LastPass ••• | MFA

Lösungsübersicht

LastPass MFA ist eine intelligentere Art der Authentifizierung.

Immer mehr Unternehmen steigen auf Cloud-Lösungen um, und immer mehr Mitarbeiter bringen eigene Hard- und/oder Software an den Arbeitsplatz mit – kein Wunder also, dass sich auch Authentifizierungslösungen rasant weiterentwickeln. Auch wenn den Mitarbeitern die Bedeutung der Sicherheit bewusst ist, wünschen sie sich dennoch schnelle, praktische und einfach funktionierende Technologien. Die verminderte Transparenz und die höhere Komplexität stellen IT-Teams vor größere Herausforderungen denn je: Sie müssen die Authentifizierung in heterogenen Umgebungen verwalten, ohne die Endbenutzer bei der Arbeit zu stören.

Angesichts dessen, dass 81 Prozent aller Sicherheitsverletzungen auf schlechte Passwörter zurückzuführen sind, liegt es auf der Hand, dass Passwörter alleine für den Schutz Ihres Unternehmens nicht ausreichen. Wie können Sie Ihre wichtigen Informationen schützen, ohne den Benutzern den Zugriff zu erschweren? Die Zwei-Faktor-Authentifizierung (2FA) ist ein guter Anfang; eine Universallösung für die Authentifizierung funktioniert jedoch bei Benutzern mit unterschiedlichen Verhaltensweisen, persönlichen Geräten, Zugriffsebenen und Eigenschaften nicht.

LastPass MFA schützt Ihr Unternehmen mit den derzeit führenden Technologien, während es Ihren Mitarbeitern den Anmeldevorgang erleichtert. Es geht über die standardmäßige Zwei-Faktor-Authentifizierung hinaus: LastPass MFA stellt sicher, dass die richtigen Benutzer zur richtigen Zeit auf die richtigen Daten zugreifen können – ohne zusätzliche Komplexität. Mit seinem einzigartigen Modell, das auf integrierter Sicherheit beruht, sorgt LastPass MFA dafür, dass biometrische Daten vertraulich und sicher bleiben. Für die Identifizierung und Authentifizierung der Benutzer werden sowohl menschliche als auch versteckte Faktoren herangezogen. LastPass MFA macht die Multifaktor-Authentifizierung intuitiv. Für Administratoren ist es einfach bereitzustellen, während es für Benutzer einfach zu verwenden ist.

Adaptive Authentifizierung, die sich an die Benutzer anpasst

Indem LastPass MFA biometrische und kontextuelle Informationen kombiniert, weist es die Identität eines Benutzers anhand mehrerer Faktoren nach – ohne den Anmeldevorgang zu verkomplizieren. Benutzer bestätigen ihre Identität mit menschlichen Faktoren wie Gesicht, Fingerabdruck, Stimme oder Iris. Darüber hinaus verifiziert sie das Gerät hinter den Kulissen anhand versteckter Faktoren wie Standort oder IP-Adresse – ohne dass der Benutzer ein Passwort eingeben muss.

Passwortloser Zugriff

Passwörter sorgen oft für Ärger und bergen Risiken. Mit Hilfe biometrischer Identifikatoren und der adaptiven Authentifizierung macht LastPass MFA Schluss damit. Der passwortlose Zugriff macht beruflich genutzte Anwendungen bequem zugänglich und steigert so die Produktivität Ihrer Mitarbeiter.

Einfache Bereitstellung für IT-Teams

LastPass MFA lässt sich schnell und einfach bereitstellen, ohne dass zusätzliche Schulungen oder Dienstleistungen erforderlich sind. Es sorgt im Handumdrehen für Sicherheit, während Sie durch weniger Passwortzurücksetzungen und Zugriffsprobleme Zeit und Ressourcen sparen.

Sicherheitsmodell nach dem Zero-Knowledge-Prinzip

Adaptive Authentifizierung

Einfache Bereitstellung und Verwaltung

Umfangreiche Sicherheitskontrollen

Reibungsloses Nutzungserlebnis

Eine höhere Sicherheit sollte der Produktivität Ihrer Mitarbeiter nicht im Weg stehen. LastPass MFA schützt jeden einzelnen Zugriffspunkt – ob ältere, Cloud-, mobile oder vor Ort installierte Anwendungen. Benutzer werden nahtlos auf allen Geräten authentifiziert, sodass Ihr IT-Team die gewünschten Authentifizierungsmethoden frei wählen kann – von SMS über Push-Benachrichtigungen bis zur adaptiven Authentifizierung. Dies bietet Ihnen für alle Anwendungsfälle maximale Flexibilität.

Präzise Steuerung von einem Ort aus

Schützen Sie Ihr Unternehmen mit einer Vielzahl von Richtlinien, 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. Die gesamte Verwaltung erfolgt über ein benutzerfreundliches Admin-Dashboard.

Sofort einsatzbereite Integrationen

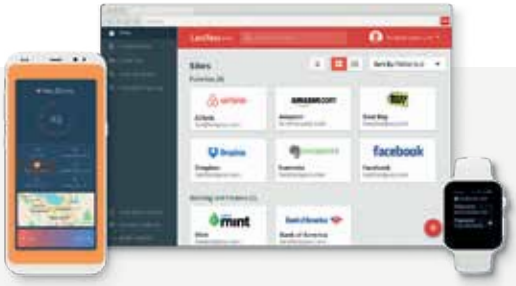
Automatisieren Sie die Benutzerbereitstellung, indem Sie LastPass in Benutzerverzeichnisse wie Active Directory, Azure AD, Okta und OneLogin integrieren. Durch die einfache Einrichtung und den minimalen täglichen Verwaltungsaufwand wächst LastPass MFA mit Ihrem Unternehmen mit.

Eine Komplettlösung für die Authentifizierung

LastPass MFA ist mit Cloud-, mobilen sowie älteren und lokal installierten Apps kompatibel, sodass Sie die Authentifizierung für jede wichtige Unternehmensanwendung zentral verwalten können. Über eine einzige Plattform erhält Ihr IT-Team Einblick in jeden Login.

Integrierte Sicherheit

LastPass MFA ist auf den Schutz und die Vertraulichkeit Ihrer Daten ausgelegt. Die biometrischen Daten werden auf Geräteebene verschlüsselt und verlassen das Gerät des Benutzers nie. Und da sie nicht an einem zentralen und möglicherweise gefährdeten Ort gespeichert werden, sind sie vor serverseitigen Angriffen geschützt.



Besuchen Sie www.lastpass.com/multifactor-authentication, um mehr zu erfahren.

05.28.2019/LMI06385b/PDF