



REMEDIAZION

# DATA RISK ASSESSMENT

REDATA PER UMBRELLA CORP

RISULTATI CRITICI

0 10 20 30 40 50 60 70

DATA DI REDAZIONE: 3.1.24

# TABELLA DEI CONTENUTI

<b>Impatto aziendale</b>	<b>03</b>
<b>Panoramica della valutazione</b>	<b>04</b>
<b>Risultati critici</b>	<b>05</b>
<b>Risultati dettagliati</b>	<b>10</b>
Postura di sicurezza dei dati	
Analisi delle minacce	
Rischio di configurazione	
Rischio di identità	
Rischio Salesforce	
<b>Passaggi successivi</b>	<b>31</b>



**“Sono rimasto sorpreso dalla rapidità con cui Varonis è riuscita a classificare i dati e scoprirne potenziali esposizioni durante la valutazione gratuita. È stato davvero illuminante”.**

Michael Smith, CISO, HKS

# PERCHÉ UMBRELLA CORP HA AVVIATO UNA VALUTAZIONE DEL RISCHIO DEI DATI DI VARONIS?

Umbrella Corp ha un requisito a livello di consiglio di amministrazione che impone di rilevare, classificare ed etichettare tutti i PII per garantire la conformità e l'efficacia DLP a valle. Il recente incidente ransomware di Umbrella Corp evidenzia l'esigenza di monitorare i dati. Senza l'intervento, l'azienda deve affrontare molte normative e livelli di esposizione dei dati non gradite alla dirigenza.

## Sfide



Classificare i dati sensibili e risolvere le esposizioni è arduo.



La quantificazione della postura di sicurezza dei dati e la presentazione dei progressi al consiglio di amministrazione è un obbligo.



L'impegno di remediation dei dati è difficile se il team è di dimensioni ridotte.



È necessario monitorare l'utilizzo dei dati e inviare alert in caso di attività anomala.



Le sottunità operano autonomamente: è necessario un programma unificato per la sicurezza dei dati.



I controlli di conformità sono manuali e incompleti.

# PANORAMICA SULLA VALUTAZIONE DEL RISCHIO DI UMBRELLA CORP

## Fonti di dati collegate e tempistica di valutazione

Varonis può connettersi a decine di fonti di dati aggiuntive. L'installazione richiede pochi minuti.



Microsoft 365

Active Directory  
+ Azure AD

Salesforce

Condivisioni  
file Windows

Google  
Workspace

**Installazione della  
piattaforma**  
1 giugno 2023

**Valutazione**

**Prova del valore**  
21 giugno 2023

**5,6 milioni**

di risorse  
(file/oggetti)

**12.000**

Identità

**805.000**

di eventi  
(media giornaliera)

**2,4 milioni**

di dati  
sensibili classificati  
(PHI, PCI, segreti)

Nota: solo una parte dell'ambiente complessivo di Umbrella Corp è stata collegata per il POC.

# RISULTATI CRITICI

## Rischi che potrebbero comportare un data breach

Di seguito sono riportati i quattro principali risultati che Varonis ritiene un rischio critico per la sicurezza dei dati.

1

Report sulle retribuzioni delle risorse umane condivisi pubblicamente tramite collegamenti "chiunque".

2

332 utenti di Salesforce possono esportare i dati di produzione.

3

Un utente esterno è un super admin in Google Workspace.

4

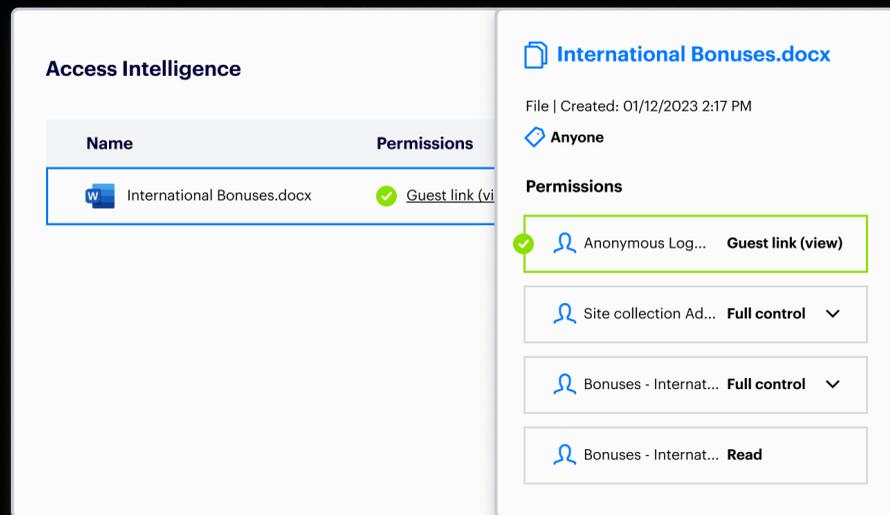
Un assistente di marketing ha attivato un alert per un accesso anomalo ai dati.



## CONCLUSIONE CRITICA N. 1

# Report sulle retribuzioni delle risorse umane condivisi pubblicamente tramite collegamenti "chiunque".

Melissa Donovan ha accidentalmente pubblicato su Internet le informazioni sui bonus dell'azienda.



**Tipo di rischio:**  
esposizione pubblica dei dati

**Controllo NIST:**  
AC-3(9): Versione controllata

**Sistema interessato:**  
Microsoft 365

**Osservazione:**  
Melissa Donovan, un partner aziendale HR, ha caricato International Bonuses.docx sul suo sito di HR Teams il 12 gennaio. La scansione di classificazione di Varonis ha individuato 231 istanze di PII all'interno del file e i nostri log mostrano che ha creato il link "Anyone" il 13 febbraio, esponendo il file a Internet. Al link hanno avuto accesso utenti anonimi da 27 diversi indirizzi IP in tutto il mondo.

**Raccomandazione:**  
revocare immediatamente l'accesso "a chiunque" a questo file disabilitando il collegamento. Disattivare la possibilità di condividere pubblicamente. Utilizzare l'automazione Varonis per revocare qualsiasi collegamento pubblico a file contenenti informazioni sensibili.

## CONCLUSIONE CRITICA N. 2

# 332 utenti di Salesforce possono esportare i dati di produzione.

Il normale profilo "Vendite" garantisce l'accesso all'esportazione. Questo accesso è troppo ampio e deve essere corretto.

The screenshot shows the 'Export Reports' configuration page in Salesforce. It displays a table of users with the following columns: Name, Email, Service, and Last Active. The table shows three users: Melissa Do..., Josh Hamm..., and Jerome Boy... All three users have the 'Producti...' service and their last active dates are in 2022.

Name	Email	Service	Last Active
Melissa Do...	user1@acmelab.com	Producti...	Mar. 3, 2022 10:12 AM (GMT...
Josh Hamm...	user2@acmelab.com	Producti...	Sept. 18, 2022 09:51 AM (GMT...
Jerome Boy...	user3@acmelab.com	Producti...	Sept. 22, 2022 08:30 AM (GMT...

**Tipo di rischio:**  
Esposizione dei dati sensibili

**Controllo NIST:**  
AC-2(7): schemi basati su ruoli

**Sistema interessato:**  
Salesforce (produzione, sandbox, sviluppo)

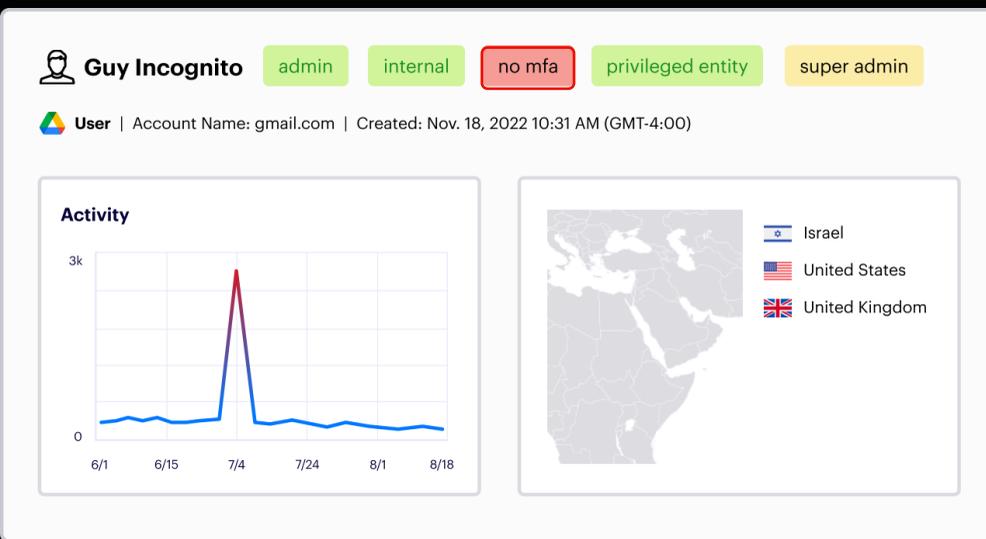
**Osservazione:**  
Le scansioni di Varonis hanno individuato una combinazione pericolosa di autorizzazioni che crea un grave rischio di data exfiltration: 332 venditori, tramite il loro profilo "Vendite", possono esportare tutti i dati relativi a lead, contatti, opportunità e account dall'istanza Salesforce di produzione di Umbrella Corp.

**Raccomandazione:**  
rimuovere l'autorizzazione per l'esportazione del report dal profilo "Vendite" e da qualsiasi altro ruolo non amministratore. Esaminare tutti i profili e i set di autorizzazioni che concedono azioni con privilegi elevati, ad esempio esportare report, modificare tutti i dati e leggere tutti i dati.

### CONCLUSIONE CRITICA N. 3

## Un utente esterno è un super admin in Google Workspace.

Guy Incognito è un super admin senza autenticazione multipla. La sua attività ha avuto un picco il 4 luglio, fatto che ha fatto scattare un alert.



#### Tipo di rischio:

account amministratore non sicuro

#### Controllo NIST:

AC-2(7): account utente privilegiati

#### Sistema interessato:

Google Workspace

#### Osservazione:

Guy Incognito è un appaltatore esterno che utilizza un account Gmail personale per accedere all'account Google Workspace di Umbrella Corp. Questo utente ha diritti di super amministratore e non ha abilitato l'MFA. Questo account è considerato ad altissimo rischio.

#### Raccomandazione:

applicare immediatamente l'autenticazione a più fattori sull'account di Guy Incognito e aggiungerlo alla lista di controllo di Varonis. Rivedere gli ultimi 30 giorni di attività, i diritti e le identità correlate dell'utente. Decidere se questo utente esterno ha davvero necessità di avere i diritti di super admin.

## CONCLUSIONE CRITICA N. 4

# Un assistente di marketing ha attivato un alert di accesso anomalo ai dati.

Darren York non deve avere accesso a dati finanziari. UEBA Varonis ha rilevato un accesso anomalo.

### Abnormal download of sensitive data from cloud data stores

Warning

Exfiltration | 06/11/2023 8:19 PM | Status: Open | Alert ID: 123F...

#### What happened

varonis.onmicrosoft.com (Azure)\Darren York has downloaded **825 sensitive files**, exceeding the account's or organization's normal behavior (20 files).

A statistical increase in the number of sensitive files downloaded from cloud data stores has been detected. This may indicate a **potential data theft or activity** that requires attention.

#### Tipo di rischio:

comportamento anomalo degli utenti

#### Controllo NIST:

AC-2(7): monitoraggio dell'account per

#### Sistema interessato:

Google Workspace

#### Osservazione:

l'assistente al marketing Darren York ha attivato un alert basato sul comportamento deviando dalla sua normale baseline per l'accesso ai dati. Varonis ha rilevato che l'utente stava accedendo ai file con dati finanziari, fatto atipico per il suo ruolo.

#### Raccomandazione:

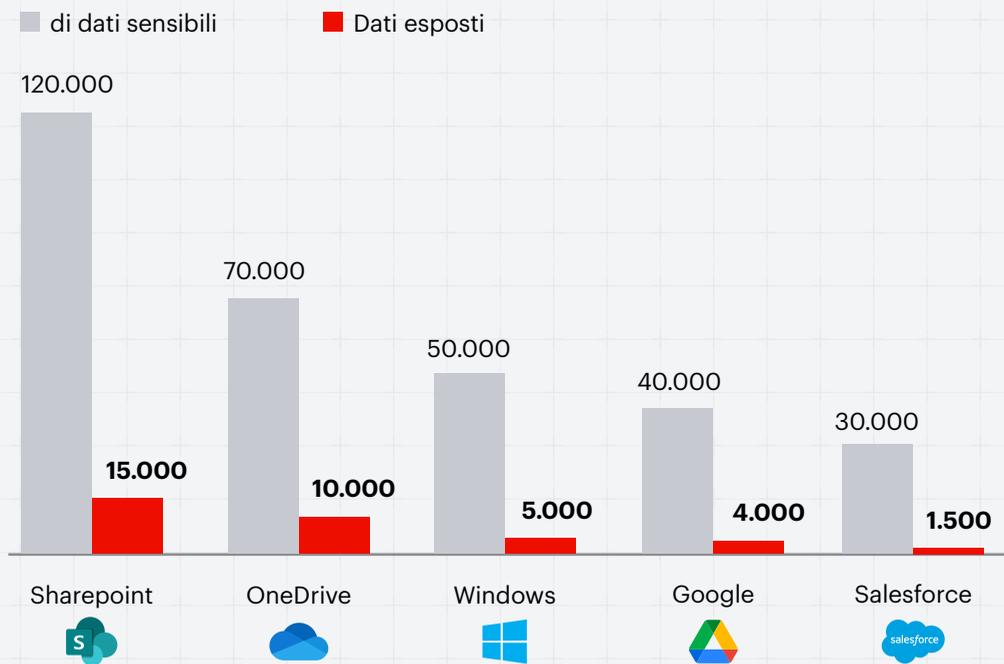
utilizzare Varonis per eseguire una query per visualizzare tutte le attività di Darren negli ultimi 30 giorni. Assicurarsi che le autorizzazioni per i dati contenenti record finanziari siano accessibili solo ai dipendenti che necessitano di accesso.

# POSTURA DI SICUREZZA DEI DATI

I dati sensibili di Umbrella Corp sono distribuiti su più servizi cloud e data store on-prem. Per ridurre al minimo il rischio di un data breach, è fondamentale che l'azienda abbia visibilità e controllo in tempo reale sul suo patrimonio di dati in rapida evoluzione, con classificazione unificata, rilevamento delle minacce e applicazione delle policy.

RISULTATI DETTAGLIATI

## Dove sono i dati più sensibili di Umbrella Corp e quanto sono a rischio?



## Principali indicatori di rischio:

<p><b>310.000</b> dati sensibili</p>	<p><b>27.000</b> eventi su dati sensibili al giorno</p>
<p><b>24.500</b> dati sensibili esposti a livello di organizzazione</p>	<p><b>11.000</b> dati sensibili esposti esternamente</p>

# Rilevamento e classificazione dei dati

## Criteria di classificazione abilitati

Abbiamo attivato 85 regole integrate e creato tre regole personalizzate durante questa valutazione del rischio. I primi quattro tipi di dati per volume sono mostrati di seguito.



### PCI-DSS

**Contenitori:** 1.160  
**Oggetti:** 12.421  
**Record:** 89.924



### Password

**Contenitori:** 160  
**Oggetti:** 421  
**Record:** 923



### PII statunitensi

**Contenitori:** 2.620  
**Oggetti:** 72.245  
**Record:** 199.104



### Codice documentazione

**Contenitori:** 1.002  
**Oggetti:** 92.420  
**Record:** 799.922

## Codice documentazione

PII	GDPR	Credenziali	Finanziario	FEDERALI
HIPAA PHI 2.0	GDPR Germania	Password	PCI-DSS 2.0	ITAR
Legge sulla privacy del Colorado	GDPR Francia	Chiavi private	SOX	Top Secret
SHIELD Act NY	GDPR Austria	Certificati	GLBA	CUI

Più altre centinaia di regole, schemi e dizionari

## La potenza della classificazione dei dati Varonis

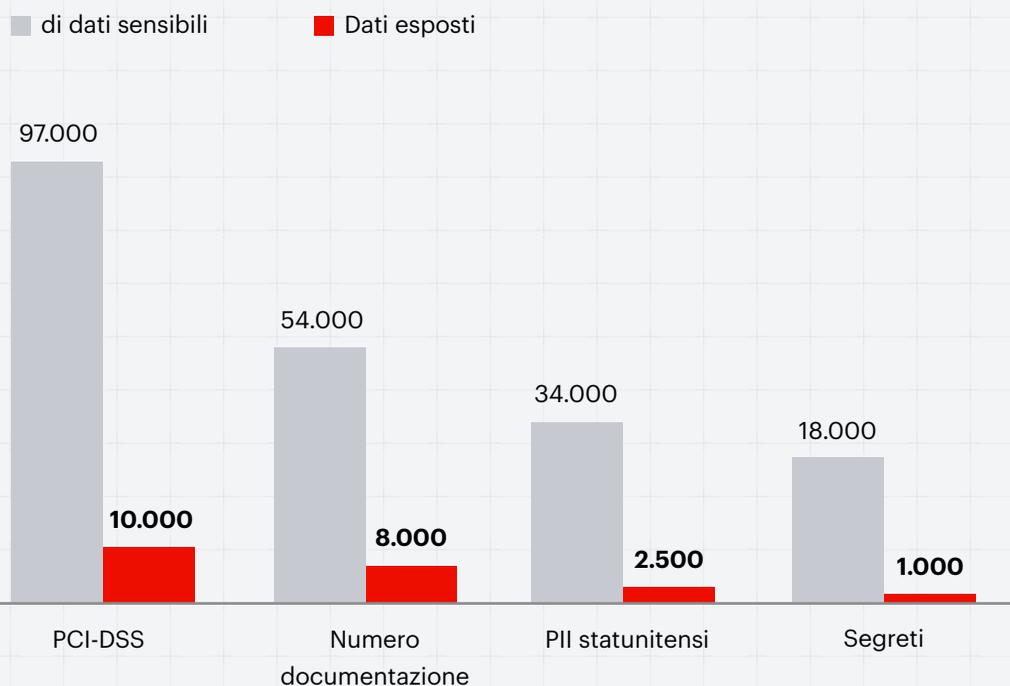
- + Scansione incrementale reale per un'individuazione efficiente e scalabile su set di dati di grandi dimensioni
- + Criteri di classificazione unificati in tutti i data store supportati
- + Testato sul campo in ambienti multi-petabyte
- + Oltre 400 regole create e testate da esperti
- + disponibili (e in crescita) pronte all'uso
- + Ambiti di scansione e campionamento personalizzabili

# Esposizione ai dati di Microsoft 365

L'esposizione ai dati in M365 non è unica per Umbrella Corp. L'azienda media dispone di oltre 40 milioni di autorizzazioni univoche per i propri dati multi-cloud e, secondo Microsoft, oltre il 50% delle autorizzazioni sono ad alto rischio e in grado di causare danni catastrofici se configurate in modo errato.

RISULTATI DETTAGLIATI

## Che tipo di dati risiedono in M365 e qual è l'esposizione di Umbrella Corp?



## Principali indicatori di rischio:

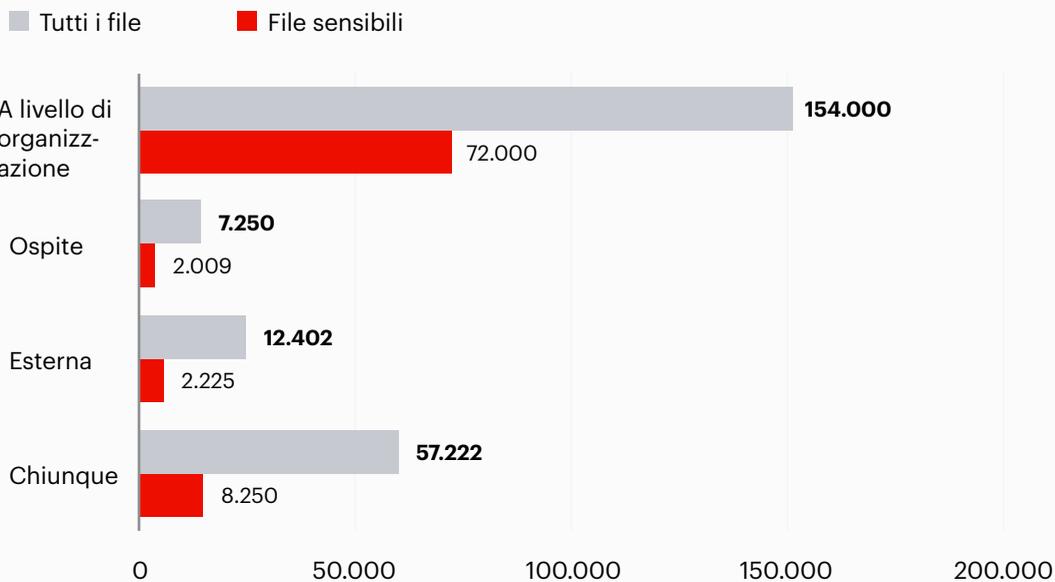


# Rischio di collaborazione

## Livelli di esposizione

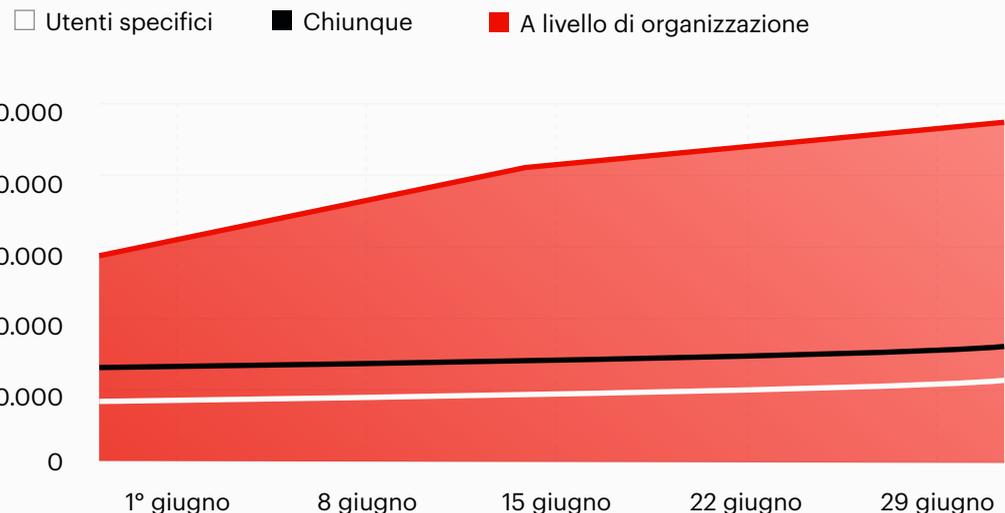
Condivisione dei link è utile per la collaborazione, ma può esporre i dati a tutti i membri dell'organizzazione, agli utenti guest o a Internet. Umbrella Corp ha una notevole esposizione dei dati sensibili grazie ai collegamenti in SharePoint e OneDrive.

### SharePoint Online e OneDrive



## Crescita link condiviso

Il blast radius di Umbrella Corp. sta crescendo rapidamente di settimana in settimana. Di seguito è riportato un grafico della crescita dei link per tipo durante il periodo di valutazione dei rischi.



# Dati esposti pubblicamente

## Dati esposti pubblicamente tramite collegamenti “chiunque”

Di seguito è riportato un piccolo esempio di file sensibili accessibili a chiunque su Internet. L'audit trail Varonis mostra il tipo di dati all'interno del file (PCI, PHI, ecc.), chi ha condiviso il link, quando e se è stato effettuato l'accesso al file tramite il link.

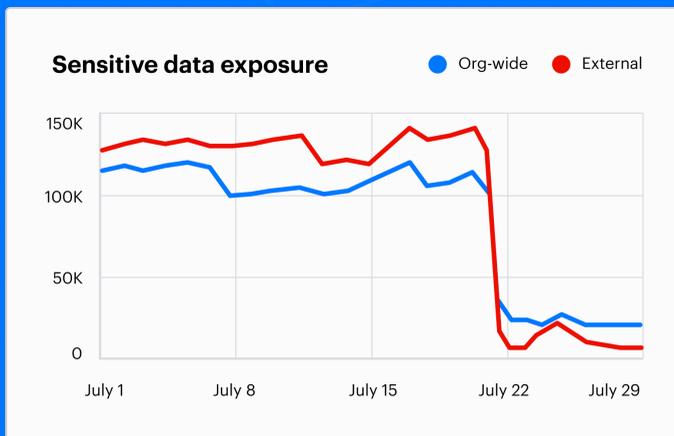
	File type	Name (resource)	Classification category	Total record
1	<input type="checkbox"/>	 JV costs for Feb-Apr.xls	*Credentials (6)	28
	<input type="checkbox"/>	 JV costs for Feb-Apr.xls	*Credentials (4)	22
	<input type="checkbox"/>	 Transaction-English-06.xls	*Credentials (4)	22
	<input type="checkbox"/>	 GL Entry.ppt	*Credentials (4)	22
2	<input type="checkbox"/>	 Employee Agreement.docx	*Financial (3)	21
	<input type="checkbox"/>	 Employee Agreement.docx	*Financial (3)	21
	<input type="checkbox"/>	 Employee Agreement.docx	*Financial (3)	21
	<input type="checkbox"/>	 Employee Agreement.docx	*Financial (3)	21

1 Fogli di calcolo con credenziali e informazioni sulla carta di credito

2 Contratti di lavoro con PII e informazioni sul conto bancario

## Con quale rapidità possiamo effettuare la remediation del rischio di link condivisi?

Un tipico cliente Varonis può eliminare rapidamente l'esposizione con l'automazione. Di seguito sono riportati i risultati di un importante istituto finanziario che ha consentito l'automazione dei privilegi minimi. Quasi il 100% dell'esposizione esterna ai dati a livello di organizzazione è stata eliminata in meno di 30 giorni.



Le politiche di automazione mantengono basso il rischio a fronte della crescita dei dati e della collaborazione continua. Con le policy impostate per l'applicazione automatica, la remediation dei nuovi rischi avviene non appena i rischi si presentano e vengono applicati costantemente i privilegi minimi.

### Policies

- Remediate org-wide exposure
- Remove collaboration links
- Remove memberships of non-org users
- Remove stale collaboration link
- Remove stale direct permissions

# Dati posizionati ed etichettati in modo insoddisfacente

## Dati smarriti: rischio di conformità al GDPR

Varonis ha scoperto record PII di cittadini dell'UE su un tenant M365 con hosting negli Stati Uniti. I file sono stati caricati il 15 luglio da un account di servizio denominato "ExportJob" che sembra essere collegato a un'attività automatizzata di Workato. Consigliamo di migrare questi dati al tenant di Umbrella Corp basato sull'UE e di modificare l'attività automatizzata.

1

Tenant M365 con sede negli Stati Uniti

2

File contenenti PII di cittadini dell'UE

The screenshot shows the 'Resources' section of the Varonis interface. A dropdown menu is open, showing 'File server: 2 values' with a list of options: 'umbrella-nyc' and 'umbrella-dallas'. Below the dropdown is a table with the following data:

Exposure level	Path	Classification results	Total record
<input type="checkbox"/> Internal	/sites/HR/Documents/Salary	GDPR Poland	42
<input type="checkbox"/> Internal	JV costs for Feb-Apr.xls	GDPR Poland	42
<input type="checkbox"/> Internal	Transaction-English-06.xls	GDPR Spain	24
<input type="checkbox"/> Internal	GL Entry.txt	GDPR Spain	24
<input type="checkbox"/> Internal	Employee Agreement.docx	GDPR Ireland	15
<input type="checkbox"/> Internal	Employee Agreement.docx	GDPR Hungary	15

## File con etichetta errata: lacuna nell'applicazione della DLP

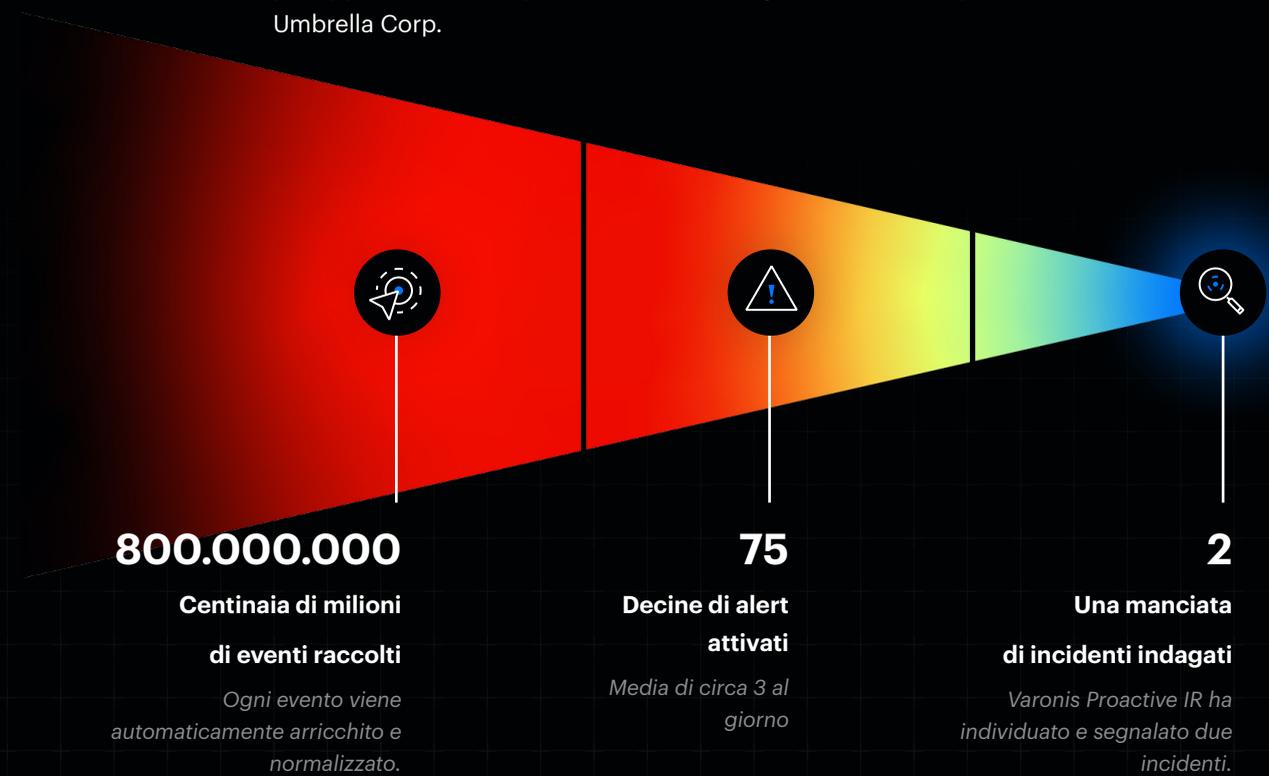
Molti file sono privi di etichette MIP o hanno etichette obsolete applicate in modo errato. Di conseguenza, l'applicazione della DLP a valle potrebbe fallire, con conseguente fuga di dati sensibili o viceversa: agli utenti viene impedito di condividere dati non sensibili etichettati erroneamente.

Abbiamo trovato oltre 27.000 file sensibili senza etichetta.

Path	Classification results	Classification labels	Name
<input type="checkbox"/> C:\Share\Finance	US PII, HIPAA PHI Data	GDPR Regulated Data (0/1)	Finance
<input type="checkbox"/> C:\Share\Finance\Controllers	US PII, HIPAA PHI Data		Controllers
<input type="checkbox"/> C:\Share\Finance\Controllers	US PII, HIPAA PHI Data		Q1 2006
<input type="checkbox"/> C:\Share\Finance\Controllers	US PII, HIPAA PHI Data		Inventory
<input type="checkbox"/> C:\Share\Finance\Controllers	US PII, HIPAA PHI Data		Revenues
<input type="checkbox"/> C:\Share\Finance\Controllers	US PII, HIPAA PHI Data		SEC

# Rilevamento e risposta alle minacce

Il monitoraggio in tempo reale di Varonis e il rilevamento delle minacce basato sul comportamento sono stati abilitati in ciascun sistema interessato. Durante il periodo di valutazione, i nostri modelli di AI sono stati addestrati su oltre 800 milioni di eventi per apprendere il comportamento unico degli utenti e dei dispositivi nell'ambiente di Umbrella Corp.



## UEBA incentrata sui dati

Gli eventi vengono arricchiti con dati, utente e contesto del dispositivo. Gli analisti della sicurezza possono eseguire query come: "Elenca tutti gli eventi di accesso ai dati sensibili da parte di account privilegiati da dispositivi connessi dalla Germania".

Identificazione account				Risoluzione da IP a dispositivo			
Operazione di	Tipo di account	Soggetto	Sensibile?	Indirizzo IP del dispositivo	Nome dispositivo	Indirizzo IP esterno	Geolocalizzazione
Amy Johnson	Dirigente	customer.xlsx	Sì	173.17.33.3	aj-03154	54.239.13.2	Canada

Arrows indicate data flow: from 'Soggetto' to 'Sensibilità dei file' and from 'Geolocalizzazione' to 'Geolocalizzazione'.

# ANALISI DELLE MINACCE

## Rapporto sull'incidente: account di servizio compromesso

### Osservazione:

il team Varonis IR ha scoperto che un account di servizio di backup è stato compromesso e ha iniziato ad accedere ai dati degli utenti.

#### Abnormal service behavior: access to atypical folders containing GDPR data

Exfiltration | 06/11/2023 8:19 PM | Status: Open | Alert ID: 123F...

#### What happened

BackupService File opened shared folder C:\Share\Finance\Controllers\Financereports.

A service account accessed folders containing GDPR data it has not accessed previously. Service accounts can be expected to perform the same actions repeatedly; therefore, a behavioral change is suspicious. Attackers may impersonate a service account and exploit its privileges.

### Mitigazione:

Varonis IR ha gestito e risolto l'incidente in pochi minuti. L'account UC\BackupService è stato immediatamente disabilitato, le sessioni attive sono state eliminate e la password è stata reimpostata. Varonis ha consegnato al team di Umbrella Corp un rapporto investigativo completo di analisi delle cause principali e le raccomandazioni.

### Dettaglio:

l'account compromesso ha avuto accesso a 142 file. 82 di questi file sono stati classificati come sensibili da Varonis.

Event time (event)	Event type...	Account name	Path (affected resource)
<input type="checkbox"/> 06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
<input type="checkbox"/> 06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
<input type="checkbox"/> 06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
<input type="checkbox"/> 06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
<input type="checkbox"/> 06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...

# RISCHIO DI CONFIGURAZIONE

Varonis analizza costantemente le configurazioni di sistema nelle piattaforme SaaS e IaaS di Umbrella Corp per determinare se qualche impostazione è rischiosa o se qualche configurazione si è allontanata dallo stato desiderato.



## Sono state rilevate 21 configurazioni errate

Salesforce presenta il maggior numero di configurazioni errate (8).



## 5 errori di configurazione molto gravi

M365 e Salesforce presentano ciascuno 2 errori di configurazione critici.



## 4 configurazioni impostate per l'applicazione automatica

Varonis può applicare automaticamente le impostazioni sicure.

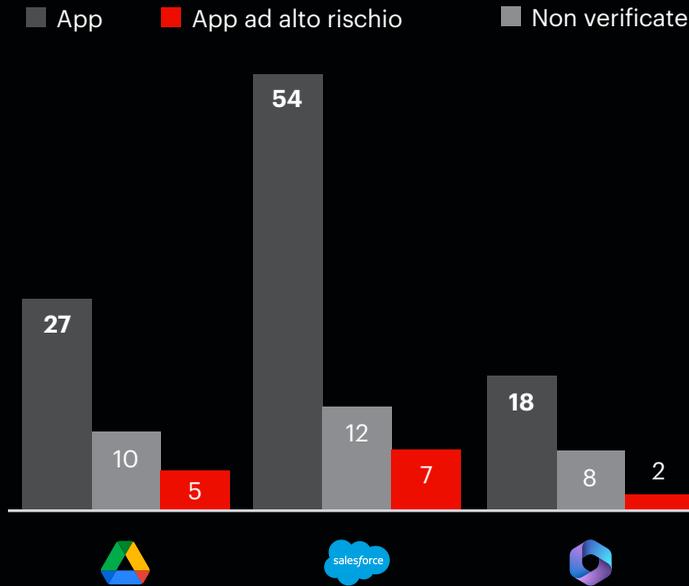
Di seguito è riportato un riepilogo dei **cinque errori di configurazione molto gravi** rilevati durante la valutazione. Tutti i dettagli e le raccomandazioni per ciascuno di essi sono disponibili nell'interfaccia utente di Varonis.

- ✓ Multi-factor authentication is not enforced for privileged users  
Jun 27, 2023 at 1:19 a.m.  Acme, Inc.
- ✓ Admins can log in as any user is enabled  
Jun 27, 2023 at 5:48 a.m.  Acme, Inc.
- ✓ Number of failed login attempts allowed before first lockout period is too high  
Jun 26, 2023 at 4:09 p.m.  Acme, Inc.
- ✓ All group owners can consent for all apps  
Jun 26, 2023 at 2:21 p.m.  Acme, Inc.
- ✓ Critical cookies are not set with sufficient security  
Nov 8, 2023 at 1:18 a.m.  Acme, Inc.

[Fai clic qui](#), per visualizzare ulteriori configurazioni SaaS e IaaS che Varonis può monitorare.

# RISCHIO DELLE APP DI TERZE PARTI

Abbiamo individuato 36 app di terze parti rischiose, inattive o non verificate.



**99**  
App di terze parti installate

**14**  
rischio elevato con ampio accesso ai dati

**22**  
App inattive

Ecco una ripartizione delle prime quattro app di terze parti, per numero di utenti, integrate con le piattaforme SaaS che Varonis sta monitorando:

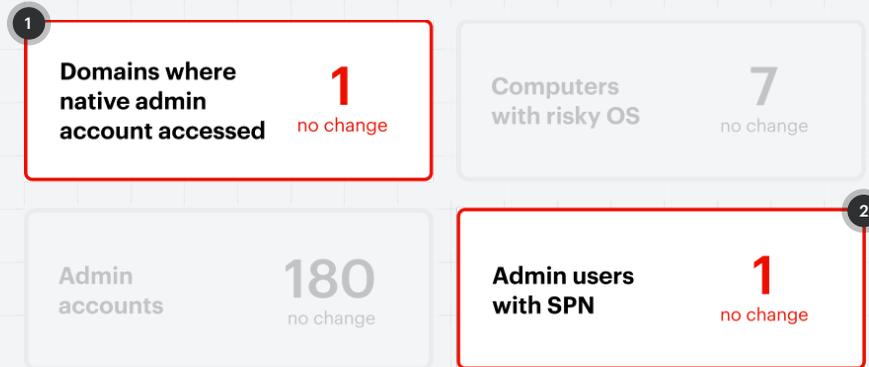
Google	Salesforce	Microsoft 365

Inoltre, abbiamo scoperto 111 utenti non attivi le cui assegnazioni di app possono essere revocate direttamente dall'interfaccia utente Varonis.

# RISCHIO DI IDENTITÀ

## Postura di sicurezza di Active Directory

Varonis scansiona il cloud di Umbrella Corp e i servizi di directory on-prem e rileva configurazioni deboli in grado di aprire percorsi agli aggressori. Questi rischi vengono aggiornati in tempo reale sulle dashboard Varonis e ti aiuteranno ad attribuire priorità all'impegno di rafforzamento di AD.

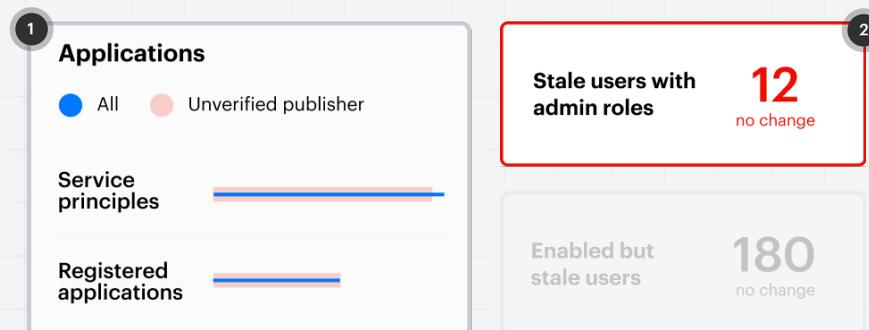


1 È raro che questo account venga utilizzato in circostanze normali. Questo potrebbe indicare un compromesso.

2 Vulnerabile al cracking delle password offline

## Postura di sicurezza Entra ID (Azure AD)

La postura Entra ID viene costantemente monitorata e valutata da Varonis. Configurazioni errate che mettono a rischio i tuoi dati vengono evidenziate nelle dashboard e nei report sui rischi.



1 Rivedi le autorizzazioni dell'app non verificate e l'accesso ai dati.

2 Questi account devono essere disattivati immediatamente.

# Monitoraggio di Active Directory

Varonis monitora gli eventi nei servizi di directory di Umbrella Corp e correla tali azioni agli eventi incentrati sui dati raccolti da piattaforme di collaborazione e data store.

Queste modifiche sono state eseguite al di fuori della finestra di controllo delle modifiche.

RISULTATI DETTAGLIATI

Event type (event)	Event time (event)	Event description	Account Name
<input type="checkbox"/> Access request	06/29/2023 5:15 a.m.	abc1234.com\Demo	Allen Carey
<input type="checkbox"/> Access authentication	06/29/2023 5:15 a.m.	abc1234.com\Demo	
<input type="checkbox"/> Access request	06/29/2023 5:15 a.m.	abc1234.com\Demo	
<input type="checkbox"/> Group member removed	06/29/2023 5:15 a.m.	"DemoUser" was removed	
<input type="checkbox"/> Group member removed	06/29/2023 5:15 a.m.	"DemoUser" was removed	
<input type="checkbox"/> Group member added	06/29/2023 5:15 a.m.	"DemoUser" was added	
<input type="checkbox"/> Group member added	06/29/2023 5:15 a.m.	"DemoUser" was added	
<input type="checkbox"/> User updated	06/29/2023 5:15 a.m.	"DemoUser" was updated	

**Admin role change events** **25**

**Failed login attempts** **8K**

**Login attempts from blacklisted locations** **832**

# Utenti esterni e account personali a rischio

**31 selected**

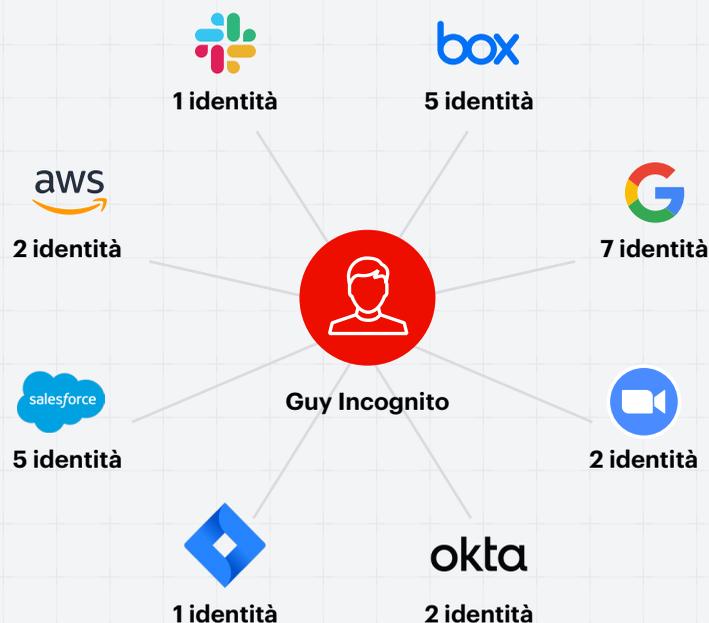
Entity name	Email	Tags
<input type="checkbox"/> Guy Incognito	admin@polyrizelab.com	admin internal no mfa +4
<input checked="" type="checkbox"/> Peter Morris	pmorris@gmail.com	admin external inactive entity +4
<input type="checkbox"/> Allen Carey	acarey@polyrizelab.com	external external entity
<input checked="" type="checkbox"/> Katherine Abner	admin1@gmail.com	external inactive entity external entity +2
<input checked="" type="checkbox"/> Allen Carey	admin@gmail.com	external inactive entity personal account +2

Gli account utente di Gmail sono obsoleti ma hanno accesso a dati sensibili.

## Mappatura delle identità correlate

Varonis individua automaticamente gli account correlati utilizzando un algoritmo proprietario. Guy Incognito è un utente amministratore di Google Workspace che utilizza un account Gmail personale senza MFA. È collegato a diverse identità negli ambienti di Umbrella Corp.

Guy ha diversi alias, un misto di account aziendali e personali.



## Divari di offboarding: account inattivi

Varonis ha individuato oltre 3.000 identità obsolete nei servizi di directory di Umbrella Corp. e nei repository di account locali.

**31 selected**

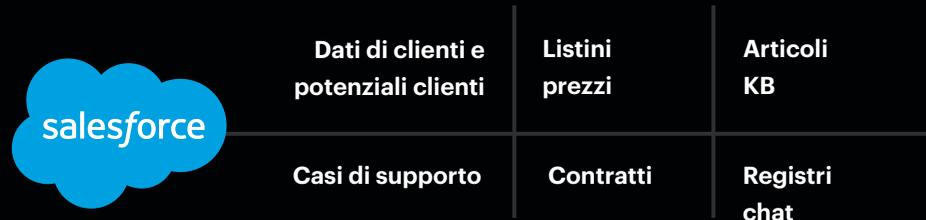
<input checked="" type="checkbox"/>	Entity name	Email	Service	Tags
<input checked="" type="checkbox"/>	Guy Incognito	admin@gmail.com		internal no mfa +4
<input checked="" type="checkbox"/>	Peter Morris	pmorris@gmail.com		external inactive entity +4
<input checked="" type="checkbox"/>	Allen Carey	acarey@gmail.com		external entity
<input checked="" type="checkbox"/>	Katherine Abner	admin1@gmail.com		inactive entity external entity +2
<input checked="" type="checkbox"/>	Allen Carey	admin@gmail.com		inactive entity personal account +2

Ex appaltatori che mantengono l'accesso dai propri account Google personali.

# RISCHIO SALESFORCE

Salesforce ospita i dati più preziosi di un'organizzazione, ma le sue complesse strutture di autorizzazione e la mancanza di visibilità su chi può accedere a tali dati lo pongono a rischio di minacce interne e informatiche.

SALESFORCE



## Ambito di valutazione

<b>Ambienti</b>	+ Produzione + Sandbox	+ Sviluppo
<b>Dati</b>	+ 234.240 dati + 8.241 documenti + 520 campi + 9.214 risorse sensibili	+ 203 dati condivisi esterni/ pubblici + 22 app di terze parti monitorate
<b>Identità</b>	+ 2.012 utenti interni + 425 utenti esterni + 124 appaltatori	+ 212 utenti guest + 55 super admin
<b>Diritti</b>	+ 889 profili + 52 profili privilegiati + 22 profili di comunità + 3 profili di ospiti	+ 55 set di autorizzazioni + 27 gruppi di set di autorizzazioni + 33 ruoli

### Principali 3 domini esterni

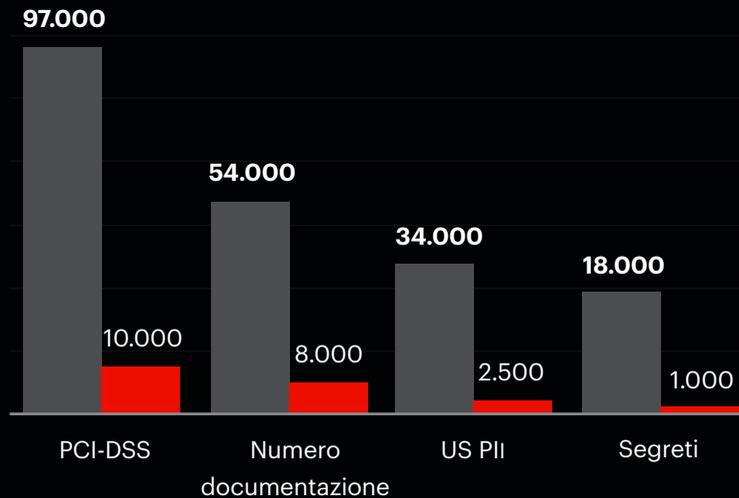


# ESPOSIZIONE DEI DATI DI SALESFORCE

Che tipo di dati risiedono in Salesforce e qual è la loro esposizione?

■ di dati sensibili

■ Dati esposti



**203.000**

Oggetti con almeno un dato sensibile

**1.500**

Dati sensibili esposti esternamente

**20.000**

Dati sensibili esposti a livello di organizzazione

SALESFORCE

## Rischio di data exfiltration di Umbrella Corp

Alcuni diritti, descritti di seguito, dovrebbero essere considerati altamente privilegiati. Se concessi a troppi utenti, questi diritti possono determinare un rischio significativo di esposizione ed exfiltration dei dati.



### 235 diritti con Export Report abilitato

Export Report consente agli utenti di esportare i dati direttamente da Salesforce. Se necessario, deve essere applicato ai set di autorizzazioni.



### 124 diritti con Visualizza tutti i dati o Modifica tutti i dati abilitati

Gli utenti con questa autorizzazione possono visualizzare e modificare tutti i dati all'interno dell'organizzazione.



### 52 diritti con API abilitate

Consente agli utenti di comunicare con tutte le API Salesforce, di escludere i dati o di eseguire altre azioni.

Varonis consente a Umbrella Corp una visione in tempo reale dei diritti critici e la possibilità di ridimensionare rapidamente gli accessi e di applicare i privilegi minimi. Consigliamo anche di impostare alert Varonis che si attivano quando questi diritti privilegiati cambiano.

# DATI SENSIBILI CONDIVISI ESTERNAMENTE

Le istanze Salesforce di Umbrella Corp consentono l'accesso agli utenti guest. Esistono anche diversi account utente che fungono da account di servizio per app di terze parti. Varonis ha rilevato oltre 1.500 record sensibili esposti esternamente, ad esempio il file W2 allegato di seguito.

SALESFORCE

**W2.png** organization-wide sensitive shared externally stale resource

Content document | Account Name: Production | Created: Sept. 18, 2022 09:51 AM (GMT-4:00)

Activities Access Compliance

Showing 7 results

Name	Permissions	Last Active	Tags
Melissa Do...	C R U D S	Mar. 3, 2022 10:12 AM (GMT...	admin internal +2
Josh Hamm...	C R U D S	Sept. 18, 2022 09:51 AM (GMT...	external +2
Jerome Boy...	C R U D S	Sept. 22, 2022 08:30 AM (GMT...	admin external +4

Gli utenti esterni all'azienda possono accedere, aggiornare o eliminare i dati PCI e PII nella tua istanza Salesforce.

Oltre a esporre i dati a utenti guest, appaltatori e altre terze parti autenticate, dalla nostra valutazione sono emersi anche dati esposti a Internet tramite collegamenti pubblici.

**DriverLicenseA11.pdf** public sensitive shared externally

Content document | Account Name: Production | Created: Sept. 18, 2022 09:51 AM (GMT-4:00)

Recent Activities Access Compliance

**Share via link**

Anyone inside or outside of your company with this link can view and download this file.

<https://salesforce.com/1234>

# ERRATE CONFIGURAZIONI DI SALESFORCE

Varonis ha rilevato e corretto quattro configurazioni errate o impostazioni predefinite non sicure a livello di organizzazione che potrebbero fornire un percorso di attacco.

- Organization-wide default configurations expose records to internal and external users  
Jun 15, 2023 at 03:35 a.m. Acme, Inc.
- Critical cookies are not set with sufficient security  
Jan 27, 2023 at 05:48 a.m. Acme, Inc.
- Single-sign on is not enabled for the organization**  
Nov 08, 2022 at 01:18 p.m. Acme, Inc.
- Clickjack protection is not fully enabled  
Dec 17, 2023 at 2:21 p.m. Acme, Inc.

Gli ex appaltatori accedevano all'account sandbox anche se gli account Okta erano stati sottoposti a deprovisioning.

## Alert Salesforce

15 alert sono stati attivati e risolti da Varonis IR, incluso un caso in cui l'insider Melissa Donovan accedeva a un numero anomalo di record rispetto alla sua baseline comportamentale. La nostra indagine ha mostrato che Melissa aveva installato un'estensione del browser che accedeva rapidamente agli URL dei record di Salesforce.



15 alerts



Melissa Donovan excessively accessed Salesforce objects

### Sensitive data exposed

Melissa Donovan

mdonovan@company.com

internal

no mfa

Melissa Donovan ha deviato dalla sua normale attività, accedendo a documenti ai quali di solito non accede.

## Monitoraggio delle modifiche dell'amministratore

Josh Hammond ha apportato diverse modifiche all'amministratore per la produzione al di fuori della finestra di controllo delle modifiche. Di seguito è riportato il registro dettagliato delle modifiche.

### Activities: Privileged

Time	Service
Jan 08, 2023 02:29 a.m.	 Production
Jan 08, 2023 02:29 a.m.	 Production
Jan 08, 2023 02:29 a.m.	 Production
Jan 08, 2023 02:29 a.m.	 Production
Jan 08, 2023 02:29 a.m.	 Production
Jan 08, 2023 02:29 a.m.	 Production

### PermSetEntityPermChanged

 Activity | Account name: Production

Overview Log Actor Overview

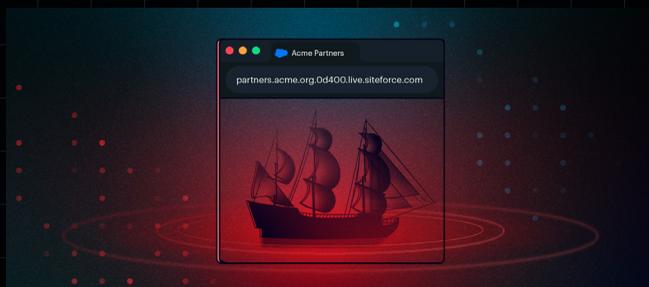
```

{
  "attributes": {
    "type": "SetupAudittrail"
    "url": "/services/dat/v53.0/subjects
SetupAudiTrail/OYm4J0004r00/
  },
  "Id": "OYO900i00489AJFLJSD",
  "Action": "PermSetEntityPermChanged",
  "CreateDate": "2023-01-08T19:29:40:000"
  "CreatedBy": "02349JGFJ0029059000aAG"
  "CreatedBy": {
    "attributes": {

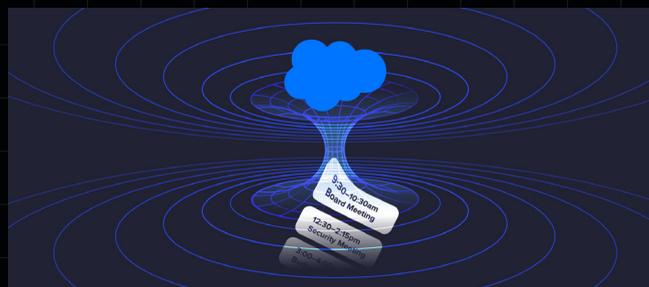
```

# RICERCA SALESFORCE

Il nostro team cerca e divulga vulnerabilità e configurazioni tossiche in Salesforce.



**Siti fantasma: furto di dati dalle comunità di vendita disattivate**



**Wormhole di Einstein: acquisizione dei calendari di Outlook e Google tramite bug dell'utente ospite di Salesforce**

## Informazioni su Varonis Threat Labs

Il nostro team di ricercatori sulla sicurezza e data scientist è tra le menti più elitarie della sicurezza informatica al mondo. Con decenni di esperienza militare, di intelligence e aziendale, il team di Varonis Threat Labs cerca in modo proattivo le vulnerabilità nelle applicazioni utilizzate dai nostri clienti per individuare le crepe prima che lo facciano gli aggressori. Tutti questi apprendimenti sono programmati nella nostra piattaforma per aiutarti a stare al passo con gli attacchi informatici.

Dai un'occhiata alle ultime ricerche: [www.varonis.com/blog/tag/threat-research](https://www.varonis.com/blog/tag/threat-research)



# RIDUCI I TUOI RISCHI SENZA ASSUMERNE NESSUNO.

La configurazione della nostra valutazione del rischio gratuita richiede pochi minuti e offre un valore immediato. In meno di 24 ore avrai una visione chiara e basata sul rischio dei dati più importanti e un percorso chiaro verso la remediation automatizzata.



## Accesso completo alla piattaforma Varonis SaaS

Ottieni accesso completo alla nostra Data Security Platform per tutta la durata della valutazione e ottieni informazioni utili per i tuoi dati più critici



## Analista IR dedicato

Essere collegati alla Varonis SaaS Data Security Platform significa che i nostri esperti tengono d'occhio gli alert e ti chiameremo se notiamo qualcosa di allarmante.



## Report sui risultati principali

Un riepilogo dettagliato dei rischi per la sicurezza dei dati e una presentazione per la dirigenza per esaminare i risultati e le raccomandazioni. Questo report sarà tuo e potrai conservarlo, anche se non diventerai cliente.

[Ottieni la tua valutazione gratuita](#)

Scelto da migliaia di clienti

ING



BlueCross  
BlueShield

Nasdaq

Coca-Cola

TOYOTA

U.S. ARMY

Penguin  
Random  
House

E\*TRADE

FORRESTER®

WAVE  
LEADER 2023

Data Security Platforms

## Varonis nominato leader nelle piattaforme per la sicurezza dei dati.

“Varonis è la **scelta migliore** per le organizzazioni che attribuiscono priorità alla visibilità profonda dei dati, alle capacità di classificazione e alla remediation automatica dell’accesso ai dati”.

Forrester Wave™: piattaforme di sicurezza dei dati, 1° trimestre 2023