So finden Sie den richtigen Passwort-Manager für Ihr Unternehmen

Ein Leitfaden zur Evaluierung und zum Vergleich verschiedener Optionen

Ihre IT-Abteilung und Ihre Mitarbeiter haben wahrscheinlich unterschiedliche Vorstellungen, was die Passwortsicherheit betrifft. Bei 85 Prozent der Datenschutzverletzungen spielt der Faktor Mensch eine Rolle (Phishing, gestohlene Zugangsdaten, Nutzerfehler). Die Passwortgewohnheiten der Mitarbeiter sind die größte Sicherheitslücke für Unternehmen. Sensible Firmendaten können großen Risiken ausgesetzt sein.[1]

Das ortsungebundene Arbeiten nimmt zu. Unternehmen müssen es ihren Mitarbeitern ermöglichen und dabei gleichzeitig für ihre Sicherheit sorgen.

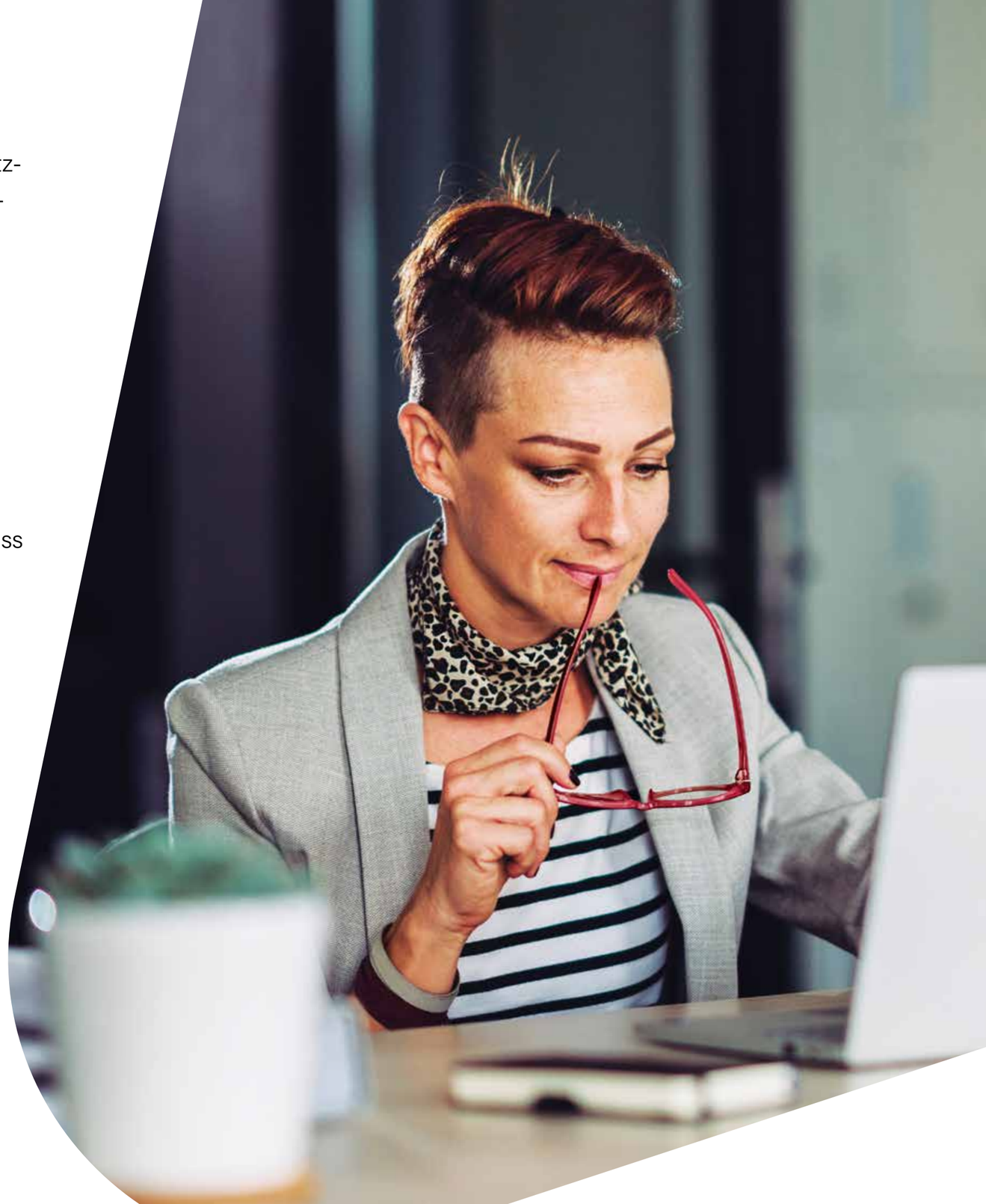
Es geht allerdings nicht nur um die Sicherheit. Passwörter erzeugen häufig Frust und schmälern die Effizienz und Produktivität.

Ein Passwort-Manager ermöglicht Mitarbeitern ein komfortables Arbeiten, ohne dass das Unternehmen Einbußen bei der Sicherheit oder Kontrolle hinnehmen muss. Beim Schutz des Unternehmens vor Datendiebstahl ist er eine tragende Säule.

In diesem Leitfaden besprechen wir:

- **Was ein Passwort-Manager ist**
- **Warum Ihr Unternehmen einen Passwort-Manager braucht**
- **Kriterien für die Evaluierung von Lösungen**
- **Best Practices bei der Implementierung eines Passwort-Managers**
- **Herausforderungen im Zusammenhang mit Passwörtern und wie ein Passwort-Manager sie bewältigt**
- **Single Sign-On (SSO) und Multifaktor-Authentifizierung (MFA) als Ergänzungen eines Passwort-Managers**

1 2021 Verizon DBIR



Was ist ein Passwort-Manager und warum ist er wichtig?

Ein Passwort-Manager ist eine Software, mit der ein Benutzer seine Passwörter speichern, verwalten und sicher verwahren kann. Er muss sich dabei nur ein einziges (idealerweise starkes) Master-Passwort merken, das ihm Zugriff auf einen Vault mit seinen restlichen Passwörtern gewährt.

Passwörter und andere sensible Daten, die im Passwort-Manager gespeichert werden, sind in der Regel verschlüsselt. Damit kann nur der Benutzer selbst auf seine Zugangsdaten zugreifen. Ein integrierter Passwortgenerator erstellt für jedes Konto ein zufälliges Passwort. Weitere Funktionen helfen dem Benutzer, seine Online-Sicherheit zu verbessern und seine persönlichen Daten optimal zu schützen.

Berichtsfunktionen geben IT-Administratoren globalen und detailgenauen Einblick in die Stärke der verwendeten Passwörter und in Anmeldeaktivitäten. Durch den Einblick in die Passwort-gewohnheiten seines Personals kann das Unternehmen gezielt die Sicherheit der einzelnen Zugangsdaten verbessern und Mitarbeitern durch die Vergabe und Verwaltung von Zugriffsrechten die Zusammenarbeit erleichtern.

Eine sichere Verwaltung, Freigabe und Nutzung von Passwörtern mindert das Risiko von Passwort-diebstählen enorm. Verschaffen sich Kriminelle Zugang zu den Netzwerken, Servern, On-Premise- oder Cloud-Anwendungen eines Unternehmens, um dort wertvolle Geschäftsdaten zu stehlen, so geschieht dies sehr häufig über gestohlene Zugangsdaten.

Warum Sie einen Passwort-Manager verwenden sollten

Wir alle müssen unzählige Passwörter wissen und verwalten – bei der Arbeit und auch privat. Das Ergebnis? Wir erstellen Passwörter, die wir uns einfach merken können, oder notieren sie uns irgendwo.

Ein paar Zahlen dazu:

- **66 % der Benutzer nutzen überall ein und dasselbe Passwort. Da ist die Frage weniger, ob solche Zugangsdaten gestohlen werden, sondern eher, wann.**[2]
- **Gut die Hälfte der in kleinen (52 %) und großen (64 %) Unternehmen gestohlenen Daten sind Zugangsdaten.**[3]
- **Im Darkweb zirkulieren 15 Milliarden gestohlene Zugangsdaten. Die Absicherung von Mitarbeiterzugangsdaten ist daher eine dringliche Aufgabe für IT-Verantwortliche.**[4]
- **Bei 85 % der Datenschutzverletzungen spielt der Faktor Mensch eine Rolle. Wir sind soziale Wesen, die zuweilen gedankenlos oder fehlerhaft handeln. Das begünstigt Phishing und den Diebstahl von Zugangsdaten.**[5]

Ein Passwort-Manager automatisiert manuelle Passwortvorgänge: das Anlegen, Verwalten, Eingeben, Zuweisen, Freigeben und Aufheben von Passwörtern. Damit müssen sich Mitarbeiter um das Memorieren und Erstellen der ganzen Passwörter keine Gedanken mehr machen. Die IT-Abteilung wiederum muss weniger Passwörter zurücksetzen und gewinnt Zeit für wertschöpfende Arbeit. Und das Unternehmen selbst stiftet Vertrauen in seine Bestrebungen, Hackern weniger Angriffsflächen zu bieten und Datenschutzverletzungen zu verhindern.

2 Psychologie der Passwörter, 2020
3 2020 Verizon DBIR
4 Digital Shadows: „From Exposure to Takeover", 2020
5 2021 Verizon DBIR

Was ein Passwort-Manager können sollte

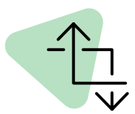
Ein guter Passwort-Manager hilft Ihnen bei der Bewältigung der folgenden Aufgaben:

1. Alle Passwörter verschlüsseln

Passwörter müssen sicher und für andere uneinsehbar aufbewahrt werden – an einem Ort, für den Sicherheits-Best-Practices gelten und auf den nur Befugte Zugriff haben.

2. Passwörter ausscheidender Mitarbeiter deaktivieren

Mitarbeitern oder externen Geschäftspartnern sollten Sie nach ihrem Ausscheiden oder dem Ende der Zusammenarbeit Passwörter entziehen können. Auditing- und Benutzerverwaltungsfunktionen geben IT-Administratoren die Möglichkeit, Zugriffsrechte zu ändern und Passwörter jederzeit auszuwechseln.

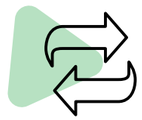


3. Wiederverwendung von Passwörtern eindämmen

IT-Administratoren benötigen Einblick in die im Unternehmen herrschenden Passwortgepflogenheiten. So erkennen sie, welche Mitarbeiter ein riskantes Passwortverhalten zeigen, und können diesen sicherere Verhaltensweisen nahelegen.

4. Den Zugriff auf Konten ohne Weitergabe von Passwörtern freigeben

Ein guter Passwort-Manager gestattet Ihnen die sichere Freigabe verschlüsselter Zugangsdaten und lässt Sie genau nachverfolgen, ob Zugangsdaten intern oder mit externen Geschäftspartnern und Kunden geteilt wurden.



5. Alle Benutzer zu Änderungen benachrichtigen

Der Austausch eines Passworts sollte Arbeitsteams nicht ausbremsen. Mit einem Passwort-Manager können Sie Passwörter stillschweigend und auf sichere Weise rotieren.

6. Einblick in die Schatten-IT nehmen

Erfassen Sie alle Zugangsdaten im Unternehmen und überblicken Sie, welche versteckten Anwendungen Mitarbeiter nutzen. Messen Sie die Auswirkung der Schatten-IT auf das Unternehmen und ergreifen Sie ggf. Maßnahmen zur Eindämmung der damit verbundenen Risiken.

7. Die Nutzung von Zugangsdaten rückverfolgen

Nutzen Sie detaillierte Ereignisprotokolle als Auditing-Instrument für den Aufbau der unternehmensweiten Compliance. Auch bei freigegebenen Zugangsdaten können Sie einzelne Aktionen bestimmten Benutzern zuweisen und so die Kontrolle wahren.

8. Benutzer warnen, wenn Zugangsdaten kompromittiert sind

Die Darkweb-Überwachung prüft kontinuierlich, ob Ihre E-Mail-Adressen in einer Datenbank gehackter Zugangsdaten auftauchen, und benachrichtigt Sie in diesem Fall.

Kriterien für die Evaluierung von Passwort-Managern

Sie sind zu dem Schluss gekommen, dass Ihr Unternehmen von einem Passwort-Manager profitieren würde. Was nun?

Sie müssen die richtige Lösung finden – und dazu müssen Sie sich über Ihre geschäftlichen Bedürfnisse und Ihre Erwartungen an einen Passwort-Manager im Klaren sein. Sodann suchen Sie nach der Lösung, die diese Bedürfnisse und Erwartungen am besten erfüllt.

Wichtigste Aspekte bei Ihrem Vergleich von Lösungen:

- **Ein reibungsloses Nutzungserlebnis:** Wie benutzerfreundlich ist die Lösung? Erleichtert sie den Mitarbeitern den Umgang mit Passwörtern?
- **Fokus auf die Sicherheit:** Ist der Passwort-Manager sicher und zuverlässig und hilft er Ihnen, Ihre Sicherheitsziele zu erreichen?
- **Eine zentralisierte Verwaltung:** Was erfordert die Implementierung von Ihnen und wie vereinfacht die Lösung das Management laufender Aufgaben?
- **Anpassbare, präzise und aktionsorientierte Steuerungsmöglichkeiten:** Bietet der Passwort-Manager Ihren Administratoren das richtige Maß an Kontrolle und Transparenz? Wie einfach können sie Maßnahmen zum Schließen von Sicherheitslücken ergreifen?
- **Ein Konto für den Schutz aller Daten:** Privat- und Berufsleben verschmelzen immer stärker. Können Mitarbeiter mit dem Passwort-Manager alle ihre digitalen Lebensbereiche absichern?

Ein reibungsloses Nutzungserlebnis

Die Passwortverwaltung kann ihre Wirkung nur dann entfalten, wenn sie von den Mitarbeitern genutzt wird. Ihr IT-Team kann von einer Lösung noch so begeistert sein – etwa weil sie gute Administrations- und Backend-Funktionen bietet –, wenn die Software bei den Mitarbeitern nicht ankommt, lohnt sich ihre Einführung nicht.

Folgendes sollte die Lösung bieten:

- Geringer Konfigurationsaufwand für die Benutzer
- Automatische Eingabe von Passwörtern im Browser
- Automatische Erfassung (neuer und vorhandener) Zugangsdaten, sobald sie genutzt werden
- Sichere und einfache Weitergabe von Passwörtern
- Automatische Synchronisation für den geräte-übergreifenden Zugriff
- Automatische Aktualisierung freigegebener Zugangsdaten
- Kompatibilität mit allen webbasierten Logins (nicht nur wenigen Cloud-Apps)
- Verschlüsselung und sichere Speicherung von Passwörtern und sonstigen sensiblen Daten
- Schutz für private und berufliche Konten
- Website für den Self-Service-Support

Wichtige Fragen:

- Wie einfach und intuitiv ist das Tool?
- Wird es die Mitarbeiter ansprechen?
- Nimmt es seinen Benutzern Arbeit ab?
- Können Mitarbeiter Passwörter freigeben und sind diese immer sichtbar?
- Was müssen Benutzer für eine Passwortfreigabe tun? Wie verwalten sie die freigegebenen Elemente?
- Erfasst die Lösung alle von Mitarbeitern genutzten Passwörter und Daten?

Empfohlene Maßnahmen:

- **Selbst ausprobieren:** Die meisten Passwort-Manager bieten eine kostenlose Version an, die von einer kleinen Benutzergruppe getestet werden kann. Wie eine Lösung funktioniert, erkennen Sie am besten, wenn Sie sich selbst damit befassen. Ein Proof of Concept mit einer bestimmten Benutzergruppe gibt Ihnen Aufschluss über die Funktionsweise der Lösung und wie intuitiv sie für neue Benutzer ist.
- **Bestandsaufnahme der verwendeten Geräte machen:** Sie wissen nicht, welche Geräte Ihre Mitarbeiter nutzen und ob es sich dabei um persönliche oder Unternehmensgeräte handelt? Dann machen Sie jetzt eine Bestandsaufnahme. Stellen Sie dann sicher, dass Ihr neuer Passwort-Manager mit diesem Gerätebestand kompatibel ist.
- **Auf Erfahrungen anderer Kunden achten:** Zahlen sprechen Klartext: Je mehr zufriedene Nutzer, desto besser. Fallstudien, Kunden-stimmen, Bewertungen in den App Stores und Testberichte von Technikexperten sind gute Anhaltspunkte dafür, ob ein Passwort-Manager die an ihn gestellten Erwartungen erfüllt.

Fokus auf die Sicherheit

In puncto Sicherheit sind bei Passwort-Managern zwei Fragen relevant: 1. Ist die Lösung selbst sicher und zuverlässig? 2. Unterstützt die Lösung Sie dabei, Ihre Sicherheitsziele zu erreichen? Ein Passwort-Manager soll das Risiko einer Datenschutzverletzung mindern und Ihr Unternehmen absichern. Welche Lösung Sie auch wählen, sie muss selbst adäquat sicher sein und Ihnen Funktionen bieten, mit denen Sie in Ihrem Unternehmen strengere Passwortrichtlinien durchsetzen können.

Folgendes sollte die Lösung bieten:

- Rein lokale Verschlüsselung (d. h. weder das Master-Passwort noch der Verschlüsselungsschlüssel sind dem Dienstanbieter bekannt)
- Führende Verschlüsselungsalgorithmen
- Best Practices zum Schutz übertragener und gespeicherter Daten
- Ein großes Portfolio an Richtlinien und feingradigen Steuermöglichkeiten für Administratoren
- Zugriff auf Daten in verschiedenen Online- und Offline-Situationen
- Integration von Multifaktor-Authentifizierung für ergänzende Sicherheit
- Aufzeigen von Sicherheitslücken oder Sicherheitsvorfällen; erwiesene Reaktionsbereitschaft und Transparenz
- Darkweb-Überwachung zum aktiven Schutz von Online-Konten

Wichtige Fragen:

- Welche Verschlüsselungsalgorithmen kommen zum Einsatz?
- Wie werden die Daten lokal und serverseitig geschützt?
- Unter welchen Umständen (falls überhaupt) erhält der Dienstanbieter das Master-Passwort oder den Verschlüsselungsschlüssel?
- Welche Richtlinien und Sicherheitseinstellungen sind verfügbar?
- Können Richtlinien auf globaler, Gruppen- und Benutzerebene angewendet werden?
- Welche Arten der Multifaktor-Authentifizierung werden angeboten und kostet diese Funktion extra?

Empfohlene Maßnahmen:

- **Interne Sicherheitsrichtlinien überprüfen:** Ihr Passwort-Manager sollte sich in Ihre bereits vorhandenen Richtlinien einfügen. Wenn in Ihrem Unternehmen Vorgaben zur Speicherung von Zugangsdaten in verschlüsseltem Format oder in einer bestimmten Region herrschen, sollte die gewählte Lösung diese einhalten können.
- **Technisches Whitepaper lesen:** Achten Sie auf die Art und Weise, wie die Daten und der Verschlüsselungsschlüssel geschützt werden (im Idealfall wird dieser Schlüssel nie an den Dienstleister übermittelt). Achten Sie auf eine redundante Auslegung der Lösung; sie beugt möglichen Ausfällen vor.
- **Liste aller Richtlinien und Steuerungsmöglichkeiten durchgehen:** Manche Passwort-Manager bieten nur ein Dutzend Richtlinien, andere dagegen hundert oder mehr. Die schiere Zahl alleine sagt nicht unbedingt etwas aus. Entscheidend ist, ob Sie mit den Richtlinien Ihre Ziele erreichen können. Ihr Passwort-Manager sollte eine detailgenaue Steuerung zulassen, sodass Sie die Anforderungen Ihres Unternehmens in Bezug auf den Kontozugriff, die Passwortgewohnheiten, die Nutzung von Funktionen und mehr umsetzen können.

Eine zentralisierte Verwaltung

Um die Passwortverwaltung für Ihr Unternehmen zu skalieren, brauchen Sie Funktionen, mit denen Sie wichtige Prozesse automatisieren können. Administratoren brauchen einen zentralen Ort, von dem aus sie den Dienst komfortabel bereitstellen und kontinuierlich pflegen können. Sie sollten außerdem Stakeholdern die positiven Effekte des Passwort-Managers sowie die allgemeinen Fortschritte des Unternehmens in puncto Passwortsicherheit aufzeigen können.

Folgendes sollte die Lösung bieten:

- Spezielle Administratorrechte für die Verwaltung und Absicherung der Installation
- Verzeichnisdienste zur Synchronisierung und Virtualisierung vorhandener Identitätsdaten
- Besonders wichtig für kleinere Unternehmen: ein Self-Service-Support, der Zeit- und Personalaufwand einspart
- Automatische Software-Updates, die wenig bis gar kein Eingreifen seitens der IT erfordern
- Möglichkeit, Lizenzen jederzeit aufzustocken, wenn Ihr Unternehmen personell wächst oder seine Strategie um weitere Sicherheitslösungen ergänzt
- Bereitstellungstools für ein einfacheres Identity-Lifecycle-Management: Identitätsdaten anlegen, weiterleiten, verwalten und deaktivieren
- Umfassenden Einblick in Ihr gesamtes Konto
- Zügige Installation

Wichtige Fragen:

- Welche Rollen gibt es? Welche Berechtigungen können Administratoren erhalten?
- Sind für die Installation der Lösung Spezialkenntnisse erforderlich? Gibt es dieses Know-how im Unternehmen oder muss es extern beschafft werden?
- Lässt sich die Benutzerverwaltung mittels Active Directory oder anderer Systeme automatisieren?
- Wie viele Administratoren werden unterstützt und welche Rechte haben sie?

Empfohlene Maßnahmen:

- **Dashboard für Administratoren erkunden:** Sehen Sie sich in Ihrer Test- und Proof-of-Concept-Phase vor allen Dingen das Administratoren-Dashboard genau an. Achten Sie darauf, ob die Lösung Folgendes bietet: eine Berichterstattung, die aussagekräftige Daten liefert, eine Benutzer- und Gruppenverwaltung, die Verwaltung gemeinsam genutzter Zugangsdaten, Richtlinien, Sicherheitsbewertungen und benutzerdefinierte Integrationen.
- **Active-Directory-Synchronisation nutzen:** Managt Ihr Unternehmen Prozesse und Dienste per Active Directory? Dann prüfen Sie diesbezüglich die Passwort-Manager, die Sie ins Auge fassen. Einige Lösungen bieten Verzeichnissynchronisation für eine automatisierte Benutzerverwaltung, die Zuweisung gemeinsam genutzter Zugangsdaten und Anwendung von Richtlinien.

Anpassbare, präzise und aktionsorientierte Steuerungsmöglichkeiten

Achten Sie beim Vergleich von Lösungen darauf, welchen Überblick und welche Steuermöglichkeiten sie Administratoren bieten. Die Lösung Ihrer Wahl muss mehr können, als Passwörter an einem Ort zu sammeln und Zugriff darauf zu gewähren – diesen Zweck erfüllt eine passwortgeschützte Excel-Tabelle ebenso, wenn auch etwas umständlicher. Ein guter Passwort-Manager erfasst auch Zugangsdaten. Er gibt Auskunft zur Sicherheit von Passwörtern und macht es sowohl dem Unternehmen als auch seinen Benutzern leicht, Sicherheitslücken zu schließen.

Folgendes sollte die Lösung bieten:

- Auf einen Blick verfügbare Informationen zu den Benutzern, ihren gespeicherten Websites und ihrem Passwortverhalten
- Trendberichte zum Passwortverhalten der Benutzer und noch bestehenden Sicherheitslücken
- Sicherheitsberichte, die Fortschritte aufzeigen bei den Bemühungen, die Wiederverwendung von Passwörtern einzudämmen
- Richtlinien und Einstellungen, die sich global, gruppen- und benutzerspezifisch anwenden lassen
- Freigabe von Zugangsdaten und Verfolgbarkeit von diesbezüglichen Aktionen individueller Benutzer
- Unternehmensweite Messung der Passwort-sicherheit
- Detaillierte Berichtsprotokolle für Audit- und Compliance-Zwecke
- Ein-Klick-Funktion zur Aufhebung von Passwörtern ausscheidender Mitarbeiter
- Sichere Kontowiederherstellung, wenn Mitarbeiter ausscheiden oder ihr Master-Passwort vergessen
- Einblick in die Schatten-IT

Wichtige Fragen:

- Kann der Zugriff auf Benutzer-, Gruppen- oder globaler Ebene beschränkt werden?
- Wie wird die Wiederverwendung von Passwörtern und anderen Sicherheitsindikatoren unternehmensweit gemessen?
- Welche Rollen mit welchen Zugriffsrechten sind verfügbar?
- Gibt es einen Audit-Pfad? Welche Details werden in den Berichten erfasst?
- Wie werden die Passwortgewohnheiten auf globaler und individueller Ebene gemessen?
- Wie werden Benutzerkonten ausscheidender Mitarbeiter deaktiviert oder entzogen?
- Wie werden Konten wiederhergestellt, falls ihre Benutzer das Master-Passwort vergessen haben?
- Können Reportingtools über die Schatten-IT im Unternehmen Aufschluss geben?

Empfohlene Maßnahmen:

- **Berichtsprotokolle überprüfen:** Achten Sie in Ihrer Testphase auf die Berichtsprotokolle, die der Passwort-Manager Administratoren zur Verfügung stellt. Welche Aktionen und Ereignisse erfassen die Berichte für Benutzer und Administratoren? Achten Sie darauf, wie detailliert die Daten sind und wie lange verfügbar.
- **Fragen zu verschiedenen Szenarien stellen:** Erkundigen Sie sich beim Anbieter, ob seine Lösung auf Benutzerebene Einblick in das Passwort-verhalten und die Zugriffsmuster geben kann. Ein guter Passwort-Manager zeigt gescheiterte Anmeldeversuche und die Aktionen von Benutzern und Administratoren an. Wichtig ist auch ein Überblick über Ihr Sicherheitsprofil, anhand dessen Sie konkrete Maßnahmen ergreifen können, um sich proaktiv vor Bedrohungen zu schützen.

Ein Konto für den Schutz aller Daten

Die Arbeits- und Privatsphäre verschmelzen immer stärker miteinander. Ihre Mitarbeiter sollten daher ihre Zugangsdaten für alle ihre Konten sicher verwahren können – besonders dann, wenn sie von ihren persönlichen Geräten auf Unternehmensressourcen wie E-Mail oder Kommunikationstools zugreifen. Das im Privaten praktizierte Passwortverhalten kann sich auf die Arbeitssphäre auswirken.

Folgendes sollte die Lösung bieten:

- Ein Passwort-Manager, mit dem Mitarbeiter – und idealerweise auch ihre Familienangehörigen – ihre privaten Zugangsdaten verwalten können
- Ein persönlicher Passwort-Manager, der die folgenden Funktionen bietet:
  - Erstellung, Speicherung und Verwaltung von Zugangsdaten
  - Freigabe von unbegrenzt vielen Ordnern
  - Passwortgenerator zum Erstellen starker, einmaliger Passwörter
  - Sicherheits-Dashboard, das die Stärke der Passwörter anzeigt
  - Darkweb-Überwachung, die den Benutzer zu kompromittierten Konten benachrichtigt

Wichtige Fragen:

- Gibt es den Passwort-Manager in einer Business-Version und als Verbraucherprodukt?
- Ist die Verbraucherlösung genauso leistungsfähig wie die Business-Version?
- Können Mitarbeiter ihren Passwort-Manager auch ihrer Familie zur Verfügung stellen?
- Kann der Passwort-Manager auf unbegrenzt vielen Geräten verwendet werden?
- Kostet die Einrichtung eines persönlichen Kontos ergänzend zum Unternehmenskonto extra?
- Müssen Mitarbeiter ihr persönliches und das dienstlich genutzte Konto miteinander verknüpfen, um immer an alle Daten zu gelangen?

Empfohlene Maßnahmen:

- **Die eigenen Richtlinien prüfen:** Hat Ihr Unternehmen eine BYOD- oder BYOA-Richtlinie zur dienstlichen Nutzung privater Geräte? Dann sollten Ihre Mitarbeiter auf all diesen Geräten ein entsprechend sicheres Passwortverhalten an den Tag legen.
- **Nahtlosen Prozess für Mitarbeiter schaffen:** Erkundigen Sie sich beim Lösungsanbieter, wie aufwendig die Einrichtung eines persönlichen Passwort-Managers ist. Die Erweiterung des Passwort-Managers sollte nichts verkomplizieren. Sie sollte Ihren Mitarbeitern etwas bringen und als Vorteil erlebt werden.

Checkliste für die erfolgreiche Einführung

Sie haben sich für einen bestimmten Passwort-Manager entschieden. Nun möchten Sie, dass möglichst viele Mitarbeiter und IT-Administratoren in Ihrem Unternehmen von dem Tool guten Gebrauch machen. Durch Heranziehen der oben genannten Bewertungskriterien auf der Suche nach einem Passwort-Manager haben Sie bereits die Basis für eine erfolgreiche Implementierung gelegt. Auf einige Schritte sollten Sie besonderes Augenmerk legen, um bei der Einführung der Lösung sicherzustellen, dass sie zu einem wichtigen Asset in Ihrem Unternehmen wird:

Das Projekt und die Ziele definieren

Wenn Sie das Thema Passwortverwaltung angehen, nutzen Sie eine exzellente Chance zur Verbesserung der Sicherheit und verbessern die Arbeitsproduktivität Ihrer Mitarbeiter enorm. Den Ausgangspunkt für Ihre Maßnahmen bildet eine solide Implementierungsstrategie.

Empfohlene Maßnahmen:

- Legen Sie Ihre Ziele bei der Implementierung eines Passwort-Managers eindeutig fest.
- Ermitteln Sie, wie sich ein Passwort-Manager in Ihre allgemeine Sicherheitsstrategie einfügt.
- Betrauen Sie jemandem mit dem Projekt, d. h. mit der Evaluierung, dem Vergleich, der Wahl und der Implementierung einer Passwortlösung.
- Analysieren Sie die bereits verwendeten Technologien. Spielt BYOD in Ihrem Unternehmen eine Rolle? Welche Cloud-Apps werden bei Ihnen genutzt? Welche anderen Lösungen für die Identitäts- und Zugriffsverwaltung (IAM) verwenden Sie? Soll Ihr Passwort-Manager in diese integriert werden? Falls ja, wie?
- Gewinnen Sie die Unterstützung der Unternehmensleitung und setzen Sie sich ein für eine Ausrichtung der Führungsstrategie an den Sicherheitszielen, die Ihr Unternehmen erreichen möchte. Klären Sie im Unternehmen dazu auf, inwiefern ein Passwort-Manager diese Ziele erreichen hilft.
- Definieren Sie, wie die erfolgreiche Einführung und die Kapitalrendite nachgewiesen werden sollen.

Richtlinien und Sicherheits-einstellungen überprüfen und in Kraft setzen

Die Standardoptionen des Passwort-Managers sorgen für ein Standardmaß an Sicherheit. Ihr Unternehmen könnte jedoch besondere Anforderungen haben. Ob zeitliche und örtliche Einschränkung des Zugriffs der Mitarbeiter auf den Passwort-Vault, Deaktivierung bestimmter Funktionen oder Verwendung spezifischer Sicherheitseinstellungen, Sie müssen sich mit den Optionen auseinandersetzen, die Ihre Lösung Ihnen bietet. Nehmen Sie Berechtigungen und Einschränkungen genau unter die Lupe und treffen Sie die entsprechenden Einstellungen, bevor Sie Ihren Mitarbeitern den Dienst zur Verfügung stellen.

Empfohlene Maßnahmen:

- Definieren Sie Ihre Sicherheitsstufe und die zu schützenden Ressourcen.
- Überprüfen Sie alle verfügbaren Sicherheitsrichtlinien und -einstellungen Ihres Passwort-Managers.
- Entscheiden Sie, welche Einstellungen global für das ganze Unternehmen gelten sollen.
- Entscheiden Sie, welche Einstellungen auf gruppenspezifischer oder individueller Ebene gelten sollen.
- Aktivieren Sie die für Ihr Sicherheitsmodell passenden Richtlinien und Einstellungen.
- Nutzen Sie ergänzende Sicherheitsmaßnahmen wie die Multifaktor-Authentifizierung.

Den Passwort-Manager für die Benutzer einführen

Der wahre Nutzen einer Lösung zeigt sich, wenn sie von den Benutzern angenommen wird. Um eine erfolgreiche Implementierung sicherzustellen, sollten Sie die Funktionen des Tools für ein effizientes Onboarding nutzen und überlegen, was zu tun ist, falls sich Benutzer nicht registrieren oder das Tool nicht nutzen.

Empfohlene Maßnahmen:

- Evaluieren Sie die verfügbaren Onboarding-Möglichkeiten und wählen Sie die beste Methode für Ihre Umgebung aus.
- Synchronisieren Sie die Lösung mit Ihren bestehenden Verzeichnissen, um so das Onboarding zu automatisieren.
- Versenden Sie Mitteilungen an die Mitarbeiter, um sie auf die Einführung des Passwort-Managers vorzubereiten.
- Laden Sie alle Mitarbeiter zur Nutzung des Tools ein und richten Sie ihre Konten ein.
- Informieren Sie alle Mitarbeiter über geltende Richtlinien und Best Practices, insbesondere in Bezug auf mehrmals verwendete Passwörter sowie die Qualität, Freigabe und Gültigkeitsdauer von Passwörtern.
- Richten Sie planmäßige Erinnerungen für Mitarbeiter ein, die sich nicht registrieren bzw. die Softwarelösung zu wenig nutzen.

Schulungen für Administratoren und Mitarbeiter organisieren

Ob im klassischen Kursformat oder als offenes Info-Angebot für Mitarbeiter, Schulungen für Administratoren und Benutzer werden das Interesse an Ihrem neuen Passwort-Manager fördern.

Empfohlene Maßnahmen:

- Decken Sie in den Mitarbeiterschulungen die wichtigsten Funktionen des Passwort-Managers ab.
- Erstellen Sie interne Onboarding-Toolkits: Handouts, Präsentationen oder Webinare.
- Geben Sie Mitarbeitern während der Schulung oder zu anderen Zeiten Gelegenheit, Fragen zu stellen.
- Nehmen Sie die Passwort-Manager-Schulung in den Onboarding-Prozess für neue Mitarbeiter auf, sodass diese automatisch mit dem Dienst vertraut gemacht werden.
- Geben Sie sich klare Richtlinien für den Umgang mit den Fragen und Supportanliegen, die Sie erreichen.

Sich für den langfristigen Erfolg positionieren

Nach der Implementierung Ihres Passwort-Managers sollte der tägliche Verwaltungsaufwand minimal sein. Nichtsdestotrotz möchten Sie wahrscheinlich dafür sorgen, dass Sie die im Laufe der Zeit erzielten Verbesserungen in Sachen Passwortsicherheit messen und so das Beste aus Ihrem Passwort-Manager holen können.

Empfohlene Maßnahmen:

- Machen Sie sich mit allen Einstellungen und Funktionen im Dashboard für Administratoren vertraut, selbst wenn Sie sie anfangs nicht brauchen.
- Überprüfen Sie die Akzeptanz und Sicherheitsbewertungen der Benutzer.
- Erstellen Sie einen Plan, um die Bewertungen der Passwortsicherheit mit der Zeit zu verbessern.

Wie harmoniert ein Passwort-Manager mit Ihren sonstigen Sicherheitslösungen?

Ein Business-Passwort-Manager stellt Ihre Unternehmenssicherheit auf ein stabiles Fundament. Eine bessere Passwortsicherheit senkt zuverlässig die Risiken, Opfer von Cyberangriffen zu werden, und sie erleichtert Unternehmensmitarbeitern den Arbeitsalltag.

Hinzu kommen ergänzende Technologien wie die Multifaktor-Authentifizierung, die an allen Zugriffspunkten für noch mehr Sicherheit sorgt. Und durch Zugriffsmethoden wie Single Sign-On kann Ihr Unternehmen seinen Mitarbeitern sogar die Authentifizierung ohne Passwort bieten.

Multifaktor-Authentifizierung (MFA)

Bei der MFA bestätigt ein Benutzer während der Authentifizierung seine Identität durch die Angabe von zwei oder mehr Details („Faktoren“). Dies verwehrt potenziellen Angreifern den Zugriff, denn mit einem gestohlenen Passwort alleine kommen sie hier nicht weiter.

Moderne MFA-Lösungen nutzen etwas, was die meisten von uns sowieso immer bei sich haben: das Smartphone. Kontextbezogene und biometrische Faktoren sorgen für eine absolut lückenlose Sicherheit. Benutzer bestätigen dabei ihre Identität mit biometrischen Faktoren wie Fingerabdruck oder Face-ID, während das Gerät sie hinter den Kulissen anhand von Kontextfaktoren wie Gerätestandort oder IP-Adresse verifiziert. Indem sie die Anforderungen der jeweiligen Anmeldesituation anpasst, sorgt die adaptive MFA dafür, dass die richtigen Benutzer zur richtigen Zeit auf die jeweiligen Daten zugreifen. Damit schlägt sie zwei Fliegen mit einer Klappe: Sie sorgt für eine höhere Sicherheit und bietet Mitarbeitern gleichzeitig eine komfortable Authentifizierung.

DARAUF MÜSSEN SIE ACHTEN:

- **Komfort für Benutzer: Möglichkeit zum Einsatz des eigenen Mobilgeräts**
- **Berücksichtigung von Hintergrundfaktoren wie Gerätestandort, Geräte-ID und IP-Adresse**
- **Unterstützung biometrischer Faktoren: Fingerabdruck und Face-ID**
- **Integrierte Sicherheit mit Verschlüsselung biometrischer Daten auf Geräteebene**
- **Kombinierbarkeit von Methoden: Push-Benachrichtigung, Biometrie und adaptive Authentifizierung**
- **Unterstützung von Cloud- und Legacy-Anwendungen, VPNs, Workstations, Identitätsanbietern und mehr**
- **Direkte Integration in den Passwort-Manager, die Administratoren und Benutzern das Leben erleichtert**

Single Sign-On (SSO)

Noch komfortabler als ein Passwort-Manager ist SSO: Hier erfolgt die Anmeldung der Mitarbeiter nicht per Passworteingabe, sondern über ein Authentifizierungsprotokoll. Anstelle für jede Anwendung die Zugangsdaten einzugeben, muss sich der Benutzer bei SSO nur einmal (beim SSO-Anbieter) authentifizieren. Danach übernimmt in einer sicheren Sitzung ein Protokoll wie SAML 2.0 im Hintergrund die weitere Authentifizierung.

SSO erspart Benutzern also die Eingabe von Passwörtern, da es nach nur einer Anmeldung sicheren Cloud-Zugriff auf mehrere Anwendungen gibt. Durch die Kombination von SSO und Passwort-Manager kann die IT sämtliche Zugriffspunkte im Unternehmen sehen und verwalten, ganz gleich ob es sich dabei um eine von ihr selbst verwaltete App handelt oder die im Portal gespeicherte Anmeldung eines Mitarbeiters auf einer Website.

DARAUF MÜSSEN SIE ACHTEN:

- **Einfache Einrichtung für Administratoren**
- **Großer Katalog an SSO-Anwendungen und möglichst viele vorintegrierte Apps**
- **Speicherung von SSO-Apps und klassischen Zugangsdaten in einem Portal**
- **Zentrales Admin-Dashboard für die Verwaltung von Richtlinien zu Passwörtern, SSO-Apps und MFA**

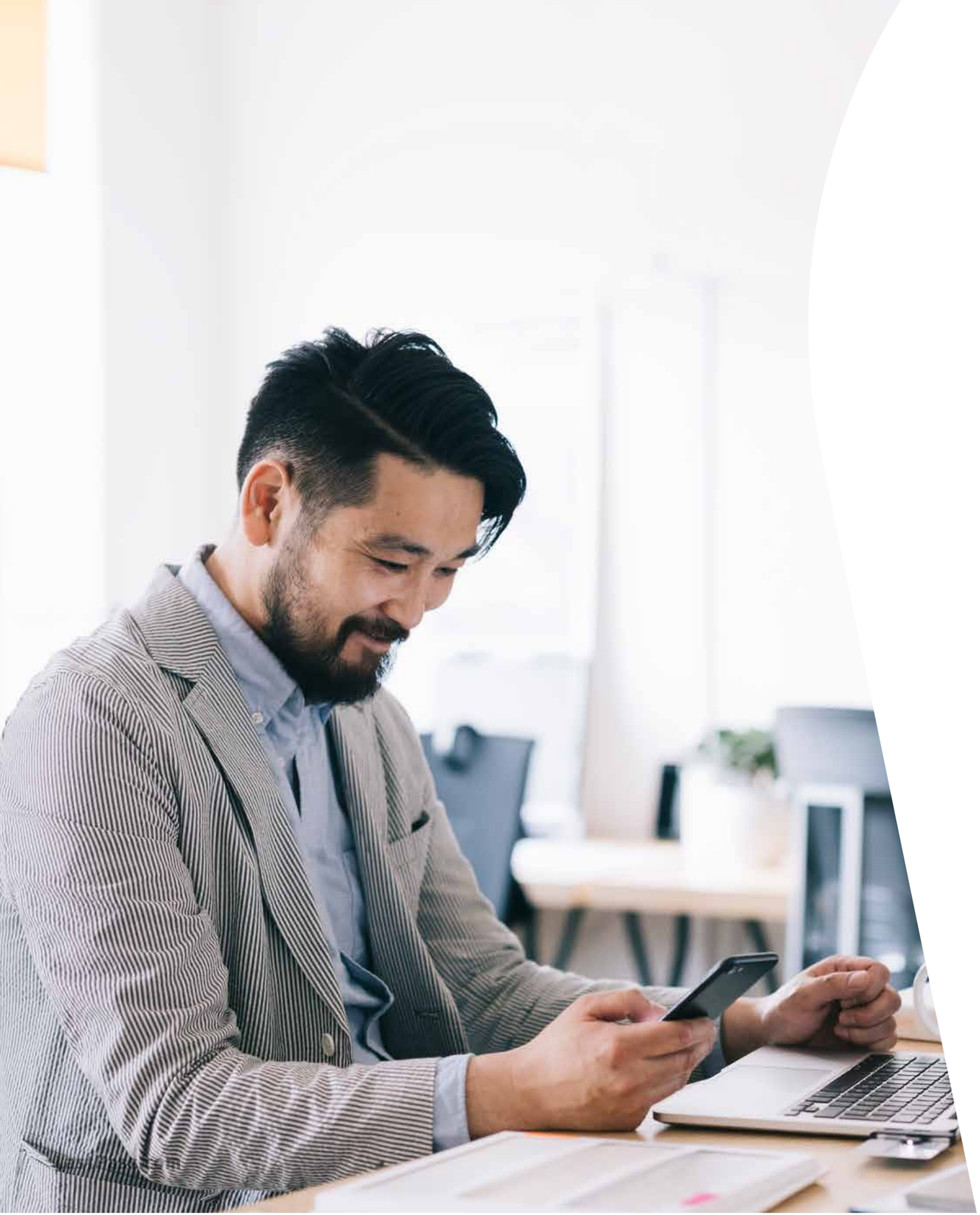
LastPass Business – für alle Anforderungen gemacht

In über 70.000 Unternehmen bietet LastPass Business Mitarbeitern ein reibungsloses Nutzungserlebnis und sorgt gleichzeitig für mehr Kontrolle und Transparenz – mit einer verwaltungs- und benutzerfreundlichen Lösung für die Passwortverwaltung. Mit LastPass Business können Mitarbeiter Zugangsdaten nahtlos erzeugen, absichern und freigeben. Die Sicherheit nach dem Zero-Knowledge-Prinzip sorgt dabei für besten Schutz.

Von der Passwortverwaltung abgesehen, bietet LastPass Business als weitere Sicherheitsfunktionen Single Sign-On (SSO) mit einfachem Zugriff auf bis zu drei Cloud-Anwendungen und Multifaktor-Authentifizierung (MFA) für den Schutz des LastPass-Vaults und dieser SSO-Anwendungen.

Der Ad-hoc-Support bietet unter anderem folgende Funktionen:

- Zentrale Administrationskonsole
- Nutzungs-Dashboard
- Universelle Passwortverwaltung
- Integration von Benutzerverzeichnissen
- Mehr als 100 Sicherheitsrichtlinien
- Detaillierte Sicherheitsberichte
- Sichere Freigabe von Passwörtern
- Darkweb-Überwachung
- SSO-Grundfunktionen
- MFA-Grundfunktionen
- Kostenloses Families-Konto für Mitarbeiter



Weitere Add-Ons:

LastPass Advanced SSO

Erweitertes Single Sign-On mit LastPass 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.

LastPass Advanced MFA

LastPass-Multifaktor-Authentifizierung der nächsten Generation schützt jeden Zugriffspunkt im Unternehmen. Cloud-Apps oder ältere Apps, VPN oder Workstations: LastPass Advanced MFA versieht Ihre Endpunkte mit einer weiteren Schutzebene und sorgt so für maximale Sicherheit.

Mit LastPass Advanced MFA sichert Ihr Unternehmen sämtliche Webanmeldungen ab und sorgt für die Verifizierung von Endpunkten – alles mit einer benutzerfreundlichen Mobilgeräte-App.

LastPass •••|
by LogMeIn

Der einfache Weg zu mehr Sicherheit für Ihr Unternehmen

Weitere Informationen