Forcepoint DSPM

Powered by GetVisibility

الكتيب

Forcepoint

التحول إلى الذكاء الاصطناعي هو التطور المستقبلي للتحول الرقمي

هل ستكون بياناتك آمنة في هذا العصر الجديد؟

تستعد معظم المؤسسات التي خضعت للتحول الرقمي إلى الاستعداد في الوقت الحالي للتطور التالي، وهو التحول إلى الذكاء الاصطناعي. ويقدم هذا العصر الجديد من الذكاء الاصطناعي العديد من المزايا التي تقدمها تطبيقات الذكاء الاصطناعي التوليدي مثل ChatGPT و Copilot و Gemini وغيرها. وبالاستفادة من تجارب التحول الرقمي التي قامت بها المؤسسات، فإنها تعلمت أن أمن البيانات يجب أن يكون أولوية قصوى. مع ذلك، وبالنسبة للعديد من المؤسسات، فإن البيانات اليوم تشبه جبلًا جليديًا ضخمًا، حيث تكون أغلبية مخفية تحت السطح. وغالبًا ما يشار إليها باسم "البيانات المظلمة" أو "بيانات الظل" ، حيث تظل غير مرئية وغير معروفة، ومع ذلك فهي تحتوي على كميات كبيرة من المعلومات الحساسة التي تتحمل المؤسسات المسؤولية عنها مسؤولية مباشرة. في الوقت الحالي، تسعى المؤسسات إلى معرفة كيفية تمكين المستخدمين من الاستفادة بأمان من تطبيقات الذكاء الاصطناعي التوليدي لتعزيز الإنتاجية والكفاءة مع ضمان حماية بياناتهم الحساسة.

توفر خدمة Data Security Posture Management (DSPM) نهجًا شاملًا لتأمين معلوماتك من الوصول غير المرخص أو الكشف أو التغيير أو تدمير البيانات. وبخلاف الأنواع الأخرى من أساليب أمن البيانات التي تركز على الأنظمة والأجهزة، فإن خدمة DSPM تركز على كامل بيانات المؤسسة نفسها، مما يضمن الامتثال ويقلل من مخاطر انتهاكات البيانات.

وفقًا لـ IDC، فإن 80% من البيانات على مستوى العالم غير مهيكلة وأن 90% من تلك البيانات لم تخضع للتحليل، ويُشار إليها أيضًا باسم "البيانات المظلمة"[1]

تخزن 90% من المؤسسات البيانات في بيئات خدمات سحابية متعددة.[2]

قامت Equifax بتسوية دعوى قضائية بقيمة 1.4 مليار دولار بسبب انتهاك بياناتها[3]، وقد تفاقم الأمر بسبب المتسللين الذين تمكنوا من الوصول إلى محرك أقراص مشترك يخزن نسخًا متعددة من أسماء المستخدمي وكلمات المرور الخاصة بالموظفين. افتقدت الشركة إلى أدوات للكشف عن والتعرف على الملفات الزائدة عن الحاجة والقديمة.

1 The Unseen Data Conundrum ,Forbes , فبراير 2022

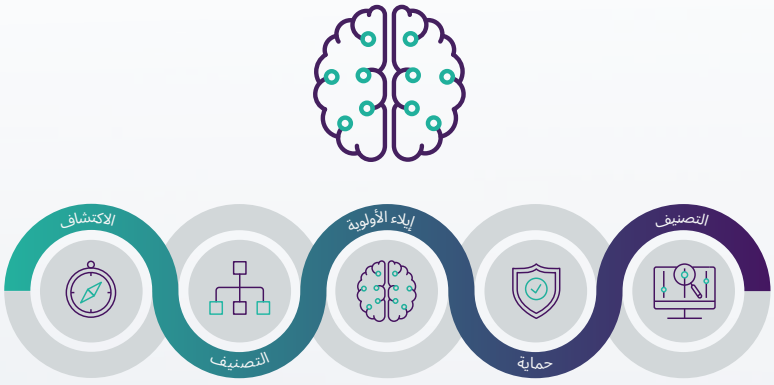
2 Dark Data: The Cloud's Unknown Security and Privacy Risk ,Forbes, يونيو 2023

3 Equifax agrees $1.38bn data breach lawsuit settlement, Finextra يناير 2020

ما الذي تتناوله خدمة DSPM؟

- **رحلة التحول إلى الذكاء الاصطناعي:** أطلق العنان لإمكانات الذكاء الاصطناعي مع خدمة Forcepoint DSPM، حيث يمكنك حماية بيانات في كل مكان مع تقنية AI Mesh المتقدمة الخاصة بنا. بفضل الرؤية المركزية المقدمة من خدمة Forcepoint DSPM والتحكم المقدم من خدمة Forcepoint ONE Data Security، فإننا نؤمّن معلومات الحساسة عبر القنوات الأساسية، ومن ذلك تطبيقات الذكاء الاصطناعي التوليدي، مثل ChatGPT و Copilot و Gemini وغيرها الكثير، مما يعزز الابتكار الرائد مع تعزيز الإنتاجية وتقليل المخاطر.
- **تحديد البيانات الحساسة:** تساعد خدمة DSPM المؤسسات على تحديد البيانات الحساسة عبر بيئات وخدمات متعددة عبر الخدمة السحابية بالإضافة إلى مواقع on-prem. يشمل ذلك فهم مكان وجود البيانات الحساسة وكيفية الوصول إليها ومعرفة من لديه أذونات للتفاعل عليها.
- **تقييم نقاط الضعف والمخاطر:** تقيّم خدمة DSPM قابلية تعرّض البيانات الحساسة للتهديدات الأمنية ومخاطر عدم الامتثال التنظيمي. من خلال تحليل الوضع الأمني للبيانات، يمكن للمؤسسات معالجة المخاطر المحتملة بشكل استباقي.
- **التركيز على البيانات في مصدرها:** على عكس أدوات أمان البيانات الأخرى التي تؤمّن الأجهزة والأنظمة والتطبيقات في المقام الأول، تركز خدمة DSPM بشكل مباشر على حماية بيانات المؤسسة بالكامل. إنها تهدف لمنع انتهاكات البيانات وضمان الامتثال من خلال تأمين البيانات في مصدرها.
- **معالجة البيانات المظلمة والبيانات الزائدة عن الحاجة والقديمة والمهملة:** تتناول خدمة DSPM بشكل مباشر البيانات المظلمة (تلك البيانات غير المرئية وغير المستخدمة في الوقت الحالي في العمليات العادية للشركات). وبالمثل، يمكن لخدمة DSPM معالجة البيانات الزائدة عن الحاجة والقديمة والمهملة، التي تنتشر على الأرجح عبر المؤسسات لأن الشركات تواصل الاحتفاظ بكميات كبيرة من البيانات لأسباب مختلفة، مما سيساعدها على الحفاظ على حالة الامتثال التنظيمي. إنها تتسبب في مخاطر أكبر للبيانات، وتساعد خدمة DSPM على إدارة هذه المخاطر.
- **معالجة البيانات التي تتجاوز الصلاحيات أو التي تتجاوز التصريحات:** نظرًا للطريقة التي تنتشر بها البيانات من خلال نسخ الإصدارات الجديدة من البيانات وتحريرها، يمكن أن تتجاوز أذونات البيانات أيضًا في كثير من الأحيان لتشمل المستخدمين والمجموعات وحتى إلى المؤسسة بأكملها. تساعد خدمة DSPM على تطبيق مفهوم "مبدأ امتيازات أقل" الذي يقلل بشكل كبير من البيانات التي يتم الإذن بها بشكل مفرط كوسيلة لمنع انتهاكات البيانات.
- **بيئات الخدمة السحابية المتعددة والخدمة الهجينة:** مع اعتماد المؤسسات على بيئات الخدمة السحابية المتعددة والخدمة الهجينة، تزداد مخاطر انتهاكات البيانات بشكل كبير. توفر خدمة DSPM الرؤية والتحكم في البيانات الحساسة عبر بيئات الحوسبة المتنوعة هذه، بالإضافة إلى المواقع on-prem.

صُممت خدمة **Forcepoint DSPM** لتتناسب مع المؤسسات الحديثة العصرية التي تحتاج إلى رؤية ثاقبة وتحكم قوي في بيانات أعمالها. إنها توفر الرؤية عبر بيئات الخدمة السحابية والخوادم المختلفة لمنع حالات انتهاك البيانات وتقليل مخاطر عدم الامتثال للوائح الخصوصية. توفر Forcepoint رؤية وتحكمًا كاملين خلال فترة استخدام البيانات، مما يتيح لها إمكانية توفير خدمة Data Security Everywhere من خلال الجمع بين **الاكتشاف الاستباقي لمخاطر البيانات** (DSPM) مع **عناصر التحكم النشطة حول كيفية استخدام البيانات** (DLP و SSE) مع **التكيف المستمر مع إجراءات كل مستخدم** Risk-Adaptive Protection.



الاكتشاف والتصنيف والتنسيق المدعوم بالذكاء الاصطناعي

توحيد الرؤية والتحكم في عرض بياناتك باستخدام خدمة Forcepoint DSPM

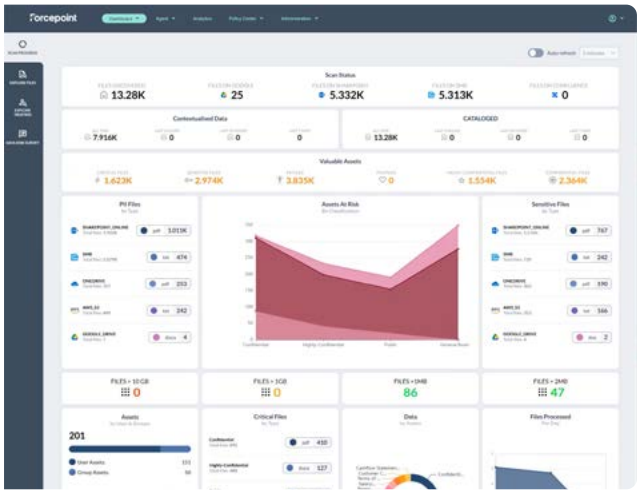
أصبح تأمين بيانات مؤسستك وإدارة هذه البيانات أكثر تعقيدًا من أي وقت مضى. توفر خدمة Forcepoint DSPM حلًا قويًا للحصول على رؤية شاملة والتحكم التام في بياناتك، بغض النظر عن الموقع. وبفضل مع سرعات الاكتشاف الرائدة في المجال وإمكانات تصنيف البيانات باستخدام AI Mesh المتقدم، تمكّنك خدمة Forcepoint DSPM من اتخاذ قرارات مستنيرة حول وضع أمن بياناتك ومعالجة المخاطر المحتملة بشكل استباقي.

تشمل المزايا الرئيسة لخدمة Forcepoint DSPM ما يلي:

الاكتشاف السريع والشامل: تكون خدمة Forcepoint DSPM قادرةً، عبر العديد من الخدمات السحابية وفي الموقع on-prem، على إجراء الفحص السريع للملفات بما يعادل حوالي مليون ملف في الساعة. ومن المألوف والمعتاد أن يكون لدى المؤسسات الكثير من التيرابايت، بل وحتى بعضها تمتلك بيتابايت، من البيانات التي تكون مسؤولة عنها. وبفضل هذا الاكتشاف عالي الأداء، تتيح Forcepoint للمؤسسات إمكانية الرؤية السريعة للبيانات عبر منصة بيانات هائلة تتضمن بين ميزاتها خدمة ChatGPT Enterprise. وعلى عكس مزودي خدمة DSPM الآخرين، لا تفرض Forcepoint رسومًا لقاء عمليات الاكتشاف -إنما يمكن للعملاء إجراء عمليات الاكتشاف بقدر ما يحلو لهم دون أي رسوم إضافية.

الدقة المعتمدة على تقنية : تكتشف خدمة Forcepoint DSPM البيانات عبر موارد الخدمة السحابية والشبكات وتصنف تلك البيانات تلقائيًا، باستخدام محرك تصنيف متقدم معتمد على الذكاء الاصطناعي. وتمكّن تقنية AI Mesh الموجودة في خدمة Forcepoint DSPM المؤسسات من الاستفادة من الدقة الفائقة التي يوفرها تصنيف البيانات Data Classification. إن بنية الذكاء الاصطناعي المتصلة بالشبكة، والتي تستفيد من نموذج GenAI Small Language Model (SML) والبيانات المتقدمة ومكونات الذكاء الاصطناعي، تجمع السياق بكفاءة من النص غير المهيكل. وبفضل إمكانية تخصيصه وكفاءته، فإنه يضمن التصنيف السريع والدقيق دون الحاجة إلى تدريب مكثف، مما يعزز الثقة والامتثال. لقد مكّنت هذه الدقة العالية، وبمستوى فائق، المؤسسات التي واجهت مشكلات في طرق التصنيف الشائعة الأخرى من تقليل الحالات الإيجابية الخاطئة بشكل كبير، ونجحت في حماية ملكيتها الفكرية، ووفرت الكثير من الوقت والموارد.

رؤية البيانات عبر منصة البيانات: تتيح لك خدمة Forcepoint DSPM فحص الأذونات لجميع الملفات والمستخدمين. يمكن لمشرفي البيانات معرفة أي الأفراد الذين يمكنهم الوصول إلى ملف أو مشاركة ملفات عبر المؤسسة. يمكنك، بنقرة واحدة، عرض الأذونات في الحال لجميع الملفات التي تخضع للفحص. توفر خدمة Forcepoint DSPM التقارير في الوقت الفعلي إلى جانب لوحة معلومات تضم تفاصيل شاملة تقدم عرضًا دقيقًا للبيانات المظلمة، بالإضافة إلى تقديم نظرة عامة على مخاطر البيانات لمساعدتك على فهم المناطق التي تنطوي على أعلى مخاطر للبيانات.



تنسيق سير العمل: تحديد الملكية بكل سهولة وتعيين جوانب المساءلة لمجموعات مختلفة من البيانات بهدف تبسيط عملية توفير المواءمة بين الجهات المعنية. يتيح هذا المزيد من مهام سير العمل الأكثر كفاءة حول الإجراءات التي يتم تنفيذها على كل مصدر وأصل للبيانات. يتطلب الإصلاح الفعال اشتراكًا وتعاونًا واسعًا خارج المؤسسة الأمنية إلى مجموعة CDO/DataOps، بالإضافة إلى وظائف، مثل التسويق والتمويل و DevOps وغيرها الكثير. تُعنى خدمة Forcepoint DSPM بتأمين وضع البيانات ليس باعتبارها مجرد مشكلة أمنية إنما أولوية في العمل.

لا تدع مخاطر البيانات توقف عملك. يمكن لخدمة Forcepoint تقديم المساعدة!

في عصرنا الرقمي الحاضر، تُعد البيانات أكثر الأصول قيمة للمؤسسات، ولكنها في الوقت نفسه قد تمثل مسؤولية كبيرة إذا لم تتم إدارتها بشكل صحيح. توفر خدمة Forcepoint DSPM نهجًا استباقيًا لتأمين بياناتك الحساسة، مما يخفف من مخاطر انتهاكات البيانات ويضمن الامتثال للوائح التنظيمية. بتنفيذ خدمة Forcepoint DSPM، يمكنك الحصول على رؤية شاملة لمنصة بياناتك وتحديد نقاط الضعف ومعالجتها، وحماية مؤسستك بشكل استباقي من الأضرار المالية والأضرار التي تلحق بالسمعة الناجمة عن انتهاكات البيانات وعدم الامتثال التنظيمي، وكل ذلك مع تأمين بياناتك في تطبيقات الذكاء الاصطناعي التوليدي. يمكنك التحكم في وضع أمان بياناتك اليوم. ابدأ في استكشاف كيف تحمي خدمة DSPM معلوماتك القيمة.

انتقل إلى www.forcepoint.com لطلب عرض توضيحي أو الاشتراك للحصول على تقييم مجاني لمخاطر البيانات حيث يمكن لمهندس الأمن أن يزودك بعينة من بياناتك الخاصة لمعرفة أنواع مخاطر البيانات التي تواجهها الآن.

Forcepoint

forcepoint.com/contact

حول Forcepoint

تبسط Forcepoint الأمان للشركات والحكومات العالمية. إن منصة Forcepoint، الشاملة المعتمدة فعليًا على الخدمة السحابية، تسهّل استخدام Zero Trust وتمنع سرقة البيانات الحساسة والملكية الفكرية أو فقدانها بغض النظر عن مكان عمل الأشخاص. يقع مقر شركة Forcepoint في أوستن، تكساس، حيث تعمل على توفير بيئات آمنة موثوقة للعملاء وموظفيها في أكثر من 150 دولة. يمكن التفاعل مع Forcepoint على www.Forcepoint.com و Twitter و LinkedIn.

[FP-DSPM-Brochure-AR] 13Sept2024