Forcepoint

Cloud Access Security Broker

تأمين البيانات الموجودة في أي تطبيق عبر الخدمة السحابية، التي يمكن الوصول إليها من أي جهاز

التحدي

- الحماية والتحكم في الوصول إلى التطبيقات المُدارة من الأجهزة الشخصية
- التحكم في تحميل البيانات الحساسة وتنزيلها في أي تطبيق من تطبيقات SaaS المُدارة
- إيقاف البرامج الضارة المخفية في ملفات بيانات الأعمال
- الكشف عن تقنية المعلومات في الظل والتحكم فيها

الحل

- أمان تطبيقات SaaS مع تقنية DLP المدمجة والحماية المتقدمة من التهديدات
- الوصول الدقيق إلى خدمة Zero Trust والتحكم في البيانات استنادًا إلى المستخدم أو الجهاز أو الموقع
- تزيد منصة AWS فائقة التحجيم من وقت التشغيل وتقلل من زمن الاستجابة
- إنفاذ خدمة DLP عبر الأجهزة المُدارة وغير المُدارة

لنتيجة

- زيادة الإنتاجية، مما يتيح للأشخاص استخدام المعلومات في أي مكان بسلاسة وأمان
- تقليل المخاطر من خلال التحكم في البيانات الحساسة في الخدمة السحابية وإيقاف البرامج الضارة
- تقليل التكاليف من خلال تبسيط عمليات الأمان باستخدام مكان واحد لتعيين السياسات
- تبسيط الامتثال مع العمليات القابلة للإثبات للتحكم في المعلومات

تتطلب نماذج القوى العاملة الجديدة اليوم أن يتمتع المستخدمون في أي مكان بوصول سريع إلى بيانات الأعمال، كما تفرض التحكم في الوصول إلى هذه البيانات في كل مكان. وهذا يعني أن الأفراد يحتاجون إلى الوصول إلى البيانات في تطبيقات SaaS مثل Microsoft 365 و Google Workspace و Slack و Jira و Salesforce بغض النظر عن موقعهم أو نوع الجهاز المُستخدَم. ومع وجود أكثر من 250 تطبيقًا من تطبيقات SaaS للمؤسسات العادية، أصبح من الصعب إدارة الرؤية والتحكم بسهولة.

حماية الوصول إلى تطبيقات الأعمال من الأجهزة الشخصية وغير المُدارة

تُبسِّط Forcepoint إدارة الأمان عبر الخدمة السحابية. تتيح خدمة أمن CASB التابعة لـ Forcepoint ONE الوصول إلى Zero Trust الذي يتيح استخدام تطبيقات SaaS الحيوية للأعمال بشكل آمن من الأجهزة الشخصية للموظفين (BYOD) والأجهزة غير المُدارة التابعة للشركاء والمتعاقدين.

التحكم في تحميل البيانات الحساسة وتنزيلها في أي تطبيق من تطبيقات SaaS المُدارة

نقدم لك مجموعة واحدة من سياسات الأمان للتحكم في البيانات الحساسة، مع الأداء الرائد في المجال بغض النظر عن مكان وكيفية اتصال الموظفين والمتعاقدين بالإنترنت. تسهل إدارة الوصول إلى هذه التطبيقات من الأجهزة المحمولة عملية التكيف والإنتاجية، بينما توفر سياسات مختلفة تستند إلى الهوية والموقع عناصر تحكم دقيقة في Zero Trust. إن الفحص المضمن للبيانات الحساسة والبرامج الضارة يحافظ على أمان البيانات عبر جميع تطبيقات SaaS. يمكنك الحصول على مزيد من الضمان حول كيفية مشاركة البيانات السرية في تطبيقات الشركة، ومع دمج ميزة Data Loss Prevention (DLP)، لا تحتاج إلى توجيه المنتجات لإيقاف انتهاكات البيانات.

إيقاف البرامج الضارة المخفية في ملفات بيانات الأعمال

يمكن لـ Forcepoint ONE CASB اكتشاف البرامج الضارة في البيانات التي يتم تمريرها بين المستخدمين وتطبيق SaaS وحظرها باستخدام محركات البرمجيات الضارة من عدة محركات لمكافحة البرمجيات الضارة تابعة لجهات خارجية. ويمكنها أيضًا الكشف عن البرامج الضارة في الملفات الموجودة في تخزين SaaS و IaaS الشهير وعزل تلك الملفات.

الكشف عن حالات استخدام تكنولوجيا المعلومات دون خبرة

تتيح خدمة Forcepoint ONE CASB تقنية معلومات الظل وتُقدِّم درجة تقييم المخاطر للتطبيقات غير المُصرَّح بها من خلال تحليل سمات متعددة. يتيح ذلك لفرق تقنية المعلومات الحصول على فهم أعمق لاستخدام SaaS داخل مؤسستهم وفرض عناصر التحكم في الأمان اللازمة. تكشف خدمة CASB عن تطبيقات SaaS غير المُدارة المستخدمة باستخدام سجلات الشبكات من جدران الحماية والوكلاء في الشركات لتمكين تطبيق سياسات أمان متسقة على تطبيقات SaaS المُصرَّح بها وغير المُصرَّح بها، بحيث تظل بيانات الأعمال آمنة في أي مكان يتم استخدامها فيه.

حل SaaS الأمني الذي يزيد من وقت التشغيل والإتاحة والإنتاجية

تم تصميم خدمة CASB لدينا على بنية معتمدة على الخدمة السحابية الأصلية وقائمة على بنية فائقة السرعة مع أكثر من 300 نقطة حضور (PoPs) و إمكانية الوصول العالمية ووقت تشغيل مثبت بنسبة 99.99% لتأمين تطبيقات SaaS بسلاسة والحفاظ على إنتاجية المستخدمين. هناك حلول أخرى تُحوِّل حركة مرور الشبكات من تطبيقات SaaS و إليها إلى مراكز بيانات خاصة بدلاً من المواقع الأقرب إلى المستخدمين والتطبيقات التي يمكنهم الوصول إليها. ويؤدي ذلك إلى ضعف الأداء، ما يتسبب في فشل التطبيقات التي تراعي زمن الاستجابة للاختراق، مثل Slack، ما يدفع الموظفين إلى البحث عن حلول بديلة عالية المخاطر.

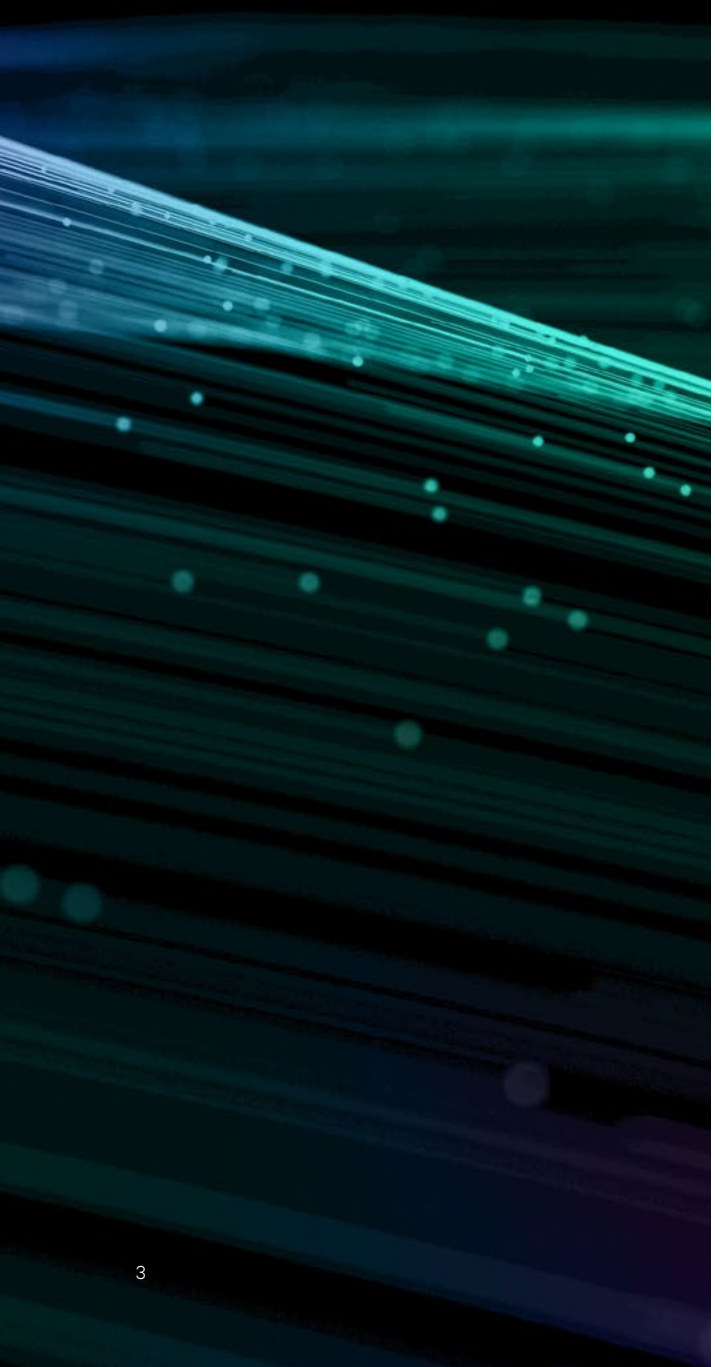
تأمين البيانات في كل مكان، للأشخاص الذين يعملون في أي مكان

تبسيط أمان الخدمة السحابية في العالم الحقيقي

من وحدة تحكم واحدة، يمكن للمسؤولين إدارة الوصول والتحكم في البيانات لمستخدمي الأجهزة المُدارة وغير المُدارة على حد سواء (مثل لأجهزة الشخصية وأجهزة كمبيوتر المتعاقدين أو الشركاء).

لنرى كيف تبسط خدمة CASB أمن الخدمة السحابية عندما يبدأ Kris، وهو محلل أعمال يعمل من المنزل، يوم عمله.

يسجل Kris في حساب Salesforce الخاص به من الكمبيوتر المحمول الذي تقدمه له الشركة.	تدير خدمة CASB في خدمة Forcepoint ONE الاتصالات بتطبيقات الأعمال، مما يتيح للمستخدمين التسجيل بسلاسة وأمان.
يتصفح Kris مباشرةً Salesforce.com أو من خلال بوابة تطبيقات الشركات.	تعيد Salesforce توجيه الجلسة إلى خدمة CASB (من خلال خدمة SAML)، مما يحلل ما إذا كان الجهاز يخضع لإدارة وموقع والوضع الأمني الخاص به. واستنادًا إلى سياسات الأمان المحددة مسبقًا، تؤكد خدمة CASB هوية Kris من خلال التوثيق المتعدد العوامل.
مُنح Kris حق الوصول إلى التطبيقات المُدارة.	تتحكم سياسات الإشراف كذلك في الوصول المباشر إلى التطبيق أو الوصول المتحكم فيه أو عدم الوصول على الإطلاق. يحدث هذا في غضون أجزاء من الثانية دون التأثير على إنتاجية الموظفين. يتم نقل جميع الزيارات من جهاز Kris والتطبيق عبر خدمة CASB (باستخدام وكيل معكوس أو إعادة توجيه).
يقرر Kris تنزيل توقعات الإيرادات من Salesforce.	تفحص خدمة CASB أي ملف تم تنزيله من التطبيق بحثًا عن البرامج الضارة والبيانات الحساسة. تبعًا للنتيجة والسياسة، يمكنها حظر ملفات البرامج الضارة وحظر البيانات الحساسة أو تتبعها أو تشفيرها. إذا كانت إحدى السياسات تقيد تنزيل البيانات الحساسة على الأجهزة غير المُدارة، فإن التنزيل مسموح به نظرًا لأن Kris يستخدم جهاز كمبيوتر محمول تابع للشركة.
يحاول Kris نقل بيانات حساسة أو ملف مصاب ببرامج ضارة عبر Slack.	كما يمكن لخدمة CASB التحقق من الملفات التي يتم تحميلها في تطبيقات SaaS. يمكن لخدمة CASB حظر التحميل تلقائيًا. ويمكنها حتى حظر تحميل الملفات إلى التطبيقات غير المُصرَّح بها باستخدام الوكيل المُوحَّد على الجهاز.



جزء من نهج Forcepoint لأمن البيانات في كل مكان

تمكّن مهمة أمن البيانات في كل مكان من Forcepoint المؤسسات من حماية البيانات عبر CASB والويب والبريد الإلكتروني والشبكة ونقاط النهاية، بحيث يمكن للأفراد العمل بأمان في أي مكان باستخدام البيانات في كل مكان.

توسيع إمكانات تقنية DLP الرائدة في المجال لتشمل تطبيقات SaaS

تمع Forcepoint، يمكن للمؤسسات استخدام سياسات تقنية Forcepoint DLP الحالية لتأمين البيانات في تطبيقات SaaS، ما يوسع نطاق أمن البيانات الرائد في المجال نفسه ليشمل الخدمة السحابية ببضع نقرات بسيطة. تساعد سياسات تقنية SaaS المُوحَّدة التي يتم تطبيقها من وحدة تحكم واحدة في توفير أمن بيانات متسق في المؤسسة لتطبيقات SaaS، وتبسيط إدارة أمن البيانات، وتقليل الاختراقات، مع تبسيط الامتثال. ويمكن للعملاء جني الفوائد الآتية من خلال هذا الدمج:

- تبسيط أمن البيانات السحابية مع سياسات ووحدة تحكم مُوحَّدة.
- تم إصدار 1700 أداة تصنيف وقالب سياسات لتوفير تغطية شاملة ودعم الامتثال لأكثر من 150 منطقة.
- إعداد التكوين مع وقت وصول إلى القيمة خلال دقائق، ما يحسن إنتاجية فرق تقنية المعلومات/أمن المعلومات.
- التخلص من منتجات الأمان الزائدة عن الحاجة والمجزأة لتحقيق وفورات كبيرة في التكاليف.

راجع كتيب Forcepoint DLP للحصول على مزيد من التفاصيل.

هل أنت جاهز لتأمين البيانات في تطبيقات الخدمة السحابية من أي جهاز؟

لنبدأ مع عرض توضيحي

forcepoint.com/contact