LastPass for Retail

Retailers drive the sale of goods and services directly to consumers for personal or household use. It includes a range of businesses, from small local shops to large multinational big box chains. Key components of the retail industry include physical stores of all sizes, e-commerce, specialty stores, discount stores, convenience stores, and more.

Retail's best defense: password management

Retailers of all types face relentless cyber threats. With high volumes of transactions, large employee bases, and access to valuable credit card information, retailers present an attractive opportunity for credential theft, making them prime targets for threat actors seeking financial gain and sensitive customer data. Threat actors exploit weak, reused, or shared passwords to infiltrate systems, steal data, and disrupt operations.

Employee turnover only worsens the problem, as outdated credentials and unrevoked access create vulnerabilities that attackers are quick to exploit. For IT and security teams, managing access privileges across shifting workforces and countless SaaS applications becomes a constant challenge.

These risks don't just impact internal operations—they directly affect the customer experience. In an industry where brand loyalty is at an all-time low, any cyberattack, data breach, or disruption to productivity can send consumers, and their wallets, elsewhere. A single incident of compromised credentials erodes trust and has lasting financial and reputational consequences for businesses already facing thin margins and fierce competition.

Small business retailers are more likely than other businesses to say they are just one major attack away from shutting down—with over one-third responding that way to the question posed by the US Chamber of Commerce.

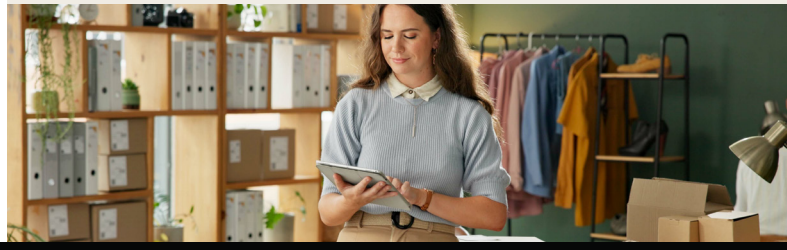
60% of all retail sector consumers and 74% of high-income consumers would likely avoid recently-breached retailers. (Cyberint)

Don't shop around passwords, secure them

As a trusted global leader in password and identity management, LastPass is uniquely positioned to solve the cybersecurity challenges retailers face. Designed for the fast-paced, high-transaction retail environment, LastPass securely creates, stores, and manages credentials while streamlining access for employees, partners, and third parties. By eliminating weak, shared, and outdated passwords, LastPass reduces the risk of credential theft—one of the most common attack methods in retail—without disrupting day-to-day operations.

With cloud-native, easy-to-use tools, LastPass balances robust security with an intuitive experience for admins and employees alike, no matter their technical expertise. Features like secure credential sharing, automated provisioning and de-provisioning, and centralized access controls simplify managing high employee turnover while preventing unauthorized access to systems and sensitive data. Advanced reporting gives IT teams the visibility they need to enforce password policies, audit access, and demonstrate compliance.

For retailers, LastPass is the solution that secures credentials, protects the customer experience, and ensures their business stays resilient against evolving cyber threats.



LastPass

LEARN MORE

LastPass Benefits for Retail

The easiest, most affordable, and most reliable way for retailers to slash cyber and operational risk is to standardize password management with LastPass company wide.

Secure	**Prevent unauthorized access**	Help prevent threat actors and unauthorized users from gaining access to applications, online accounts, sensitive information, and systems.
	Stop account takeover and data breaches	Ensure the reliability and accessibility of online accounts and applications, and the privacy of credentials.
	Control shadow IT	Give organizations visibility into and management over unapproved and over-provisioned SaaS apps, allowing administrators to track credential sharing, manage access privileges, and spot vulnerabilities.
	Extend secure access management	Integrate seamlessly with major identity providers (IdPs) like Microsoft Entra, enhancing user management throughout the employee lifecycle.
Comply	**Meet cyber insurance requirement**	Make it easy for organizations to meet password and access management requirements for cyber insurance.
	Support compliance	Aids organizations in meeting compliance standards set by regulations like GDPR, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA, and SOX, as well as cybersecurity frameworks such as NIST, CISA, Zero Trust, and NERC-CIP.
	Meet partner security requirements	Helps organizations comply with strict partner security standards through robust access controls, password sharing rules, strong authentication mechanisms, and actionable reporting.
Streamline	**Deliver intuitive experiences to every user**	Offers hundreds of customizable policies, flexible privileges, detailed reporting, and various authentication options, making it an indispensable tool in a tech stack.
	Standardize password protection	Simplify credential management for employees across the entire organization.
	Alleviate help desk friction	Reduce the burden on IT helpdesks caused by frequent credential issues, such as lost passwords and account lockouts.
Collaborate	**Maximize teamwork through sharing**	Streamline password and information sharing both inside and outside the company, helping to boost productivity and efficiency for partners, freelancers, and remote workers.
	Maximize adoption + usage	Boost adoption and usage among employees by offering an intuitive and user-friendly interface that simplifies password management tasks.
	Promote a security culture	Help administrators ensure all employees actively contribute to a security-focused culture, protecting against common threats like leaked or stolen credentials to uphold fiduciary responsibility.