Forcepoint ONE: تبسّط منصة الخدمة السحابية الأمان من أجل قوى عاملة هجينة

أمن البيانات أولًا

يزداد الأمن تعقيدًا، ولكن هناك طريقة أفضل. يعمل المستخدمون الآن من أي مكان باستخدام البيانات المنتشرة في كل مكان - في مواقع الويب وتطبيقات السحابة والتطبيقات الخاصة.

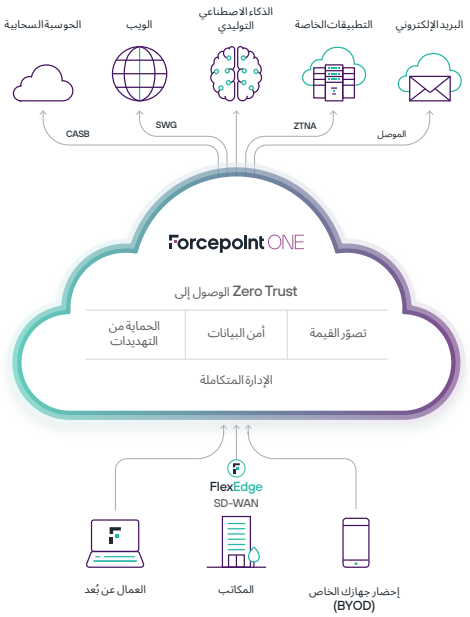
من أجل دعم مبادرات العودة إلى المكتب وفرق أمان القوى العاملة الهجينة تحتاج إلى منصة الأمن المتقارب التي تضع البيانات في مركز الصورة. يجب أن تكون عناصر التحكم في الأمن قادرة على التوسع عبر شبكة الويب والخدمة السحابية والوصول إلى التطبيقات الخاصة مع رؤية وتحكم متسقين بحيث يمكن للمؤسسات نقل الخسارة لوقف فقدان البيانات قبل.

وبفضل الحل المعتمد على البيانات في المقام الأول، يمكن تأمين بيانات الأعمال في كل مكان لجميع .العاملين في أي مكان.

Forcepoint ONE تبسط الأمن

إن خدمة Forcepoint ONE هي منصة سحابية متكاملة توفر الأمان بكل بساطة. ويمكنك بسرعة استخدام خدمات Zero Trust و Security Service Edge (خدمة SSE، المكون الأمني لـ SASE) لأننا جمعنا سويًا الخدمات الأمنية المهمة، بما في ذلك SWG، CASB، وZTNA.

إطلاق العنان للإنتاجية من خلال الاستفادة بأمان من التقنيات الجديدة مثل الذكاء الاصطناعي التوليدي (GenAI) من خلال التحكم في الوصول إلى أنواع مختلفة من مواقع GenAI وفرض حواجز الحماية بشكل مستمر لحماية البيانات الدقيقة ومنع التضرر من البرامج الضارة.



حالات الاستخدام

- اكتساب الرؤية والتحكم في تفاعلات القوى العاملة الهجينة باستخدام البيانات الموجودة في شبكة الويب والخدمة السحابية والتطبيقات الخاصة
- منع إساءة استخدام البيانات الحسّاسة التي يتم الوصول إليها من الأجهزة المُدارة أو غير المُدارة.
- التحكم في الوصول إلى محتوى الويب عالي المخاطر والأنواع المختلفة من مواقع الذكاء الاصطناعي التوليدي (GenAI).
- توفير الوصول الآمن والسريع عن بُعد إلى موارد الأعمال والتطبيقات الخاصة دون تعقيد الشبكات الافتراضية الخاصة (VPN).

الحل

- تتيح منصة واحدة وموحدة إدارة سياسات الأمان المتسقة عبر جميع تطبيقات الأعمال.
- الخدمة الشاملة المُقدّمة عبر الخدمة السحابية التي تحمي الوصول والبيانات من خلال الجمع بين وسيط الوصول إلى الخدمة السحابية لبوابة الحماية من المواقع الإلكترونية الضارة والوصول إلى الشبكة صفرية الثقة
- الحماية المتقدمة المتكاملة من التهديدات وأمن البيانات لإبعاد المهاجمين وإبقاء البيانات الحسّاسة بداخلها.
- قدرات إضافية مثل RBI مع CDR للوصول إلى مواقع الويب صفرية الثقة و CSPM لفحص مستأجري الخدمة السحابية العامة بحثًا عن التكوينات الخطيرة.
- خدمة Forcepoint Classification لوضع علامات على البيانات.

النتيجة

- التبسيط - تجمع الخدمة بين جوانب الأمان للويب والخدمة السحابية والتطبيقات الخاصة في منصة موحدة (دون الحاجة إلى دعم الوكلاء).
- الحديثة - تجمع بين مبادئ الثقة الصفرية وبنية حافة خدمة الوصول الآمن والأمان المتقدم مثل عزل المتصفح عن بُعد وتعقيم الملفات التي تم تنزيلها.الحماية المتقدمة المتكاملة من التهديدات وأمن البيانات لإبعاد المهاجمين وإبقاء البيانات الحسّاسة بداخلها.
- في كل مكان - متاح على مستوى العالم، بأكثر من 300 نقطة حضور (PoPs).
- موثوقة - توفر وقت تشغيل بنسبة 99.99% منذ عام 2015.
- سريعة - تستخدم الإنفاذ الموزع والتدرج التلقائي للقضاء على نقاط الاختناق.

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

تتضمن قدرات الثقة الصفرية الأصلية السحابية في Forcepoint ONE ما يلي:

- **أمن الحيلولة دون فقدان البيانات بدون وكيل للسحابة والتطبيقات الخاصة.** استخدام تطبيقات الويب الخاصة للأعمال بأمان من الأجهزة الشخصية، مع الحفاظ على أمان البيانات الحساسة.
- **الحماية المتكاملة المتقدمة ضد التهديدات وأمان** البيانات. منع فقدان البيانات أو تسريبها وإيقاف المتسللين من الوصول إلى البيانات باستخدام عناصر تحكم متسقة في كل مكان.
- **بوابات موحدة للوصول إلى الخدمة السحابية والويب والتطبيقات الخاصة.** التحكم في الوصول المستند إلى الهوية إلى تطبيقات الأعمال المُدارة في مكان واحد لكل من بوابة الويب الآمنة ووسيط أمن الوصول السحابي والوصول إلى الشبكات صفرية الثقة.
- **قابلية التوسع الديناميكية مع الوصول العالمي.** توفر 300 نقطة حضور مبنية على خدمات أمازون ويب اتصالًا سريعًا ومنخفض زمن الاستجابة ووقت تشغيل بنسبة 99.99% بغض النظر عن مكان عمل الأشخاص.

الأمن الموحد للويب والخدمة السحابية والتطبيقات الخاصة

- **السحابة:** يفرض وسيط أمن الوصول السحابي الوصول الدقيق إلى تطبيقات للشركات والبيانات من أي جهاز. يحظر وسيط أمن الوصول السحابي تنزيل البيانات الحساسة ويحظر تحميل البرامج الضارة في الوقت الحقيقي. يمسح البيانات في حالة سكون SaaS و IaaS الشائعة بحثًا عن البرامج الضارة والبيانات الحساسة والمعالجات حسب الحاجة. يكتشف وسيط أمن الوصول السحابي تطبيقات تقنية المعلومات الظلية ويتحكم في الوصول من أي جهاز مُدار.
- **الويب:** تراقب خدمة SWG وتتحكم في التفاعلات مع أي موقع ويب بناءً على المخاطر والفئة، وتحظر تنزيل البرامج الضارة أو تحميل البيانات الحساسة إلى حسابات مشاركة الملفات الشخصية والبريد الإلكتروني. إن أمان الويب على أجهزتنا يفرض 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.

أمن البيانات والحماية من التهديدات على نطاق واسع

- **الحيلولة دون فقدان البيانات:** تخضع الملفات والنصوص عند تحميلها وتنزيلها للفحص بحثًا عن بيانات حساسة ويتم حظرها أو تتبعها أو تشفيرها أو تنقيحها حسب الاقتضاء. تساعد أكثر من 190 قاعدة محددة مسبقًا عمن قواعد الحيلولة دون فقدان البيانات على تبسيط الامتثال التنظيمي وتوفير وقت سريع للقيمة. يتيح التكامل السهل مع قواعد الحيلولة دون فقدان البيانات للشركات من Forcepoint أمن البيانات في كل مكان - على نقطة النهاية وفي الشبكة وعلى الويب وفي الخدمات السحابية.
- **فحص البرامج الضارة:** تخضع الملفات عند تحميلها وتنزيلها للفحص بحثًا عن البرامج الضارة ويتم حظرها عند اكتشافها.

الرؤية والتحكم المتكاملين

- **مجموعة الإدارة المتكاملة** للتكوين والمراقبة والإبلاغ عبر قنوات SSE.
- **سياسات تسجيل الدخول** للتحكم في الوصول إلى تطبيقات الويب أو الخدمة السحابية أو التطبيقات الخاصة بناءً على موقع المستخدم ونوع الجهاز ووضعية الجهاز وسلوك المستخدم ومجموعة المستخدمين. تساعد هذه المعلمات في منع عمليات الاستيلاء على الحسابات.
- **سياسات DLP سهلة الاستخدام** للتحكم في تنزيل وتحميل البيانات والبرامج الضارة لتطبيقات SaaS المدارة والتطبيقات الخاصة ومواقع الويب، بالإضافة إلى البيانات المخزنة في SaaS و IaaS المُدارة.
- **وكيل على الجهاز** لنظامي التشغيل Windows وMacOS لدعم SWG، أو CASB، أو CASB لتطبيقات العملاء غير المرتبطة بالمتصفح والتحكم في تكنولوجيا معلومات الظل.
- **التحليلات الموحدة وتصوير القيمة** للحصول على رؤى سريعة حول المخاطر الأمنية والاستخدام العام وتأثير منصة أمن الخدمة السحابية الشاملة.

القدرات الإضافية المتاحة حسب الحاجة

- **إدارة وضع أمن الخدمة السحابية:** بفحص خدمات الويب من AWS و Azure و GCP بحثًا عن التكوينات الخطرة وتوفير المعالجة اليدوية والآلية.
- **إدارة وضع الأمن من SaaS**: بفحص إعدادات مستأجري Salesforce و ServiceNow و Office 365 بحثًا عن التكوينات المحفوفة بالمخاطر وتوفير المعالجة اليدوية والآلية.
- **عزل المتصفح عن بُعد:** : تحمي المستخدم من البرامج الضارة المنقولة عبر الويب على أجهزته المحلية من خلال تشغيل متصفح في جهاز افتراضي مستضاف على الخدمة السحابية. يستخدم مجلس الإنماء والإعمار لتعقيم الملفات التي تم تنزيلها خلال جلسة عزل المتصفح عن بُعد لأي برامج ضارة أو عناصر أجنبية.
- **تصنيف Forcepoint:** تصنيف البيانات باستخدام الاقتراحات المدعومة بالذكاء الاصطناعي لتعزيز دقة التصنيف.
- **AMDP:** يحلل سلوك الملف في برنامج ضار يتم التحكم فيه لتحديد المحتوى المخفي والضار.

الاشتراكات التي تفتح باب البساطة

الاشتراكات السنوية المتاحة لكل مستخدم:

- **الإصدار الشامل** لأمن الويب والخدمة السحابية والتطبيقات الخاصة.
- يتضمن **إصدار أمان** الويب بوابة الويب بالإضافة إلى خدمة CASB المضمنة لتطبيقات الخدمة السحابية غير المحدودة، وRBI الأساسية للمواقع غير المصنفة والمسجلة حديثًا لإضافة دعم واجهة برمجة التطبيقات لتطبيقات الخدمة السحابية والدعم للتطبيقات الخاصة لاحقًا.
- **إصدار الوصول إلى الشبكات صفرية الثقة** يحمي عددًا غير محدود من التطبيقات الخاصة.
- **إصدار وسيط أمن الوصول السحابي** يحمي عددًا غير محدود من تطبيقات الخدمة السحابية المضمنة، ويتضمن واجهات برمجة التطبيقات لثلاثة تطبيقات مع القدرة على إضافة حزم تطبيقات إضافية أو إجراء استطلاعات مخصصة لواجهة برمجة التطبيقات.
- **جميع الاشتراكات** تشمل إدارة الخدمة السحابية المركزية، والسياسات مع منع فقدان البيانات، والوصول الآلي عبر وكيل النقطة النهائية والإبلاغات الشاملة.

forcepoint.com/contact