



Purview Information Protection

Mantieni i tuoi dati sensibili protetti
dentro e fuori dall'azienda

Purview Information Protection: tutti i dettagli

Cos'è Purview Information Protection, i casi d'utilizzo
e i benefici attesi

Purview Information Protection: che cos'è?

Microsoft Purview è una soluzione che aiuta le aziende a proteggere i dati sensibili, a garantire la conformità normativa e ad ottimizzare la gestione delle informazioni, occupandosi nello specifico di supportare la **Data Security**, la **Data Governance** e la **Compliance**.

Information Protection fa parte di questa soluzione e include:

- Classificazione ed etichettatura dei dati
- Crittografia
- Prevenzione della perdita di dati (DLP)
- Protezione dei dispositivi
- Gestione centralizzata delle regole
- Individuazione e analisi dei dati
- Gestione del ciclo di vita dei dati

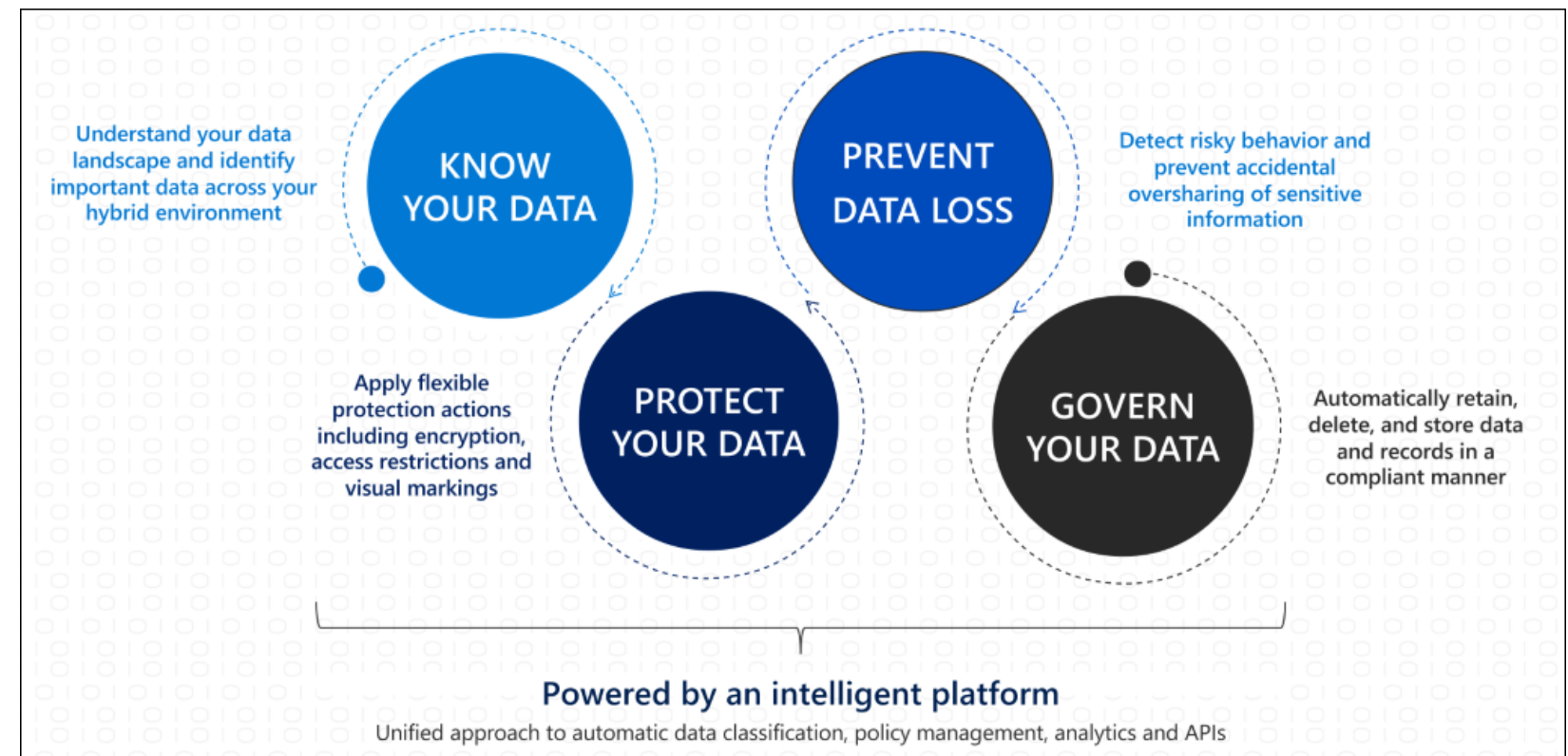


Image Source: Microsoft Purview Information Protection

Purview Information Protection: come funziona?

Purview Information Protection si integra con Microsoft 365, le soluzioni di Microsoft Azure Security e altri servizi cloud e per proteggere le informazioni, classificarle e gestirle utilizza diverse tecnologie che hanno scopi ben specifici.

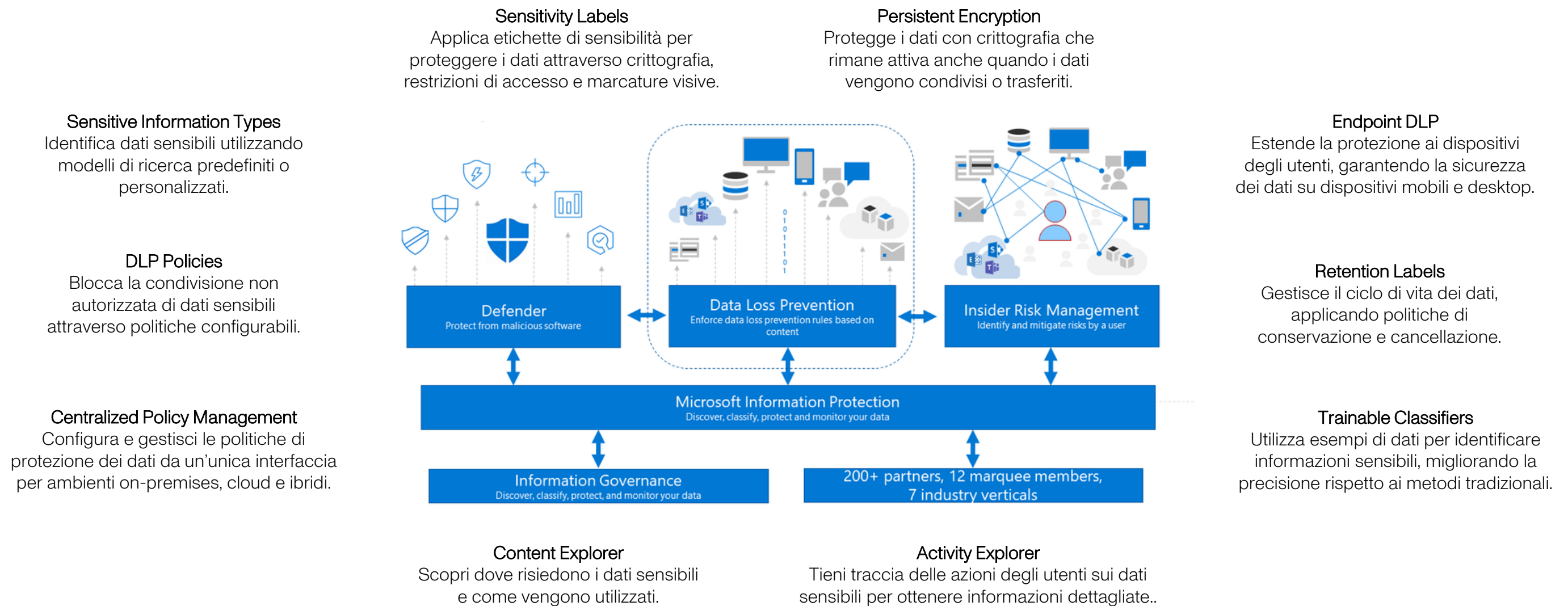


Image source: Microsoft Unified DLP

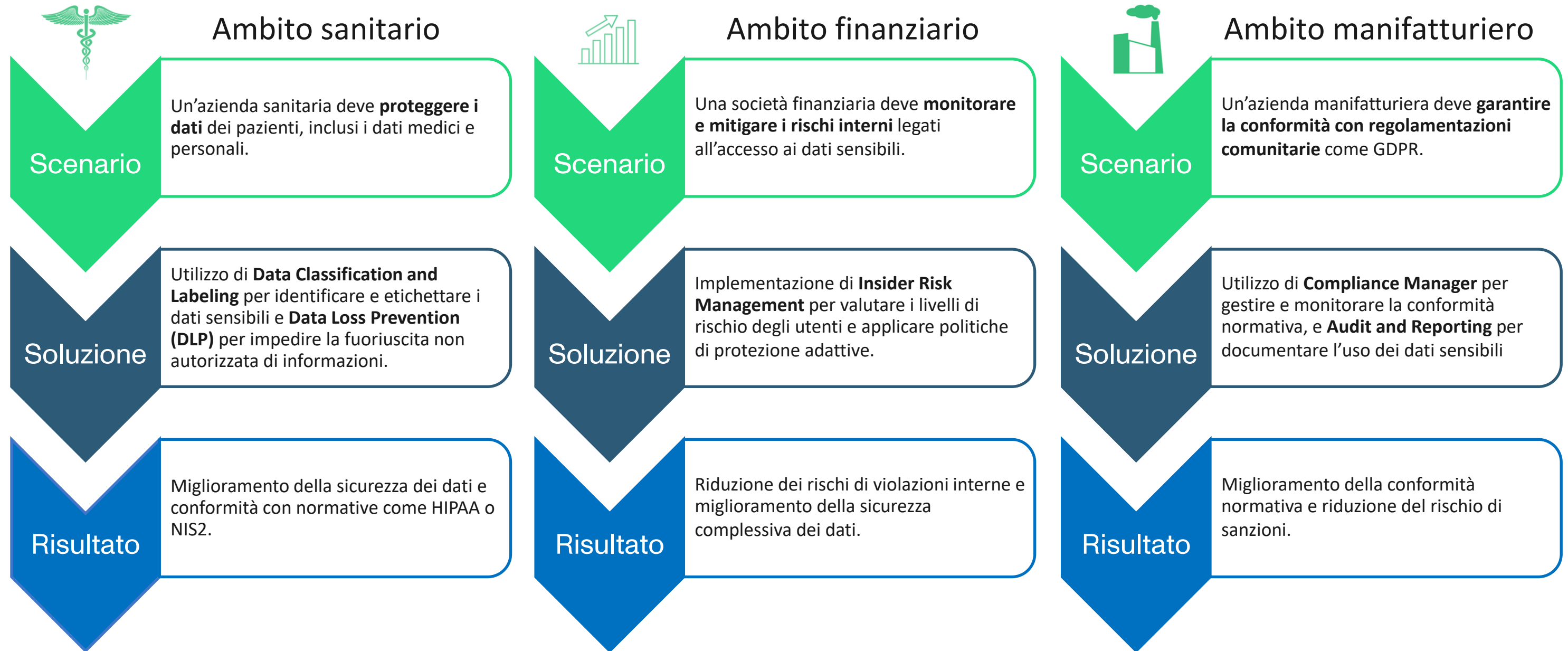
Purview Information Protection: cosa protegge?

La protezione è fatta su diverse fonti



Purview Information Protection: i casi di utilizzo

Alcuni esempi reali



Purview Information Protection: i benefici

Microsoft Purview Information Protection protegge i dati sensibili da vari rischi, tra cui:

- **Perdita di dati:** utilizza politiche di Data Loss Prevention (DLP) per impedire la condivisione non autorizzata di informazioni sensibili.
- **Accessi non autorizzati:** applica crittografia e restrizioni di accesso per garantire che solo gli utenti autorizzati possano accedere ai dati protetti.
- **Minacce interne:** monitora e gestisce i rischi interni valutando le azioni degli utenti sui dati sensibili.

Inoltre:

- Facilita e promuove la collaborazione **sia all'interno che all'esterno dell'organizzazione** fornendo funzionalità di condivisione sicura e **proteggendo automaticamente** i dati sensibili in uscita.
- Permette di **standardizzare le impostazioni di sicurezza** e introdurre la classificazione per Teams, Gruppi e Siti.

Il progetto

L'approccio proposto e i passi da seguire

Approccio e metodologia

Nel contesto di **progetti complessi** che richiedono **cambiamenti infrastrutturali** e il **coinvolgimento degli utenti**, il nostro approccio metodologico si basa sull'implementazione di un progetto pilota.

Questo ci permette di **analizzare dettagliatamente** le configurazioni esistenti e di pianificare un deployment in produzione **efficace e senza intoppi**.

Vantaggi del progetto PILOTA

- **Ottimizzazione della Pianificazione:** Il progetto pilota riduce significativamente le attività di pianificazione necessarie per il deployment in produzione, poiché l'assessment fornirà tutte le informazioni essenziali per una completa adozione della tecnologia.
- **Gestione della Complessità:** Considerata la complessità intrinseca del progetto, è impraticabile stimare con precisione tempi e costi. Il pilota permette di distribuire una soluzione standardizzata con un massimo di un paio di personalizzazioni.
- **Pianificazione del Deployment:** La fase finale di deployment in produzione si concentrerà sulla pianificazione e implementazione delle personalizzazioni e sulla distribuzione definitiva.

Implementazione del progetto PILOTA

Analisi dettagliata

Il progetto pilota consente un'analisi meticolosa delle configurazioni e delle policies esistenti, garantendo una comprensione approfondita delle infrastrutture attuali.

Test con superuser

Durante la fase pilota, la tecnologia verrà testata con un gruppo selezionato di superuser, permettendo l'identificazione e la risoluzione di problematiche non emerse durante l'assessment iniziale.

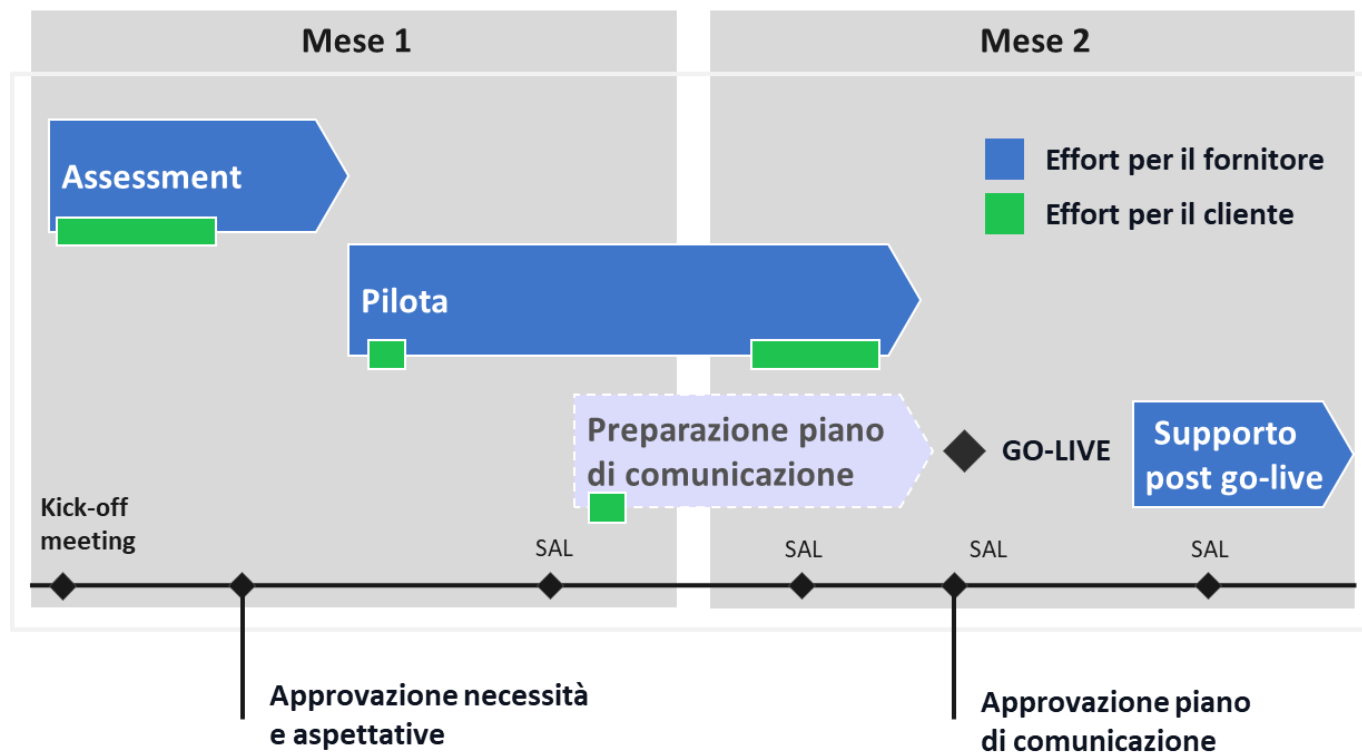
Limitazione delle personalizzazioni

Per assicurare il rispetto dei tempi e dei costi previsti, il numero di configurazioni personalizzate sarà limitato.

Obiettivo finale

Assicurare che tutte le esigenze aziendali siano pienamente soddisfatte e che l'implementazione finale avvenga in modo fluido e senza intoppi.

Timeline e fasi del progetto PILOTA



Fase	Attività	Dev4Side	Cliente
Assessment	Definizione degli Obiettivi	Collaboreremo con il cliente per identificare gli obiettivi specifici del progetto pilota, concentrandoci sulla protezione dei dati sensibili e sulla conformità normativa.	Fornirà input sugli obiettivi aziendali e sui dati critici da proteggere.
	Raccolta dei Requisiti	Condurremo workshop con le parti interessate per raccogliere i requisiti di sicurezza e conformità.	Parteciperà ai workshop e fornirà documentazione sui requisiti aziendali.
	Valutazione dell'Infrastruttura Esistente	Effettueremo un'analisi dettagliata dell'infrastruttura IT attuale per identificare eventuali lacune.	Fornirà accesso alle risorse IT e alle informazioni necessarie per l'analisi.
	Selezione delle Tecnologie	Consiglieremo le funzionalità di Microsoft Purview Information Protection e DLP più adatte alle esigenze del cliente.	Valuterà le nostre raccomandazioni e approverà le tecnologie selezionate.
Pilota	Pianificazione del Progetto Pilota	Definiremo il perimetro del progetto pilota e creeremo un piano di implementazione dettagliato.	Collaborerà nella definizione del perimetro e approverà il piano di implementazione.
	Implementazione del Progetto Pilota	Configureremo le soluzioni di Purview Information Protection e DLP e condurremo i test iniziali.	Fornirà supporto operativo e risorse per l'implementazione.
	Monitoraggio e Valutazione	Monitoreremo l'efficacia delle soluzioni implementate e raccoglieremo feedback.	Fornirà feedback continuo e segnalerà eventuali problemi o miglioramenti necessari.
	Ottimizzazione e Scalabilità	Apporteremo le modifiche necessarie basate sui risultati del monitoraggio e pianificheremo l'espansione del progetto.	Collaborerà nell'implementazione delle modifiche e nella pianificazione della scalabilità.

Timeline e fasi del progetto: Next steps

Dopo il successo del progetto pilota, procederemo con le attività di deployment in produzione. È importante notare che queste attività post-pilota non sono comprese nell'offerta attuale, tuttavia, grazie all'analisi dettagliata e ai risultati ottenuti durante il pilota, saremo in grado di proporre un valore estremamente accurato e realistico per il deployment in produzione.

Le seguenti attività saranno proposte e svolte, previa accettazione della nuova offerta:

Finalizzazione del piano di deployment

- Consolidare i feedback raccolti durante il pilota per perfezionare il piano di deployment in produzione.

Deployment in produzione

- Eseguire il deployment delle soluzioni su scala aziendale, monitorando attentamente le performance e risolvendo eventuali problemi in tempo reale.

Supporto post-deployment

- Fornire supporto continuo per garantire che le soluzioni implementate funzionino correttamente e che gli utenti abbiano l'assistenza necessaria per qualsiasi problema o domanda.

Change Management

Per facilitare l'adozione dello strumento si propongono:

- Un **piano di comunicazione** personalizzato con teaser e un video di lancio
- Un **corso dal vivo** per il passaggio di conoscenza per la gestione della soluzione
- Un corso in modalità **micro-learning** per la formazione degli utenti finali, con formati più facilmente assimilabili
 - Testi brevi
 - Audio e video pillole
 - Quiz interattivi
 - Flashcards

MICRO-LEARNING

Impara a conoscere Purview Information Protection in 10 minuti

Che cos'è Purview Information Protection?

Microsoft Purview

Information Protection

Sensitivity labels

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels.](#)

+ Create a label Publish labels Export Refresh

Name	Priority	Scope	Created by
Personal	0 - lowest	File, Email	
Public	1	File, Email	
General	2	File, Email	
Confidential	5	File, Email	
Highly Confidential	9	File, Email	
All Employees	10	File, Email	
Specified People	11	File, Email	
Project - Falcon	12	File, Email, Meetings	Megan Brown
Project Orion	13	File, Email, Meetings, Site, UnifiedC...	MCO Administrator
14 - highest	14	File, Email, Meetings	Megan Brown

2. Nel menù a sinistra, cliccare su "Sensitivity labels".

00:00 / 00:24



Il tuo miglior partner Microsoft

Ti aiutiamo a sfruttare al massimo le
potenzialità del cloud e dell'AI nel tuo lavoro



sales@dev4side.com