

Forcepoint Data Security Cloud

دمج الشفافية وسهولة التحكم للاستمتاع بسلسلة Data Security Everywhere

مكّن الأشخاص من استخدام الملكية الفكرية والبيانات الحساسة للابتكار بثقة وتمكن في الوقت نفسه من خفض التكاليف ومستوى التعقيد المرتبطين بحماية البيانات الحساسة. قلل مخاطر انتشار البيانات عبر السحابة والذكاء الاصطناعي التوليدي والأجهزة البعيدة.

الرهانات

أصبحت حالات اختراق البيانات أكثر شيوعًا وأكثر تطورًا، لكن ليس من الضروري أن تحدث لك. وتكلفة عدم القيام بأي شيء هي تكلفة الاختراق، وقد كلفت المؤسسات العام الماضي ما متوسطه 5 ملايين دولار، بحسب شركة IBM. ولعل الأهم: يمكن أن يؤدي فقدان ثقة العملاء إلى فقدان العملاء، وتأخر الصفقات مع العملاء الحاليين والمستقبليين، وربما حتى انهيار العلاقات مع الشركاء. قد يؤدي ضعف الوضع الأمني العام إلى ارتفاع أقساط التأمين السيبراني. في الحالات القصوى، قد يرفض الموفرون التغطية حتى.

البيانات هي شريان حياة الأعمال

تعاني المؤسسات اليوم من طفرة في البيانات، مدفوعة بالتبني السريع للحوسبة السحابية والذكاء الاصطناعي التوليدي. تعمل هذه التقنيات القوية على تحويل الشركات، مما يتيح التحليلات المتقدمة والأتمتة والخدمات المخصصة. مع ذلك، فإن انفجار البيانات هذا يأتي مصحوبًا بجانب مظلم: الارتفاع الكبير في حالات اختراق البيانات.

التحدي

إن التحدي المتمثل في تأمين البيانات الهائلة والمتناثرة والامتثال للوائح الخصوصية أمر شاق. وقد يؤدي الفشل في القيام بذلك إلى خسائر مالية كبيرة وفقدان ثقة العملاء وعقوبات تنظيمية. هذه لحظة حاسمة يتحتم فيها على المؤسسات إيجاد حل لا يسخر فقط قوة التقنيات الجديدة مثل الذكاء الاصطناعي التوليدي إنما أيضًا يحمي أصولها الأكثر قيمة، ألا وهي البيانات.

ومع تزايد وتيرة التغيير في هذا العالم الهجين المدفوع بالذكاء الاصطناعي، فإن الخصوم يزدون من قدراتهم يوميًا. في الواقع، هذا العام فقط، أصدر المتسللون خدمة تصيد احتيالي كخدمة تُعد باستنساخ أي موقع ويب بدقة مذهلة. باستخدام الذكاء الاصطناعي، يمكنهم بعدها إنشاء هجمات تصيد مخصصة باستخدام هذه المواقع المستنسخة خلال عشر دقائق فقط. أصبح من الأسهل أيضًا خداع الأشخاص لمشاركة البيانات التي لا ينبغي لهم مشاركتها. اليوم، يعتمد الموظفون على عدد متزايد باستمرار من التطبيقات والخدمات التي قد تعرض بياناتك للخطر.



Forcepoint Data Security Cloud

نقاط التحكم



نقطة نهاية



الذكاء الاصطناعي التوليدي



الويب



تطبيقات SaaS



IaaS / PaaS



الخدمات



البريد الإلكتروني



التطبيقات الخاصة

البيانات في وضع السكون

البيانات قيد الاستخدام

البيانات قيد التنقل

الحماية المتقدمة

السياسات القادرة على التكيف مع المخاطر والتطبيق

تصنيف الذكاء الاصطناعي

التحليلات المتقدمة

الإدارة الموحدة

إدارة السحابة

إدارة On-prem

واجهة برمجة التطبيقات / السوق

وكيل واحد

مكتمل مع

← الهوية

← نظام التذاكر

← SIEM

← SOAR

← XDR

زيادة الإنتاجية | خفض التكاليف | الحد من المخاطر | تبسيط جوانب الامتثال

Forcepoint Data Security Cloud مشغل بواسطة Data Security Everywhere

وعلى عكس الحلول المجزأة ذات الثغرات والتكرار التي تفتقر إلى القدرة على تصنيف البيانات وفهمها تلقائيًا وبدقة، والتي تغطي عددًا قليلًا فقط من القنوات أو لديها حماية غير مكتملة على القنوات الحيوية مثل نقاط النهاية، تجمع Forcepoint Data Security Cloud بين الرصد فائق السرعة والتصنيف وتحديد الأولويات والمعالجة المدعومة بالذكاء الاصطناعي مع قدرات منع فقدان البيانات الرائدة في الصناعة، من نقاط النهاية إلى السحابة وكل ما بينها.

تقدم AI Mesh الفريدة من نوعها الخاصة بـ Forcepoint Data Security Cloud أعلى مستويات الدقة وأفضل سياق لإدارة البيانات والحفاظ على أمانها؛ وتقوم risk-adaptive protection الرائدة بأتمتة عملية إنفاذ السياسات وتبسيطها، كما توفر تغطيتها الواسعة للقنوات والمراقبة المستمرة صورة أفضل عن المخاطر الديناميكية التي تواجه البيانات الحساسة أينما يتم الوصول إليها واستخدامها.

لهذا السبب، يجب الآن أكثر من أي وقت مضى أن نوقف المخاطر التي تواجه البيانات الحساسة قبل أن تتحول إلى حالات اختراق، وذلك من خلال منصة مثل Forcepoint Data Security Cloud.

Forcepoint Data Security Cloud هي منصة أمان مدعومة بالذكاء الاصطناعي وتعمل على السحابة، تجمع ما بين الشفافية وسهولة التحكم في البيانات الحساسة للاستمتاع بسلسلة حماية البيانات في كل مكان. وهي تتيح إدارة سياسات الشفافية والتحكم عبر كل القنوات الرئيسية من مكان واحد. كما تراقب باستمرار البيانات الحساسة أثناء استخدامها وعدم استخدامها ونقلها، مما يسمح للمؤسسات برصد مخاطر البيانات والاستجابة لها قبل أن تصبح حالات اختراق. يدمج Forcepoint Data Security Cloud بين حماية البيانات والحماية المتقدمة من التهديدات لحماية المعلومات الحساسة ومنع البرامج الضارة من الوصول إلى البيانات الحساسة.