Advanced Data Loss Prevention (DLP)

per **Acronis** Cyber Protect Cloud

Lancio previsto: marzo 2022

Soluzione DLP pensata per gli MSP con creazione automatica di policy specifiche per il cliente

Dalle ricerche emerge che il 72% dei dipendenti condivide informazioni aziendali sensibili; non sorprendono quindi i risultati di uno studio del Ponemon Institute secondo i quali il 45% di tutte le violazioni è causato da incidenti correlati al personale interno. Per configurare e controllare il corretto funzionamento delle tradizionali soluzioni DLP capaci di mitigare questo tipo di rischi sono necessarie competenze di sicurezza vaste e costose: le policy DLP non sono infatti universali ma specifiche per ogni azienda e comportano un processo di configurazione lungo, manuale e costoso, imprescindibile tuttavia per individuare le esigenze peculiari dell'azienda e associarle manualmente alle policy DLP.

Acronis Advanced DLP offre gli strumenti per rendere il provisioning e la gestione più semplici che mai, allo scopo di prevenire le fughe di dati dai workload dei clienti attraverso dispositivi periferici e comunicazioni di rete. La soluzione consente di generare in modo automatico policy DLP di base che potrai adattare alle esigenze aziendali mettendo a punto policy specifiche per ogni cliente.

Estendi l'offerta di servizi con funzionalità ottimizzate per la prevenzione della perdita di dati

CONTROLLI DLP CON RICONOSCIMENTO DEL CONTESTO E DEL CONTENUTO	GENERAZIONE AUTOMATICA DI POLICY DLP DI BASE SPECIFICHE PER IL CLIENTE	APPLICAZIONE ADATTIVA DELLE POLICY DLP
Proteggi i dati sensibili dei clienti impedendo che vengano sottratti dai workload tramite dispositivi periferici e comunicazioni di rete, con analisi del contenuto e del contesto dei trasferimenti di dati e con controlli preventivi basati su policy.	Non è necessario approfondire i dettagli delle informazioni aziendali dei clienti né definire le policy manualmente. Le policy DLP di base specifiche per l'azienda vengono create automaticamente tramite il monitoraggio dei flussi di dati sensibili in uscita. I clienti potranno convalidare queste policy prima che vengano applicate dal sistema.	Evita le attività manuali generalmente necessarie per gestire e adeguare le policy DLP dopo la prima applicazione. L'opzione di applicazione adattiva delle policy espande automaticamente le policy applicate con i nuovi flussi di dati mai utilizzati in precedenza e individuati nei workload dei clienti.

Genera nuove opportunità di profitto

- **Incrementa l'utile per cliente** con i servizi DLP gestiti da MSP, attualmente molto richiesti
- **Attrai più clienti** dimostrando il valore dei servizi che offri con una modalità di osservazione che aumenta la consapevolezza dei clienti sugli eventi DLP
- **Tieni sotto controllo il TCO e incrementa i margini di profitto** con una più semplice suddivisione dei livelli di servizio, grazie a una singola piattaforma che integra backup e disaster recovery, anti-malware di ultima generazione, sicurezza e-mail, gestione dei workload e DLP

Incrementa la produttività e tieni sotto controllo i costi

- **Riduci il tempo dedicato al provisioning e alla configurazione** con la creazione automatizzata di policy DLP di base specifiche per il cliente
- **Allinea le policy DLP alle esigenze dell'azienda, riducendo al minimo gli errori** con la possibilità di aggiungere una giustificazione facoltativa da parte dell'utente finale per i trasferimenti di dati sensibili durante la creazione delle policy di base, e con la convalida semplificata prima dell'applicazione delle policy
- **Semplifica la conformità e il reporting e aumenta la visibilità delle prestazioni DLP** configurando la raccolta di registri, gli avvisi e i widget informativi

Riduci i rischi di perdita dei dati per i clienti

- **Riduci al minimo il rischio di violazioni dei dati causate dal personale interno dei clienti** impedendo la fuga di informazioni sensibili tramite dispositivi periferici e comunicazioni di rete
- **Riduci le conseguenze degli errori umani e facilita l'applicazione di policy accettabili** per l'utilizzo dei dati a livello dell'intera azienda
- **Rafforza la conformità normativa dei clienti** proteggendo i dati regolamentati

Offri servizi DLP che si differenziano da quelli della concorrenza

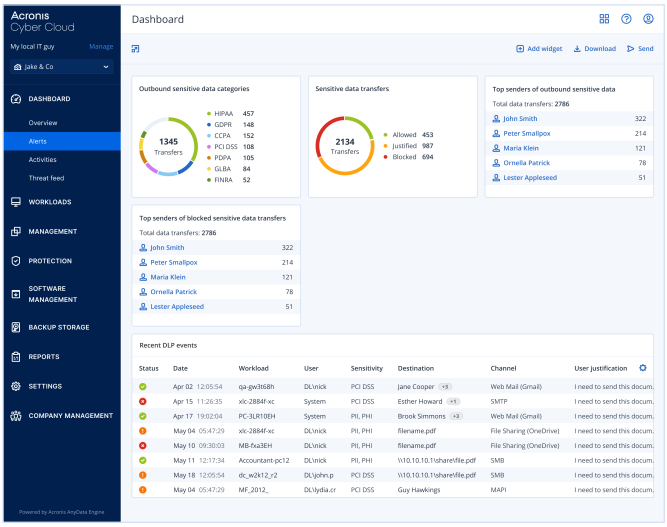
GENERAZIONE AUTOMATIZZATA DI POLICY DLP	POLICY DLP SPECIFICHE PER IL CLIENTE	VASTA GAMMA DI CANALI CONTROLLATI	CONTROLLI DLP COMPLETI	CYBER PROTECTION CENTRALIZZATA DA UN'UNICA CONSOLE
Riduci le attività manuali e il rischio di errori. Semplifica il provisioning generando automaticamente le policy DLP di base per ogni cliente.	Monitora i flussi di dati sensibili in uscita di tutta l'organizzazione, per associare automaticamente i processi di business del cliente alle policy DLP adatte alle sue specifiche esigenze. Offri assistenza facoltativa agli utenti finali per una maggiore precisione e richiedi la convalida del cliente prima dell'applicazione di una policy.	Controlla i flussi di dati nei canali di rete e locali, inclusi supporti di storage rimovibili, stampanti, unità mappate e appunti reindirizzati, e-mail e webmail, sistemi di messaggistica istantanea, servizi di condivisione di file, social network e protocolli di rete.	Predisponi un controllo indipendente dal browser web dei trasferimenti di dati verso i social media e i servizi webmail e di file sharing. Abilita l'ispezione del contenuto dei messaggi istantanei in uscita e il rilevamento dei dati sensibili nelle immagini sui computer remoti e offline.	Tieni sotto controllo il TCO, riduci i costi di gestione e incrementa i margini di profitto grazie a una singola soluzione che integra backup, disaster recovery, anti-malware di ultima generazione, sicurezza e-mail, gestione dei workload e DLP.

Semplifica il provisioning dei clienti, la generazione e la gestione delle policy DLP

Advanced Data Loss Prevention (DLP) semplifica le attività di provisioning e gestione degli MSP grazie a due diverse modalità operative:

Modalità di osservazione

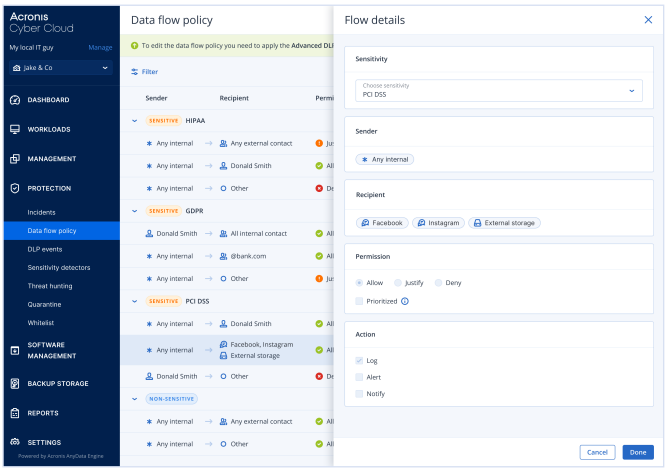
Dimostra il valore dei servizi di prevenzione della perdita dei dati e aumenta la consapevolezza dei clienti sugli eventi DLP. In modalità di osservazione, l'agente monitora i computer endpoint dei clienti per individuare i flussi di dati sensibili in uscita al fine di generare le policy DLP di base in modo automatico oppure, facoltativamente, con la richiesta di una giustificazione da parte dell'utente finale per i trasferimenti di dati considerati più a rischio.



Modalità di applicazione

Una volta convalidata insieme al cliente, la policy DLP potrà essere applicata per iniziare a proteggere i dati. In modalità di applicazione è possibile scegliere come applicare le policy DLP:

- **Applicazione rigida**: applica la policy DLP come stabilito, senza modificarla con nuove regole per i flussi di dati. Viene bloccato qualsiasi trasferimento dei dati che non corrisponde a una regola del flusso di dati definita nella policy, a meno che l'utente finale non richieda un'eccezione specifica per l'azienda che consente di ignorare temporaneamente il blocco.
- **Applicazione adattiva**: applica la policy DLP con flessibilità, consentendo di aggiungere nuove regole per consentire flussi di dati aziendali non osservati in precedenza.



Acronis

Per saperne di più, visita
www.acronis.com