LastPass

SSO ist nicht genug: Die Zukunft ist passwortlos

Wischen ⟶

Mit Single Sign-On (SSO) lassen sich Konten zentral verwalten, sodass Angestellte einfach und sicher auf ihre Cloud-Apps zugreifen können.

SSO kann aber Lücken hinterlassen.

Angesichts dessen, dass 80 % der Datenschutzverletzungen auf kompromittierte Zugangsdaten zurückzuführen sind, gilt es, jede Identität im Unternehmen zu schützen.

Sehen wir uns an, warum SSO zwar sinnvoll ist, aber zum Schutz Ihres Unternehmens nicht ausreicht – und wie Sie diese Lücke schließen können.

**Verizon DBIR

Welche Sicherheitslücken hinterlässt SSO?

Nicht alle Apps sind mit SSO-Technologien kompatibel.

Wenn Ihr Unternehmen spezielle Apps oder unübliche Softwarelösungen verwendet, funktionieren diese oft nicht mit SSO. Dies kann Hackern Schlupflöcher eröffnen.

Wie Die Passwortlose Authentifizierung Diese Lücken Schließt

Eine passwortlose Lösung deckt jeden Zugriffspunkt im Unternehmen ab. Angestellte können einfach und sofort auf ihre Websites und Apps zugreifen.

Ein Passwort weniger – was bringt Ihnen das?

HÖHERE BENUTZER-AKZEPTANZ

Ihre Angestellten können sofort auf ihren Vault zugreifen, ohne ein Passwort eingeben zu müssen.

HÖHERE PRODUKTIVITÄT

Ihre Angestellten (und Ihr IT-Team) können sich auf wichtigere und rentablere Aufgaben konzentrieren.

HÖHERE SICHERHEIT

Weniger Passwörter bedeuten weniger Möglichkeiten für Datenschutzverletzungen und Hackerangriffe.

Die Zukunft ist passwortlos

Schützen Sie jede Identität mit LastPass.

LastPass kontaktieren