proofpoint®

Proofpoint Information Protection

Architettura delle soluzioni

Proteggi i tuoi collaboratori. Difendi i tuoi dati.

Componenti della soluzione Proofpoint Information Protection

Proofpoint Information Protection si basa su Proofpoint Nexus, una suite di tecnologie ottimizzate dall'IA. Queste tecnologie sono progettate per identificare i dati sensibili, prevenire la perdita di dati e bloccare le minacce interne su diversi canali. Nexus si basa su modelli linguistici avanzati e analisi comportamentale per rilevare le potenziali condivisioni di dati sensibili da parte degli utenti, accidentali o intenzionali. Può anche identificare i comportamenti anomali, come nel caso in cui utenti non autorizzati consultano o spostano i dati.

La soluzione offre anche un controllo granulare attraverso policy automatiche che possono bloccare o correggere le attività a rischio in tempo reale. Correlando gli accessi ai dati e il loro spostamento con i comportamenti degli utenti, Nexus aiuta a proteggere i dati sensibili, come i dati personali, i dati del settore delle carte di pagamento e altri contenuti classificati a livello di email, endpoint e applicazioni cloud.

Inoltre, Nexus potenzia le funzionalità di Proofpoint Data Loss Prevention (DLP) unificando la gestione e l'analisi con l'IA avanzata. I team della sicurezza possono così monitorare l'accesso ai dati e i loro spostamenti, garantendo la conformità con le normative sulla privacy come il GDPR e la legge HIPAA. Le aziende possono quindi adattare le policy alle loro esigenze specifiche. Questo permette di avere una protezione mirata senza interrompere le operazioni aziendali legittime.

Proofpoint Information Protection include diversi prodotti e la maggior parte dei prodotti seguenti possono essere integrati nella soluzione.

Proofpoint Insider Threat Management (ITM) e Proofpoint Endpoint DLP prevengono la perdita di dati e i danni alla reputazione causati da utenti interni malintenzionati, negligenti o inconsapevoli. Proofpoint correla le attività degli utenti con gli spostamenti dei dati, consentendoti di identificare i rischi legati agli utenti, rilevare le violazioni dei dati causate dagli utenti interni e accelerare la risposta agli incidenti. Ti aiuta anche a prevenire la sottrazione dei dati tramite chiavette USB, cartelle di sincronizzazione cloud, stampe, ecc. Il suo unico agent endpoint leggero ti offre la flessibilità necessaria per monitorare gli utenti quotidiani e a rischio nonché i collaboratori ad alto rischio.

Proofpoint Cloud DLP combina funzionalità di sicurezza dei dati incentrata sulle persone (inclusa la DLP in linea) e governance delle applicazioni cloud. Protegge i dati sensibili, governa le applicazioni OAuth e ti aiuta a mantenere la tua conformità con le normative sulla privacy e sulla sicurezza dei dati. Questa soluzione CASB multimodale supporta modelli di implementazione basati su API e proxy, inclusa la DLP per i terminali personali utilizzati sul posto di lavoro (BYOD).

Proofpoint Email DLP contribuisce a prevenire la perdita di dati sensibili attraverso l'email. Ti aiuta anche a rispettare i requisiti normativi come lo standard PCI, il GDPR, i codici PII e SOX, la legge HIPAA e diverse leggi di protezione dei dati personali, grazie a policy pronte all'uso che si allineano con questi standard. Puoi anche creare dizionari personalizzati, inclusa la classificazione ottimizzata dall'IA, per identificare e proteggere i dati unici per la tua azienda. Proofpoint Email DLP è facile da implementare. Puoi impostarlo come parte di un sistema di sicurezza dell'email esistente, o integrarlo in un programma DLP aziendale.

Proofpoint Adaptive Email DLP si basa sull'IA comportamentale per identificare i comportamenti consueti dei tuoi collaboratori in merito all'invio delle email, le loro relazioni di fiducia e il modo in cui comunicano i dati sensibili. Quindi analizza ogni email per rilevare i comportamenti anomali e segnala agli amministratori potenziali perdite di dati. Avvisa gli utenti in tempo reale e previene la perdita di dati sensibili attraverso l'email. Attualmente, Proofpoint Adaptive Email DLP non può essere integrato con la nostra piattaforma Proofpoint Information Protection e non verrà trattato in questo documento.

Proofpoint Information Protection è totalmente in modalità SaaS. La sua applicazione backend Analytics fornisce funzionalità unificate di gestione e reportistica, tra cui visualizzazioni, rilevamento delle anomalie, interrogazioni di big data, revisioni assistite da computer e gestione dei casi. Offre anche dashboard per monitorare il tuo livello di sicurezza, le tendenze della sicurezza e i rischi di non conformità in tempo reale. La soluzione permette di generare report che includono indicatori rivolti alla dirigenza.

Architettura logica di Proofpoint Enterprise DLP

La soluzione Proofpoint Enterprise DLP fornisce agli amministratori della sicurezza strumenti per proteggere i dati sensibili e analizzare in modo efficiente gli incidenti negli ambienti, riducendo in modo significativo i rischi di violazione dei dati a cui la tua azienda è esposta.

Dal punto di vista della gestione degli incidenti, l'obiettivo primario della soluzione DLP è fornire una console unica per ridurre il tempo dedicato all'analisi dei log, velocizzare le indagini e la correzione degli incidenti e, in generale, per accrescere l'efficacia dei team.

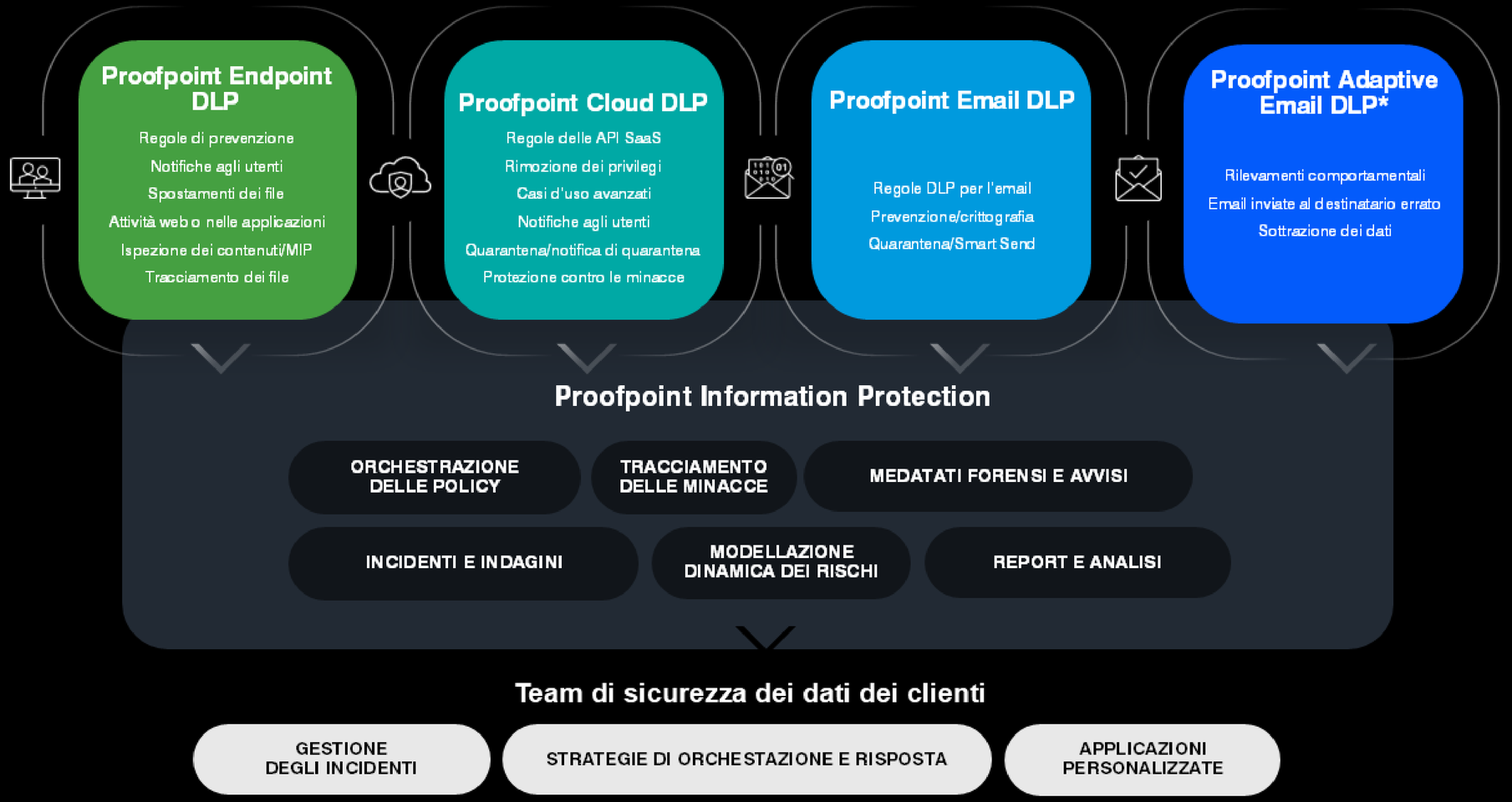
Diversi componenti di rilevamento separati collaborano in una soluzione integrata. Un'architettura della soluzione descrive la configurazione, le regole e le policy per l'implementazione del prodotto. Inoltre, definisce chiaramente i rischi per l'azienda e i fattori trainanti del programma DLP.

Possono essere quindi create regole specifiche per l'azienda per fornire visibilità e controllo su attività designate che prevedono informazioni aziendali. Possono essere create regole DLP per avvisare un analista degli incidenti di sicurezza o orchestrare la correzione automatica intracanale. Regole granulari offrono funzionalità di risposta flessibili per non bloccare attività aziendali legittime.

Inoltre, attività ad alto rischio e incidenti importanti possono essere facilmente identificati, raccolti, esportati e condivisi con i team responsabili. Ciò riduce il carico di lavoro e i costi associati alla gestione degli incidenti e permette ai team di proteggere meglio l'azienda e i suoi utenti dalle conseguenze negative della perdita di dati.

Architettura di riferimento di Proofpoint Enterprise DLP

Ecco come si presenta il flusso di attività e la comunicazione tra i componenti della soluzione DLP:

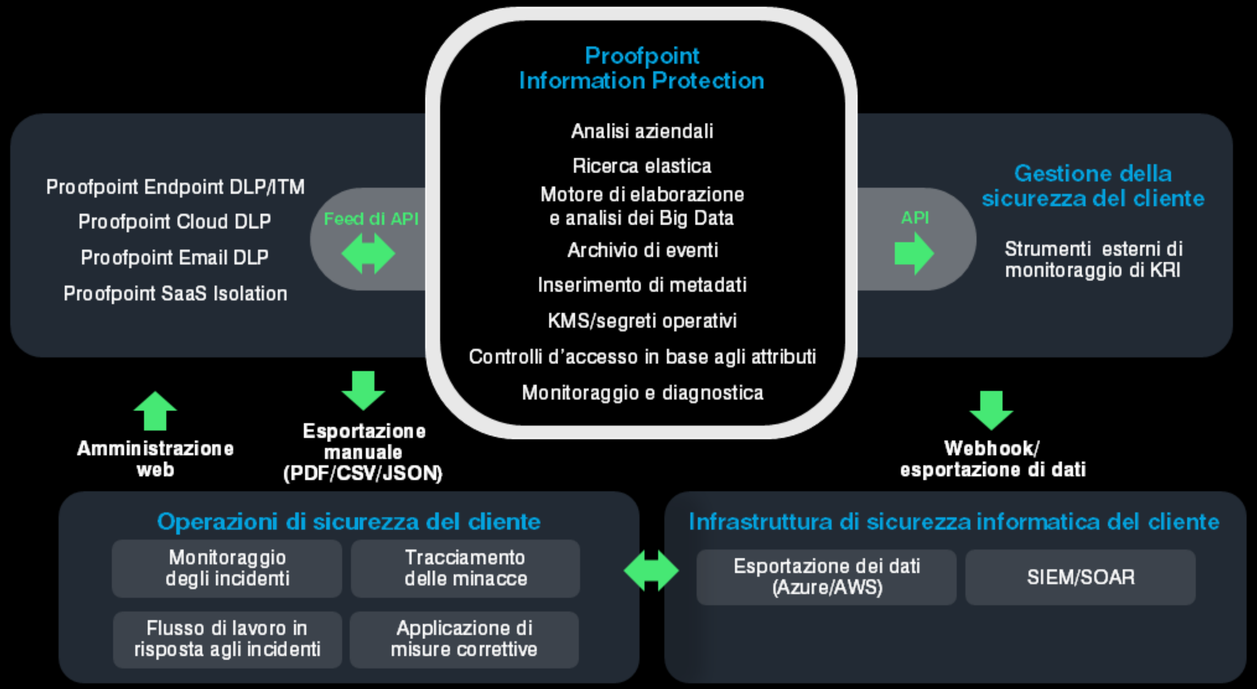


*Integrazioni future

Documento N.: 1207-005-05-01

Analisi unificata per Proofpoint Information Protection

Architettura di analisi unificata per Proofpoint Information Protection a livello di endpoint, cloud e email.



Analisi unificata per la gestione degli avvisi, delle indagini e della risposta

La gestione degli avvisi unificata fornisce analisi dei dati e report per tutti gli eventi raccolti dalla soluzione. Ti consente inoltre di gestire i flussi di lavoro degli avvisi. Questa funzionalità di analisi dei dati supporta molti casi d'uso avanzati come le esplorazioni nell'ambito del monitoraggio delle minacce, il rilevamento delle anomalie e la classificazione degli avvisi per priorità assistita da computer.

L'applicazione Analytics ti permette di creare regole di rilevamento specifiche, che, a loro volta, generano avvisi che un analista degli incidenti di sicurezza può classificare per priorità. In caso di violazione, un'email o un evento di webhook in uscita contenente i dettagli dell'avviso viene inviato a un'applicazione ricevente terza, come una soluzione SIEM/SOAR o un sistema di messaggistica istantanea.

Gli strumenti SIEM di Splunk e altri fornitori possono essere integrati con Proofpoint Information Protection per fornire una vista unificata delle minacce interne, degli spostamenti laterali e delle sottrazioni di dati. Ciò ti aiuta a identificare rapidamente gli utenti coinvolti e correlare le informazioni rispetto a altre fonti di eventi.

Tramite integrazioni, la nostra piattaforma può anche segnalare a ServiceNow le sottrazioni di dati o le violazioni della conformità. ServiceNow può quindi avvisare i suoi clienti e creare altri ticket o flussi di lavoro in base agli avvisi. Un'integrazione con la DLP ServiceNow velocizza le indagini e la risposta.

Accesso alla piattaforma e controlli della privacy

I collaboratori di Proofpoint non hanno in alcun modo accesso ai tuoi dati, a meno che il tuo team non li condivida con loro. Se concedi loro l'accesso, i membri del personale di Proofpoint o del tuo team possono utilizzare il Proofpoint User Center per collegarsi al sistema. In alternativa, l'accesso può essere assegnato tramite un profilo, che è essenzialmente un utente temporaneo.

Gli avvisi devono essere configurati in base all'uso di un account di amministrazione con privilegi elevati. Per garantire la sicurezza dell'account, è necessario cambiare la password associata. Può anche essere tenuta in deposito o suddivisa tra le parti responsabili.

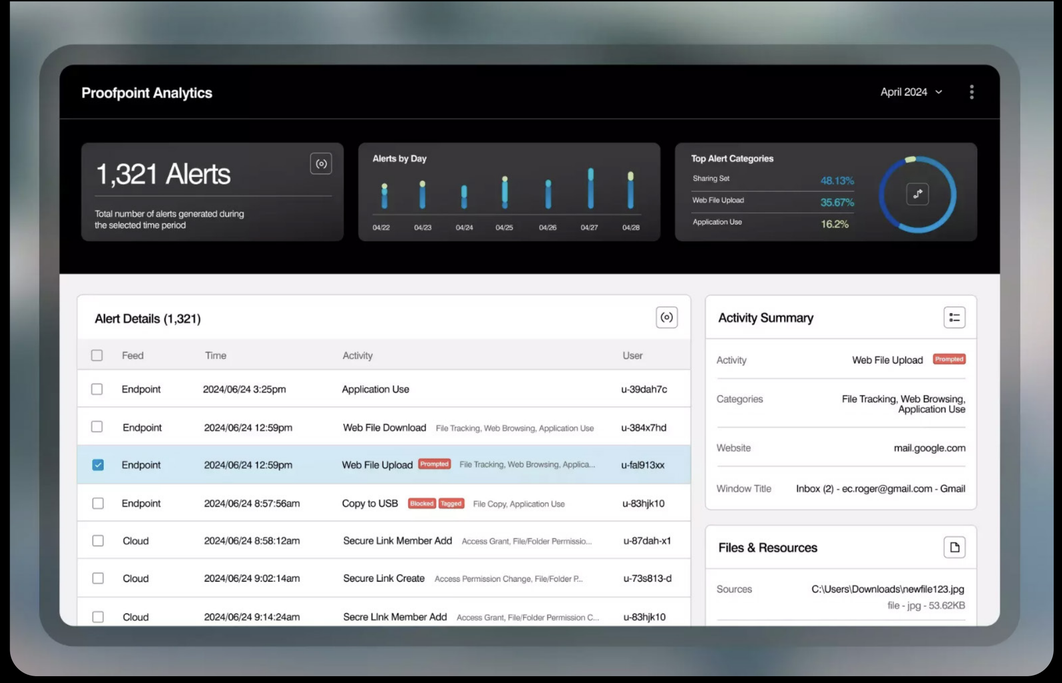
Si raccomanda vivamente di utilizzare il protocollo SAML o OAuth2.0 per integrare i metodi di autenticazione cloud, come l'autenticazione unica (SSO) e l'autenticazione a più fattori (MFA). Hai anche la possibilità di collegare diversi fornitori di identità.

Per farlo, devi accedere a "Administration > Account Settings" (Amministrazione > Parametri dell'account) nella piattaforma Proofpoint Information Protection per configurare un fornitore di identità in base ai parametri richiesti. Dovrai anche configurare il tuo fornitore di identità affinché si colleghi alla piattaforma Proofpoint Information Protection.

L'account amministratore ha un accesso totale e non anonimizzato a tutti i parametri e i dati nella piattaforma. Le credenziali d'accesso devono quindi essere protette e trattate come estremamente riservate. Gli account amministratore locali aggiuntivi possono essere creati durante i test di prodotto nella sezione "Administration > Account Settings" (Amministrazione > Gestione degli utenti). A ogni account possono essere assegnate le sue policy di accesso come necessario. Tuttavia, nella maggior parte dei casi, l'aggiunta di altri amministratori richiederà la limitazione del loro controllo e del loro accesso amministrativo.

Proofpoint Information Protection si basa su principi della privacy-by-design. Solo le persone che ne hanno davvero bisogno possono accedere ai dati sensibili e alle informazioni di identificazione degli utenti. Proofpoint dispone di data center regionali negli Stati Uniti, in Europa, Australia, Canada (fine 2024) e Giappone (solo dati degli endpoint). Ciò ti consente di separare facilmente i dati a livello geografico. Per esempio, un raggruppamento negli Stati Uniti può gestire i dati negli Stati Uniti, che vengono inviati al data center degli Stati Uniti. Policy di accesso granulare permettono al tuo amministratore di assegnare un accesso in modo che un analista della sicurezza basato negli Stati Uniti possa vedere solo i dati degli Stati Uniti.

Con Proofpoint Information Protection, gli amministratori di sistema possono anche configurare i dati forensi (dati di identificazione personale, informazioni di identificazione sanitaria, dati del settore delle carte di pagamento) che desiderano mascherare nella console e nascondere l'identità di un utente per eliminare i bias da parte degli analisti. Puoi rendere anonimo il nome utente, il nome dell'host, l'indirizzo IP, le informazioni sull'ubicazione e i nomi dei file. Quando l'identità di un utente deve essere conosciuta più avanti nel corso di un'indagine, l'analista di sicurezza può richiedere la de-anonimizzazione dei dati, che può essere concessa dall'amministratore.



Accesso alla console web

Amministratori e analisti possono collegarsi alla piattaforma utilizzando un browser compatibile. Possono gestire policy e regole, esaminare gli avvisi, correggere direttamente gli incidenti, analizzare i set di dati raccolti e consultare i report in base alle attività degli utenti acquisite.

Per gestire sotto-entità distinte, molte aziende possono accedere a diversi sub-locatari sulla piattaforme Proofpoint.

Notifiche della piattaforma

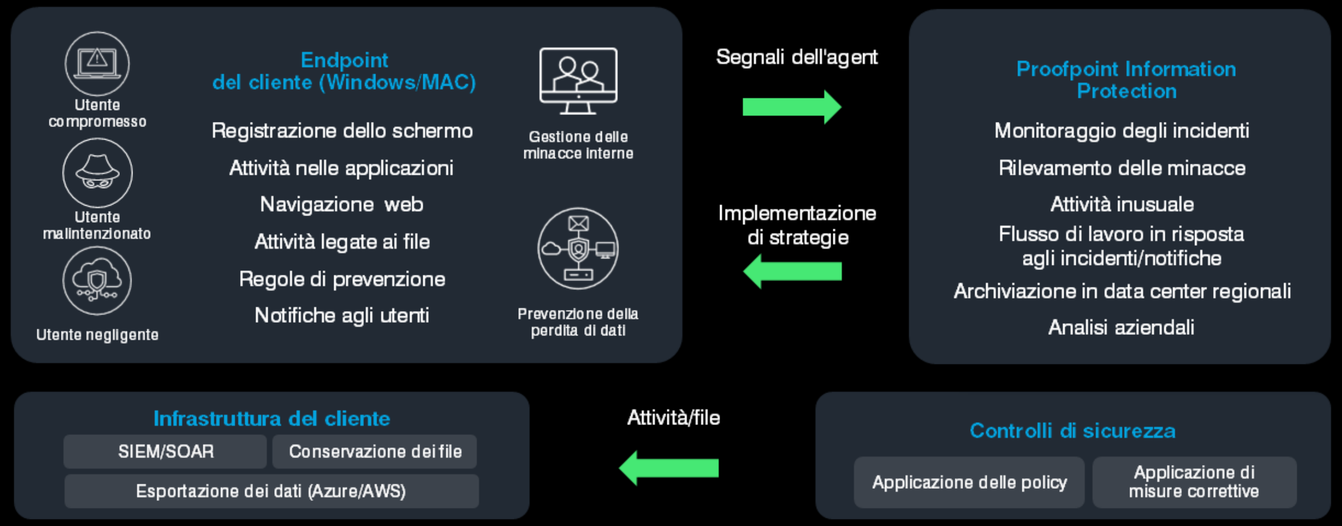
Gli avvisi possono essere monitorati e elaborati nella piattaforma Proofpoint. Tali operazioni possono essere effettuate anche esternamente in conformità con le tue procedure interne di gestione degli incidenti. Dovrai quindi identificare gli indirizzi email che riceveranno gli avvisi generati dalla piattaforma Proofpoint Information Protection. Anche i sistemi esterni (SIEM, SOAR, ITSM) possono essere configurati per ricevere gli avvisi.

Applicazioni esterne

Le applicazioni esterne possono accedere alla piattaforma Proofpoint tramite API REST.

Architettura di riferimento di Proofpoint Endpoint DLP e Proofpoint ITM

L'agent singolo per la DLP e delle minacce interne (ITM) raccoglie e carica i dati sulla piattaforma applicando anche le policy DLP.



CONFIGURAZIONE dell'agent endpoint DLP/ITM

L'agent Proofpoint Endpoint DLP viene installato sugli endpoint dei clienti che operano con versioni compatibili di Windows o macOS. Per installare l'agent in produzione, devi utilizzare metodi senza sorveglianza e i tuoi strumenti di installazione remota del software standard.

Non appena viene distribuito, l'agent registra i metadati che descrivono le attività dell'utente. Non richiede regole esplicite. I metadati vengono caricati e elaborati in modo sicuro dalla piattaforma Proofpoint Information Protection. Per amministrare e configurare l'agent, utilizza l'applicazione "Administration > Endpoints" (Amministrazione > Endpoint) della piattaforma.

Gli agent endpoint di Proofpoint possono essere implementati in modalità silenziosa. Ciascuno di essi viene eseguito nella memoria dell'utente con un consumo minimo di risorse e può aggiornarsi automaticamente. Dopo l'installazione o l'aggiornamento, non è richiesto il riavvio del sistema. Gli agent non entrano in conflitto con la sicurezza degli endpoint esistenti e non interrompono il funzionamento di altre applicazioni né causano delle prestazioni.

Gli agent installati e il server ITM comunicano in modo asincrono tramite il protocollo HTTP. Gli agent DLP utilizzano la crittografia TLS per comunicare con i servizi cloud di Proofpoint. I requisiti del firewall per la connettività sono elencati nel nostro portale della documentazione online.

Gli agent che devono collegarsi attraverso un proxy dinamico utilizzeranno i parametri del proxy definiti a livello di sistema operativo. Il sistema operativo deve essere configurato in modo da utilizzare un proxy dinamico per le applicazioni che operano sotto l'account di sistema (non l'account utente). È inoltre possibile utilizzare un proxy statico. Questo parametro viene configurato al momento dell'installazione degli agent.

Alcuni software antivirus e EDR (Extended Detection and Response) vengono eseguiti su richiesta e analizzano i file eseguibili e i processi di conservazione o bloccano le comunicazioni automaticamente. Per assicurare la stabilità delle funzionalità, devi escludere i nostri processi dall'ispezione da parte di altri strumenti di sicurezza. Non avrai bisogno di inserire applicazioni specifiche nell'elenco di autorizzazione del nostro strumento, poiché è poco probabile che il nostro approccio leggero interferisca con le azioni di un agent endpoint in modalità kernel.

Componenti dell'agent endpoint Windows per l'inserimento nell'elenco di autorizzazione
Per inserire nell'elenco di autorizzazione i nostri file affinché siano esclusi dall'ispezione dei sistemi EDR e antivirus, consulta **questa guida.**

NOTA: per visualizzare le notifiche o acquisire le schermate su macOS, devi anche assicurarti che i parametri della privacy siano concessi ai nostri processi distribuendo il file di configurazione mobile. Questo processo è dettagliato nella nostra documentazione online.

L'agent endpoint di Proofpoint supporta due tipi di proxy. Nel caso di un proxy dinamico, utilizza un file di configurazione automatica del proxy (PAC) a livello di sistema operativo. Nel caso di un proxy statico, fornisci il nome dell'host e la porta al momento dell'installazione. Per impostare le credenziali d'accesso di default che l'agent utilizzerà, compila i campi Dominio, Nome utente e/o Password al momento dell'installazione.

Aggiornamento dell'agent
Come piattaforma SaaS, Proofpoint può integrare rapidamente delle nuove funzionalità nell'agent. Proofpoint fornisce anche una versione con supporto a lungo termine (LTS) dell'agent per i clienti che non sono in grado di supportare il nostro programma di rilascio. Tuttavia, consigliamo in genere di installare l'ultima versione dell'agent supportato.

Consigliamo l'utilizzo del servizio di aggiornamento automatico per mantenere gli agent aggiornati in base a una policy di aggiornamento preconfigurata. Quando un amministratore decide di aggiornare l'agent, deve solo modificare o creare una policy che definisce la versione di destinazione e le condizioni per l'applicazione dell'aggiornamento. Il programma di aggioramento dell'agent viene elaborato sugli endpoint e quindi assicura che le versioni corrette vengano scaricate e installate automaticamente.

Certificato root
Gli endpoint installati devono avere un certificato root valido. Proofpoint firma l'agent con un certificato root valido per assicurare che il cliente sappia che proviene da Proofpoint. Questo certificato dipende da un certificato root valido e ha una data di scadenza annuale.

Monitoraggio dell'integrità dell'agent
Informazioni sull'integrità dell'agent, come gli errori e il marcatore temporale delle ultime registrazioni, sono visibili "Administration > Endpoints > Endpoint Catalog" (Amministrazione > Endpoint > Catalogo degli endpoint)". L'agent Windows ha capacità di auto-riparazione e include un servizio cloud di sorveglianza IT che riavvia l'agent in caso di disattivazione o arresto di quest'ultimo. Viene avviato anche il processo di registrazione dell'agent Mac, che riavvia l'agent qualora quest'ultimo venga disattivato o interrotto.

Rafforzamento dell'agent
La configurazione dell'agent e i file di log sugli endpoint possono essere interamente crittografati. Durante l'installazione, può essere applicato un rafforzamento aggiuntivo, per esempio l'applicazione di una chiave di sicurezza per impedire la disinstallazione dell'agent o l'attribuzione di un nuovo nome ai suoi processi.

Configurazione del raggruppamento degli endpoint
I raggruppamenti degli agent separano gli agent in funzione della posizione di archiviazione regionale e dei periodi di conservazione dei dati.

Regole di prevenzione a livello degli endpoint vengono distribuite attraverso policy di agent differenziate. Eseguono azioni come la visualizzazione di avvisi o il blocco dell'utente. In contemporanea, l'agent annota sul registro i segnali dei metadati relativi alle attività dell'utente legate alle applicazioni. Questi log vengono inviati al motore di analisi di Proofpoint per essere elaborati. Le schermate sono opzionali.

I dati elaborati vengono archiviati nel data center AWS regionale preferito (al momento Stati Uniti, Europa, Asia-Pacifico, Giappone e Canada) in base al parametro di raggruppamento degli agent selezionati.

Parametri delle policy degli agent
Le policy degli agent definiscono il contenuto acquisito dall'agent Proofpoint. e vengono attribuite a raggruppamenti di agent. Puoi quindi configurare i parametri e applicarli contemporaneamente agli endpoint di diversi raggruppamenti.

Puoi assegna diverse policy degli agent a un raggruppamento di agent. In questo caso, puoi classificarli nell'ordine che preferisci per definire in modo più preciso i parametri applicati ai diversi agent. Questo ordine stabilisce i parametri che vengono attivati conformemente alla policy dell'agent.

Prevenzione a livello degli endpoint e notifiche agli utenti

La modifica dei comportamenti degli utenti per ridurre il rischio di violazione dei dati è un componente essenziale di qualsiasi programma DLP o di gestione dei rischi interni efficace. Quando le regole DLP vengono implementate sugli endpoint gestiti, possono essere utilizzate per bloccare le violazioni alle policy e informarne gli utenti. Ciò influenza il loro comportamento e riduce anche il rischio di violazione dei dati.

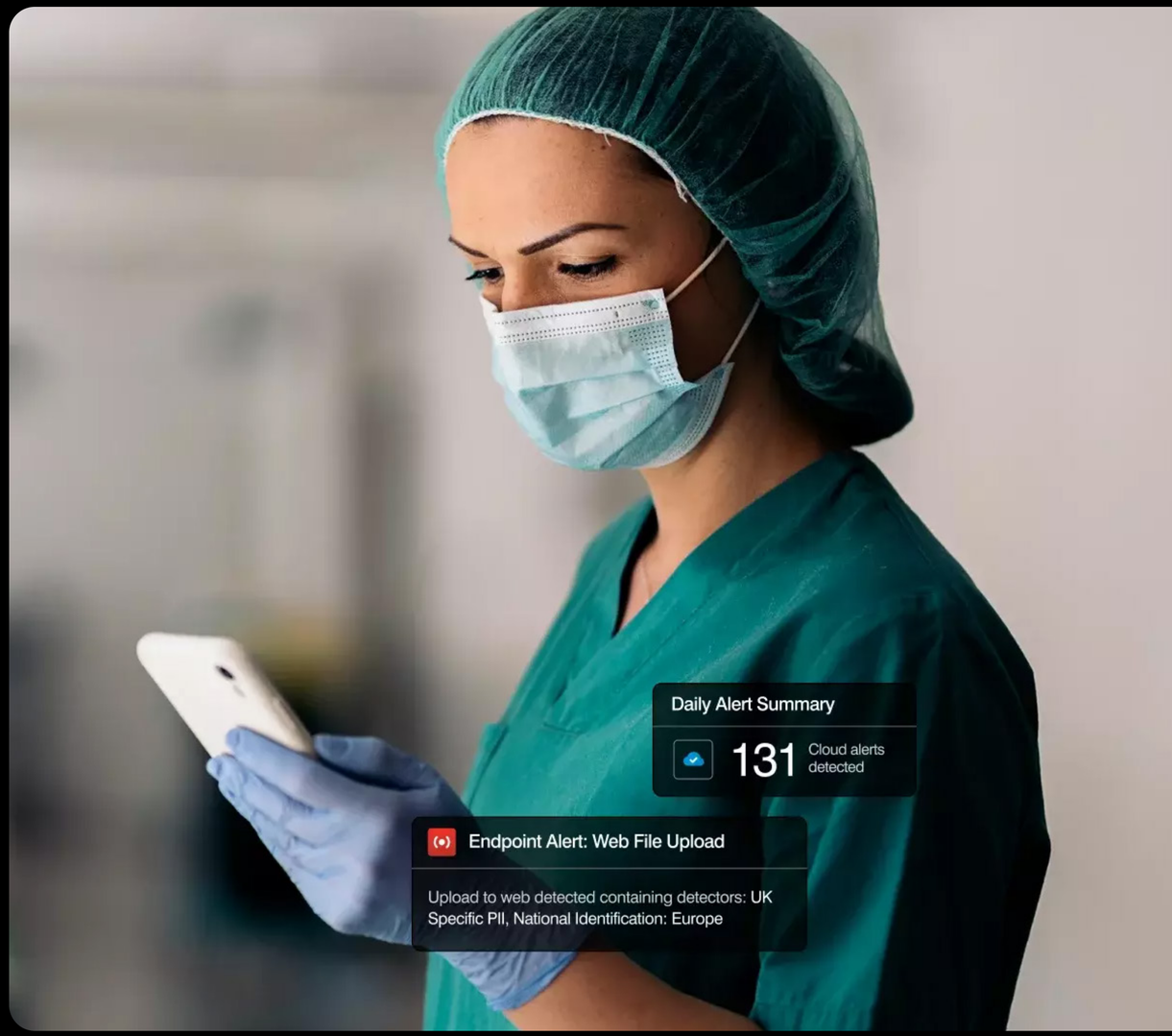
Le regole di prevenzione sono concepite per modificare i comportamenti degli utenti nel momento in cui informazioni aziendali sensibili vengono esfiltrate. Inizialmente, un approccio comune consiste nel sorvegliare cosa fanno gli utenti grazie a metadati dell'attività visibili negli avvisi o nelle esplorazioni. Quando i team esaminano gli avvisi, possono utilizzarli per adattare le regole in modo che siano allineate con le priorità e i processi di rilevamento degli incidenti dell'azienda.

Una volta che il processo è maturo, è possibile implementare delle regole. A questo punto, quando gli utenti non rispettano le policy, gli verrà impedito di compiere un'azione e ne saranno informati tramite un messaggio di blocco. Per continuare la loro attività, verranno invitati a selezionare una giustificazione predefinita o personalizzata.

Le notifiche all'utente vengono solitamente personalizzate con un messaggio che descrive la policy infranta. Includono anche il logo ufficiale dell'azienda e un link alla pagina web che dettaglia le sue policy di sicurezza. La dimensione dell'immagine importata per il logo dell'azienda deve essere inferiore a 56 kB (tipo MIME image/*).

Gli utenti scoprono le fasi da seguire quando un'attività viene bloccata o come formulare un reclamo relativo all'interruzione. È inoltre una buona idea includere un link verso la pagina intranet dedicata alla sicurezza dell'azienda che spiega la necessità di un tale programma DLP.

Le regole di rilevamento generano avvisi nella nostra applicazione Analytics, dove uno specialista in risposta agli incidenti può gestirle. Esaminano i metadati raccolti, che vengono generati da alcune attività degli utenti sugli endpoint. I metadati vengono registrati dall'agent in base ai parametri della policy dell'agent, come la frequenza e la risoluzione delle schermate e vengono gestiti nella console di amministrazione.



Configurazione di Proofpoint Cloud DLP

Proofpoint Cloud DLP supporta un'architettura senza agent. Utilizza API cloud per proteggere le principali applicazioni cloud. Offre anche una DLP in linea per i dispositivi BYOD, utilizzando l'isolamento del browser dopo che un utente si autentica per accedere a un'applicazione cloud.

Proofpoint Cloud DLP si collega ai principali servizi cloud di un'azienda e alle sue applicazioni SaaS/IaaS approvate tramite le API corrispondenti. Potrai così godere di funzionalità bidirezionali, tra cui la correzione di incidenti di sicurezza cloud, in tempo quasi reale.

Proofpoint Cloud DLP è estremamente potente e assicura la correzione con lo stesso stack dei rilevatori DLP utilizzato da Proofpoint Endpoint DLP.

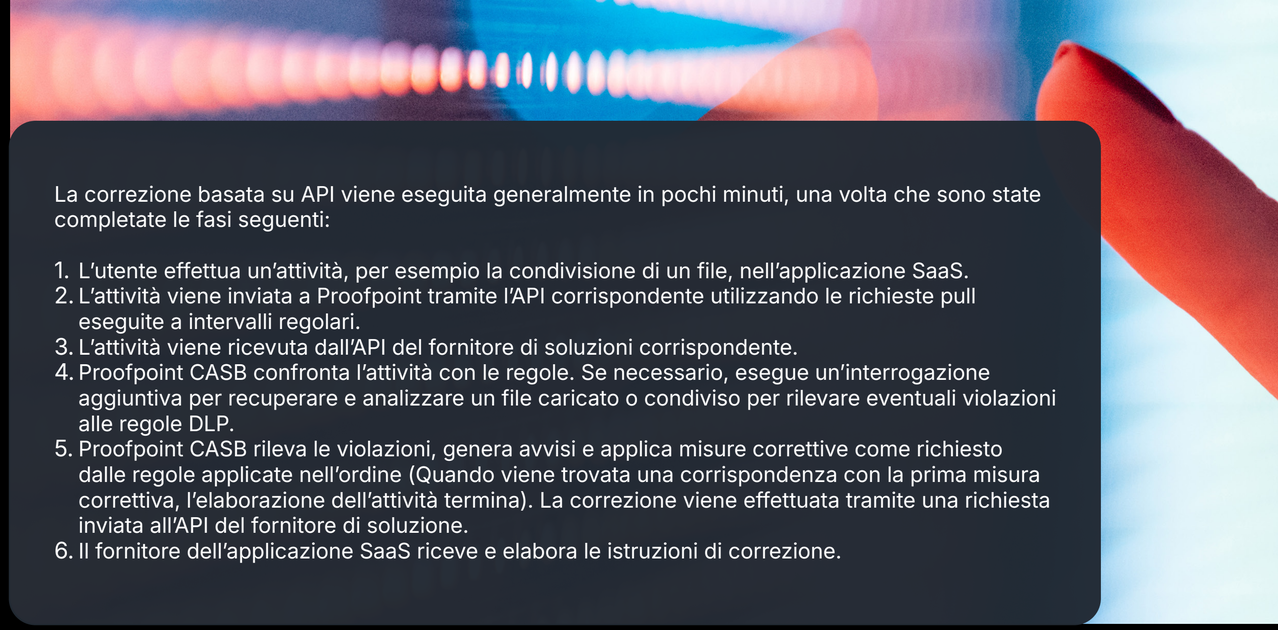
Proofpoint CASB Adaptive Access Controls estende le funzionalità di Proofpoint Cloud DLP a un'ampia gamma di casi d'uso avanzati in tempo reale, come la ricognizione e il blocco dei dispositivi non gestiti nonché l'accesso da posizioni a alto rischio tramite la nostra integrazione SAML/OIDC con fornitori di identità cloud.

Puoi anche ottenere un controllo DLP ancor più granulare sui caricamenti e i download dei file tramite un navigatore utilizzando un'integrazione con Proofpoint SaaS Isolation e senza agent. La soluzione è quindi adatta alla DLP sui dispositivi BYOD. I connettori API Okta per Proofpoint semplificano le integrazioni SAML. Possiamo applicare automaticamente controlli adattivi per le applicazioni federate per Okta.

Come passo ulteriore, i servizi IaaS come Azure e AWS possono essere configurati per il monitoraggio DLP. Proofpoint fattura queste API separatamente.

All'inizio, le API dei fornitori per alcune delle tue applicazioni cloud verranno connesse a Proofpoint Cloud DLP a fini di monitoraggio della sicurezza.

Puoi creare regole specifiche in Proofpoint Cloud DLP per identificare e correggere le violazioni delle policy DLP aziendali nei servizi cloud. Puoi anche applicare regole di governance automatizzate alle applicazioni OAuth di terze parti, che mantengono l'accesso di sistemi e dati ai tuoi principali servizi SaaS e aziendali, come Microsoft 365 e Google Workspace.



La correzione basata su API viene eseguita generalmente in pochi minuti, una volta che sono state completate le fasi seguenti:

1. L'utente effettua un'attività, per esempio la condivisione di un file, nell'applicazione SaaS.
2. L'attività viene inviata a Proofpoint tramite l'API corrispondente utilizzando le richieste pull eseguite a intervalli regolari.
3. L'attività viene ricevuta dall'API del fornitore di soluzioni corrispondente.
4. Proofpoint CASB confronta l'attività con le regole. Se necessario, esegue un'interrogazione aggiuntiva per recuperare e analizzare un file caricato o condiviso per rilevare eventuali violazioni alle regole DLP.
5. Proofpoint CASB rileva le violazioni, genera avvisi e applica misure correttive come richiesto dalle regole applicate nell'ordine (Quando viene trovata una corrispondenza con la prima misura correttiva, l'elaborazione dell'attività termina). La correzione viene effettuata tramite una richiesta inviata all'API del fornitore di soluzione.
6. Il fornitore dell'applicazione SaaS riceve e elabora le istruzioni di correzione.

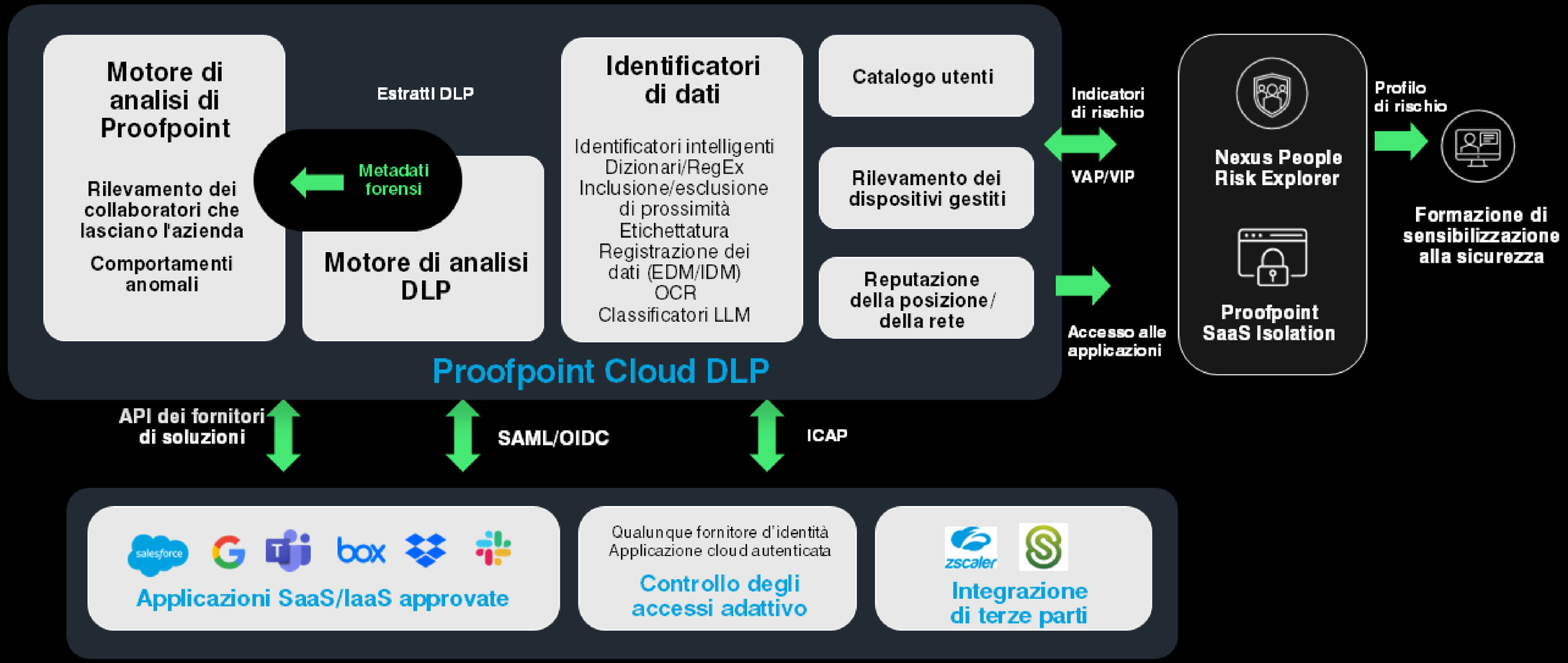
Proofpoint CASB Adaptive Access Controls permette il controllo online delle applicazioni supportate senza agent. Attraverso l'integrazione SAML 2.0 o OIDC con il tuo fornitore di identità, possiamo applicare una protezione aggiuntiva a qualsiasi applicazione autenticata utilizzando Proofpoint Cloud DLP.

Per configurare Proofpoint CASB Adaptive Access Controls, le richieste di connessione utente devono essere autenticate dal fornitore dell'identità. Possiamo quindi applicare una regola che autorizza l'accesso alle applicazioni cloud aziendali approvate, ma solo sotto certe condizioni.

Le policy possono essere basate su parametri come l'accesso di un utente all'applicazione SaaS da un dispositivo non gestito, al di fuori dell'intervallo di uscita di una rete di origine della rete, da un luogo a rischio o altri fattori ad alto rischio. Puoi disporre di un controllo ancor più granulare sull'accesso alle applicazioni cloud tramite un browser utilizzando un'integrazione aggiuntiva con Proofpoint SaaS Isolation. L'integrazione con il nostro stack DLP sarà così effettuata in tempo reale, senza dover utilizzare un agent.

Per unificare ulteriormente la DLP e offrire visibilità sulla perdita di dati su più canali, Proofpoint supporta anche l'integrazione ICAP con Zscaler e Citrix ShareFile. Per farlo, configura il client ICAP della tua applicazione di terze parti reindirizzando il suo traffico verso il nostro servizio DLP dopo aver configurato il tuo set di rilevatori DLP per quel canale nella nostra piattaforma.

Architettura di riferimento di Proofpoint Cloud DLP



Configurazione di Proofpoint Email DLP

Proofpoint Email DLP utilizza un gateway email in linea fornito da Proofpoint per elaborare le email in uscita. Questo gateway è integrato nella tua architettura email in uscita.

Proofpoint ti suggerirà come configurare la tua infrastruttura e i tuoi sistemi in funzione della tua architettura email esistente, sia che tu stia testando il gateway email in uscita di Proofpoint Email DLP o lo stia mettendo in produzione.

Se utilizzi già Proofpoint per il tuo gateway email in uscita, Proofpoint Email DLP dovrà semplicemente essere attivato direttamente sul tuo gateway email Proofpoint esistente acquistando una licenza per il modulo di conformità alle normative. Non verrà apportata alcuna modifica al tuo flusso di email. Non c'è nessuna conseguenza per gli standard SPF e DMARC, né per il "riscaldamento" degli indirizzi IP (IP Warmup).

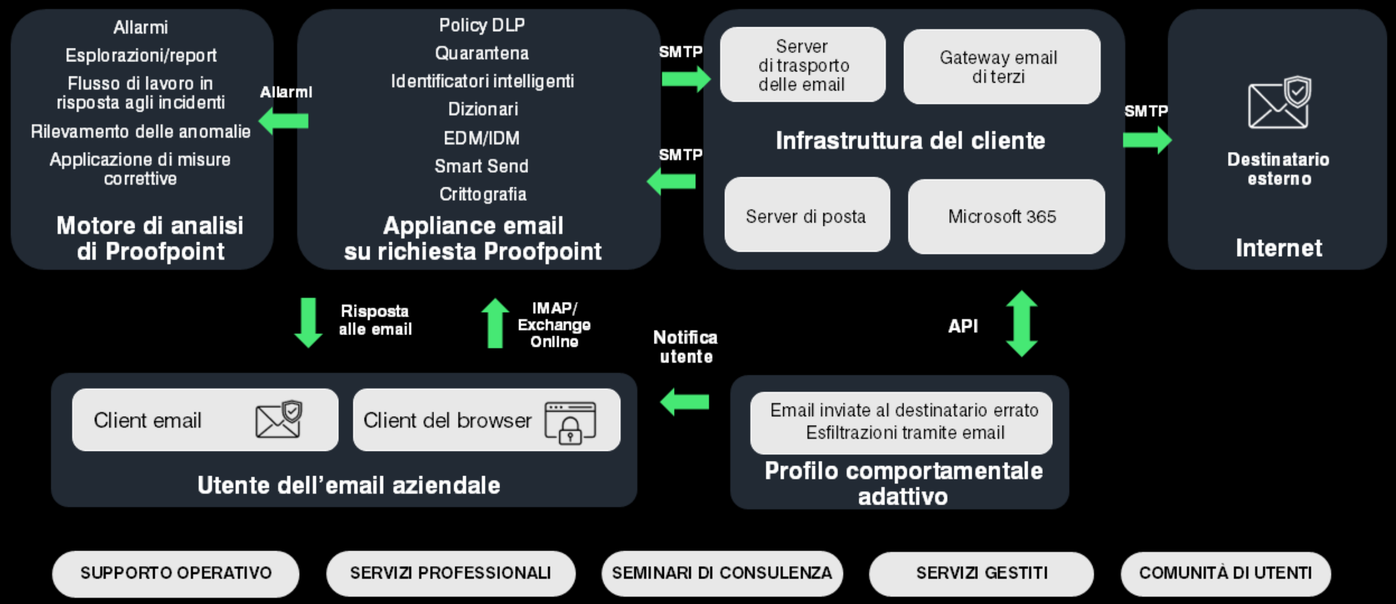
Una volta attivato Proofpoint Email DLP, puoi valutare l'intera gamma di funzionalità DLP, inclusa la creazione di report, l'implementazione, le notifiche utente e le interazioni.

Se non utilizzi Proofpoint come ultimo tratto del tuo flusso di elaborazione delle email, il gateway email cloud Proofpoint verrà integrato nella tua infrastruttura email in uscita come tratto SMTP aggiuntivo. Idealmente, dovrebbe essere inserito prima di un gateway email esistente per evitare modifiche aggiuntive all'infrastruttura.

Una volta che il servizio email in uscita è stato integrato, puoi utilizzare l'intera gamma di funzionalità DLP, inclusa la creazione di report, l'implementazione, le notifiche utente e le interazioni.

Architettura di riferimento di Proofpoint Email DLP

Interconnessione dei componenti di Proofpoint Email DLP e comunicazione con un utente dell'email aziendale



Documento N.: 1207-005-05-01

Disaster recovery

Proofpoint gestisce le attività di disaster recovery internamente alla sua piattaforma. In caso di interruzione di uno dei suoi servizi, Proofpoint implementerà il suo piano di disaster recovery, che include la fornitura di report periodici sulla situazione. Questi report includono una breve descrizione dell'evento, l'impatto sui clienti e una stima del ripristino della normale attività. Il programma di continuità aziendale documentato di Proofpoint descrive come i processi aziendali vengono ripristinati. Il piano viene riesaminato almeno una volta all'anno, e viene eseguita una simulazione su base annuale. I dettagli possono essere richiesti come parte di un esame SOC 2 Type 1 tramite Proofpoint.

Se i servizi cloud Proofpoint non sono raggiungibili sulla rete, l'applicazione delle regole DLP esistenti non sarà interessata. Tutte le regole DLP vengono applicate direttamente all'agent attraverso le policy delle macchine. La loro applicazione non richiede alcuna comunicazione con un server.

Se in questo lasso di tempo vengono apportate modifiche a delle regole di prevenzione dall'amministratore, le macchine riceveranno le modifiche solo quando avranno stabilito una connessione con i servizi Proofpoint. Questa attività si verifica ogni 10 minuti.

In termini di rilevamento, una perdita di connettività fa sì che l'agent memorizzi gli eventi selezionati definiti nel raggruppamento di agent e nei parametri della policy dell'agent, gestiti nella console di amministrazione. Quando il dispositivo avrà ristabilito la comunicazione con l'applicazione, verranno caricati i metadati per gli eventi selezionati.

Livello di riservatezza dei dati

Puoi applicare controlli di sicurezza in modo coerente e globale creando regole DLP basate su identificatori di dati sensibili.

Il livello di riservatezza dei dati viene definito dalla portata delle conseguenze negative che la divulgazione di un gruppo di dati avrebbe su un'azienda. Tali conseguenze includono la perdita di fiducia da parte dei clienti e dei suoi azionisti, perdite finanziarie dirette e ammende imposte dall'autorità di regolamentazione.

Rilevatori DLP per Proofpoint Cloud DLP e Proofpoint Endpoint DLP
I rilevatori DLP Proofpoint qui identificati si applicano esclusivamente alle regole Proofpoint Cloud DLP e Proofpoint Endpoint DLP. Se desideri utilizzare l'analisi dei contenuti per Proofpoint Endpoint DLP, devi seguire questi passaggi:

- Il componente di analisi dei contenuti deve essere attivato durante l'installazione dell'agent endpoint. In alternativa, quest'ultimo deve essere aggiornato.
- L'analisi dei contenuti degli endpoint deve essere attivata a livello di raggruppamento di agent per le seguenti attività: caricamento di file web, sincronizzazione di file web, copia su chiave USB, download di file web, apertura di documenti, stampa, incolla di testi dagli appunti e copia su un drive di rete.
- Se desideri utilizzare set di rilevatori DLP per l'analisi dei contenuti, i rilevatori devono essere aggiunti alla configurazione del gruppo di agent e implementati sugli agent endpoint.

Un volta implementati, i rilevatori possono essere utilizzati nelle regole di rilevamento o prevenzione. La logica delle regole di prevenzione implementate sull'agent include l'implementazione degli endpoint (giustificazione o blocco) e il rilevatore di dati sensibili.

Per le applicazioni cloud collegate a Proofpoint Cloud DLP, il motore delle policy potrà utilizzare i rilevatori DLP poco dopo essere stati configurati nell'applicazione DLP. Le regole Proofpoint Cloud DLP sono configurate per generare degli avvisi nella piattaforma. Tuttavia, in modalità scrittura, possono applicare misure correttive in funzione del tipo di connessione per le applicazioni SaaS (API o in linea) utilizzando le regole nell'applicazione Proofpoint Cloud DLP. Le regole Proofpoint Cloud DLP possono integrare le violazioni delle regole DLP nella loro logica. Questa proprietà delle regole viene sincronizzata automaticamente con i rilevatori delle applicazioni DLP. Tutte le attività cloud nelle applicazioni SaaS aziendali integrate alimentano l'applicazione Analytics. Gli avvisi Proofpoint Cloud DLP configurati appariranno nella console. Tutte le misure correttive possono essere gestite e visualizzate direttamente dagli avvisi.

Proofpoint DLP riconosce i dati sensibili in movimento e in corso d'uso grazie a questi tre metodi:

1. **File con un'etichetta di riservatezza visiva (Microsoft Information Protection)**

   Se hai un programma di classificazione dei dati che utilizza le etichette Microsoft, possiamo identificare le etichette e i dati identificativi dei tenant Microsoft (MIP). Questi possono essere quindi utilizzati all'interno di regole.

2. **File contenenti corrispondenze dei contenuti definite dai rilevatori DLP Proofpoint**

   I rilevatori DLP Proofpoint identificano i contenuti sensibili grazie a identificatori intelligenti predefiniti, parole chiave di dizionari pronte all'uso o personalizzate, classificatori, ecc.

3. **File con marcatori contestuali come metadati (nome del file, percorso, estensione del file, tipo di file effettivo, proprietà del documento) o file provenienti da URL tracciati.**

   In Proofpoint Endpoint DLP, un file scaricato sull'endpoint tramite un browser compatibile viene automaticamente tracciato. Tutte le attività legate al file sul dispositivo (copia, spostamento, eliminazione, cambio di nome, ecc.) vengono tracciate. Una volta che il file lascia la macchina tramite un canale di uscita specifico, non viene più tracciato. Tutte le attività legate ai file tracciati vengono acquisite dall'agent, e lo storico può essere visualizzato nella cronologia dei file.

   I file tracciati provengono perciò sempre da URL utilizzati da un browser per localizzare i file. L'agent endpoint può essere utilizzato in modo che le regole di rilevamento e prevenzione monitorino e controllino le attività effettuate sui file che provengono dai servizi web sensibili.

Rilevatori DLP per Proofpoint Email DLP

Devono essere configurate delle regole DLP per Proofpoint Email DLP nella soluzione Proofpoint Email Security (PPS/PoD). Tuttavia, questo processo non rientra nell'ambito del presente documento.

Il modulo di conformità normativa della nostra soluzione Proofpoint Email Security è configurato per effettuare l'analisi richiesta, registrare l'avviso richiesto in base a una regola Proofpoint Email DLP e eseguire le azioni di elaborazione tra canali. L'applicazione di misure correttive può comportare lo spostamento del messaggio in una cartella di quarantena locale per l'elaborazione, la crittografia del messaggio, la risposta all'utente tramite email e l'abbandono del messaggio oppure l'invio all'utente di una risposta intelligente che lo invita a esaminare il proprio messaggio prima di approvarlo.

Tutte le attività che violano una policy Proofpoint Email DLP appariranno negli avvisi. Sono inclusi i dettagli delle email, che possono essere scaricate e riviste direttamente da un amministratore.

Identificatori, rilevatori e set DLP

Le espressioni dei nostri rilevatori sono scritte in una sintassi proprietaria. Includono qualsiasi combinazione booleana per cinque tipi di condizione: identificatori intelligenti, dizionari, inclusione/esclusione di prossimità e set di dati EDM e IDM. Il loro ordine di elaborazione è indicato tra parentesi (). Gli URL tracciati verranno visualizzati come (elenchi di) URL specifici visibili all'agent quando un file viene scaricato con un browser dalla posizione designata.

I dizionari personalizzati sono elenchi di termini specifici del cliente utilizzati dai rilevatori DLP per localizzare i dati potenzialmente sensibili nei file. Quando un file viene analizzato, un rilevatore confronta tutte le parole e frasi nel file con tutti i termini contenuti nei dizionari attivati.

Gli identificatori intelligenti personalizzati vengono integrati in modo più stretto nella piattaforma e gestiti dal team di progettazione Proofpoint. In alcuni casi, devono essere creati per eseguire dei checksum sui valori, per esempio un numero di carta fedeltà specifico per il cliente o un algoritmo che utilizza espressioni regolari e del codice.

Una gran parte dell'implementazione iniziale è dedicata al perfezionamento e all'adattamento dei marcatori di dati sensibili. Tale approccio permette di garantire un basso tasso di falsi positivi e un'elevato tasso di accuratezza.

I rilevatori di analisi dei contenuti indicano le condizioni di corrispondenza per i dati sensibili in base ai dizionari e agli identificatori intelligenti inclusi.

I set di rilevatori includono i rilevatori DLP utilizzati dall'agent endpoint. Devono essere inclusi nei parametri di configurazione del raggruppamento di agent e implementati.

Altre funzionalità avanzate di ispezione dei contenuti:

- Riconoscimento ottico dei caratteri (OCR) che permette di estrarre i testi dalle immagini per l'analisi DLP
- Corrispondenza esatta dei dati per un rilevamento estremamente preciso tramite le corrispondenze multicolonna di dati tabellari strutturati
- Corrispondenza di dati indicizzati (analisi dell'impronta digitale dei documenti) per il caricamento dei file non strutturati e l'esecuzione di un'analisi di affinità sui file trasmessi tramite un canale di uscita.

Attualmente, le funzionalità avanzate non sono disponibili sull'agent endpoint a causa di limitazioni delle risorse Tuttavia, queste limitazioni spariscono quando si verifica il processo di analisi nel cloud. Queste funzionalità sono disponibili esclusivamente per Proofpoint Cloud DLP e Proofpoint Email DLP.

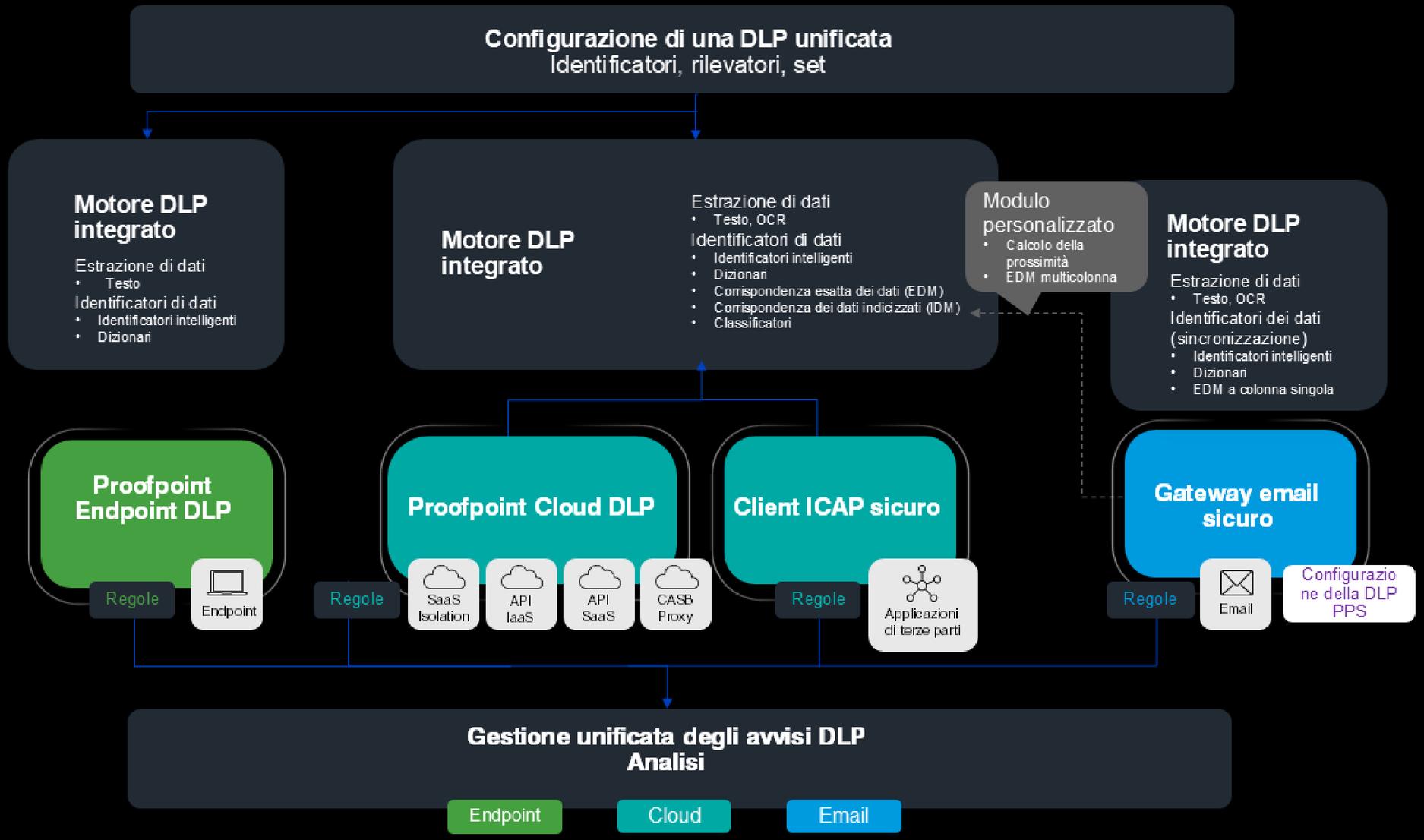
Esportazione di archivi/dati offline

La nostra funzionalità di esportazione di dati ti permette di replicare i tuoi dati in sicurezza al di fuori di Proofpoint. Sei tu a specificare i dati da esportare, tra cui i dati delle attività, gli avvisi e gli eventi. Non esistono limiti di conservazione per i dati esportati. Una volta terminata l'esportazione, puoi manipolare i dati per analizzarli e correlarli.

I dati possono essere replicati su un bucket AWS S3/Azure di proprietà del cliente, che è indipendente dall'applicazione Proofpoint. Puoi quindi integrarli in altri strumenti di analisi come le soluzioni SIEM e data lake.

I dati esportati risalgono a 15 minuti prima dell'attivazione dell'esportazione, che viene eseguita ogni 15 minuti.

Estrazione e identificatori dei dati per canale DLP



Documento N.: 1207-005-05-01

proofpoint.

Per saperne di più, visita il sito proofpoint.com/it

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui l'85% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: www.proofpoint.com/it.