Forcepoint | SECLORE

Sintesi della soluzione

Seclore per Forcepoint DLP

Sfida

- Una soluzione DLP può impedire che i dati sensibili lascino l'azienda oppure monitorarli dopo che sono sfuggiti al tuo controllo. Se blocchi i dati in uscita, interrompi i flussi di lavoro a scapito della produttività, mentre se opti per il monitoraggio, i dati vengono trasmessi senza protezione e abbandonati al loro destino.

Soluzione

- Aggiungere automaticamente dei controlli persistenti e granulari sull'uso dei dati rilevati
- Assegnare e revocare dinamicamente e immediatamente le autorizzazioni sui file
- Associare le autorizzazioni di sicurezza alle regole di business DLP
- Proteggere i dati sugli endpoint, nella rete o all'interno delle e-mail
- Acquisire dettagli forensi sull'uso dei dati

Risultato

- Accelerare la distribuzione delle soluzioni DLP per tagliare i costi e velocizzare il "time to value"
- Ridurre drasticamente i falsi positivi per contenere gli oneri amministrativi
- Consentire la collaborazione costante tra gli operatori dentro e fuori l'azienda
- Mantenere il controllo e monitorare i dati sensibili quando lasciano l'azienda
- Superare le verifiche e assicura la conformità alle normative

DLP (Data Loss Prevention) individua i dati sensibili e impedisce che escano dalla rete aziendale. Ma cosa succede dopo che i dati sono stati rilevati? Che cosa fai con tutti gli incidenti scoperti? Come fai a proteggere la collaborazione con partner commerciali esterni e di terze parti, se le e-mail vengono bloccate all'endpoint o vengono inviate non protette? Come puoi proteggere i file condivisi tramite il cloud o che i tuoi collaboratori esterni visualizzano su dispositivi mobili? Come fai a recuperare dei dati sensibili finiti nelle mani sbagliate?

Seclore Rights Management e Forcepoint DLP

DLP è in grado di ispezionare il contenuto dei documenti e individuare i dati sensibili. Una volta che hai rilevato i dati sensibili, puoi aggiungere automaticamente i controlli (diritti) d'uso appropriati sui documenti e sulle interazioni con i dati. Integrando Seclore Rights Management ottieni il controllo completo sulle informazioni e persino la possibilità di revocare completamente il diritto di accesso, anche oltre i confini della tua azienda. Non appena Forcepoint DLP rileva dei dati sensibili, Seclore può proteggerli immediatamente con le policy di utilizzo appropriate. I controlli persistenti e granulari di Seclore sull'uso dei dati restano associati al file ovunque esso sia, all'interno o all'esterno dell'azienda, e proteggono i dati mentre sono in uso (file in lavorazione), in transito (inviati tramite e-mail) e a riposo (a prescindere dal formato file, dal dispositivo e dal sistema operativo).

Potenza raddoppiata

Seclore Rights Management ti aiuta a cambiare l'approccio alla sicurezza da "reattivo" a "proattivo" quando utilizzi Forcepoint DLP. Tradizionalmente la DLP è configurata in modalità di "monitoraggio", cioè con dashboard, report e avvisi per tenere traccia delle informazioni che lasciano l'azienda. La modalità di monitoraggio è un'applicazione standard della DLP, ma il problema resta la sicurezza dei dati sensibili che escono dall'azienda. Se i tuoi dati sensibili cadono nelle mani di un malintenzionato o se hai bisogno di recuperarli da una terza parte, dovrai attivarti per riaverli. Con Seclore il controllo è sempre nelle tue mani.

Inoltre Seclore Rights Management accelera significativamente l'adozione di Forcepoint DLP. Se hai incertezze sulla regola di business da applicare ai dati rilevati (bloccarli, metterli in quarantena, autorizzarli ecc.), la protezione automatica con Seclore può diventare l'azione predefinita. In questo modo eviti anche di dover cambiare continuamente la configurazione.

Che cosa rileva DLP

- → Esamina i contenuti per rilevare:
  - Parole chiave
  - Schemi ricorrenti
  - Fingerprint digitali
  - Riconoscimento ottico dei caratteri (OCR)
- → Impedisce che i dati sensibili lascino il perimetro aziendale
- → Registra gli incidenti all'interno dell'azienda

Che cosa protegge Rights Management

- → Protegge i contenuti:
  - Con controlli granulari sull'uso
  - Specificando chi può accedere a cosa, dove, quando e come
  - Limitando e revocando gli accessi
  - Nei dati in uso, in transito e a riposo
- → Permette agli utenti esterni autorizzati di accedere ai dati sensibili
- → Traccia e controlla i dati all'interno e all'esterno dell'impresa

Abbinando Seclore RM e Forcepoint DLP puoi controllare chi può accedere a un documento, come può utilizzarlo, quando e da quale computer o dispositivo. Se aggiungi dei controlli sull'uso persistenti e incentrati sui dati, puoi estendere la portata di Forcepoint DLP ai documenti che viaggiano attraverso le reti pubbliche e dei partner, a quelli archiviati nel cloud o usati in servizi di condivisione file oppure ai documenti utilizzati a partire da dispositivi mobili.

Protezione istantanea: sugli endpoint, in rete o nel cloud

I dati sensibili individuati durante le scansioni di Forcepoint DLP (negli endpoint, in rete o nel cloud) possono essere protetti istantaneamente da Seclore Rights Management. Ad esempio, le policy di protezione di Seclore possono essere associate al rilevamento di parole chiave o espressioni regolari sensibili (come i numeri delle carte di credito). I controlli sull'uso assicurano che nessun utente al di fuori dell'ufficio responsabile (e tantomeno al di fuori dell'azienda) possa utilizzare quel documento anche se lo ha ricevuto. Con Forcepoint DLP la protezione viene estesa ulteriormente utilizzando il fingerprinting di precisione per identificare i dati sensibili ovunque si trovino (ad esempio sui file server) o mentre vengono distribuiti dagli utenti; in questo modo gli amministratori possono concentrare la loro attenzione su utenti e comportamenti più rischiosi.

Questa protezione è, inoltre, quasi immediata e completamente automatica. L'applicazione automatica dei controlli sull'uso basati sulle policy di rilevamento di DLP comporta l'assenza di passaggi aggiuntivi per i dipendenti, ovvero meno costi di formazione e meno sforzi per gestire i cambiamenti.

Figura 1: Risultati del rilevamento associati automaticamente alla policy di protezione.

Seclore Rights Management e Forcepoint DLP Endpoint

Forcepoint DLP può analizzare i documenti e rilevare i dati riservati che si trovano sugli endpoint di rete. Forcepoint DLP può abbinare delle parole chiave (ad esempio, proiezioni di entrate), schemi ricorrenti ed espressioni regolari (ad esempio, numeri di carte di credito) e può anche controllare cartelle specifiche o cercare documenti in formati specifici. Dopo il rilevamento, Seclore protegge queste informazioni sensibili, applicando la policy Seclore pertinente per prevenire la fuga o l'uso improprio di tali dati, sulla base delle definizioni della policy impostate dall'amministratore dell'azienda. Con Forcepoint DLP le policy di rete possono essere estese anche ai dispositivi non collegati alla rete e applicate a livello dei singoli endpoint, in modo da proteggere i dati anche quando gli utenti operano da remoto.

Vantaggi

- → Protezione automatica delle informazioni sensibili, in rete o fuori rete
- → Ridotta necessità di affidarsi agli utenti per la protezione dei dati sensibili
- → Protezione associata stabilmente al file, a prescindere che sia archiviato, in transito e in uso

Figura 2: Rilevamento sugli endpoint

Seclore Rights Management e Forcepoint DLP Network

Forcepoint DLP analizza i documenti sensibili che risiedono nei file server. La protezione dei dati che viaggiano all'interno e all'esterno dell'azienda è fondamentale. Con DLP Network, i dati in uso vengono protetti mediante il monitoraggio dei loro flussi attraverso canali di comunicazione come e-mail e web. Seclore estende la protezione alle informazioni sensibili per evitarne la fuga o usi impropri.

Figura 3: Rilevamento in rete

Seclore Data Classification e Forcepoint DLP

Seclore Data Classification, con la tecnologia di Boldon James, funziona in sinergia con Forcepoint DLP per ridurre i falsi positivi durante il rilevamento dei dati.

- → **Un utente classifica**, ad esempio, un documento di Office semplicemente facendo clic su un'etichetta di classificazione nella barra multifunzione di Office.
- → **Forcepoint DLP marca** il documento in base alla classificazione selezionata.
- → **Seclore Rights Management protegge** il documento con la policy di utilizzo appropriata. La protezione Seclore resta attiva ogni volta che il documento viene aperto, ovunque nel mondo.
- → **Con il fingerprinting di Forcepoint** puoi sapere anche se solo una parte di un documento viene copiata, incollata o modificata, per consentirti di rilevare e prevenire l'esfiltrazione dei dati.
- → Tutte le attività eseguite sul documento sono registrate in un archivio centrale, in tempo reale. Poiché la classificazione del documento viene selezionata dall'utente, le **possibilità di falsi positivi sono praticamente zero.**

Seclore protegge automaticamente le mail con Forcepoint Email Security

DLP Email Security viene spesso eseguito in modalità di rilevamento, a causa del rischio di falsi positivi, ma eventuali comportamenti anomali degli utenti vengono rilevati solo a fatto compiuto. Per i dati che devono uscire dalla rete per motivi di business, non c'è altra scelta che permettere l'invio delle e-mail senza alcuna protezione.

Seclore offre una soluzione semplice e ottimizzata a questi problemi. Quando le e-mail vengono elaborate da DLP Email Gateway, la funzionalità di protezione automatica di Seclore Rights Management protegge l'e-mail e i suoi allegati con la policy di utilizzo appropriata. In questo modo i destinatari non possono usare l'e-mail in modo scorretto né divulgarla dopo averla ricevuta e letta. Una policy di autorizzazione di DLP diventa così una policy "per i prossimi 10 giorni" con Seclore.

Con la protezione automatica delle e-mail di Seclore Rights Management, le esigenze di sicurezza vengono soddisfatte senza ostacolare la collaborazione tramite e-mail, di importanza critica per il business. La condivisione dei dati può continuare, preservando la sicurezza e la conformità. E tutto ciò con una trasparenza completa per il mittente e il destinatario dell'e-mail.

Figura 4: Seclore e Forcepoint DLP

Decrittografia sicura delle e-mail per il rilevamento dei contenuti con Forcepoint DLP

Una sfida che i sistemi DLP devono affrontare è scoprire i contenuti sensibili nelle e-mail e negli allegati crittografati per decidere se un'e-mail deve essere condivisa o bloccata. Seclore Decrypter for Email risolve questo problema consentendo un accesso sicuro alle e-mail e agli allegati crittografati Seclore. Quando l'e-mail protetta viene decrittografata, Forcepoint DLP può cercare schemi ripetitivi e contenuti sensibili e prendere decisioni appropriate (consentire / bloccare / proteggere). Seclore Decrypter for Email funziona insieme a Email Auto-Protector di Seclore per automatizzare la protezione delle e-mail prima di inviarle all'esterno dell'azienda.

Le aziende che utilizzano Seclore Rights Management e Forcepoint DLP ora possono confermare la conformità alle normative, in quanto Forcepoint DLP può rilevare, tracciare e verificare tutti i file, protetti o meno.

Vantaggi principali per il business

Protezione automatizzata dei dati
L'integrazione della tecnologia DRM (Digital Rights Management) in DLP automatizza l'intero processo di classificazione, protezione, controllo sull'uso e audit. Il passaggio dal rilevamento alla protezione avviene senza soluzione di continuità. Il processo di protezione DRM è completamente trasparente per l'utente finale.

Implementazioni DLP più veloci
Il DRM può essere impostato come regola di business "predefinita" di DLP per ottenere vantaggi immediati da DLP subito dopo l'implementazione.

Sicurezza e conformità oltre il firewall
L'integrazione DLP-DRM protegge e verifica i dati ovunque viaggino: nelle reti dei fornitori e dei partner, in reti pubbliche, nel cloud o in dispositivi mobili.

Meno anomalie
DLP può essere configurato per trattare i file protetti da DRM come file sicuri per i quali non occorre generare avvisi. Questo riduce nettamente il numero di anomalie registrate.

Oneri minimi di formazione
La formazione richiesta per gli utenti finali è quasi nulla, dato che la protezione è automatica e un documento protetto si apre nell'applicazione nativa come qualsiasi altro documento.

Business più agile
La capacità di proteggere le informazioni che viaggiano oltre i confini aziendali risolve una sfida spinosa di conformità, riduce significativamente i rischi di sicurezza e permette l'adozione sicura di servizi di file-sharing, BYOD e cloud computing.

Verifica end-to-end e conformità alle normative
L'integrazione DLP-DRM assicura la conformità agli obblighi normativi per l'intero ciclo di vita dei dati non strutturati, sia all'interno che all'esterno della rete aziendale.

Applicazione delle policy IT a terze parti
L'integrazione DLP-DRM aiuta a imporre a collaboratori, fornitori, partner e altre terze parti le policy IT aziendali e di governance dei dati.

Informazioni su Forcepoint

Forcepoint è l'azienda leader nel settore della sicurezza informatica per la protezione degli utenti e dei dati. La sua missione è tutelare le aziende e guidare la crescita e la trasformazione digitale. Le soluzioni human-centric di Forcepoint si adattano in tempo reale alle modalità di interazione uomo/dati, consentono un accesso sicuro e, allo stesso tempo, permettono ai dipendenti di creare valore. Dalla sua sede di Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti in tutto il mondo.

forcepoint.com/contact

Informazioni su Seclore

Seclore propone la prima piattaforma di sicurezza data-centric del mercato basata su browser. La piattaforma Seclore offre alle organizzazioni la flessibilità necessaria per usare le soluzioni migliori della categoria per rilevare, identificare, proteggere e verificare l'uso dei dati ovunque viaggino, sia all'interno che all'esterno del perimetro aziendale. La capacità di automatizzare il processo di sicurezza incentrato sui dati permette alle aziende di proteggere appieno le informazioni, riducendo al minimo inconvenienti e costi. Oltre 2000 aziende in 29 Paesi utilizzano Seclore per realizzare i loro obiettivi di sicurezza, governance e conformità dei dati.

seclore.com/contact