Netwrix Password Secure

PLANET 33 netwrix

PASSWORTSICHERHEIT UND -VERWALTUNG LEICHT GEMACHT

Unternehmen stehen vor der Herausforderung, die Passwörter ihrer Mitarbeiter sicher zu verwalten und zu speichern, was zu potenziellen Sicherheitsrisiken und Ineffizienzen führt. Ein Passwort-Manager bietet eine zentralisierte, benutzerfreundliche Lösung, die die Sicherheit erhöht, die Kennwortverwaltung vereinfacht und die Einhaltung von Best Practices und Branchenstandards gewährleistet.

Erhöhte Passwortsicherheit: Netwrix Password Secure bietet erweiterte Verschlüsselung, Multi-Faktor-Authentifizierung, automatische Passwortrotation, Passwortrichtlinien und vieles mehr. Es unterstützt Sie dabei, das Risiko von Sicherheitsverletzungen durch schwache oder mehrfach genutzte Passwörter zu reduzieren.

Zentralisierte Sichtbarkeit und Kontrolle: Netwrix Password Secure ermöglicht es IT-Administratoren, den Benutzerzugriff zu verwalten und zu überwachen sowie alle passwortbezogenen Prozesse zentral zu steuern. Die Lösung bietet Transparenz der passwortbezogenen Aktivitäten und ermöglicht Echtzeit-Prüfungen und -Reporting. Bei einer selbst gehosteten Lösung bleiben alle sensiblen Daten stets in der Hand des Kunden.

Erhöhte Produktivität: Netwrix Password Secure verschlankt die Workflows der Passwortverwaltung und reduziert den Zeit- und Arbeitsaufwand für die Benutzerverwaltung. Dies steigert die Produktivität von IT-Teams und Benutzern gleichermaßen, da Mitarbeiter schnell und sicher auf die benötigten Ressourcen zugreifen können.

USE CASES

PASSWORTSICHERHEIT UND -VERWALTUNG

Sichere Passwortspeicherung
Speichern und schützen Sie Passwörter und andere sensible Daten in einer hochsicheren und verschlüsselten Umgebung, um unbefugten Zugriff zu verhindern.

Passwort-Generierung:
Generieren Sie starke, komplexe und eindeutige Passwörter für jeden Benutzer und jede Anwendung, um das Risiko von Passwortverstößen zu verringern.

Passwort-Rotation:
Automatisches Rotieren von Passwörtern in vordefinierten Intervallen, um sicherzustellen, dass veraltete Anmeldedaten keine Sicherheitsrisiken darstellen.

Passwort-Sharing:
Erleichtern Sie den sicheren Austausch von Passwörtern zwischen autorisierten Benutzern oder Teams, ohne sensible Informationen preiszugeben.

Passwortrichtlinien für externe Ressourcen:
Erzwingen Sie Regeln für die Komplexität von Passwörtern, Ablaufrichtlinien und andere Sicherheitsstandards, um eine strenge Passworthygiene aufrechtzuerhalten, und setzen Sie die Passwortrichtlinien externer Ressourcen außer Kraft, um die Sicherheit zu erhöhen.

BENUTZERZUGANG UND AUTHENTIFIZIERUNG

Single Sign-On (SSO) und Ein-Klick-Anmeldung:
Ermöglichen Sie Anwendern den Zugriff auf mehrere Anwendungen und Dienste mit einem einzigen Satz von Anmeldeinformationen mit nur einem Klick und verbessern Sie so die Benutzerfreundlichkeit

---

Rollenbasierte Zugriffskontrolle:
Weisen Sie Zugriffsberechtigungen auf der Grundlage von Benutzerrollen und Verantwortlichkeiten zu und stellen Sie so sicher, dass Mitarbeiter nur auf die Ressourcen zugreifen können, die sie benötigen.

Notfall-Zugang:
Bieten Sie autorisierten Personen einen Mechanismus für den Zugriff auf kritische Konten oder Systeme in Notfällen, z. B. bei Mitarbeiterabgängen oder Systemausfällen.

Benutzer-Self-Service:
Ermöglichen Sie den Benutzern die Verwaltung von Passwörtern und Zugängen innerhalb definierter Sicherheitsparameter und reduzieren Sie so den Aufwand für den IT-Support.

BETRIEBSEFFIZIENZ UND COMPLIANCE

Mobile Erreichbarkeit:
Stellen Sie mobile Apps oder reaktionsschnelle Weboberflächen bereit, um einen sicheren Passwortzugriff auf verschiedenen Geräten zu ermöglichen und so die Flexibilität und Produktivität zu erhöhen.

Auditing und Protokollierung:
Führen Sie detaillierte Aufzeichnungen über passwortbezogene Aktivitäten, damit Administratoren zu Compliance- und Sicherheitszwecken nachvollziehen können, wer wann auf was zugegriffen hat.

Einhaltung von Vorschriften und Berichterstattung:
Erstellen Sie Berichte und Dashboards für Compliance-Audits, um die Einhaltung von Sicherheitsstandards und -vorschriften zu demonstrieren.

KEY FEATURES

SICHERHEIT

Passwort-Richtlinien
Durchsetzung von Komplexitätsanforderungen und Rückmeldung über die Qualität von Passwörtern, automatische Überprüfung von manuell eingegebenen Passwörtern anhand von Richtlinien.

Kennwort-Generator
Erstellen Sie benutzerdefinierte, phonetische oder richtlinienbasierte Passwörter mit einem Klick.

Hierarchische Verschlüsselung
Die Daten werden in einem zweistufigen Verfahren verschlüsselt, das auf der Rolle des Benutzers und der Mitgliedschaft des Benutzers in dieser Rolle basiert.

Sitzungsverwaltung
Zeigen Sie alle aktiven Client-Sitzungen an und beenden Sie sie manuell beenden.

Passwort-Maskierung
Passwörter mit Schutz der Privatsphäre können nicht aufgedeckt oder in die Zwischenablage kopiert werden.

Rollenbasierte Zugriffskontrolle
Rollenbasierte Zugriffskontrolle mit vererbbaren Einstellungen und Rechten.

Zwei-Faktoren-Authentifizierung
Für den Zugriff auf sicherheitskritische Daten kann ein zusätzlicher Faktor (One-Time-Password) für die Anmeldung verwendet werden.

Passwort-Historie
Alle früheren Versionen eines Datensatzes. Falls erforderlich, kann ein älterer Stand wiederhergestellt werden.

Web Viewer über Browser
Export der gewünschten Zugangsdaten in ein passwortgeschütztes HTML-Dokument, das auch ohne Internetzugang genutzt werden kann.

Offline-Client
Daten lokal hochverschlüsselt speichern und automatisch synchronisieren, wenn eine Verbindung zum Server wiederhergestellt wird.

Eingeschränkte Benutzer
Gewähren Sie Zugriff auf das System ohne Passwörter anzuzeigen.

Sicherheitsstufen für Einstellungen
Passen Sie die Einstellungen an Benutzerrollen und Arbeitsabläufe an und schränken Sie die Optionen für einige Benutzer ein, während Sie anderen einen erweiterten Zugriff gewähren.

Sitzungsaufzeichnung
RDP/SSH-Sitzungen können aufgezeichnet werden.

Revisionssicheres Logbuch und Berichte
Protokollieren Sie alle Aktionen eines Benutzers revisionssicher.

Anbindung an Hardware-Sicherheitsmodule (HSM)
Erhöhter Schutz durch Auslagerung der Server / Schlüssel auf ein HSM.

Temporärer Zugang
Der Zugang zu Passwörtern kann begrenzt werden.

Notfall-Web-Viewer (2FA-geschützt)
Sicherer Zugriff in kritischen Situationen, mit Zwei-Faktor-Authentifizierung für zusätzlichen Schutz.

Live-Benachrichtigungen
Benachrichtigen Sie Benutzer per Pop-up oder E-Mail über wichtige Ereignisse, wie z. B. die Freigabe eines Passworts.

Mehr-Augen-Prinzip für Passwortfreigabe
Um ein Passwort einzusehen, ist die Zustimmung von mindestens einem weiteren Benutzer erforderlich. Zusätzlich kann die Angabe eines Grundes für die Anfrage verlangt werden.

Interessieren Sie sich für Netwrix Password Secure oder haben Sie eine Frage?
Wir sind für Sie da. Schreiben Sie uns an sales@planet33.com und wir melden uns in Kürze bei Ihnen zurück.

Autofill bei lokalen Anwendungen
Die Zugangsdaten können auch automatisch für lokale Anwendungen eingegeben werden.

Tagging von Passwort-Datensätzen
Datensätze können mit Schlüsselwörtern versehen werden, um sie schneller Wiederauffinden versehen werden. Nach diesen Schlüsselwörtern kann gesucht werden.

Dynamisches Dashboard
Konfigurieren Sie Dashboards, um einen klaren Überblick über die wichtigsten Kennzahlen Ihrer Wahl zu erhalten, z. B. über die Qualität der Passwörter in Ihrem Unternehmen.

Eingabehilfe
Passwörter werden vergrößert dargestellt, um Sonderzeichen hervorzuheben, wobei jeder Großbuchstabe farblich hervorgehoben wird.

Organisatorische Struktur
Abbildung der gesamten Unternehmenshierarchie mit entsprechenden Berechtigungen.

Papierkorb
Passwörter können in den Papierkorb verschoben, bei Bedarf wiederhergestellt oder dauerhaft gelöscht werden.

Dokumentenverwaltung
Benutzer können Dokumente wie z.B. Zertifikate in verschlüsselter verschlüsselt speichern und Änderungen nachverfolgen.

Wahl zwischen einfacher und erweiterter Ansicht
Wählen Sie zwischen einer vereinfachten Ansicht mit wesentlichen Funktionen und einer Vollansicht mit erweiterten Funktionalitäten.

Flexible Rechtevorlagen
Erstellen Sie individuelle Vorlagen für die Zuweisung von Berechtigungen für neu erstellte Datensätze.

Browser-Erweiterungen
Optimieren Sie Online-Anmeldungen mit Autofill-Funktionalität.

Generierung von externen Links
Versenden Sie Links zu Passwortdatensätzen.

Interessieren Sie sich für Netwrix Password Secure oder haben Sie eine Frage?
Wir sind für Sie da. Schreiben Sie uns an sales@planet33.com und wir melden uns in Kürze bei Ihnen zurück.

AUTOMATION

Automatische Bereinigungen
Automatisches Löschen alter Datensätze, z. B. von ehemaligen Mitarbeitern.

Aufgabensystem
Automatisieren Sie wiederkehrende Aufgaben wie die Active Directory-Synchronisation.

Automatische Live-Backups
Automatisieren Sie Backups in Echtzeit.

Identitätsanbieter (mit SAML)
Melden Sie sich ohne Passwort an, indem Sie Netwrix Password Secure als Identity Provider verwenden, um verschlüsselte Anmeldedaten an den Service Provider zu übertragen.

Discovery Service für Dienstkonten
Scannen Sie das Netzwerk nach lokalen Dienstkonten und erkennen automatisch die Rücksetzung von Passwörtern.

Passwort zurücksetzen
Setzen Sie Passwörter automatisch auf einen neuen unbekannten Wert - sowohl in Netwrix Password Secure als auch in der Anwendung. Heartbeat prüft manuell oder automatisch, ob die in Netwrix Password Secure gespeicherten Anmeldedaten des Benutzers mit denen auf den jeweiligen Systemen übereinstimmen.

FUNKTIONELLE STANDARDS

Modernste Verschlüsselung
Passwörter werden auf dem Client mit gängigen und bewährten Methoden verschlüsselt, über TLS übertragen und in der Datenbank gespeichert (RSA/AES/PBKDF2).

Schutz durch Transport Layer Security-Verbindung (TLS)
Dauerhaft geschützte Verbindungen durch aktuelles TLS (1.2 und 1.3)

INSTALLATION UND HOHE VERFÜGBARKEIT

MSI-Software-Verteilung
Die erweiterte Ansicht (Full-Client) kann automatisch verteilt und installiert werden, und zwar über Microsofts Standard-MSI-Dateiverfahren.

SQL-Clustering
Bei Ausfall eines Datenbank-servers übernimmt ein anderer Server dessen Aufgaben zur Redundanz und Leistungssteigerung durch Lastverteilung.

Zugriffskontrollliste (ACL)
Der Zugriff auf die Datenbank ist nur für freigegebene Clients möglich.

Terminal Server Unterstützung
Zentrale Installation der erweiterten Ansicht (Full- Client) auf einem Terminalserver. Zuweisung einer Instanz für jeden Benutzer.

Skalierbarkeit
Mit einer zustandslosen Multi-Tier-Architektur bietet Netwrix PasswordSecure eine gleichbleibende Leistung bei wachsenden Unternehmen.

Lastverteilung über mehrere Anwendungsserver
Wenn sich ein einzelner Server als unzureichend erweist, können mehrere Server (die auch weltweit verteilt sein können) eingesetzt werden.

LOGIN FÜR NETWRIX PASSWORD SECURE

Anmeldung ohne Passwort
Bei Netwrix Password Secure können Sie sich mit einer Smartcard oder einem FIDO2-kompatiblen Token anmelden.

Login-Sperre
Wiederholte Fehlanmeldungen verursachen automatische temporäre Sperren, die mit jedem weiteren Fehlversuch verlängert werden, bis ein Administrator den Zugang entsperrt.

Multi-Faktor-Authentifizierung:
Wählen Sie aus verschiedenen zusätzlichen Faktoren, um die Sicherheit des Anmeldevorgangs weiter zu erhöhen.

Interessieren Sie sich für Netwrix Password Secure oder haben Sie eine Frage?
Wir sind für Sie da. Schreiben Sie uns an sales@planet33.com und wir melden uns in Kürze bei Ihnen zurück.

INTEGRATIONEN

Syslog-Server Unterstützung (SIEM)
Automatische Übertragung von Log-Dateien an einen zentralen Syslog-Server

---

Integrierter SSH-Client
Benutzer können eine sichere SSH-Verbindung innerhalb von Netwrix Password Secure mit den bereits gespeicherten Anmeldedaten aufbauen.

Kerberos-Verbindung
Active Directory-Benutzer können sich über das Kerberos-Protokoll authentifizieren.

Integrierter RDP-Client
Benutzer können eine sichere RDP-Verbindung innerhalb von Netwrix Password Secure mit den bereits gespeicherten Anmeldedaten herstellen.

RADIUS-Verbindung
Active Directory-Benutzer können sich sich über das RADIUS-Protokoll authentifizieren.

PKI-Integration
Zusätzlicher Schutz durch Verwendung eines Zertifikats als zweiter Faktor.

Active Directory-Integration
Verwalten Sie Benutzer über Active Directory.

API
Automatisieren und integrieren Sie die Funktionalitäten von Netwrix Password Secure.

Microsoft Entra ID Integration
Verwalten Sie Benutzer über Microsoft Entra ID.