KIEL-IT

netwrix

Netwrix Password Secure

Sicherheit und Verwaltung von Passwörtern leicht gemacht

Bei der sicheren Verwaltung und Speicherung von Passwörtern Ihrer Mitarbeiter sehen sich Unternehmen mit Herausforderungen konfrontiert. Die Folge sind mögliche Sicherheitsrisiken und ineffiziente Prozesse. Mit einem Passwortmanager der Enterprise-Klasse steht Ihnen eine zentrale, benutzerfreundliche Lösung zur Verfügung, mit der Sie die Sicherheit verbessern, die Passwortverwaltung vereinfachen und die Compliance mit Best Practices und Branchenstandards gewährleisten können.

Verbesserte Passwortsicherheit

Netwrix Password Secure stellt Funktionen für erweiterte Verschlüsselung, Multi-Faktor-Authentifizierung (MFA), automatische Passwortrotation, Passwortrichtlinien und viele weitere Aufgaben bereit. Sie können damit das Risiko von Sicherheitsverletzungen aufgrund von unsicheren oder wiederverwendeten Passwörtern mindern.

Umfassender Einblick und zentrale Kontrolle

Mit Netwrix Password Secure können IT-Administratoren den Benutzerzugriff verwalten und überwachen sowie alle passwortbezogenen Prozesse über eine zentrale Konsole steuern und auf diese Weise optimierte Abläufe sicherstellen. Die Lösung umfasst Funktionen für die Echtzeitüberwachung und Berichterstellung, die zentralen Einblick in sämtliche Aktivitäten im Zusammenhang mit Passwörtern gewähren. Mit einer selbst gehosteten Lösung behalten Unternehmen die Kontrolle über alle sensiblen Daten.

Höhere Produktivität

Netwrix Password Secure optimiert Workflows für die Passwortverwaltung, sodass der Benutzerzugriff einfacher verwaltet werden kann. Dies ermöglicht eine höhere Produktivität sowohl der IT-Teams als auch der Anwender, da Mitarbeiter schnell und sicher auf die benötigten Ressourcen zugreifen können.

ANWENDUNGSSZENARIEN

PASSWORTSICHERHEIT UND COMPLIANCE

- **Sichere Speicherung von Passwörtern:** Speichern und schützen Sie Passwörter und andere vertrauliche Anmeldeinformationen in einer hochgradig sicheren und verschlüsselten Umgebung, um unerlaubte Zugriffe zu verhindern.

- **Passworterstellung:** Erstellen Sie sichere, komplexe und individuelle Passwörter für jeden Benutzer und jede Anwendung, um das Risiko von Datenschutzverletzungen aufgrund unsicherer Passwörter zu mindern.

- **Passwortrotation:** Rotieren Sie Passwörter automatisch in bestimmten Zeitabständen, um sicherzustellen, dass veraltete Anmeldedaten kein Sicherheitsrisiko darstellen.

- **Passwörter teilen:** Ermöglichen Sie autorisierten Benutzern oder Teams Passwörter gemeinsam zu nutzen, ohne dadurch vertrauliche Informationen zu exponieren.

- **Durchsetzung von Passwortrichtlinien:** Implementieren Sie einheitliche oder individuelle Richtlinien für die Passwortkomplexität und -länge, Password Resets und andere Sicherheitsstandards, um eine optimale Passworthygiene zu gewährleisten. Damit wird auch der Verwendung von Passwörtern entgegengewirkt, die zu schwach sind und nur den Mindestanforderungen von Drittanbietern (externe Websites und Anwendungen) entsprechen.

ZUGRIFF UND AUTHENTIFIZIERUNG VON BENUTZERN

- **Single Sign-On (SSO) und Anmeldung mit einem Klick:** Bieten Sie Benutzern die Möglichkeit, mit ihren Anmeldedaten mit nur einem Klick auf verschiedene Anwendungen und Services zuzugreifen. So verbessern Sie das Benutzererlebnis und verhindern Passwortmüdigkeit.

- **Rollenbasierte Zugriffskontrolle:** Weisen Sie Zugriffsberechtigungen auf der Basis von Benutzerrollen und Verantwortlichkeiten zu, damit Ihre Mitarbeiter ausschließlich auf die benötigten Ressourcen zugreifen können.

- **Notfallzugriff:** Richten Sie einen Mechanismus ein, mit dem autorisierte Benutzer im Notfall (z. B. beim Ausscheiden von Mitarbeitern oder Systemausfällen) auf wichtige Konten oder Systeme zugreifen können.

- **Self-Services für Benutzer:** Ermöglichen Sie es Benutzern, Passwörter und Zugriffsrechte innerhalb vorgegebener Sicherheitsparameter selbst zu verwalten und so den IT-Support zu entlasten.

OPERATIVE EFFIZIENZ UND COMPLIANCE

- **Mobiler Zugriff:** Stellen Sie mobile Apps oder leistungsfähige Weboberflächen bereit, um einen sicheren, passwortgeschützen Zugriff über verschiedene Geräte zu ermöglichen und dadurch die Flexibilität und Produktivität zu erhöhen.
- **Überwachung und Protokollierung:** Erfassen Sie zu Compliance- und Sicherheitszwecken detaillierte Protokolle zu allen passwortbezogenen Aktivitäten, damit Administratoren nachverfolgen können, welche Benutzer wann worauf zugegriffen haben.
- **Compliance und Berichterstellung:** Erstellen Sie Berichte und Dashboards für Compliance-Audits, mit denen Sie die Einhaltung von Sicherheitsstandards und -vorschriften wie CMMC, DSGVO oder dem Grundschutzkompendium des BSI nachweisen können.

Diese Anwendungsszenarien helfen Unternehmen, die Sicherheit zu verbessern, ihre Prozesse für die Passwortverwaltung zu optimieren, die Compliance zu gewährleisten und das Risiko von Datenschutzverletzungen infolge von unsicheren oder falsch verwendeten Passwörtern zu mindern.

WICHTIGE FUNKTIONEN

Sicherheit

- **Passwortrichtlinien**

  Setzen Sie Anforderungen an die Komplexität von Passwörtern durch und geben Sie Feedback zur Qualität der Benutzerpasswörter. Überprüfen Sie die eingegebenen Passwörter automatisch auf Einhaltung der Richtlinien.

- **Ende-zu-Ende-Verschlüsselung**

  Netwrix Password Secure arbeitet mit Ende-zu-Ende-Verschlüsselung, bei der jedes Secret separat verschlüsselt und die zu übertragenden Daten erst beim Empfänger entschlüsselt werden.

- **Passwort-Generator**

  Erstellen Sie mit nur einem Klick individuelle, phonetische oder richtlinienbasierte Passwörter.

- **Passwortmaskierung**

  Geschützte Passwörter können nicht angezeigt oder in die Zwischenablage kopiert werden.

- **Hierarchische Verschlüsselung**

  Daten werden in einem zweistufigen Prozess auf Basis der Benutzerrolle und der Gruppenmitgliedschaft des Benutzers im Rahmen dieser Rolle verschlüsselt.

- **Rollenbasierte Zugriffskontrolle**

  Profitieren Sie von rollenbasierter Zugriffskontrolle mit vererbbaren Einstellungen und Rechten.

- **Zwei-Faktor Authentifizierung**

  Bei der Anmeldung kann ein zusätzlicher Faktor (Einmalpasswort) für den Zugriff auf sicherheitskritische Daten verwendet werden.

- **Sitzungsverwaltung**

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

- **Passwort-Historie**

  Es werden alle vorherigen Versionen eines Datensatzes gespeichert. Bei Bedarf ist die Wiederherstellung eines früheren Zustands möglich.

- **Revisionssichere Protokolle und Berichte**

  Führen Sie ein revisionssicheres Protokoll aller Aktionen eines Benutzers.

- **Web Viewer über den Browser**

  Exportieren Sie die erforderlichen Zugriffsdaten in ein passwortgeschütztes HTML-Dokument, das auch ohne Internetzugriff verwendet werden kann.

- **Verbindung mit Hardwaresicherheitsmodulen (HSM)**

  Die Auslagerung der Serverschlüssel auf ein HSM sorgt für höheren Schutz.

- **Offline-Add-on**

  Speichern Sie Daten lokal mit starker Verschlüsselung und synchronisieren Sie diese automatisch, sobald die Verbindung zum Server wiederhergestellt wird.

- **Emergency Web Viewer (mit Zwei-Faktor Authentifizierung)**

  Gewährleisten Sie einen sicheren Zugriff in kritischen Situationen und profitieren Sie mit Zwei-Faktor-Authentifizierung von zusätzlichem Schutz.

- **Benutzer mit eingeschränktem Zugriff**

  Gewähren Sie Zugriff auf das System, ohne Passwörter anzuzeigen.

- **Freigabe von Passwörtern nach dem Mehraugen-Prinzip**

  Die Freigabe eines Passworts muss von mindestens einem weiteren Benutzer genehmigt werden. Sie können außerdem festlegen, dass die Anforderung begründet werden muss.

- **Sicherheitsstufen für Einstellungen**

  Passen Sie Einstellungen an die Rollen und Workflows von Benutzern an und schränken Sie die Optionen für bestimmte Benutzer ein, während Sie anderen erweiterten Zugriff gewähren.

- **Live-Benachrichtigungen**

  Benachrichtigen Sie Benutzer in Pop-ups oder per E-Mail über wichtige Ereignisse wie die Anzeige ihres Passworts.

- **Aufzeichnung von Sitzungen**

  RDP/SSH-Sitzungen können aufgezeichnet werden.

- **Temporärer Zugriff**

  Der Zugriff auf Passwörter kann zeitlich beschränkt werden.

Produktivität

- **Automatisches Ausfüllen in lokalen Anwendungen**

  In lokalen Anwendungen ist auch eine automatische Eingabe von Zugriffsdaten möglich.

- **Dokumentenverwaltung**

  Benutzer können Dokumente wie Zertifikate verschlüsselt speichern und Änderungen nachverfolgen.

- **Tagging von Passwortdatensätzen**

  Für den schnelleren Abruf können Datensätze mit Keywords gekennzeichnet werden. Sie können nach diesen Keywords suchen.

- **Wahl zwischen Standard- und erweiterter Ansicht**

  Wählen Sie zwischen einer vereinfachten Ansicht mit grundlegenden Funktionen und der vollständigen Ansicht mit erweiterten Funktionen.

- **Organisationsstruktur**

  Bilden Sie die gesamte Unternehmenshierarchie mit den entsprechenden Autorisierungen ab.

- **Flexible Rechtevorlagen**

  Erstellen Sie individuelle Vorlagen, mit denen Sie Berechtigungen für neue Datensätze zuweisen können.

- **Browsererweiterungen**

  Optimieren Sie Online-Anmeldungen mit Funktionen für automatisches Ausfüllen.

- **Abtipp-Hilfe**

  Passwörter werden vergrößert angezeigt. Dadurch sind Sonderzeichen besser erkennbar und Großbuchstaben werden farblich markiert.

- **Erzeugung externer Links**

  Versenden Sie Links für den Zugriff auf Passwortdatensätze.

- **Dynamisches Dashboard**

  Konfigurieren Sie Dashboards, in denen die gewählten Kennzahlen (z. B. zur Qualität der Passwörter) übersichtlich dargestellt werden.

- **Papierkorb**

  Passwörter können in den Papierkorb verschoben werden. Bei Bedarf können sie wiederhergestellt oder dauerhaft gelöscht werden.

Automatisierung

- **Automatische Bereinigung**

  Löschen Sie alte Datensätze z. B. ehemaliger Mitarbeiter automatisch.

- **Automatische Live-Backups**

  Automatisieren Sie Backups in Echtzeit.

- **Tasksystem**

  Automatisieren Sie Routineaufgaben wie die Synchronisierung von Active Directory.

- **Identity Provider**

  Melden Sie sich ohne Passwort an, indem Sie Netwrix Password Secure als Identitätsanbieter für die Übertragung verschlüsselter Anmeldedaten an den Dienstanbieter nutzen.

- **Password Reset**

  Legen Sie für Passwörter sowohl in Netwrix Password Secure als auch in der Anwendung automatisch einen unbekannten Wert fest. Führen Sie manuelle oder automatische Überprüfungen durch, ob die in Netwrix Password Secure gespeicherten Anmeldeinformationen eines Benutzers mit denen in den jeweiligen Systemen übereinstimmen.

- **Discovery Service für Dienstkonten**

  Durchsuchen Sie das Netzwerk nach lokalen Dienstkonten und erkennen Sie Password Resets automatisch.

Funktionale Standards

- **Hochmoderne Verschlüsselung**

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

- **Schutz durch TLS-Verbindungen**

  Durch Unterstützung von TLS 1.2 und 1.3 sind Verbindungen permanent geschützt.

Installation und Hochverfügbarkeit

- **MSI-Softwareverteilung**

  Die erweiterte Ansicht kann automatisch verteilt und über das standardmäßige MSIDateiverfahren von Microsoft installiert werden.

- **Unterstützung für Terminalserver**

  Die erweiterte Ansicht kann auf einem Terminalserver installiert werden. Jedem Benutzer wird eine Instanz zugewiesen.

- **SQL-Clustering**

  Bei einem Ausfall des Datenbankservers werden dessen Aufgaben von einem anderen Server übernommen. Durch diese Lastverteilung profitieren Sie von Redundanz und zuverlässiger Performance.

- **Skalierbarkeit**

  Mit einer zustandslosen mehrstufigen Architektur bietet Netwrix Password Secure auch bei wachsenden Anforderungen konsistente Performance.

- **Access Control List (ACL)**

  Der Zugriff auf die Datenbank ist nur für freigegebene Clients möglich.

- **Lastverteilung auf mehrere Anwendungsserver**

  Reichen die Kapazitäten eines einzelnen Servers nicht aus, können mehrere (weltweit verteilte) Server genutzt werden.

Anmeldung in Netwrix Password Secure

- **Passwortlose Anmeldung**

  Melden Sie sich mit einer Smartcard oder einem FIDO2-konformen Token in Netwrix Password Secure an.

- **Multi-Faktor-Authentifizierung**

  Wählen Sie unter verschiedenen zusätzlichen Faktoren, um die Sicherheit des Anmeldevorgangs weiter zu erhöhen.

- **Anmeldesperre**

  Wiederholte fehlgeschlagene Anmeldeversuche führen automatisch zu einer vorübergehenden Sperre. Mit jedem weiteren fehlgeschlagenen Versuch verlängert sich die Dauer dieser Sperre, bis sie von einem Administrator aufgehoben wird.

BENUTZERTYPEN UND ANSICHTEN

Netwrix Password Secure

Standard und Advanced User: Die wichtigsten Unterschiede

Dieses Dokument enthält einen Vergleich der Funktionen für Standard und Advanced User von Netwrix Password Secure. Es werden lediglich die wichtigsten Unterschiede dargestellt.

ALLGEMEIN	Standard User	Advanced user
Umschalten zwischen Standard- und erweiterter Ansicht	Nein, nur Standard-Ansicht	Ja
Benutzer	Alle Mitarbeiter	IT-Team und Mitarbeiter mit erweiterten Zuständigkeiten (z. B. Teamleiter)
Anwendung	Web App	Windows & Web App
Primäres Anwendungsszenario	Tägliche Anmeldung auf Websites und in Anwendungen	Verwaltung von Benutzern und Datensätzen
Erforderliche Vorkenntnisse	Keine	Technische Grundkenntnisse, Schulung verfügbar
Wichtigste Aufgaben	Automatisches Anmelden, Erstellen und Verwalten von Passwörtern	Umfassende Passwortverwaltung einschließlich Überwachung und Dokumentation sämtlicher Zugriffe

PASSWORTVERWALTUNG	Standard User	Advanced user
Erstellen und Bearbeiten von Datensätzen	Verwenden von Vorlagen	Verwenden von Vorlagen und manuell
Anzeigen/Bearbeiten von Berechtigungen	Nein	Ja
Paralleles Bearbeiten mehrerer Datensätze	Nein	Ja
Automatischer Abgleich von Passwörtern mit Anwendungen	Ja	Auch manuell
AUTOMATISCHES ANMELDEN	**Standard User**	**Advanced user**
SSO mit automatischer Eingabe von Anmeldedaten	Ja	Ja
Automatische Voreinstellung von Anwendungen für SSO	Ja, mit Assistenten	Auch manuell
Unterstützte Anwendungen für SSO	Websites, Windows-Anwendungen, RDP-/SSH-Verbindungen	Websites, Windows-Anwendungen, RDP-/SSH-Verbindungen
Passwortlose Authentifizierung in Anwendungen ohne SSO	Ja, über SAML-Protokoll	Ja, über SAML-Protokoll
Unterstützung für Einmalpasswörter (OTP)	Ja	Ja
SUCHE	**Standard User**	**Advanced user**
Schnellsuche in Passwortdatensätzen	Ja	Ja
Erweiterte Filteroptionen für die Suche	Nein	Ja, umfassende Konfigurations- und Erweiterungsmöglichkeiten mit Widgets
Tagging-System	Ja	Ja
DESIGN	**Standard User**	**Advanced user**
Anzeige	Listen- und Kachelansicht	Detaillierte Listenansicht
Sortierung	Kacheln können per Drag & Drop manuell angepasst werden	Spalten können manuell angepasst werden, Spalteninhalte sind automatisch anpassbar
Strukturfilter	Registerkarten	Strukturbaum

INTEGRATIONEN

- **Unterstützung für Syslog- Server (SIEM)**

  Protokolldateien werden automatisch an einen zentralen Syslog-Server übertragen.

- **Integrierter RDP-Client**

  Benutzer können mit Netwrix Password Secure eine sichere RDP-Verbindung herstellen und dabei die bereits gespeicherten Anmeldeinformationen verwenden.

- **Integrierter SSH-Client**

  Benutzer können mit Netwrix Password Secure eine sichere SSH-Verbindung herstellen und dabei die bereits gespeicherten Anmeldeinformationen verwenden.

- **RADIUS-Verbindung**

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

- **Kerberos-Verbindung**

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

- **PKI-Integration**

  Die Verwendung eines Zertifikats als zweiten Faktor bietet zusätzlichen Schutz.

- **Active Directory-Integration**

  Verwalten Sie Benutzer über Active Directory.

- **Microsoft Entra ID-Integration**

  Verwalten Sie Benutzer über Microsoft Entra ID.

- **API**

  Automatisieren und integrieren Sie Funktionen von Netwrix Password Secure.

BEREITSTELLUNG

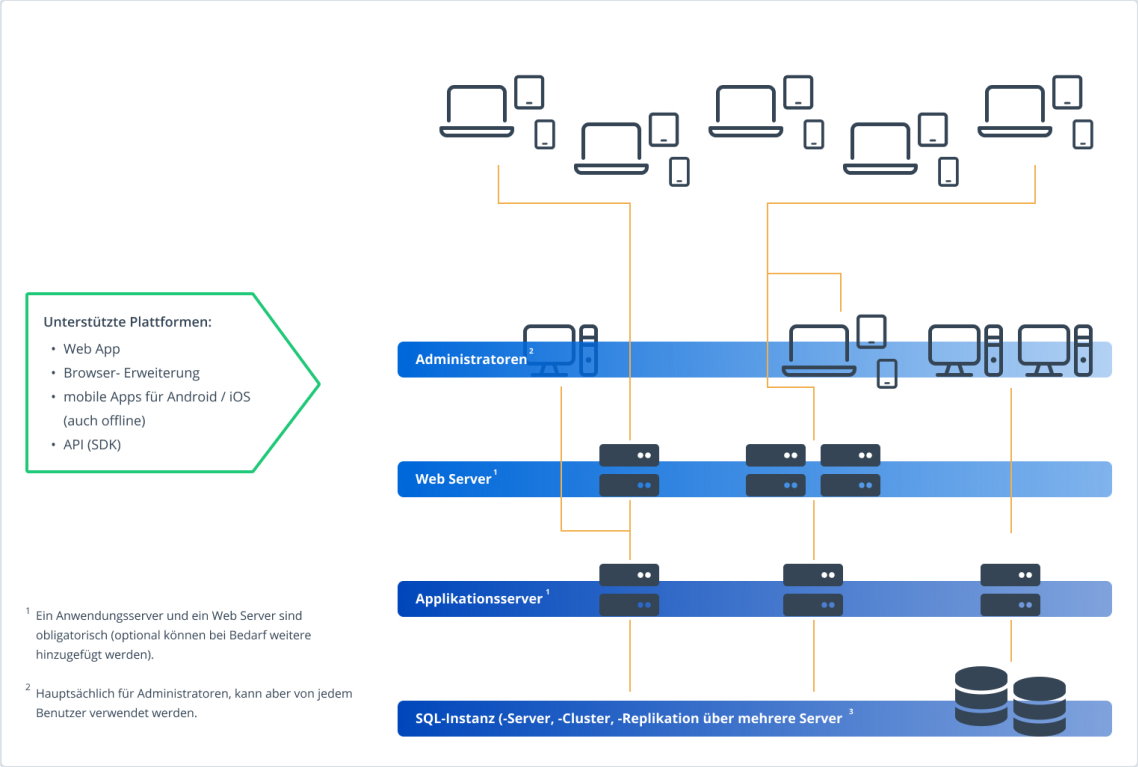
Beispiel A: Kleine Umgebung	Beispiel B: Mittlere Umgebung	Beispiel C: Große Umgebung
ein Windows-Server im Einsatz • SQL-Instanz (mindestens SQL Express) • Netwrix Password Secure Anwendungsserver • Netwrix Password Secure Webserver Verbindungen: Alle Clients verbinden sich mit diesem Server (über verschiedene Ports).	SQL-Instanz oder –Cluster Ein Netwrix Password Secure Anwendungsserver (oder mehrere für höhere Verfügbarkeit und Leistung), der auf einem Windows Server läuft. Ein Netwrix Password Secure Webserver (oder mehrere), der auf demselben Windows Server oder einem anderen Webserver läuft. Verbindungen: Administratoren, die die Windows App verwenden, verbinden sich direkt mit dem Anwendungsserver; alle anderen Benutzer verbinden sich mit dem Webserver.	SQL-Cluster Zwei Netwrix Password Secure Anwendungsserver (oder mehr zur Lastverteilung), die auf einem Windows Server laufen. Ein Netwrix Password Secure Webserver (oder mehr), der auf einem lastverteilten Webserver wie IIS oder NGINX läuft. Verbindungen: Admins, die die Windows-App verwenden, verbinden sich direkt mit dem Anwendungsserver; alle anderen Benutzer verbinden sich mit den Webservern.

*Es sind viele andere Konfigurationsmöglichkeiten möglich

LIZENZIERUNG

Grundlage für die Lizenzierung im Rahmen eines Abonnements ist die Anzahl der User und Advanced User.

ARCHITEKTURDIAGRAMM



Dieses Diagramm veranschaulicht die Funktionsweise von Netwrix Password Secure in einer IT-Umgebung. Die Anmeldeinformationen von Benutzern, Passwortrichtlinien und andere Daten werden ausschließlich in der internen SQL Server-Datenbank des Kunden gespeichert. Dadurch wird umfassende Datenhoheit gewährleistet.

Kunden können die Anzahl der Clients, Anwendungsserver, Datenbankserver und Web-Endpunkte nach Bedarf erhöhen, um eine effiziente Lastverteilung und möglichst geringe Latenz zu erzielen. Damit ermöglicht Netwrix Password Secure eine hohe Performance auch in großen und auf mehrere Regionen verteilten Umgebungen.

Administratoren können alles über eine zentrale Konsole verwalten und überwachen, während Anwender über eine einfache Weboberfläche, Browsererweiterung oder mobile App sicher auf ihre Anmeldeinformationen zugreifen können. Über die App haben Benutzer sogar sicheren Zugriff auf ihre Daten, wenn die Internetverbindung schlecht oder unterbrochen ist.

Fachhandelspartner:

Kiel-IT GmbH
Hamburger Chaussee 169
24113 Kiel

0431-57085500
vertrieb@kiel-it.de