LastPass for insurance agencies

Insurance agencies serve as intermediaries between insurance companies and clients, offering guidance on policy selection, selling various insurance products, assisting with claims, providing customer support, and assessing risks to determine appropriate coverage.

Insurance agencies should protect passwords like they do assets—with a robust [password] policy

Insurance data is inherently sensitive and confidential, making them prime targets for credential-driven cyberattacks. Threat actors often exploit weak or stolen credentials through phishing, social engineering, and other tactics to gain unauthorized access to systems by exploiting passwords and identities, potentially leading to account takeovers and data breaches. These incidents put both the agency and its customers at significant risk, jeopardizing trust and exposing personal and financial information to misuse.

The insurance industry's digital transformation has introduced complex identity and access management challenges. From data storage across cloud platforms to managing access privileges for employees and third-party collaborators, agencies face a growing risk of unauthorized access.

Over-reliance on outdated systems, coupled with inadequate credential management, amplifies these vulnerabilities. Compliance with regulations such as GDPR, CCPA, and HIPAA is essential to avoid financial penalties and legal consequences. Ensuring robust password management is no longer optional—it's critical to safeguarding operations and maintaining customer trust. lost productivity, and the organization at risk of breaches, ransomware, reputational harm, and regulatory penalties.

In fact, over 88% of insurance leaders use third-party providers for some service provision, and agencies increasingly rely on technology to deliver personalized solutions in real-time, thereby expanding the attack surface.

Prevent unauthorized access and loss of data

As a trusted global leader in password and identity management, LastPass is uniquely positioned to solve the credential-driven security challenges insurance agencies face. With a focus on safeguarding sensitive data, LastPass enables agencies to create, store, manage, share, and protect credentials seamlessly, ensuring privacy and accessibility without sacrificing security. Designed to meet the demands of an industry rooted in trust and confidentiality, LastPass provides a centralized solution for robust credential management, reducing the risks associated with password-related breaches.Financial institutions must balance stringent security and compliance requirements with the need for a smooth experience for administrators and end users alike, including third-party collaborators.

Insurance agencies must balance stringent compliance requirements with the need for efficient collaboration between employees and third-party providers**.** LastPass offers a cloud-native platform that simplifies secure access and sharing, enforces tailored access policies, and provides real-time visibility into credential usage. Advanced reporting capabilities ensure that agencies can easily demonstrate compliance with regulations like GDPR, CCPA, and HIPAA, while also identifying and mitigating risks before they escalate. With LastPass, insurance agencies can protect their business and their customers with confidence, creating a secure foundation for growth and reliability in an increasingly digital world.

LastPass benefits for insurance agencies

The easiest, most affordable, and most reliable way for insurance agencies 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.