

Sicurezza intelligente per l'ambiente di lavoro moderno

Microsoft 365 Enterprise E5 offre soluzioni di sicurezza intelligenti e complete in ambito di gestione delle identità e degli accessi, protezione delle informazioni, protezione dalle minacce e gestione della sicurezza

Il cloud intelligente offre l'opportunità di migliorare l'approccio alla sicurezza

Una delle principali sfide nella trasformazione digitale consiste nel garantire la sicurezza nell'intero panorama digitale di un'azienda senza ridurre la produttività degli utenti. Il raggruppamento di singole soluzioni può determinare un livello complesso di sicurezza che sovraccarica le operazioni e spinge gli utenti ad aggirare le misure di sicurezza. Il cloud computing consente alle aziende di condividere segnali a livello globale, modificando il loro approccio alla sicurezza.

Un approccio rivolto alla sicurezza delle piattaforme può ridurre le complessità

In questo nuovo mondo in cui i dati e gli utenti girano liberamente, è sempre più importante avere una suite integrata di strumenti di sicurezza. Microsoft 365 è una soluzione completa e intelligente che aiuta a proteggere i dati aziendali e a difendersi dagli utenti malintenzionati, sfruttando al contempo le opportunità rivoluzionarie presentate dal cloud computing. Le sue soluzioni di sicurezza si integrano facilmente e condividono le informazioni della moltitudine di segnali di sicurezza su Intelligent Security Graph nell'intero ecosistema Microsoft globale. Con Microsoft 365 è possibile ridurre il numero di fornitori di servizi di sicurezza da gestire e tutelare l'azienda senza compromettere la produttività.

Microsoft 365 garantisce la sicurezza di utenti, dati, dispositivi e applicazioni

I dati rappresentano il bene più prezioso per un'azienda. Ciononostante, la maggior parte delle società non è in grado di riconoscere i dati sensibili e controllarne l'accesso. La protezione dei dati richiede un approccio a più livelli che ha inizio con un'esperienza positiva di autenticazione degli utenti con criteri per controllare l'accesso alle informazioni riservate, indipendentemente dalla posizione o dal dispositivo. Microsoft 365 include la protezione delle identità, che getta le basi per un accesso sicuro ai dati, ai dispositivi e alle applicazioni. Vari strumenti avanzati per la protezione dalle minacce comunicano tra loro per correlare le informazioni sulle minacce nell'intera impronta digitale e automatizzare la protezione, agevolando il workload nel team delle operazioni di sicurezza. Le informazioni indicano alcuni modi per ottimizzare la configurazione degli strumenti e fornire una misura quantificabile del livello generale di sicurezza.



Gestione delle identità e degli accessi

- Azure Active Directory
- Microsoft Cloud App Security
- Windows Hello
- Windows Credential Guard



Protezione dalle minacce

- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Microsoft Cloud App Security



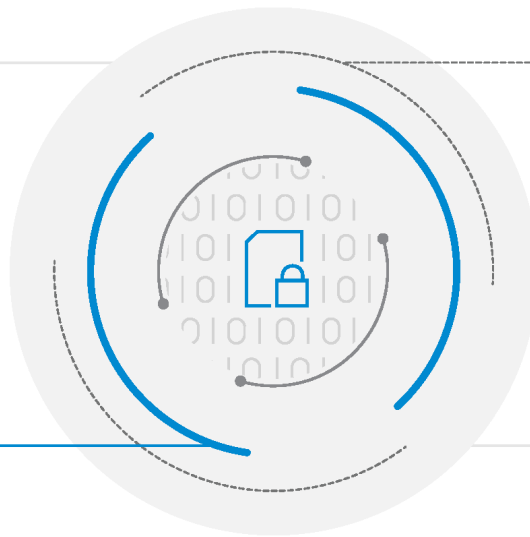
Protezione delle informazioni

- Azure Information Protection
- Windows Information Protection
- Microsoft Cloud App Security
- Prevenzione della perdita dei dati di Office 365
- Microsoft Intune
- BitLocker



Gestione della sicurezza

- Centro sicurezza e conformità Microsoft
- Windows Defender Security Center
- Microsoft Secure Score



"Le persone tendono ad aggirare livelli eccessivamente complessi di sicurezza. Microsoft 365 offre funzionalità native, visibilità sull'ambiente operativo e semplicità per tutti i dipendenti.

Con una strategia di trasformazione digitale mediante tecnologie native supportate da piattaforme sicure come la nostra, avevamo bisogno di ottenere il meglio da tutti i prodotti Microsoft, combinati in Microsoft 365 Enterprise E5".

Simon Hodgkinson: Group Chief Information Security Officer - BP, Regno Unito

Microsoft 365 Enterprise E5 unifica la produttività degli utenti e la sicurezza dell'azienda in un'unica suite

I clienti che adottano la suite di produttività Microsoft possono conseguire significativi vantaggi in termini di sicurezza. Sebbene nessun fornitore di servizi di sicurezza sia in grado di coprire l'intera impronta digitale, grazie agli investimenti e alla scalabilità di Microsoft all'interno delle aziende i nostri clienti possono creare un programma di sicurezza completo e adattivo con una posizione di vantaggio.



Un approccio basato su una piattaforma di sicurezza consente di ridurre il numero di fornitori da gestire



I singoli prodotti sono creati appositamente per l'integrazione, riducendo il costo totale di proprietà



Le funzionalità di sicurezza native riducono le complessità e i tempi di distribuzione



La sicurezza intelligente e adattativa offre agli utenti maggiore libertà sul lavoro, ovunque si trovino e su qualsiasi dispositivo



Le funzionalità di sicurezza si estendono oltre Microsoft per proteggere le piattaforme, le app e i servizi di terze parti



Le funzionalità di integrazione standard si connettono ad altri strumenti di sicurezza (nativi o di terze parti)



La protezione dalle minacce acquisisce le informazioni da una moltitudine di segnali di sicurezza in Intelligent Security Graph nell'intero ecosistema Microsoft globale



Con Azure Active Directory, Korn Ferry autentica e protegge non solo le applicazioni Office 365, ma anche 60 applicazioni aziendali di terze parti, tra cui SAP e Salesforce.com.

"Con Azure Active Directory abbiamo dovuto configurare solo una volta l'autenticazione a più fattori per decine di applicazioni: ora proteggiamo l'intera azienda con una soluzione Single Sign-On. Possiamo impostare criteri più rigidi per i dipendenti esterni rispetto a quelli interni, richiedendo l'autenticazione a più fattori sui dispositivi non gestiti o per determinate applicazioni. Con Microsoft 365, non dobbiamo più effettuare una scelta tra mobilità e sicurezza: possiamo usufruire di entrambe".

Bryan Ackermann: Chief Information Officer, Korn Ferry

Sicurezza completa e adattativa

La tecnologia ha rivoluzionato le procedure di lavoro delle aziende. Dal momento che le persone introducono in azienda dispositivi, app e dati, la protezione delle risorse aziendali richiede un approccio alternativo. È importante individuare il giusto equilibrio tra funzionalità potenti e complesse e un livello generale di sicurezza a lungo termine con il personale e il budget correnti.



Gestione delle identità e degli accessi

- Blocca automaticamente l'accesso per gli utenti se le loro identità o i loro dispositivi sono compromessi o richiedono l'autenticazione a più fattori per elevati livelli di rischio
- Ricevi avvisi quando le credenziali di un utente sono in vendita nel Dark Web e aggiorna il loro livello di rischio
- Scopri le app cloud di terze parti in uso e valuta il loro livello di rischio, in modo da poterle autorizzare o bloccare
- Individua, limita e monitora le identità con privilegi e il loro accesso alle risorse
- Usi un'unica soluzione in grado di proteggere l'identità in locale e nelle directory cloud
- Elimina le password mediante biometria o pin



Protezione delle informazioni

- Proteggi i dati sensibili all'esterno dell'azienda tramite posta elettronica, USB o un'app SaaS di terze parti
- Imposta criteri di sicurezza che possano essere applicati automaticamente se cambia la procedura di accesso ai dati da parte degli utenti, se l'identità di un utente è compromessa o se i dati diventano obsoleti
- Identifica automaticamente le informazioni riservate, come i numeri delle carte di credito o i codici bancari, e applica un'etichetta con protezione al file (questa etichetta può essere automatica o fornire un'indicazione all'utente)
- Analizza i file di dati cronologici locali per ricavare informazioni potenzialmente riservate
- Consenti ad alcuni partner e clienti di accedere alle informazioni riservate
- Rileva e proteggi i dati sensibili che rientrano nell'ambito di normative di adeguamento, come il GDPR



Protezione dalle minacce

- Rileva gli attacchi dai segnali in locale e nel cloud
- Monitora gli endpoint con la possibilità di metterli in quarantena per analizzarli e cancellare il dispositivo, se compromesso
- Usi la protezione avanzata della posta elettronica da tentativi di phishing e minacce sconosciute (zero-day)
- Rileva e rimuovi attacchi ransomware, quindi recupera i file
- Rileva automaticamente anomalie e comportamenti sospetti di utenti ed endpoint senza dover creare regole e perdere tempo a perfezionarle
- Riduci i falsi positivi aggregando contestualmente gli avvisi per identificare uno specifico vettore di attacco
- Esamina automaticamente gli avvisi degli endpoint e correggi le minacce, rimuovendole da tutti i computer interessati
- Insegna agli utenti a proteggersi dagli attacchi di phishing tramite posta elettronica simulando un attacco in un ambiente sicuro



Gestione della sicurezza

- Misurazione quantificabile del tuo livello generale di sicurezza che include soluzioni Microsoft e di terze parti, con la possibilità di stabilire uno standard tra le aziende del tuo settore o di dimensioni analoghe
- Azioni consigliate per migliorare il livello generale di sicurezza
- Report dettagliati sulle minacce più recenti, in modo da poter rispondere a domande come: "Sono sufficientemente protetto dai vettori di minaccia di ultima generazione?"
- Report diagnostici su eventi e incidenti

Accedi a un livello di sicurezza aziendale intelligente e completo

Scarica una versione di prova, esercitati con un modello di verifica o scopri di più all'indirizzo aka.ms//M365E5/Security