Forcepoint DLP

BLOCCA LA PERDITA E IL FURTO DI DATI, MANTIENI CONFORMITÀ E SALVAGUARDIA IL MARCHIO, LA REPUTAZIONE AZIENDALE E LA PROPRIETÀ INTELLETTUALE

FORCEPOINT
POWERED BY Raytheon

Forcepoint DLP

BLOCCA LA PERDITA E IL FURTO DI DATI, MANTIENI CONFORMITÀ E SALVAGUARDIA IL MARCHIO, LA REPUTAZIONE AZIENDALE E LA PROPRIETÀ INTELLETTUALE

Da una reputazione compromessa a multe e sanzioni normative, una violazione dei dati può avere conseguenze devastanti. Forcepoint DLP ti consente di identificare e di proteggere i tuoi dati sensibili ovunque si trovino – agli endpoint, nel Cloud o in sede. Espandi il tuo business e promuovi innovazione con l'uso di servizi di collaborazione Cloud-based, quali Microsoft Office 365 e Box. Proteggi i tuoi asset di maggior valore residenti nei laptop Mac OS X e Microsoft Windows. Proteggi i tuoi dati personali, la tua proprietà intellettuale e soddisfa i requisiti di conformità in modo rapido per mezzo di una libreria con policy pronte all'uso, grazie alle funzioni DLP esclusive di Forcepoint per il blocco del furto di dati.

La prevenzione contro la perdita di dati (DLP) potenzia il tuo business

- Riduci il rischio della perdita di dati mediante l'adozione di servizi Cloud-based quali Microsoft Office 365 e Box che ti garantiscono una maggiore visibilità dei dati.
- Implementa controlli efficaci di sicurezza che puoi facilmente analizzare per soddisfare requisiti di conformità e requisiti normativi.
- Identifica i tuoi dati più sensibili incorporati nelle immagini, quali dati scannerizzati e schermate.
- Identifica e previeni minacce di attacchi interni con l'analisi del comportamento.
- Cerca e proteggi facilmente file archiviati in dispositivi endpoint Mac, Microsoft Windows e Linux.
- Unifica le tue soluzioni di sicurezza, coordina le policy di difesa, condividi l'intelligence tra molteplici punti e trai vantaggio da una gestione centralizzata della sicurezza dei tuoi dati.
- Il centro di gestione degli incidenti e il workflow delle email consentono che l'analisi di incidenti relativi alla perdita di dati e la risposta a tali incidenti siano eseguite da personale qualificato.

Funzioni chiave

- Riconoscimento di dati sensibili incorporati in immagini, documenti scannerizzati e schermate.
- Utilizzo sicuro di servizi Cloud-based quali Microsoft Office 365 e Box mantenendo visibilità e controllo dei dati sensibili.
- Drip DLP monitora l'attività di trasferimento di dati cumulativi nel corso del tempo al fine di scoprire eventuali fughe di dati in piccole quantità.
- Identificazione dei dipendenti ad alto rischio mediante il rilevamento di attività indicative di un possibile furto di dati.
- Rilevamento dei dati registrati mediante impronte digitali (fingerprinted) su dispositivi endpoint collegati o meno alla rete aziendale.
- Dispositivi endpoint supportati da Mac OS X e Microsoft Windows.
- Rilevamento di dati sensibili in uscita dall'organizzazione tramite e-mail, upload nel web, IM e client di servizi Cloud-based. Comprende la decrittografia SSL quando utilizzata con Forcepoint Web Security.

"TRITON Architecture data security è la soluzione più efficace che abbiamo trovato per proteggerci e prevenire la perdita di dati."

— Amir Shahar, Information Security Manager, Cellcom Israel Ltd.

Funzioni di Forcepoint DLP

SOSTIENI L'INNOVAZIONE CON DETERMINAZIONE

La soddisfazione delle esigenze del cliente e il mantenimento della tua competitività di mercato richiedono innovazione e il sostegno dell'adozione di nuove tecnologie da parte dei tuoi dipendenti. Forcepoint DLP ti consente di trarre vantaggio da potenti sevizi Cloud-based quali Microsoft Office 365, Box e SalesForce.com nonché di sostenere la crescita e innovazione della tua organizzazione. Forcepoint DLP potenzia il tuo personale che lavora in roaming mediante la protezione dei dati sensibili e della proprietà intellettuale, sia internamente che esternamente alla rete.

MANTIENI E DIMOSTRA CONFORMITÀ

Un'ampia libreria di policy pronte a essere usate facilita l'implementazione di controlli da parte del personale IT al fine di soddisfare requisiti normativi e proteggere le proprietà intellettuali. Puoi scegliere le policy più idonee a soddisfare i tuoi requisiti di conformità e le policy necessarie alla protezione della tua proprietà intellettuale. Forcepoint ti offre una serie di funzioni avanzate per il rilevamento degli IP, dotate della flessibilità sufficiente a soddisfare esigenze di protezione dei dati con un'interfaccia GUI intuitiva che ti consente di selezionare le policy più idonee a proteggere la tua proprietà intellettuale e i tuoi dati più sensibili mediante l'uso di un unico template. Forcepoint ti aiuta anche a soddisfare requisiti di auditing mediante la generazione di report standardizzati che puoi personalizzare a seconda delle necessità.

IDENTIFICA E PROTEGGI DATI SENSIBILI INCORPORATI IN UN'IMMAGINE

Una schermata dannosa o una documentazione preesistente scannerizzata e archiviata come un'immagine potrebbe contenere zone vulnerabili alle soluzioni DLP tradizionali, ma non a Forcepoint DLP. Grazie all'OCR (Optical Character Recognition – Riconoscimento ottico dei caratteri) puoi identificare e proteggere facilmente i dati sensibili incorporati in un'immagine. Questa funzione ti consente di controllare il flusso di dati sensibili incorporati in una schermata, nelle pagine trasmesse via fax, in smart phone e foto di tabelle nonché assegni, ricevute e file pre-esistenti scannerizzati, e ti protegge dagli attacchi avanzati e dalle minacce di attacchi interni finalizzati al furto di dati. Altre funzioni esclusive ti aiutano a identificare crittografie personalizzate e metodi di "Drip Data Loss" (perdita lenta di dati) utilizzati spesso per evadere il rilevamento.

IDENTIFICA IL COMPORTAMENTO DI UTENTI AD ALTO RISCHIO E ISTRUISCI ADEGUATAMENTE GLI UTENTI AL FINE DI RENDERLI PIÙ CONSAPEVOLI

Da errori commessi dall'utente a intenzioni dannose, gli utenti finali sono spesso i primi responsabili di incidenti con perdita di dati. Forcepoint DLP utilizza tecniche di analisi del comportamento per identificare in modo proattivo gli utenti che pongono un alto rischio:

- Utenti inesperti pongono spesso un alto rischio a causa di cattive abitudini che possono essere evidenziate e corrette prima che si verifichi una perdita reale.
- Dipendenti scontenti possono venire identificati ai primi segni di esecuzione di un'attività dannosa.

Forcepoint DLP fornisce agli utenti l'accesso ai dati di cui hanno bisogno per espandere il business mitigando nel contempo eventuali minacce interne.

Componenti di Forcepoint DLP

Esistono due opzioni di base disponibili in Forcepoint DLP che possono essere implementate insieme o separatamente al fine di conseguire i tuoi obiettivi di sicurezza. Queste due opzioni offrono la flessibilità necessaria a soddisfare le esigenze odierne oltre a un adattamento continuo alla crescita dell'azienda.

FORCEPOINT DLP DISCOVERY	Per garantire la sicurezza dei dati, bisogna sapere dove si trovano. Forcepoint DLP Discovery ti consente di trovare e proteggere i tuoi dati sensibili nell'ambito dell'intera rete nonché i dati sensibili archiviati nei servizi Cloud-based quali Microsoft Office 365 e Box. Con l'aggiunta di Forcepoint DLP Endpoint, la potenza di Forcepoint DLP Discovery può essere estesa agli endpoint di Mac OS X e Microsoft Windows sia su rete che fuori rete.
FORCEPOINT DLP NETWORK	L'ultima possibilità di bloccare il furto di dati è quando sono in via di trasmissione tramite e-mail e i canali Web. Forcepoint DLP Network ti aiuta a identificare e impedire la perdita accidentale di dati o dovuta a eventi dannosi causati da attacchi esterni o da minacce interne, quest'ultimo un fenomeno in continua crescita. Combatti le tecniche di evasione delle minacce avanzate con il potente OCR per il riconoscimento dei dati incorporati in un immagine. Utilizza "Drip DLP" per bloccare il furto di dati, un blocco di dati per volta, e per monitorare il comportamento ed eventuali anomalie ai fini dell'identificazione degli utenti ad alto rischio.
FORCEPOINT DLP ENDPOINT	Forcepoint DLP Endpoint estende OCR, "Drip DLP" e altre funzioni di controllo del furto di dati agli endpoint di Mac OS X e Microsoft Windows, sia su rete che fuori rete. Forcepoint consente la condivisione di dati archiviati su dispositivi di storage mobili utilizzando una crittografia dei file incentrata sulle policy. Monitora gli upload sul web compreso HTTPS e altri upload nel Cloud, quali Microsoft Office 365 e Box. Integrazione completa con Outlook, Notes e altri client email utilizzando la stessa interfaccia utente delle soluzioni di Forcepoint applicate a dati, web, e-mail e endpoint.
MODULO ANALISI IMMAGINI	Per conformità con la normativa in vigore in molte parti del mondo, o semplicemente per garantire un ambiente libero da molestie, il modulo Analisi immagini offre una funzione di identificazione di immagini esplicite, quali immagini pornografiche, archiviate nella rete dell'organizzazione o in fase di trasferimento mediante e-mail o canali Web.

“Dormo meglio la notte sapendo che i nostri dati sono al sicuro con Forcepoint.”

—Ahmet Taskeser, Senior SIMM Leader, Finansbank

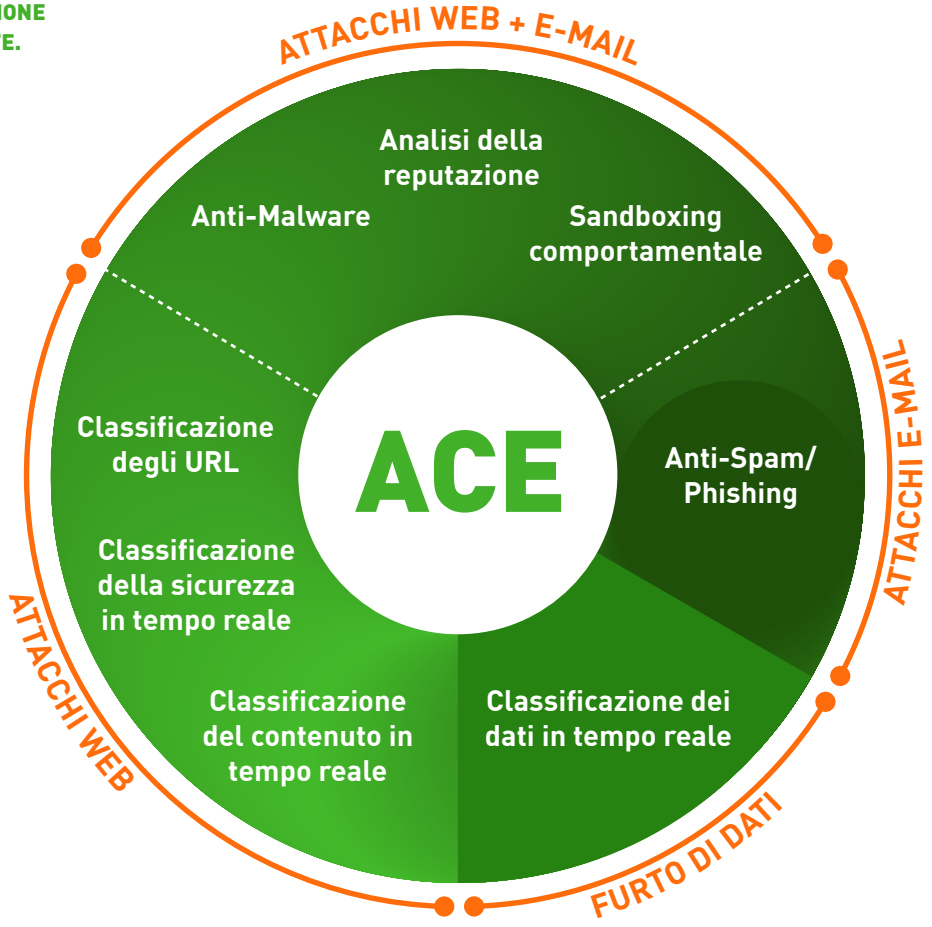
Il potere dietro le soluzioni TRITON Architecture

ACE (Advanced Classification Engine)

Forcepoint ACE offre difese contestuali online e in tempo reale per web, e-mail, dati e sicurezza mobile utilizzando un sistema di classificazione composita del rischio e analisi predittiva per garantire la sicurezza più efficace disponibile nel mercato. Minimizza inoltre l'esposizione a rischi mediante un'analisi del traffico in ingresso e in uscita e difese orientate ai dati per la protezione, leader nel settore, contro il furto di dati. Classificatori per una sicurezza in tempo reale mediante l'analisi di dati e contenuti – il risultato di anni di ricerche e sviluppo – consentono ad ACE di rilevare più minacce rispetto a qualsiasi motore anti-virus tradizionale (tale prova viene aggiornata quotidianamente al sito http://securitylabs.forcepoint.com). ACE è la difesa principale alla base di tutte le soluzioni Forcepoint TRITON Architecture ed è supportata da Forcepoint ThreatSeeker Intelligence.

SET INTEGRATO DI FUNZIONI DI VALUTAZIONE DELLE DIFESE IN 8 AREE CHIAVE DISTINTE.

- 10.000 analisi disponibili per sostenere ispezioni condotte in profondità.
- Un motore di sicurezza predittivo vede diversi passi avanti.
- Operazioni inline non soltanto monitorano le minacce, ma le **bloccano.**



Forcepoint ThreatSeeker Intelligence

Forcepoint ThreatSeeker Intelligence, gestito da Forcepoint Security Labs, offre un'intelligence di sicurezza collettiva alla base di tutti i prodotti di sicurezza Forcepoint. Integra più di 900 milioni di endpoint, compreso gli input di Facebook e, insieme alle difesa della sicurezza di Forcepoint ACE, analizza fino a 5 miliardi di richieste al giorno. Questa diffusa sensibilizzazione alle minacce della sicurezza consente a Forcepoint ThreatSeeker Intelligence di offrire aggiornamenti della sicurezza in tempo reale che bloccano minacce avanzate, malware, attacchi di phishing, adescamenti e truffe, oltre a fornire le più recenti classificazioni web. Forcepoint ThreatSeeker Intelligence è impareggiabile in dimensioni e nell'uso delle difese ACE in tempo reale per l'analisi degli input collettivi. (Con l'aggiornamento a Forcepoint Web Security, Forcepoint ThreatSeeker Intelligence ti aiuta a ridurre la tua esposizione alle minacce web e al furto di dati.)

TRITON Architecture

Grazie alla migliore sicurezza disponibile nel mercato, l'architettura Forcepoint TRITON Architecture unificata offre una protezione al punto del clic in tempo reale e le difese inline di Forcepoint ACE. Le impareggiabili difese in tempo reale di ACE sono sostenute da Forcepoint ThreatSeeker Intelligence e dalla profonda esperienza maturata nel settore dai ricercatori di Forcepoint Security Labs. La potenza dei risultati ottenuti risiede in un singola e unificata architettura con un'unica interfaccia utente e un sistema unificato di intelligence applicata alla sicurezza.

CONTACT
www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_DLP_IT] 400004IT.030117

FORCEPOINT
POWERED BY Raytheon