ForgeRock®

WHITE PAPER

Go passwordless

mantenendo l'autenticazione sicura.

Il problema con le password

Come sa ogni professionista della gestione delle identità e degli accessi, spesso le password rappresentano un problema. Gli utenti preferirebbero evitare di dover creare account protetti da password. Allo stesso tempo, i team responsabili della sicurezza si preoccupano degli attacchi di phishing via e-mail, dei furti di credenziali e delle violazioni dei dati.

In media ogni utente ha più di 90 account. Poiché ricordare le password è difficile, oltre il 50% degli utenti riutilizza le stesse password in diversi siti Web.[1] Il ricorso a password basate su informazioni personali rende gli account vulnerabili agli attacchi a dizionario. L'uso di un sistema di gestione delle password offre un'opzione per risolvere il problema, ma spesso gli stessi servizi di questo tipo sono vulnerabili.[2]

Nel "2021 Data Breach Investigations Report (DBIR)" di Verizon, il 61% delle violazioni ha coinvolto credenziali.[3]

Il **ForgeRock Consumer Identity Breach Report 2022** ha riscontrato che l'accesso non autorizzato è stato il metodo di attacco preferito dagli hacker nel 50% delle violazioni.[4]

Purtroppo le violazioni associate al furto di credenziali non se ne andranno molto presto. Le aziende possono cercare di proteggere se stesse e i propri dipendenti e clienti tramite corsi di formazione sulla sicurezza, misure di protezione delle e-mail e tecniche di autenticazione avanzate. Eppure, finché l'autenticazione mediante nome utente e password non sarà sostituita da metodi più sicuri, il furto delle credenziali continuerà a rappresentare una tattica preferita dai malintenzionati.

Questo documento presenta ForgeRock Passwordless Authentication, una soluzione basata su standard del settore in grado di ridurre o eliminare la necessità di affidarsi all'autenticazione mediante nome utente e password, garantendo nel contempo alla vostra azienda un livello di sicurezza superiore.

Ma prima vediamo quali alternative vengono utilizzate oggi.

Autenticazione avanzata

Oggi sono molte le applicazioni e i servizi che ricorrono alla cosiddetta "strong authentication", o autenticazione avanzata, che può essere a due fattori (Two-Factor Authentication, 2FA) o multifattoriale (Multi-Factor Authentication, MFA).

Nel caso dell'autenticazione 2FA, l'utente deve prima autenticarsi mediante un nome utente e una password, quindi utilizzando un secondo fattore quale un codice temporaneo (One-Time Passcode, OTP). Il codice normalmente viene fornito tramite un'app di autenticazione, in risposta a una notifica push su un'app mobile oppure (ma in modo meno sicuro) attraverso il protocollo di messaggistica di testo SMS. Inoltre con la 2FA il secondo fattore deve essere presentato a ogni tentativo di autenticazione.

L'autenticazione MFA incorpora caratteristiche più dipendenti dal contesto e svariati tipi di autenticatori, quali il dispositivo dell'utente, il browser, l'indirizzo IP, l'ubicazione o l'orario. Alcune soluzioni MFA potrebbero richiedere all'utente di autenticarsi in misura maggiore o minore, a seconda del contesto della sessione.

Combinando due o più tipi di fattori si aumenta la sicurezza, ma se tali fattori non sono univoci, si rischia di ottenere l'effetto contrario.

Il principio alla base di entrambi questi metodi è il fatto che l'autenticazione avanzata dovrebbe richiedere all'utente di autenticarsi mediante una combinazione di almeno due fattori univoci. Il nome utente e la password sono fattori di "conoscenza" (informazioni note all'utente). Il dispositivo mobile, il token hardware o la smart card sono fattori di "possesso" (appartengono all'utente). E gli elementi biometrici, quali le impronte digitali o gli identificatori di riconoscimento facciale, costituiscono esempi di "inerenza" (ciò che è l'utente).

I siti Web che richiedono agli utenti di autenticarsi tramite nome utente e password, quindi chiedono loro di presentare altri fattori di conoscenza, come ad esempio le "domande di sicurezza" che gli utenti potrebbero dimenticare con il tempo, rendono superfluo il secondo fattore di autenticazione. Le risposte a domande di sicurezza comuni (ad esempio il nome da nubile della madre) sono disponibili mediante record pubblici, i social network o l'ingegneria sociale.

I metodi 2FA e MFA sono più sicuri dell'autenticazione tramite nome utente e password, ma presentano alcune limitazioni specifiche. Con il tempo, l'autenticazione 2FA può infastidire gli utenti che sono costretti ad autenticarsi due volte a ogni accesso, soprattutto se è necessario passare a un'app di autenticazione o a un messaggio SMS per individuare il codice temporaneo da inserire. L'autenticazione MFA può risultare difficile da implementare e spesso fa riferimento a regole di policy di configurazione che non consentono l'agilità e l'accesso granulare necessario ai team di sicurezza. Inoltre la corretta implementazione di MFA o 2FA dipende prevalentemente dalla potenza e dalla flessibilità della soluzione di gestione delle identità e degli accessi utilizzata dall'azienda.

Un approccio all'autenticazione basato su standard

Per l'autenticazione avanzata si dimostra più funzionale un approccio basato su standard, in grado di ridurre o eliminare la necessità di nome utente e password. Gli analisti di Gartner raccomandano di sostituire le password con l'autenticazione biometrica. In particolare, prevedono che il 60% delle grandi aziende internazionali e il 90% delle medie imprese sostituiranno le password con altri metodi per oltre il 50% dei casi di utilizzo dell'identità entro il 2022.[5]

Nel 2019, il World Wide Web Consortium (W3C) ha ratificato lo standard Fast Identity Online 2 (FIDO2) Web Authentication (WebAuthn), che supporta l'autenticazione senza nome utente e senza password.

I fornitori di browser, sistemi operativi e hardware stanno sottoscrivendo la FIDO (Fast Identity Online) Alliance e hanno iniziato a distribuire il supporto per FIDO2.[6]

Lo standard FIDO originale, noto anche come Universal 2 Factor (U2F), si basa su un modello scalabile a chiave pubblica/privata in cui per ogni servizio viene generata una nuova coppia di chiavi. Ciò consente di mantenere la separazione fra coppie di chiavi, salvaguardando la privacy.[8] Allo stesso tempo, l'autenticazione per i servizi online non ha più bisogno della password, che viene sostituita da una chiave di sicurezza hardware.

Lo standard FIDO2, più recente, rappresenta l'evoluzione "senza nome utente e senza password" di FIDO e sfrutta le credenziali memorizzate sul dispositivo dell'utente. FIDO2 comprende due specifiche:

- Un'API basata sul Web, denominata **Web Authentication (WebAuthn)**, consente di autenticarsi per le applicazioni Web senza ricorrere a password ma utilizzando la crittografia a chiave pubblica e alcuni autenticatori. WebAuthn supporta credenziali conformi allo standard originale FIDO U2F e credenziali FIDO2.

- Il **protocollo CTAP2** (Client to Authenticator Protocol) FIDO2 consente la comunicazione fra applicazioni client e autenticatori conformi a FIDO2 tramite browser e sistemi operativi compatibili con FIDO2.

Tipi di autenticatori

FIDO2 si affida a coppie di chiavi pubblica/privata memorizzate in modo sicuro sull'hardware locale e a browser compatibili con FIDO2 che interagendo con i servizi generano credenziali sicure, riferite a chiavi pubbliche/private, per ogni servizio. Le chiavi private in ogni coppia di chiavi vengono memorizzate localmente e non abbandonano mai l'autenticatore dell'utente. Le chiavi pubbliche vengono utilizzate dal server di autenticazione per crittografare e firmare le comunicazioni con i dispositivi endpoint dell'utente.

È la capacità di memorizzazione dell'autenticatore locale dell'utente a stabilire la possibilità di abilitare l'autenticazione senza nome utente e senza password.

Gli **autenticatori per piattaforma**, basati sul modulo TPM (Trusted Platform Module) o il Secure Enclave installato in molti computer portatili e telefoni, solitamente vengono sbloccati da un sensore biometrico, come in Microsoft Windows Hello o Apple TouchID.

Gli **autenticatori hardware multipiattaforma o "roaming"** presentano le rivendicazioni di accesso di un utente a un altro servizio o dispositivo. Si tratta, ad esempio, delle chiavi di sicurezza Google Titan, delle chiavette YubiKey o degli autenticatori Duo che utilizzano protocolli USB, NFC (Near-Field Communication) e Bluetooth. Quando l'autenticatore si attiva - in seguito all'inserimento in una porta USB, alla pressione di un pulsante o a un semplice tocco - invia una risposta firmata che convalida l'accesso dell'utente. Anche gli smartphone possono fungere da autenticatori.

Facendo riferimento alle credenziali sicure memorizzate nell'hardware affidabile dell'utente, FIDO2 WebAuthN abilita l'autenticazione senza nome utente e senza password, eliminando virtualmente il potenziale di violazione dei dati associato al furto delle credenziali.

ForgeRock Passwordless Authentication

ForgeRock Passwordless Authentication implementa lo standard FIDO2 WebAuthn in ForgeRock Intelligent Access. Consente di progettare percorsi utente sicuri e ottimizzati per l'autenticazione senza password e, in determinati casi, anche senza nome utente.

ForgeRock Passwordless Authentication riduce la superficie della vostra azienda esposta agli attacchi, eliminando virtualmente il furto di credenziali associato a phishing, riutilizzo di password, riempimento di credenziali, keylogger e altro.

Vantaggi dell'autenticazione senza password

- **Sicura:** le credenziali di accesso sono univoche per ogni sito Web e non abbandonano mai il dispositivo dell'utente. A differenza di nome utente e password, le credenziali non vengono mai trasmesse sul cavo, pertanto si elimina il rischio di attacchi person-in-the-middle.
- **Comoda:** utilizza semplici metodi incorporati, quali lettori di impronte digitali o videocamere, o sfrutta chiavi di sicurezza FIDO intuitive. I consumatori possono selezionare il dispositivo più adatto per le loro esigenze.
- **Privata:** le chiavi sono univoche e non possono essere utilizzate per tenere traccia degli utenti da un sito all'altro. I dati biometrici non abbandonano mai il dispositivo dell'utente.

"Siamo nella posizione di assicurare a tutti i nostri utenti un'esperienza molto più soddisfacente, grazie all'eliminazione di nomi utente e password - e di ridurre le chiamate al desk dell'assistenza a causa di password dimenticate".

— Doug Neumann, Responsabile IT, U.S. National Nuclear Security Administration

Funzionamento dell'autenticazione senza password

ForgeRock supporta l'autenticazione senza password tramite le strutture ad albero e i nodi di registrazione e autenticazione specifici per WebAuthn di ForgeRock Intelligent Access. Per autenticarsi senza password, l'utente deve prima registrarsi, verificando il proprio nome utente e la password in riferimento all'archivio delle identità, in modo che ForgeRock possa identificare l'utente stesso e il suo dispositivo.

Quando un utente tenta di registrare il proprio dispositivo per la prima volta, ForgeRock Intelligent Access rileva se tale dispositivo supporta lo standard WebAuthn. Se la registrazione del dispositivo ha buon esito, ForgeRock istruisce il dispositivo dell'utente a generare una coppia univoca di chiavi pubblica/privata per comunicare con ForgeRock. Quando l'utente esegue l'autenticazione per il proprio dispositivo mediante il sensore biometrico incorporato, la chiave privata dell'utente, che è stata archiviata in modo sicuro nella memoria persistente e che non abbandona mai il dispositivo, diventa disponibile per firmare le richieste di autenticazione.

ForgeRock genera una richiesta diretta al dispositivo dell'utente e vi applica la crittografia sfruttando la chiave pubblica dell'utente. La chiave privata nel dispositivo dell'utente firma la richiesta, quindi ForgeRock provvede alla verifica necessaria mediante la chiave pubblica dell'utente. Questo processo stabilisce una connessione sicura fra il dispositivo hardware dell'utente e ForgeRock, per cui negli accessi successivi diventa possibile ricorrere all'autenticazione senza password.

In ogni caso, i tradizionali percorsi utente basati su nome utente e password dovrebbero essere mantenuti in abbinamento all'autenticazione step-up, come metodo alternativo qualora l'utente non possa autenticarsi con ForgeRock mediante il proprio dispositivo affidabile registrato (ad esempio se quest'ultimo non è disponibile o viene smarrito o rubato).

Uso dell'autenticazione senza password e senza biometria

Alcune persone non possono utilizzare la biometria oppure le loro aziende non la supportano. È comunque possibile abilitare l'autenticazione senza password ricorrendo a qualsiasi autenticatore esterno (informazioni note all'utente o dispositivi in suo possesso) protetto da un codice PIN, come ad esempio smart card compatibili con FIDO2, chiavi di sicurezza hardware conformi a FIDO2 o a Universal 2 Factor (U2F) o infine smartwatch. ForgeRock supporta funzionalità di autenticazione senza password conformi a FIDO2 Web Authentication per numerosi autenticatori, formati di attestazione e tipologie. Per ulteriori informazioni, consultate la **Panoramica della soluzione**.

Configurazione dell'autenticazione senza password

L'autenticazione senza password è un set di funzionalità in ForgeRock Intelligent Access progettato per supportare lo standard FIDO2/WebAuthn. Gli utenti possono registrare dispositivi affidabili e utilizzare queste funzioni incorporate per memorizzare le credenziali localmente. Nelle strutture ad albero di ForgeRock Intelligent Access sono inclusi tre nodi preconfigurati. Per creare percorsi utente è sufficiente trascinare e rilasciare questi nodi nell'interfaccia utente della soluzione. Per ulteriori informazioni sulle strutture ad albero e i nodi di ForgeRock Intelligent Access, consultate il white paper "**Introducing ForgeRock Intelligent Access**."

Registrazione di un dispositivo

Gli utenti devono innanzitutto autenticarsi tramite nome utente e password, quindi registrare il proprio dispositivo prima di poter usufruire dell'autenticazione senza password. A tale scopo, create il percorso utente e aggiungete un nodo di registrazione WebAuthn dopo il nodo relativo alla decisione di raccolta del nome utente/della password e della memorizzazione dei dati. Se l'utente riesce a registrare correttamente un autenticatore del tipo appropriato, ovvero conforme alle proprietà del nodo, la valutazione della struttura ad albero continua insieme alla segnalazione del risultato positivo. L'autenticazione senza password non riesce se il client non supporta WebAuthn - ad esempio, se il browser in uso non è supportato o se l'utente si è registrato mediante il tipo di autenticatore scorretto. Quando la registrazione del client raggiunge il time-out, viene segnalato un errore del client.

Convalida dell'identità dell'utente

Per essere considerato sicuro, qualsiasi autenticatore utilizzato per l'autenticazione senza password dovrebbe essere convalidato in riferimento all'identità di un utente. È compito delle aziende convalidare gli utenti in relazione ai loro autenticatori, di persona o attenendosi a un processo di verifica dell'identità digitale affidabile, da eseguire alla registrazione degli autenticatori stessi. Per ulteriori informazioni sui livelli di assicurazione dell'identità e i processi di verifica dell'identità digitale che è possibile impostare in ForgeRock Intelligent Access, scaricate il white paper, **Reduce the Total Cost of Fraud**.

Abilitazione dell'autenticazione senza nome utente

Per consentire all'utente di autenticarsi senza dover inserire il nome utente per le future autenticazioni, attivate "Username to device" a destra del nodo di registrazione.

Per l'autenticazione senza nome utente è necessario che gli autenticatori dell'utente supportino la memorizzazione di chiavi residenti.

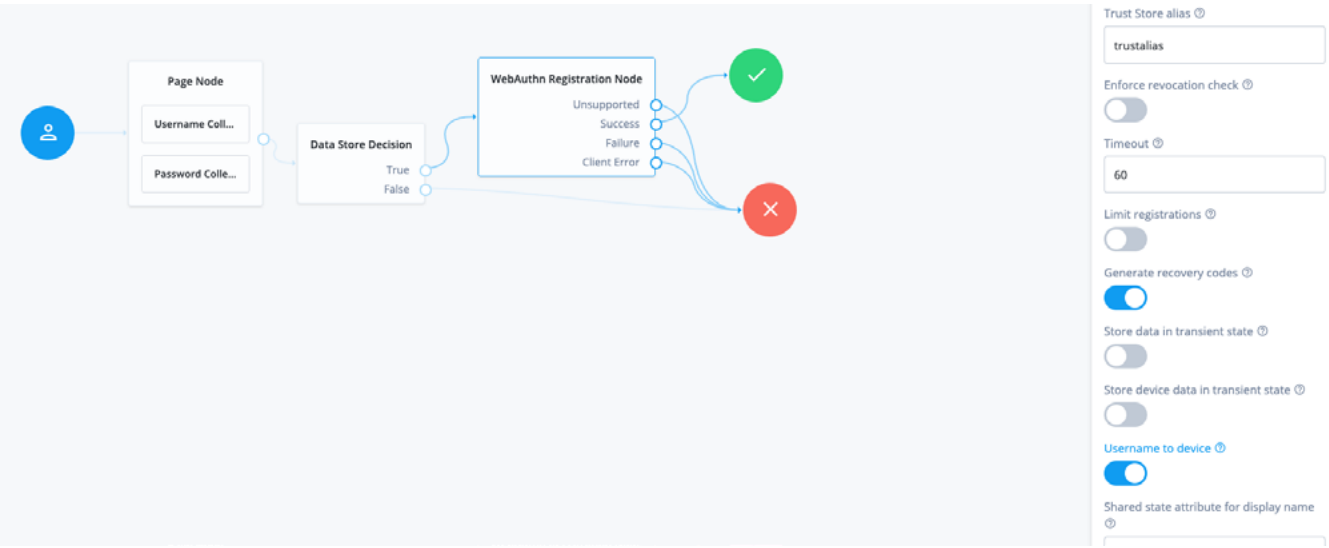

Figura 1: registrazione senza password con l'autenticazione senza nome utente abilitata

Quando l'utente, dopo essersi registrato correttamente, desidera accedere, il nodo di autenticazione WebAuthn si attiva e mostra all'utente un percorso di accesso "senza nome utente".

Analisi di un dispositivo

Se preferite eseguire analisi ulteriori sul dispositivo di un utente e ritardarne la registrazione finché il risultato dell'analisi non è completo, potete aggiungere il nodo di memorizzazione dispositivi WebAuthn nella struttura ad albero di registrazione WebAuthn. Questo nodo è facoltativo.

L'esempio seguente illustra come utilizzarlo. Supponiamo che desideriate abilitare l'autenticazione senza nome utente e senza password, ma solo per i dipendenti che utilizzano computer portatili aziendali realizzati da un determinato produttore e solo per i computer portatili nei quali sia installato un modulo TPM biometrico. Potete aggiungere alla struttura ad albero di registrazione il nodo di memorizzazione dispositivi WebAuthn, insieme a un nodo decisionale con uno script personalizzato, concepito per acquisire dati di attestazione specifici del dispositivo (ad esempio il numero di serie e, per maggiore sicurezza, una catena di certificati che consenta di verificare l'originalità del dispositivo). In questo modo si impedisce persino a utenti validi di autenticarsi da dispositivi non gestiti e si rafforza la posizione dell'azienda, in termini di sicurezza.

Per abilitare il nodo di memorizzazione dispositivi WebAuthn, attivate "Store data in transient state" a destra nella schermata. Lo stato transitorio indica che i dati del dispositivo sono archiviati solo nella memoria temporanea, dove ForgeRock può utilizzarli per l'analisi.

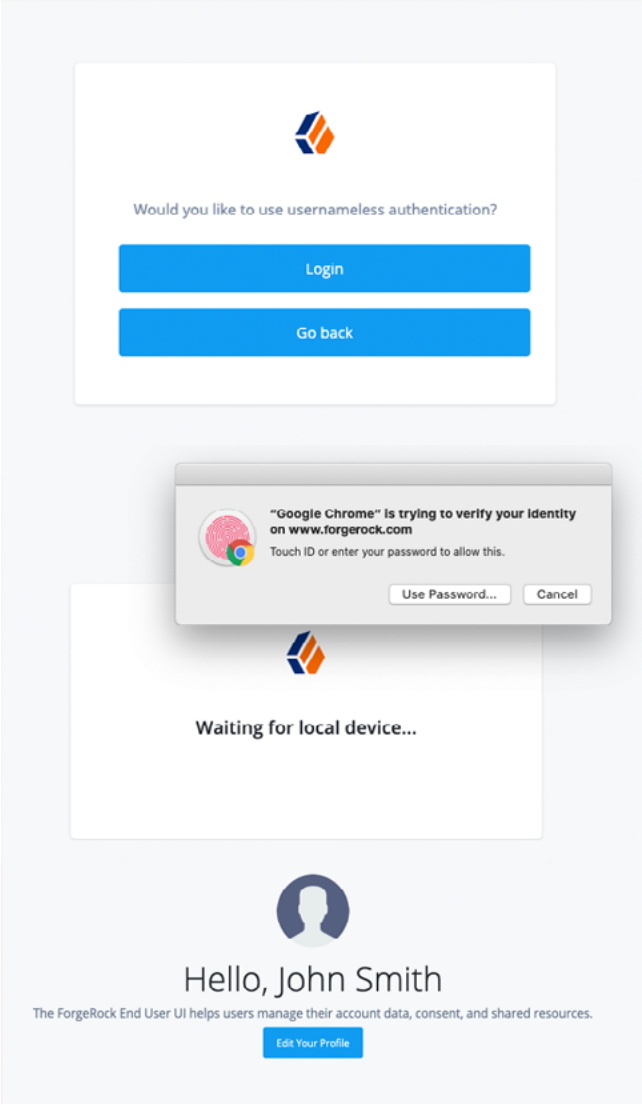

Figura 2: autenticazione senza nome utente

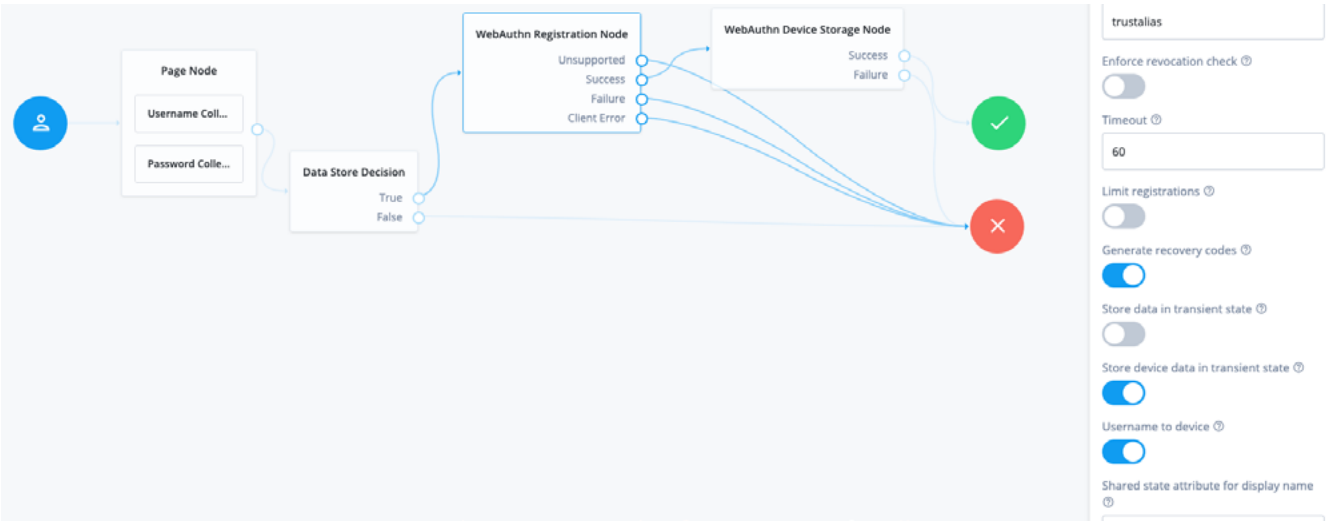

Figura 3: nodo di memorizzazione dispositivi WebAuthn in un percorso di registrazione

Alternative all'autenticazione senza password

Gli utenti devono sempre avere a disposizione un'alternativa all'autenticazione senza password, per tutelarsi in caso di smarrimento o furto del dispositivo registrato oppure se stanno utilizzando un browser o un dispositivo che ancora non supporta le credenziali FIDO2 e WebAuthn. La vostra azienda può progettare percorsi utente che raccolgono credenziali (nome utente e password) e aggiungere l'autenticazione MFA, incorporando il modulo TPM della piattaforma, le notifiche push mobili o autenticatori di terze parti.

Quando utilizzare l'autenticazione senza password

ForgeRock Passwordless Authentication è l'ideale per gli utenti del personale che si autenticano per accedere ad applicazioni nel cloud o in loco. ForgeRock Passwordless Authentication supporta sia l'accesso iniziale che l'autenticazione step-up, inclusa l'autorizzazione alle transazioni. Per ulteriori informazioni sull'autenticazione step-up e l'autorizzazione alle transazioni, consultate il white paper, "**Introducing ForgeRock Intelligent Access**."

Poiché sono sempre più numerosi i browser e le applicazioni consumer che iniziano a supportare FIDO2 e lo standard WebAuthn, potrete progettare percorsi utente senza password anche per casi di utilizzo dei clienti. Lo standard WebAuthn oggi viene impiegato sui social media, nei servizi finanziari, nei giochi e nelle applicazioni di memorizzazione nel cloud.

> ForgeRock Passwordless Authentication supporta sia l'accesso iniziale che l'autenticazione step-up, inclusa l'autorizzazione alle transazioni.

Conclusione

ForgeRock Intelligent Access agevola la progettazione rapida di percorsi di autenticazione sicuri senza nome utente e senza password per i casi di utilizzo di dipendenti e clienti. È possibile progettare questi percorsi utente in pochi minuti e supportare diversi autenticatori simultaneamente, ottenendo risparmi significativi in confronto alle soluzioni di autenticazione avanzata già esistenti. ForgeRock Passwordless Authentication offre un livello superiore di sicurezza, comodità e privacy per i vostri utenti.

[1] https://fidoalliance.org/what-is-fido/
[2] https://www.welivesecurity.com/2020/03/19/security-flaws-found-in-popular-password-managers/
[3] https://enterprise.verizon.com/resources/reports/dbir/
[4] https://www.forgerock.com/resources/2022-consumer-identity-breach-report
[5] https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/
[6] https://www.theverge.com/2020/6/24/21301509/apple-safari-14-browser-face-touch-id-logins-webauthn-fido2
[7] https://www.yubico.com/blog/what-is-fido2/