

UNVARNISHED REVIEWS

1Password vs. Bitwarden vs. LastPass: The SSO Tier Trap and the 2025 Settlement

Market Position: Big Picture

The password manager category is growing fast: Independent market research generally clusters around \$3.4-4.6 billion for 2026, growing at roughly 20-22% compound annual growth rate through the early 2030s, though estimates vary depending on whether enterprise privileged-access management is folded into the category. Company-specific market-share rankings for these three products are genuinely inconsistent across sources in a way this report should be upfront about: One widely cited business-software tracker ranks 1Password first by a wide margin (72% adoption among businesses using a password manager), while consumer-usage surveys rank LastPass and Bitwarden ahead of 1Password instead. The two data sets appear to be measuring different populations, business-tool adoption versus individual consumer usage, not contradicting each other so much as answering different questions, but neither should be read as a single settled ranking.

The one figure with solid, company-disclosed backing: 1Password reported crossing \$400 million in annual recurring revenue in November 2025, up from \$250 million in 2023, a real growth trajectory even though it is a disclosed company milestone rather than an audited public filing. Bitwarden and LastPass (now part of GoTo) do not disclose comparably specific figures, so this report does not attempt to force a like-for-like revenue comparison across all three.

1Password, Bitwarden, and LastPass are the three most widely deployed password managers for teams and businesses, and all three are credible, well-reviewed products. Bitwarden leads on price and transparency, the only one of the three that is open-source and offers a self-hosted deployment path. 1Password leads on polish and non-technical-user adoption, and is the default choice for organizations heavy on Apple devices. LastPass remains the most widely deployed by raw customer count, with the largest user review volume of the three, but it carries a distinct history: a 2022 breach whose consequences are still unfolding in 2025, and a business pricing structure that gates full SSO access behind its highest tier.

The finding that should change how any of the three gets evaluated: LastPass's 2022 breach was not resolved when the incident response ended. In 2025, three years later, LastPass settled a US class action lawsuit for \$24.5 million over losses tied to stolen vault backups, and the UK's Information Commissioner's Office fined LastPass UK Ltd for failures affecting more than one million UK data subjects. Organizations still running LastPass, or evaluating it now, are inheriting a company mid-consequence, not one that closed the book in 2023.

Platform Ratings at a Glance

Platform	G2 Rating	Reviews (G2)	Notable Distinction
Bitwarden	4.6-4.7 / 5	~960-1,800	Ranked first in Enterprise User Satisfaction on the G2 Enterprise Grid for eleven consecutive quarters, per G2's comparison data.
1Password	4.6 / 5	~1,235-1,809	Highest-rated for autofill reliability and non-technical adoption in independent testing.
LastPass	4.4-4.5 / 5	~1,962-2,084	Largest review volume of the three, consistent with the longest market tenure and widest installed base.

The rating gap between LastPass and the other two is modest, but Users specifically flag renewal price increases and the free tier's single-device-type restriction as recurring complaints, both discussed below.

The LastPass Breach: Still Not Over in 2025

The underlying incident is well documented. In August 2022, an attacker compromised a LastPass engineer's corporate laptop and exfiltrated source code and an encrypted copy of the key protecting customer backups. In September 2022, the same attacker compromised a senior DevOps engineer's home computer, exploited through a vulnerability in third-party media software, and used a keystroke logger to obtain credentials granting access to LastPass's cloud storage. Between September and October 2022, the attacker copied backups of customer vault data, including unencrypted metadata such as website URLs, company names, billing addresses, and IP addresses, alongside encrypted fields such as usernames and passwords. LastPass has stated the encrypted fields remain protected by its zero-knowledge architecture and cannot be decrypted without each user's master password. That claim is accurate but incomplete: Many affected accounts, particularly older ones, had weak PBKDF2 iteration counts, in some cases as low as 100,000, a setting that was LastPass's own default years earlier and became inadequate as computing power increased. Combined with weak or reused master passwords, this made a meaningful subset of the stolen vaults crackable through offline brute-force attacks, attacks with no time pressure and no alerting, since the attacker already possessed the data.

What changes the risk calculus for a 2026 buyer is what has happened since. In 2025, LastPass settled a US class action lawsuit for \$24.5 million covering losses tied to the stolen vault backups. Separately, the UK's Information Commissioner's Office issued a monetary penalty against LastPass UK Ltd in November 2025 for failures to implement appropriate technical and organizational measures, affecting more than one million UK data subjects. Neither of these is a 2022 story. Both are 2025 consequences of a breach that took nearly three years to fully resolve through litigation and regulatory review.

The legal and regulatory consequences aren't the only evidence this remains active. TRM Labs, a blockchain intelligence firm, documented that the same vault backups stolen in 2022 were still being used to drain cryptocurrency wallets as recently as 2025, direct, ongoing harm traceable to the original breach, not a legal echo of it. LastPass has since raised its default PBKDF2 iteration count for new accounts, a genuine but forward-looking fix: It does nothing to protect vaults already stolen in 2022, which remain permanently outside LastPass's control and crackable indefinitely if the master password is weak.

Users who followed LastPass's guidance, a strong, unique master password not reused elsewhere, remained protected throughout: LastPass's zero-knowledge encryption means the stolen vault contents are not decryptable without that password. The exposure was real for anyone with a weak or reused master password, and the metadata theft (which sites each user accessed) itself created a durable phishing and targeting risk independent of whether any vault was ever cracked.

The SSO Tier Trap: A Pattern Across All Three, Sharpest at LastPass

Single sign-on and SCIM auto-provisioning, the features that let a company's identity provider control who has access to the password vault at all, are gated behind the top-priced tier at all three vendors. This is not unique to any one of them, but the severity differs meaningfully.

Bitwarden's Teams tier (roughly \$3-\$4/user/month) does not include SSO. Enterprise (roughly \$5-\$6/user/month) adds SAML 2.0 and OpenID Connect support along with SCIM 2.0 auto-provisioning, compatible with Entra ID, Okta, Google Workspace, Duo, JumpCloud, and Ping. The gate exists, but it is a clean two-tier structure.

1Password's Business tier (roughly \$7.99-8.99/user/month) includes SSO integration as a standard feature, the least gated structure of the three, though enterprise-scale deployments above roughly 250 users typically move to custom pricing regardless.

LastPass has the most granular, and most gated, structure. Teams (roughly \$4-\$4.25/user/month) includes no SSO at all. Business (roughly \$7/user/month) adds SSO, but capped at 3 connected apps, along with SCIM provisioning. Organizations that need SSO across more than 3 applications, a routine requirement for any company running more than a handful of core business tools, must move to a Business Max or add-on tier priced around \$8.84-\$9/user/month for unlimited SSO apps. A 30-person team on the capped Business tier pays roughly \$2,714/year; the same team on the uncapped tier pays roughly \$3,182/year, a jump that exists purely to remove an artificial app-count ceiling, not for any additional security capability.

The Other Pricing Story: 1Password's First Increase in Years

Effective March 27, 2026, 1Password raised its individual and family subscription prices by as much as 33%, its first increase in several years according to the company's notice to customers. The individual plan rose from \$3.99 to \$4.99/month (\$35.88 to \$47.88/year), and the family plan rose from \$6.95 to \$7.99/month (\$59.88 to \$71.88/year). 1Password attributed the increase to continued investment in security and features including phishing protection and faster device setup. The increase applies to individual and family plans specifically; published Business tier pricing was not part of this announced change.

Pricing (July 2026)

Platform	Team Tier (No/Limited SSO)	Top Tier (Full SSO)	Self-Host Option
Bitwarden	\$3-\$4/user/month (Teams)	\$5-\$6/user/month (Enterprise)	Yes, only vendor of the three
1Password	\$19.95/month flat, up to 10 users (Teams)	\$7.99-\$8.99/user/month (Business)	No
LastPass	\$4-\$4.25/user/month (Teams, no SSO)	\$8.84-\$9/user/month (Business Max, unlimited SSO)	No

All figures are third-party pricing-tracker estimates and vendor list prices, not negotiated contract figures. Confirm current rates before budgeting.

Costs the Pricing Table Misses

- **LastPass's SSO app cap.** The published Business-tier price looks competitive until the 3-app SSO limit forces an upgrade for any organization running a normal SaaS stack.
- **1Password's Teams-tier ceiling.** The flat \$19.95/month Teams plan covers only up to 10 users; organizations at 11 users or more move to per-seat Business pricing immediately, a step change rather than a gradual scale.
- **Add-on MFA and premium support at LastPass.** Advanced authentication methods (hardware tokens, biometric integrations) can add \$1-\$3/user/month on top of published Business pricing.
- **Renewal pricing.** Users specifically flag LastPass renewal increases as a recurring complaint; get renewal-year pricing in writing before signing a multi-year term with any of the three.

TCO Comparison: 25-Person Company, Full SSO Requirement, 3 Years

Modeled scenario: 25 employees, SSO required across more than 3 connected applications, using the tier each vendor requires to meet that requirement at the pricing published above.

Platform	Required Tier	Monthly Rate	3-Year Total
Bitwarden	Enterprise	\$5.50/user (midpoint)	\$4,950
1Password	Business	\$8.49/user (midpoint)	\$7,641
LastPass	Business Max (uncapped SSO)	\$8.92/user (midpoint)	\$8,028

Bitwarden is the clear cost leader at this scale once full SSO is required, roughly 38% less than 1Password and 62% less than LastPass over three years. The LastPass figure also isolates the SSO-cap trap in dollar terms: Staying on the capped Business tier would cost \$6,300 over three years, meaning the jump to remove the artificial 3-app ceiling costs \$1,728 over the contract, real money spent solely to undo a limit the base tier didn't need to have in the first place.

Complexity Comparison

Deployment architecture is the dividing line here: LastPass and 1Password are both cloud-only, while Bitwarden is the only one of the three that offers a genuine self-hosted path, a choice that shapes admin overhead more than any other factor in this table.

Dimension	1Password	Bitwarden	LastPass
Implementation	1Password's own marketing describes provisioning as pasting a bearer token into an identity provider with no installation or server maintenance required; independent enterprise-sysadmin sources corroborate this as the most polished deployment experience of the three, backed by a dedicated onboarding team	Cloud deployment is comparable in speed to the other two; the self-hosted option (official Docker Compose deployment with API, Identity, Admin, NGINX, and database containers) is real infrastructure work most organizations don't take on unless self-hosting is a specific requirement	Fastest raw deployment of the three per independent sources: Browser-based with no device agents required, deployable across an organization in an afternoon, though this speed advantage doesn't extend to its admin console, which the next row covers
Admin dependency	Lowest of the three per independent enterprise-sysadmin accounts; minimal configuration overhead for SSO and SCIM integration is cited as a specific reason to choose it when admin time is the binding constraint	Moderate for the cloud tier; one independent source puts initial admin setup at roughly 3-5 hours of documentation on first rollout, and its Collections-based sharing model requires more initial setup thinking than group-based approaches. Self-hosting adds real, ongoing patching and uptime responsibility on top of that	Independently documented as requiring more SCIM configuration effort than 1Password, and its admin console is described by an enterprise sysadmin source as less polished, a real ongoing cost even though initial deployment is fast
Learning curve	Consistently rated the most guided and non-technical-friendly of the three across independent sources, a documented driver of high adoption rates among end users specifically, not just admins	Functional but described consistently as less polished than 1Password; its Collections and Send-based sharing model is a different mental model from folder-based sharing that admins and end users both need to learn	Comparable to Bitwarden for end users given its browser-based simplicity, but the admin side carries a real, separate learning curve tied to its less-guided console

The self-hosting decision is the fork this table turns on. Choosing Bitwarden's self-hosted path trades subscription cost for real, ongoing infrastructure ownership, patching, uptime, and backup responsibility that 1Password's cloud-only model and LastPass's cloud-only model both eliminate entirely. For organizations without that responsibility as a requirement, 1Password's admin experience is independently and consistently rated the smoothest of the three, the direct product of dedicated onboarding support and minimal SSO/SCIM configuration overhead. LastPass's fast initial deployment doesn't carry through to ongoing administration, where its console is the least polished of the three per independent accounts, a real gap between how quickly it goes live and how easy it stays to run.

The Decision Framework

Choose Bitwarden if: Budget and code-level transparency matter most. It is the only self-hostable option of the three, has the cleanest two-tier SSO structure, and User data shows it leading Enterprise User Satisfaction for eleven consecutive quarters.

Choose 1Password if: Non-technical adoption and polish matter most, particularly in Apple-heavy environments, and your organization is small enough for flat Teams pricing or large enough to negotiate custom Business terms.

Choose LastPass if: You have specific institutional reasons to stay (existing deployment, specific integration dependencies) and have already enforced mandatory master password rotation and MFA fleet-wide. Confirm the SSO app-count cap against your actual application count before signing, and budget for the uncapped tier if you run more than 3 SSO-connected apps.

Everyone: Enforce strong, unique master passwords regardless of vendor. LastPass's 2022 breach caused real, ongoing harm, not just at the time, but for years afterward, concentrated in accounts where master passwords were weak or reused and, for older accounts specifically, where iteration counts hadn't been strengthened before the breach occurred.

The Bottom Line

Bitwarden and 1Password are both credible, well-reviewed choices with clean, comparatively minor tier-gating patterns. LastPass remains a technically capable product with the largest installed base of the three, but it carries two distinct 2026 realities that a sticker-price comparison won't show: a breach whose legal and regulatory consequences were still landing in 2025, three years after the incident, and a pricing structure where a routine SSO requirement, more than 3 connected apps, forces an upgrade past the plan most buyers would otherwise choose.