Forcepoint

9 passi verso il successo con la Data Protection

Proteggere i dati significa comprendere i potenziali rischi a cui sono esposti i dati e come intervenire nel caso in cui si manifestino.

Ma come conciliare le esigenze operative dell'azienda e la necessità di mantenere al sicuro i dati?

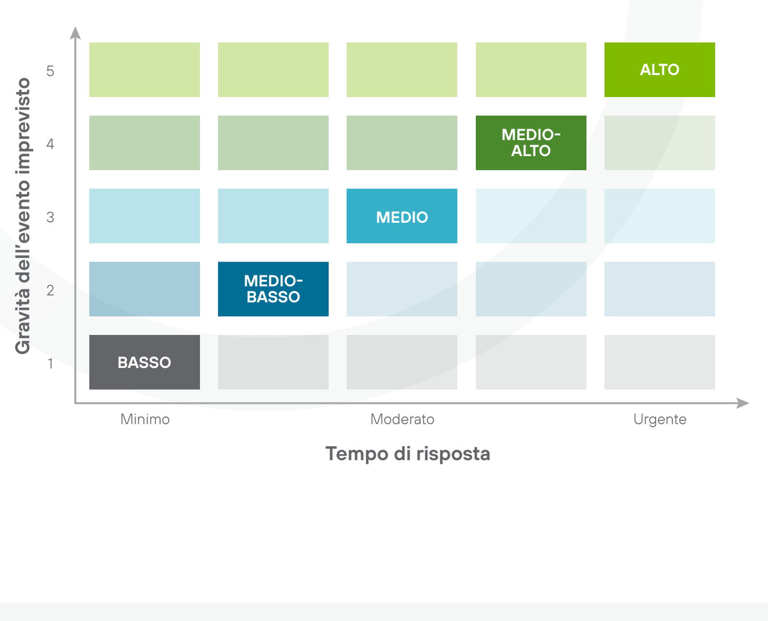
I nove passi che seguono ti guideranno nell'implementazione di controlli di protezione dei dati che sono al tempo stesso misurabili, efficaci e pratici per le tue attività quotidiane e nell'individuazione di opportunità per rafforzare la tua soluzione mediante la protezione adattiva al rischio dei dati.

1 Creazione di un profilo di rischio informatico

Un profilo di rischio aiuta a capire cosa esigere da una soluzione di protezione dei dati. In primo luogo, è necessario indicare i rischi che si desidera mitigare ed elencare i tipi di dati ai quali si riferiscono, raggruppandoli per tipo di dati in base alle necessità. Quindi, è importante definire le reti, gli endpoint e i canali cloud nei quali tali dati potrebbero potenzialmente andare persi, insieme ai controlli attualmente utilizzati per metterli in sicurezza.

2 Creazione di un grafico dei livelli di gravità degli eventi di compromissione dei dati e relativi tempi di risposta

La correlazione tra ciascun tipo di dati e il suo impatto sull'azienda consentirà di stabilire la priorità delle risposte e di mantenere concentrate le risorse di sicurezza laddove sono più efficaci. Per alcune aziende quest'attività può rivelarsi impegnativa. La prima mossa: definire "a tavolino" insieme ai proprietari dei dati quali sono i tipi di dati da proteggere e quali sono i rischi in caso di compromissione. Quindi, si passa a classificare ciascuno dato su una scala di 1:5 (1= basso impatto, 5= alto impatto) e a definire un tempo di risposta accettabile per ognuno, a seconda della gravità del rischio (i dati ad alto rischio dovranno essere messi in sicurezza per primi).



La differenza di una soluzione adattiva al rischio

La protezione dei dati adattiva al rischio è concepita per assegnare priorità alle attività ad alto rischio, applicare in modo autonomo i controlli in base al rischio e ridurre il tempo necessario per analizzare un evento imprevisto.

3 Stabilire una risposta agli eventi imprevisti di compromissione dei dati per canale e gravità

Essere un passo avanti nella protezione dei dati significa sapere come reagire agli eventi imprevisti prima che si verifichino. Elenca tutti i canali della rete, gli endpoint e il cloud in cui fluiscono i dati. Quindi, stabilisci una risposta adeguata per gli eventi imprevisti a basso o alto impatto, in base alle esigenze del canale.

La differenza di una soluzione adattiva al rischio

Una soluzione adattiva al rischio tiene conto del livello di rischio di ogni individuo che viene in contatto con i dati, consentendo di adeguare le risposte agli eventi imprevisti in base al rischio individuale. Ad esempio, l'adattamento delle risposte in modo da eseguire semplicemente un controllo per gli utenti a basso rischio e imporre invece un blocco solo per gli utenti ad alto rischio garantisce che ciascun membro del team possa svolgere il suo lavoro senza compromettere i dati o incidere sulla produttività dell'utente.

Canali	Livello 1 Basso	Livello 2* Medio-basso	Livello 3 Medio	Livello 4* Medio-alto	Livello 5* Alto	Note
E-mail	Crittografia	Invio allegati e-mail	Quarantena	Quarantena		Crittografia
Web						Proxy da bloccare
Web sicuro						Ispezione SSL
FTP	Controllo	Controllo/notifica	Blocco/notifica	Blocco/avviso	Blocco	Proxy da bloccare
Stampante di rete						Installa DLP Printer Agent
Personalizzato						
Applicazioni cloud			Quarantena con nota	Quarantena		

*Granularità aggiuntiva disponibile con la Data Protection adattiva al rischio

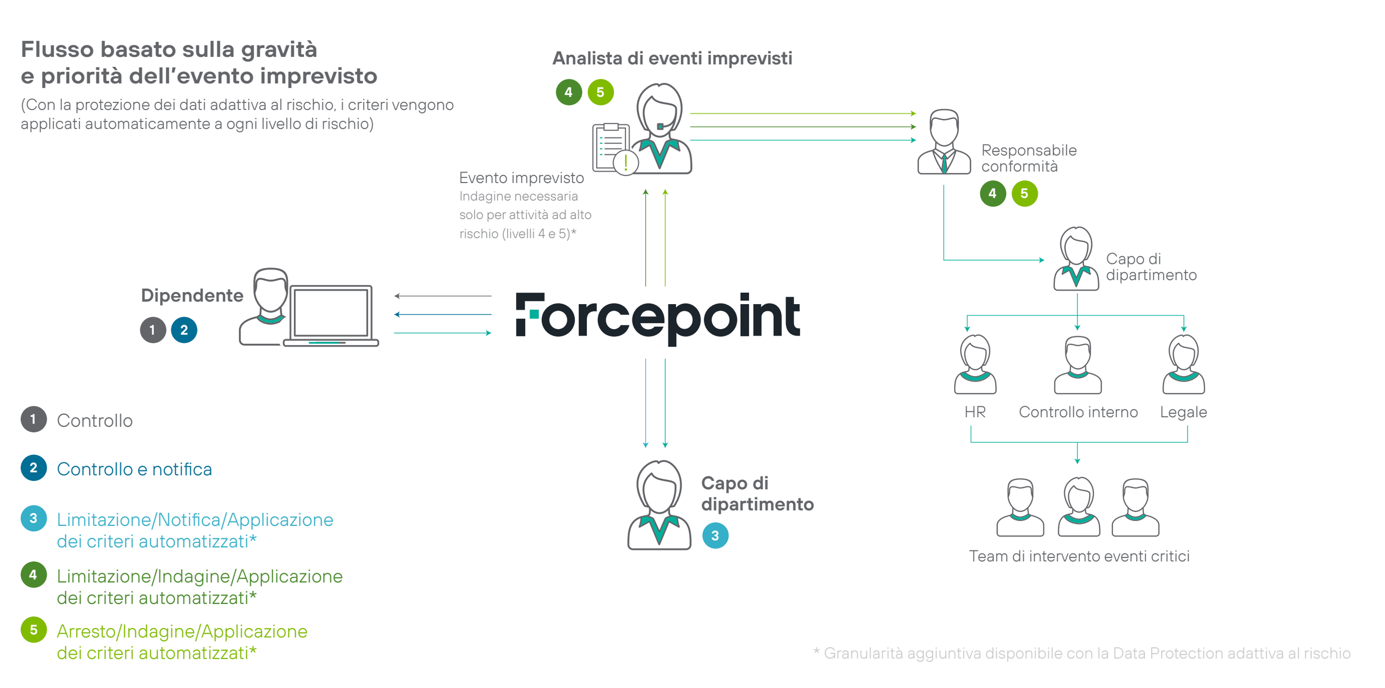
4 Stabilire un flusso di lavoro degli eventi imprevisti

Definisci con chiarezza il flusso di lavoro di risposta per eventi imprevisti a basso o alto impatto per assicurarti che i team di sicurezza possano entrare in azione nel momento stesso in cui viene rilevato un evento imprevisto. Per gli eventi a basso impatto, è opportuno automatizzare il processo dove possibile. In questo modo la larghezza di banda resta disponibile per la risoluzione diretta di eventi imprevisti ad alto impatto.

La differenza di una soluzione adattiva al rischio

Una soluzione adattiva al rischio consente di analizzare gli eventi imprevisti in base al livello di rischio individuale, senza dover ricorrere a un analista per determinare l'azione migliore da intraprendere. Gli eventi imprevisti associati a individui a basso rischio non costituiscono una minaccia per l'azienda; pertanto è opportuno lasciare che seguano il loro corso (adottando ulteriori protezioni come la crittografia per il trasferimento di file tramite USB o l'invio automatico degli allegati di posta elettronica) al fine di mantenere la produttività.

Gli amministratori possono adottare lo stesso approccio proattivo con persone ed eventi imprevisti ad alto rischio, bloccando o limitando automaticamente alcune azioni specifiche fino all'intervento di un analista in grado di condurre un'indagine.



5 Assegnare ruoli e responsabilità

Definisci i ruoli nel team per migliorare la stabilità del programma di protezione dei dati, la scalabilità e l'efficienza operativa. Assegna i ruoli chiave, ad esempio amministratori tecnici, analisti di eventi imprevisti, investigatori forensi e auditor, e conferisci i diritti e l'accesso a ciascuno di essi.

6 Avviare il progetto in modalità di monitoraggio

Una volta implementata la soluzione di protezione dei dati di rete, un periodo di monitoraggio ti consentirà di identificare degli schemi ricorrenti nell'attività e di creare una linea di base che ti aiuti a riconoscere il comportamento abituale degli utenti. Completato questo periodo, analizza il comportamento osservato e presenta le conclusioni al team esecutivo, offrendo dei consigli su come mitigare i rischi. A questo punto è possibile mettere in pratica tali consigli, monitorarne la riuscita e presentarli nuovamente ai dirigenti.

La differenza di una soluzione adattiva al rischio

Con una soluzione adattiva al rischio, l'analisi degli eventi imprevisti in modalità di solo controllo (diversa dalla modalità di imposizione graduale) metterà in evidenza la riduzione degli eventi imprevisti che richiedono indagini, senza compromettere i dati. Inoltre, si potranno osservare più incidenti positivi senza impegnare risorse per false minacce.

7 Passare alla protezione proattiva

Le informazioni acquisite in modalità di monitoraggio forniranno il livello di fiducia necessario per passare alla modalità di blocco per gli eventi ad alto rischio o conformemente a quanto previsto dal piano di risposta. Durante l'implementazione della protezione dei dati negli endpoint e nelle applicazioni cloud autorizzate, i risultati verranno monitorati, analizzati, segnalati, ottimizzati e nuovamente riferiti al team esecutivo.

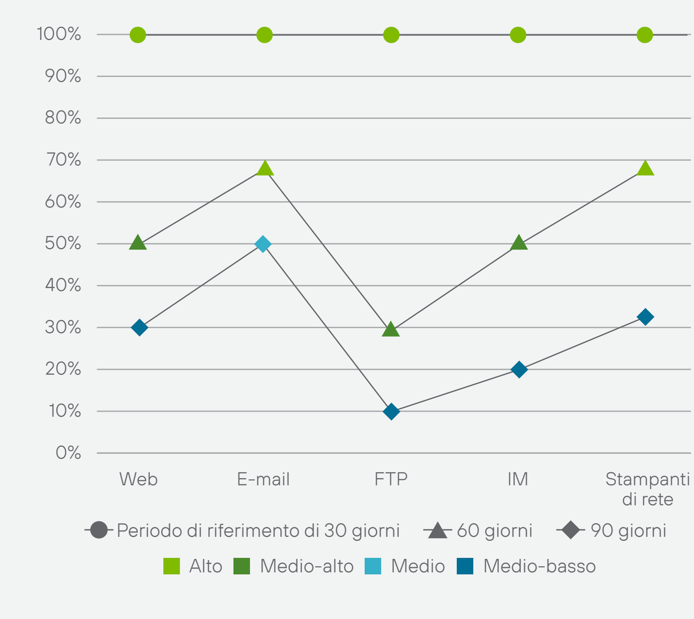
8 Integrare i controlli della Data Protection a livello aziendale

Quando deleghi le responsabilità ai supervisori della sicurezza dei vari reparti, pensa all'efficienza. Ad esempio, i proprietari dei dati sono già responsabili di eventuali perdite di dati: se assegni a loro la responsabilità degli eventi imprevisti, li aiuti a comprendere in che modo i dati vengono utilizzati da terzi e a valutarne il rischio, eliminando passaggi inutili.

Per incominciare, chiedi al team di sicurezza di tenere una riunione introduttiva per illustrare i controlli di protezione dei dati agli altri membri. Quindi organizza un corso di formazione per i nuovi membri del team e prevedi un periodo di tempo di affiancamento per la risposta agli eventi imprevisti, durante il quale acquisiranno familiarità con i processi. Per rafforzare quei processi, prendi in considerazione anche la possibilità di offrire un coaching in tempo reale.

9 Tenere traccia dei risultati della riduzione del rischio

La preparazione per questa fase è cominciata al punto 6; ora si procede in questo modo: raggruppa gli eventi imprevisti correlati in base a criteri quali gravità, canale, tipo di dati e normativa. Quindi, definisci i periodi di monitoraggio e riduzione del rischio in modo che abbiano la stessa durata (per cominciare, fai una prova assegnando due settimane a ciascun periodo) per preservare l'integrità dei risultati.



Numero di eventi imprevisti in un periodo di 90 giorni

Eventi imprevisti	E-mail	Web	FTP	IM	Stampante di rete
Periodo di riferimento di 30 giorni	150	200	50	10	45
60 giorni	100	100	15	5	30
Riduzione del rischio su 60 giorni	33%	50%	70%	50%	33%
90 giorni	76	60	5	2	15
Riduzione del rischio su 90 giorni	49%	70%	90%	80%	67%

Obbiettivi

60 giorni	90 giorni
Riduzione oltre il 25%	**Riduzione oltre il 50%**

La differenza di una soluzione adattiva al rischio

Con un approccio adattivo al rischio, è opportuno mettere a confronto gli eventi imprevisti acquisiti in modalità di solo controllo (tutti gli eventi imprevisti) e gli eventi imprevisti che richiedono un approfondimento, con applicazione graduale. Il riepilogo deve mostrare il numero di eventi imprevisti per ogni livello di rischio 1-5, contrapposti a quelli che effettivamente richiedono un approfondimento (livelli di rischio 4-5).

Sia che si adotti un approccio tradizionale o che si incrementi la sicurezza con una protezione dei dati adattiva al rischio, questa formula comprovata contribuirà a raggiungere l'obiettivo.

Vuoi vedere la protezione adattiva al rischio in azione?

Fai clic qui

Forcepoint