Forcepoint

Forcepoint Data Security

إن خدمة DLP على مستوى المؤسسات موحدة عبر جميع القنوات الرئيسة ومُدارة ببساطة من الخدمة السحابية.

أضحى أمن البيانات اليوم جزءًا مهمًا من استراتيجية أي شركة. ولكن حين تظن مؤسستك أنها أحكمت سيطرتها على الجانب المرتبط بأمن البيانات، يبرز لها التحدي الجديد: الاستخدام الآمن لتطبيقات الذكاء الاصطناعي التوليدي (GenAI). ومع وجود بيانات هائلة على الأجهزة وبيئات الخدمات السحابية، ومع ظهور تطبيقات الذكاء الاصطناعي التوليدي (GenAI) الآن، قد يبدو أن حماية البيانات الحساسة في عالم الذكاء الاصطناعي مهمة مستحيلة.

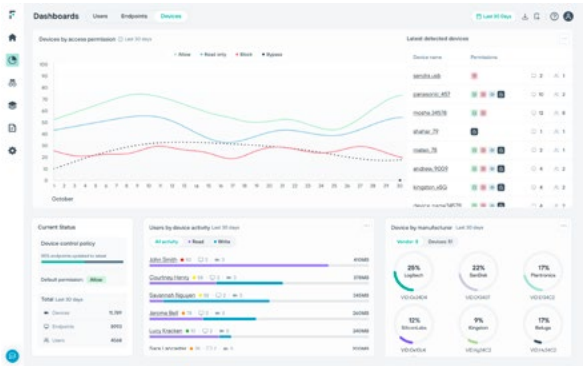
إن خدمة Forcepoint Data Security هي حل DLP معتمد على الخدمة السحابية صُمّم خصيصًا للمؤسسات الحديثة. ويحمي حل DLP SaaS هذا المعلومات الحساسة ويمنع حالات اختراق البيانات ويتيح الامتثال للوائح الخصوصية في جميع أنحاء العالم. يوفر الحل النشر السريع وإدارة السياسات، ويبسط حماية البيانات، ويقدم الإدارة الموحدة عبر تطبيقات الذكاء الاصطناعي التوليدي وتطبيقات الخدمة السحابية والويب والبريد الإلكتروني ونقاط النهاية. توفر خدمة Forcepoint Risk-Adaptive Protection رؤى حول مخاطر المستخدمين في الوقت الفعلي. يمكن الاستمتاع بالتكاليف المنخفضة وتقليل المخاطر وزيادة الإنتاجية مع خدمة Forcepoint Data Security.

التحديد القوي لبيانات Enterprise DLP عبر جميع القنوات

- أكثر من 1700 سياسة أمنية منشأة مسبقا على حسب معايير كل دولة في العالم وعلى طبيعة عمل المنشأة
- معالجة اللغات الطبيعية (NLP)
- الكشف المتقدم الصحيح عن نوع الملفات الذي يغطي أكثر من 900 نوع من الملفات ت

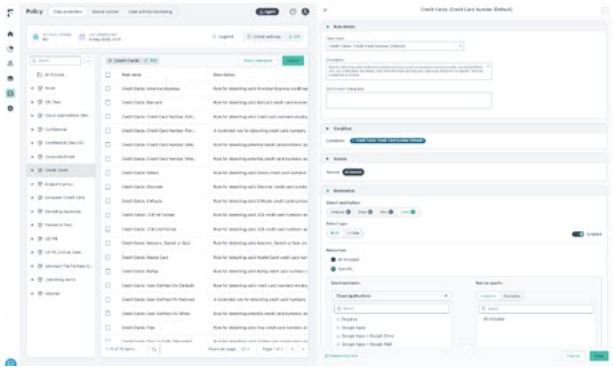
استخدام تطبيقات الذكاء الاصطناعي التوليدي بأمان

ابدأ رحلة التحول إلى الذكاء الاصطناعي اليوم مع Forcepoint، حيث يمكنك زيادة الإنتاجية وتعزيز الكفاءة من خلال الاستخدام الآمن لتطبيقات الذكاء الاصطناعي التوليدي، مثل ChatGPT، و Copilot، و Gemini، وغيرها الكثير. وباستخدام خدمة Forcepoint Data Security، يمكنك تدريب المستخدمين على كيفية استخدام تطبيقات الذكاء الاصطناعي التوليدي استخدامًا صحيحًا، وفحص المعلومات الحساسة وحظرها خلال عمليات التحميل واللصق تلقائيًا، وتسجيل محاولات إساءة الاستخدام للبيانات الحساسة.



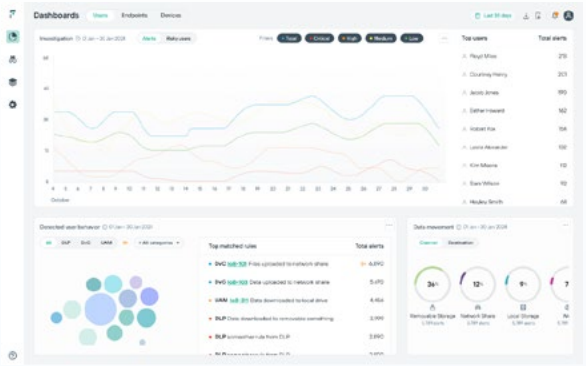
الإدارة الموحدة - "سياسة واحدة تُطبق على الكل"

يمكنك إدارة جميع خدمات Forcepoint بسلاسة من واجهة Forcepoint Data Security إمكانية التحكم في جميع القنوات (CASB و SWG والبريد الإلكتروني ونقطة النهاية) من خلال سياسة واحدة، ما يضمن التوحيد عبر جميع نقاط الخروج الرئيسة. بنقرة واحدة، يمكن نشر سياسة جديدة أو تطبيق سياسة موجودة عبر جميع القنوات الرئيسة. المراقبة بشكل ملائم لحوادث DLP من لوحة معلومات موحدة، ما يتيح لك الحصول على عرض شامل لأمن البيانات عبر مؤسستك



اعدادات وتطبيق السياسات المبسط

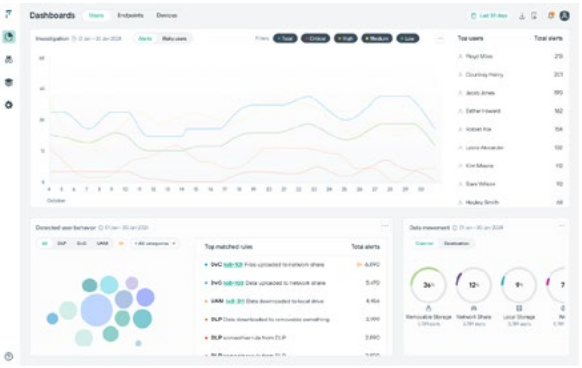
- تبسيط الإدارة باستخدام التحديثات المستمرة للحصول على أحدث السياسات وأدوات التصنيف والقوالب المحددة مسبقًا.
- وضع سياسات ببضع نقرات فقط ونشرها في دقائق بدلًا من ساعات.
- الحصول على سياسات امتثال فريدة لأكثر من 160 منطقة و90 دولة لضمان الامتثال للمعايير الخاصة في كل دولة عالمية.



إدارة سهلة للحوادث والتنبيهات

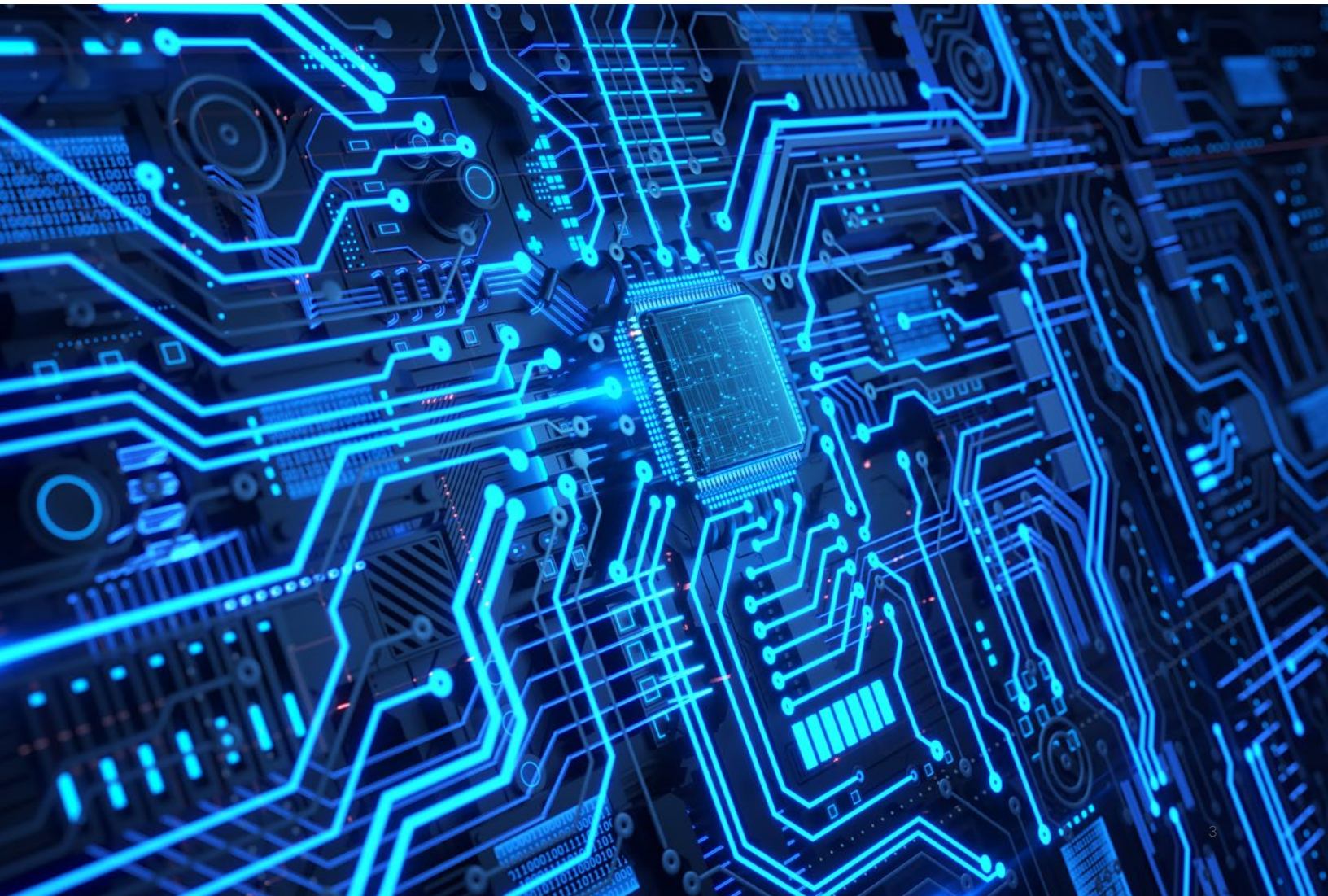
الحصول على عرض كامل لجميع الحوادث والتنبيهات في الوقت الفعلي تقريبًا عبر لوحة معلومات التقارير. بفضل الإمكانية المُضافة لإعداد التقارير، يحصل المسؤولون على عرض شامل عبر تطبيقات الخدمة السحابية وحركة المرور على الويب والبريد الإلكتروني ونقاط النهاية. يعزز التحكم الأصلي في الأجهزة أمن البيانات والتحكم في الوصول للوسائط القابلة للإزالة مثل محركات أقراص USB. تتكامل خدمة Forcepoint Data Security بسلاسة مع خدمة Risk-Adaptive Protection، حيث توفر سياقًا وفهمًا في الوقت الفعلي لنية المستخدم من خلال التركيز على السلوك والتفاعل مع البيانات. تتيح قدرات Forensics إمكانية الحصول على رؤى أعمق حول حركة البيانات، ما يتيح التحقيق الفعال في الحوادث الأمنية لتعزيز إنفاذ السياسات وتبسيط الامتثال. تتم إدارة كل ذلك من خلال وكيل واحد وواجهة مستخدم واحدة.

* يتطلب التكامل مع خدمة Risk-Adaptive Protection (نقطة النهاية مطلوبة للإبلاغ عن درجة المخاطر) وحدة SKU منفصلة (إضافة إلى خدمة Forcepoint Data Security).



حل SaaS المعتمد على الخدمة السحابية

- خفض التكاليف الإجمالية.
- عدم تحمل تكاليف لإعداد الأجهزة والبرامج في الموقع.
- يوفر الحل الأصلي المعتمد على الخدمة السحابية قابلية توسع أكبر وأكثر كفاءة.
- إدارة بسيطة لأمن البيانات مع تحديثات مستمرة إلى الميزات الجديدة وإصلاحات الأخطاء وتصحيحات الأمان.
- التحديثات التلقائية عبر الهواء لنقطة النهاية.
- يتم النشر على AWS عالميًا مع وقت تشغيل بنسبة 99.99% دون أي وقت توقف مجدول.
- مبنية على إنترنت الأشياء AWS لسهولة التوسع واستيعاب مئات الآلاف من نقاط النهاية.



توفر خدمة Forcepoint Data Security حلاً شاملاً لإدارة السياسات العالمية عبر جميع القنوات، بما في ذلك تطبيقات الذكاء الاصطناعي التوليدي وتطبيقات الخدمة السحابية والويب والبريد الإلكتروني ونقاط النهاية. وبفضل توفر مجموعة كبيرة من القوالب والسياسات وأدوات التصنيف المحددة مسبقًا، فإننا نبسط عبء العمل لديك، مما يتيح إدارة الحوادث بشكل مبسط ويسمح لك بتحديد أولويات المهام المهمة.

الميزات	الفوائد
أكثر من 1700 سياسة أمنية منشأة مسبقا على حسب معايير كل دولة في العالم وعلى طبيعة عمل المنشأة	تبسيط النشر الأولي لخدمة DLP والإدارة المستمرة للسياسات باستخدام السياسات/القوالب/أدوات التصنيف المعدة مسبقًا
معالجة اللغات الطبيعية (NLP)	دقة غير متوقعة للتعرف على أنواع البيانات الشائعة (وهي PII وPHI وPCI) بناءً على المحتوى الموصوف باستخدام أكثر من 300 نص لغة طبيعية محددة مسبقًا
الكشف المتقدم الحقيقي عن نوع الملف	أكثر من 900 نوع من الملفات بغض النظر عما إذا كانت قد تمت إعادة تسميتها لتجنب الاكتشاف، بما في ذلك التعرف الضوئي على الحروف والنصوص في الصور OCR
التحكم الموحد في السياسات عبر CASB و SWG والبريد الإلكتروني ونقاط النهاية	إدارة جميع القنوات من داخل سياسة واحدة. اعداد السياسة يتم مرة واحدة، والنشر عبر جميع القنوات
الإعداد الموحد للتقارير عبر CASB و SWG والبريد الإلكتروني ونقاط النهاية	الإعداد الموحد للتقارير عبر CASB و SWG والبريد الإلكتروني ونقاط النهاية
سياسات الامتثال لأكثر من 150 منطقة حول العالم بشكل غير مباشر، 90 دولة	السياسات المتاحة بشكل دائم لتمكين الامتثال للمعايير الخاصة في كل دولة على مستوى العالم
التحديثات التلقائية	تبسيط إدارة أمن البيانات من خلال التحديثات الآلية لأحدث السياسات وأدوات التصنيف والقوالب المحددة مسبقًا
الوصول السريع إلى التنبيهات في لوحة معلومات الإبلاغ (بوابة الخدمة السحابية)	الاطلاع على جميع الحوادث والتنبيهات في الوقت الفعلي تقريبًا من لوحة معلومات فعالة ومنظمة
دمج إعداد التقارير	الاطلاع على جميع التقارير عبر DLP و Device Control و Risk-Adaptive Protection في واجهة مستخدم متكاملة
تحديد الأولويات للحوادث	عرض أهم عشرة إجراءات تتطلب اهتمامًا فوريًا في واجهة الحادث. إلى جانب درجة تقييم Risk-Adaptive Protection، يمكن أن يتضمن عددًا من الحوادث وشدة المخاطر للمستخدمين لتحديد أولويات سير العمل
Forensics	يوفر الرؤية حول حركة البيانات للتحقيق في الحوادث الأمنية، وفهم سبب حالات اختراق البيانات، وإجراء تحقيقات مفصلة في الحوادث، وتعزيز فعالية السياسات، ودعم الاحتياجات القانونية□الامتثال.
التحديثات المستمرة	إزالة الحاجة إلى التفاعل مع قسم تكنولوجيا المعلومات بشأن تحديثات الوكلاء، مما يقلل من الوقت اللازم لنشر التحديثات
الرؤية لإدارة الوكيل	الحصول على الرؤية حول حالة نشر نقاط النهاية والعثور بسرعة على المشكلات مع الوكلاء
الاتصال بالشبكة غير مطلوب لإنفاذ نقاط النهاية	ليست هناك حاجة إلى الاتصال بالشبكة لصالح نقاط النهاية للحصول على رؤية واضحة للانتهاكات الأمنية. تتم حماية البيانات دائمًا بغض النظر عن الاتصال بالشبكة
التكامل مع ميزة التحكم في الجهاز	توسيع أمن البيانات والتحكم في الوصول للوسائط القابلة للإزالة إلى وكيل واحد وواجهة مستخدم واحدة
التكامل مع Risk-Adaptive Protection	يتطلب الإنفاذ الآلي للسياسات في الوقت الفعلي والمراعي للسياق بالإضافة إلى إدارة الحوادث من وكيل واحد/واجهة مستخدم واحدة وحدة SKU منفصلة لحماية Risk-Adaptive Protection (إضافة إلى Forcepoint Data Security)
وقت تشغيل بنسبة 99.99% دون أي وقت توقف مجدول	يتم النشر على AWS عالميًا مع وقت تشغيل بنسبة 99.99%

forcepoint.com/contact

Forcepoint

© Forcepoint 2024. Forcepoint وشعار Forcepoint هما علامتان تجاريتان مملوكتان لصالح شركة Forcepoint. جميع العلامات التجارية الأخرى المستخدمة في هذه الوثيقة هي ملك لأصحابها.

[FP-Data Security Datasheet-AR] 02Jul2024