Forcepoint

Una giornata nella vita dei dati sensibili

Un'impiegata. Un mattino ordinario. Un'esplosione esponenziale del rischio sui dati. Ecco come succede e come fermarlo.

Il Rischio è Già Qui

53%

DEGLI INCIDENTI INTERNI SONO ACCIDENTALI O NEGLIGENTI

DTEX 2026 Costo dei Rischi Interni

13%

DEGLI INCIDENTI VENGONO CONTENUTI IN MENO DI 30 GIORNI

DTEX 2026 Costo dei Rischi Interni

200+ Giorni

TEMPO MEDIO DI RISOLUZIONE DEGLI INCIDENTI INTERNI (DOLOSI E ACCIDENTALI)

IBM 2025
Costo di una Violazione dei Dati

$19.5 Milioni

COSTO MEDIO ANNUO TOTALE DEGLI INCIDENTI INTERNI

DTEX 2026
Cost of Insider Risks

Ecco Alice

Alice è una rappresentante commerciale che si sta preparando per un incontro con un partner ad alto rischio. Sta svolgendo il suo lavoro. **Non sta cercando di causare un incidente di sicurezza. Scopri cosa succede ai dati sensibili mentre si prepara.**

Salesforce → Excel

Alice esegue un report sui suoi principali account strategici in Salesforce e lo scarica come file Excel. I dati includono nomi degli account, contatti e dati sui ricavi.

PII regolamentate, PI e dati degli account strategici escono da un ambiente CRM controllato.

Excel → Cloud

Carica il file su una piattaforma di collaborazione per condividerlo con il suo team. SharePoint. Box. OneDrive. Non importa quale.

I dati critici esistono ora in più posizioni, accessibili a chiunque disponga delle autorizzazioni.

Excel → AI pubblica

Alice utilizza uno strumento AI pubblico per riassumere le tendenze e creare punti di discussione. Carica il file Excel direttamente nel prompt.

I dati critici sono stati caricati su una Shadow AI con un prompt rischioso.

Output AI → Slack

Condivide il riepilogo generato dall'AI con il suo team su Slack.

Nuovi contenuti che includono elementi di dati critici si diffondono in un canale di collaborazione.

Slack → E-mail esterna

Alice invia il riepilogo via e-mail a un partner esterno all'organizzazione.

I dati critici vengono esportati tramite il canale più rischioso, senza controlli di accesso o audit.

Cosa è appena successo?

PII. Proprietà intellettuale. Informazioni strategiche. In un solo giorno, tutto ciò è esploso su piattaforme di collaborazione, storage cloud, strumenti AI e confini di fiducia esterni. Alice non voleva causare problemi. Stava semplicemente cercando di lavorare in modo più intelligente e veloce. È questo che rende il rischio interno così difficile da gestire: nella maggior parte dei casi non è doloso. È umano.

Un nuovo approccio:
Sicurezza Che Segue i Dati

La protezione dei dati sensibili richiede un approccio continuo che si adatta in tempo reale. Non una checklist. Non un insieme di policy statiche. Un ciclo. **Forcepoint chiama questo approccio Data Security Everywhere.**

Scoprire
Stabilire la visibilità sui dati sensibili ovunque si trovino

Classificare
Identificare il tipo, l'utilizzo aziendale e il livello di sensibilità dei dati

Dare priorità
Concentrare l'attenzione dove il rischio è maggiore

La protezione dei dati sensibili non è una checklist. **È un ciclo continuo.**

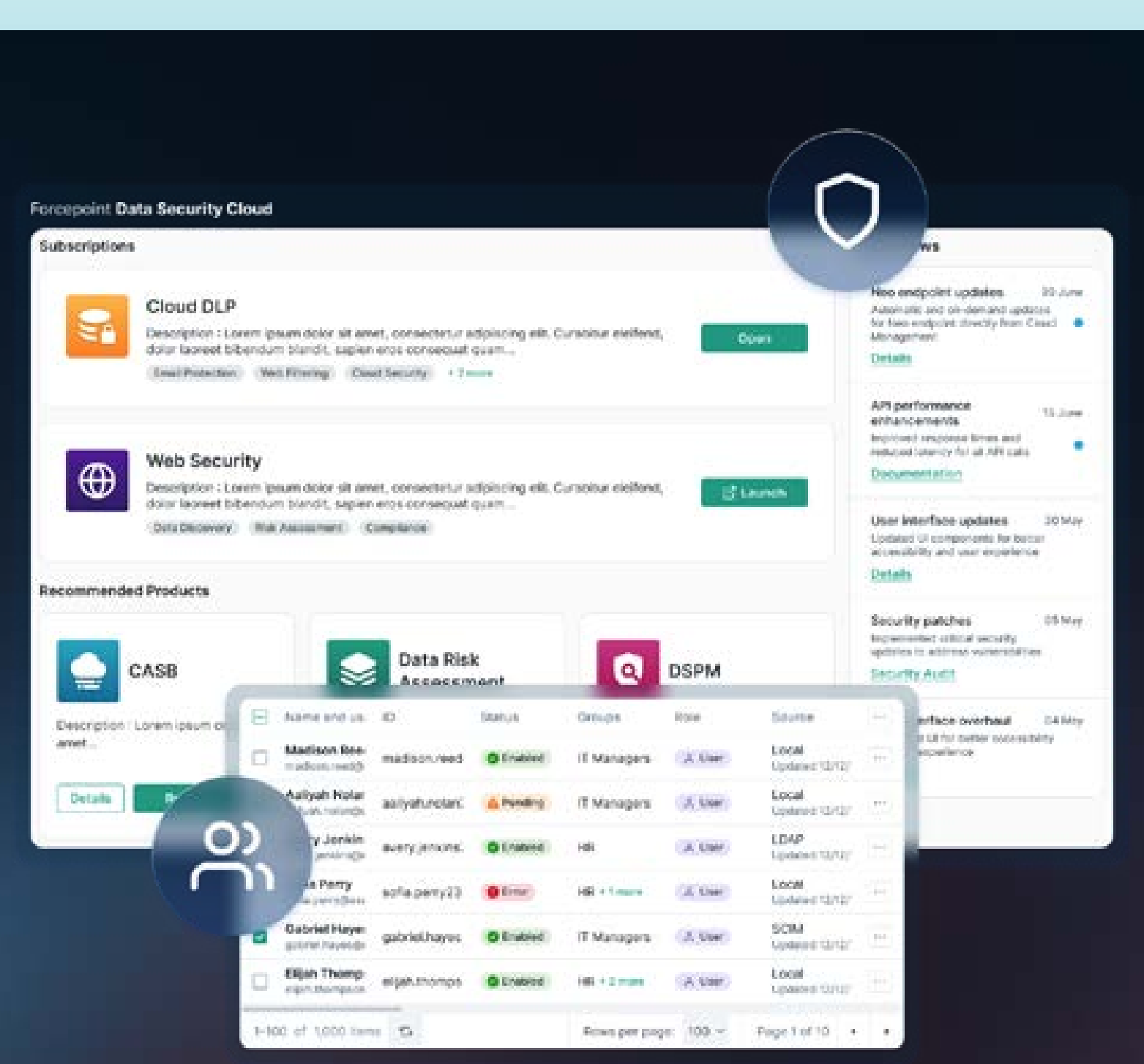
Proteggere
Applicare le policy in modo coerente su tutti i canali per ridurre il rischio

Rimediare
Affrontare le vulnerabilità prima che diventino violazioni

Forcepoint Data Security Cloud

Tutti e cinque i passaggi si collegano in un'unica piattaforma unificata: Forcepoint Data Security Cloud. Una sola piattaforma. Un solo insieme di policy. Visibilità completa in ogni ambiente in cui i dati vivono, si muovono e vengono utilizzati.

Scopri di più



Forcepoint

[FP-A Day In The Life-IT] 21Apr2026