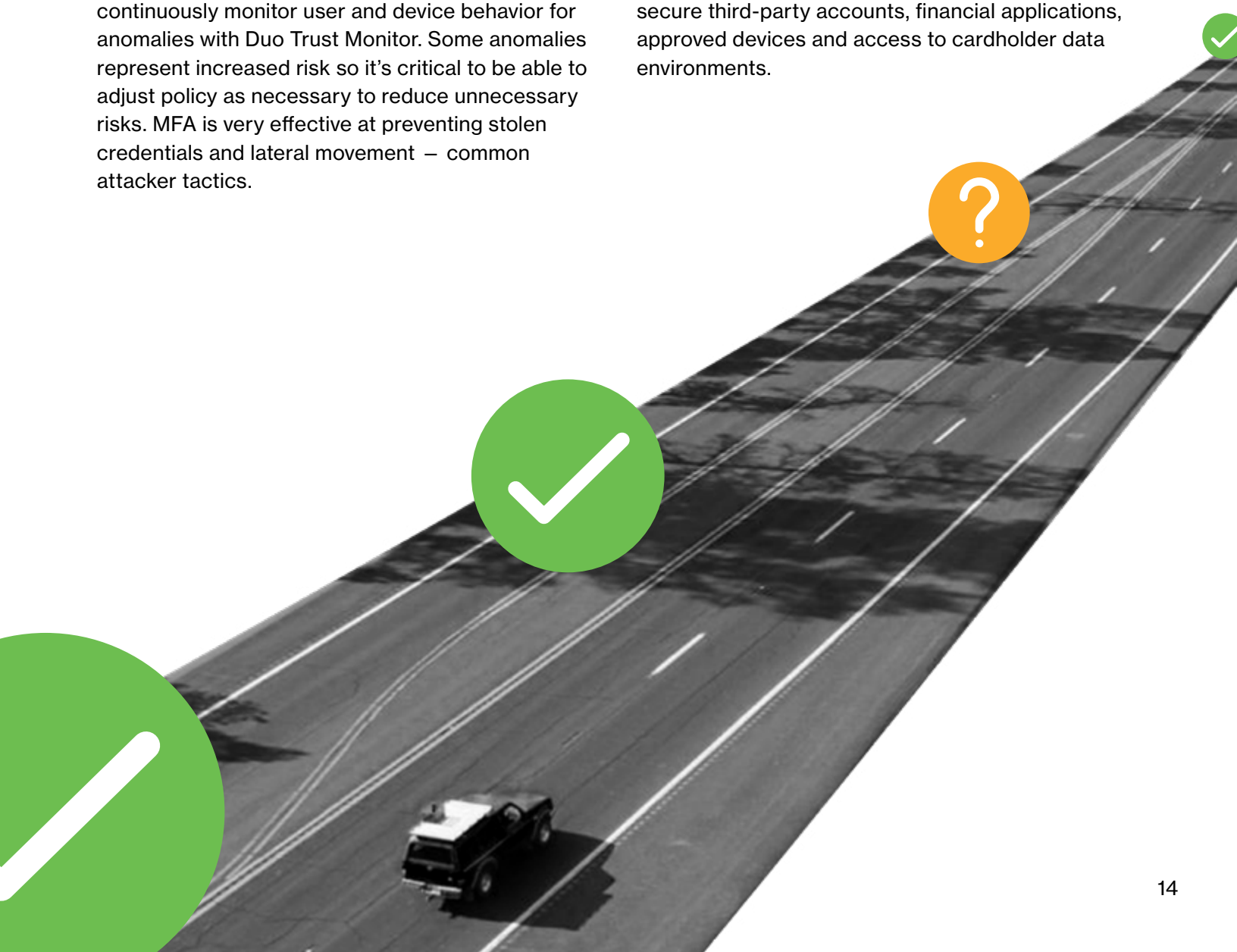
Zero-Trust Principles

With the shift to remote work came the de-perimeterization of the traditional walled garden security approach of granting trust inside the corporate network. Duo MFA is the first step to a zero-trust security approach by ensuring users and their devices are trustworthy at every corporate access request, regardless of where it comes from. Duo secures access across applications and networks in the cloud and on premises.

Zero trust is the gold standard for remote access because it assumes no one is trusted, and therefore does not allow access until trust is verified in multiple ways – starting with MFA and adaptive policy controls that Duo offers. After initial authentication access is granted, teams can continuously monitor user and device behavior for anomalies with Duo Trust Monitor. Some anomalies represent increased risk so it's critical to be able to adjust policy as necessary to reduce unnecessary risks. MFA is very effective at preventing stolen credentials and lateral movement – common attacker tactics.

Policies Make Security Simple and Effective

A strong zero-trust strategy changes the level of access or trust based on contextual data about the user or device requesting access. It also limits access to only users that really need it. With Duo, you can set up detailed adaptive access policies in minutes via a simple, intuitive administrator dashboard, and manage rules globally or for specific applications or user groups. Detect user location, device, role, and more at every login, set security policies based on these attributes, check for anomalous access, and continuously monitor policy efficacy – all without interrupting your users' daily workflows. This becomes important to secure third-party accounts, financial applications, approved devices and access to cardholder data environments.



04. Case Study

La-Z-Boy Goes Zero Trust to Meet Compliance Guidelines

La-Z-Boy is a producer of reclining chairs and the manufacturer/distributor of residential furniture in the United States. Founded in 1927 in Monroe, Michigan, 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 $1.7 billion in sales in 2020.

MFA and Zero Trust

La-Z-Boy wanted to protect corporate, manufacturing and retail employees by implementing a zero-trust framework of "never trust, always verify." When COVID first hit and employees were sent home, La-Z-Boy experienced an increase in hacking attempts after the rollout of Office 365. La-Z-Boy wanted to implement MFA authentication to secure trusted access to applications and their VPN.

They needed a solution that worked with their existing systems and could grow with their future security needs, while giving insight and the ability to manage all devices (corporate or BYOD – bring your own device) connecting to the network. 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. When evaluating MFA vendors La-Z-Boy wanted an MFA solution to protect against unauthorized access to applications. They chose Duo MFA.

According to Craig Vincent, director of IT infrastructure and operations at La-Z-Boy , "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."

How Duo Helps with Compliance:

- Reduces the risk of outside access to the cardholder data environment.
- Validates user identities.
- Secure endpoints and meet the compliance requirements of CCPA, GDRP, PCI DSS, and more with audit trails and alerts. Provides visibility into which corporate-managed and unmanaged devices are accessing company applications and data.
- Ensures that only healthy, trusted devices gain access to sensitive resources and can block unauthorized devices.

> "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."
>
> – Craig Vincent, Director of IT Infrastructure and Operations, La-Z-Boy

05. Conclusion

The changing retail cybersecurity landscape requires better and more effective retail security solutions, ones that can prevent a breach from happening, instead of waiting to remediate after the fact.

Retail organizations in particular need to guard against remote attacks on their point-of-sale (POS) environments and their networks in order to protect consumers from theft of personal and financial information, while meeting industry compliance requirements like PCI DSS and modern security best practices. Free MFA is not always better. There are hidden costs to some MFA solutions such as upfront, capital, licensing, support, maintenance and operating costs.

Social engineering and spear phishing are successful because they exploit the human element of an organization's security. Adopting and implementing a zero-trust security philosophy that starts with strong MFA and a trusted access platform like Duo is important for staying ahead and preventing retail attacks.

Duo Security is the leading multi-factor authentication (MFA) and secure access solution. Duo's Managed Service Provider (MSP) program provides partners with a best-in-class security solution that is easy to set up, scale with their business and manage from a single console.

Visit duo.com/msp for more information.

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at cisco.com/go/secure.