LastPass •••|

APS IT diensten

Wachtwoordroof: Waarom de toekomst Wachtwoordloos moet zijn

Welkom

Peter van Zeist

Gepassioneerd Duiker, Smart-Home Enthousiast,
Formule 1 Fan, **Manager, Solutions Consulting EMEA**
& Principal Solutions Consultant

Peter.vanZeist@LastPass.com

Agenda

1. Crisis in gecompromitteerde inloggegevens
2. Voordelen voor eindgebruikers
3. Wachtwoordloos
4. Veiligheid
5. Vragen en samenvatting

LastPass

PERSONEN EN WACHTWOORDEN:
EEN STEEDS GROTER WORDEND TOEGANGSPUNT VOOR DE

Crisis in gecompromitteerde inloggegevens

#1 BEDREIGING

86% van datalekken zijn het gevolg van gecompromitteerde inloggegevens

LastPass

[1] *Verizon Data Breach Investigation Report, 2023*

Wachtwoordbeveiliging ligt in handen van onze medewerkers

9/10

GEBRUIKERS WETEN DAT ZE EEN WACHTWOORD-PROBLEEM HEBBEN

51%

VAN DE MENSEN VERTROUWEN OP HUN GEHEUGEN OM WACHTWOORDEN TE ONTHOUDEN

2/3

HERGEBRUIKEN WACHTWOORDEN KEER OP KEER

DIT MENSELIJKE GEDRAG LEIDT TOT RISICO'S...

LastPass

BLOOTSTELLINGSPUNT UITBREIDEN

Het creëren van een steeds groter wordend aanvalsoppervlak voor elke functie

Het aantal wachtwoorden stijgt!

Wachtwoorden zijn nog lang niet 'dood'

x2 Meer nieuwe accounts in 2021 dan in het voorgaande jaar.

Kleine en middelgrote bedrijven
(1-25 Medewerkers)

Ø85 Wachtwoorden per werknemer

Grote bedrijven
(>1k Medewerkers)

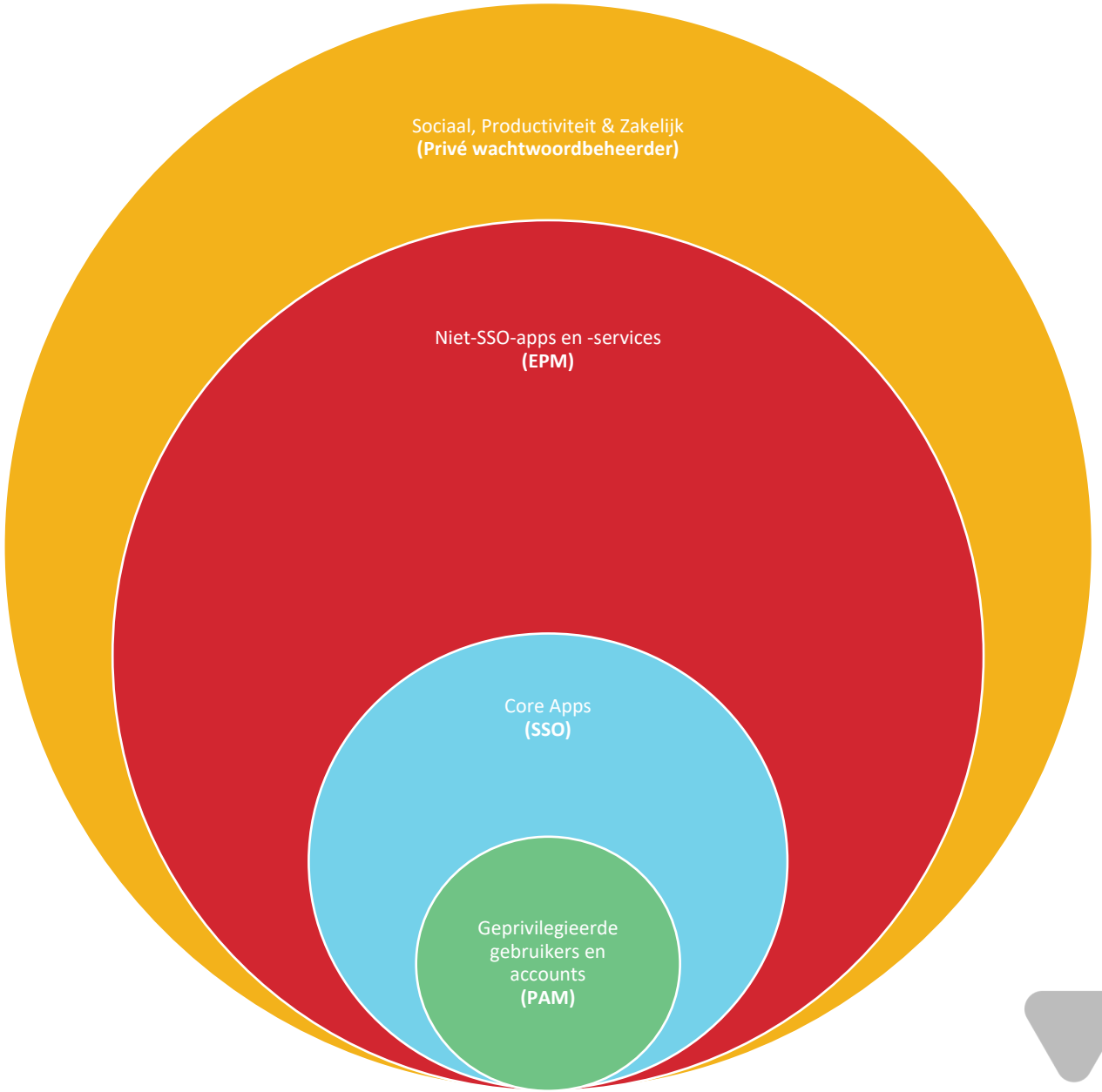
Ø25 Wachtwoorden per werknemer

LastPass

Bron: LastPass PoP Report

EEN NIEUWE GENERATIE CLOUDKEUZES

Eindgebruikers blijven een explosie van apps gebruiken die niet beveiligd zijn met SSO



LastPass

ONS STANDPUNT: GA VERDER

Gemak is slechts het startpunt...

Echt succes op het gebied van wachtwoord-beveiliging komt voort uit het veranderen van menselijk gedrag

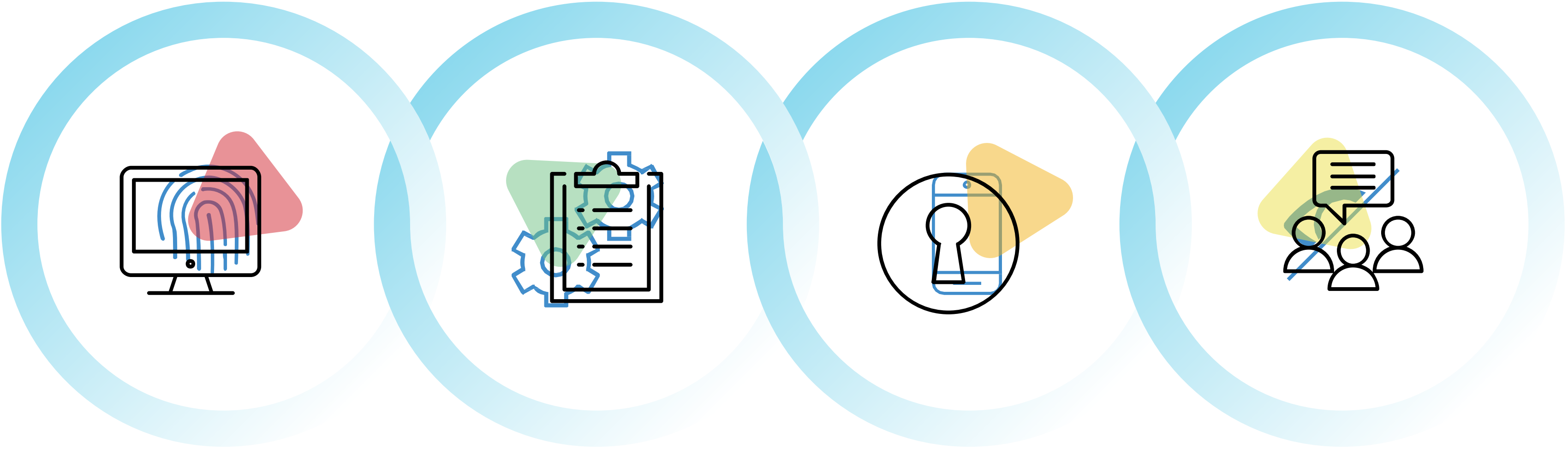
LastPass

HET PROBLEEM

Slechte gewoonten zijn helaas normaal en gebruikelijk in elke organisatie

DE OPLOSSING

LastPass heeft een alomvattende impact



Gebrek aan inzicht en overzicht

Slechte wachtwoordgewoonten

Gebrek aan wachtwoordbeveiliging op ALLE apparaten

Onveilig delen van gevoelige informatie

Bedrijfsbrede overkoepelende wachtwoordbeveiliging en overzicht

Gedetailleerde controle wachtwoordhygiëne (lengte, complexiteit)

Uitgebreide bescherming van alle apparaten op alle werkplaatsen

Gevoelige gegevens veilig delen

LastPass

Gartner Research

Innovation Insight: Workforce Password Management Tools

Published: 18 March 2024

Summary

Met toenemende complexe wachtwoordbeleidsregels hebben gebruikers moeite om bij te blijven en kunnen ze kiezen voor onveilige shortcuts. Security- en risicobeheerders die zich richten op IAM zouden workforce password management tools moeten omarmen om gebruikers te helpen wachtwoorden te beheren en de inlogervaring te vereenvoudigen.

Included in Full Research

Overview

Key Findings

- Organizations create complex password policies and too often fail to enforce them rigorously. These tedious policies are ineffective in addressing different kinds of password attacks.
- Password length and complexity requirements impact user experience (UX), which can drive users to unsecure behaviors, such as storing passwords in unprotected files.
- Workforce password management (WPM) tools can simplify access to legacy applications that do not support federation. Deployment of these solutions is less labor-intensive compared to alternative identity access management (IAM) tools.

Recommendations

LastPass

Voordelen voor eindgebruikers

Platformonafhankelijk

Altijd waar je het nodig hebt.

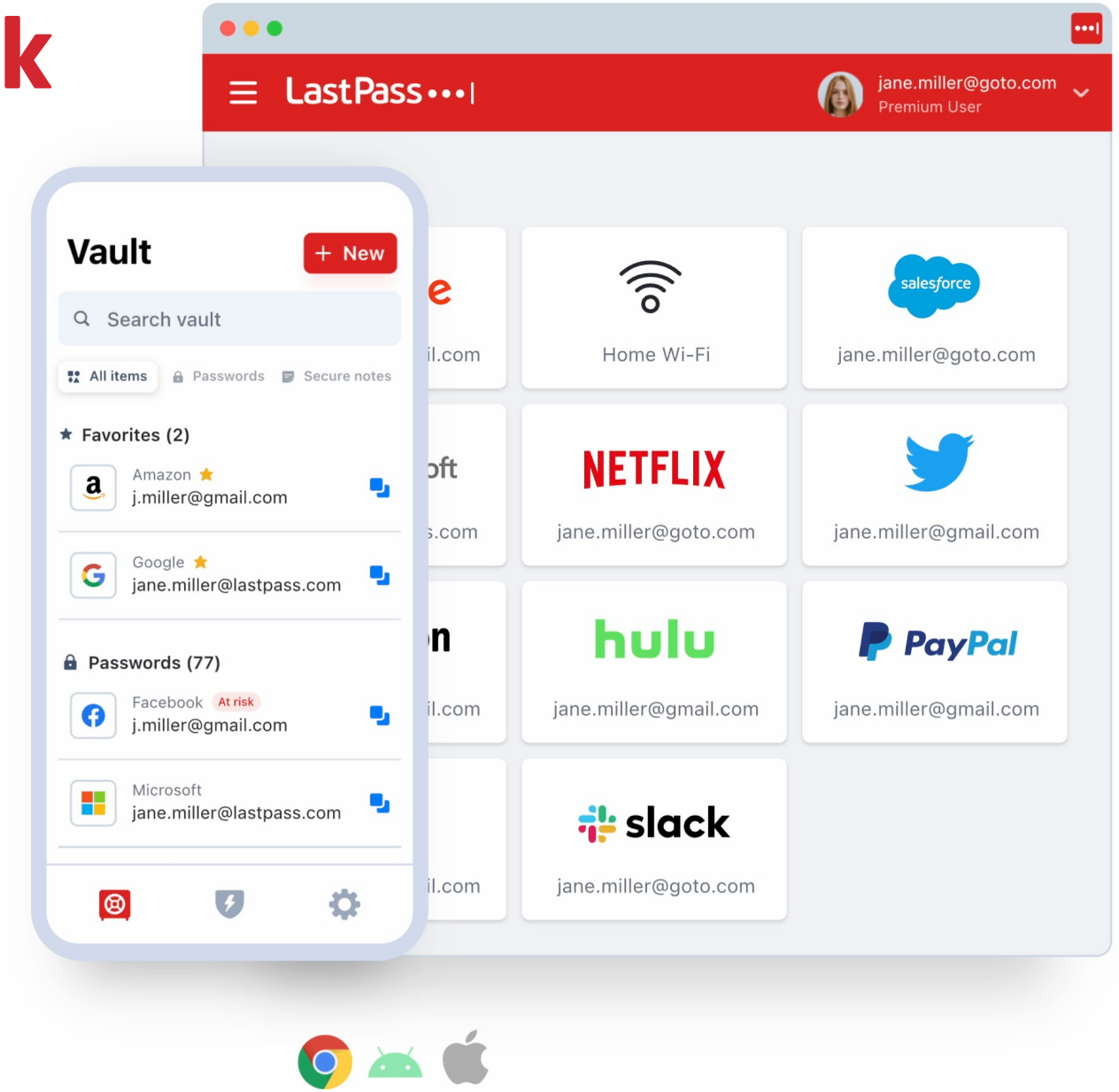
Verkrijgbaar als

Browser-extensie
Chrome, Firefox, Edge, Safari & Opera

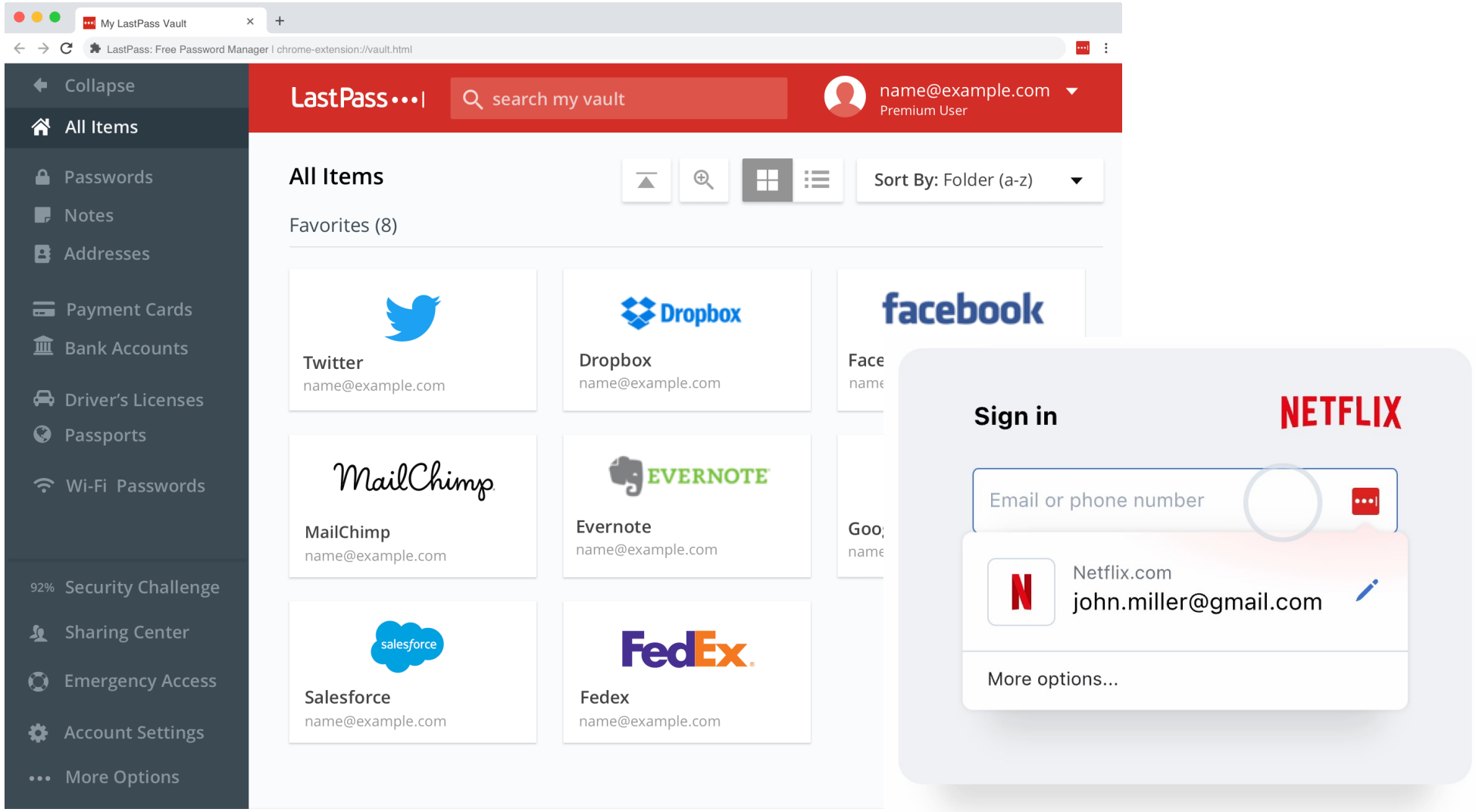
Desktop-applicatie
Windows & Mac

Mobiele applicatie
iOS & Android

Webversie

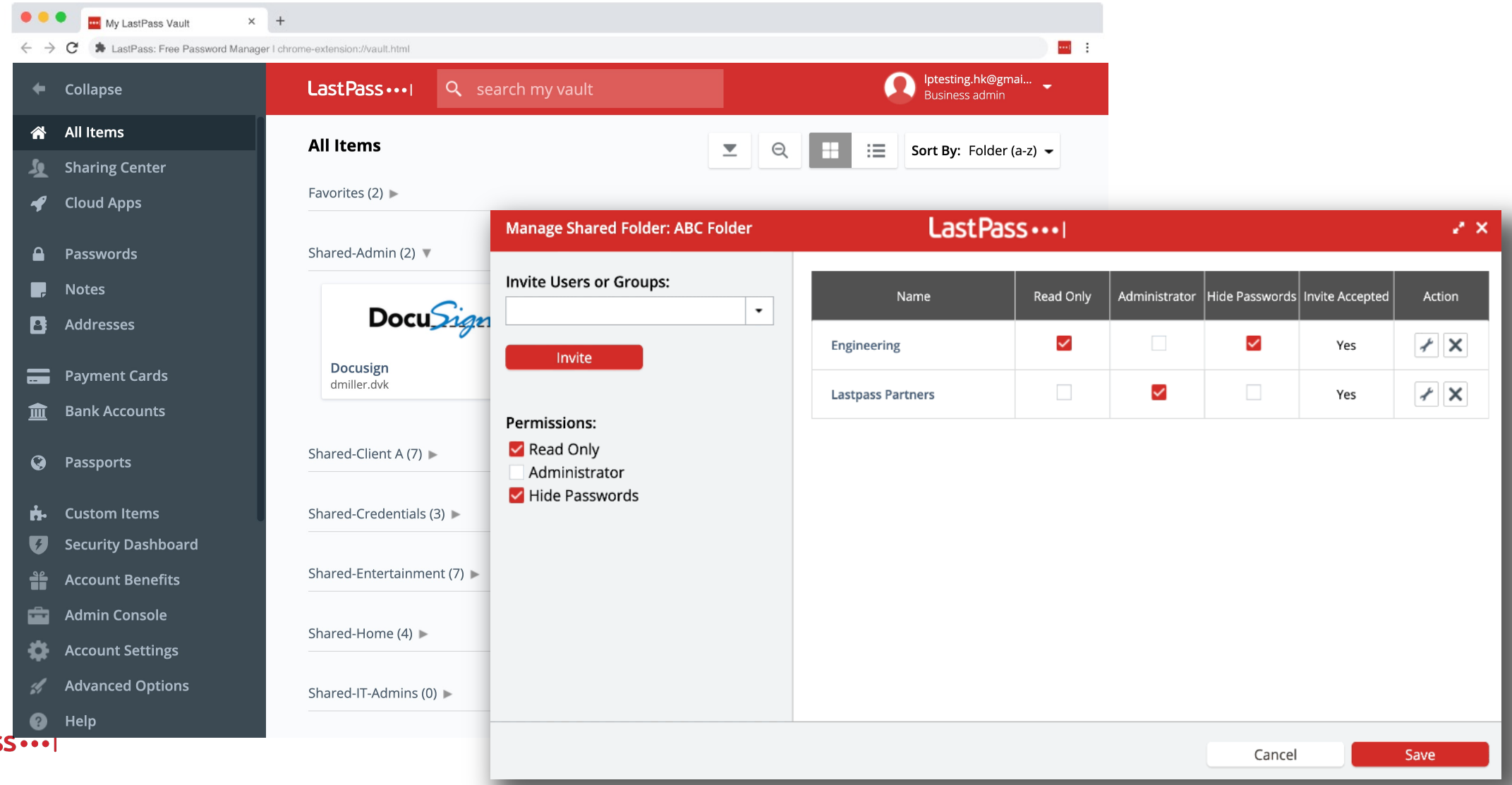


Ervaring van de eindgebruiker

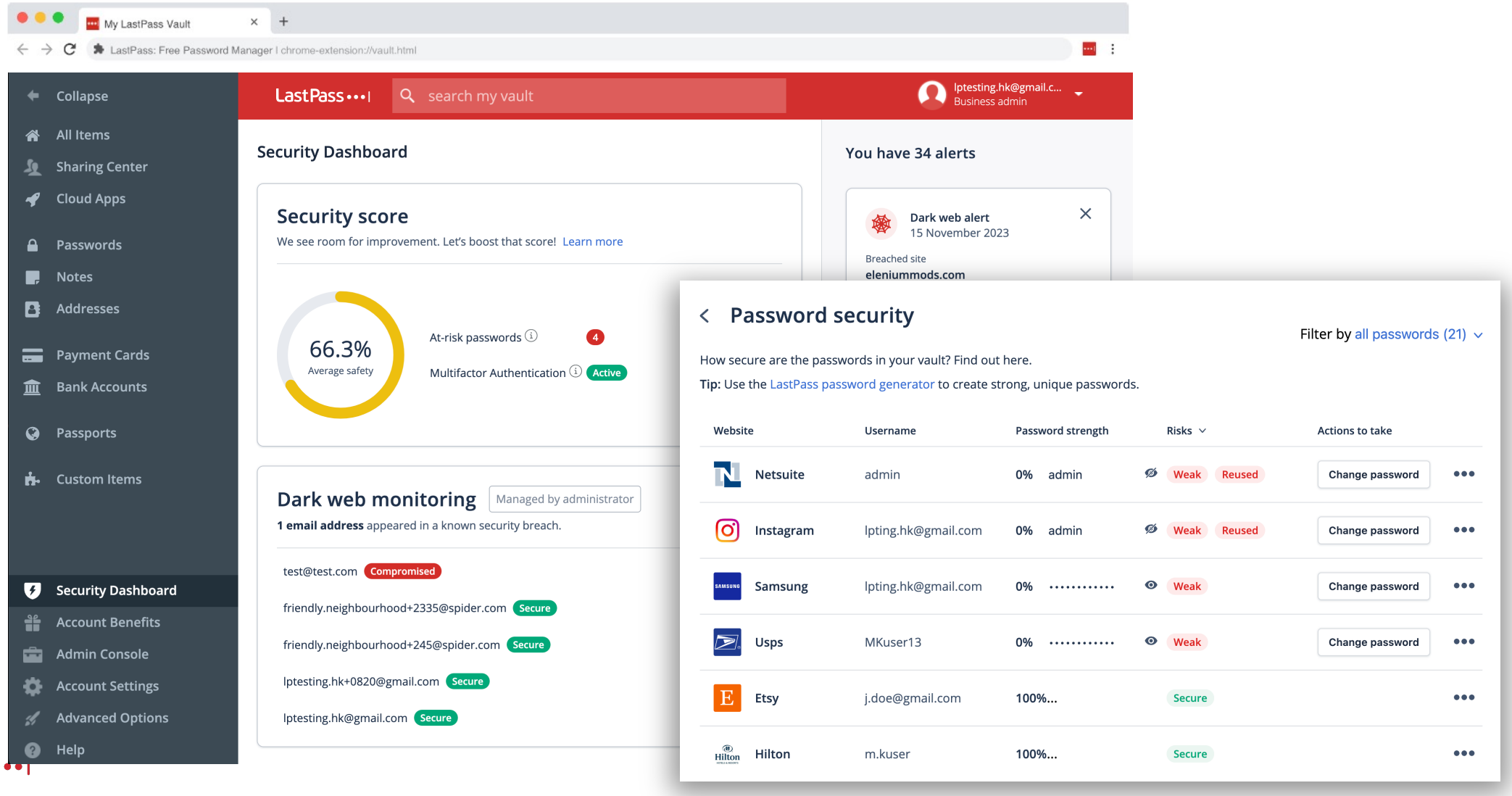


LastPass

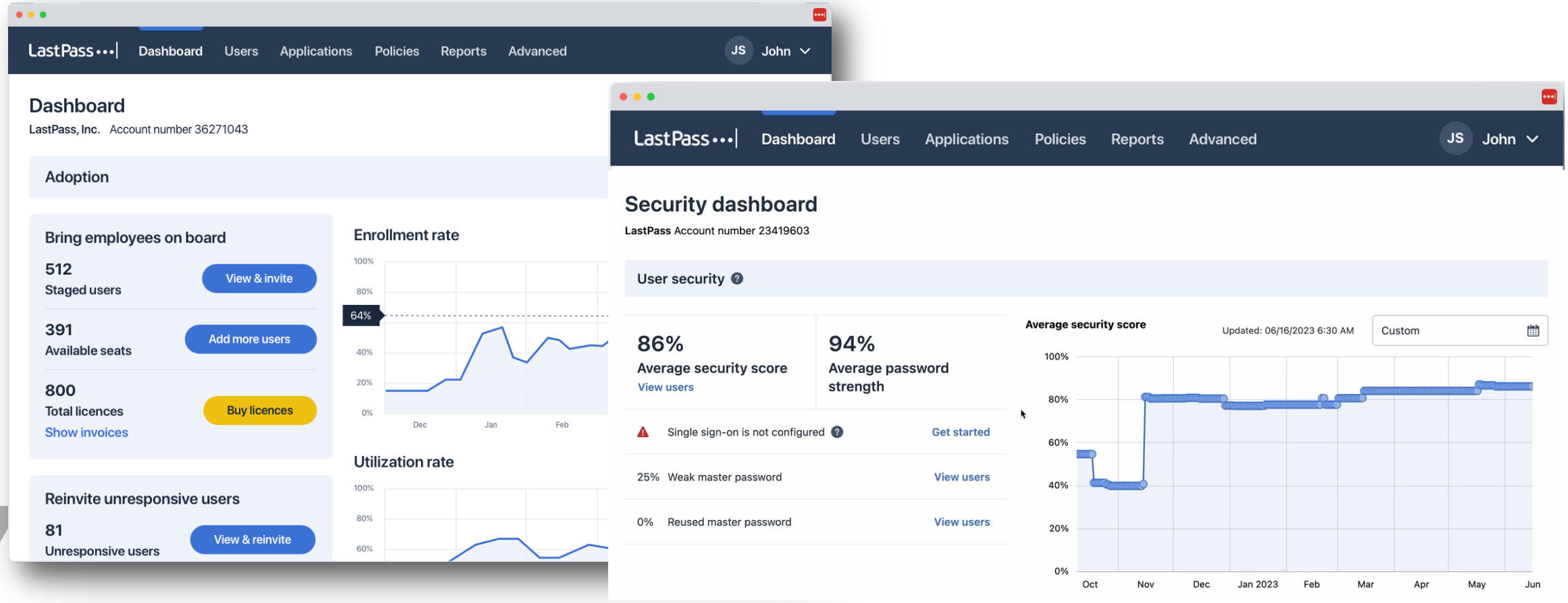
Veilig delen van inloggegevens



Blijf op de hoogte van uw beveiliging

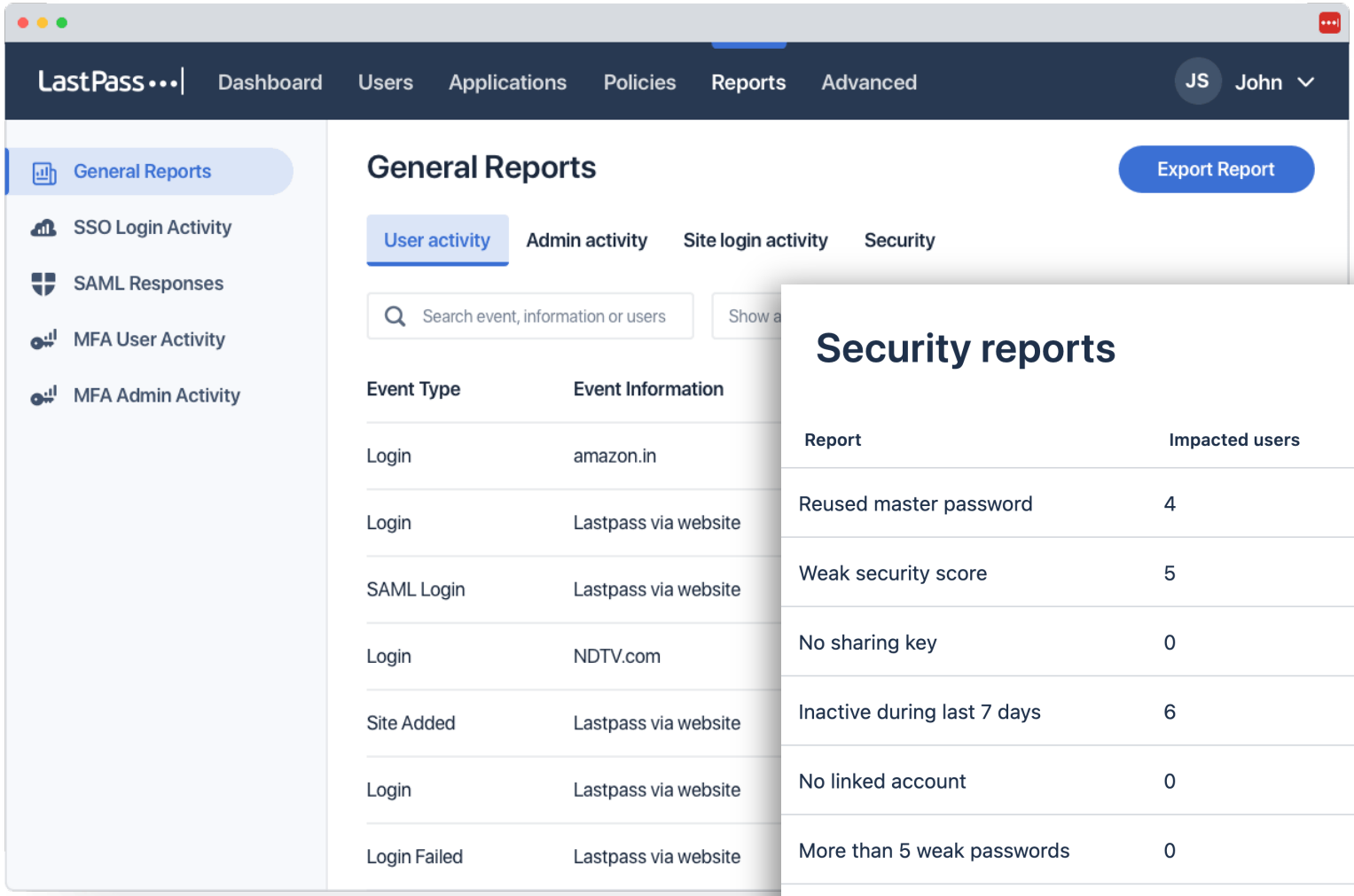


Beheerders dashboard voor acceptatie en beveiliging



LastPass

Gedetailleerde rapportage



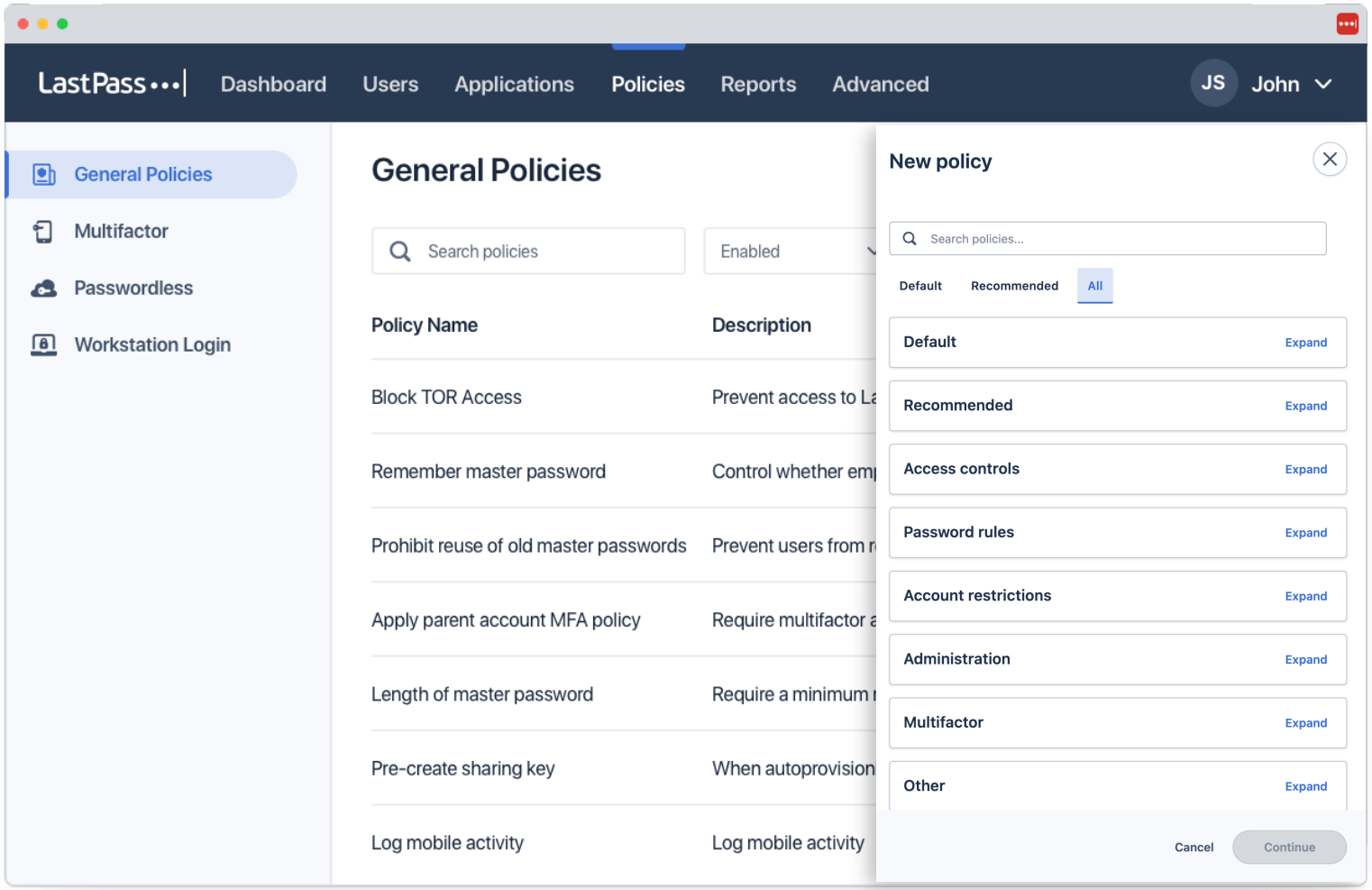
Security reports

Request update

Report	Impacted users	% of users impacted
Reused master password	4	44.45 %
Weak security score	5	55.56 %
No sharing key	0	0.00 %
Inactive during last 7 days	6	66.67 %
No linked account	0	0.00 %
More than 5 weak passwords	0	0.00 %
More than 3 duplicate passwords	0	0.00 %

LastPass

Uitgebreid beveiligingsbeleid



LastPass

Families as a Benefit

Bescherming van zakelijke EN privégegevens

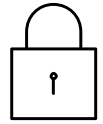
Goede wachtwoordhygiëne - niet alleen op het werk, maar ook thuis!

Met Families as a Benefit krijgt elke medewerker van u **6 gratis privélicenties** - om te delen met vrienden en familie.

Verbind beide accounts voor **gemakkelijke toegang!**

LastPass

Waarom implementeren steeds meer organisaties LastPass?



Risicobeperking

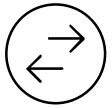
Vermindering van risico's die gepaard gaan met de hygiëne van inloggegevens, zoals phishing en sociale aanvalsvectoren.

Naleving van de regelgeving (NIS2...)

Zorgen voor de mogelijkheid om beleid te implementeren en beheeractiviteiten rond wachtwoordbeheer te registreren.

Inloggegevens delen

Volg en beheer het delen van wachtwoorden om risico's en misbruik te voorkomen, terwijl u controle krijgt en aansprakelijkheden van derden minimaliseert.



Schaduw-IT

Vermindering van de risico's die gepaard gaan met de kloof tussen de verificatie van bedrijfs-ID's en persoonlijke wachtwoordhygiëne.

Vereenvoudiging

Gemakkelijker voor werknemers om veilig toegang te krijgen tot werk- en persoonlijke inloggegevens op laptops en smartphones en deze te beheren.

LastPass

Wachtwoordloos

LastPass

Belang van complexe wachtwoorden

Aantal tekens	Getallen	Kleine letters	Kleine en hoofdletters	Getallen, kleine en hoofdletters	Getallen, kleine en hoofdletters + speciale tekens
4	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
5	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
6	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
7	Onmiddellijk	Onmiddellijk	1 Sek	2 Sek	4 Sek
8	Onmiddellijk	Onmiddellijk	28 Sek	2 Min	5 Min
9	Onmiddellijk	3 Sek	24 Min	2 Uur	6 Uur
10	Onmiddellijk	1 Min	21 Uur	5 Dagen	2 Weken
11	Onmiddellijk	32 Min	1 Maanden	10 Maanden	3 Jaren
12	1 Sek	14 Uur	6 Jaren	53 Jaren	226 Jaren
13	5 Sek	2 Weken	322 Jaren	3k Jaren	15k Jaren
14	52 Sek	1 Jaar	17k Jaren	202k Jaren	1m Jaren
15	9 Min	27 Jaren	898k Jaren	12m Jaren	77m Jaren
16	1 Uur	713 Jaren	46m Jaren	779m Jaren	5Mrd Jaren
17	14 Uur	18k Jaren	2Mrd Jaren	48Mrd Jaren	380Mrd Jaren
18	6 Dagen	481 Jaren	126Mrd Jaren	2Bn Jaren	26Bn Jaren

https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Belang van complexe wachtwoorden

2020

Aantal tekens	Getallen	Kleine letters	Kleine en hoofdletters	Getallen, kleine en hoofdletters	Getallen, kleine en hoofdletters + speciale tekens
4	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
5	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
6	Onmiddellijk	Onmiddellijk	Onmiddellijk	1 Sek	5 Sek
7	Onmiddellijk	Onmiddellijk	25 Sek	1 Min	6 Min
8	Onmiddellijk	5 Sek	22 Min	1 Uur	8 Uur
9	Onmiddellijk	2 Min	19 Uur	3 Dage	3 Weeken
10	Onmiddellijk	58 Min	1 Maanden	7 Maanden	5 Jaren
11	2 Sek	1 Dag	5 Jaren	41 Jaren	400 Jaren
12	25 Sek	3 Weeken	300 Jaren	2k Jaren	34k Jaren
13	4 Min	1 Jahr	16k Jaren	100k Jaren	2m Jaren
14	41 Min	51 Jaren	800k Jaren	9m Jaren	200m Jaren
15	6 Uur	1k Jaren	43m Jaren	600m Jaren	15bn Jaren
16	2 Dage	34k Jaren	2bn Jaren	37bn Jaren	1tn Jaren
17	4 Weeken	800k Jaren	100bn Jaren	2tn Jaren	93tn Jaren
18	9 Maanden	23m Jaren	6tn Jaren	100tn Jaren	7qd Jaren

3 Jaar

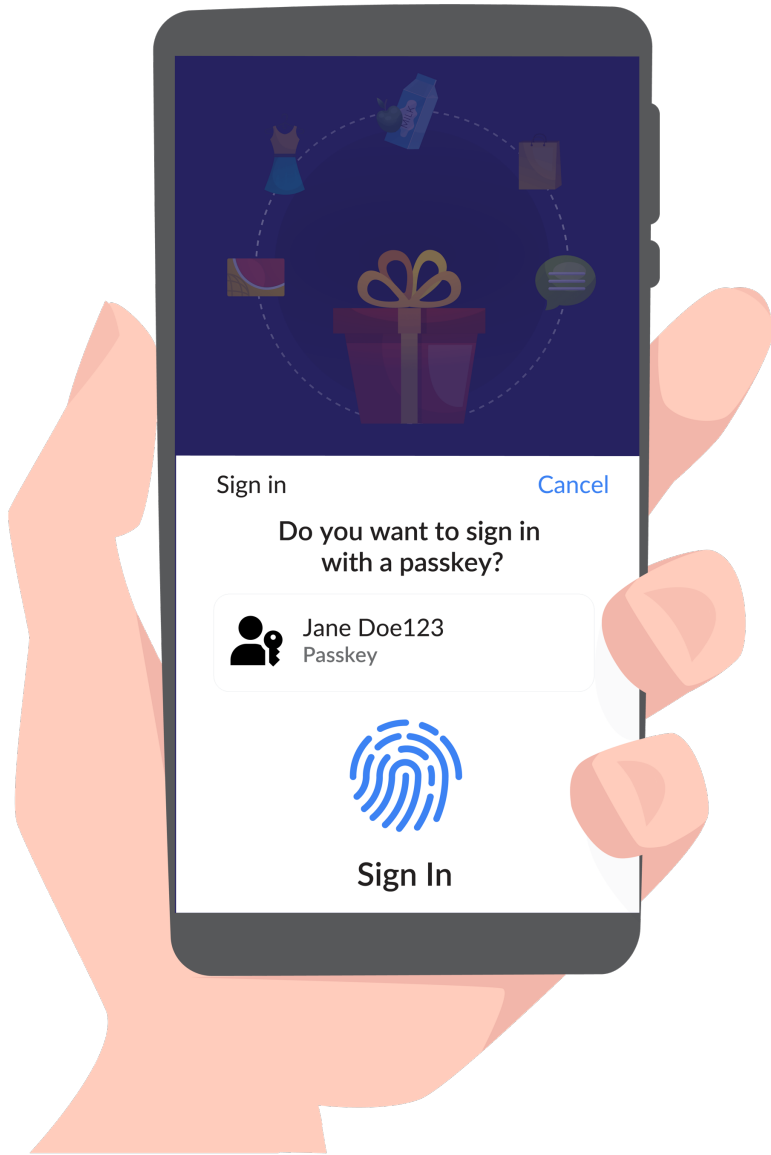
2023

Aantal tekens	Getallen	Kleine letters	Kleine en hoofdletters	Getallen, kleine en hoofdletters	Getallen, kleine en hoofdletters + speciale tekens
4	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
5	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
6	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk	Onmiddellijk
7	Onmiddellijk	Onmiddellijk	1 Sek	2 Sek	4 Sek
8	Onmiddellijk	Onmiddellijk	28 Sek	2 Min	5 Min
9	Onmiddellijk	3 Sek	24 Min	2 Uur	6 Uur
10	Onmiddellijk	1 Min	21 Uur	5 Dagen	2 Weken
11	Onmiddellijk	32 Min	1 Maanden	10 Maanden	3 Jaren
12	1 Sek	14 Uur	6 Jaren	53 Jaren	226 Jaren
13	5 Sek	2 Weken	322 Jaren	3k Jaren	15k Jaren
14	52 Sek	1 Jaar	17k Jaren	202k Jaren	1m Jaren
15	9 Min	27 Jaren	898k Jaren	12m Jaren	77m Jaren
16	1 Uur	713 Jaren	46m Jaren	779m Jaren	5Mrd Jaren
17	14 Uur	18k Jaren	2Mrd Jaren	48Mrd Jaren	380Mrd Jaren
18	6 Dagen	481 Jaren	126Mrd Jaren	2Bn Jaren	26Bn Jaren

LastPass

Wat zijn Passkeys?

Passkeys zijn een vorm van wachtwoordloze authenticatie die een snellere, eenvoudigere en veiligere aanmelding bij applicaties mogelijk maken als vervanging van wachtwoorden.



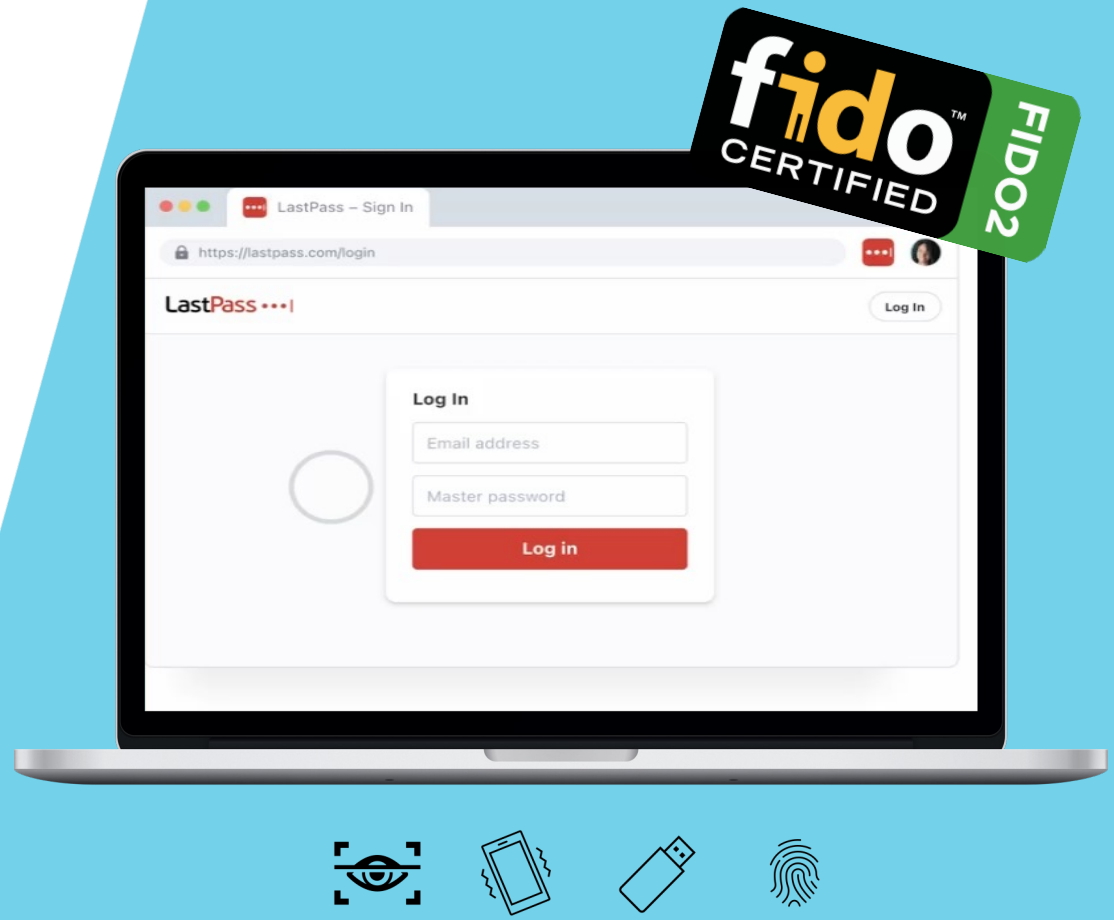
LastPass

Wachtwoordloos inloggen met FIDO2-compatibiliteit

KIES HOE U WACHTWOORDLOOS WILT INLOGGEN

Alle gebruikers kunnen nu inloggen op hun kluis met FIDO2-compatibele authenticators, met biometrie of hardwaresleutels.

FIDO2-compatibele authenticatiemechanismen maken gebruik van het WebAuthN-protocol, de toonaangevende wachtwoordloze beveiligingsstandaard, zodat u er zeker van kunt zijn dat uw aanmelding veilig en gemakkelijk is!



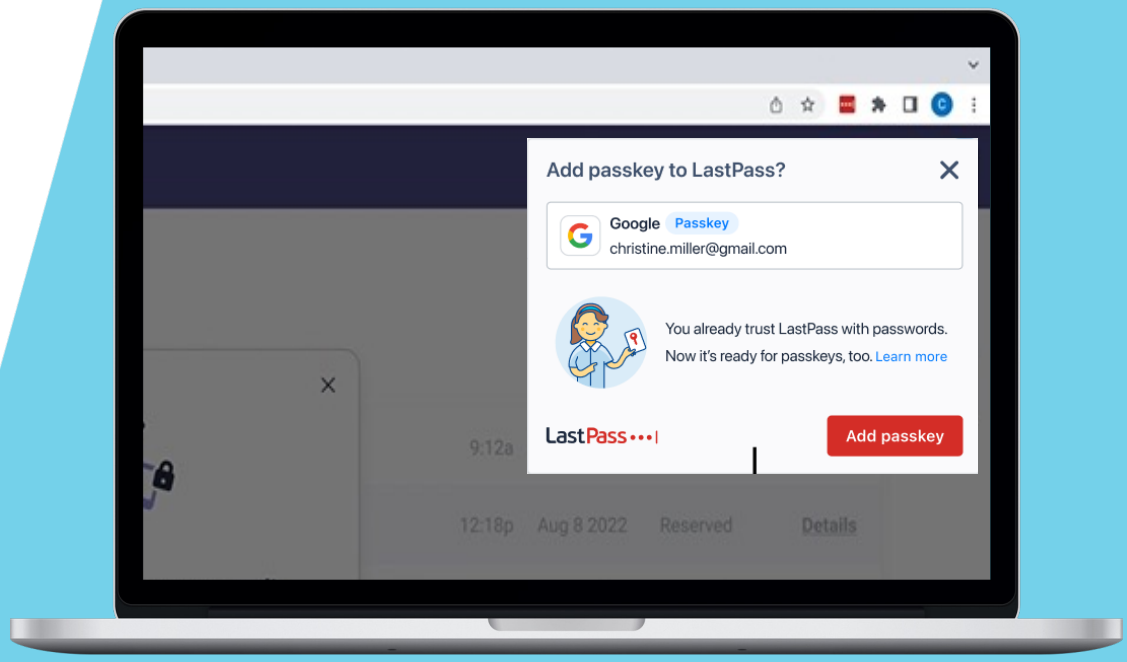
LastPass

Ondersteuning van Passkeys

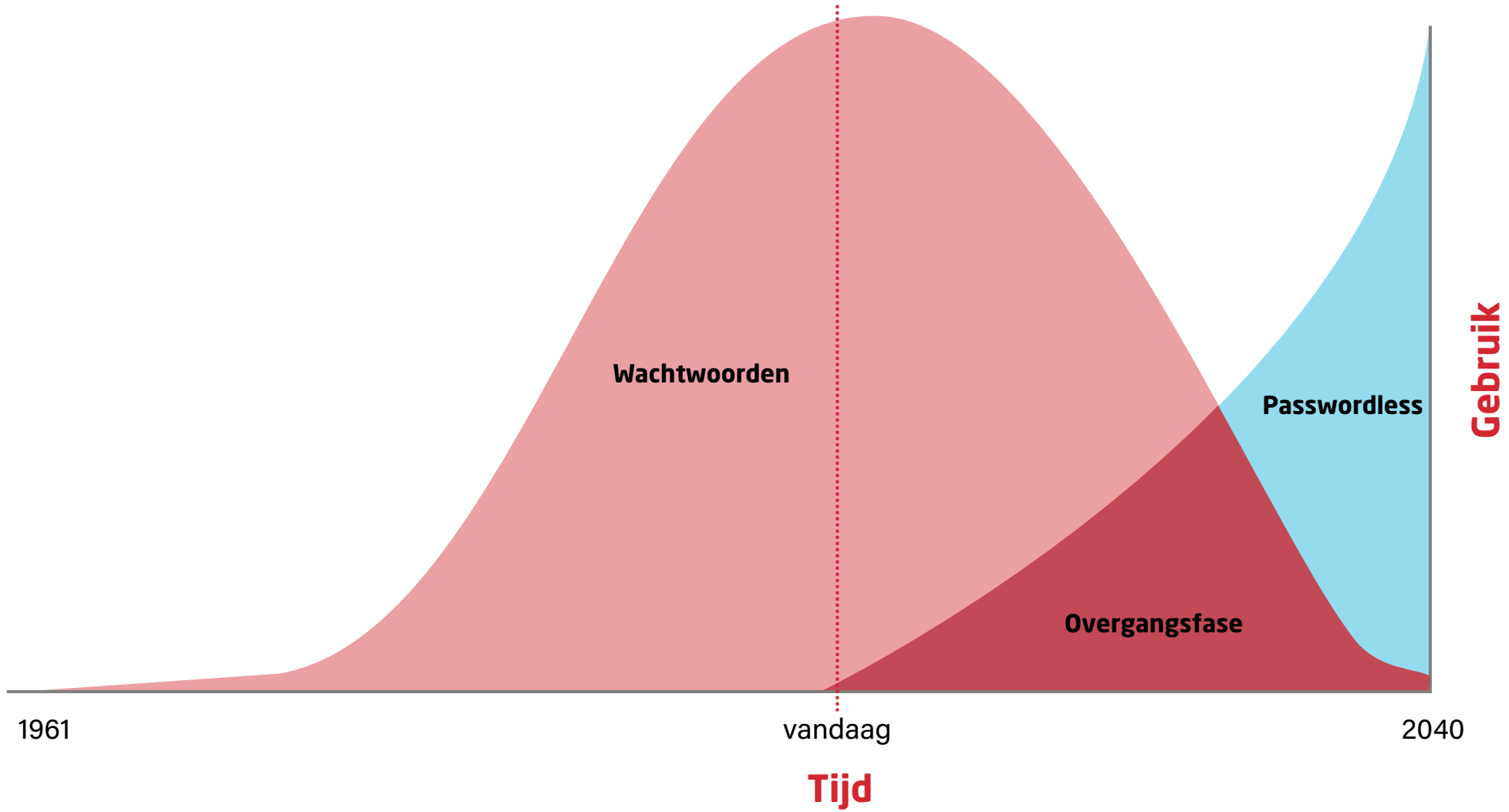
DE REIS NAAR EEN WACHTWOORDLOZE TOEKOMST GAAT VERDER

Gebruikers kunnen passkeys maken, opslaan, beheren en delen zoals ze dat doen met wachtwoorden, inclusief automatisch aanvullen van gebruikersnaam/e-mailadres en automatisch inloggen op sites die wachtwoordsleutels ondersteunen - rechtstreeks binnen de LastPass-browserextensie.

In tegenstelling tot passkey-beheer binnen een ecosysteem zoals Apple of Google, biedt LastPass toegang tot passkeys, ongeacht het apparaat, de browser of het besturingssysteem.



Wachtwoord(r)evolutie



LastPass

Waarom LastPass voor Passkeys?

Centrale toegang tot alle wachtwoorden en passkeys

Overal beschikbaar op alle platforms

Meer controle via beleidsregels

Gedetailleerd inzicht in de rapporten

One ~~Ring~~ Tool to rule them all!

LastPass

Veiligheid

LastPass

Beveiliging Architectuur

Zero-Knowledge-model om uw gegevens geheim te houden, zelfs voor ons.

Beveiligingsmaatregelen op topniveau

LastPass maakt gebruik van AES-256 gegevensversleuteling, samen met PBKDF2 hashing en SHA-256 salting.

Privacy by design

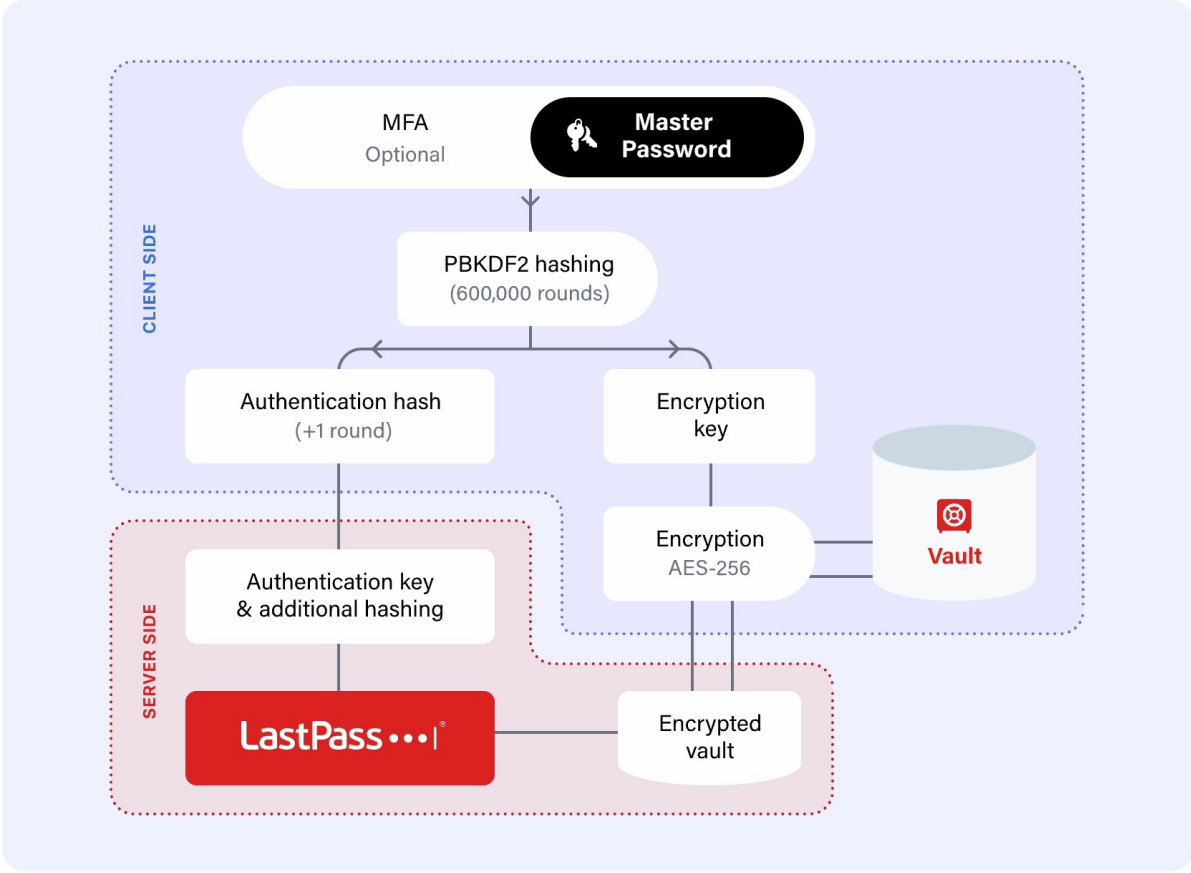
LastPass handhaaft een wereldwijde gegevensprivacy programma dat is ontworpen om de gegevens te beschermen van klanten, gebruikers en eindgebruikers.

Regelmatige beveiligingsaudits

LastPass maakt gebruik van vertrouwde, wereldwijde beveiligingsorganisaties om regelmatige controles en testen van de LastPass-service en infrastructuur uit te voeren.

Bug bounty programma

LastPass futureprooft zijn beveiligingsmaatregelen door ondersteuning van een bug bounty-programma waarbij white-hat hackers gevonden bugs en kwetsbaarheden kunnen indienen.



LastPass

Hebben jullie vragen?

SOC 2 Typ II 2023

SOC 3 2023

BSI C5 2023

ISO 27001 2023

LastPass

Samenvatting

Passwort Management is meer dan relevant!
Het is de basis van elke beveiligingsstrategie

Organisaties moeten wachtwoordloos worden!
Om uw klanten toekomstbestendig en veilig te maken

LastPass is de perfecte partner!
Met een compleet wall-to-wall aanbod, professioneel, gebruiksvriendelijk en veilig platform

LastPass ••• | APS IT diensten

Hartelijk Bedankt!