FREJA ID UNBEGRENZTE ZUGANGSBERECHTIGUNGEN
FREJA SSP VEREINFACHTE NUTZERREGISTRIERUNG
FREJA CONNECT CLOUD SINGLE SIGN-ON
FREJA MOBILE LOGIN UND TRANSAKTIONSSIGNIERUNG

DIE FREJA PRODUKT-FAMILIE

Verwaltung und Kontrolle des wertvollsten Guts in der digitalen Welt – Identität

VERISEC

FREJA | IDENTITY & ACCESS MANAGEMENT

FREJACONNECT
Seite 12

FREJAMOBILE
Seite 16

FREJAID
Seite 4

FREJASSP
Seite 8

FREJA FAMILIE

WERTE AUS DIGITALEN IDENTITÄTEN SCHAFFEN

In unserer heutigen Welt, in der wir immer vernetzt sind, sind unsere digitalen Identitäten ein Teil unseres Lebens geworden. Da wir immer wertvollere Daten und Güter über das Internet verwalten, können wir uns zum Schutz unserer digitalen Identitäten nicht länger auf herkömmliche Methoden verlassen. Feste Passwörter sind nicht nur unsicher, sie bringen auch teure Verwaltungsarbeiten für das Zurücksetzen der Passwörter mit sich und schränken die Möglichkeiten Ihres Unternehmens für die Verwaltung von Identitäten und Zugangsberechtigungen ein.

Die Freja Produktfamilie bietet Ihrem Unternehmen Tools zur Verwaltung und Kontrolle digitaler Identitäten im großen Rahmen:

- **Freja ID** ist ein Authentifizierungsserver auf Grundlage offener Standards. Er bietet eine Zwei-Faktor-Authentifizierung und generiert Einmalpasswörter.
- **Freja Selbstbedienungsportal** ist ein Tool für die Benutzerregistrierung und die Bereitstellung von Geräten.
- **Freja Connect** ermöglicht die Nutzung von Unternehmenszugangsberechtigungen für Cloud Single Sign-on.
- **Freja Mobile** ist eine Lösung der nächsten Generation für die mobile Authentifizierung und Transaktionssignierung.

In einer Welt, in der unser Berufs- und Privatleben von der Verknüpfung miteinander abhängt, bietet die Freja Produktfamilie die notwendigen Tools zur Verwaltung und Kontrolle des höchsten Guts in dieser digitalen Welt - der Identität.

Über Verisec

Seit 2002 ist Verisec Vorreiter im Bereich der digitalen Identitäten. In den frühen Tagen der Internetsicherheit waren Banken das Hauptziel für Angriffe und Verisec hat sich in bei Banken im nordischen Raum durch das Angebot neuester Sicherheitslösungen schnell einen guten Ruf erarbeitet. Das Wort der innovativen schwedischen Gesellschaft machte die Runde und wir konnten bald Kunden auf der ganzen Welt mit sicheren Identitäts- und Zugangsverwaltungslösungen helfen. Heute arbeiten wir mit einigen der weltgrößten Banken, Regierungen und Unternehmen zusammen und schützen und verwalten digitale Identitäten im Internet gemäß dem neuesten Stand der Technik.

FREJA ID

UNBEGRENTZE ZUGANGSBERECH-TIGUNGEN

Freja ID ist eine innovative Lösung für eines der größten Probleme des Internet-Zeitalters: Wie können Sie Identitäten, Zugänge und Berechtigungen für eine große Anzahl Nutzer sicher verwalten und gleichzeitig Lizenz- und Token-Kosten kontrollieren.

Freja ID wurde für die Verwaltung einer unbegrenzten Anzahl von Identitäten und Zugängen entwickelt. Es ermöglicht Ihrem Unternehmen, eine unbegrenzte Anzahl Nutzer, Anwendungen und Geräte zu festen Kosten zu verwalten. Freja ID bringt Ihnen die Sicherheit einer Zwei-Faktor-Authentifizierung mit einem einmaligen Passwort und wird von Regierungen, Unternehmen und Banken auf der ganzen Welt verwendet. Mitarbeiter erhalten über Freja ID einen sicheren Zugang zu internen Netzwerken. Das System kann aber auch einen sicheren Zugang in viel größerem Rahmen ermöglichen: für e-Commerce-Kunden, Spieler auf Spiele-Webseiten oder sogar für Bürger, die städtische Dienstleistungen in Anspruch nehmen.

Benutzerfreundlichkeit und Flexibilität

Für den Benutzer erleichtert Freja ID den Login-Vorgang erheblich, indem es das Merken komplexer Passwörter und Richtlinien zur Passwortänderung überflüssig macht. Freja ID beruht auf offenen Standards und kann mit allen hard- und softwarebasierten OATH-Tokens verwendet werden. Mit Freja ID haben Sie die Freiheit, für verschiedene Nutzer verschiedene Token-Arten auszuwählen und zu mischen.

Freja ID unterstützt Kerberos und kann verwendet werden, um die Authentifizierung mit AD-Passwörtern für den VPN-Zugriff zu erweitern. Dies kann einen wichtigen ersten Schritt der Standardisierung einer einheitlichen Passwortpolitik für den Zugriff auf alle Unternehmensanwendungen darstellen. Und in Kombination mit Freja Connect können Sie mit Freja ID eine einzige, einheitliche Passwortpolitik für interne und Cloud-basierte Anwendungen einführen.

Einfachheit als Standard

Montage und Integrierung von Freja ID erfordern keine langen, komplexen und kostspieligen Installationsprojekte. Die Einfachheit ist das Herzstück unseres Systems, da es nicht in laufende Prozesse eindringt und die in Ihren Verzeichnissen oder Benutzerdatenbanken gespeicherten

Daten wieder verwendet. Alles ist in der Lieferung enthalten und die typische Einrichtung dauert weniger als einen Tag. Unser Rekord liegt sogar bei nur 49 Minuten!

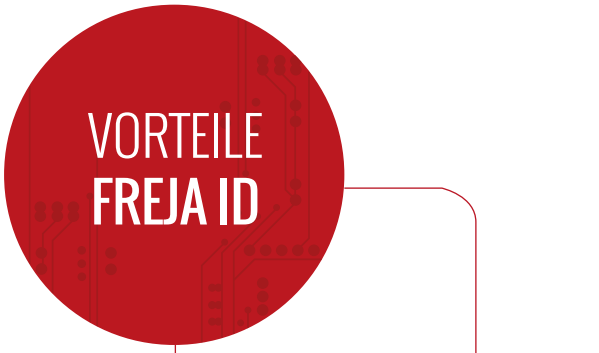
Die Lösung für Identitäten im großen Stil

Unabhängig davon, ob Sie sicheren Zugang für ein paar Hundert Mitarbeiter oder für über eine Million Kunden bereitstellen müssen - Freja ID ist die Lösung! Mit einer höheren Sicherheit gehen auch viele andere Vorteile einher: die Produktivität steigt, da empfindlichere Daten über das Internet verwaltet werden können und Verwaltungskosten gesenkt werden, da Passwörter nicht mehr länger vom IT Help Desk zurückgesetzt werden müssen. Auch ein einfacher Login-Vorgang kann den Gewinn steigern. Wenn Sie ein Portal haben, über das Kunden sich anmelden müssen, um Dienste in Anspruch zu nehmen oder etwas zu kaufen, halten vergessene Passwörter oder komplizierte Abläufe beim Zurücksetzen des Passwortes Ihre Kunden tatsächlich davon ab, Geschäfte mit Ihnen zu machen.

Der Schutz digitaler Identitäten ist für den Schutz Ihrer digitalen Vermögenswerte unabdingbar. Die Folgen, wenn Sie Ihre Identitäten nicht schützen, können verheerend sein. Stellen Sie sich vor, was passiert, wenn kritisches Geschäftswissen gehackt wird. Oder die Auswirkungen auf Ihre Markenreputation, wenn alle Zugangsberechtigungen Ihrer Kunden nach einem Passwortraub im Internet veröffentlicht werden. Feste Passwörter sind Geschichte. Freja ID ist die Zukunft.

"DAS FREJA PRODUKT ERMÖGLICHT UNS DIE AUTHENTIFIZIERUNG VON MITARBEITERN, DIE VON MEHREREN ORTEN AUS ARBEITEN, UND ES IST AUSSERDEM FLEXIBEL UND SKALIERBAR GENUG FÜR EINE ERWEITERUNG IN DER ZUKUNFT - NICHT NUR INNERHALB UNSERES EIGENEN UNTERNEHMENS, SONDERN AUCH BEI UNSEREN SERVICE-PARTNERN."

ICT Projektmanager bei einem lokalen UK Rat

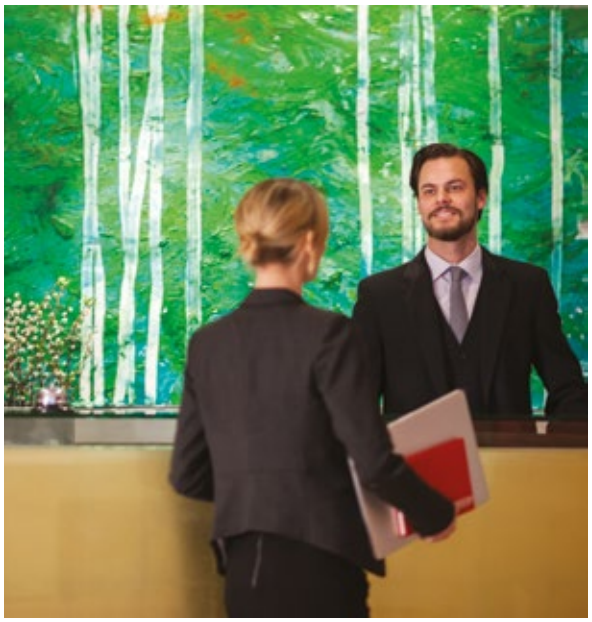


Nutzer

- Kein Ärger mit Passwörtern mehr
- Keine zeitaufwendigen Vorgehensweisen zur Passwortänderung notwendig
- Remote-Arbeit mit der gleichen Sicherheitsstufe wie vor Ort möglich

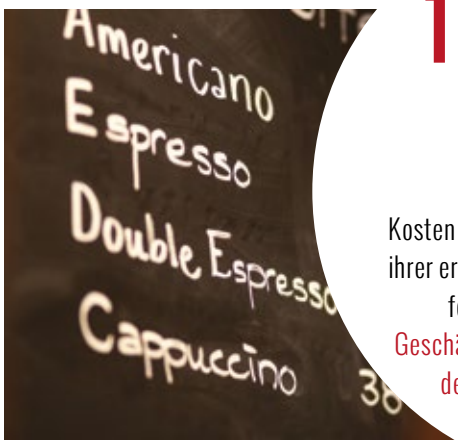
Unternehmen

- Unbegrenzte Lizenzen halten die Kosten unter Kontrolle
- Steigerung der Produktivität durch höhere Sicherheit
- Eingriffsfreie Integration mit mehreren Verzeichnissen
- API für eine einfache Integration mit Anwendungen
- Alles im Lieferumfang enthalten, einfach nur einstecken und los geht's
- Kompatibel mit allen OATH-basierten Tokens, einschließlich kostenloser Smartphone-Token
- Der flexible Sicherheitsmodus passt sich bestehenden Sicherheitsrichtlinien an.



171 million USD

Kosten für den 2011 Sony Playstation Hack ihrer ersten Benutzerkontendatenbank mit festen Passwörtern. Verlorene Geschäftsmöglichkeiten und Schädigung des Markenrufs sind dabei nicht berücksichtigt.



FREJASSP

EINFACHERE BENUTZERREGIS-TRIERUNG

Das Freja Selbstbedienungsportal ist eine Ergänzung zu Freja ID, die die sichere Benutzerregistrierung vereinfacht und dabei sicherstellt, dass die richtigen Berechtigungen für die richtige Hardware oder den richtigen Software- oder virtuellen Token bereitgestellt werden.

Wenn nicht die richtige Person die richtigen Zugangsberechtigungen für die Zugangsdaten ihrer Login-Tokens bekommt, ist es egal, wie sicher die Authentifizierungslösung ist. Der Schutz einer Identität kann einen hohen Verwaltungsaufwand bedeuten, wenn sie "manuell", d. h., von Angesicht zu Angesicht geschützt wird. In diesem Fall muss der Benutzer zu einem bestimmten Ort innerhalb des Unternehmens gehen und einen Identitätsnachweis vorzeigen, wonach er den Token bekommt, der dieser Identität zugewiesen ist. Auch, wenn diese Vorgehensweise sicher ist, ist sie sehr ressourcenaufwendig und übertrifft die Kosten der Authentifizierungslösung häufig bei Weitem.

Geringerer Kosten- und Verwaltungsaufwand

Das Konzept eines automatisierten Bereitstellungs-prozesses ist ein Meilenstein auf dem Weg zur Implementierung einer effizienten Authentifizierungslösung. Indem der Nutzer selber die Registrierung und die Bereitstellung des Tokens übernimmt, nimmt das Freja Selbstbedienungsportal dem Unternehmen eine Menge Verwaltungsarbeit ab. Es ist natürlich sinnlos, Nutzer ihre eigene Identität bestätigen zu lassen. Deshalb muss der Nutzer während der Registrierung einen Identitätsnachweis erbringen. Dies können die Anmeldedaten - Benutzername und Passwort - für bestehende Verzeichnisstrukturen sein. Wenn der Nutzer vorher noch keine Beziehung zu dem Unternehmen hatte, können diese in Form eines PIN-Codes per Einschreiben versendet werden, das nur nach Vorlage einer gültigen Identifizierung in Empfang genommen werden kann.

Vorteile für den Nutzer

Die Nutzer können von überall über einen Webbrowser auf das Freja Selbstbedienungsportal zugreifen und die Registrierung erfordert nur wenige Schritte und dauert weniger als fünf Minuten. Wenn die Verbindung zwischen dem Nutzer-Token und Ihrem Verzeichnis

hergestellt ist, hält das Freja Selbstbedienungsportal einen Kommunikationskanal mit dem Verzeichnis bereit, um Aufzeichnungen zu aktualisieren, Tokens zu ersetzen oder PIN-Codes zurückzusetzen, was der Nutzer auch direkt selbst erledigen kann. Für eine noch einfachere Nutzung können wir das Portal individualisieren und an den Stil und die Denkweise Ihres Unternehmens anpassen.

Vier einfache Schritte

Im Freja Selbtbedienungsportal erfolgt die Bereitstellung in vier sehr einfachen Schritten:

- **Auswahl:** Der Nutzer wählt den Gerätetyp aus (Hardware-Token, Google Authenticator etc.)
- **Registrierung:** Der Nutzer registriert einen Identitätsnachweis. Das können entweder ein Domain-Benutzername und ein Passwort oder eine Kombination von beidem mit einem zusätzlichen Identitätsnachweis sein (z. B. ein Einmalpasswort von einem bestehenden Authentifizierungssystem, von dem migriert wird)
- **Aktivierung:** Für Hardware-Geräte aktiviert der Nutzer den Token durch Eingabe der Seriennummer auf der Rückseite des Gerätes im Selbtsbedienungsportal. Für den Google Authenticator verwendet der Nutzer die Kamera seines Smartphones, um einen im Selbtsbedienungsportal angezeigten QR-Code einzuscannen.
- **Verifizierung:** Schließlich kann der Nutzer verifizieren, dass die oben genannten Schritte erfolgreich ein Sicherheitsgerät bereitstellen und dieses mit ihm oder ihr verbunden haben.

"DAS FREJA GERÄTE- UND SELBSTBEDIENUNGSPORTAL HAT UNS ERMÖGLICHT, EINE KOSSTENEFFEKTIVE, BENUTZERFREUNDLICHE AUTHENTIFIZIERUNGSLÖSUNG ANZUBIETEN, DIE SICH EINFACH IN UNSERE BESTEHENDEN SYSTEME INTEGRIEREN LÄSST."

ICT Infrastructure Team Leader bei einem lokalen UK Rat

VORTEILE FREJA SSP

Unternehmen

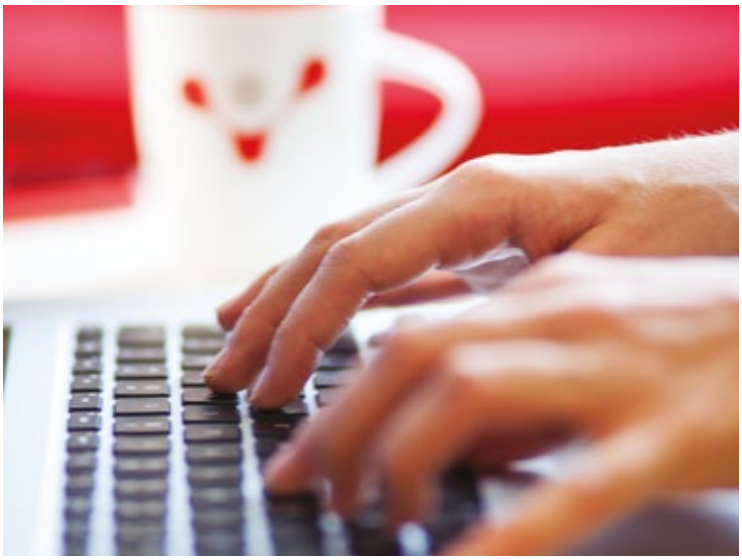
- Senkung von Kosten und Verwaltungsaufwand für die Nutzerregistrierung
- Einrichtung für große Nutzergruppen möglich
- Mit allen OATH-Token kompatibel; Hardware, virtuell und mobil
- Möglichkeit der Verwendung kostenloser Smartphone-Tokens, z. B. Google Authenticator
- Kundenindividuelle Gestaltung der Nutzerportaloberfläche
- Verlinkung zu internen Help Desks und Support-Teams möglich
- Unbegrenzte Lizenzen; Hinzufügen von Nutzern ohne zusätzliche Kosten

Nutzer

- Weniger Zeitaufwand bei der Registrierung (weniger als fünf Minuten)
- Möglichkeit, PIN-Codes ohne den Help Desk zurückzusetzen oder zu ändern

17%

aller Anrufe beim IT Help Desk betreffen das Zurücksetzen von Passwörtern (bei 22 USD pro Anruf gibt es hier ein großes Einsparpotenzial)



FREJACONNECT

CLOUD SINGLE SIGN-ON

Freja Connect ermöglicht Ihrem Unternehmen, wieder die Kontrolle über die Identitäten in der Cloud zu übernehmen, indem Nutzer Ihre Zugangsberechtigungen des Unternehmens auch für den Zugang zu Diensten außerhalb des internen Netzwerks verwenden können.

Heutzutage sind Cloud-Dienste ein normaler Bestandteil alltäglicher Abläufe im privaten und öffentlichen Bereich. Cloud-Dienste lösen viele Probleme, schaffen aber leider auch neue. Das Speichern kritischer Daten außerhalb des Unternehmensnetzwerks, geschützt nur durch schwache, feste Passwörter, die der Nutzer selbst festlegt, stellt ein Risiko dar. Fast 70 % der Nutzer verwenden das gleiche Passwort für mehrere Seiten - eine große Sicherheitssorge und ein Hinweis auf die Notwendigkeit, Identitäten in-house zu kontrollieren. Ob die Websites der Mitarbeiter mit ihrer Arbeit in Zusammenhang stehen, oder nicht - Ihre Geschäfte sind gefährdet, wenn Passwörter mehrfach verwendet werden. Wenn eine Seite gehackt wird, haben die Eindringlinge Zugriff auf alle Seiten, für die dieses Passwort verwendet wurde.

Wer hat die Kontrolle?

Was passiert wenn Ihre Mitarbeiter zwar strenge Passwort-Richtlinien einhalten, aber dann kündigen? Stellen Sie sich einen früheren Vertriebsvertreter vor, der immer noch Zugriff auf Ihr Cloud-basiertes CRM-System hat, wenn er eine neue Stelle bei einem Konkurrenten antritt. Mit Hunderten oder Tausenden Angestellten, von denen jeder eine Reihe von Cloud-Diensten nutzt, stehen Sie bei der Kontrolle des Zugriffs auf Ihre kritischen Daten vor großen Herausforderungen.

Aus Sicht der Nutzer ist die Verwaltung mehrerer fester Passwörter lästig, ganz zu schweigen von dem Stress, den das Zurücksetzen vergessener Passwörter mit sich bringt. Ein wichtiger Grund, warum viele das gleiche Passwort für mehrere Systeme verwenden.

Eine Identität kontrolliert sie alle

Freja Connect ist die Lösung für all diese Herausforderungen. Wenn Sie sich bei einem Cloud-Dienst anmelden, wird Ihre Authentifizierungsanfrage an Ihr internes Authentifizierungssystem weitergeleitet. Das bedeutet, dass Sie Ihre Zugangsberechtigungen des Unternehmens verwenden können. Das könnte der Nutzername und das Passwort für das Verzeichnis sein, aber natürlich auch ein 2FA-Hardware-Token oder eine mobile Anwendung - je nachdem, was Sie in Ihrem Unternehmen verwenden. Kurzum: Freja Connect gibt Ihrem Unternehmen die Kontrolle über die Identitäten und Zugänge innerhalb der Cloud zurück. Das bedeutet auch, dass die Nutzer eine einzige Identität für alle Zugänge haben und Sie einen einzigen Kontrollpunkt und eine Terminierungsstrategie haben.

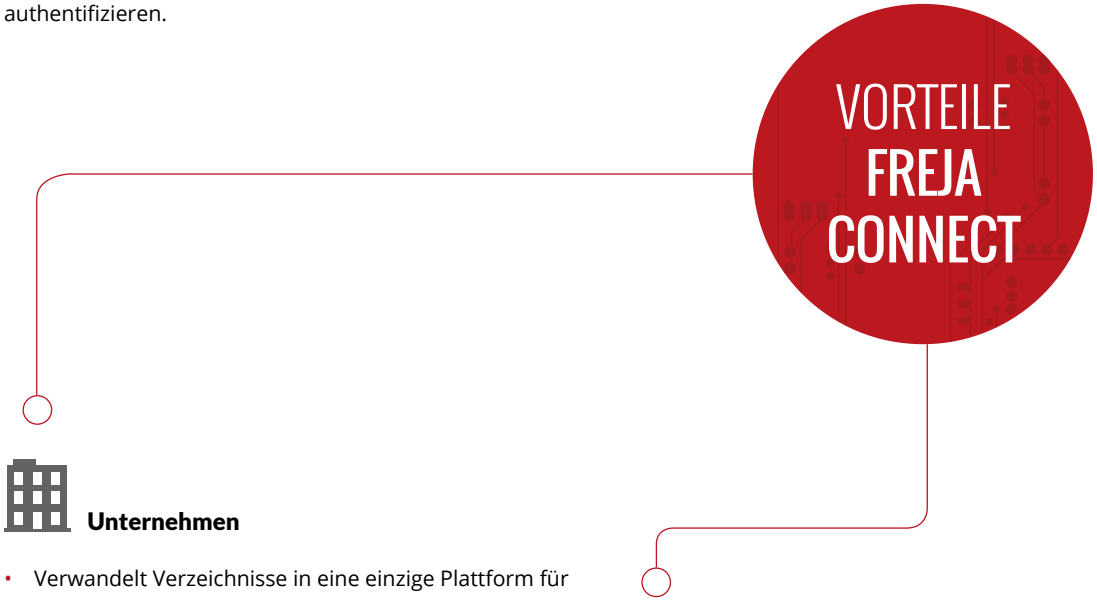
Sie gewinnen nicht nur die Kontrolle zurück, Sie steigern auch in vielerlei Hinsicht die Sicherheit. Wenn ein Cloud-Dienst, den Ihre Mitarbeiter verwenden, gehackt wurde, sind die Zugangsberechtigungen trotzdem noch in guten Händen, da sie sicher in Ihrem internen Netzwerk gespeichert sind. Außerdem sind Ihre bestehenden Passwortrichtlinien für die Cloud-basierte Authentifizierung ausgelegt. Außerdem bietet Freja Connect Ihnen die Möglichkeit, für den Zugang zu Cloud-Diensten eine Zwei-Faktor-Authentifizierung einzusetzen.

Einfache Bedienung für jeden

Freja Connect erleichtert dem Nutzer das Leben. Er muss nicht mehr den Überblick über Dutzende Passwörter behalten, sondern kann die Zugangsberechtigungen des Unternehmens überall verwenden. Die Funktion Web Single Sign-on ermöglicht dem Nutzer einen reibungslosen Workflow. Er kann zwischen verschiedenen Cloud-Diensten wechseln, ohne sich jedes Mal erneut zu authentifizieren.

Da Freja Connect Ihr bestehendes Authentifizierungssystem verwendet, lässt es sich schnell installieren und einfach konfigurieren. Die intuitive Nutzeroberfläche ermöglicht Administratoren einfaches Verwalten von Nutzern, Hinzufügen von Cloud-Diensten und Kontrollieren von Berechtigungen.

Das Cloud-Computing ist eine der größten technologischen Innovationen der heutigen Zeit und der Trend steht fest: eine stetig zunehmende Anzahl von Anwendungen und Diensten wird außerhalb des internen Netzwerks verwaltet. Große Nachteile sind jedoch der Verlust der Identitätskontrolle, die Sicherheitsrisiken fester Passwörter und die Ineffizienz durch das Verwalten mehrerer Zugangsberechtigungen. Jetzt gibt es eine Lösung für all diese Herausforderungen - Freja Connect.



Unternehmen

- Verwandelt Verzeichnisse in eine einzige Plattform für die Cloud-Identität
- Baut auf bestehenden Authentifizierungssystemen auf
- Erhöhte Sicherheit für in der Cloud gespeicherte Daten
- Verringert Kosten für die Verwaltung von Benutzerkonten
- Beschleunigt die Einrichtung von Cloud-Diensten
- Verhindert den Diebstahl von Identitäten
- Ermöglicht eine strenge Authentifizierung für Cloud-Zugänge
- Schafft einen einzigen Kontroll- und Terminierungspunkt

Nutzer

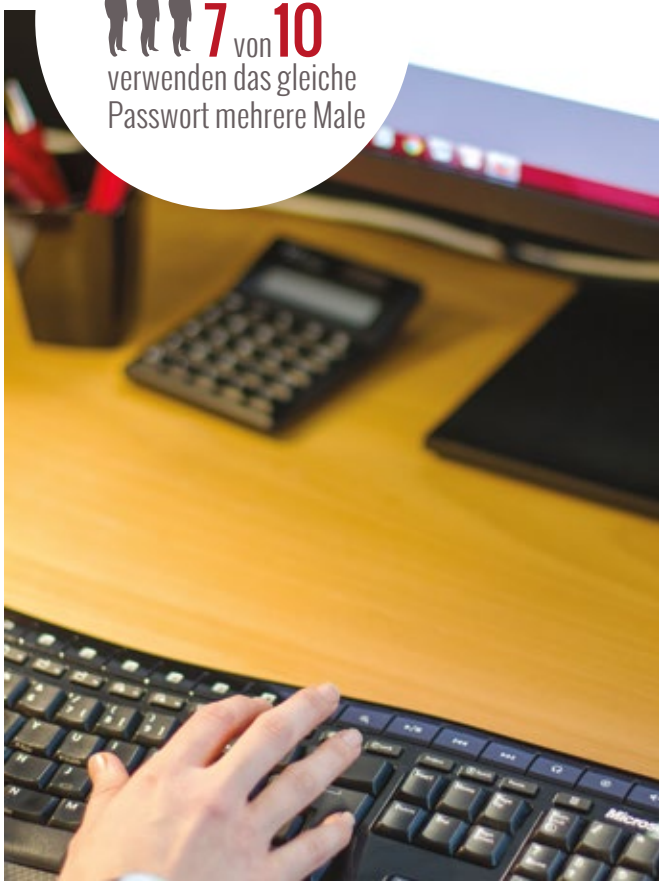
- Ein Login für alles
- Keine stressige Verwaltung mehrerer Passwörter mehr
- Single Sign-on steigert Produktivität und Komfort
- Spart Zeit beim Zurücksetzen von Passwörtern und geplanten Änderungen

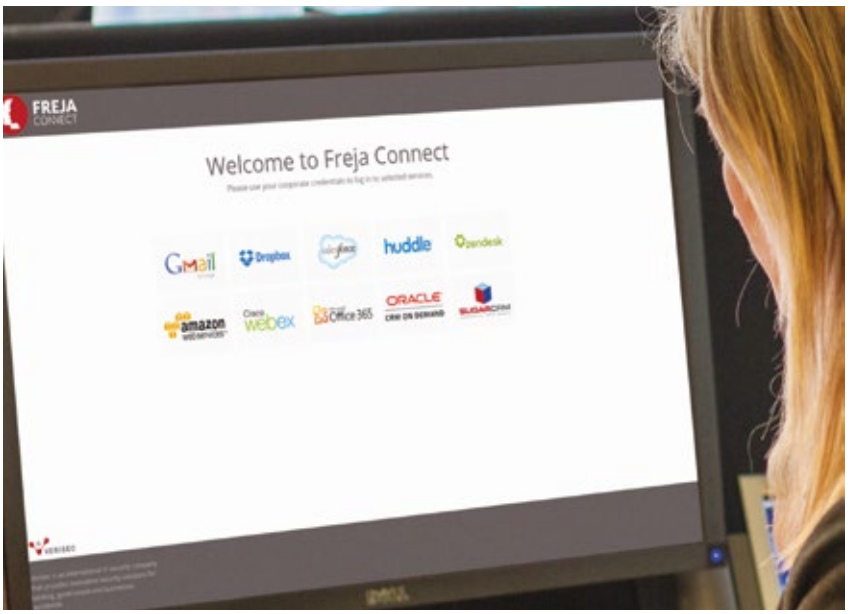
300%

Steigerung von Passwortdiebstählen 2012

7 von 10

verwenden das gleiche Passwort mehrere Male





FREJAMOBILE

SICHERE ANMELDUNG UND TRANSAKTIONS-SIGNIERUNG

Freja Mobile erfindet die Technologie für digitale Identitäten neu, die der Funktion von Smartphones wahrlich zum Durchbruch verholfen hat und bietet höhere Sicherheitsstufen und mehr Bedienkomfort für Anmeldung und Signierung.

Die traditionelle Methode zur Bewältigung der Sicherheitsrisiken von festen Passwörtern war die Verwendung von Hardware-Tokens, die ein Einmalpasswort generieren. Aber das Ersetzen all Ihrer verschiedenen Passwörter durch Hardware-Tokens wäre einfach nicht nachhaltig, wenn man die große Anzahl von Internetdiensten betrachtet, die wir heutzutage nutzen.

Eine neue Sicherheitsstufe

Mit der Einführung von Smartphones wurde eine neue Generation Passwort-Tokens geboren. Dabei wurden einfach die Funktionen eines Hardware-Tokens in eine mobile Anwendung gepackt. Diese Anwendungen generieren jedoch nur ein Einmalpasswort und das ist weit davon entfernt, der Tatsache gerecht zu werden, dass ein Smartphone ein stets verbundener Computer mit einem Bildschirm ist, der mehr anzeigen kann, als nur ein Passwort.

Freja Mobile ist die nächste Technologiegeneration für digitale Identitäten. Es nutzt die Eigenschaften von Smartphones, die eine ganz neue Sicherheitsstufe und höheren Bedienkomfort ermöglichen. Mit Freja Mobile zeigt Ihr Smartphone genau an, was Sie bestätigen, und welche Transaktionsart Sie signieren. Es löst auch die große Herausforderung der sicheren Bereitstellung von Smartphones über das Internet, indem es ermöglicht, eine große Anzahl Nutzer einfach und kostengünstig zu registrieren.

Intelligente Architektur

Freja Mobile besteht aus zwei Teilen - dem mobilen Authentifizierungsserver und der Smartphone-Anwendung. Es kann zum Login sowie für die Transaktionssignierung verwendet werden. Die Authentifizierung wird auf einem sicheren, separaten Kanal direkt an den genutzten Dienst weitergeleitet,

wodurch der Nutzer nicht mehr länger ein Passwort oder einen Code vom Mobiltelefon manuell an den Webbrowser übertragen muss. Dies eliminiert das Risiko von Man-in-the-Middle- und Man-in-the-Browser-Angriffen.

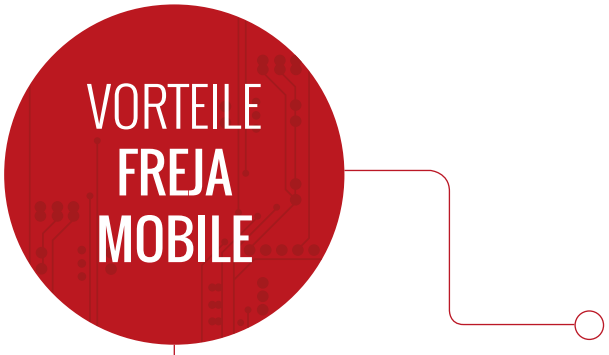
Entfernen der Passwörter

Aus Nutzersicht müssen Sie einfach nur Ihren Benutzernamen im Browser eingeben. Der mobile Authentifizierungsserver sendet dann über den sicheren Kanal eine Anfrage an das Mobiltelefon. Anstelle eines Einmalpasswortes erhalten Sie eine Nachricht, die genau beschreibt, wozu Sie gerade zustimmen. Beispielsweise der Name der Website, auf der Sie sich anmelden. Um die Anmeldung zu bestätigen, geben Sie einfach Ihren PIN-Code im Telefon ein und die Anmeldung wird über den sicheren Kanal verarbeitet.

Der gleiche Ablauf wird bei Transaktionssignierungen angewendet, wobei dem Nutzer eine Nachricht mit den genauen Einzelheiten zu der signierten Transaktion angezeigt wird. Das macht die Technologie sicher genug, um Geldtransaktionen und andere Transaktionen auszuführen, die die höchste Sicherheitsstufe erfordern. Die Freja Mobile-Technologie kann überall eingesetzt werden, wo feste Passwörter oder Tokens mit mehreren Faktoren verwendet werden. Dazu gehören Unternehmensnetzwerke, öffentliche Dienste, e-Commerce, Banking, Spiele und andere Dienste, wo eine Kombination aus hoher Sicherheit und Benutzerfreundlichkeit für große Nutzergruppen benötigt wird. Freja Mobile kann als Standalone-Anwendung oder in Ihre bestehenden Anwendung integrierte Komponente verwendet werden.

Eine Revolution für die Identität

Freja Mobile ist hinsichtlich der Benutzerfreundlichkeit wirklich revolutionär, aber der wirkliche Vorteil für ihr Unternehmen ist die Tatsache, dass es Mobiltelefone in ein vertrauenswürdiges Sicherheitsgerät verwandelt. Die zusätzliche Sicherheitsstufe, die der mobile Authentifizierungsserver bietet, verwandelt das Mobiltelefon in ein Gerät, das sicher für jede Art von Anmeldung oder Transaktion ist.



Nutzer

- Automatische Anmeldung und Transaktionssignierung
- Kein Ärger mit Passwörtern mehr
- Bessere Kontrolle durch "Sehen, was man unterschreibt"
- Wegfallen der manuellen Passworteingabe

Unternehmen

- Sichere mobile Geräte für Werttransaktionen und Anmeldung
- Bereitstellung einer großen Anzahl von Geräten über das Internet
- Schnellere Bereitstellung von Diensten, die einen sicheren Zugang erfordern
- Wegfallen des Aufwands zum Zurücksetzen von Passwörtern
- Vermeidung der Kosten für Hardware-Tokens
- Verhinderung von MiM-, MiB- und Phishing-Angriffen
- Ausschöpfen der geschäftlichen Möglichkeiten von Smartphones

Aktuell gibt es 6,8 Milliarden Menschen auf diesem Planeten. 4 Milliarden davon besitzen ein Mobiltelefon. Aber nur 3,5 Milliarden benutzen eine Zahnbürste.

Ihr Mobiltelefon hat eine höhere Rechenleistung als die Computer, die für dieMondlandung der Apollo 11 verwendet wurden.

KONTAKT

SCHWEDEN

sales@verisec.com

+46 8 723 09 00

VERINIGTES KÖNIGREICH

sales@verisec.com

0800 917 8815 (gebührenfrei)

Verisec AB, Box 2034, 131 02 Nacka, Schweden. sales@verisec.com. +46 (0)8 723 09 00. Telefon aus dem Vereinigten Königreich (gebührenfrei) 0800 917 8815

Weitere Informationen über Verisec und Kontaktinformationen unserer Büros im Vereinigten Königreich und in Serbien finden Sie auf www.verisec.com.