LastPass for Real Estate Agencies and Brokerages

The real estate industry involves the buying, selling, renting, and management of land and buildings – including commercial, residential and industrial. It also includes activities such as land management and investments.

Credentials are the keys to an organization

Real estate agencies and brokerages face significant cyber threats, with credential theft being a primary tactic used by threat actors to infiltrate systems. These organizations manage highly sensitive client data, such as personal information, financial details, and property records, making them prime targets for cybercriminals. The consequences of a breach extend beyond operational disruptions, potentially damaging an agency's reputation and client trust. In a competitive, high-pressure industry where relationships and deals are paramount, any compromise in security can lead to lost business and diminished client loyalty, which can have long-lasting effects.

As the real estate industry becomes more tech-native, the adoption of social media platforms, SaaS tools, and collaborative apps has introduced new complexities in managing access and security. Many agencies, particularly smaller teams within larger organizations, rely on these tools for real-time information sharing, deal management, and communication with clients and partners. This increases the number of access points that need to be secured, making credential management a critical issue.

With teams often working across multiple platforms and devices, and constant turnover within fast-moving environments, maintaining secure access and preventing unauthorized credential sharing becomes an ongoing challenge—one that must be addressed to safeguard both agency operations and client data.

With the recent shift toward remote work and PropTech (property technology and software designed for use in the industry)—data security is a critical differentiator real estate professionals must master to maintain customer trust and safeguard their data, while still enabling more digital transactions.

It's critical to protect your assets

LastPass provides a robust solution to the cybersecurity challenges real estate agencies and brokerages face. It enables seamless creation, storage, management, and secure sharing of credentials across teams, ensuring strong security without compromising accessibility. By centralizing credential management, LastPass simplifies access controls, enforces best practices, and supports compliance with industry regulations.

With real estate agencies increasingly relying on SaaS tools, social media, and collaborative platforms, LastPass mitigates the risks of this digital transformation. Its cloud-native solution integrates with these tools to enhance security while making it easy for both tech-savvy and non-technical users to adopt secure practices. Features like secure sharing, MFA, and detailed reporting provide real-time visibility and quick detection of vulnerabilities, reducing the administrative burden of managing access while boosting productivity and compliance.

LastPass

LEARN MORE

LastPass Benefits for Real Estate Agencies and Brokerages

The easiest, most affordable, and most reliable way for real estate agencies and brokerages 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.