Cesare Vellani – Pre-Sales – Avangate Security by Elovade
cesare.vellani@avangate.it

Perchè si dovrebbe usare un Password Manager?

1. Per contrastare l'attività dei **cybercriminali**

2. Per evitare il cosiddetto "**effetto domino**" e la debolezza delle password usate

3. Per aiutare a minimizzare la possibilità di rimanere vittima di un **attacco di phishing**

4. Per aumentare l'efficienza della **postura di sicurezza aziendale**

5. Per essere facilmente **compliant** con le recenti "best practices" legate alla gestione delle password

Perchè si dovrebbe usare un Password Manager di tipo ***Corporate***?

In generale perchè...

- Ad ogni tipologia di utente, il prodotto **dedicato**!
- Per evitare problemi generati **dall'interno**
- Per poter gestire efficacemente i **collaboratori esterni**

Perchè si dovrebbe usare un Password Manager di tipo ***Corporate***?

Nello specifico perchè...

1. Per avere completa **visibilità** sulla gestione delle password

2. Per applicare efficientemente le **policy** di sicurezza aziendali

3. Per poter implementare logiche **RBAC (Role Based Access Control)**

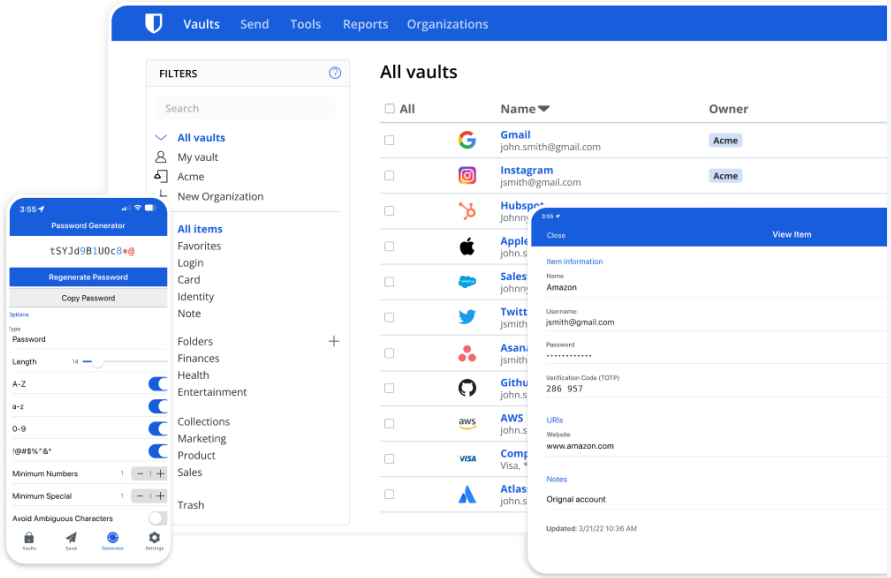
4. Per poter **condividere** le password in modo sicuro ma semplice tra i dipendenti

5. Per poter gestire facilmente **l'on\off-boarding** dei dipendenti

6. Per monitorare anche il pericolo "**dark web**"

7. Per essere "compliant" con le recenti **normative** (NIS2, DORA, ecc.)

Informazioni su Bitwarden



Gestione delle credenziali per privati e organizzazioni

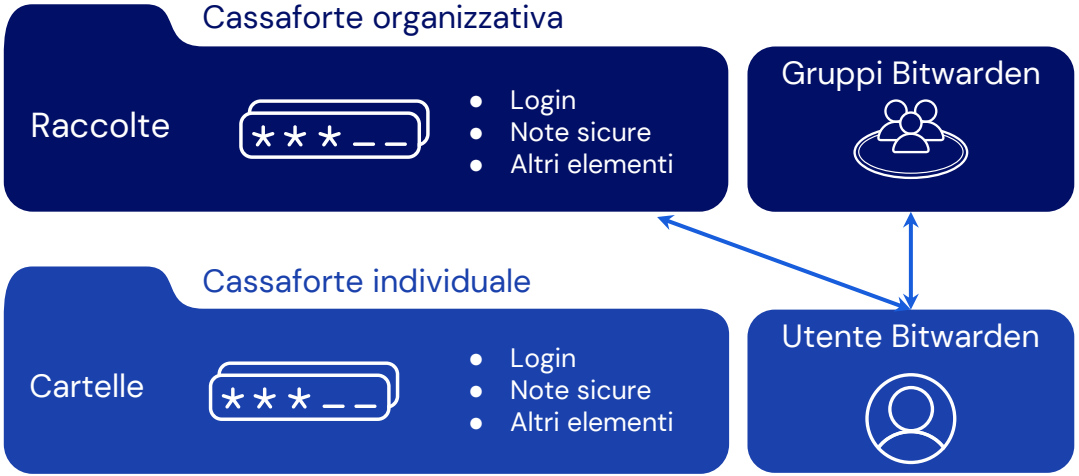
- Gestione password, gestione segreti, autenticatore, Passwordless.dev
- Fondata nel 2016, con sede in California
- Al servizio di milioni di utenti finali e decine di migliaia di aziende in tutto il mondo
- Architettura open source affidabile, multipiattaforma e protetta con crittografia end-to-end

bitwarden

Comprendere i vault di Bitwarden

- Elemento: un oggetto in Bitwarden che rappresenta un login, una carta di credito, un'identità, una nota sicura o una chiave SSH. Un elemento può far parte di molte raccolte, senza necessità di duplicarlo
- Cassaforte individuale - La cassaforte di un utente è il luogo in cui sono archiviati gli elementi di proprietà di quell'utente
- Cassaforte dell'organizzazione: una cassaforte di elementi la cui proprietà non appartiene a un utente specifico, ma all'organizzazione stessa. Solo le casseforti dell'organizzazione contengono Raccolte
- Raccolte - Raggruppano gli elementi per la condivisione sicura con gli utenti all'interno di un'organizzazione. Gli utenti e i gruppi hanno accesso alle Raccolte
- Preferiti e cartelle - Personalizza la visualizzazione di ciascun utente consentendogli di organizzare qualsiasi elemento a cui ha accesso

Organizzazione Casseforti, Raccolte, Gruppi



Tutti i dati della cassaforte sono protetti con crittografia end-to-end e "zero-knowledge"

Client Bitwarden

Bitwarden Password Manager può integrarsi con i sistemi IT esistenti

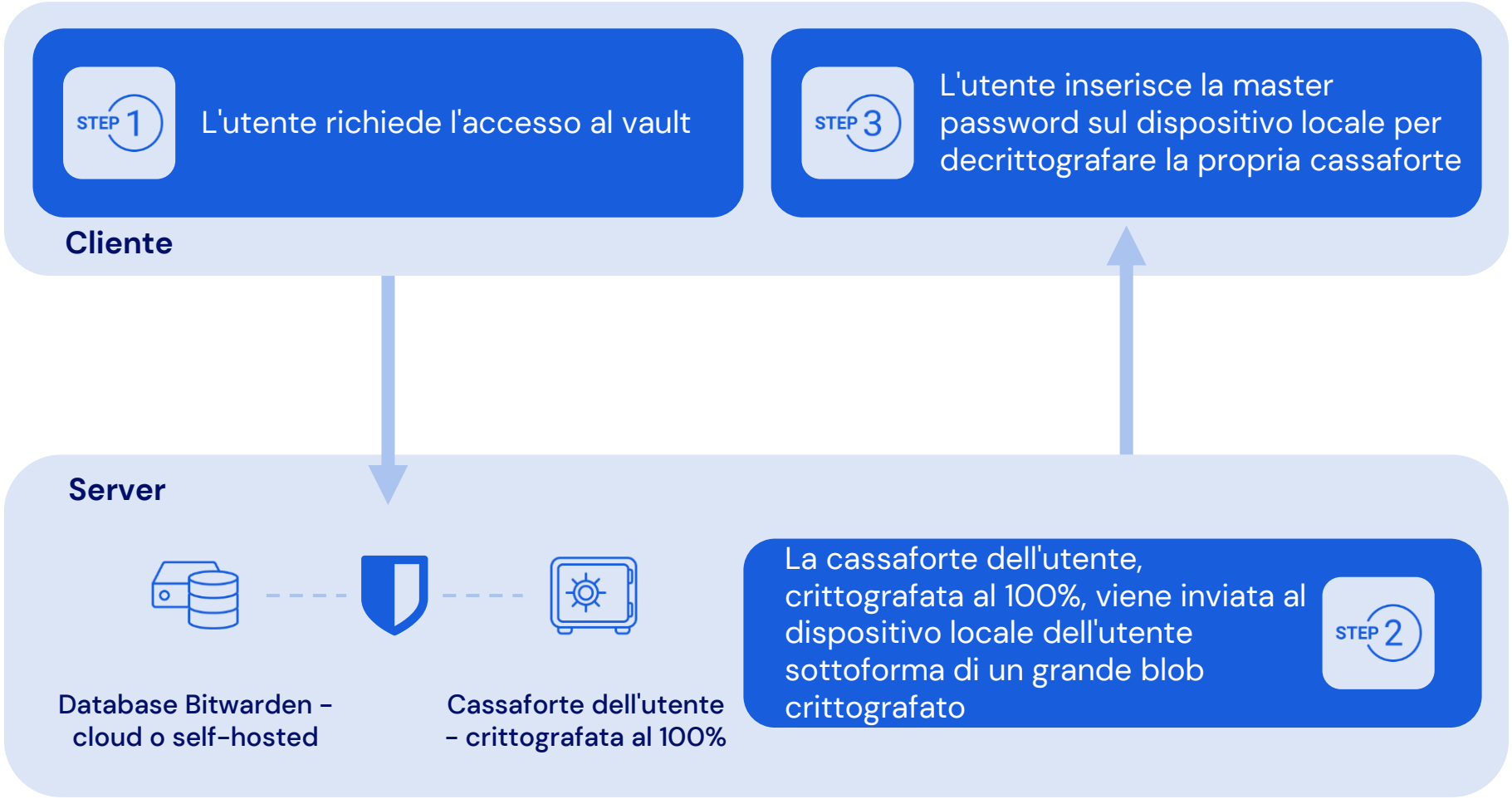
- Single Sign-on
- Provisioning SCIM
- 2FA
- SIEM
- e altro ancora

Certificazioni Bitwarden

Che cos'è la crittografia “zero-knowledge”?

Crittografia “zero-knowledge” significa:

- Tutti i dati della cassaforte sono completamente crittografati
- Bitwarden non ha accesso alla tua master password né alle chiavi di crittografia
- La crittografia viene eseguita localmente sul tuo dispositivo
  - AES-256 bit: usato per la cifratura dei dati del vault
  - PBKDF2 SHA-256 o Argon2: per derivare la chiave crittografica a partire dalla master password (anti brute-force)
- Bitwarden non ha mai accesso ai tuoi dati non crittografati


STEP 1
L'utente richiede l'accesso al vault
STEP 3
L'utente inserisce la master password sul dispositivo locale per decrittografare la propria cassaforte
Cliente
Server
La cassaforte dell'utente, crittografata al 100%, viene inviata al dispositivo locale dell'utente sottoforma di un grande blob crittografato
STEP 2
Database Bitwarden - cloud o self-hosted
Cassaforte dell'utente - crittografata al 100%

Utilizza Bitwarden come vuoi

È disponibile il cloud hosting

bitwarden.com – Stati Uniti

bitwarden.eu – UE

Self-hosting utilizzando il proprio server

mycompany.com

Condivisione dei dati

Condivisione cifrata dei dati

- Condividi i tuoi dati sensibili in modo sicuro e flessibile **RBAC** (**Role Based Access Control**) con singoli colleghi o gruppi di lavoro aziendali
- **Bitwarden Send** - Trasmetti informazioni cifrate (testo o file) con chiunque tramite un link sicuro condivisibile via email, chat, ecc

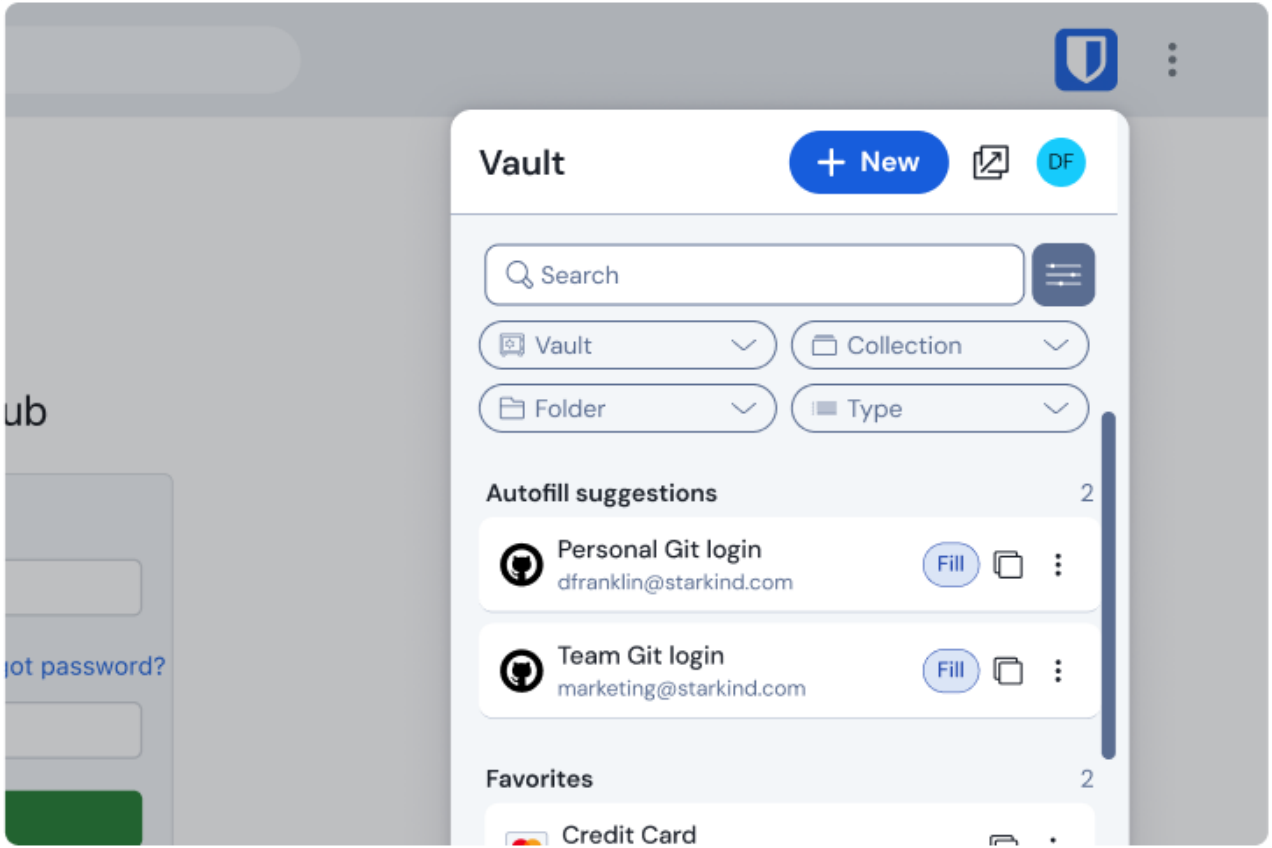
Disponibile su tutti i dispositivi

Client Bitwarden

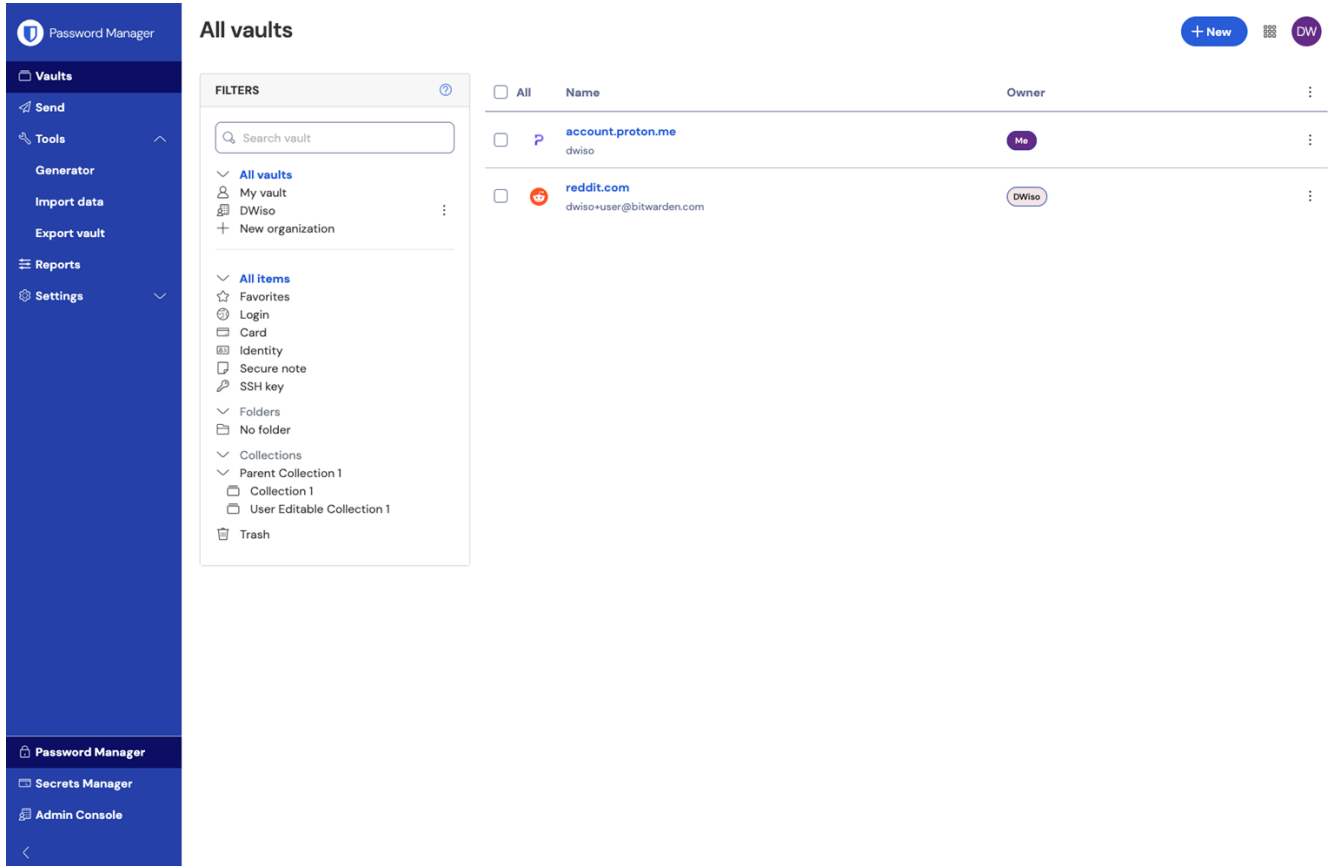
- Desktop
  - Mac, Linux o Windows
- Estensioni browser
- Applicazioni mobili
  - iOS
  - Android o FDroid
- App web
- Riga comando (CLI)

Tutti i browser, desktop e piattaforme mobili più diffusi

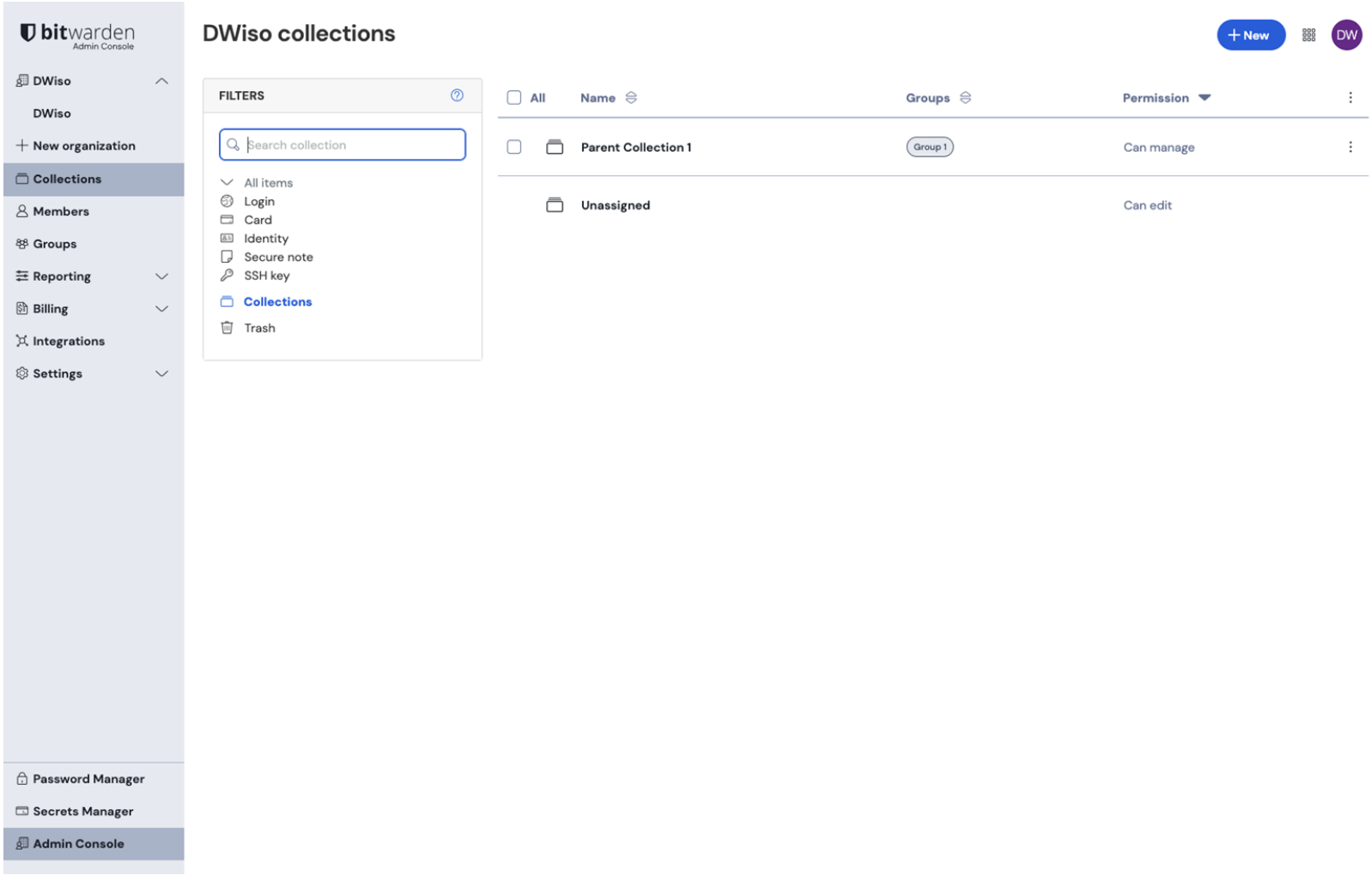
L'esperienza utente di Bitwarden: Estensione per browser


Vault
New
DF
Search
Vault
Collection
Folder
Type
Autofill suggestions
2
Personal Git login
dfranklin@starkind.com
Fill
Team Git login
marketing@starkind.com
Fill
Favorites
2
Credit Card

L'esperienza utente di Bitwarden: Cassaforte Web


Password Manager
Vaults
Send
Tools
Generator
Import data
Export vault
Reports
Settings
Password Manager
Secrets Manager
Admin Console
All vaults
+ New
DW
FILTERS
Search vault
All vaults
My vault
DWiso
New organization
All items
Favorites
Login
Card
Identity
Secure note
SSH key
Folders
No folder
Collections
Parent Collection 1
Collection 1
User Editable Collection 1
Trash
All
Name
Owner
account.proton.me
dwiso
Me
reddit.com
dwiso+user@bitwarden.com
DWiso

Console di amministrazione


bitwarden
Admin Console
DWiso
DWiso
New organization
Collections
Members
Groups
Reporting
Billing
Integrations
Settings
Password Manager
Secrets Manager
Admin Console
DWiso collections
New
DW
FILTERS
Search collection
All items
Login
Card
Identity
Secure note
SSH key
Collections
Trash
All
Name
Groups
Permission
Parent Collection 1
Group 1
Can manage
Unassigned
Can edit

Onboarding degli utenti

Accedi tramite uno dei tre metodi disponibili

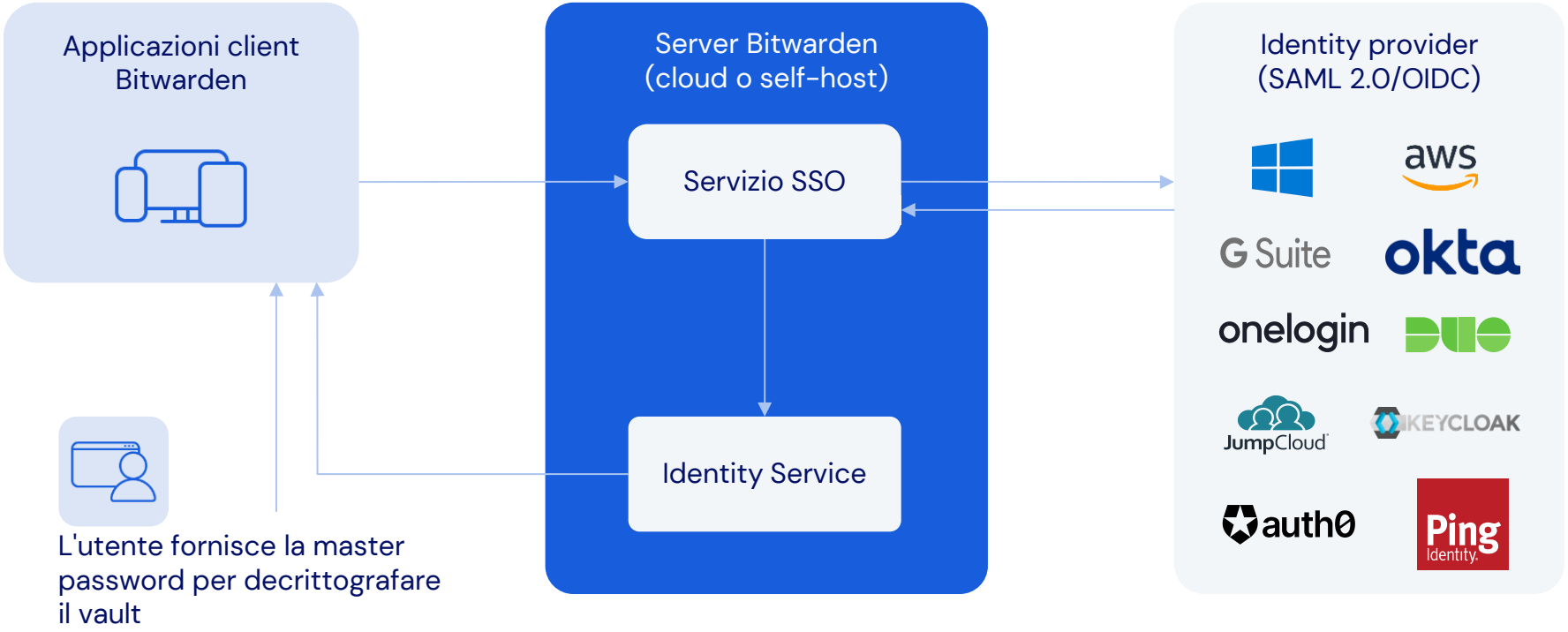
Single sign-on

SCIM o tool Directory Connector

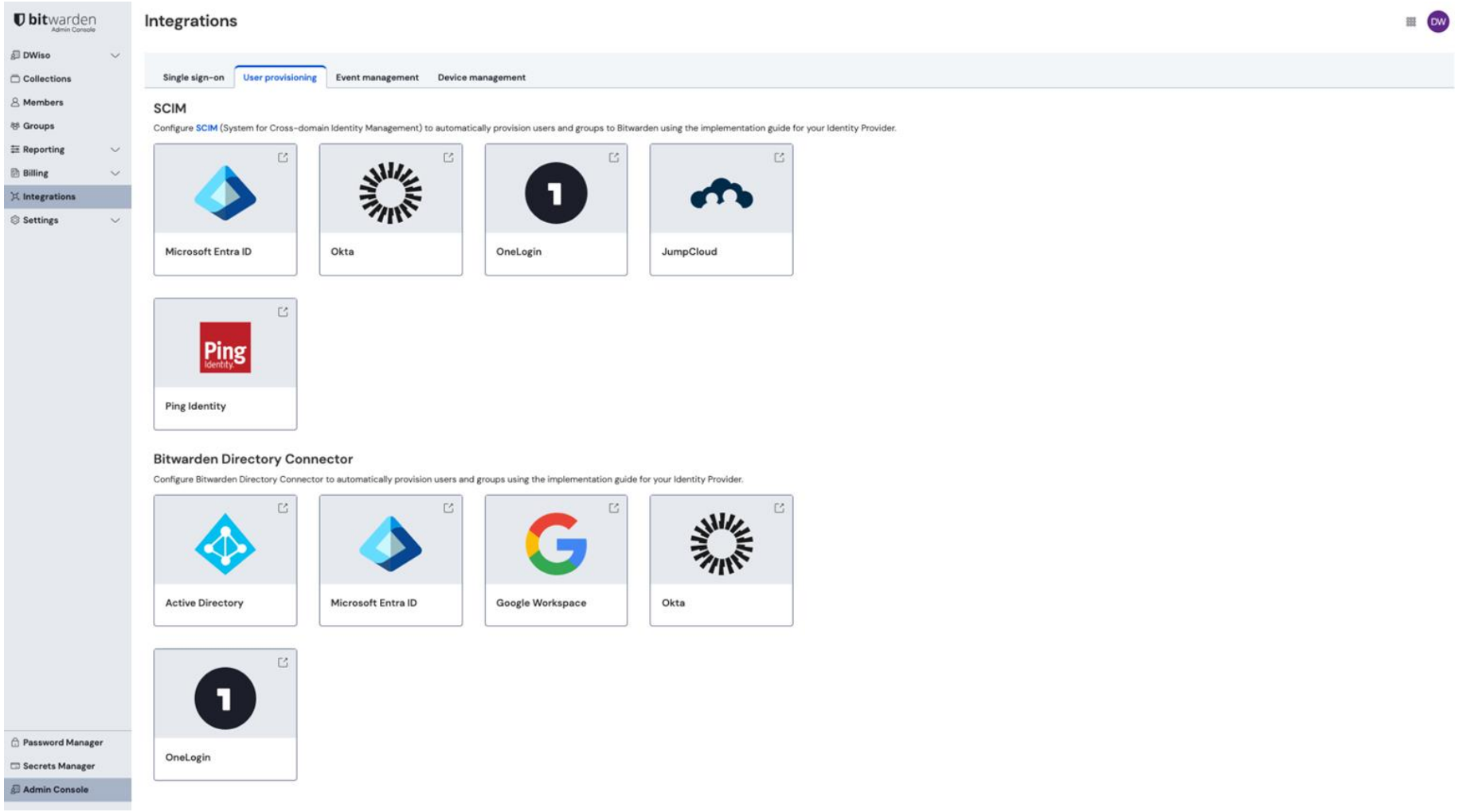
Manualmente

Onboarding degli utenti: SSO

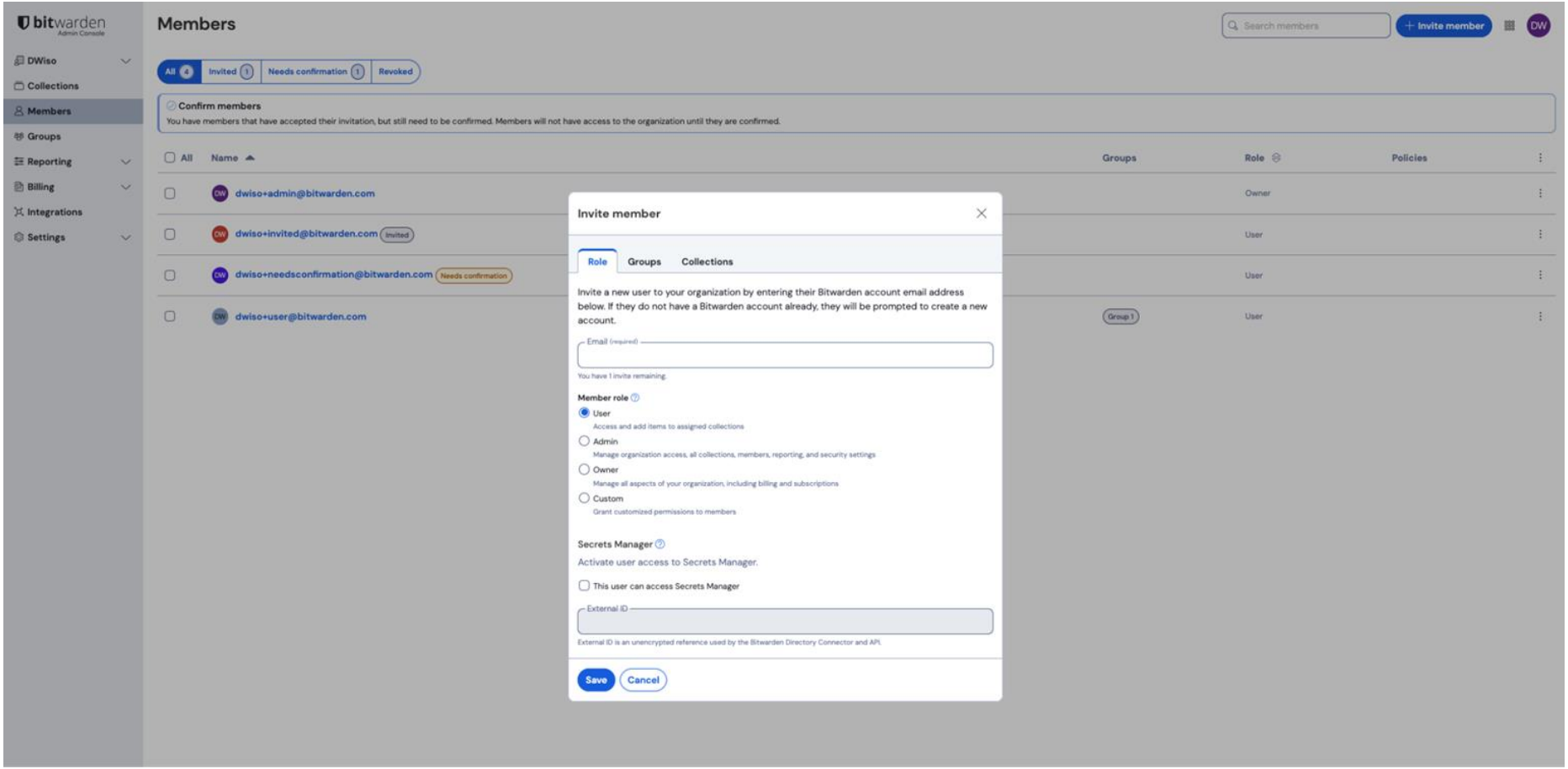
Accesso con SSO



Onboarding degli utenti: SCIM o Directory Connector


bitwarden
Admin Console
DWiso
Collections
Members
Groups
Reporting
Billing
Integrations
Settings
Password Manager
Secrets Manager
Admin Console
Integrations
DW
Single sign-on
User provisioning
Event management
Device management
SCIM
Configure SCIM (System for Cross-domain Identity Management) to automatically provision users and groups to Bitwarden using the implementation guide for your Identity Provider.
Microsoft Entra ID
Okta
OneLogin
JumpCloud
Ping Identity
Bitwarden Directory Connector
Configure Bitwarden Directory Connector to automatically provision users and groups using the implementation guide for your Identity Provider.
Active Directory
Microsoft Entra ID
Google Workspace
Okta
OneLogin

Onboarding degli utenti: Aggiunta manuale degli utenti


bitwarden
Admin Console
DWiso
Collections
Members
Groups
Reporting
Billing
Integrations
Settings
Members
Search members
Invite member
DW
All 4
Invited 1
Needs confirmation 1
Revoked
Confirm members
You have members that have accepted their invitation, but still need to be confirmed. Members will not have access to the organization until they are confirmed.
All
Name
Groups
Role
Policies
dwiso+admin@bitwarden.com
Owner
dwiso+invited@bitwarden.com
Invited
User
dwiso+needsconfirmation@bitwarden.com
Needs confirmation
User
dwiso+user@bitwarden.com
Group 1
User
Invite member
Role
Groups
Collections
Invite a new user to your organization by entering their Bitwarden account email address below. If they do not have a Bitwarden account already, they will be prompted to create a new account.
Email (required)
You have 1 invite remaining.
Member role
User
Access and add items to assigned collections
Admin
Manage organization access, all collections, members, reporting, and security settings
Owner
Manage all aspects of your organization, including billing and subscriptions
Custom
Grant customized permissions to members
Secrets Manager
Activate user access to Secrets Manager.
This user can access Secrets Manager
External ID
External ID is an unencrypted reference used by the Bitwarden Directory Connector and API.
Save
Cancel

Reportistica:
Registri eventi e reportistica

Integrazioni SIEM (Security Information and Event Management) predefinite

- Azure Sentinel
- Splunk
- Panther
- Rapid7
- Elastic

API RESTful disponibili per l'integrazione con altri sistemi

bitwarden
Admin Console

Reports

DW

- DWiso
- Access Intellige...
- Collections
- Members
- Groups
- Reporting
  - Event logs
  - Reports
- Billing
- Integrations
- Settings

Identify and close security gaps in your organization's accounts by clicking the reports below.

Exposed passwords

Passwords exposed in a data breach are easy targets for attackers. Change these passwords to prevent potential break-ins.

Reused passwords

Reusing passwords makes it easier for attackers to break into multiple accounts. Change these passwords so that each is unique.

Weak passwords

Weak passwords can be easily guessed by attackers. Change these passwords to strong ones using the password generator.

Unsecure websites

URLs that start with http:// don't use the best available encryption. Change the login URIs for these accounts to https:// for safer browsing.

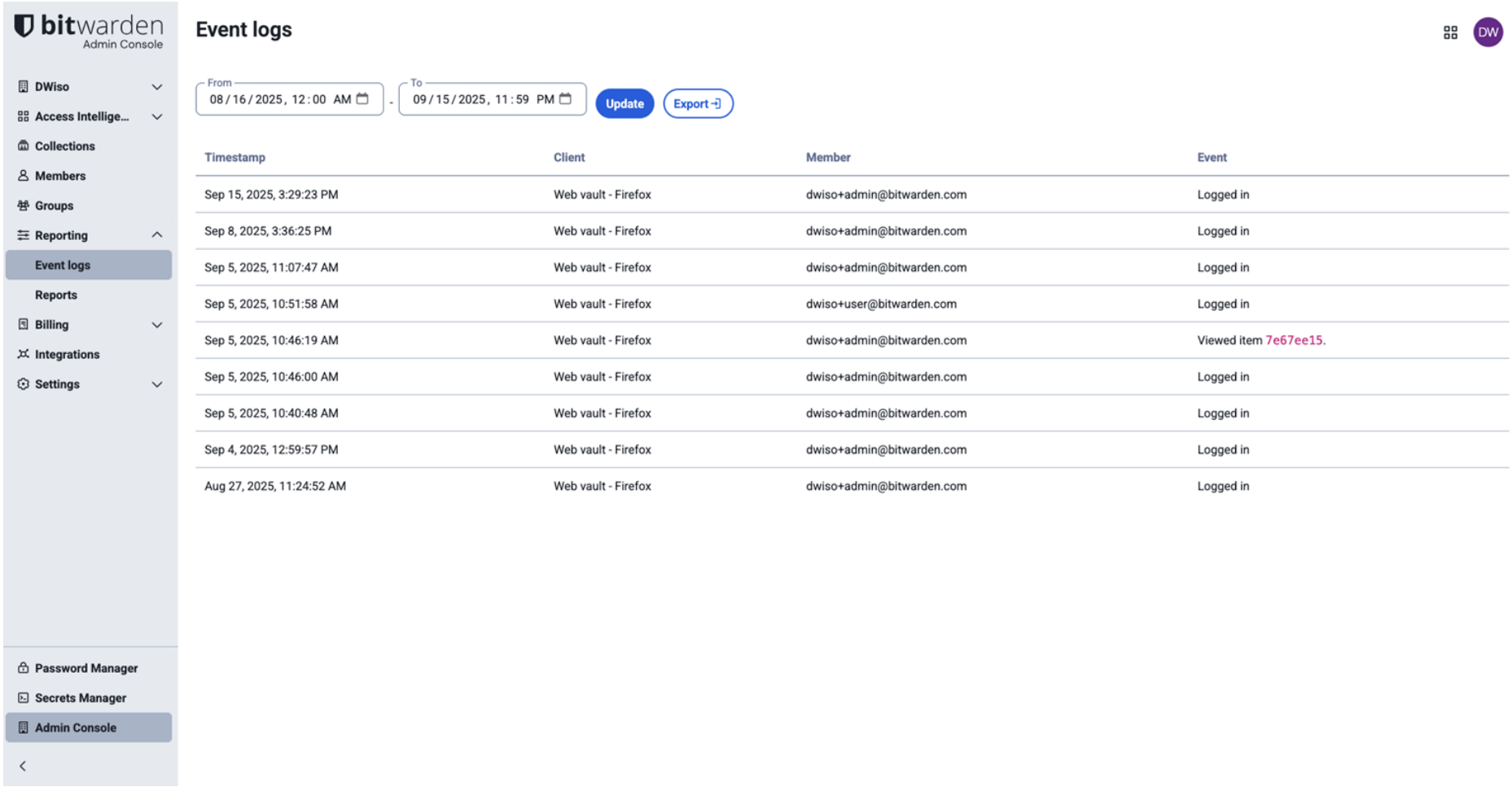
Inactive two-step login

Two-step login adds a layer of protection to your accounts. Set up two-step login using Bitwarden authenticator for these accounts or use an alternative method.

Member access

Ensure members have access to the right credentials and their accounts are secure. Use this report to obtain a CSV of member access and account configurations.

- Password Manager
- Secrets Manager
- Admin Console


bitwarden
Admin Console
DWiso
Access Intellige...
Collections
Members
Groups
Reporting
Event logs
Reports
Billing
Integrations
Settings
Password Manager
Secrets Manager
Admin Console
Event logs
DW
From
08 / 16 / 2025, 12 : 00 AM
To
09 / 15 / 2025, 11 : 59 PM
Update
Export
Timestamp
Client
Member
Event
Sep 15, 2025, 3:29:23 PM
Web vault - Firefox
dwiso+admin@bitwarden.com
Logged in
Sep 8, 2025, 3:36:25 PM
Web vault - Firefox
dwiso+admin@bitwarden.com
Logged in
Sep 5, 2025, 11:07:47 AM
Web vault - Firefox
dwiso+admin@bitwarden.com
Logged in
Sep 5, 2025, 10:51:58 AM
Web vault - Firefox
dwiso+user@bitwarden.com
Logged in
Sep 5, 2025, 10:46:19 AM
Web vault - Firefox
dwiso+admin@bitwarden.com
Viewed item 7e67ee15.
Sep 5, 2025, 10:46:00 AM
Web vault - Firefox
dwiso+admin@bitwarden.com
Logged in
Sep 5, 2025, 10:40:48 AM
Web vault - Firefox
dwiso+admin@bitwarden.com
Logged in
Sep 4, 2025, 12:59:57 PM
Web vault - Firefox
dwiso+admin@bitwarden.com
Logged in
Aug 27, 2025, 11:24:52 AM
Web vault - Firefox
dwiso+admin@bitwarden.com
Logged in

Piani di licenza

	Teams	Enterprise
Vault “zero-knowledge” per web login, note sicure, carte di credito, identità e chiavi SSH	Illimitato	Illimitato
Condivisione sicura dei dati\elementi salvati	Illimitato	Illimitato
Accesso al Password Manager multi-dispositivo	✓	✓
Sincronizzazione multi-dispositivo del vault	✓	✓
Generatore di password	✓	✓
Numero minimo di utenti	1	1
Numero massimo di utenti	Illimitato	Illimitato
Numero massimo di «Raccolte»	Illimitato	Illimitato

	Teams	Enterprise
Export cifrato del vault	✓	✓
Bitwarden Send	Testo e file	Testo e file
Two-step login (2FA)	App di autenticazione, email, Yubikey, FIDO2 e Duo	App di autenticazione, email, Yubikey, FIDO2 e Duo
Supporto Duo per organizzazioni	✓	✓
Allegati cifrati agli elementi	1 GB per utente + 1 GB condivisi	1 GB per utente + 1 GB condivisi
TOTP integrato	✓	✓
Contatti personali di emergenza	✓	✓
Report stato salute del vault	✓	✓

	Teams	Enterprise
Supporto Prioritario	✓	✓
Log Eventi	✓	✓
Gruppi di Utenti	✓	✓
Acceso via API	✓	✓
Directory Connector	✓	✓
Integrazione con Secrets Manager (add-on)	✓	✓
Login via SSO	-	✓

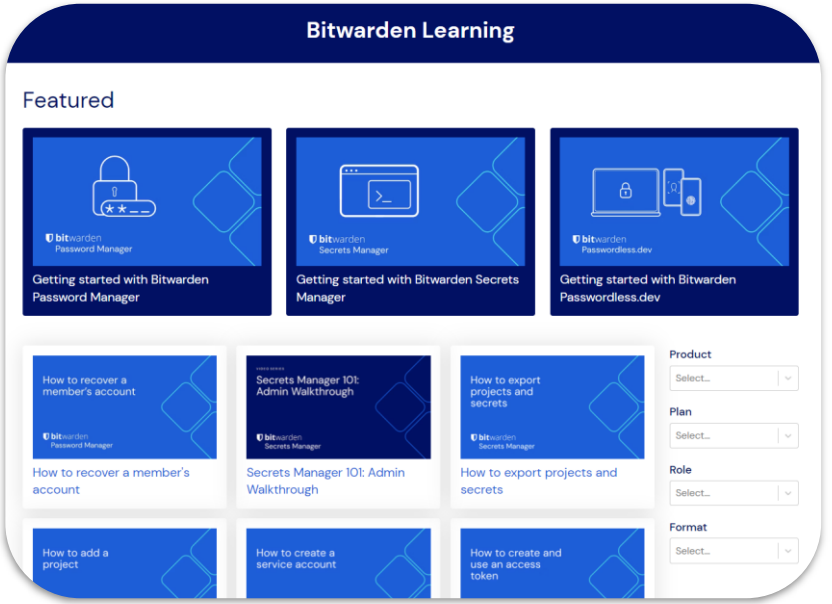
	Teams	Enterprise
Policy Enterprise	-	✓
Recupero Account	-	✓
Installazione Locale	-	✓
Membri: ruolo personalizzato	-	✓
Membri: voucher «Families»	-	✓
Supporto SCIM	✓	✓
Prezzi di riferimento	€48,00\utente\anno	€72,00\utente\anno

Desideri maggiori informazioni?

bitwarden.com/learning

Che tu abbia bisogno di imparare come registrare i tuoi clienti o che tu stia creando il tuo primo oggetto in cassaforte, il Centro di apprendimento Bitwarden ti offre video, guide pratiche e molto altro, con contenuti nuovi e aggiornati ogni mese!

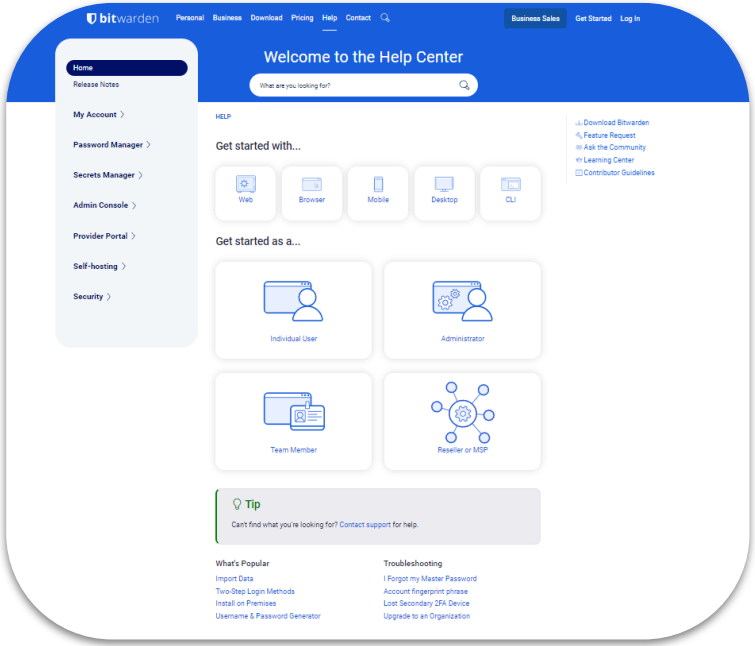
- Bitwarden 101 per l'onboarding di utenti e amministratori
  Password Manager 101: Guida introduttiva per gli utenti
  Password Manager 101: Guida introduttiva per amministratori



bitwarden.com/help

Visita il Centro assistenza per consultare la documentazione relativa a tutti gli aspetti di Bitwarden.

- Elementi della cassaforte
  https://bitwarden.com/help/managing-items/
- Gruppi di utenti
  https://bitwarden.com/help/about-groups/
- Raccolte
  https://bitwarden.com/help/about-collections/
- Inserimento degli utenti e successione
  https://bitwarden.com/help/onboarding-and-succession/
- Qual è il piano più adatto al mio cliente?
  https://bitwarden.com/help/what-plan-is-right-for-me/



Bitwarden Families gratuito

Piano Famiglie gratuito per Enterprise

- Account completamente separato
- Accesso alle funzionalità Premium
- Condivisione con un massimo di 5 familiari o amici
- Mantieni l'account per sempre

Cosa succede se me ne vado?

I tuoi dati rimangono tuoi, in ogni caso.

Intelligence sugli Accessi

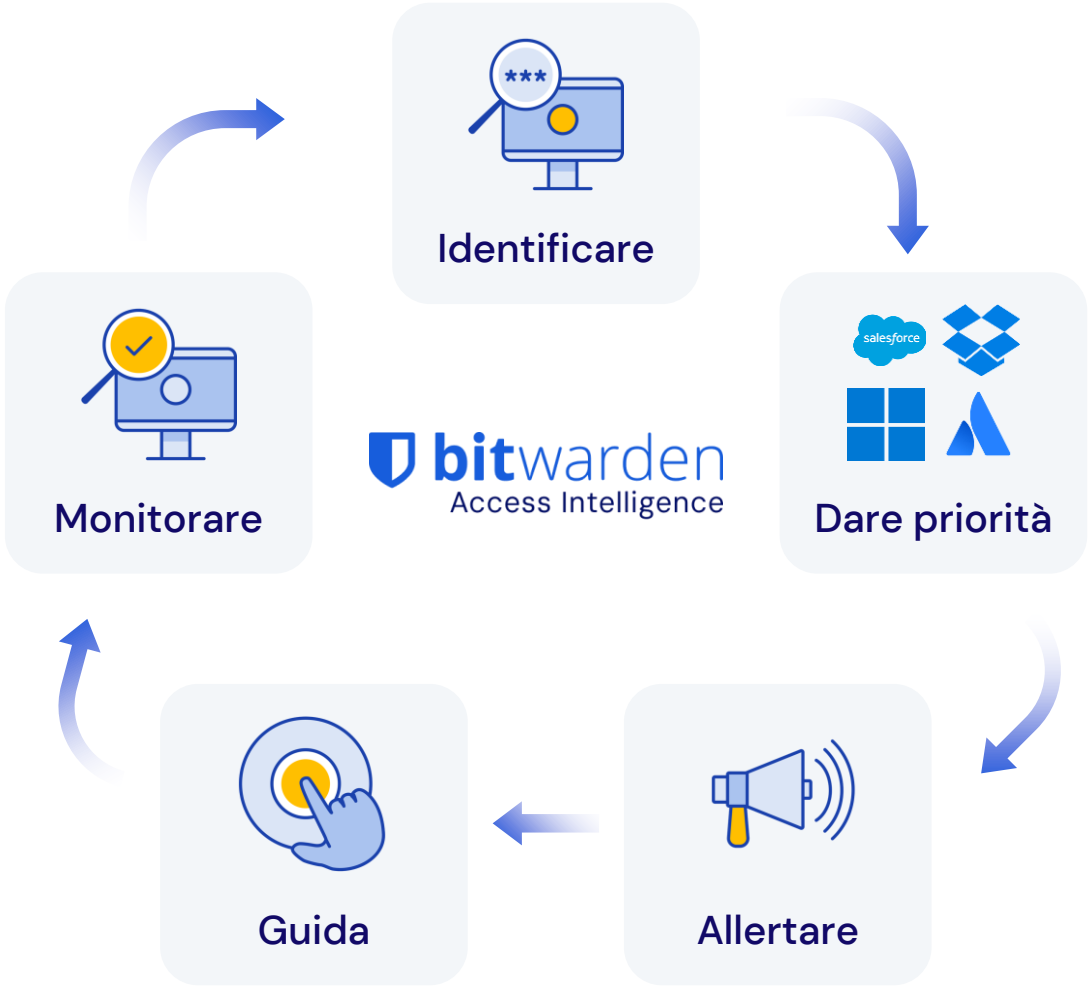
Perché la “Intelligence sugli Accessi” è diversa

1. **Visibilità delle applicazioni:** ottieni visibilità sulle credenziali a rischio e sulle applicazioni associate, garantendo una comprensione contestuale della postura di sicurezza dell'azienda.

2. **Dai priorità a ciò che è importante:** dai priorità alle applicazioni critiche per un monitoraggio e una correzione accurati, assicurandoti che le applicazioni più critiche siano protette per prime.

3. **Rimedio guidato:** è facile per gli utenti finali aggiornare le credenziali una volta ricevuto un avviso di credenziali a rischio, guidandoli direttamente alla schermata di modifica della password dell'applicazione e offrendo loro la possibilità di generare e salvare una nuova password forte.

4. **Difesa dal phishing:** Bitwarden offre una protezione superiore contro il phishing che identifica automaticamente e reindirizza gli utenti lontano dai siti di phishing.


Identificare
Dare priorità
Allertare
Guida
Monitorare
bitwarden
Access Intelligence

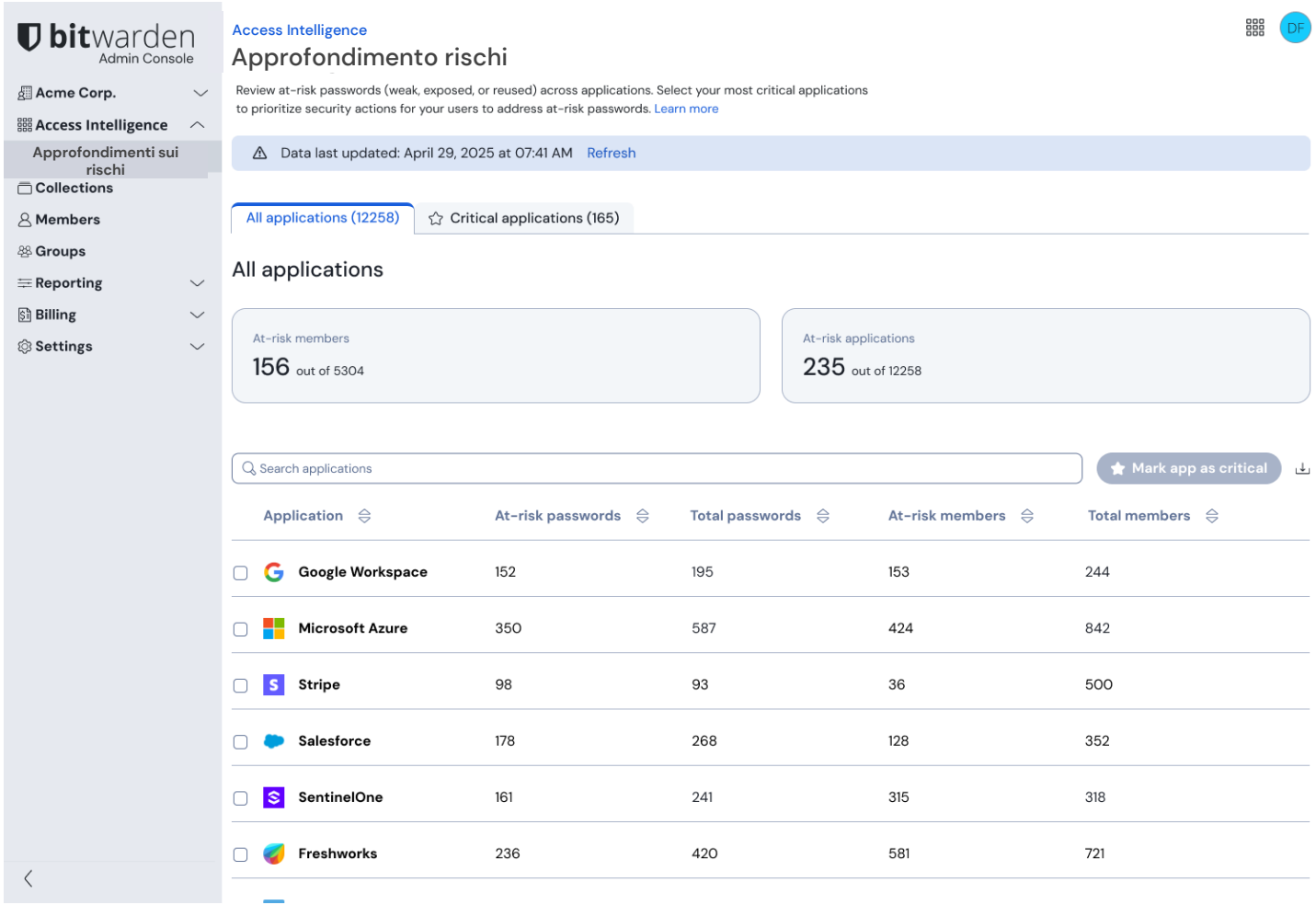
Intelligence sugli Accessi

Approfondimento Rischi - Screenshot

bitwarden

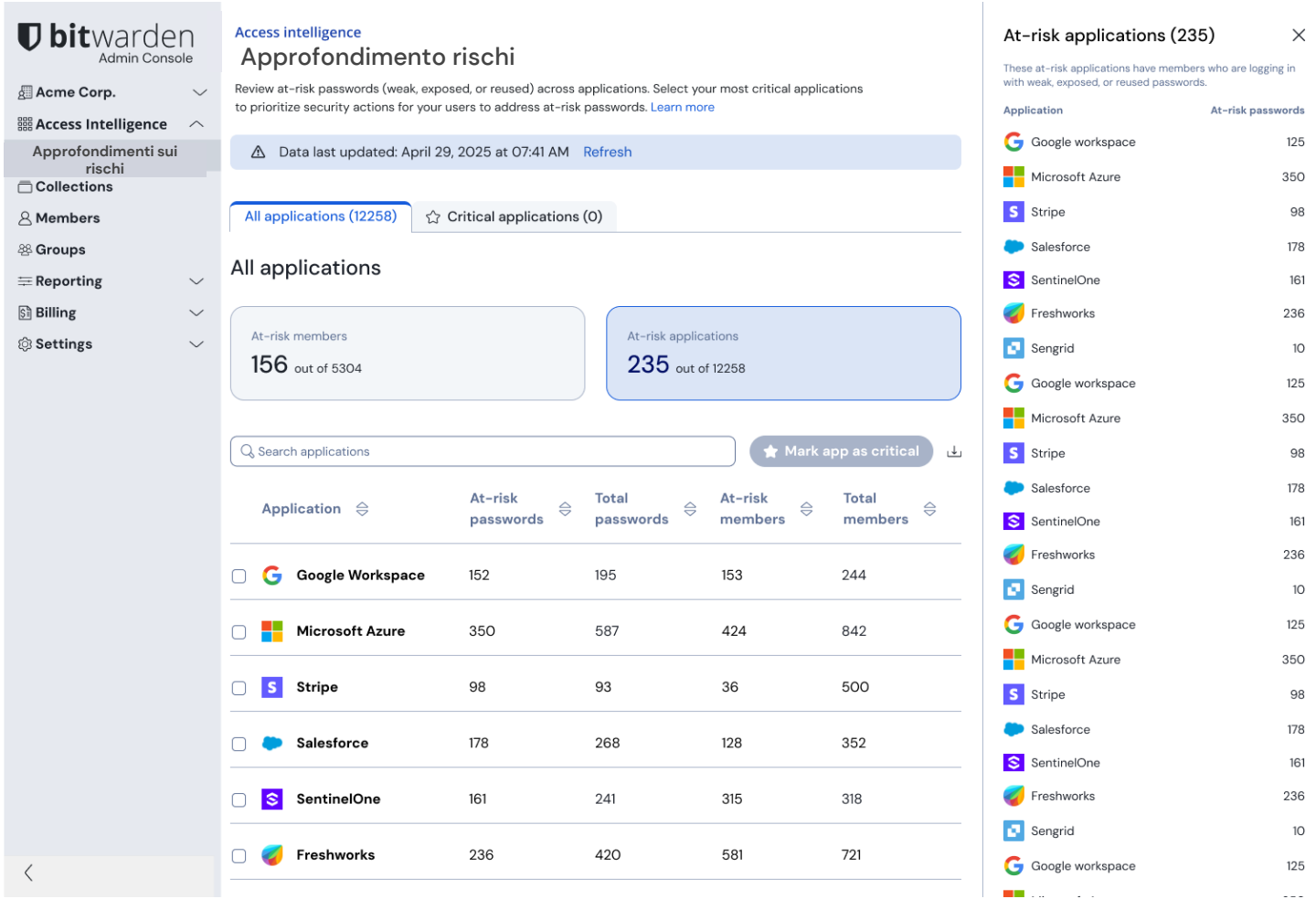
Dashboard Approfondimento Rischi

- Disponibile tramite la Console di amministrazione.
- Le altre dashboard sono statiche.
- "Approfondimento Rischi" aiuta amministratori e dipendenti ad agire.



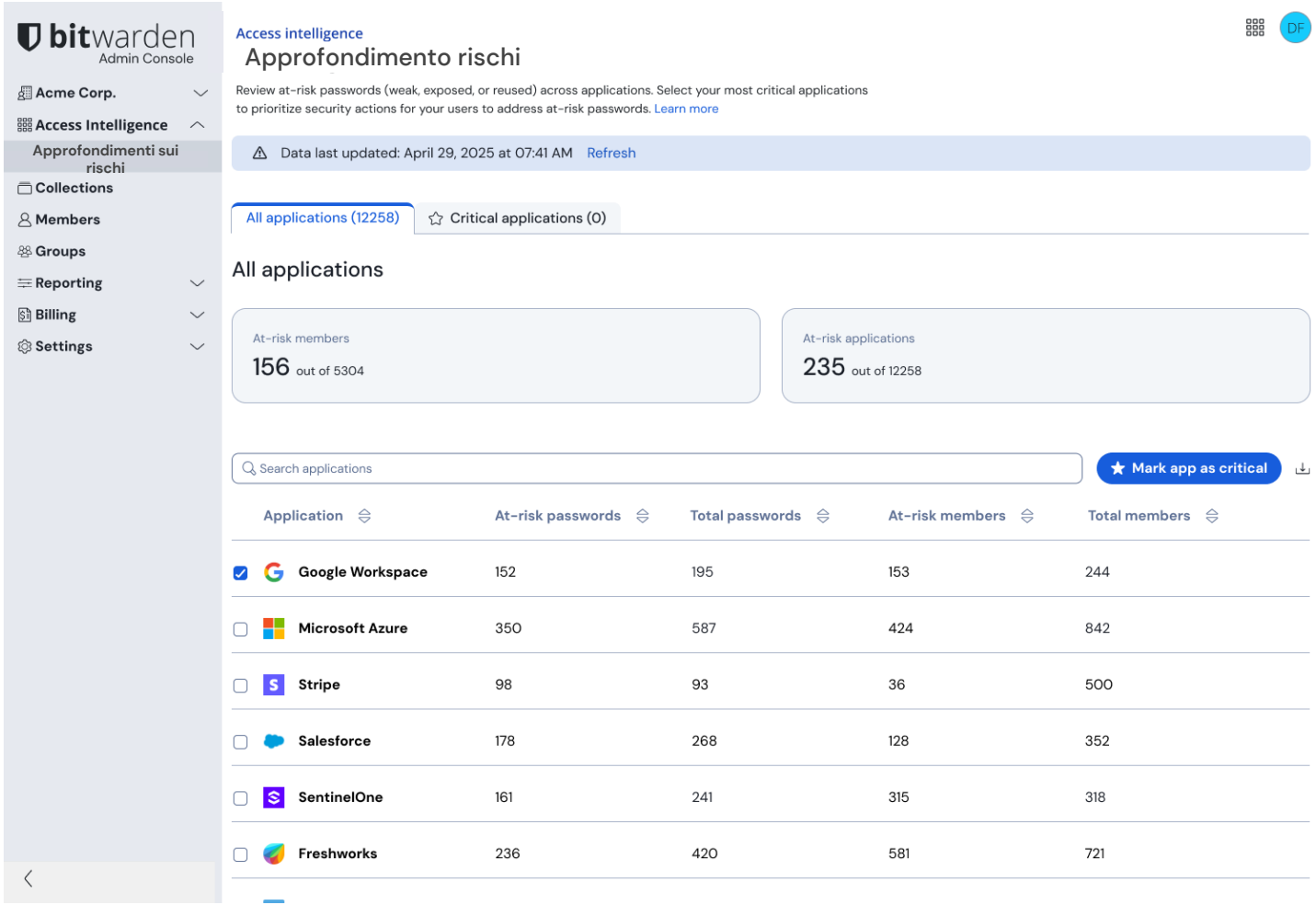
Identifica: tutte le applicazioni

- Possibilità di visualizzare tutte le applicazioni con accessi associati nella tua organizzazione.
- Le password a rischio sono password deboli, riutilizzate, senza 2FA o esposte.
- Restringi i risultati per visualizzare solo le applicazioni a rischio.



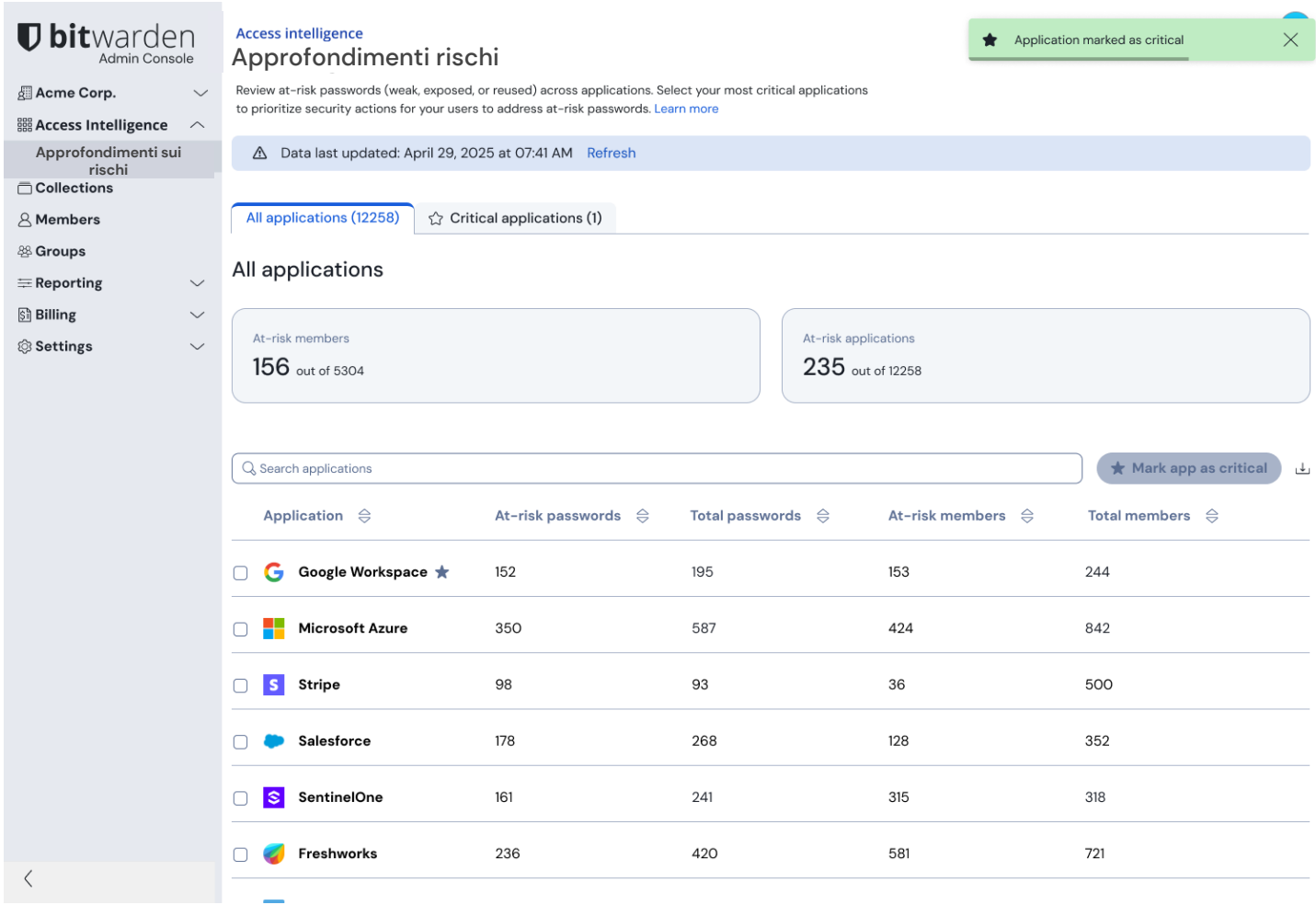
Assegna priorità: contrassegna l'app come critica

- Assicura che le applicazioni più critiche siano protette per prime.
- Applicazioni critiche per l'azienda come CRM, ecosistemi di lavoro e strumenti di pianificazione finanziaria.
- Contrassegna le applicazioni come critiche per ulteriori interventi correttivi.



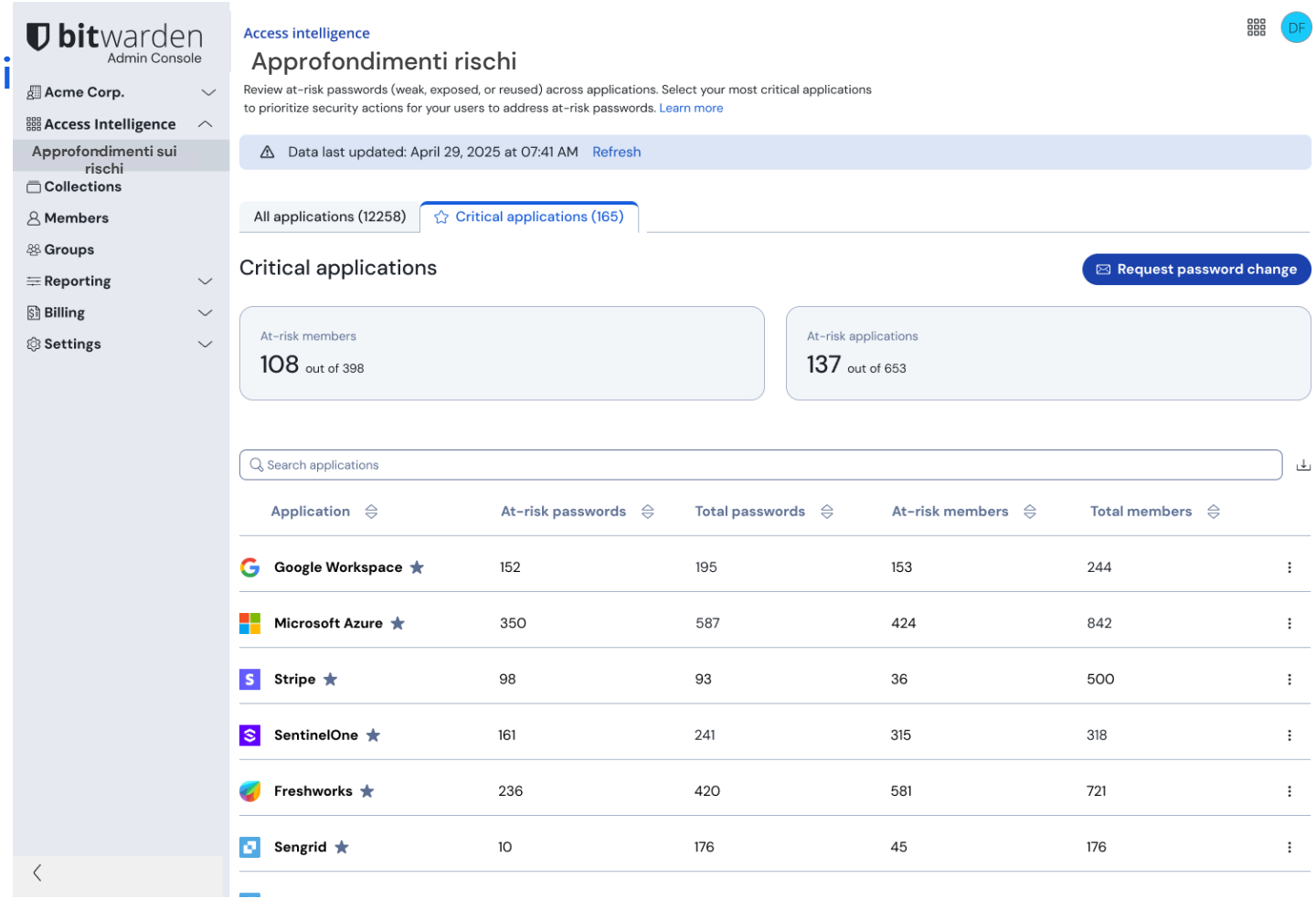
Assegna priorità: contrassegna l'app come critica

- Assicura che le applicazioni più critiche siano protette per prime.
- Applicazioni critiche per l'azienda come CRM, ecosistemi di lavoro e strumenti di pianificazione finanziaria.
- Contrassegna le applicazioni come critiche per ulteriori interventi correttivi.



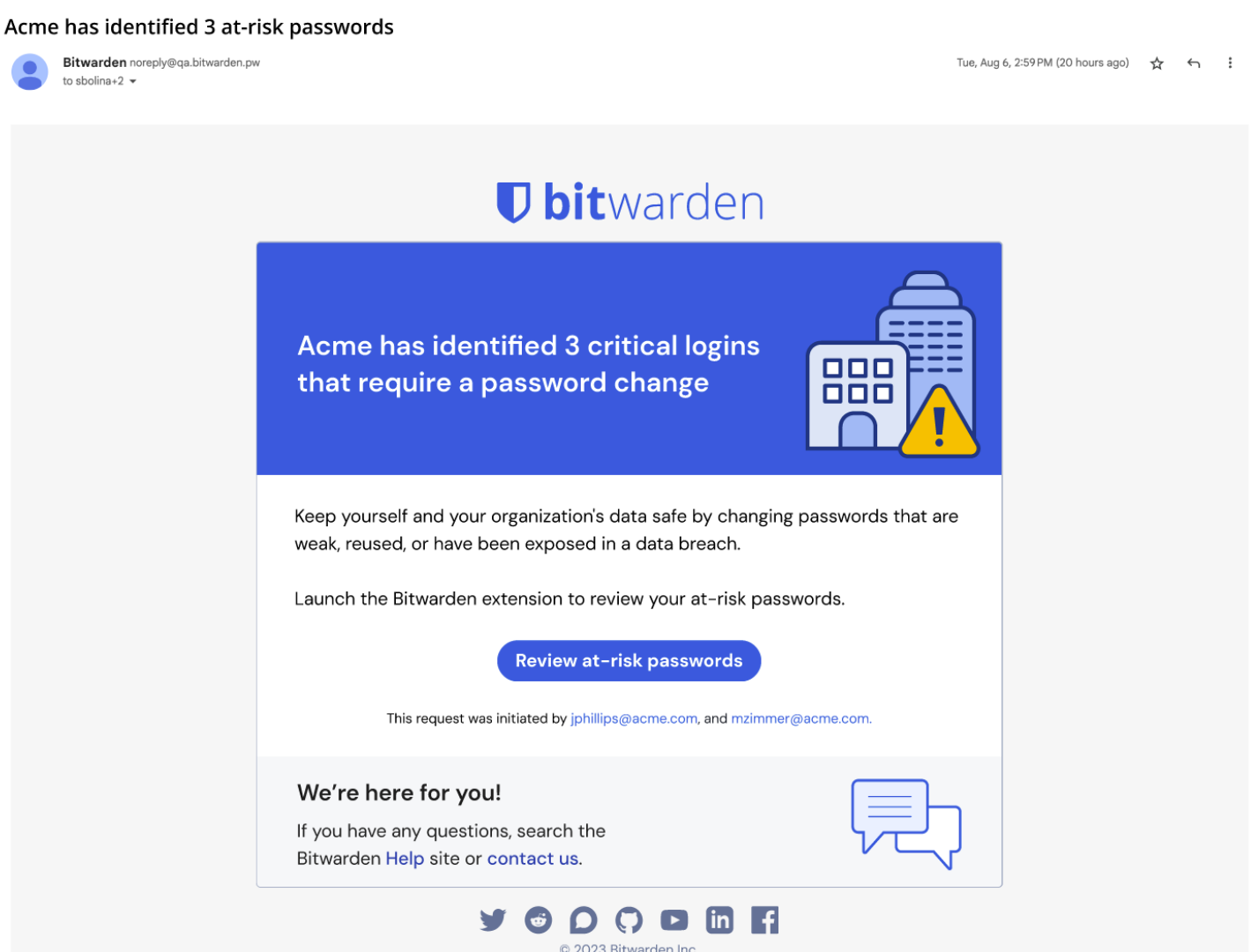
Priorità: Applicazioni critiche

- Visualizza tutte le applicazioni critiche per l'azienda e le credenziali e gli utenti a rischio associati.
- Richiedere una modifica della password per avvisare immediatamente tutti i dipendenti con credenziali a rischio.



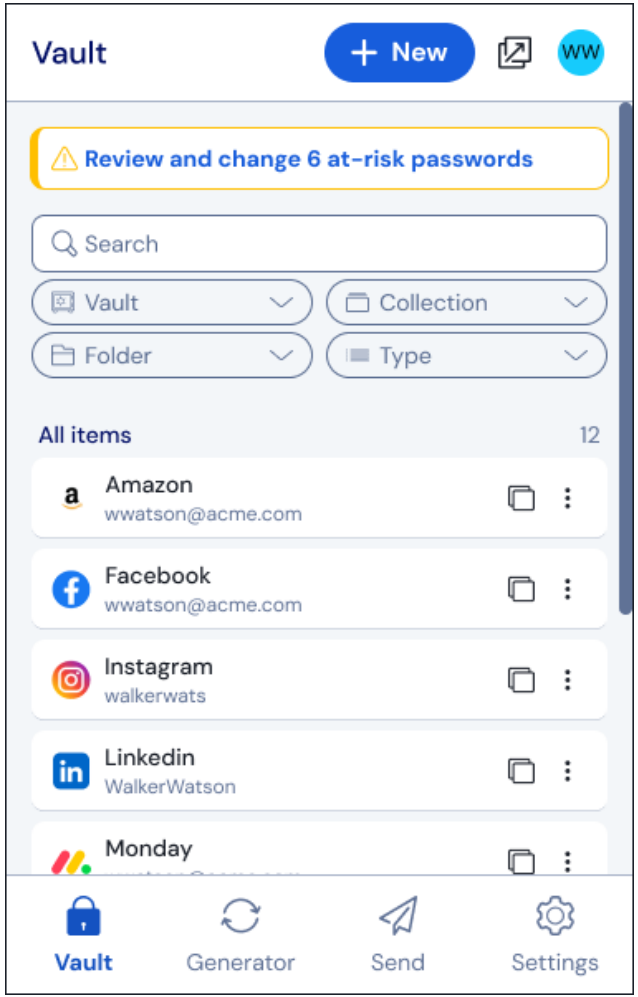
Avviso: Notifica via e-mail ai dipendenti

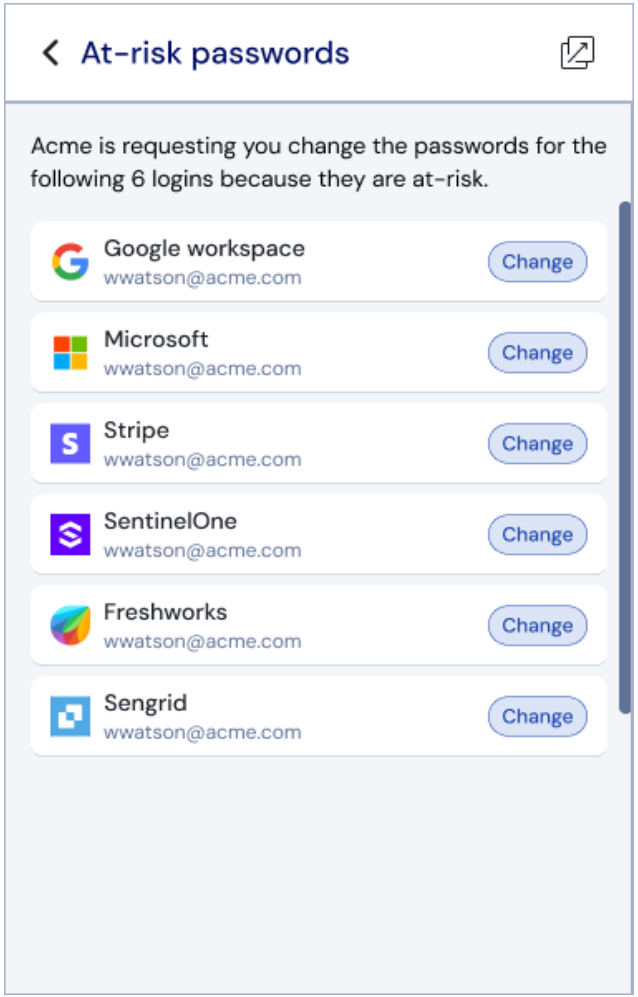
- La richiesta di modifica della password attiva le notifiche per i dipendenti.
- Cliccando su "**Rivedi password a rischio**" i dipendenti verranno reindirizzati all'estensione del browser Bitwarden.



Avviso: Notifiche in-app

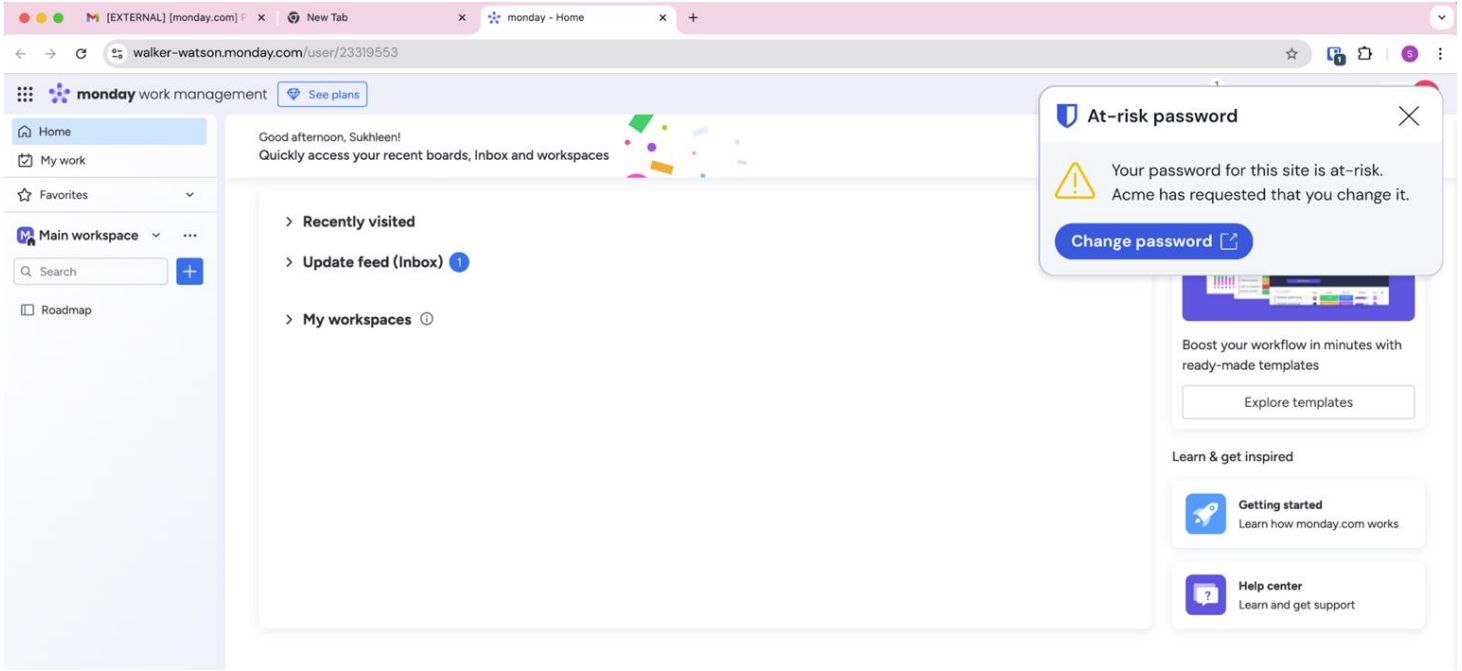
- I dipendenti ricevono anche notifiche in-app.
- Esamina l'elenco completo delle password a rischio che richiedono un aggiornamento.





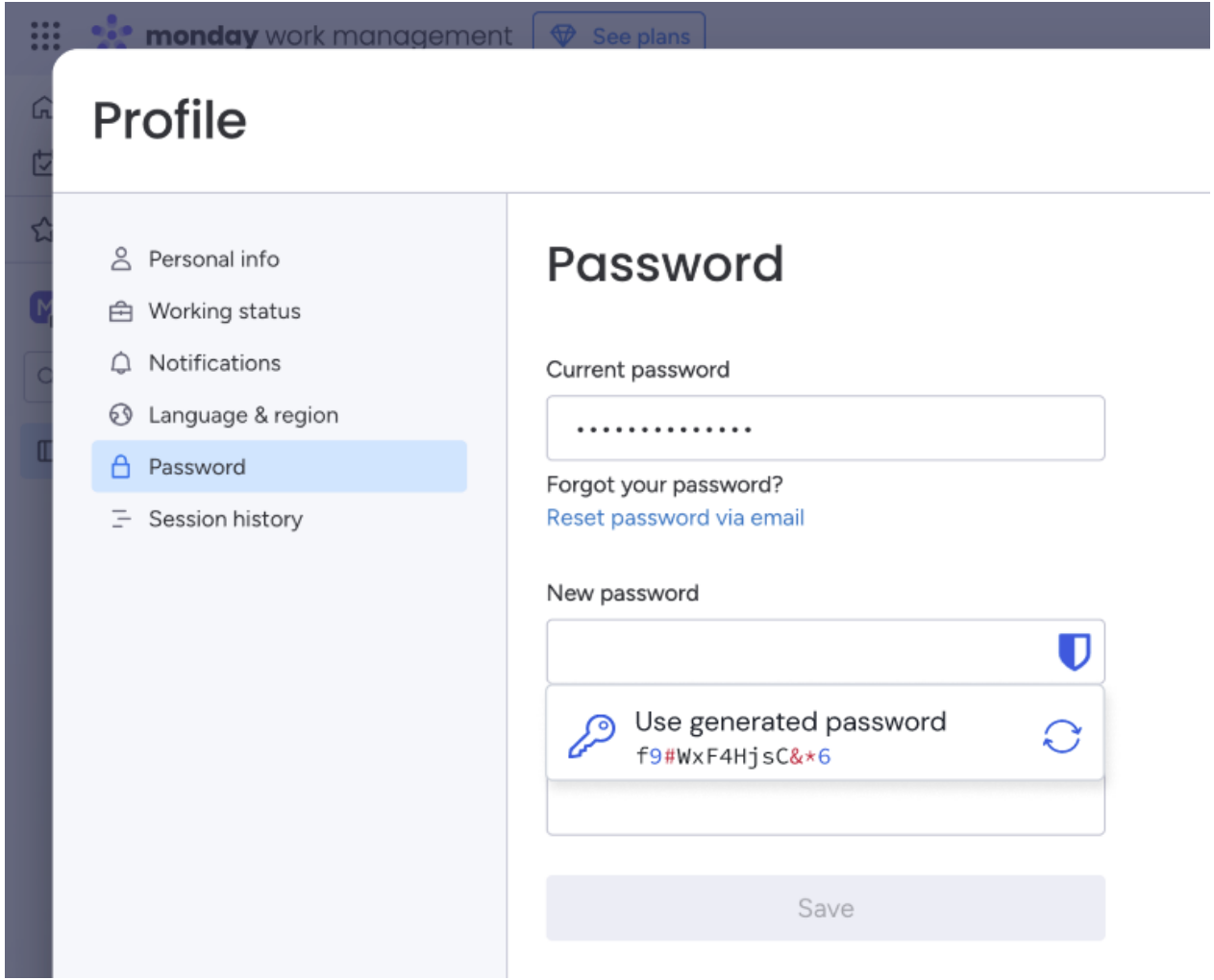
Avviso: Notifiche dell'applicazione

- Il dipendente accede a un sito web con una password a rischio associata
- Ricevi una richiesta di aggiornamento della password



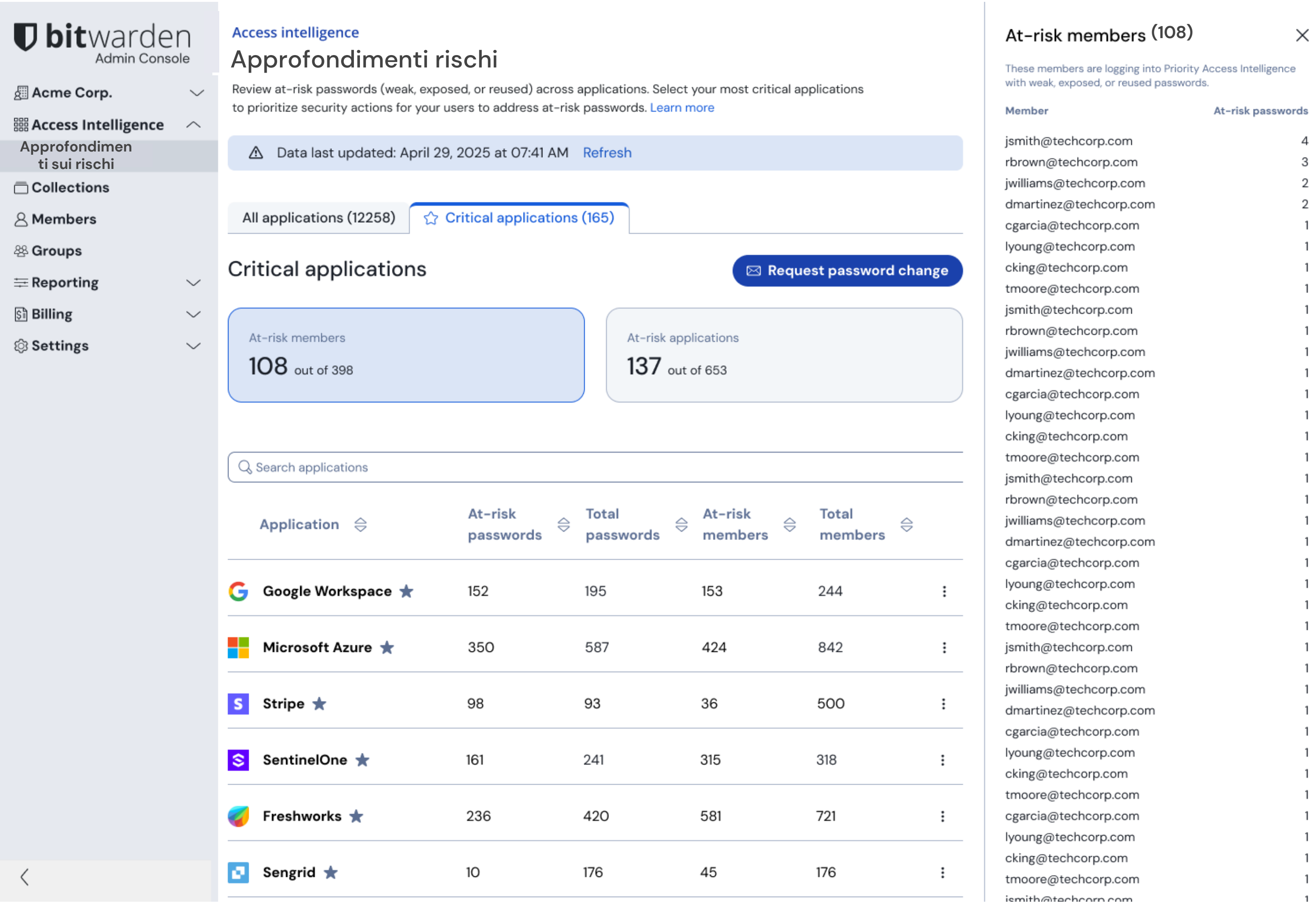
Guida: Aggiornamento password

- Bitwarden reindirizza automaticamente i dipendenti al modulo di modifica password associato a tale applicazione.
- Suggerisce una password alternativa forte e generata in modo casuale, quindi la salva.
- È semplicissimo intervenire sulle password deboli e rafforzare la sicurezza aziendale.



Monitoraggio: membri a rischio

- Monitora i progressi verso le modifiche sicure suggerite.
- Ispeziona i membri a rischio per ulteriori azioni.
- Ricomincia il processo con altre applicazioni.

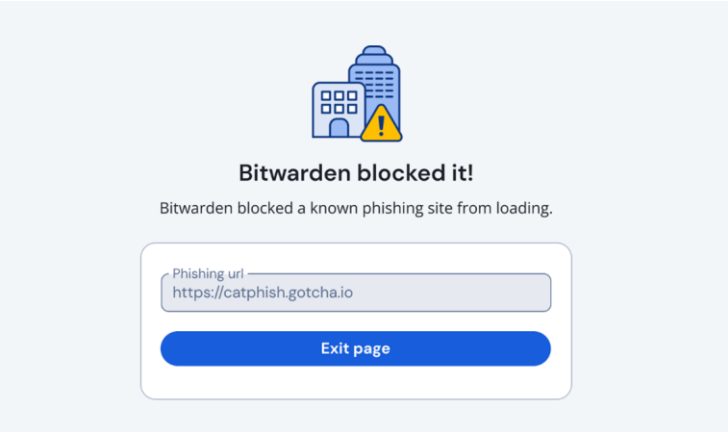


Intelligence degli Accessi

Blocco avanzato del phishing

bitwarden

Blocco avanzato del phishing



- Identifica i siti di phishing noti tramite estensione del browser
- Reindirizza immediatamente l'utente lontano dal sito
- Le future versioni del prodotto offriranno agli amministratori IT visibilità sui rischi di phishing all'interno dell'organizzazione
- Bitwarden utilizza Phishing.Database, un repository open source aggiornato regolarmente, per identificare e bloccare i link di phishing

Thank you!

bitwarden


bitwarden