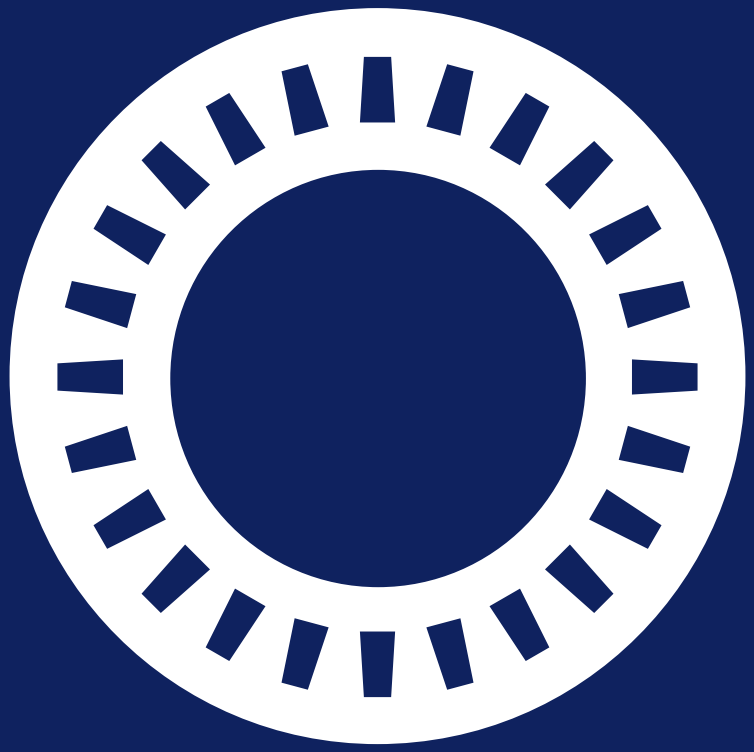
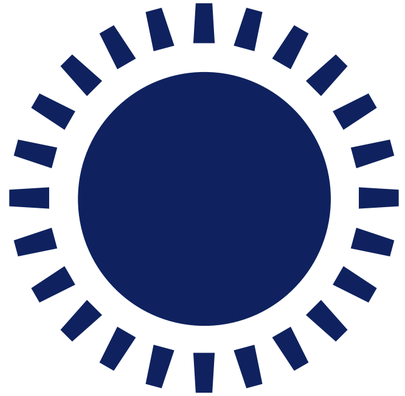




PASSWORD SAFE
by MATESO

Passwörter verschaffen Zugang zu Informationen.

Nur wem?

Passwörter sollen Zugänge vor unberechtigten Zugriffen durch Dritte schützen. Aber sind Sie sicher, dass jeder, der in Ihre passwortgesicherten Bereiche eindringt, dazu auch autorisiert ist? Hacker können Zugänge in Bruchteilen von Sekunden knacken. Wussten Sie, dass Deutschland unter den Top 6 der Länder ist, die am meisten angegriffen werden? Allein auf die IT-Infrastruktur der Bundesregierung finden täglich rund 3000 Cyber-attacken statt. Password Safe hilft Ihnen Ihre Daten mit hochmoderner Verschlüsselungstechnologie zu schützen.

13 Min.
PIXAR
Senior Director
PW:webp4c

6 Minuten
BBC
Manager
PW:[firstname]1985

0,02 Sekunden
NIKE
Global Director
PW:[firstname]

5 Min.
Senior Director
PW:wuxi6969

0* Sekunden
IBM
Senior Manager
PW:123456

12 Min.
PayPal
Senior Engineer
PW:ez1422

2,5 Sekunden
Former Senior
PW:s3ash311

Senior Director
PW:123[yearofbirth]

0,07 Sekunden

Manager
PW:[firstinitialanddob]

4 Min.

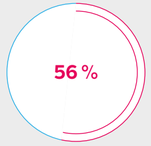
* **So lange hat es gedauert, bis diese Passwörter entschlüsselt waren.**

Quelle: http://wpengine.com/unmasked/

Es geht um Verantwortung.

Werden Sie dieser gerecht?

Ihre Unternehmensdaten sind Ihr Kapital. Man sollte meinen, dass gerade die marktführenden Unternehmen diesen Satz verinnerlicht haben und für ein Maximum an Sicherheit sorgen. Der Datenschutz ist in Deutschland per Gesetz geregelt, wer gegen ihn verstößt dem drohen empfindliche Strafen. Aber was verstehen wir unter Daten? Sind Daten wirklich »nur« Informationen, die ein Computer verarbeitet, oder verbirgt sich hinter dem Begriff nicht viel mehr – nämlich Ideen, Entwicklung, Forschung, Firmengeheimnisse, Expertise, Erfahrung, Leidenschaft und manchmal auch ganze Lebensgeschichten? Dies gilt es zu schützen: mit hoch komplexen Passwörtern, generiert durch Password Safe.



nutzen das gleiche Passwort für berufliche und private Zwecke!

1 von 7 würde sein Passwort an Dritte verkaufen!

geben ihr Passwort an Teammitglieder weiter

1 von 5 wurde schon einmal Opfer einer Datenpanne

Die Gewohnheitsfalle

Mit dem rasanten Fortschritt in der Computertechnik steigen auch die Ansprüche an die Datensicherheit. Die gesetzlichen Anforderungen werden stets den aktuellen Gegebenheiten angepasst und über Ländergrenzen hinaus geregelt – 2018 wird das Bundesdatenschutzgesetz von der EU-Datenschutzgrundverordnung abgelöst. Keine leichten Voraussetzungen für die zuständigen Datenschutzbeauftragten und Administratoren! Denn ihre Aufgabe ist es, die gesetzlichen Vorschriften umzusetzen und die Sicherheit im Unternehmen in Einklang mit einer einfachen Bedienbarkeit durch die Mitarbeiter zu bringen. Diese müssen sensibilisiert sowie die Sicherheit an heiklen Punkten durch die entsprechende Software maximiert werden.

Password Safe hilft Administratoren bei der automatischen Absicherung der Zugänge durch privilegiertes Password Management und unterstützt den Anwender mit einer benutzerfreundlichen anpassbaren Oberfläche.

Albtraum Datendiebstahl

Stellen Sie sich vor, Ihre direkten Mitbewerber halten Ihre vertraulichsten Firmeninterna in den Händen. Ein Albtraum! Das Thema Datendiebstahl bringen die meisten in direkten Zusammenhang mit einem Hackerangriff. Der Gedanke liegt nahe, denn täglich fallen die Daten unzähliger Unternehmen in die Hände von Cyberkriminellen. Tatsächlich aber lauern die größten Gefahren für einen Datendiebstahl in den eigenen Reihen. Mitarbeiter, die unzufrieden sind, die gekündigt wurden oder vielleicht sogar Geld für die Weitergabe von Firmendaten bekommen. Sie als Unternehmer könnten in diesem Fall einen irreparablen finanziellen oder Imageschaden erleiden.

Password Safe schützt vor Datendiebstahl, indem brisante Zugänge mit einem Mehr-Augen-Prinzip abgesichert sind. Der Abruf eines Passworts ist somit nur mit der Freigabe von einer oder mehreren Personen möglich. Zusätzlich werden alle Aktionen protokolliert, so dass Sie als Unternehmer für externe Audits gerüstet sind.

»Der menschliche Faktor wirkt sehr zuverlässig. Alle Fehler, die man machen kann, werden gemacht.«

Bengt Beckman
schwedischer Kryptoanalytiker

Machen Sie den Test …

- Nutzen Sie einen teamfähigen Passwort Manager?
- Werden Ihre Daten lokal gespeichert?
- Ist die Rechteverwaltung bis auf Feldebene geregelt?
- Können bereichsübergreifend Berechtigungen vergeben werden?
- Gibt es ein Reporting System für Sicherheitsaudits?
- Ist ein Mehr-Augen-Prinzip gewährleistet?
- Ist eine ausfallsichere Konfiguration möglich?
- Sind die Passwörter komplex und einzigartig sowie automatisch generiert?
- Können Passwörter automatisch mit einem Single-Sign-On-Agent eingetragen werden?
- Übernimmt Ihr Passwort Manager nicht nur das Speichern von Dateien und Anhängen sondern verschlüsselt diese zugleich?
- Werden wichtige Accounts durch eine Mehrfaktor-Authentifizierung geschützt?
- Ist der Firmensitz des Herstellers in Deutschland, damit Sie von den strengen Datenschutzbestimmungen profitieren?

… und verwalten Sie Ihre Passwörter sicher!

Passwörter müssen sicher sein, gesetzliche Datenschutzbestimmungen eingehalten und der menschliche Faktor als Sicherheitsrisiko möglichst ausgeschlossen werden. Diesen hohen Anforderungen kann ein Unternehmen nur mit einem professionellen Password-Management-System gerecht werden.

Vertrauen ist gut. Sicherheit ist besser.

Vertrauen Sie Ihren Mitarbeitern. Aber nicht beim Thema Sicherheit!
Schon allein die Bezeichnung »vertrauliches« Passwort offenbart die Problematik: nämlich die menschliche Komponente im Zusammenhang mit der Sicherheit. Vertrauen setzt eine persönliche Ebene voraus, aber kein Unternehmer weiß, wie es in seinen Mitarbeitern wirklich aussieht. Sind sie auch loyal, wenn es mal zu Spannungen kommt? Heutzutage ist es kinderleicht Informationen auf illegalem Weg über das Darknet zu verkaufen. Password Safe kann vor Datendiebstahl schützen, indem brisante Zugänge speziell abgesichert werden.

Scheinbar sichere Passwörter sind leicht zu entschlüsseln

Beliebt: Einfach ein paar Zahlen dahinter setzen:

passwordexample**1**	23.84 %
passwordexample**2**	6.72 %
passwordexample**3**	3.86 %
passwordexample**4**	3.19 %
passwordexample**5**	3.35 %

So schnell werden Passwörter geknackt:

FyD*8f	**ca. 5 Sek.**
W!bCvm)5	**ca. 9 Std.**
(UN?v*UG7p!9	**ca. 485 Jahre**

Beispielrechner mit 4 Milliarden Passwörtern pro Sekunde inkl. Wörterbuch.

Die Top 5 der am meisten benutzten Passwörter:

1. **123456**
2. **password**
3. **12345678**
4. **qwerty**
5. **123456789**

12qwasyx

Tastatur-Pattern sind leicht zu durchschauen.

Schlechte Passwörter sind tickende Zeitbomben

123456 … Passwort geknackt. Oftmals reichen Bruchteile von Sekunden aus, um Passwörter zu entschlüsseln – je unsicherer sie sind, desto schneller geht es. Den Wenigsten ist die Brisanz sicherer Passwörter bewusst. Nur so ist zu erklären, dass die schlechtesten Passwörter zugleich die sind, die am häufigsten verwendet werden. Sie sind einfach zu merken und noch viel leichter zu hacken. Ein Passwort mit weniger als 6 Zeichen gilt schon lange nicht mehr als gut und auch 8 Stellen sind als unsicher einzustufen. Erst ab 12 Zeichen, mit Groß- und Kleinschreibung sowie Sonderzeichen wird ein Passwort wirklich sicher. Tendenz steigend!

Password Safe erstellt für jeden Account ein sicheres Passwort, das einzeln hochgradig verschlüsselt ist. Passwortrichtlinien und Generatoren erhöhen zudem die Sicherheit.

Social Engineering – jeder hinterlässt Spuren

Cyberkriminelle greifen Mitarbeiter in Unternehmen oft ganz gezielt an, indem sie sich persönliche Informationen über den Menschen zu Nutze machen. Das geht ganz einfach, da viele Angestellte große Teile Ihrer Privatsphäre in sozialen Netzwerken preisgeben. Diese Informationen sammeln die Angreifer via Social Engineering. Je mehr sie herausfinden, desto leichter kann ein Passwort-Rate-Angriff durchgeführt werden und der Zugriff auf vertrauliche Daten ebenso einfach wie unbemerkt erfolgen. 79 % der gehackten Accounts gehen auf das Konto von Social Engineering Angriffen! Wird die Cyberattacke entdeckt, ist es schon zu spät. Neben dem Datenverlust sind die finanziellen Schäden für das Unternehmen enorm.

Password Safe generiert automatisch Passwörter, die nicht einmal der Rechteinhaber kennen muss. Brisante Informationen werden speziell verschlüsselt und durch das Mehr-Augen-Prinzip geschützt. Brute-Force-Angriffe sind damit aussichtslos.

Sicherheit ist keine Option.

Sicherheit ist ein Muss!

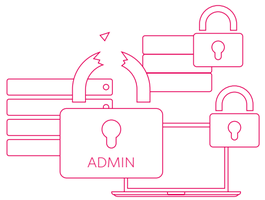
Denken Sie jetzt nicht, die Großen machen es besser. In den USA war das Passwort für die dort stationierten Minuteman-Atomraketen vermutlich über zwanzig Jahre die vollkommen banale Zahlenkombination 00000000. Damit wäre die nukleare Vernichtung großer Teile unseres Planeten quasi per Knopfdruck möglich gewesen. Solche Beispiele sind für uns kein Maßstab, aber Sie treiben uns an, die Welt ein bisschen sicherer zu machen. Es gibt noch viel zu tun. Packen wir es an!

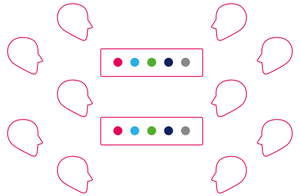
Schwachstelle der IT

Service Accounts und administrative Zugänge sind zentrale Schwachstellen im Unternehmen. Typischerweise besteht eine IT-Infrastruktur aus einer Vielzahl von Servern, Datenbanken, Netzwerkgeräten und Druckern. Diese werden über persönliche, generische und sogar lokale Admin Accounts gesteuert und verwaltet. Gerade diese privilegierten Accounts wurden in letzter Zeit vermehrt als Einfallstor für Datensabotage und -diebstahl genutzt: sowohl von Insidern wie auch von Cyberkriminellen.

Identische Passwörter

Oftmals werden für verschiedene Accounts die gleichen Passwörter verwendet und diese über einen langen Zeitraum nicht verändert. Das ist insofern nachvollziehbar, weil praktisch, aber im Sinne der Sicherheit nicht vertretbar. Eine große Gefahr besteht bei sogenannten Shared Accounts, bei der eine Gruppe von mehreren Administratoren das identische Passwort nutzt, um auf das System zuzugreifen und es zu verwalten – beispielsweise bei Windows oder Datenbanksystemen wie MSSQL. Jede Nachvollziehbarkeit geht verloren, obwohl sie zwingend wäre.





»Die sichere Verwaltung der administrativen Benutzerkonten gehört zu den größten Herausforderungen der heutigen IT.«

Christian Strobel
COO | MATESO GmbH

Gefahr im Klartext

Passwörter werden gerne Im Klartext via E-Mail und Chat verschickt oder auf handschriftlichen Zetteln übergeben. Aber was passiert dann mit diesen Notizen und wer kann die E-Mails außerdem noch lesen? Meist handelt es sich dabei um Passwörter, die für einen Service-, Software- oder Application Account vergeben werden und Nutzer autorisierten Zugriff zu bestimmten Anwendungen haben. Jedoch können auch unbefugte Personen so problemlos auf das System zugreifen und sensible Unternehmensdaten anzapfen – und zwar, ohne dass dies überhaupt bemerkt wird. Außerdem ist die Weitergabe der Daten nicht protokolliert und weder nachvollziehbar, noch für Audits verfügbar.

Entdecken & Managen

Password Safe analysiert das Unternehmensnetzwerk, ermittelt rechtebezogen alle Service Accounts, liest die Daten zügig ein und generiert automatisch sichere Passwörter. Jedes Passwort ist komplex und hochverschlüsselt und wird in regelmäßigen zeitlichen Abständen neu generiert und ausgetauscht.

Kein unbefugter Zugriff

Password Safe schützt die Passwörter privilegierter Accounts, optional auch durch ein Hardware-Sicherheits-Modul (HSM). So wird verhindert, dass sich Mitarbeiter unbefugten Zugriff verschaffen. Nicht nur Service Accounts auch sämtliche Endgeräte, Software und Logins werden unterstützt.

Audits: Kontrolliert protokolliert

Password Safe protokolliert durch das Managen der privilegierten Accounts alle Aktivitäten. Der Schutz von vertraulichen Informationen ist dadurch gewährleistet. Selbst bei einem Passwortzugriff – wie dem Aufdecken des Passworts durch einen Mitarbeiter – kann über das Benachrichtigungssystem der zuständige Verantwortliche unmittelbar informiert werden.

Der Service Account: Einfallstor für Cyberattacken.

Ein guter Angreifer sucht sich immer den schwächsten Punkt. Ein beliebtes Ziel von Cyberangriffen sind Service Accounts und Zugänge von Administratoren. Diese haben oftmals identische Passwörter, die quasi nie geändert werden. Solche Benutzerkonten sind besonders schützenswert, da neben den firmeninternen Daten auch Kundendaten auf dem Spiel stehen. Generische, persönliche oder lokale Admin Accounts bieten nicht die nötige Sicherheit. Zudem macht die Vielzahl von Servern, Datenbanken und Geräten dies zu einem außerordentlich aufwendigen Unterfangen. Password Safe generiert zuverlässige Passwörter – immer wieder neu.

23 gute Gründe für Password Safe

1 Ende-zu-Ende Verschlüsselung

Die Daten werden hierarchisch verschlüsselt in einer offenen Datenbank abgelegt. Weder der Administrator noch unbefugte und unerwünschte Dritte haben die Möglichkeit Passwörter aus der Datenbank auszulesen oder zu kompromittieren.

2 Rechte bis auf Datensatzfeldebene

Innerhalb von Password Safe können Berechtigungen bis auf Datensatzfeldebene vergeben werden. Bereichsübergreifende Passwörter sind somit kein Problem mehr, ebenso wenig wie Dubletten, da Rumpfinformationen wie Beschreibungen und Benutzernamen abrufbar sind.

3 Password Discovery & Reset

Password Safe macht durch das Managen der privilegierten Accounts jedes Unternehmen in Sachen Sicherheit zukunftsfähig. Alle Aktivitäten werden protokolliert. Selbst im Falle eines unerwünschten Passwortaustauschs würde eine schnelle Neukonfiguration die Sicherheit wiederherstellen.

Best in Class

4 Mehr-Augen-Prinzip (Siegel)

Password Safe unterstützt das Mehr-Augen-Prinzip bereits seit 2003. Damals war es eines der ersten Produkte mit derartiger Funktion. Jahrelange Erfahrungen in diesem Bereich machen unser Mehr-Augen-Prinzip zum Sichersten seiner Klasse.

Best in Class

5 Single-Sign-On Engine

Password Safe kann Windows Anwendungen, Remote Desktops oder SSH Verbindungen ebenso komfortabel verwalten wie Internetseiten. Die automatische Eintragung sowie der Login ohne das Aufdecken des Passworts sind unverzichtbar.

6. **Session Recording und Monitoring**
7. **Mandanten- und hostingfähig**
8. **Temporäre Freigaben**
9. **Anpassbare Dashboards**
10. **Filter- und Volltextsuche**
11. **Tag System zur Datenklassifizierung**
12. **API Schnittstelle**
13. **Active Directory Integration**
14. **Automatische Reports**
15. **Passwortrichtlinien und Generator**
16. **Mehr-Faktor-Authentifizierung**
17. **Sichere Dokumentenablage**
18. **Anpassbare Eingabemasken**
19. **Offline-Modus**
20. **Stateless Multi-Tier-Architektur**
21. **Hochverfügbar über Clustering**
22. **Verteilte Standorte über Replikation**
23. **Sicherheitsstufen sowie vererbbare Einstellungen über Organisationsstrukturen**

Harte Fakten?
Haben wir mehr als genug.

Vertrauen Sie auf den Marktführer. Überall müssen Passwörter vergeben werden. Sicher sollen sie sein, mindestens 12-stellig, mit Groß- sowie Kleinschreibung und Sonderzeichen; am besten für jeden Account ein anderes und in kurzen zeitlichen Abständen ein neues usw. Das ist privat schon kaum umsetzbar und in großen Firmen schwer zu realisieren. Password Safe ist flexibel in bestehende Strukturen integrierbar und äußerst anpassungsfähig. Das spart Ressourcen und ist effektiv. Mittlerweile vertrauen über 10.000 Firmenkunden auf MATESO – den Marktführer in Deutschland, Österreich und der Schweiz.

19

der Top 30
Dax-Unternehmen
vertrauen auf
Password Safe

10.000+

Unternehmen
weltweit arbeiten
mit Password Safe

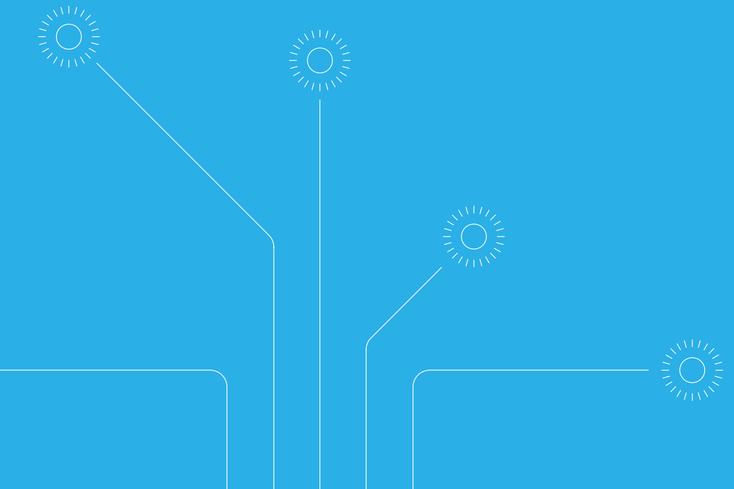
1998

Start der
Erfolgsgeschichte
von Password Safe

Warum wir das können?
Aus Erfahrung wird man gut.

Ohne Weiterentwicklung kein Wachstum. Weltweit setzen mehrere Millionen User Password Safe ein, 19 der Top 30 DAX Unternehmen vertrauen auf uns. Warum? Weil Selbstkritik und Selbstoptimierung Teil unserer Philosophie sind. Wir hören nicht auf zu suchen, nach den kleinsten Funktionen, die man verbessern könnte, nach Technologien, die einen weiter bringen, nach Entwicklungen, die es noch nie gab. Unsere Konzepte sind keine Utopie, wir überprüfen sie bereits in der Design-phase auf Machbarkeit und Sicherheit – alles im Mehr-Augen-Prinzip. Nur so können wir Qualität erarbeiten und Sicherheit versprechen.

Komplexe Strukturen brauchen sichere und produktive Systeme.



Mit zunehmend komplexer werdenden Strukturen im Unternehmen bekommt auch das Thema Sicherheit mehr und mehr Relevanz. Die System-Administratoren haben eine große Verantwortung gegenüber der Datensicherheit im Unternehmen, denn die Konfiguration von Firewalls, Servern und Zugängen ist ein sehr sensibles Aufgabengebiet. Password Safe vergibt Berechtigungen rollenbasiert bis auf Datensatzfeldebene.

Durch die nativ integrierten Verbindungsmöglichkeiten wie RDP oder SSH sowie der automatischen Eintragung (SSO) können sich die Administratoren mit komplexen Passwörtern effektiv authentifizieren. Zudem ermöglicht Password Safe die Nutzung der Daten zur automatischen Anmeldung, und zwar ohne dass der Anwender das Passwort überhaupt einsehen kann. Automatische Reports informieren die Benutzer periodisch per E-Mail über die Aktualität der Daten. Selbstverständlich gibt es die Möglichkeit Passwörter automatisch - bei Zugriff oder nach Ablauf – zurückzusetzen. So sind die Service Accounts geschützt.

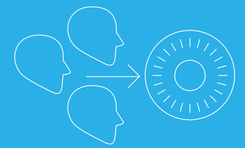
Password Safe bringt Sicherheit in komplexe Strukturen und gewährleistet produktive Abläufe.

Integrierter Remote-Desktop und SSH Client

Verwaltung und Kontrolle sämtlicher RDP und SSH Verbindungen. Protokollierter Zugriff gemäß der frei konfigurierbaren Berechtigungen.

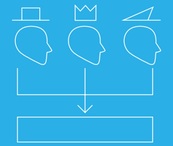
Temporäre Freigaben

Zeitlich befristete Berechtigungen für Benutzer und Rollen. Optimal im Vertretungsfall anwendbar.



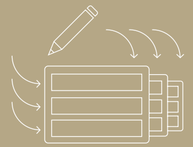
Active Directory Integration (LDAP)

Übernahme von bestehenden Benutzer- und Gruppenstrukturen aus dem Active Directory. Automatische Synchronisation der Benutzer und dessen Mitgliedschaften.



Flexible Rollen und Rechteverwaltung

Rollenbasierte Organisation der Datenbank. Die Rechtevergabe auf Benutzer und Daten ist individuell konfigurierbar.

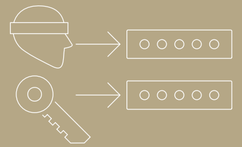


Anpassbare Datenstruktur

Freie Gestaltung der Formularfelder und Eingabemasken. Dies ermöglicht eine flexible Anpassung an jede Firmenstruktur.

Offline-Funktionalität

Passwortverwaltung auch ohne Verbindung zum Server. Die Synchronisation der Änderungen erfolgt nach Reintegration in das Netzwerk im Hintergrund.



Automatische Eintragung ohne Passwort aufdecken

Sichtsperre auf schützenswerte Passwörter. Je nach Konfiguration kann das Passwort via Single-Sign-On Agent verdeckt eingetragen werden.

Dokumentenverwaltung

Dokumente können verschlüsselt und versioniert in der Datenbank abgelegt werden. Eine Verknüpfung mit Passwörtern ist ebenso möglich.

Eine kompetente Verwaltung von Daten in Systemhäusern ist äußerst komplex, denn es muss nicht nur die Sicherheit der firmeninternen Informationen gewährleistet sein, sondern zugleich auch der Schutz aller Kundendaten. Die Einhaltung der gesetzlichen Vorgaben ist dabei zwingend und für ein umfassendes Password Management eine Herausforderung, insbesondere bei sehr großen Häusern.

Password Safe bietet eine sichere und zugleich effiziente Möglichkeit, die hoch verschlüsselten Daten zentral zu verwalten. Die anpassbare Datenstruktur ermöglicht das Erfassen von komplexen Kontaktinformationen und Passwörtern bis hin zu einfachen Lizenzdateien und Dokumentationen, die in die Datenbank geladen werden können. Zudem kann das Systemhaus die Password Safe Lösung auch seinen Kunden zur Verfügung stellen und diese sicher betreuen. Zugriffe werden stets protokolliert und dokumentiert.

Auf Passwörter, die bei Kunden vor Ort benötigt werden, kann der Mitarbeiter via Offline-Modus zugreifen oder alternativ mit dem WebViewer arbeiten.

Password Safe bietet durch die zentrale Verwaltung der Passwörter eine flexible und sichere Lösung für hochverschlüsselte Datenbanken.

Daten müssen zentral und flexibel verwaltet werden.

50 Hertz Transmission GmbH
Admiral Sportwetten GmbH
AEB GmbH
Airbus Defence and Space GmbH
Admiral Sportwetten GmbH
Allianz
AUDI AG
ALPLA Werke Alwin Lehner GmbH & Co KG
AXA Technology
Basler Fashion GmbH
Berliner Volksbank
Bertelsmann Sonopress
BKW Energie AG
BMW AG
Bonnfinanz
Bundesamt für Informatik u. Telekommunikation
Bundesamt für Naturschutz
Bundesamt für Seeschifffahrt und Hydrographie
Bundesministerium für Bildung und Forschung
Canon (Schweiz) AG
Commerzbank AG
Credit Suisse
Daimler AG
DAK
Dell
Deuter Sport GmbH
Deutsche Börse
Deutsche Post
Die Continentale
e.on
EADS
EDEKA ZENTRALE AG & Co. KG
Energie Steiermark Technik GmbH
Europcar
Fendt-Caravan
Flughafen Berlin
Flughafen München

Commerzbank AG

» Die Commerzbank ist das zweitgrößte Kreditinstitut in Deutschland und eines der bedeutendsten in Europa. Sie hat mehr als 60 Standorte in gut 50 Ländern und betreut rund 14 Millionen Privat- sowie 1 Million Geschäfts- und Firmenkunden weltweit. Zur Verwaltung von Zugängen, Identitäten und Passwörtern setzt die Commerzbank in Deutschland und Singapur das Produkt Password Safe and Repository der Firma MATESO ein. Die auf die Praxis sehr gut abgestimmten Funktionen wie Historie oder änderbare Formulare, sowie die gute Bedienbarkeit, ermöglichen ein effektives, zentrales und sicheres Management der Benutzerdaten einer Großbank. «

Marko Kiebitz
Application Manager | Stellvertretender Gruppenleiter

pcm GmbH

» Die pcm GmbH begleitet als erfolgreich und überregional agierendes IT-Systemhaus Kunden auf dem Weg in die d!conomy. Neben den durchdachten und dynamischen Lösungen der vier pcm-Geschäftsbereiche Telekommunikation, Dokumenten Management Systeme, Monitoring und IT-Infrastruktur spielt gerade im letztgenannten Bereich die Fernwartung eine bedeutende Rolle. Mit Password Safe haben wir die richtige Software gefunden, um unseren Kunden die höchste Sicherheit im Umgang mit vertraulichen und sensiblen Daten zu bieten. «

Ole Kollbach
Leiter Marketing

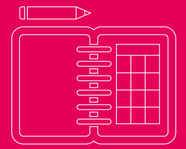
Flughafen Wien AG
flyeralarm Dienstleistungs GmbH
Frankfurter Sparkasse
Gemalto AG
Generali
Gerolsteiner Brunnen
GfK SE Data Services
GLS IT-Services GmbH
Hanseatic Bank Hamburg
Henkel
Hewlett Packard
HSR Hochschule für Technik Rapperswil
Hypo Vereinsbank AG
IG Metall
Industrie- und Handelskammer Dresden
Joey's Pizza International GmbH
Klinikum Nürnberg
Krombacher Brauerei
Landesamt für Steuern und Finanzen
Landesbank Berlin
Lidl
Linz AG
Löwen Entertainment GmbH
Luzerner Kantonsspital
MAN Diesel & Turbo SE
Marquardt Service GmbH
Messe Frankfurt
METTLER-TOLEDO International Inc.
Münchner Rückversicherung AG
NAVIGON AG
Neckermann
Netto
Nordex Energy GmbH
o2
Oberschwabenklinik
Olympic Airways
Österreichisches Generalkonsulat
Philip Morris Intl.
Philips
posterXXL GmbH
PricewaterhouseCoopers
ProSiebenSat.1
R + V Allgemeine Versicherung
RENK Aktiengesellschaft Augsburg
RICOH Schweiz AG
Rofin-Sinar Laser GmbH
RTL Radio Center Berlin GmbH
RWE
Salzgitter Flachstahl GmbH
Samsung
Securicor Geld- und Wertdienste
Sennheiser electronic GmbH & Co. KG
Siemens AG
Staatliche Toto Lotto GmbH
Südwestrundfunk SWR
TeamViewer GmbH
Thüringer Landesrechenzentrum
Thyssen Krupp
Tiwag Tiroler Wasserkraft AG
Toll Collect GmbH
T-Online International AG
TUI
Unitymedia
Universität Leipzig
Vodafone
Völkl Sports GmbH & Co. KG
Volksfürsorge
Volkswagen
WEKA MEDIA GmbH & Co. KG
Winterthur Versicherungen
yellowworld AG
Zuger Kantonalbank
uvm.

Aus der Praxis. Unsere Anwender.

Mehr Kundenstimmen unter
www.passwordsafe.de/anwenderberichte

Siegel

Es wird individuell festgelegt, wer im Mehr-Augen-Prinzip versiegelte Datensätze freigeben und brechen darf. Betroffene Personen werden automatisch über das Benachrichtigungssystem informiert.



Logbuch

Revisionssichere Protokollierung jeglicher Aktionen innerhalb der Datenbank. Effektive Auswertungen durch Einsatz granularer Logbuch Filter.

Session Monitoring

Tracking und Reporting von untyptischem Benutzerverhalten durch Password Safe inklusive automatischer Benachrichtigungen.

Datensatz Historie

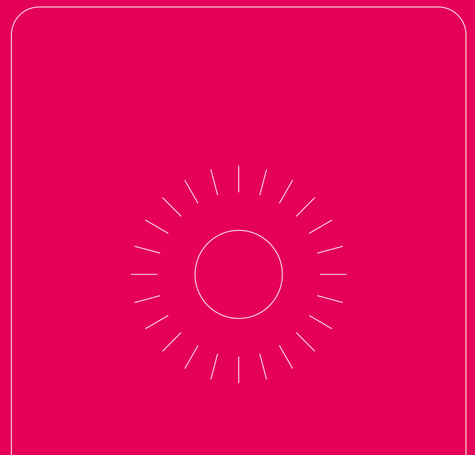
Vollkommene Transparenz durch Gegenüberstellung sämtlicher versionierter Datensätze. Jeglicher Datenstand kann wiederhergestellt werden.

Bankhäuser sind Hochsicherheitszonen – auch im Bezug auf den Datenschutz. Eine besonders hohe Verschlüsselung der Daten und deren Freigabe durch streng reglementierte Authentifizierungen von Personen gehören zu den Sicherheitsstandards. Mit Hilfe von Password Safe and Repository ist eine digitale und zugleich sichere Verwaltung der Passwörter gewährleistet. Passwortbriefe mit veralteten Passwörtern sind in einigen Banken zwar noch üblich, sollten aber längst der Vergangenheit angehören.

Unser Siegel-System beim Abrufen der Passwörter funktioniert über ein Mehr-Augen-Prinzip, das eine lückenlose Protokollierung ermöglicht. Das Abrufen eines Passworts kann nur über eine vorher definierte Freigabe erfolgen. Außerdem muss die Entnahme eines Passwortes durch eine oder mehrere digitale Unterschriften autorisiert werden. Bei einem Siegelbruch oder dem Öffnen bestimmter Passwörter kann auf Wunsch ein Sicherheitsbeauftragter via E-Mail informiert werden.

Password Safe gewährleistet die Sicherheit der Daten. Durch die digitale Passwortverwaltung werden Sicherheitsstrukturen in Ihrem Unternehmen entzerrt und die Flexibilität und Effizienz gesteigert.

Eine digitale und sichere Verwaltung der Passwörter muss gewährleistet sein.



Sicherheit muss praktikabel sein und Risikofaktoren ausschließen.

Jeder Mitarbeiter, der in Datensystemen arbeitet, muss sich zahlreiche Passwörter merken. Je komplexer die Systeme werden, desto größer die Herausforderung eigene Passwörter zu verwalten. Handgeschriebene Notizzettel und auf dem Server abgespeicherte Passwortdokumente oder schlicht äußerst einfach strukturierte Passwörter sind gern praktizierte Lösungen für diese Problematik.

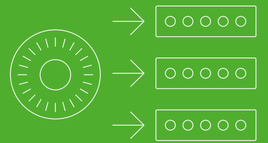
Vor allem die unzähligen Dienstkonten, die durch schlechte Passwörter »gesichert« sind, stellen ein großes Sicherheitsrisiko für das gesamte Unternehmen dar. Der automatische Passwort Reset erzeugt nicht nur hochverschlüsselte Passwörter, sondern generiert diese immer wieder neu, so dass ein maximaler Schutz der Zugänge stets gewährleistet ist. Mit Password Safe and Repository können alle Mitarbeiter ihre Daten sicher und zentral verwalten. Eine integrierte Rechteverwaltung stellt sicher, dass Mitarbeiter nur auf die Daten zugreifen können, für die sie zugangsberechtigt sind.

Gerade beim Firmenrollout steht die Skalierbarkeit der Software im Vordergrund – Password Safe wird auf mehreren Anwendungsservern und Datenbank-Clustern betrieben. Im Falle eines Ausfalls der Hardware übernimmt ein Backup-System die zuverlässige Wiederherstellung der Daten.

Password Safe entlastet Ihre Mitarbeiter und schützt Ihre Systeme automatisiert.

Dashboard

Frei konfigurierbare Dashboards geben je nach Modul sofortige Auskunft über wichtige Ereignisse.



Automatische Eintragung (SSO) via Agent

Automatisierte Eintragung an Internetseiten und Anwendungen via Single-Sign-On Agent auch ohne Verwendung des Hauptclients.

Auditing & Reporting

Tägliche, automatisierte Reports halten Sie auf dem Laufenden. Das Filtersystem unterstützt Sie bei der Auswahl der Daten.

Hochverfügbarkeit

Durch unsere Multi-Tier-Architektur ist eine Hochverfügbarkeit über Datenbankclustering und Loadbalancing der Anwendungsserver jederzeit möglich.

1

Kontrollierter durch Reports und Logbuch

Das interne Logbuch gibt Ihnen stets Überblick, wer auf welche Passwörter und Dokumente Zugriff hat. Auch bei wechselnden Arbeitnehmern behalten Sie die Kontrolle.

2

Stabiler durch Vermeidung von System-Resets

Ersparen Sie sich eine langwierige und kostspielige Wiederherstellung oder Neukonfigurationen von Systemen. Mit Password Safe geht kein Login mehr verloren.

3

Effektiver durch automatisierte Passworteintragung

Das automatische Eintragen von Passwörtern in Anmeldefeldern ist nicht nur sicherer, es ist auch schneller und kostensparend. Phising-Angriffe sind ausgeschlossen.

4

Sicherer durch komplexe Passwörter

Password Safe erstellt automatisiert komplexe und absolut sichere Passwörter. Das erhöht den Schutz Ihrer Systeme und damit die Sicherheit Ihrer Daten enorm. Außerdem entfällt der »Faktor Mensch« als größtes Sicherheitsrisiko. Die Anwender kennen die Passwörter nicht im Klartext.

5

Übersichtlicher durch zentrale Verwaltung

Die zentrale Passwortverwaltung sorgt für einen schnellen Zugriff und vermeidet das aufwendige wie langwierige Suchen und Verwalten von unsicheren Passwörtern in Tabellen oder auf Papier.

6

Beständiger durch anpassbare Strukturen

Password Safe passt sich den individuellen Gegebenheiten Ihres Unternehmens an und integriert sich einfach in bestehende oder wachsende Strukturen. Die flexible und gleichzeitig zentrale Datenstruktur ermöglicht eine zukunftsorientierte Ausrichtung.

Jeder kann effektiv sein.

Man muss nur seine Struktur überdenken.

Sicherheitslücken sind teuer. Das Wort »sicher« bedeutet stabil, erschütterungsfest, geborgen, definitiv, bestimmt und unbedingt. Für uns steckt hinter dem Begriff Sicherheit aber auch Effektivität. Effektiv zu sein, heißt optimal zu wirtschaften und die Zeit nicht mit unnötigen Dingen zu verbringen: wie mit Systemabstürzen, Neukonfigurationen und der Suche nach Zetteln. Denn das kostet neben Nerven auch Zeit und Geld und setzt zudem die Sicherheit Ihrer Daten aufs Spiel. Password Safe garantiert Ihnen absolut sichere Passwörter, die zentral verwaltet sind und durch die automatische Eintragung die Prozesse beschleunigt. Gleichzeitig fügt sich Password Safe in bestehende Strukturen ein und kann mit ihnen wachsen – das ist sowohl zeitlich als auch finanziell effizient und sicher zugleich. Versprochen.

Ihre Kosten im HelpDesk

100
Mitarbeiter

7
Anzahl der Passwortanfragen an den Helpdesk pro Mitarbeiter im Jahr

20,- €
Durchschnittliche Kosten pro Helpdesk-Anfrage

14.000,- €
Kosten pro Jahr

Ihre Kosten durch manuelle Passworteingabe

100
Mitarbeiter

8
Anzahl der Anmeldungen pro Mitarbeiter/Tag*

3.200,- €
Durchschnittsgehalt Mitarbeiter/Monat

9.777,78 €
Kosten pro Jahr

23.777,78 €
jährliche Gesamtkosten durch Helpdesk und manuelle Passworteingabe

Ihre Kosten für Password Safe Enterprise

100
Mitarbeiter

0
Anfragen im Helpdesk und kein Zeitverlust durch Anmeldungen

97,74 €
Kosten pro Mitarbeiter

9.773,75 €**
Anschaffungskosten

14.004,03 €
Return on Invest (ROI) im ersten Jahr

210 Tage
bis zum Break Even

*10 Sekunden für eine Passworteingabe bei 220 Tagen; ** inkl. Softwarepflege für 12 Monate / Preis zzgl. gesetzlich gültiger MwSt.
Quellen: http://passwordresearch.com/stats/statindex.html (PasswordResearch.com)
http://www.destatis.de/jetspeed/portal/cms/ (Statistisches Bundesamt Deutschland)

Kosten durch unsichere oder vergessene Passwörter

Schaden bei Datenverlust

unbezahlbar!

Sie würden Ihr Passwort Management gerne verbessern? Dann testen Sie uns doch! Natürlich kostenlos.
Melden Sie sich einfach unter **passwordsafe.de** zum Test an und laden Sie Password Safe herunter. Wir zeigen Ihnen in einem ausführlichen Webinar, wie Sie Ihr Passwort- und Identitäts-management besser und sicherer machen.

Sicherheit zahlt sich aus.
Schneller als Sie denken!

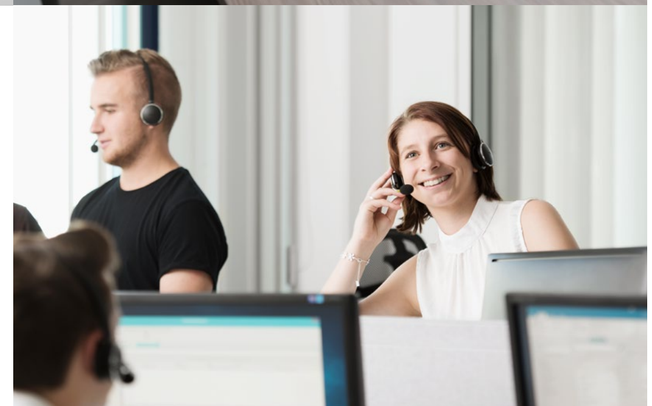
Password Safe zahlt sich aus – auch das ist sicher. Die Anschaffung sowie die Integration von komplexen Softwarelösungen in bestehende Strukturen ist immer ein großer Schritt für die Unternehmen. Zudem haben hervorragende Lösungen immer ihren Preis. Aber die primäre Frage sollte nicht lauten, »Was kostet das«?, sondern »Rechnet sich das«? Wir sind mit unserer Berechnung zu folgendem Ergebnis gekommen: Bei 100 Mitarbeitern sparen Sie 14.000 € bereits im ersten Jahr. Der Break Even beim »Return on Invest« ist schon nach 210 Tagen erreicht. Die Kosten für Systemausfälle aufgrund von Sicherheits-lücken und Datendiebstahl sind übrigens in der Kalkulation nicht berücksichtigt – wir dachten, es reicht auch so an guten Argumenten.

Thomas Malchar
CEO

Christian Strobel
COO

»Sicherheit ist für
uns keine Option.
Es ist ein Versprechen
an unsere Kunden,
für das wir täglich
hart arbeiten.«

Thomas Malchar
CEO | MATESO GmbH



Password Safe entstand bereits Ende der 90er Jahre aus einem konkreten Bedürfnis: Es gab zum damaligen Zeitpunkt keine Software, welche sich thematisch professioneller Passwortverwaltung widmete. Thomas Malchar, Geschäftsführer der MATESO GmbH, entwickelte daraufhin eine pragmatisch aufgebaute Anwendung, welche vorerst lediglich im eigenen Firmenumfeld genutzt wurde. Dass aus dieser Idee die Marktführerschaft im gesamten deutschsprachigen Raum wächst, war zu jenem Zeitpunkt noch nicht absehbar.

Aufgrund stetig ansteigender Nachfrage erkannte Thomas Malchar recht schnell das grenzenlose Potential und begann 2001 gezielt mit der Vermarktung von Password Safe. Ab 2006 bereicherte Christian Strobel, aktuell COO und Mitglied der Geschäftsleitung das Team aus Sicherheitsexperten.

Ohne jegliches Outsourcing vereint die MATESO GmbH die Geschäftsbereiche Entwicklung sowie Service & Support in den Neusässer Geschäftsräumen vor den Toren von Augsburg. Mit Version 8 wird das Vertriebskonzept auf die Distribution umgestellt. Der bis dahin innerbetrieblich gesteuerte Direktvertrieb wird hierdurch für den weltweit expandierenden Markt auf die Zukunft vorbereitet. Beim Personal verlässt man sich aufgrund der hochspezialisierten Anforderungen schon lange nicht mehr nur auf den Arbeitsmarkt. Die bedarfsgerechte Ausbildung von Fachkräften in den weitläufigen Geschäftsräumen mit modernster IT-Peripherie ist ein wesentlicher Schlüssel zum Erfolg.

Gute Ideen.
Dahinter stecken wir.

MATESO
technology on software

Service ist unser Geschäft, Perfektion unser Ziel und Ihre Zufriedenheit unsere Garantie. Stillstand ist für uns keine Option. Dafür sorgen die stetigen Rückmeldungen unserer Kunden. Sie bestätigen auf der einen Seite durch ihr Lob, das wir auf dem richtigen Kurs sind. Andererseits motivieren sie uns mit ihren Wünschen und Anregungen tagtäglich zur kundenorientierten Weiterentwicklung unserer Produkte. Es geht immer weiter.

Getestet.
Und für gut befunden.

Die Sicherheit steht stets an höchster Stelle. Aus diesem Grund wurde die SySS damit beauftragt einen Penetrationstest durchzuführen.

»Die SySS GmbH bewertet das Sicherheitsniveau der getesteten Softwareanwendung Password Safe and Repository 8 als sehr hoch. Die Vertraulichkeit sensibler Daten wie Passwörter und Dokumente wird dabei durch sichere kryptografische Verfahren und einen eingeschränkten Zugriff auf entsprechendes Schlüsselmaterial gewährleistet. Bezüglich der Schutzziele, Integrität und Verfügbarkeit konnte die SySS GmbH keine Schwachstellen finden.«

Sebastian Schreiber | Geschäftsführer SySS GmbH

SySS
THE PENTEST EXPERTS.

Die MATESO GmbH ist ebenso mit dem Produkt »Password Safe and Repository« Mitglied der TeleTrusT Initiative »IT-Security made in Germany« und bestätigt hiermit folgende Eigenschaften:

- Der Unternehmenshauptsitz ist in Deutschland.
- Das Unternehmen bietet vertrauenswürdige IT-Sicherheitslösungen an.
- Die angebotenen Produkte enthalten keine versteckten Zugänge.
- Die IT-Sicherheitsforschung und -entwicklung des Unternehmens findet in Deutschland statt.
- Das Unternehmen verpflichtet sich, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

D 2.2017 www.oup-kom.de

PASSWORD SAFE
by MATESO

MATESO GmbH
www.passwordsafe.de
info@passwordsafe.de
Fon +49 821 74 77 87-0