McAfee Data Loss Prevention Endpoint

Non diventare il prossimo caso di cronaca per aver perso i tuoi dati.

Stai perdendo dati a tua insaputa? Le informazioni dei tuoi clienti, proprietà intellettuale, dati finanziari e file del personale potrebbero fuoriuscire dalla tua azienda in questo preciso momento. E i responsabili non sono solo gli hacker, sono i tuoi stessi dipendenti. La perdita dei dati, accidentale e dolosa, può avvenire attraverso canali comuni come posta elettronica, post web, drive USB e caricamenti nel cloud, con un costo potenziale nell'ordine di milioni. Ogni giorno ci sono aziende che subiscono perdite di dati a causa della fuoriuscita, dolosa o involontaria, di informazioni. E se potessi bloccare in modo semplice ed efficace la fuga dei dati? Ti piacerebbe poter soddisfare i requisiti di conformità del settore e governativi e proteggere la proprietà intellettuale? Ora puoi grazie alla soluzione completa McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).

Protezione contro la fuoriuscita di dati, dal dispositivo al cloud

McAfee DLP Endpoint è integrato con il modulo DLP di McAfee MVISION CLOUD. Le policy DLP in locale possono essere facilmente estese al cloud con un semplice clic in meno di un minuto[1]. I tag di classificazione DLP in locale sono condivisi con le policy DLP cloud per garantire il rilevamento coerente della perdita di dati.

Funzionalità di protezione avanzate

McAfee DLP Endpoint offre protezione completa per tutti i possibili canali di fuoriuscita dei dati, tra cui dispositivi di archiviazione rimovibili, cloud, email, messaggistica istantanea, web, stampanti, appunti, acquisizione schermo, applicazioni per la condivisione dei file, etc.

Vantaggi principali

- **Protezione contro la fuoriuscita di dati, dal dispositivo al cloud:** estende con facilità le policy DLP in locale al cloud per garantire il rilevamento coerente della perdita di dati.
- **Funzionalità di protezione avanzate:** sfrutta fingerprinting, classificazione e tagging dei file per proteggere dati sensibili non strutturati come la proprietà intellettuale e segreti commerciali.
- **Gestione centralizzata:** l'integrazione nativa con il software McAfee® MVISION ePolicy Orchestrator® (MVISION ePO™) permette di ottimizzare la gestione di policy e incidenti[2].
- **Applicazione della conformità:** assicura la conformità rivolgendosi alle azioni quotidiane dell'utente, come l'invio di email, la pubblicazione su cloud, il download su dispositivi rimovibili e altro.

Seguici su:

Le principali caratteristiche di McAfee DLP Endpoint includono:

- Possibilità di impostare le etichette di Microsoft Azure Information Protection (AIP) per i dati in movimento e di riconoscere i file con etichetta AIP[3].
- L'integrazione con l'analisi comportamentale degli utenti (UEBA) di terze parti contrasta le minacce interne. Esegue analisi di sicurezza per rilevare comportamenti insoliti e altamente pericolosi di utenti ed entità.
- Classificazione manuale: permette agli utenti di classificare manualmente i documenti, aumenta la sensibilizzazione in merito alla protezione dei dati dei dipendenti e riduce il carico amministrativo.
- Scansioni e remediation avviabili dall'utente: gli utenti finali possono eseguire le scansioni di scoperta degli endpoint e avviare le azioni di remediation automatica.
- Classificazione flessibile inclusi dizionari, espressioni regolari e algoritmi di validazione, documenti registrati e supporto per soluzioni di classificazione dell'utente finale di terze parti.
- Tecnologia unica di assegnazione dei tag per l'identificazione dei documenti in base alla loro provenienza che aiuta a evitare che informazioni sensibili di applicazioni web, di rete e condivisioni di rete vengano duplicate, rinominate o escano dalle sedi aziendali.
- Supporto avanzato alla virtualizzazione per proteggere i desktop remoti e le soluzioni VDI (Virtual Desktop Infrastructure).

Gestione centralizzata

- Gestito da una console di gestione cloud nativa - McAfee MVISION ePO - per una gestione ottimizzata delle policy e degli incidenti[4].
- Condivide gli stessi motori di classificazione, policy e flussi di lavoro degli incidenti con McAfee® MVISION Cloud (CASB) e McAfee® Network DLP.
- Molteplici policy e serie di regole riutilizzabili offrono la possibilità di definire diverse policy DLP all'interno dell'azienda, e consentono di creare policy in base a ufficio, dipartimento, normativa e altro ancora.
- Un maggior livello di dettaglio nella gestione degli eventi permette di effettuare query, filtrare e visualizzare in base alle caratteristiche dell'evento (per esempio, numero seriale del dispositivo, nome del file prova e gruppi).
- Funzionalità di monitoraggio e auditing centralizzate degli eventi.
- Controllo accessi basato su ruoli migliorato (noto anche come separazione dei compiti) per la gestione delle policy e per la disamina degli eventi.
- Semplice accesso all'interfaccia dell'help desk.
- **Educazione dell'utente:** riscontri in tempo reale tramite un pop-up educativo aiutano a modellare la cultura e la consapevolezza della sicurezza aziendale.

Piattaforme supportate

- Microsoft Windows 10 (32 e 64 bit)
- Microsoft Windows 8 o 8.1 (32 e 64 bit)
- Microsoft Windows 7 (32 e 64 bit)
- Microsoft Windows Server 2019
- Microsoft Windows 2016 (64 bit)
- Microsoft Windows 2012 (64 bit) e Microsoft Windows 2012 R2 (64 bit)
- Microsoft Windows 2008 (32 e 64 bit) e Microsoft Windows 2008 R2 (32 e 64 bit)
- macOS Catalina 10.15 o versioni successive
- macOS Mojave 10.14 o versioni successive
- macOS High Sierra 10.13 o versioni successive
- macOS Sierra 10.12 o versioni successive
- macOS X El Capitan 10.11 o versioni successive
- macOS X Yosemite 10.10 o versioni successive
- macOS X Mavericks 10.9.0 o versioni successive

Browser supportati

- Microsoft Internet Explorer versione 11 o successive

Applicazione della conformità e formazione dell'utente finale

Poiché i confini dell'azienda si fanno sempre più flebili, per le aziende è sempre più difficile applicare la conformità. McAfee DLP Endpoint non solo può aiutarti a monitorare i comportamenti quotidiani dell'utente, ma anche assicurare la conformità formando gli utenti stessi. Tramite la semplice pressione di un tasto, McAfee DLP Endpoint fornisce report dettagliati per dimostrare a revisori, responsabili aziendali e altri interessati che sono state messe in atto misure di conformità interna e con le normative. Offre policy basate su modelli per normative e casi d'uso, rendendo più semplice mantenere la conformità. Gli utenti ricevono riscontri in tempo reale tramite pop-up per l'applicazione in base alla policy aziendale; queste opportunità formative in pillole ti aiutano a creare una cultura per la sicurezza aziendale più solida.

1. Basato su test di laboratorio interni McAfee.
2. McAfee DLP Endpoint 11.5 o versioni successive
3. Ibidem
4. Ibidem

- Mozilla Firefox 48 o versioni successive
- Google Chrome 65 o versioni successive

Software McAfee ePO supportato

- McAfee ePO 5.9.1 e 5.10 per DLP 11.1 o versioni successive

Supporto per McAfee MVISION ePO (SaaS)

- Per le versioni DLP 11.5 o successive, non è richiesta l'installazione di software o estensioni DLP. Sono necessari nome utente e password per autenticare l'accesso a McAfee MVISION ePO.

Per un elenco completo di piattaforme, browser e software supportati, fare riferimento alla Knowledge Base McAfee.

Ulteriori informazioni

Ulteriori informazioni sono disponibili sul sito www.mcafee.com/it/products/dlp-endpoint.aspx.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it