

McAfee Data Loss Prevention Prevent

Implementazione delle policy per la protezione delle informazioni sensibili

L'aumento del numero di persone che condividono elettronicamente le informazioni fa incrementare le probabilità che qualcuno spedisca inavvertitamente o intenzionalmente informazioni sensibili a destinatari non autorizzati e metta a repentaglio i dati aziendali riservati. Le informazioni possono uscire dall'azienda tramite molti differenti canali: email, web, messaggistica immediata (IM) o FTP. Alcuni messaggi o transazioni sono consentiti, ma devono essere crittografati per garantire la riservatezza dei dati. Altri tipi di comunicazioni sono invece del tutto inaccettabili in qualsiasi circostanza e devono essere bloccate. Implementare le policy giuste al momento giusto è fondamentale per garantire la sicurezza dei dati, la conformità normativa e la protezione della proprietà intellettuale.

Implementazione delle policy di sicurezza per i dati in movimento

In ogni reparto di ogni azienda, le persone condividono i dati utilizzando più applicazioni e una serie di protocolli. Per evitare la fuga di dati accidentale o intenzionale, le aziende devono poter impedire in modo proattivo la fuoriuscita delle informazioni sensibili dalla rete e implementare processi di business corretti.

McAfee® Data Loss Prevention Prevent (McAfee DLP Prevent) consente di applicare le policy relative alle informazioni che escono dalla rete attraverso vari

canali (email, webmail, messaggistica immediata, wiki, blog, portali, HTTP/HTTPS e FTP) grazie all'integrazione con i gateway MTA (Message Transfer Agent) utilizzando SMTP (Simple Mail Transfer Protocol) o con i proxy web conformi al protocollo ICAP (Internet Content Adaptation Protocol). Se viene rilevata la violazione di una policy, McAfee DLP Prevent consente di adottare una serie di misure correttive, ad esempio l'applicazione di crittografia, blocco, reindirizzamento e messa in quarantena, per garantire la conformità alle normative sulla riservatezza delle informazioni sensibili e per ridurre il rischio delle minacce alla sicurezza.

Vantaggi principali

Sfrutta l'infrastruttura esistente

- Proteggi l'email aziendale attraverso l'integrazione con i gateway MTA (Message Transfer Agent) utilizzando SMTP con le intestazioni X-header per garantire blocco, bouncing, cifratura, quarantena e reindirizzamento.
- Controlla il traffico attraverso l'integrazione con i proxy web conformi a ICAP (Internet Content Adaptation Protocol) per bloccare le violazioni del contenuto su HTTP, HTTPS, IM, FTP e webmail.

Implementa le policy in modo proattivo per tutti i tipi di informazioni.

- Proteggi più di 300 tipi di contenuti diversi.
- Implementa le policy per le informazioni che sai essere sensibili e per le informazioni non ovvie di cui non sei a conoscenza.
- Sfrutta la scalabilità per supportare centinaia di migliaia di connessioni contemporanee.

SCHEDA TECNICA

Pienamente unificato con il software McAfee ePolicy Orchestrator

McAfee DLP Prevent è pienamente unificato con il software McAfee® ePolicy Orchestrator® (McAfee ePO™) e con McAfee Data Loss Prevention Endpoint (McAfee DLP Endpoint) grazie alla comune gestione di policy, eventi e casi. Gli amministratori possono creare una singola policy di protezione per email e web nel software McAfee ePO, da distribuire a endpoint e rete. In aggiunta, McAfee DLP Endpoint e McAfee DLP Prevent condividono un motore di classificazione comune che permette una sola policy per email e web. I dizionari comuni e la sintassi delle espressioni regolari (regex) offrono continuità per la creazione di regole comuni per la protezione di web ed email. Con la gestione centralizzata le soluzioni McAfee DLP offrono la visibilità da un singolo pannello di controllo e fanno aumentare l'efficienza aziendale riducendo i carichi amministrativi.

Monitora l'email mobile

McAfee DLP Prevent per le email mobile offre una protezione sensibile ai contenuti della posta elettronica mobile intercettando le email scaricate nel dispositivo mobile tramite il proxy ActiveSync con capacità DLP. Inoltre è capace di intercettare ActiveSync sia su Microsoft Exchange in sede sia su Microsoft Office 365 Hosted Exchange. È totalmente gestito dal software McAfee ePO ed è incluso nella licenza di McAfee DLP Prevent. Non richiede l'installazione di nessun agente nei dispositivi mobili. Con McAfee DLP Prevent per le email mobile, le imprese possono monitorare la conformità delle email, raccogliere prove e proteggere i dispositivi mobili gestiti e non gestiti.

Integrazione con i proxy web e i gateway MTA per una maggiore protezione

McAfee DLP Prevent si integra con i proxy web (attraverso ICAP) e i gateway MTA (attraverso le intestazioni X-header) per eseguire l'azione richiesta. Poiché interrompe le transazioni non autorizzate a livello di applicazione anziché chiudere semplicemente la sessione TCP, misura che non contribuisce a modificare il comportamento dell'applicazione, McAfee DLP Prevent avvisa l'applicazione di avvio che la trasmissione è stata negata per una violazione alle policy. Questo garantisce una protezione dei dati superiore per l'azienda, poiché McAfee DLP Prevent impara cosa deve essere protetto e impedisce all'applicazione di ripetere lo stesso comportamento.

Protezione per le informazioni sensibili note e ignote

Grazie alla sua capacità di classificare più di 300 tipi diversi di contenuto, McAfee DLP Prevent ti aiuta a garantire la sicurezza delle informazioni che devono restare riservate (numeri di carte di credito, codici fiscali, dati finanziari). Ti aiuta inoltre a capire quali sono le informazioni o i documenti che richiedono protezione, come le proprietà intellettuali altamente complesse. McAfee DLP Prevent incorpora un'ampia gamma di policy che includono conformità, uso accettabile e proprietà intellettuale, consentendoti di abbinare interi documenti o una loro parte a una serie completa di regole, al fine di proteggere tutte le informazioni sensibili, sia note che sconosciute.

Classifica, analizza e poni rimedio alla fuga di dati.

- Filtra e controlla le informazioni sensibili per identificare i rischi noti o sconosciuti.
- Indicizza e implementa policy di sicurezza estremamente precise per tutti i tipi di contenuto.
- Applica le policy di accesso alla condivisione file per impedire agli utenti di accedere a informazioni o archivi in modalità non autorizzate.

Specifiche

Throughput di sistema

Fino a 150 Mbit/s di analisi, indicizzazione e conservazione completa dei contenuti.

Integrazione nella rete

Si integra nella rete come appliance fuori percorso, che è attiva all'interno del percorso di dati attraverso MTA e proxy web conformi a ICAP.

Tipi di contenuti

Supporta la classificazione file per oltre 300 tipi di contenuto, compresi:

- Documenti Microsoft Office
- File multimediali
- P2P

SCHEDA TECNICA

Personalizzazione di viste e report degli eventi

Attraverso il software McAfee ePO puoi personalizzare le viste riassuntive degli eventi di sicurezza e le azioni successive in base a qualsiasi coppia di punti pivot contestuali. Sono disponibili viste elenco, dettagliate e di riepilogo con le tendenze. McAfee DLP Prevent comprende anche molti report predefiniti, ciascuno dei quali può essere visualizzato, salvato per un uso successivo o pianificato per la consegna periodica.

Classificazione dati complessa

McAfee DLP Prevent consente alla vostra azienda di proteggere ogni tipo di dati sensibili, dai dati comuni e con formato fisso alle complesse proprietà intellettuali estremamente variabili. Grazie alla combinazione di questi meccanismi di classificazione degli oggetti, McAfee DLP Prevent si avvale di un motore di classificazione estremamente accurato e dettagliato che blocca le informazioni sensibili e identifica i rischi nascosti o sconosciuti. I meccanismi di classificazione degli oggetti comprendono:

- **Classificazione multilivello:** riguarda sia le informazioni contestuali che i contenuti in formato gerarchico.
- **Registrazione documenti:** comprende le firme biometriche delle informazioni che vengono modificate.
- **Analisi grammaticale:** rileva la grammatica o la sintassi di ogni elemento, come documenti di testi, fogli di calcolo o codici sorgente.
- **Analisi statistica:** registra il numero di volte che una firma, una forma grammaticale o una corrispondenza biometrica compare in un documento o file in particolare.
- **Classificazione dei file:** identifica i tipi di contenuto a prescindere dall'estensione applicata al file o dalla compressione.

Opzioni del fattore di forma e del tipo di appliance

McAfee DLP Discover è disponibile come appliance hardware o virtuale. Per maggiori dettagli consulta la **scheda tecnica dell'appliance hardware McAfee DLP 6600**.

- Codici sorgente
- File di progettazione
- Archivi
- File crittografati

Protocolli supportati

Supporta HTTP, HTTPS, FTP e i protocolli di messaggistica immediata attraverso un protocollo ICAP verso un proxy conforme a ICAP. Per informazioni sui protocolli supportati dal proxy in dotazione, rivolgiti al fornitore del proxy. Supporta SMTP mediante l'integrazione con i gateway MTA.

Policy incorporate

- Incorpora un'ampia gamma di policy e regole per le esigenze più comuni, compresa la conformità alle normative, la proprietà intellettuale e l'uso accettabile.
- Offre la personalizzazione completa delle regole per rispondere a esigenze aziendali specifiche sfruttando il database acquisizioni di McAfee.



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

McAfee, il logo McAfee, ePolicy Orchestrator e McAfee ePO sono marchi o marchi registrati di McAfee, LLC o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. Copyright © 2017 McAfee, LLC. 3332_0717 LUGLIO 2017