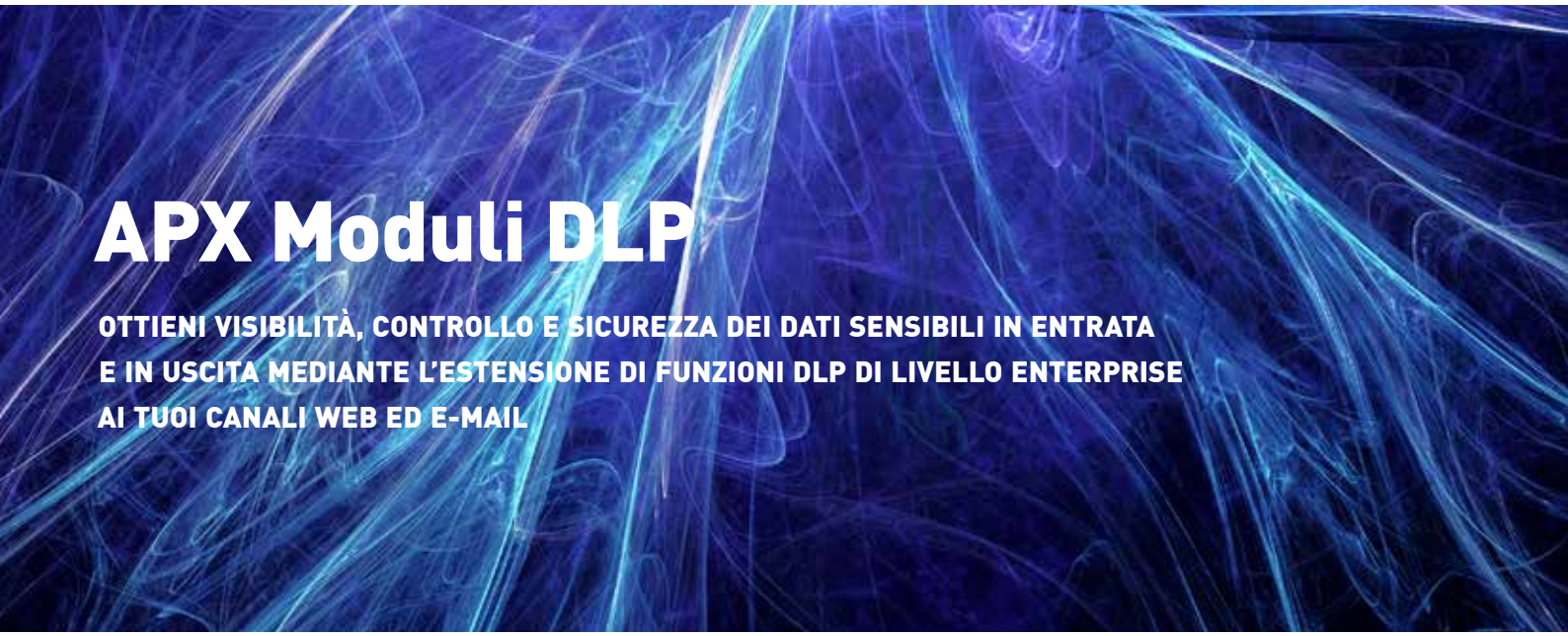
FORCEPOINT
POWERED BY Raytheon

Datasheet



APX Moduli DLP

OTTIENI VISIBILITÀ, CONTROLLO E SICUREZZA DEI DATI SENSIBILI IN ENTRATA E IN USCITA MEDIANTE L'ESTENSIONE DI FUNZIONI DLP DI LIVELLO ENTERPRISE AI TUOI CANALI WEB ED E-MAIL

Da una reputazione compromessa a multe e sanzioni normative, una violazione dei dati può avere conseguenze devastanti per la tua organizzazione. Inoltre, con le forze di lavoro che diventano sempre più mobili, è essenziale acquisire visibilità dei dati sensibili in entrata e in uscita dalla rete.

Per bloccare il furto di dati, dimostrare conformità e salvaguardare il marchio e la proprietà intellettuale, le tue difese IT devono funzionare all'esterno della tua organizzazione. Devi proteggere i tuoi dati sensibili nei canali web ed e-mail utilizzati dalla tua forza di lavoro mobile al di fuori della rete. L'estensione delle tue difese alle funzioni DLP di livello enterprise ti garantiscono una protezione applicata ai canali web ed e-mail e molto altro ancora.

PERCHÉ USARE I MODULI DLP DI WEB ED E-MAIL?

I Moduli DLP di Web e E-mail traggono vantaggio da una tecnologia estremamente accurata, leader nel settore per conformità e soddisfazione di requisiti normativi, mediante l'estensione delle funzioni DLP di livello enterprise ai canali Web ed e-mail. Offrono una visibilità in tempo reale e storica nella trasmissione di dati sensibili in qualsiasi momento. Grazie a una serie di funzioni esclusive, quali OCR (riconoscimento ottico dei caratteri) e l'identificazione di una crittografia personalizzata, Forcepoint™ porta la DLP di livello enterprise a un nuovo livello.

- Un'estesa libreria di template pronti a essere usati ti consente di impostare e implementare policy per l'identificazione e il blocco del furto dei tuoi dati cruciali.
- Grazie a facili procedure guidate, l'implementazione dei Moduli DLP di Web ed E-mail non è mai stata così semplice per il tuo personale.
- Acquisisci visibilità dei dati in ingresso e in uscita dalla rete attraverso i canali web ed e-mail.
- Previeni il "drip" (perdita lenta) e il furto lento e metodico di numeri di carte di credito o di altra documentazione, uno o due alla volta.
- Blocca le minacce interne con analisi del comportamento che identificano e segnalano i comportamenti che rappresentano un rischio per la tua organizzazione.
- OCR (Riconoscimento ottico dei caratteri) espone il testo incorporato nelle immagini per prevenire che i dati vengano occultati all'interno di schermate, foto e altre immagini.
- Con AP-EMAIL, puoi applicare policy DLP al traffico di Microsoft Office 365 per la massima protezione dei dati sensibili in combinazione con l'adozione di nuove tecnologie.
- La correzione dei dati sensibili ti consente di analizzare, bloccare, consentire l'uso, segnalare, notificare, mettere in quarantena* o crittografare* i dati sensibili quando vengono rilevati. (*soltanto per il Modulo DLP di E-mail.)

UNA SOLUZIONE CHE IMPLEMENTA E PROTEGGE I MIEI DATI PIÙ CRUCIALI DA UNA FUGA DALLA RETE TRAMITE I CANALI WEB ED E-MAIL

Grazie a un'estesa libreria di template pronti per l'uso e di policy, Forcepoint consente un rapido avvio con la simultanea protezione dei tuoi dati sensibili.

HO BISOGNO DI UNA GESTIONE ESEGUITA DAL PERSONALE ESISTENTE

L'architettura Forcepoint TRITON® offre un'integrazione completa delle funzioni di generazione di report, gestione di dati e gestione delle policy in un'unica interfaccia utente applicata alle soluzioni web, e-mail, dati, Cloud e dispositivi mobili.

IDENTIFICA E ISTRUISCI GLI UTENTI CHE PONGONO ALTI RISCHI

L'analisi del comportamento identifica e segnala coloro che presentano un rischio per l'organizzazione in base a cattive abitudini o perfino dipendenti scontenti.

NON SO QUALI DATI ESCANO DALLA MIA RETE E COME ESCONO

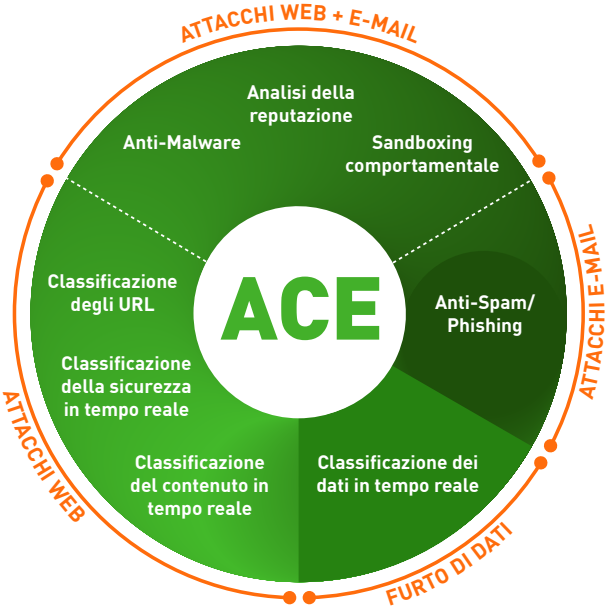
Acquisisci la visibilità necessaria dei tuoi dati in ingresso e in uscita attraverso i canali web e le e-mail con Forcepoint Web and Email DLP.

VISIBILITÀ DI DATI SENSIBILI INCORPORATI IN IMMAGINI DA FILE PRE-ESISTENTI SCANNERIZZATI

Forcepoint Optical Character Recognition (Riconoscimento ottico dei caratteri - OCR) è in grado di vedere un testo all'interno delle immagini e imporre policy per la prevenzione della fuga dalla rete di dati incorporati nelle immagini.

DEVO ACCERTARE CHE I DATI SOGGETTI A NORMATIVA NON ESCANO DALLA RETE IN PICCOLI GRUPPI

Blocca la fuga lenta e metodica dei dati con Forcepoint Drip DLP. Osservando eventi cumulativi nel corso del tempo, identifica il furto "drip" di una documentazione o di un numero di carta di credito per volta.



LA DIFFERENZA DI FORCEPOINT:

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 a ACE di rilevare più minacce rispetto a qualsiasi motore anti-virus tradizionale (dati di prova vengono aggiornati giornalmente al sito http://securitylabs.Forcepoint.com). ACE è la difesa principale alla base di tutte le soluzioni Forcepoint TRITON ed è supportata da Forcepoint ThreatSeeker Intelligence Cloud.

CONTATTO

www.forcepoint.com/contact

SU FORCEPOINT

[DATASHEET_MODULE_DLP_IT]-100007IT.011416

FORCEPOINT
TRITON® APX