LastPass •••|

LÖSUNGSÜBERSICHT

Der einfache Weg zu mehr Sicherheit für Ihr Unternehmen

LastPass Business: Passwortverwaltung mit Multifaktor-Authentifizierung (MFA) der nächsten Generation

80 Prozent aller Sicherheitsverletzungen sind auf schlechte Passwörter zurückzuführen.[1] Passwörter alleine reichen also für den Schutz Ihres Unternehmens nicht aus. Wie aber können Sie Ihre Geschäftsdaten und -ressourcen absichern, ohne den Benutzern den Zugriff zu erschweren? Mitarbeitern ist die Bedeutung der Sicherheit bewusst. Dennoch wünschen sie sich schnelle, praktische und einfach funktionierende Technologien. Unternehmen stehen daher vor einer größeren Herausforderung denn je: Sie müssen Passwörter absichern und die Authentifizierung in heterogenen Umgebungen verwalten, ohne die Endbenutzer bei der Arbeit zu stören.

LastPass bietet Ihren Mitarbeitern ein reibungsloses Nutzungserlebnis und gibt der IT-Abteilung mehr Kontrolle und Transparenz – mit einer verwaltungs- und benutzerfreundlichen Lösung für Passwortverwaltung nebst MFA. Dank der Kombination aus beidem können Unternehmen alle Webanmeldungen absichern; die Möglichkeit zur Sperrung einzelner Zugriffspunkte bringt zusätzliche Sicherheit für das Unternehmensnetzwerk.

LastPass Business

LastPass Business bietet eine Passwortverwaltung, mit der Mitarbeiter Zugangsdaten anlegen, absichern und nahtlos freigeben können. Die Lösung gibt Administratoren Einblick und Kontrolle und sorgt durch das Zero-Knowledge-Prinzip von LastPass für Sicherheit.

LastPass-Multifaktor-Authentifizierung der nächsten Generation

Die Multifaktor-Authentifizierung von LastPass schützt jeden Zugriffspunkt in Ihrem Unternehmen. Cloud-Apps oder ältere Apps, VPN oder Workstations: LastPass MFA versieht Ihre Endpunkte mit einer weiteren Schutzebene und sorgt so für maximale Sicherheit.

Passwortverwaltung und Multifaktor-Authentifizierung

Umfangreiche Sicherheitskontrollen

Flexible Integrationen

Einfache Benutzerverwaltung und Berichterstattung

Reibungsloses Nutzungserlebnis

Eine höhere Sicherheit sollte der Produktivität Ihrer Mitarbeiter nicht im Weg stehen. Erleichtern Sie ihnen das Leben – durch Zugriff und Authentifizierung für alle Anwendungen über einen Anbieter. Mit LastPass können Mitarbeiter im Nu auf alle bei der Arbeit benötigten Websites und Tools zugreifen und jeden Zugriff darüber hinaus durch Multifaktor-Authentifizierung schützen.

Bequeme Passwortfreigabe

Sichere, flexible und rückverfolgbare Freigabe von Zugangsdaten innerhalb von Teams mit besonders intensiver Zusammenarbeit. Durch Nutzung generierter Passwörter und Aufhebung von Zugriffsrechten in Echtzeit sorgt LastPass außerdem dafür, dass ehemalige Mitarbeiter keine Firmendaten mitnehmen, wenn sie das Unternehmen verlassen.

Flexible und präzise Steuerungsmöglichkeiten

Schützen Sie Ihr Unternehmen mit einer Vielzahl von Richtlinien für die Passwortverwaltung und Multifaktor-Authentifizierung, die den Benutzerzugriff auf Einzel-, Gruppen- und Unternehmensebene regeln. Die Richtlinien lassen sich detailgenau konfigurieren, falls eine App etwa nur von bestimmten Orten aus oder zu bestimmten Zeiten zugänglich sein soll.

Passwortfreier Zugriff

Passwörter sorgen oft für Ärger und bergen Risiken. Mit LastPass erleichtern Unternehmen ihren Mitarbeitern die Passwortverwaltung. Die Passwortverwaltung erfasst und speichert alle Webanmeldungen, und MFA ersetzt Passwörter, wo immer möglich, durch eine passwortfreie Authentifizierung. Gemeinsam sorgen Passwortverwaltung und MFA für mehr Sicherheit und verbessern durch den einfacheren Umgang mit Passwörtern die Produktivität der Mitarbeiter.

Biometrische und kontextbezogene Daten

Durch eine Kombination aus biometrischen und kontextuellen Informationen weist LastPass MFA die Identität eines Benutzers anhand mehrerer Faktoren nach, und zwar ohne komplizierten Anmeldevorgang. Benutzer bestätigen ihre Identität mit biometrischen Faktoren wie Fingerabdruck oder Face-ID. Darüber hinaus verifiziert sie die Lösung hinter den Kulissen anhand von Kontextfaktoren wie Standort oder IP-Adresse, ohne dass hierfür ein Passwort eingeben muss.

Sofort einsatzbereite Integrationen

Mit Hilfe skalierbarer, automatisierter Integrationen in Benutzerverzeichnisse erleichtert Ihnen LastPass das On- und Offboarding von Benutzern. Zu unseren nahtlosen Integrationen zählen Microsoft Active Directory, Microsoft Azure AD, OneLogin, Okta, Google Workspace, PingOne und PingFederate.

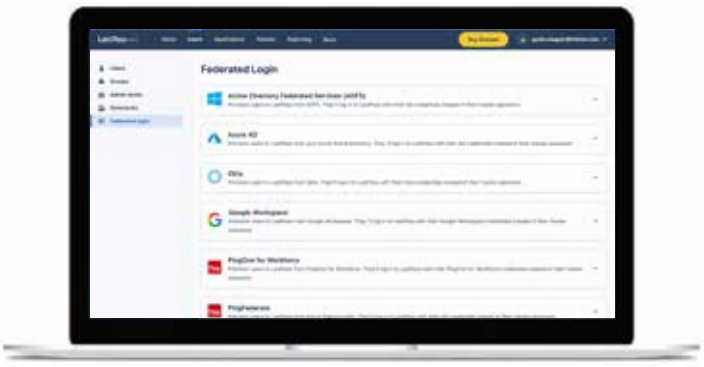
Außerdem integriert sich LastPass in SIEM-Lösungen (Sicherheitsinformations- und Ereignismanagement) und gibt Ihnen so über ausgefeilte Berichts- und Warnfunktionen besseren Einblick in Ihr Unternehmensnetzwerk. LastPass Business integriert sich in Splunk und Azure Sentinel; weitere Integrationen werden folgen.

Mehr Einblick durch Darkweb-Überwachung

Unerkannte Datenschutzverletzungen sind jetzt kein Thema mehr. LastPass schützt die Konten Ihrer Mitarbeiter durch kontinuierliche Darkweb-Überwachung. Sind die Daten eines Mitarbeiters von verdächtigen Aktivitäten betroffen, erhält er Nachricht dazu.

Integrierte Sicherheit

LastPass ist auf den Schutz und die Vertraulichkeit Ihrer Daten ausgelegt. Sämtliche Benutzerdaten werden auf Geräteebene ver- und entschlüsselt, was bedeutet, dass nicht einmal wir das Master-Passwort – und die in LastPass gespeicherten vertraulichen Daten – kennen. Zusätzlich werden die biometrischen Daten auf Geräteebene verschlüsselt und verlassen das Gerät des Benutzers nie.



Folgende Funktionen bieten Ihrem Unternehmen optimale Kontrolle und Ihren Benutzern den Komfort, den sie erwarten:

Zentrales Dashboard für Administratoren	Das Admin-Dashboard umfasst die automatisierte Benutzerverwaltung, Richtlinien, Diagnose-Dashboards und vieles mehr.
Universelle Passwortverwaltung	LastPass vereinfacht den Zugriff auf alle Anwendungen und kann Zugangsdaten automatisch für die Benutzer erfassen, speichern und eingeben.
Benutzerintegrationen	Automatisieren Sie das On- und Offboarding, die Gruppenverwaltung, die Verbundanmeldung und mehr mit Active Directory, Azure AD, Okta, OneLogin, Google Workspace, PingOne, PingFederate oder einer eigens entwickelten API.
Mehr als 100 Sicherheitsrichtlinien	Diese Richtlinien helfen Ihnen, Best Practices in dem ganzen Unternehmen umzusetzen und Einfluss auf das Passwortverhalten der Mitarbeiter zu nehmen.
Detaillierte Sicherheitsberichte	Mit Hilfe der automatisierten und detaillierten Berichte lassen sich Aktionen mit einzelnen Benutzern in Zusammenhang bringen, was Ihrem Unternehmen die Einhaltung von Vorschriften erleichtert. SIEM-Integrationen für Splunk und Azure Sentinel liefern Ihnen aufschlussreiche Insights.
Sichere Freigabe von Passwörtern	Dank LastPass können Ihre Teams Apps flexibel, sicher und ohne Einbußen bei der Rechenschaftspflicht oder Sicherheit gemeinsam nutzen.
Darkweb-Überwachung	LastPass schützt die Konten Ihrer Mitarbeiter durch kontinuierliche Darkweb-Überwachung. Sind die Daten eines Mitarbeiters von verdächtigen Aktivitäten betroffen, erhält er Nachricht dazu.
Multifaktor-Authentifizierung der nächsten Generation	Zugriff auf LastPass Authenticator, das Cloud-Apps, ältere Apps, VPNs und Workstations mit passwortfreiem Zugriff versieht. Detailgenaue Richtlinien für Geofencing, Zugriffszeiten und IP-Adressen geben Administratoren Kontrolle und sorgen für noch mehr Sicherheit.
Single Sign-On	Geben Sie Mitarbeitern Zugriff auf wichtige Arbeitstools durch einen einfacheren Zugriff auf bis zu drei Cloud-Anwendungen.
Families as a Benefit	Jeder Mitarbeiter erhält ein privates LastPass-Konto sowie fünf zusätzliche Lizenzen für Familienmitglieder oder Freunde. Passwörter sind so dank LastPass immer geschützt.

Weitere Möglichkeiten:

Erweitertes Single Sign-On mit LastPass	LastPass-Single-Sign-On gibt Mitarbeitern komfortablen Zugriff auf eine unbegrenzte Anzahl Cloud-Anwendungen und erleichtert der IT deren Bereitstellung – in derselben Lösung, die auch zum Speichern von Passwörtern verwendet wird. Mit Single Sign-On für die wichtigsten Anwendungen und einem Passwort-Manager, der alles andere erfasst und schützt, bietet Ihnen LastPass umfassenden Schutz für jeden Zugriffspunkt – und Ihren Mitarbeitern bequemen Zugriff auf ihre Arbeit.

Quellen:

1 Verizon, Data Breach Investigations Report (DBIR), 2020.