Forcepoint

يومٌ في حياة البيانات الحساسة

موظفةٌ واحدة. صباحٌ عادي. انفجارٌ هائل في مخاطر البيانات. إليك كيف يحدث ذلك وكيف تمنعه.

المخاطرة موجودة بالفعل

53%

من الحوادث الداخلية ما هو عرضي أو ناتج عن إهمال

تكلفة المخاطر الداخلية DTEX 2026

13%

من الحوادث ما يُحتوى في أقل من 30 يومًا

تكلفة المخاطر الداخلية DTEX 2026

متوسط الوقت اللازم لحل الحوادث الداخلية (الخبيثة والعرضية)

IBM تكلفة تقرير خرق البيانات

+200 يوم

إجمالي متوسط التكلفة السنوية للحوادث الداخلية

تكلفة المخاطر الداخلية DTEX 2026

$19.5 مليون دولار

تعرّف على أليس

أليس مندوبةُ مبيعات تستعدّ لاجتماع شراكة بالغ الأهمية. إنها تؤدي عملها. **لا تحاول إثارة حادثة أمنية**

راقب ما يحدث للبيانات الحساسة بينما تتهيأ للاجتماع

Excel ← Salesforce

تُشغِّل أليس تقريرًا عن أهم حساباتها الاستراتيجية في Salesfroce وتنزّله بصيغة ملف Excel. تتضمن البيانات أسماء الحسابات وجهات الاتصال وأرقام الإيرادات.

تخرج بيانات المعلومات الشخصية الخاضعة للتنظيم، وبيانات الملكية الفكرية، وبيانات الحسابات الاستراتيجية من بيئة CRM الخاضعة للرقابة.

Excel ← السحابة

ترفع الملف إلى منصة تعاون لمشاركته مع فريقها. OneDrive. Box. Sharepoint. لا يهم أيّها.

أصبحت البيانات الحساسة موجودةً في مواقع متعددة في متناول أي شخص يمتلك الصلاحية.

Excel ← الذكاء الاصطناعي العام

تستخدم أليس أداةً للذكاء الاصطناعي متاحةً للعموم لتلخيص الاتجاهات وصياغة نقاط النقاش. ترفع ملف Excel مباشرةً إلى النافذة الحوارية.

جرى رفع بيانات حساسة إلى ذكاء اصطناعي خفيّ مع استعلام عالي المخاطر.

مخرجات الذكاء الاصطناعي ← Slack

تشارك الملخص الذي أنشأه الذكاء الاصطناعي مع فريقها عبر Slack.

ينتشر محتوى جديد يشمل عناصر من البيانات الحساسة في قناة تعاون مشترك .

Slack ← البريد الإلكتروني الخارجي

ترسل أليس الملخص عبر البريد الإلكتروني إلى شريك خارج المنظمة.

تُصدَّر البيانات الحساسة عبر القناة الأعلى خطورة دون أي ضوابط وصول أو تدقيق.

ماذا حدث للتو؟

بيانات PII. الملكية الفكرية. المعلومات الاستراتيجية. في يوم واحد، انتشر كل ذلك عبر منصات التعاون والتخزين السحابي وأدوات الذكاء الاصطناعي وحدود الثقة الخارجية. لم تقصد أليس إثارة أي مشكلة. كانت تحاول ببساطة العمل بذكاء أكبر وسرعة أعلى. هذا هو ما يجعل مخاطر التهديد الداخلي بالغة الصعوبة في الإدارة: معظمها لا يكون خبيثًا. إنه إنساني بطبعه.

نهجٌ جديد:
أمنٌ يتبع البيانات أينما ذهبت

تتطلب حماية البيانات الحساسة نهجًا مستمرًا يتكيّف في الوقت الفعلي. ليس قائمةً للتحقق. ليس مجموعةً من السياسات الثابتة. بل دورةً متكاملة.

يُسمّي Forcepoint هذا النهج Data Security Everywhere

اكتشاف

تأسيس رؤية شاملة للبيانات الحساسة أينما

تصنيف

تحديد نوع البيانات واستخدامها التجاري

تحديد الأولويات

تركيز الاهتمام على المناطق الأعلى خطورة

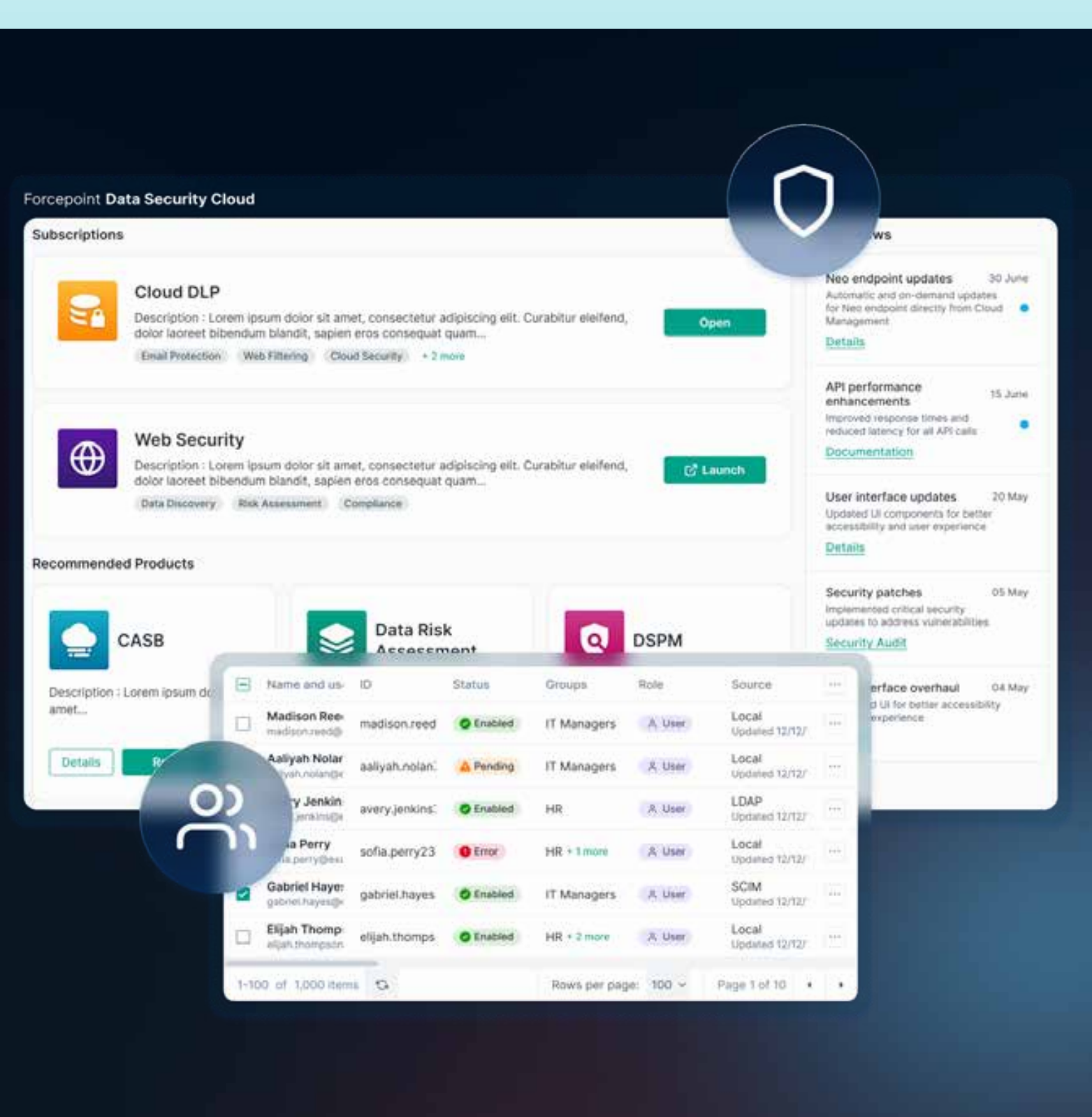
حماية البيانات الحساسة ليست قائمةَ تحقّق. إنها دورةٌ مستمرة.

حماية

تطبيق السياسات بصورة متسقة عبر جميع القنوات للحدّ من المخاطر

المعالجة

معالجة نقاط الضعف قبل أن تتحول إلى اختراقات



Forcepoint Data Security Cloud

تتكامل الخطوات الخمس في منصة موحدة واحدة: Forcepoint Data Security Cloud. منصةٌ واحدة. مجموعةٌ واحدة من السياسات. رؤيةٌ شاملة في كل بيئة تعيش فيها البيانات وتتنقل وتُستخدم.

اكتشف المزيد

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

Forcepoint