

L'autenticazione senza password è una realtà

Accedi in modo semplice e sicuro alla cassaforte di LastPass



Punta al massimo della sicurezza con il minimo dello sforzo

In un mondo sempre più orientato alla digitalizzazione, diventa impossibile evitare di lasciare tracce digitali quando creiamo nuovi account o ne usiamo le credenziali. Per un'impresa, come anche per i suoi lavoratori, è fondamentale favorire la produttività e raggiungere quotidianamente gli obiettivi prefissati. Per garantire protezione a livello aziendale, risulta quindi necessario implementare criteri di sicurezza che spingano il personale ad adottare l'approccio giusto con le password.

Proprio per questo, una delle sfide che tutte le imprese sono chiamate ad affrontare in materia di sicurezza consiste nel tentativo di raggiungere il giusto equilibrio tra semplicità e protezione. Da una parte servono criteri o strumenti che possano essere efficacemente implementati, ma dall'altra questi devono risultare facili da configurare, usare e gestire perché, altrimenti, il personale tornerà a rimettere in pratica il solito approccio inadeguato alle password. Ma finalmente non sei più costretto a scegliere tra sicurezza e semplicità: ora puoi averle entrambe attivando l'autenticazione senza password per accedere alla cassaforte di LastPass.

Metti il pilota automatico alle password principali

Tutti gli utenti finali di LastPass possono effettuare l'accesso al gestore di password tramite LastPass Authenticator attivando l'autenticazione senza password mentre creano il proprio account, quando vi accedono per la prima volta oppure direttamente dalle impostazioni. Una volta completata la configurazione guidata, possono accedere alla loro cassaforte senza doverne mai digitare la password sui dispositivi attendibili.

Aspetta a dire addio alla password principale

Anche se lo scopo finale consiste nel liberarsi completamente dalle password, le tecnologie per l'autenticazione senza password sono in costante evoluzione e, per raggiungerlo, è dunque necessario un approccio graduale. Per il momento, la password principale continuerà a essere utilizzata per confermare le modifiche alle impostazioni dell'account che hanno effetti sulla sicurezza e nei casi in cui un tentativo di autenticazione non dovesse avere esito positivo. Dal momento che gli utenti useranno questa password con minore frequenza, assicurati che impostino le opzioni di recupero dell'account in modo da avere sempre un'opzione di riserva per riottenere l'accesso.



Esperienza utente semplificata



Meno complicazioni dovute alle password



Più produttività per gli amministratori IT



Autenticazione sicura

[Prova l'autenticazione senza password](#)

Un mondo senza password è possibile

Esperienza utente semplificata

Usando LastPass Authenticator, i dipendenti non hanno bisogno di inserire la password principale per accedere alla cassaforte e gestire le credenziali degli account. Assicura un accesso istantaneo e agevole, riducendo enormemente le complicazioni dovute alle password. Distribuisci il nostro gestore di password per proteggere la vita digitale della tua organizzazione e poi ottimizzane l'accesso liberando il personale dalle password.

Standard di sicurezza più severi

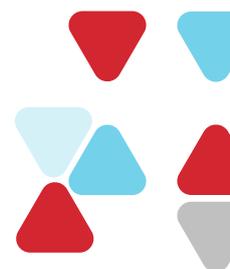
I tuoi dipendenti adesso possono impostare una password principale ancora più complessa, dal momento che non avranno più bisogno di digitarla, un requisito che puoi applicare attraverso criteri di sicurezza più rigidi. Ridurre la frequenza con cui il personale è tenuto a usare e inserire la password principale contribuisce a proteggere loro e la tua azienda dalla criminalità informatica.

Le complicazioni scendono, l'adozione sale

Ridurre le complicazioni dovute alle password ha l'effetto di aumentare l'accesso alla cassaforte di LastPass, il che ne favorisce l'adozione in tutta l'organizzazione. Una maggiore adozione da parte del personale si traduce in un migliore approccio complessivo alle password e, di conseguenza, in una sensibile riduzione dei rischi per la sicurezza informatica.

Maggiore produttività

Quando le password vengono eliminate dall'equazione, i dipendenti non mettono più in pausa il loro lavoro per ripristinarle né rischiano di rimanere tagliati fuori dai loro account e, di conseguenza, il personale informatico non deve più dedicare il proprio tempo a occuparsi di questi problemi. In questo modo, tutto l'organico aziendale può concentrarsi sulle iniziative in grado di apportare un reale valore, anziché perdere tempo con le password.



Liberati dalle password con LastPass Business