PRODUKT-
BLATT

FREJA®

STRENGE AUTHENTIFIZIERUNG FÜR SICHERE CLOUD-, NETZWERK- UND ANWENDUNGSANMELDUNG

Freja Authentication Appliance ist eine Komplettlösung für eine wirksame Authentifizierung für den sicheren Zugriff auf Cloud-Dienste und Unternehmensnetzwerke. Mit unserem einzigartigen Lizenzierungsmodell – ohne Pro-Nutzer-Kosten - können Sie eine unbegrenzte Anzahl von Personen authentifizieren und für größere Benutzergruppen zu niedrigen Kosten einen sicheren Zugang ermöglichen.

Wichtigste Vorteile

- Unbegrenzte Benutzerlizenzen senken die Authentifizierungskosten
- Unterstützt Hardware- und Mobiltelefon-SW-Tokens für alle Plattformen, USB-Tokens, PC- und Mac-Softwareclient-Tokens, SMS- und E-Mail-OTPs und PIN-Mailer
- Verwendung mit Google Authenticator möglich, wodurch keine Kosten für Tokens entstehen
- Lieferung als Hardware, virtuelle Lösung oder als gehosteter Authentifizierungsdienst
- Remote-Upgrade und -Verwaltung
- Einfache Installation –Rekordzeit : 49 Minuten
- Regelbasierte Zugriffsverwaltung abhängig von Gerätetyp und Nutzerzugriffspunkten
- Unterstützt Föderationen und einmalige Anmeldungen mit integrierter SAML-Maschine
- Basiert auf offenen Standards für die Authentifizierung (OATH)

Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung oder 2FA bezeichnet ein System, bei dem zwei Faktoren gemeinsam verwendet werden, um den Identitätsnachweis zu stärken. Weitverbreite Faktortypen sind beispielsweise:

Wissensfaktoren: Faktoren, die wir gelernt haben, wie PIN oder Passwort. Oft umschrieben mit: Etwas, das man weiß.

Technische Faktoren: Faktoren technischer Natur, wie Passwort-Token, Mobiltelefon, Smartcard oder Bankkarte. Oft umschrieben mit: Etwas, das man hat.

Ein Beispiel für die Verwendung einer Zwei-Faktor-Authentifizierung im Alltag ist das Abheben von Geld am Geldautomaten. Bei einem Geldautomaten wird eine Karte (technischer Faktor) mit einer Persönlichen Identifizierungsnummer oder PIN (Wissensfaktor) verwendet. Wenn einer der oder beide Faktoren fehlen, ist es unmöglich, Geld abzuheben.

Ein Token (oder Generator für einmalige Passwörter) ist ein physikalisches Gerät, dass bei jeder Verwendung ein neues Passwort erzeugt.

Ein “Soft Token” ist ein Software-basierter Authenticator, der in einem Smartphone, Tablet-Computer oder PC (auch Mac) enthalten sein kann.

FREJA | IDENTITY & ACCESS MANAGEMENT

VERISEC

Warum Freja?

- Wenn Sie kein System zur strengen Authentifizierung haben.
- Wenn Sie bereits eine Lösung verwenden, aber Ihre Kosten reduzieren und/oder die Anzahl der Benutzer steigern möchten.
- Wenn Sie möchten, dass Ihre Nutzer Dienste mit denen anderer Organisationen teilen, und gleichzeitig eine hohe Vertrauenswürdigkeit und Verantwortlichkeit aufrechterhalten möchten.

Freja kann eingesetzt werden, um die Authentifizierung zu stärken, wenn von einem entfernten Ort auf ein lokales Netzwerk zugegriffen werden soll oder jemand sich bei einer spezifischen Anwendung einloggen soll (veraltete Anwendungen oder Lösungen mit einmaliger Anmeldung). Wenn Sie kein wirksames Authentifizierungssystem haben, ist Freja DIE Lösung für Sie.

Traditionell gab es eine Reihe von Anbietern, die als Grundlage für Ihre Lösungen eher proprietäre Codes verwenden, als offene Standards. Tokens sind teuer und müssen gegebenenfalls regelmäßig teuer ersetzt werden. Und da die Lösung proprietär ist, gibt es, wenn der Kunde sie einmal gekauft hat, keine alternativen Anbieter, von denen Produkte bezogen werden können.

Da Freja auf offenen Standards basiert, kann der Kunde verschiedene Anbieter zu Vorzugspreisen auswählen. Durch das Lizenzierungsmodell auf Gerätebasis wird Freja nicht teurer, je mehr Benutzer hinzugefügt werden. Kunden, die bereits eine Lösung verwenden und die Benutzung verstärken oder Kosten senken (oder beides) möchten, sollten sich Freja anschauen.

Merkmale

Selbstverwaltung: Über das Selbstverwaltungsportal können Benutzer ihre Hardware- und Software-basierten Authenticatoren registrieren. Diese Funktion verringert die Einführungszeit und die Kosten für den Einsatz der Tokens und die Benutzeraktivierung drastisch.

Sicherheit: Zwei-Faktor-Authentifizierung erhöht die Netzwerkzugangssicherheit. Freja umfasst außerdem zwei APIs, die gemeinsam mit Web-Anwendungen, Lösungen mit einmaliger Anmeldung oder anderen Anwendungen verwendet werden können, um die Authentifizierung zu externalisieren und zu stärken.

Minimale Auswirkungen auf die bestehende Infrastruktur: Freja ist ein Gerät, das mit minimalem Konfigurationsaufwand an eine bestehende Infrastruktur angeschlossen werden kann. Bestehende Verzeichnisse können verwendet werden, ohne Schemata aktualisieren oder größere Änderungen an der Umgebung vornehmen zu müssen.

Schnelle Bereitstellung: Da Freja ein Gerät ist, kann es in weniger als einem Tag aufgestellt und konfiguriert werden. Aus diesem Grund ist die Installation in unseren Gerätepreisen enthalten.

Skalierbarkeit: Freja soll sowohl technisch als auch kommerziell skalieren. Das System kann für interne Benutzer oder in Kombination mit großen externen Benutzergruppen wie Zulieferern, Kunden und Vertragsberatern verwendet werden.

Niedrige Gesamtbetriebskosten: Mit dem einzigartigen Lizenzierungsmodell und der Verwendung von offenen Standards als Grundlage bietet Freja hohe Sicherheit bei niedrigen Gesamtbetriebskosten.

Über Verisec

Verisec ist ein internationales IT-Sicherheitsunternehmen, das für Banken, Regierungsbehörden und mittelständische bis große Unternehmen weltweit innovative Sicherheitslösungen anbietet.

Wenn Sie mehr Informationen zu Freja Geräten wünschen, kontaktieren Sie uns bitte unter sales@verisec.com, +46 (0)8 723 09 00.

Verisec AB, Box 2034, 131 02 Nacka, Schweden. sales@verisec.com. +46 (0)8 723 09 00
Weitere Informationen über Verisec und die Kontaktdaten unserer Büros im Vereinigten Königreich und in Serbien finden Sie auf www.verisec.com

PS-Freja-1310-GERMAN