LastPass for professional services

This sector includes accounting and auditing, consulting, engineering and architecture, information technology, legal services, marketing and advertising, and more.

Poor password practices are doubly concerning for professional services

The professional services industry provides specialized, knowledge-based services to their clients through contracts, acting as an extension of their team. As such, they are responsible for managing and safeguarding their clients' data in addition to their own, making them a lucrative target for cybercrime.

Compromised credentials are the easiest way for attackers to gain unauthorized access to this information, leading to potential data breaches, financial fraud, and reputational damage. For the clients, these breaches can result in loss of trust, financial setbacks, and exposure of proprietary information, creating a ripple effect of harm across businesses and industries.

Beyond security risks, access and collaboration needs present significant challenges for this sector. There is a regular exchange of information, such as logins to applications, social media accounts, or internal databases, with internal teams and external collaborators. Without effective tools to grant, manage, and revoke access, operations can suffer from inefficiencies, lost productivity, and unintentional security vulnerabilities.

74% of all breaches involve the human element, including the use of stolen credentials, social engineering, and errors.

10% of cybercrime within professional services results from miscellaneous error.

Convenient and secure access management

As a trusted global leader in password and identity management, LastPass is uniquely equipped to solve the credential challenges faced by professional service providers. Designed to meet the demands of a highly collaborative and credential-driven industry, LastPass empowers organizations to securely create, store, manage, share, and protect valuable credentials without sacrificing security, privacy, or ease of use. By providing a centralized and secure platform, LastPass eliminates the risk of credential mismanagement, ensuring sensitive business and client data remain protected from unauthorized access.

LastPass simplifies collaboration by enabling secure and controlled access to shared credentials for internal teams or external contractors. Simple access management ensures that team members only see what they need, while automated revocation ensure that access is promptly removed when no longer required. Additionally, LastPass delivers advanced reporting and visibility tools that help businesses maintain compliance and monitor credential usage. With LastPass, professional service providers can streamline collaboration and boost security to confidently protect both their business and their clients.

LastPass benefits for professional services

The easiest, most affordable, and most reliable way for professional services organizations 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.