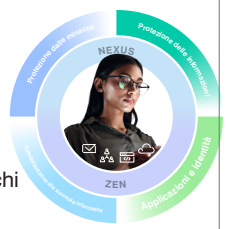
Fusioni e acquisizioni: prevenire la perdita di dati

Utilizza Proofpoint Adaptive Email DLP per prevenire la perdita di dati sensibili durante fusioni e acquisizioni

Vantaggi principali

- Previeni la perdita di dati accidentale e intenzionale tramite l'email.
- Evita i danni alla reputazione della tua azienda.
- Migliora la sensibilizzazione alla sicurezza informatica in tutta la tua azienda.
- Beneficia di una sicurezza dell'email efficace, semplice da gestire e che limita l'impatto sulle attività degli utenti.
- Riduci i tempi di valorizzazione grazie a una protezione attiva in sole 48 ore.

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a mitigare le quattro principali categorie di rischi legati agli utenti.



Le fusioni e acquisizioni aumentano in modo significativo il numero di persone che condividono informazioni riservate tra le aziende via email. Per i team della sicurezza delle informazioni è inoltre difficile tracciare tutti collaboratori e le terze parti coinvolti. Questi fattori aumentano il rischio di perdita di dati sensibili.

Proofpoint Adaptive Email Data Loss Prevention (DLP) risolve questi problemi. Proofpoint Adaptive Email DLP si basa sull'intelligenza artificiale (IA) comportamentale per identificare i comportamenti dei tuoi collaboratori in merito all'email, le loro relazioni di fiducia e il modo in cui condividono i dati sensibili. La nostra soluzione analizza le email per rilevare i comportamenti anomali e informare gli amministratori. Inoltre avvisa gli utenti in tempo reale, prima che si verifichino fuoriuscite di dati importanti.

Perché le fusioni e acquisizioni aumentano i rischi

Durante le operazioni di fusioni e acquisizioni, le aziende devono condividere numerose informazioni riservate: dati personali, documenti del consiglio d'amministrazione, dati di private equity, ecc.

Secondo una ricerca di Gartner, queste transazioni aumentano i rischi di perdita di dati per diversi motivi:

- Possono verificarsi conflitti tra le pratiche di sicurezza delle due aziende.
- L'incertezza o la segretezza relative alla transazione possono generare ansia, che può portare i collaboratori a agire in modi insoliti o dannosi.
- Spesso, si presentano nuove esigenze tecniche. Per esempio, una volta finalizzata la transazione, le aziende devono adottare tre diverse modalità operative: prima della fusione, durante la transizione e dopo la fusione. La superficie d'attacco è molto più ampia durante questo periodo.

Come Proofpoint Adaptive Email DLP protegge i tuoi dati sensibili

La perdita di dati sensibili può danneggiare la reputazione della tua azienda ed essere costosa da risolvere. Proofpoint Adaptive Email DLP ti evita questi danni. La nostra soluzione utilizza l'IA comportamentale per rilevare e bloccare la perdita di dati accidentale e intenzionale tramite l'email. L'IA analizza oltre dodici mesi di dati dell'email per identificare i comportamenti di invio delle email dei tuoi collaboratori, le loro relazioni di fiducia e il modo in cui gestiscono i dati sensibili.

Proofpoint Adaptive Email DLP utilizza l'IA così addestrata per identificare i comportamenti anomali in tempo reale: invio di un'email al destinatario errato, invio di dati sensibili a un account non autorizzato e meno sicuro o sottrazione deliberata di informazioni. Quando rileva dei problemi, Proofpoint Adaptive Email DLP mostra agli utenti dei messaggi in tempo reale. Gli utenti possono quindi correggere le loro azioni per evitare la perdita di dati, senza l'intervento aggiuntivo di un amministratore.

Nell'ambito di fusioni e acquisizioni, queste funzionalità permettono di evitare che dati riservati finiscano nelle mani sbagliate mantenendo la continuità delle comunicazioni strategiche.

Blocca le email inviate al destinatario errato

Può accadere che un utente invii un'email alla persona sbagliata. Si tratta di una causa comune di perdita di dati nelle aziende. Questi incidenti sono difficili da prevenire attraverso regole e policy. Conoscendo le abitudini dei collaboratori relative alle email, Proofpoint Adaptive Email DLP può avvertire gli utenti prima che inviino un'email al destinatario errato.

Previeni l'invio di allegati sbagliati

L'invio di un allegato sbagliato avviene quando un utente invia un'email al destinatario giusto ma allega il file sbagliato. Come per le email inviate al destinatario errato, Proofpoint Adaptive Email DLP utilizza l'IA per rilevare l'invio di allegati sbagliati. Quindi avvisa gli utenti in tempo reale.

Blocca le esfiltrazioni via email

Le regole email possono bloccare efficacemente la perdita di dati. Tuttavia, operano solo per tipi noti e predefiniti di dati: informazioni personali, dati del settore delle carte di pagamento, numeri della previdenza sociale, ecc.

Proofpoint Adaptive Email DLP identifica e classifica i tuoi dati sensibili. Identifica anche gli account email personali degli utenti in base al loro comportamento. Se un collaboratore cerca di inviare dati sensibili a se stesso o ad altri, la nostra soluzione può bloccare o tracciare le sue attività, in base alla sua configurazione.

Figura 1. Proofpoint Adaptive Email DLP avvisa gli utenti in tempo reale in caso di invio di email al destinatario errato.

Figura 2. La dashboard Proofpoint Adaptive Email DLP fornisce ai team della sicurezza delle informazioni piena visibilità sulle minacce trasmesse via email.

Forma gli utenti in tempo reale

La visualizzazione di messaggi di formazione in tempo reale aiuta gli utenti a evitare di commettere errori e di infrangere le regole. Complementare alla formazione di sensibilizzazione alla sicurezza informatica, Proofpoint Adaptive Email DLP spiega agli utenti i rischi legati alle email. Grazie a questi messaggi di formazione, gli utenti possono correggere gli errori in tempo reale ed evitare la perdita di dati.

Identifica le minacce a cui sei esposto

La dashboard Proofpoint Adaptive Email DLP fornisce ai team della sicurezza un'istantanea di tutte le email verificate dal sistema. La dashboard mostra le email a rischio rilevate e bloccate, tra cui le email inviate al destinatario errato e i file allegati erroneamente, nonché i tentativi di esfiltrazione tramite email. Mostra anche i miglioramenti della sicurezza nel tempo per gli utenti e per l'azienda.

Informazioni come le principali policy personalizzate e gli utenti più a rischio aiutano gli analisti a concentrarsi su ciò che è più importante. Queste informazioni velocizzano le indagini e aiutano i team della sicurezza a collaborare con gli utenti per migliorare il modo in cui gestiscono i dati.

Beneficia di un'amministrazione semplice

Proofpoint Adaptive Email DLP richiede un'installazione e una configurazione minime. In sole 48 ore, inizia a prevenire la perdita di dati attraverso l'email. Permette interventi di sicurezza accurati e efficaci senza interrompere le normali attività dei tuoi utenti.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito **proofpoint.com/it**.