Forcepoint

Une journée dans la vie des données sensibles

Une employée. Un matin ordinaire. Une explosion exponentielle du risque de données. Voici comment cela se produit et comment l'arrêter.

Le Risque est Déjà Là

53%

DES INCIDENTS INTERNES SONT ACCIDENTELS OU NÉGLIGENTS

DTEX 2026 Coût des Risques Internes

13%

DES INCIDENTS SONT CONTENUS EN MOINS DE 30 JOURS

DTEX 2026 Coût des Risques Internes

200+ Jours

DÉLAI MOYEN DE RÉSOLUTION DES INCIDENTS INTERNES (MALVEILLANTS ET ACCIDENTELS)

IBM 2025
Coût d'une Violation
de Données

$19,5 Millions

COÛT ANNUEL MOYEN TOTAL DES INCIDENTS INTERNES

DTEX 2026
Coût des Risques Internes

Voici Alice

Alice est une commerciale qui prépare une réunion partenaire à fort enjeu. Elle fait son travail. Elle n'essaie pas de provoquer un incident de sécurité. **Découvrez ce qui arrive aux données sensibles pendant ses préparatifs.**

Salesforce → Excel

Alice génère un rapport sur ses comptes stratégiques prioritaires dans Salesforce et le télécharge sous forme de fichier Excel. Les données incluent les noms de comptes, les contacts et les chiffres de revenus.

Des PII réglementées, des PI et des données de comptes stratégiques quittent un environnement CRM contrôlé.

Excel → Cloud

Elle téléverse le fichier vers une plateforme de collaboration pour le partager avec son équipe. SharePoint. Box. OneDrive. Peu importe.

Les données critiques existent désormais à plusieurs endroits, accessibles à toute personne disposant des autorisations.

Excel → IA publique

Alice utilise un outil d'IA public pour résumer les tendances et créer des points de discussion. Elle téléverse le fichier Excel directement dans le prompt.

Des données critiques ont été téléversées vers une IA fantôme avec un prompt risqué.

Résultat IA → Slack

Elle partage le résumé généré par l'IA avec son équipe dans Slack.

Un nouveau contenu incluant des éléments de données critiques se propage dans un canal de collaboration.

Slack → E-mail externe

Alice envoie le résumé par e-mail à un partenaire extérieur à l'organisation.

Les données critiques sont exportées via le canal le plus risqué, sans contrôle d'accès ni d'audit.

Que vient-il de se passer ?

PII. Propriété intellectuelle. Informations stratégiques. En une seule journée, tout cela a explosé sur les plateformes de collaboration, le stockage cloud, les outils d'IA et les frontières de confiance externes. Alice n'avait pas l'intention de causer un problème. Elle essayait simplement de travailler de manière plus intelligente et plus rapide. C'est ce qui rend le risque interne si difficile à gérer : la plupart du temps, il n'est pas malveillant. Il est humain.

Une Nouvelle Approche:
Une Sécurité Qui Suit Les Données

La protection des données sensibles nécessite une approche continue qui s'adapte en temps réel. Pas une liste de contrôle. Pas un ensemble de politiques statiques. Un cycle. **Forcepoint appelle cette approche Data Security Everywhere.**

Découvrir
Établir une visibilité sur les données sensibles où qu'elles se trouvent

Classifier
Identifier le type, l'usage métier et le niveau de sensibilité des données

Prioriser
Concentrer l'attention là où le risque est le plus élevé

La protection des données sensibles n'est pas une liste de contrôle.
C'est un cycle continu.

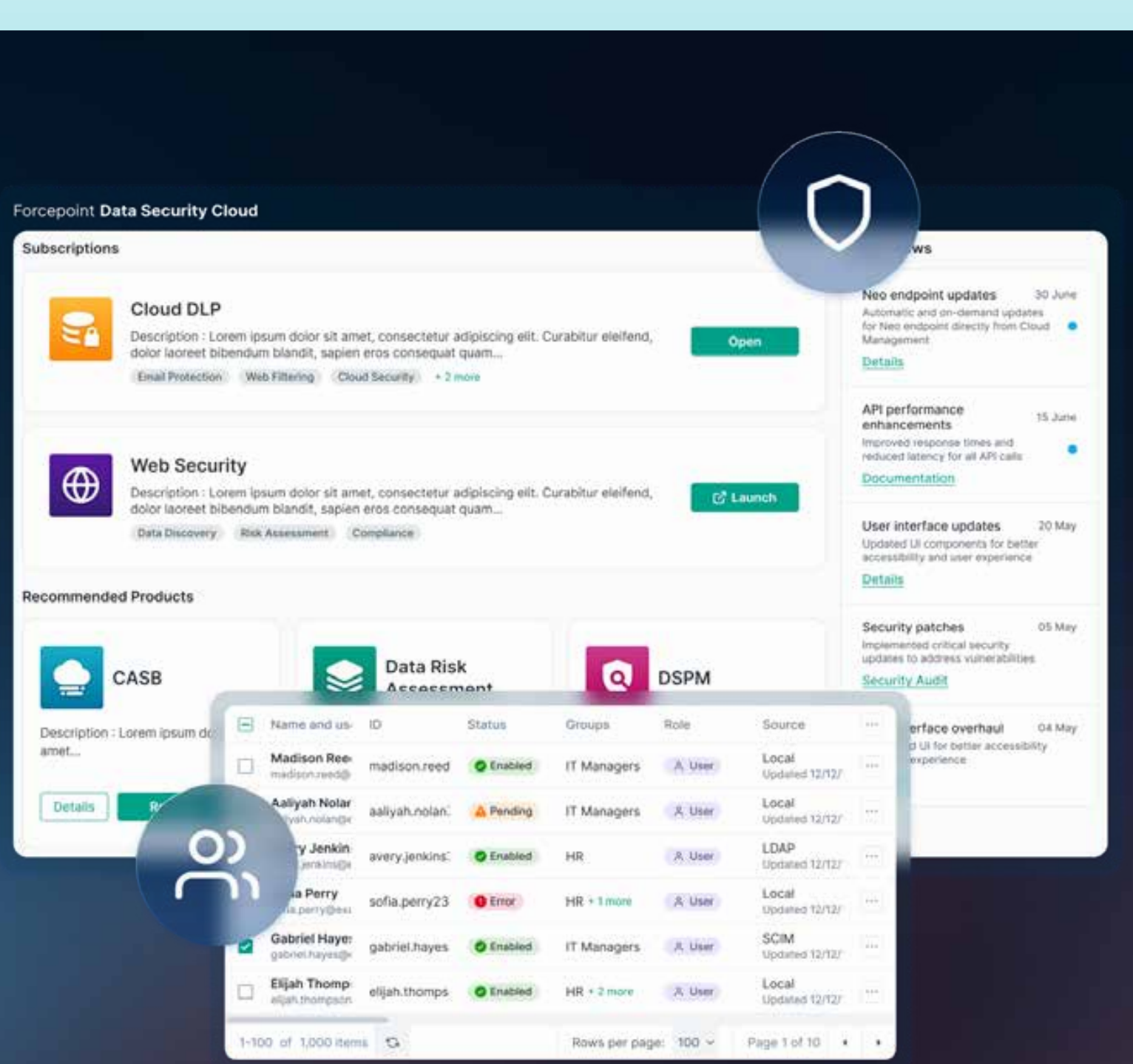
Protéger
Appliquer des politiques de manière cohérente sur tous les canaux pour réduire le risque

Remédier
Traiter les vulnérabilités avant qu'elles ne deviennent des violations

Forcepoint Data Security Cloud

Les cinq étapes se connectent dans une plateforme unifiée : Forcepoint Data Security Cloud. Une seule plateforme. Un seul ensemble de politiques. Une visibilité complète dans chaque environnement où les données vivent, circulent et sont utilisées.

En savoir plus



Forcepoint

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