Forcepoint

Cloud Access Security Broker

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

تشترط نماذج القوى العاملة الجديدة اليوم على المستخدمين في أي مكان التمتع بالوصول السريع إلى بيانات الأعمال في كل مكان، مع ذلك التحكم في الوصول إلى هذه البيانات في كل مكان. يعني هذا أن الأشخاص يحتاجون إلى الوصول إلى البيانات الموجودة في تطبيقات الخدمة السحابية مثل Microsoft 365 وGoogle Workspace و Slack وJira وSalesforce من أي نوع من الأجهزة أو المواقع. مع وجود أكثر من 250 تطبيق من تطبيقات SaaS من أجل رؤية وتحكم متوسطي المستوى للمؤسسات، فإنها قد تصبح غير قابلة للإدارة بسهولة.

حماية الوصول إلى تطبيقات الأعمال من الأجهزة الشخصية وغير المُدارة

تبسط Forcepoint الأمان عبر الخدمة السحابية. توفر خدمة أمان CASB التابعة لـ Forcepoint ONE إمكانية الوصول إلى خدمة Zero Trust التي تتيح الاستخدام الآمن لتطبيقات الخدمة السحابية المهمة للأعمال 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 لخدمة Forcepoint ONE CASB اكتشاف البرامج الضارة في البيانات التي يتم نقلها بين المستخدمين وتطبيق SaaS وحظرها باستخدام محركات البرامج الضارة من Bitdefender و Trellix. 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 تكنولوجيا معلومات الظل وتقدم درجة تقييم المخاطر للتطبيقات غير الخاضعة للرقابة من خلال تحليل سمات متعددة. يتيح ذلك لفرق تكنولوجيا المعلومات الحصول على فهم أعمق لاستخدام SaaS داخل مؤسستهم وفرض عناصر التحكم الأمنية اللازمة. تكشف خدمة CASB عن تطبيقات SaaS غير المُدارة المستخدمة بالاستفادة من سجلات الشبكات أو مع القياس عن بُعد من خدمة Forcepoint ONE Security Web Gateway لتمكين تطبيق سياسات الأمان المتسقة على تطبيقات SaaS الخاضعة للمعاقبة وغير الخاضعة للمعاقبة، بحيث تظل بيانات الأعمال آمنة في أي مكان يتم استخدامها.

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 حالات استخدام تكنولوجيا المعلومات دون خبرة

الحل

- أمان التطبيقات عبر الخدمة السحابية مع خدمة 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

تزيد خدمة CASB في خدمة Forcepoint ONE من وقت التشغيل والتوافر والإنتاجية

إن خدمة CASB لدينا هي جزء من خدمة Forcepoint ONE، وهي منصة الخدمة السحابية القائمة على خدمة Hyperscaler والتي تضم أكثر من 300 نقطة حضور وسهولة وصول عالمية ووقت تشغيل مثبت بنسبة 99.99% لتأمين تطبيقات الخدمة السحابية بسلاسة والحفاظ على إنتاجية المستخدمين. الحلول الأخرى التي تحول حركة مرور الشبكة من وإلى تطبيقات الخدمة السحابية إلى مراكز البيانات الخاصة بدلاً من المواقع الأقرب إلى المستخدمين والتطبيقات التي يمكنهم الوصول إليها. وهذا يؤدي إلى ضعف الأداء، مما يتسبب في فشل التطبيقات التي تراعي زمن الاستجابة مثل خدمة Slack وفي البحث عن حلول عالية المخاطر

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

تبسيط أمان الخدمة السحابية في العالم الحقيقي

توفر منصة Forcepoint ONE السحابية "خدمة سهلة" لتنفيذ أمن الخدمة السحابية.

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.	يمكن لخدمة CASB أيضًا التحقق من الملفات التي يتم تحميلها في تطبيقات الخدمة السحابية. يمكن لخدمة CASB حظر التحميل تلقائيًا. ويمكنها حتى حظر تحميل الملفات إلى التطبيقات غير الخاضعة للرقابة باستخدام الوكيل الموحد على الجهاز.

جزء من حل أمني موحد للتطبيقات على الويب والخدمة السحابية والتطبيقات الخاصة

بالإضافة إلى خدمة CASB ، تؤمن منصة Forcepoint One الشاملة الوصول إلى معلومات الأعمال على أي موقع ويب وتطبيق خاص:

- **الويب:** تراقب بوابة الويب الآمنة التفاعلات مع أي موقع ويب وتتحكم فيها بناءً على المخاطر والفئة، مما يحظر تنزيل البرامج الضارة أو عمليات تحميل البيانات الحساسة إلى مشاركة الملفات الشخصية وحسابات البريد الإلكتروني. تفرض بوابة الويب الآمنة التابعة لنا سياسات الاستخدام المقبول على الأجهزة المُدارة الموجودة في أي مكان.
- **التطبيقات الخاصة:** يؤمن الوصول إلى شبكات الثقة الصفرية ويبسط الوصول إلى التطبيقات الخاصة دون التعقيد أو المخاطرة المرتبطة بالشبكات الافتراضية الخاصة.
- **إمكانات إضافية،** مثل فحص مزودي الخدمة السحابية بحثًا عن التكوينات الخطرة في الخدمة السحابية لإدارة أوضاع الأمان (CSPM) وإدارة أوضاع الأمان (SSPM) من SaaS حسب الحاجة.

اقرأ موجز حل Forcepoint ONE للحصول على مزيد من التفاصيل.

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

لنبدأ مع عرض توضيحي

forcepoint.com/contact