LastPass for financial services

Financial services is a subsector of critical infrastructure that spans accountants, banks, brokers, credit unions, crypto payment processors, family offices, FinTech, investment firms, platforms and more.

Passwords present a unique risk for financial services

Financial services organizations are prime targets for cyberattacks because due to the transactional nature of the industry, businesses operate in a heighted, fast-paced cyber threat environment, while managing sensitive customer data and financial assets. Threat actors use tactics like infostealers, phishing, and AI-driven social engineering campaigns to compromise passwords and identities, often leading to account takeovers and ransomware incidents.

Further, as these organizations increasingly adopt cloud-first strategies with numerous Software as a Service (SaaS) application, they face mounting challenges managing passwords and access securely. The rapid growth of these applications often leads to SaaS sprawl and shadow IT, where employees using unauthorized tools and apps create additional vulnerabilities and visibility gaps.

The shift to remote and hybrid work has only amplified collaboration and access risks, creating gaps that attackers exploit. Remote collaboration tools often lack centralized oversight, making it difficult to track and control user activity and when employees use unauthorized applications or tools to collaborate (e.g., personal email or messaging apps), they bypass security protocols and expose data to risks. Combined, these factors put customers at risk of fraud and social engineering, employees at risk of inefficiency and lost productivity, and the organization at risk of breaches, ransomware, reputational harm, and regulatory penalties.

According to the 2024 Verizon DBIR, system intrusion, miscellaneous errors, and social engineering represent 78% of breaches in the financial services industry.

Advanced password protection and security transparency

As a trusted global leader in password and identity management, LastPass is uniquely positioned to address the cybersecurity and productivity challenges financial services organizations face. Designed to meet the complex demands of a credential-driven industry, LastPass empowers organizations to create, store, manage, share and protect valuable credentials seamlessly—without compromising security, privacy, or accessibility.

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. LastPass delivers a cloud-native solution tailored to these needs by safeguarding sensitive credentials, enabling secure access and sharing for internal and external teams, and enforcing security-driven access policies that increase visibility and control to ensure compliance.

With advanced reporting, key stakeholders gain insight and are prepared for audit, making LastPass your go-to tool to prevent unauthorized access and instill confidence that your organization is prepared to face today's evolving threats.

LastPass benefits for financial services

The easiest, most affordable, and most reliable way for financial services organizations to slash cyber and operational risk is to standardize password management with LastPass across the enterprise.

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	**Standardize password protection**	Offers hundreds of customizable policies, flexible privileges, detailed reporting, and various authentication options, making it an indispensable tool in a tech stack.
	Extend secure access management	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.