

Protezione delle informazioni per Contoso Corporation

Articolo • 04/04/2023 • 5 minuti per la lettura

Contoso è seriamente preoccupato per la sicurezza delle informazioni. La perdita o la distruzione della proprietà intellettuale che descrive i loro progetti di prodotti e le tecniche di produzione proprietarie li metterebbero in uno svantaggio competitivo.

Prima di spostare gli asset digitali sensibili nel cloud, Contoso si è assicurato che i requisiti di classificazione e protezione delle informazioni locali fossero supportati dai servizi basati sul cloud di Microsoft 365 per le aziende.

Classificazione della sicurezza dei dati di Contoso

Contoso ha eseguito un'analisi dei dati e ha determinato i livelli di classificazione seguenti.

Livello 1: base	Livello 2: dati sensibili	Livello 3: dati altamente regolamentati
<p>I dati vengono crittografati e sono disponibili solo per gli utenti autenticati.</p> <p>Fornito per tutti i dati archiviati in locale e nell'archiviazione e nei carichi di lavoro basati sul cloud. I dati vengono crittografati mentre si trovano nel servizio e passano dal servizio ai dispositivi client.</p> <p>Esempi di dati di livello 1 sono le normali comunicazioni aziendali (posta elettronica) e i file dei dipendenti di amministrazione, vendita e supporto.</p>	<p>Livello 1 più autenticazione avanzata e protezione da perdita dei dati.</p> <p>L'autenticazione avanzata include Azure AD Multi-Factor Authentication (MFA) con convalida SMS.</p> <p>Prevenzione della perdita dei dati Microsoft Purview garantisce che le informazioni sensibili o critiche non vengano spostate al di fuori del cloud Microsoft.</p> <p>Esempi di dati di livello 2 sono le informazioni legali e finanziarie e i dati di ricerca e sviluppo per i nuovi prodotti.</p>	<p>Livello 2 più i livelli più elevati di crittografia, autenticazione e controllo.</p> <p>I livelli di crittografia più elevati per i dati statici e nel cloud, conformi alle norme internazionali, combinati con MFA con smart card e il controllo granulare, nonché avvisi.</p> <p>Esempi di dati di livello 3 sono le informazioni personali dei clienti e dei partner, le specifiche di progettazione dei prodotti e le tecniche di produzione proprietarie.</p>

Livello 1: base	Livello 2: dati sensibili	Livello 3: dati altamente regolamentati

Criteri informativi di Contoso

Nella tabella seguente sono elencati i criteri informativi di Contoso.

Valore	Access	Conservazione dei dati	Protezione delle informazioni
Valore aziendale basso (Livello 1: Base)	Consentire l'accesso a tutti.	6 mesi	Usare la crittografia.
Valore aziendale medio (Livello 2: Dati sensibili)	Consentire l'accesso a dipendenti, subappaltatori e partner di Contoso. Usare MFA, Transport Layer Security (TLS) e Mobile Application Management (MAM).	2 anni	Usare i valori hash per l'integrità dei dati.
Valore aziendale elevato (Livello 3: Dati altamente regolamentati)	Consentire l'accesso ai dirigenti e responsabili di progettazione e produzione. Rights Management System (RMS) solo con dispositivi di rete gestiti.	7 anni	Usare le firme digitali per il non ripudio.

Percorso contoso per la protezione delle informazioni con Microsoft 365 per le aziende

Contoso ha seguito questi passaggi per preparare Microsoft 365 per le aziende per i requisiti di protezione delle informazioni:

1. Identificare le informazioni da proteggere

Contoso ha esaminato in modo approfondito gli asset digitali esistenti che si trovano nei siti e nelle condivisioni file di SharePoint locali e ha classificato ogni asset.

2. Determinare i criteri di accesso, conservazione e protezione dei dati per i livelli di dati

In base ai livelli di dati, Contoso ha determinato requisiti dettagliati per i criteri, che sono stati utilizzati per proteggere le risorse digitali esistenti mentre venivano spostate nel cloud.

3. Creare etichette di riservatezza e le relative impostazioni per i diversi livelli di informazioni

Contoso ha creato etichette di riservatezza per i livelli di dati con l'etichetta per dati altamente regolamentati, tra cui crittografia, autorizzazioni e filigrane.

4. Spostare dati da siti e condivisioni file di SharePoint locali ai nuovi siti di SharePoint

I file di cui è stata eseguita la migrazione ai nuovi siti di SharePoint hanno ereditato le etichette di conservazione predefinite assegnate al sito.

5. Formare i dipendenti su come usare le etichette di riservatezza per i nuovi documenti, come interagire con Contoso IT durante la creazione di nuovi siti di SharePoint e archiviare sempre gli asset digitali nei siti di SharePoint







La modifica delle cattive abitudini di archiviazione delle informazioni dei lavoratori è spesso considerata la parte più difficile della transizione di protezione delle informazioni per il cloud. L'IT e la gestione di Contoso dovevano fare in modo che i dipendenti etichettassero e archiviassero sempre le proprie risorse digitali nel cloud, si astenessero dall'usare condivisioni file locali e non usassero servizi di archiviazione cloud o unità USB di terze parti.

Criteri di accesso condizionale per la protezione delle informazioni

Nell'ambito dell'implementazione di Exchange Online e SharePoint, Contoso ha configurato il set seguente di criteri di accesso condizionale e li ha applicati ai gruppi appropriati:

- [Criteri di accesso alle applicazioni gestite e non gestite sui dispositivi](#)
- [Criteri di accesso di Exchange Online](#)
- [Criteri di accesso di SharePoint](#)

Ecco il set risultante di criteri contoso per la protezione delle informazioni.

Livello di protezione	Tipo di dispositivo	Criteri di accesso condizionale di Azure AD				Criteri di conformità dei dispositivi Intune	Criteri di protezione delle app di Intune	Criteri di accesso ai dispositivi SharePoint
Protezione di base		Richiedi computer conformi	Blocca i client che non supportano l'autenticazione moderna	Blocca i client ActiveSync	Utilizza restrizioni imposte dall'app di SharePoint Online (in questo modo Azure utilizza le impostazioni specificate in SharePoint Online e tale regola si applica a tutti gli utenti ma interessa solo l'accesso ai siti inclusi nei criteri di accesso di SharePoint Online).	Definisci criteri di conformità (un criterio per ogni piattaforma)		
		Sono richieste app approvate (impone la protezione delle app per dispositivi mobili per telefoni e tablet)	(i client che non utilizzano l'autenticazione moderna possono ignorare le regole di accesso condizionale, quindi è importante bloccarli)				Definisci i criteri di protezione delle app (iOS e Android)	
Dati sensibili		Richiedi computer e dispositivi mobili conformi						Criteri di controllo di accesso: consentono l'accesso solo tramite browser a siti specifici di SharePoint da dispositivi non gestiti
		(impone la gestione di Intune per computer e telefoni/tablet)						
Protezione per ambienti altamente regolamentati								Criteri di controllo di accesso: bloccano l'accesso a siti specifici di SharePoint da dispositivi non gestiti
								

❗ Nota

Contoso ha inoltre configurato criteri di accesso condizionale aggiuntivi per l'identità e l'accesso. Vedere **Identità per Contoso Corporation**.

Questi criteri assicurano che:

- Le app consentite e le azioni che possono eseguire con i dati dell'organizzazione sono definite dai criteri di protezione delle app.
- I computer e i dispositivi mobili siano compatibili.
- Exchange Online usa Office 365 crittografia dei messaggi (OME) per Exchange Online.
- SharePoint usa restrizioni applicate dall'app.
- SharePoint usi i criteri di controllo di accesso per l'accesso solo dal browser e per bloccare l'accesso ai dispositivi non gestiti.

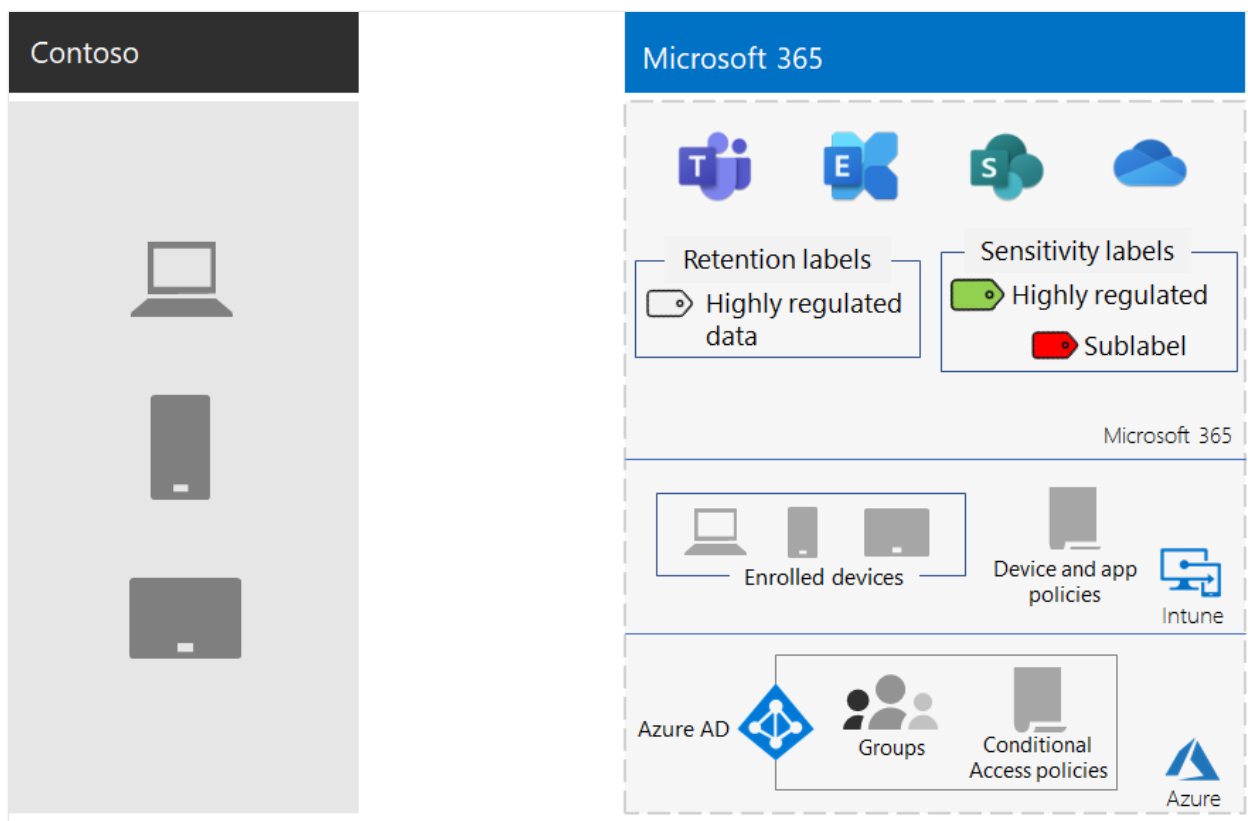
Mapping delle funzionalità di Microsoft 365 per le aziende ai livelli di dati contoso

Nella tabella seguente i livelli di dati contoso vengono mappati alle funzionalità di protezione delle informazioni in Microsoft 365 per le aziende.

Livello	Servizi cloud Microsoft 365	Windows 10 e App Microsoft 365 per grandi imprese	Sicurezza e conformità

Livello	Servizi cloud Microsoft 365	Windows 10 e App Microsoft 365 per grandi imprese	Sicurezza e conformità
Livello 1: base	Criteri di accesso condizionale di SharePoint ed Exchange Online Autorizzazioni sui siti di SharePoint	Etichette di riservatezza BitLocker Windows Information Protection	Criteri di accesso condizionale dei dispositivi e criteri di Mobile Application Management
Livello 2: dati sensibili	Livello 1 plus: Etichette di riservatezza Etichette di conservazione di Microsoft 365 nei siti di SharePoint Prevenzione della perdita dei dati per SharePoint ed Exchange Online Siti di SharePoint isolati	Livello 1 plus: Etichette di riservatezza su risorse digitali	Livello 1
Livello 3: dati altamente regolamentati	Livello 2 plus: Bring your own key (BYOK) encryption and protection for trade secret information Azure Key Vault per applicazioni line-of-business che interagiscono con i servizi di Microsoft 365	Livello 2	Livello 1

Ecco la configurazione di Contoso information protection risultante.



Passaggio successivo

Informazioni su come Contoso usa le [funzionalità di sicurezza di Microsoft 365 per le aziende per](#) la gestione delle identità e degli accessi, la protezione dalle minacce, la protezione delle informazioni e la gestione della sicurezza.

Vedere anche

[Microsoft Defender per Office 365](#)

[Panoramica di Microsoft 365 per le aziende](#)

[Guide dei laboratori di testing](#)