

Guida del valutatore alle soluzioni Proofpoint Information Protection

2024

La valutazione di un prodotto software per assicurarsi che sia adatto alla propria organizzazione è una parte importante del processo di acquisto. Una proof-of-concept, comunemente detta POC, è un metodo standard per fare esattamente questo. Acquisire esperienza pratica con un prodotto software aiuta l'acquirente a determinare rapidamente se le sue esigenze aziendali e i suoi casi d'uso vengono soddisfatti. La riuscita di una POC elimina le congetture e offre un'esperienza tangibile, perciò le POC hanno un ruolo molto importante nel processo decisionale.

Un buon paragone è quello con l'acquisto di un'auto: è quasi certo che non si compra un'auto nuova senza prima averla provata. La stessa esperienza pratica è offerta da Proofpoint per i suoi prodotti Proofpoint Information Protection, tramite una POC completamente ospitata che ti aiuterà a comprendere il modo in cui la tua organizzazione può proteggersi dalle perdite di dati e dalle minacce interne.

Le problematiche delle POC

Nonostante i vantaggi derivanti dallo svolgimento di una POC, diverse problematiche possono impedire alle POC di decollare e avere successo. Problemi più comuni:

- Mancanza di casi d'uso chiaramente definiti.
- Ottenimento di autorizzazione e approvazioni interne.
- Personale limitato.
- Nessun accesso ai computer di prova.

Proofpoint offre un approccio innovativo alla POC che allevia tali problematiche e ti consente di testare il nostro software in modo rapido ed efficiente.

POC Proofpoint: veloce, efficiente, efficace

Proofpoint offre un modo rapido e semplice per acquisire esperienza pratica con le soluzioni Proofpoint Information Protection. La nostra POC, in un ambiente completamente ospitato, ti fornisce tutti gli strumenti necessari per difendere i dati e bloccare le minacce interne. In due settimane potrai testare cinque dei casi d'uso più comuni. Una volta completata la POC, Proofpoint ti aiuterà a documentare i risultati per condividerli con i tuoi team.

1. Inizio

Puoi iniziare a usare la POC di Proofpoint Information Protection fin dal primo giorno, senza bisogno di alcuna configurazione o approvazione. Ti verranno forniti due computer virtuali e gli accessi per simulare le azioni degli utenti. Per analizzare quest'ultime, avrai inoltre accesso all'ambiente SaaS di Proofpoint Information Protection. Lavorando dalla console centralizzata si ottiene una visibilità approfondita sul comportamento degli utenti, con la relativa cronologia, metadati dettagliati e schermate. È inoltre possibile assegnare le priorità agli avvisi, affrontare gli incidenti, cercare le minacce e gestire le politiche, tutto dalla stessa console grazie alla visualizzazione multicanale di endpoint, email, cloud e web.

2. Casi d'uso

Nel corso di due settimane potrai testare cinque degli scenari utente e casi d'uso più comuni:

- Un collaboratore interno malintenzionato che cerca di sottrarre dati sensibili.
- Un utente che dà prova di negligenza con i dati sensibili.
- Un utente negligente che gestisce male i dati nelle applicazioni dell'IA generativa.
- Un utente compromesso (per un attacco di phishing) che perde i dati a vantaggio dell'aggressore.
- Un utente compromesso (ad esempio per attacchi tramite telefonata (TOAD, Telephone-Oriented Attack Delivery)) che perde i dati a vantaggio dell'aggressore.

3. Conclusioni

Dopo aver svolto la POC comprenderai meglio come Proofpoint accelera il tuo programma di prevenzione delle perdite di dati o di protezione dalle minacce interne. Verrà elaborato un riepilogo che evidenzia i casi d'uso e i vantaggi.

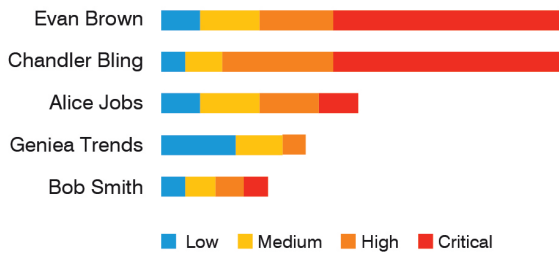
Esempio dei criteri di valutazione

Proof-of-concept Defend Data

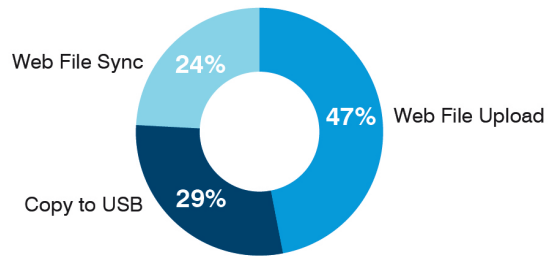
- Monitorare attivamente gli utenti a rischio in una dashboard centralizzata.
- Comprendere quali sono i dati che fuoriescono dall'azienda e in che modo.
- Comprendere perché è scattata una regola e quali dati sensibili sono stati rilevati.
- Dimostrare i cambiamenti nel comportamento dei dipendenti per mantenere la conformità e ridurre il rischio.
- Rilevare l'uso di un'applicazione non autorizzata.
- Rilevare e prevenire la sottrazione dei dati sensibili tramite caricamento web, USB, sincronizzazione cloud.
- Identificare e prevenire la sottrazione dei dati sensibili tramite email.
- Rilevare e contrastare automaticamente le minacce basate sul cloud e le sottrazioni dei dati.
- Monitorare, rilevare e prevenire l'uso dei siti di IA generativa.
- Rilevare le modifiche al nome e al tipo di un file.
- Bloccare automaticamente le email con la maggiore probabilità di essere casi di perdita di dati.
- Cercare e filtrare i dati delle attività per trovare rapidamente le risposte.
- Visualizzare la cronologia delle attività di un utente prima, durante e dopo un incidente.
- Visualizzare i dati storici dell'attività di un utente.
- Acquisire schermate come prove forensi.
- Distinguere tra un utente negligente, compromesso e malintenzionato.
- Esportare un rapporto sull'attività degli utenti utilizzabile da Risorse Umane e Ufficio Legale.
- Formare gli utenti con notifiche a comparsa e giustificazioni.

Information Protection Summary

Most Risky Users (Number of Alerts)



Most File Exfiltration by Type



8

Users browsing to GenAI websites

20

Files automatically remediated for oversharing

45

Blocks of unapproved web file upload

80

Sensitive emails send to unauthorized accounts

Vantaggi di una POC di Proofpoint

Facile configurazione

Senza la necessità di configurazioni o approvazioni, puoi iniziare a testare Proofpoint Information Protection immediatamente in un ambiente completamente ospitato.

Valore rivelato rapidamente

Una POC con Proofpoint viene completata in meno di due settimane, il che costituisce un modo rapido e semplice per acquisire esperienza pratica e accelerare il processo decisionale.

Risultati misurabili

Puoi testare cinque degli scenari utente e casi d'uso più comuni con l'accesso completo alle soluzioni Proofpoint Information Protection, ottenendo la visibilità multicanale su endpoint, email, web e cloud.

POC Proofpoint: non è la solita POC

CRITERI	POC STANDARD	PROOFPOINT
Tempo di configurazione	Da settimane a mesi a seconda delle autorizzazioni	Entro poche ore
Durata	Da settimane a mesi	Meno di 2 settimane
Impegno del cliente	Significativo	Minimo
Computer di prova dedicati	Necessari per la POC	Non necessari per la POC
Casi d'uso	Devono essere chiaramente definiti	I casi d'uso più comuni sono già pronti; possono essere ampliati con casi d'uso specifici

I clienti vedono il valore della POC di Proofpoint

"Il fatto che Proofpoint abbia pensato di offrire e mettere insieme tutto questo per i clienti ha cambiato le carte in tavola. Nessun altro lo fa... Ci ha fatto risparmiare un sacco di tempo per entrare nella fase di test di questo progetto."

Security Architect, società di spedizioni Fortune 500

INFORMAZIONI SU PROOFPOINT

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.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.