DATENBLATT

Password Manager

Optimale Benutzererfahrung, niedrigere Support-Kosten und höhere Sicherheit

Vorteile

- Geringerer Aufwand für Helpdesk und IT-Personal bei der routinemäßigen Kennwortverwaltung
- Drastischer Rückgang der Ausfallzeiten
- Sofortige Investitionsrendite
- Höhere Zufriedenheit bei Benutzern und IT-Personal aufgrund der einfachen Handhabung und Bereitstellung
- Höhere Netzwerksicherheit
- Synchronisierung von Kennwörtern zwischen unterschiedlichen Systemen
- Höhere Sicherheit dank Integration mit mehrstufiger Authentifizierung über Defender

Überblick

Bei den meisten Helpdesk-Anfragen geht es um die Zurücksetzung von Kennwörtern. Da Organisationen auch zunehmend darum bemüht sind, strengere Sicherheitsrichtlinien zu implementieren, wird die Kennwortverwaltung immer aufwendiger. Benutzer müssen sich immer komplexere Kennwörter ausdenken und diese Kennwörter immer öfter ändern. Die Wahrscheinlichkeit, dass sie ihre Kennwörter vergessen und Support anfordern müssen, steigt damit drastisch. Organisationen, die mehrere unterschiedliche Systeme und Anwendungen per Kennwort sichern, haben ein noch größeres Problem. Es entsteht ein Dilemma: Wie lässt sich die Sicherheit steigern, bei einer gleichzeitigen Senkung der Kosten für den Benutzer-Support?

Password Manager ist eine einfache und sichere Self-Service-Lösung, mit der Benutzer selbstständig Kennwörter zurücksetzen und Konten entsperren können. Sie erlaubt es Administratoren, strengere Kennwortrichtlinien zu implementieren und dadurch gleichzeitig den Helpdesk zu entlasten. Unternehmen müssen dadurch nicht länger Kompromisse bei der Sicherheit machen, um Kosten einzusparen.

Funktionen und Merkmale

Verbesserte Sicherheit

Mit Password Manager können Organisationen sichere Datenzugriffsrichtlinien implementieren, die über die nativen Microsoft® Active Directory® Steuerungsfunktionen hinausgehen. Mit der Lösung verbessern Sie die Sicherheit durch das Eliminieren von Helpdesk-Fehlern, Sie reduzieren das Bedürfnis Ihrer Benutzer, Passwörter aufzuschreiben, und erschweren unerlaubte Zugriffe durch erratene Passwörter. Die integrierte Datenverschlüsselung erlaubt globalen Zugriff bei gleichbleibend hoher Datensicherheit.

Investitionsrendite durch Benutzereinbindung

Mit Password Manager können Benutzer die einfachsten Kennwortverwaltungsaufgaben selbst übernehmen. Dies schont das IT-Budget Ihres Unternehmens und führt zu einer schnellen Investitionsrendite.

Eine Investition, die sich lohnt

Password Manager gibt Ihnen eine langfristige Lösung für ein immer akuter werdendes Problem an die Hand. Die Investition in diese Lösung lohnt sich für alle Unternehmen, die um eine höhere operative Effizienz der IT und mehr Sicherheit bemüht sind.

- Kosteneffektivität dank Aufbau auf der vorhandenen Active Directory Infrastruktur: Mit Password Manager können Sie Ihre bestehende Active Directory Infrastruktur noch besser nutzen. Sie können die Lösung außerdem schnell bereitstellen und eine sofortige Investitionsrendite erzielen. Darüber hinaus bietet sie eine präzisere gruppenbasierte Kennwortrichtlinie als Windows Server.
- Weniger Aufwand und Kosten für den Helpdesk und höhere Benutzerproduktivität: Mit Password Manager können Benutzer ihre Kennwörter selbst zurücksetzen und Kontosperren aufheben, ohne sich mit dem Helpdesk oder Administrator in Verbindung setzen zu müssen.
- Benutzerhilfe auf Abruf: Password Manager bietet Online-Erläuterungen zur Kennwortrichtlinie. Darüber hinaus werden die Benutzer automatisch benachrichtigt, wenn ein Kennwort die vorgegebenen Anforderungen nicht erfüllt, und können konforme Kennwörter generieren, ohne den Helpdesk zu bemühen.
- GINA Erweiterungen für das Windows Anmeldedialogfeld: Um den Benutzern das Zurücksetzen von Kennwörtern zu erleichtern, können Administratoren im Windows Anmeldedialogfeld eine Schaltfläche hinzufügen, mit der Kennwörter vor der Anmeldung zurückgesetzt werden können. Damit ist es nicht nötig, öffentliche Kiosks oder kostspielige telefonbasierte Systeme zu konfigurieren.

Erzwingung von Unternehmensstandards

Password Manager unterstützt mehr organisatorische Richtlinien und Datensicherheitsstandards als jede andere Lösung.

- Strenge Richtlinienerzwingung: Password Manager erzwingt die Durchsetzung von Standards, die Administratoren definiert haben, protokolliert misslungene Authentifizierungsversuche und sperrt die entsprechenden Konten bei Bedarf.
- Zwingende Registrierung: Password Manager bietet eine Reihe von Mechanismen, um sicherzustellen, dass sich Benutzer registrieren und die Software auch verwenden. Die Lösung sorgt also selbst dafür, dass sie ihren Zweck erfüllt.
- Zuverlässige Authentifizierung: Die persönlichen Profile für Benutzer enthalten Fragen mit eindeutigen Antworten, die sich die Benutzer gut merken, von Unbefugten aber nicht leicht erraten werden können. Darüber hinaus kann Password Manager in Defender integriert werden, um eine sicherere Authentifizierung per Einmalkennwort zu implementieren – wahlweise in Kombination mit dem Frage-Antwort-Profil oder als Ersatz für das Profil.
- Sicherheit und Einfachheit: Password Manager kann nahtlos in Windows integriert und von Benutzern aus mehreren Domänen, mit oder ohne Vertrauensstellungen, genutzt werden. Starke Datenverschlüsselung und sichere Kommunikation werden durch Unterstützung für führende Technologien wie Microsoft CryptoAPI und SHA-256 sichergestellt.

Überwachung der Systemaktivität

Password Manager stellt robuste Protokollierungs- und Berichterstellungsfunktionen für Administratoren bereit und erleichtert diesen die Überwachung der Systemaktivität und die Korrektur von Anomalien.

Unterstützung von Initiativen zur Identitätsverwaltung

Password Manager verfügt über eine reaktionsschnelle Weboberfläche und bietet Kennwortverwaltung für alle mit Microsoft Identity Integration Server (MIIS) verbundenen Systeme. Die Lösung kann außerdem für nicht von Microsoft stammende Betriebssysteme wie Unix und Linux eingesetzt werden, und zwar durch Authentication Services; die Ergänzung von Zwei-Faktor-Authentifizierung über Defender.

One Identity Hybrid-Abonnement

Erweitern Sie die Möglichkeiten des Password Manager mit dem One Identity Hybrid-Abonnement, das Ihnen zusätzliche, über die Cloud gelieferte Funktionen und Dienste bietet. Erhalten Sie Zugriff auf unbegrenzte Starling Two-Factor Authentication, um den Zugriff von Administratoren und Endbenutzern mit Password Manager zu schützen, der das Add-on zur telefonischen Verifizierung ersetzt. Ein einziges Abonnement ermöglicht die Bereitstellung aller One Identity-Lösungen.

Über One Identity

Das Quest Software-Unternehmen One Identity ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Dank unseres einzigartig breiten und integrierten Portfolios mit Angeboten zur Identitätsverwaltung einschließlich Kontoverwaltung, Identitätsgovernance und -verwaltung sowie Verwaltung privilegierten Zugriffs haben Unternehmen mehr Macht, ihr volles Potential zu erreichen, wo Sicherheit dadurch erreicht wird, dass Identitäten im Kern des Programms platziert werden, so dass für alle Benutzertypen, Systeme und Daten der richtige Zugriff gewährt wird. Weitere Informationen erhalten Sie unter OneIdentity.com.

Datasheet_2019_PasswordManager_US_RS_55939