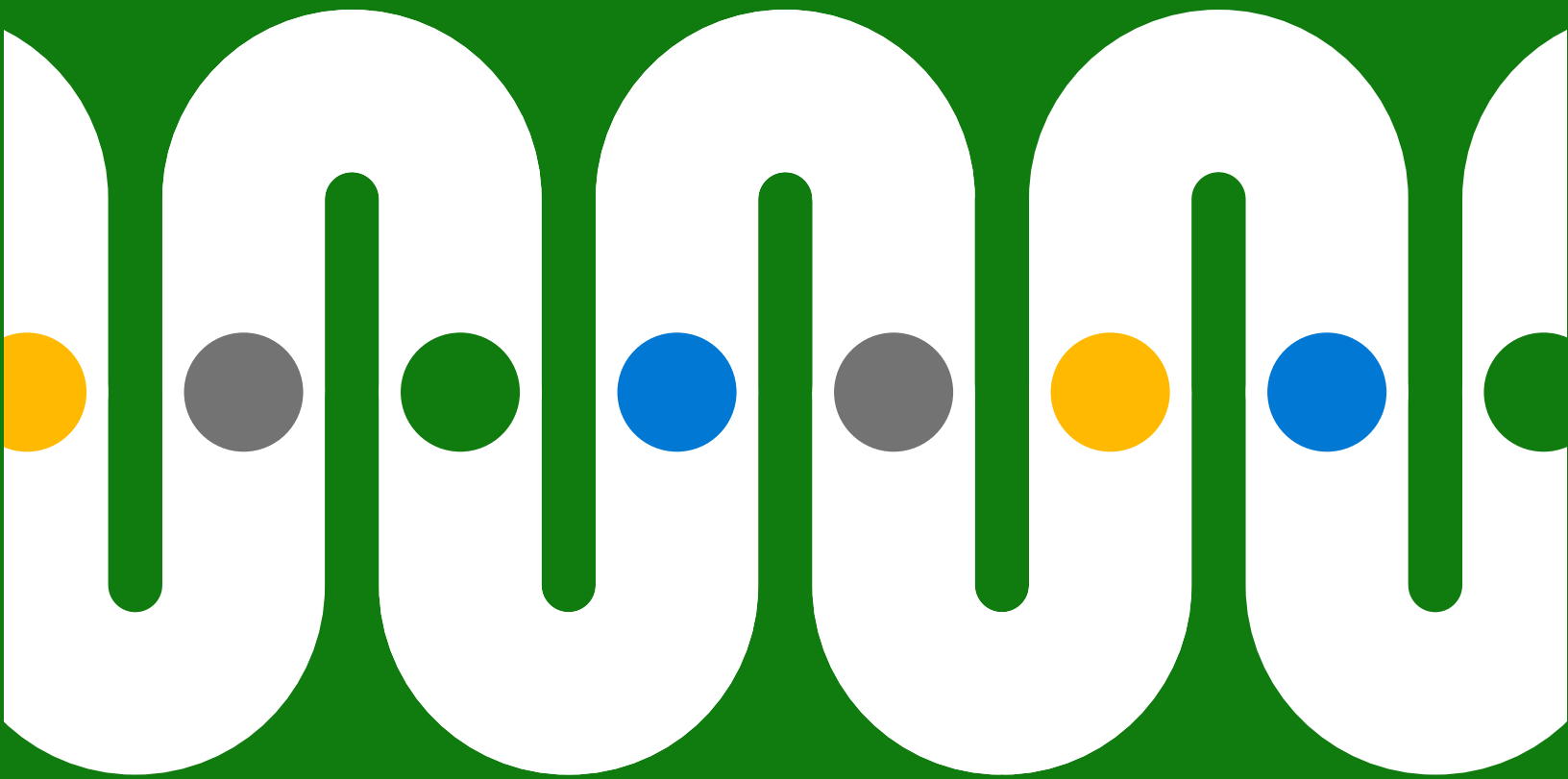
Microsoft Security

Tre passaggi per la protezione dei dati end-to-end



Indice

Un sondaggio condotto tra i decision maker responsabili dell'adeguamento ha rivelato che il 95% era preoccupato per le problematiche legate alla protezione dei dati.[2]

Introduzione

Con il lavoro ibrido, le organizzazioni hanno registrato un incremento enorme della loro impronta digitale, che si estende ben oltre l'ufficio tradizionale.

Ciò ha portato a un aumento della frammentazione e dell'esfiltrazione dei dati, operazioni rese complicate dalla rapida crescita in una moltitudine di applicazioni, dispositivi e posizioni. Molti lavoratori, inoltre, hanno cambiato ruolo alla ricerca di una maggiore soddisfazione o flessibilità. E questo aspetto ha aggravato la situazione, creando nuovi punti deboli nei patrimoni di dati in continua crescita.[1]

Per tutti questi fattori, i CIO e i CISO stanno rivalutando l'approccio alla protezione dei dati. In un sondaggio di monitoraggio condotto tra oltre 500 decision maker statunitensi responsabili dell'adeguamento, quasi tutti (95%) erano preoccupati per le problematiche legate alla protezione dei dati.[2]

[1] "In che modo Microsoft può contribuire a ridurre i rischi interni durante il grande rimpasto", Alym Rayani, Microsoft Security, 28 febbraio 2022.

[2] "Sondaggio condotto a settembre 2021 tra 512 decision maker statunitensi responsabili dell'adeguamento", commissionato a Vital Findings da Microsoft.

I team IT e addetti alla sicurezza sono alla ricerca di modi migliori per gestire l'intero ciclo di vita dei dati, in ambienti multicloud, del cloud ibrido e locali. Questo approccio end-to-end prevede tre passaggi principali:

Passaggio 1. Identificazione dei dati

Determina dove risiedono i dati, di che tipo sono e come vengono utilizzati o condivisi.

Passaggio 2. Classificazione dei dati

Classifica ed etichetta i dati in modo da poter applicare i criteri e la mitigazione dei rischi corretti.

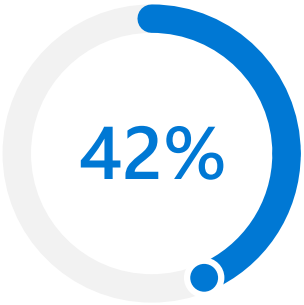
Passaggio 3. Prevenzione della perdita dei dati

Trova un equilibrio tra la riduzione dei rischi e la flessibilità per le persone grazie a funzionalità di rilevamento e controllo intelligenti.

Quali sono gli obiettivi di questo approccio? Colmare le lacune e ridurre al minimo i rischi senza compromettere la produttività.

Passaggio 1

Identificazione dei dati



Alla domanda su quanti dei loro dati siano "oscuri", il 42% delle organizzazioni ha risposto che almeno la metà lo sono.[3]

Questi dati "nascosti" possono assumere varie forme, dagli allegati delle e-mail e dalle registrazioni delle chiamate dei clienti ai registri dei computer e ai video.

Se non riesci a identificare i dati, dove risiedono, di che tipo sono e come vengono utilizzati o condivisi, non puoi applicare i criteri o la protezione corretti.

Le organizzazioni moderne generano continuamente grandi quantità di dati. Non si tratta solo di documenti, e-mail e messaggi, ma di informazioni di tutti i tipi, dai video della sicurezza ai dati di geolocalizzazione. E questa situazione è complicata dalla proliferazione di app, dispositivi e storage, in locale e nel cloud.

Identificare tutti questi dati può essere difficile. Il 42% delle organizzazioni afferma che almeno la metà dei dati è "oscura"[3], ovvero che le informazioni vengono raccolte, ma non sono note o non vengono utilizzate per scopi aziendali. A volte i dati diventano oscuri quando il lavoratore che li ha creati cambia progetto o ruolo. Spesso, semplicemente, non esistono sistemi per identificarli al momento della creazione o della modifica.

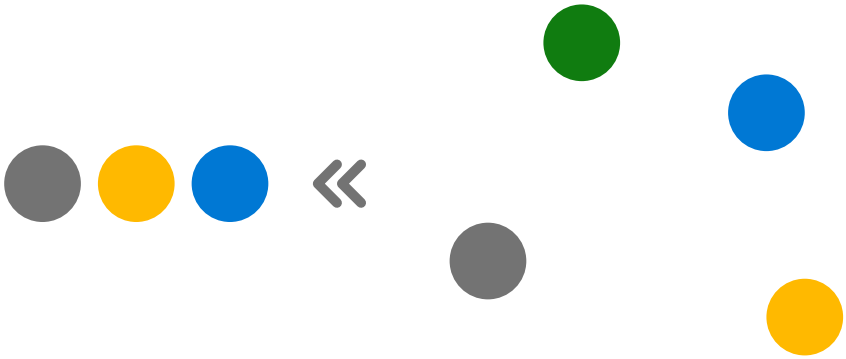
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group, luglio 2022.

Desideri creare un flusso di lavoro di individuazione end-to-end su una piattaforma?

Ulteriori informazioni sull'individuazione dei dati in Microsoft Purview sono disponibili su **Microsoft.com**.

Questa situazione non farà che complicarsi. Si prevede che la quantità di nuovi dati creati, acquisiti, replicati e utilizzati raddoppierà entro il 2026. In particolare i dati aziendali cresceranno due volte più velocemente rispetto ai dati dei consumatori.[4]

L'intelligenza artificiale e l'apprendimento automatico possono aiutare, riconoscendo i dati sensibili, quali indirizzi e-mail, dati sanitari, numeri di carte di credito o proprietà intellettuale, e classificandoli automaticamente. Possono inoltre aumentare la precisione della classificazione ed esaminare i dati in modo retroattivo. Questi processi di identificazione possono riguardare l'intero patrimonio di dati, preservando, raccogliendo, analizzando, esaminando ed esportando il contenuto ovunque si trovino, in qualsiasi cloud.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC, maggio 2022.

Passaggio 2

Classificazione dei dati

Le classificazioni e i criteri devono seguire i dati mentre si spostano.

Ad esempio, se un dipendente copia i numeri di carte di credito da un documento Word in un foglio di calcolo Excel di Microsoft, la classificazione e i criteri devono applicarsi automaticamente a entrambi i documenti.

Una classificazione appropriata dei dati consente di determinare i criteri e la mitigazione dei rischi corretti per garantire che tipi di dati diversi non vengano usati in modo accidentale o intenzionale o non vengano utilizzati senza autorizzazione. La crittografia e la filigrana possono proteggere ulteriormente i dati, inattivi, in transito o in uso.

Ma la classificazione e i criteri devono seguire i dati mentre si spostano all'interno dell'organizzazione. I criteri di etichettatura e protezione non possono essere limitati a documenti separati, ma devono riguardare l'intero patrimonio digitale: dai repository locali a quelli basati su cloud, dalle app SaaS (Software-as-a-Service) alle app native per il sistema operativo.

Gli approcci tradizionali alla classificazione implicano un lavoro manuale considerevole, che comporta il rischio di commettere errori o di trascurare inavvertitamente dati importanti. I classificatori predefiniti e sottoponibili a formazione possono contribuire ad automatizzare questo processo e una soluzione integrata consente agli amministratori di gestire i criteri a livello centrale, in tutti i sistemi.

Desideri gestire e proteggere meglio i dati sensibili nel tuo ambiente?

Ulteriori informazioni sulla classificazione e sulla protezione dei dati in Microsoft Purview sono disponibili su **Microsoft.com**.

Passaggio 3

Prevenzione della perdita dei dati

I criteri DLP possono impedire azioni di non adeguamento.

Ad esempio, se un dipendente tenta di scaricare un foglio di calcolo con i numeri di carte di credito su un'unità flash o di caricarlo in un archivio cloud, i criteri DLP potrebbero identificare l'attività come non adeguata e impedirla.

Desideri rilevare e controllare le informazioni sensibili in modo intelligente?

Ulteriori informazioni sulla prevenzione della perdita dei dati in Microsoft Purview sono disponibili su **Microsoft.com**.

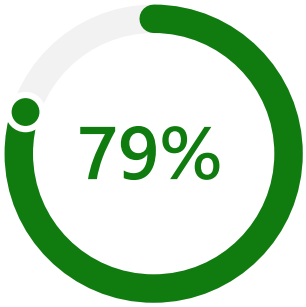
Dopo avere identificato e classificato i dati, le soluzioni di prevenzione della perdita dei dati (DLP) possono applicare i criteri di protezione end-to-end in grado di mitigare le minacce, quali i dati oscuri e l'esfiltrazione dei dati, in modo che i dipendenti attuali ed ex, intenzionalmente o inavvertitamente, non condividano, espongano o trasferiscano i dati sensibili senza autorizzazione.

Le soluzioni DLP intelligenti utilizzano il contesto per trovare un equilibrio tra la flessibilità e il blocco delle azioni ad alto rischio. Ad esempio, gli individui potrebbero essere in grado di continuare con un'azione dopo che sono stati informati dei rischi potenziali e dei criteri applicabili. In questo modo è possibile proteggere i dati sensibili e formare gli utenti per comprendere meglio i rischi.

Le soluzioni DLP consentono di proteggere la proprietà intellettuale e altri dati aziendali critici, migliorando al tempo stesso l'adeguamento a normative come il Regolamento generale sulla protezione dei dati (GDPR), la specifica Health Information Portability and Accountability Act (HIPAA) e il California Consumer Privacy Act (CCPA).

Un approccio completo alla DLP applica i criteri in tutta l'organizzazione in modo coerente, proteggendo gli "anelli più deboli" nel ciclo di vita dei dati.

Protezione dei dati integrata, non annessa



Un sondaggio condotto tra i decision maker dell'adeguamento ha mostrato che il 79% aveva acquistato più prodotti per l'adeguamento e la protezione dei dati.

La maggioranza ne aveva acquistati tre o più.[5]

Molte organizzazioni hanno provato un approccio "annesso" alla protezione dei dati, usando più soluzioni per gestire le parti separate del ciclo di vita dei dati. Questo approccio, però, costringe i team addetti alla sicurezza, alla governance dei dati, all'adeguamento e agli affari legali a trovare una soluzione eterogenea che spesso è inefficace e mette a dura prova le risorse.

Un approccio "integrato" può colmare le lacune, combinando l'identificazione dei dati, la classificazione dei dati e la prevenzione della protezione dei dati. Una soluzione integrata consente di gestire e applicare più facilmente i criteri a livello centrale. Riduce inoltre i tempi di formazione per gli utenti che ricevono notifiche sui criteri in modo familiare, all'interno delle applicazioni.

[5] "Sondaggio condotto a febbraio 2022 tra 200 decision maker statunitensi responsabili dell'adeguamento (n=100 599-999 dipendenti, n=100 1.000+ dipendenti)", commissionato a MDC Research da Microsoft.

Una soluzione integrata, predefinita: Microsoft Purview

Microsoft Purview consente di affrontare le problematiche del luogo di lavoro decentralizzato e ricco di dati di oggi con un set completo di soluzioni che ti aiutano a governare, proteggere e gestire l'intero patrimonio di dati.

Vai oltre la governance.

Ulteriori informazioni sulla protezione dei dati con Microsoft Purview >

Ti interessa un'area specifica della protezione dei dati? Ottieni informazioni più dettagliate su come Microsoft Purview può aiutarti con:

Individuazione dei dati >

Classificazione e protezione dei dati >

Prevenzione della perdita dei dati >

Microsoft Security

©2022 Microsoft Corporation. Tutti i diritti sono riservati. Questo documento viene fornito "così com'è". Le informazioni e le opinioni contenute in questo documento, inclusi gli URL e altri riferimenti a siti Web Internet, possono variare senza preavviso. Qualsiasi rischio correlato all'uso del documento è a carico dell'utente. Questo documento non garantisce alcun diritto legale sulla proprietà intellettuale di alcun prodotto Microsoft. Il presente documento può essere copiato e utilizzato esclusivamente per uso interno e a scopo di riferimento.