

Forcepoint DSPM



الكتيب

Forcepoint



وفقاً لـ IDC، فإن 80% من البيانات على مستوى العالم غير مهيكلة وأن 90% من تلك البيانات لم تخضع للتحليل، ويُشار إليها أيضاً 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 بياناتها³، وقد تفاقم الأمر بسبب المتسللين الذين تمكنا من الوصول إلى محرك أقراص مشترك يخزن نسخاً متعددة من أسماء المستخدمين وكلمات المرور الخاصة بالموظفيين. اقتدرت الشركة إلى أدوات للكشف عن والتعرف على الملفات الزائدة عن الحاجة والقديمة.

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 للتحول التالي، وهو التحول إلى الذكاء الاصطناعي. ويفدم هذا العصر الجديد من الذكاء الاصطناعي العديد من المزايا التي تقدمها تطبيقات الذكاء الاصطناعي التوليدية مثل Gemini و Copilot و ChatGPT 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 جليدًا ضحماً، حيث تكون أغلبية مخفية تحت السطح. وغالباً 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 تحمل المسؤولية عنها مسؤولية مباشرة. في الوقت الحالي، تسعى المؤسسات إلى معرفة كيفية تمكين المستخدمين من الاستفادة بأمان من تطبيقات الذكاء الاصطناعي التوليدية لتعزيز الإنتاجية والكفاءة مع ضمان حماية بياناتهم الحساسة.



توفر خدمة Data Security Posture Management (DSPM) نهجاً شاملًّا لتأمين معلوماتك من الوصول غير المرخص أو الكشف أو التغيير أو تدمير البيانات. على عكس الأنظمة الأخرى من أساليب أمن البيانات التي تركز على الأنظمة والأجهزة، تركز DSPM على بيانات المؤسسة بالكامل، سواء كانت منظمة أم غير منظمة، وسواء كانت ملكية فكرية أم بيانات خاضعة للتنظيم، وسواء كانت موجودة في السحابة أو الشبكات الخاصة، ما يضمن الامتثال ويقلل من مخاطر اختراقات البيانات.

ما الذي تتناوله خدمة DSPM؟

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 تسبب 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 أدوات 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.

بيانات الخدمة السحابية المتعددة والخدمة الهجينة:

مع اعتماد المؤسسات على بيانات الخدمة السحابية المتعددة والخدمة الهجينة، تزداد مخاطر انتهاكات البيانات بشكل كبير. توفر خدمة DSPM الرؤية والتحكم في البيانات السحابية عبر بيانات الحوسية المتنوعة هذه، بالإضافة إلى المواقع on-prem.

المراقبة المستمرة للمخاطر:

تتيح الوظيفة الإضافية Forcepoint Detection and Response (DDR) رصد المخاطر الجديدة المتعلقة بالبيانات بشكل فور حدوثها. لا حاجة لانتظار إجراء فحص الكامل التالي، حيث يمكن رصد المخاطر التي تهدد أمن بياناتك بشكل ديناميكي لمعالجتها.

رحلة التحول إلى الذكاء الاصطناعي: أطلق العنان لإمكانات الذكاء الاصطناعي مع خدمة Forcepoint DSPM في كل مكان مع تقنية AI Mesh المتقدمة الخاصة بنا. بفضل الرؤية المركزية والمعالجة من Forcepoint DSPM وعناصر التحكم في الحظر في الوقت الفعلي من Forcepoint DLP، تقوم بتأمين معلوماتك الحساسة عبر القنوات الرئيسية، بما في ذلك تطبيقات الذكاء الاصطناعي التوليدية، مثل Gemini Copilot ChatGPT وغيرها الكثير، مما يعزز الابتكار الرائد مع تعزيز الإنتاجية وتقليل المخاطر.

تحديد البيانات الحساسة: تساعد DSPM المؤسسات على تحديد البيانات الحساسة عبر بيانات وخدمات سحابية متعددة، بالإضافة إلى الواقع المحلي، بما في ذلك البيانات المنظمة وغير المنظمة على حد سواء. يشمل ذلك وجود البيانات الحساسة وكيفية الوصول إليها ومعرفة من لديه أدوات لتفاعل عليها.

تقييم نقاط الضعف والمخاطر: تقييم خدمة DSPM قابلية تعريض 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 تؤمن 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.

يُصمم حل **Forcepoint DSPM** ليتناسب مع المؤسسات الحديثة التي تحتاج إلى رؤية ثاقبة وتحكم قوي في بياناتها الحساسة. إنه يوفر الرؤية على مستوى بيانات الخدمة السحابية والخوادم المختلفة لمنع حالات انتهاك البيانات وتحقيق مخاطر عدم الامتثال للوائح الخصوصية. توفر Forcepoint Data Security Everywhere من خلال الجمع بين **الاكتشاف الاستباقي لمخاطر البيانات** (DSPM) و**التحكم النشط في كيفية استخدام البيانات** (DLP) مع **التكيف المستمر مع إجراءات كل مستخدم** (Risk-Adaptive Protection). تمكن من رصد مخاطر البيانات بشكل ديناميكي مع المراقبة المستمرة (Forcepoint DDR) لمنع حالات اختراق البيانات وحماية وضع أمن البيانات لديك.



الاكتشاف والتصنيف والتنسيق المدعوم بالذكاء الاصطناعي

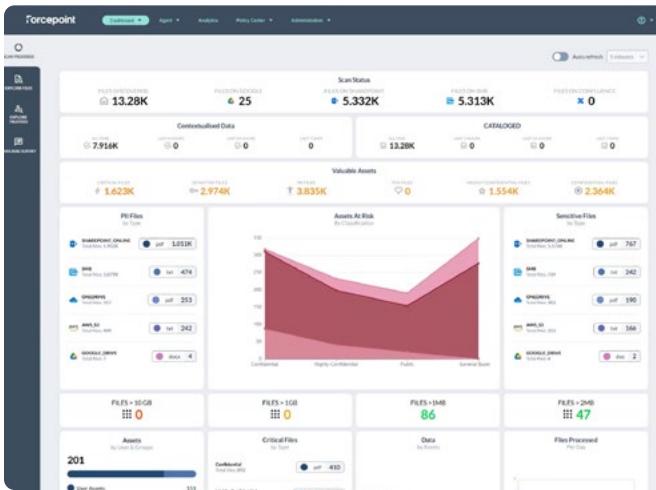


توحيد الرؤية والتحكم في عرض بياناتك باستخدام خدمة Forcepoint DSPM

أصبح تأمين بيانات مؤسستك وإدارة هذه البيانات أكثر تعقيداً من أي وقت مضى. توفر خدمة Forcepoint DSPM حلّاً قوياً 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 AI Mesh، تمكّنك خدمة Forcepoint DSPM من اتخاذ قرارات مستنيرة حول وضع أمن بياناتك ومعالجة المخاطر المحتملة بشكل استباقي.

تشمل المزايا الرئيسية لخدمة Forcepoint DSPM ما يلي:

رؤيا البيانات عبر نطاق البيانات: تتيح لك Forcepoint DSPM فحص الأذونات لكل 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 Forcepoint DSPM لوحة معلومات تضم تفاصيل شاملة تقدم عرضاً دقيقاً للبيانات المظلمة، بالإضافة إلى تقديم نظرة عامة على مخاطر البيانات لمساعدتك في فهم المناطق التي تتطوّي على أعلى مخاطر البيانات.



الاكتشاف سريع وشامل: يمكن Forcepoint DSPM من فحص الملفات وقواعد البيانات بسرعة عبر السحابة المتعددة وفي المبني. لا عجب أن تمتلك بعض المؤسسات كميات كبيرة من البيانات تصل إلى تيرابايت، في حين أن بعضها قد يصل إلى بيتابايت، بل إن المؤسسات الكبرى قد تحفظ بيانات بحجم الإكسابايت وتكون مسؤولة عن إدارتها. وبفضل قدرات الاكتشاف عالية الأداء، تتيح Forcepoint DSPM للمؤسسات إمكانية الرؤية السريعة لبيانات عبر نطاق بيئات واسع، يشمل خدمة ChatGPT Enterprise. وخلافاً لمقدمي خدمات DSPM الآخرين، لا تفرض Forcepoint رسوماً مقابل عمليات المسح الضوئي للاكتشاف، حيث يمكن للعملاء إجراء عمليات المسح الضوئي للاكتشاف 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 تلقائياً، 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 (SML) GenAI Small Language Model، 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 يعزّز الثقة والامتثال. لقد مكّنت هذه الدقة العالمية، 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.

Forcepoint DDR:مكون إضافي قوي في Forcepoint DSPM، وهو حل أساسي لمعالجة حالات اختراق البيانات. وهو يوفر رصداً مستمراً للمخاطر فضلاً عن رؤية محسنة للمخاطر البيانات، مما يضمن قدرة المؤسسات على رؤية التغيرات التي تطرأ على البيانات والتي من المحتمل أن تؤدي إلى حالات اختراق البيانات في الوقت الذي تحدث فيه وبصورة فعالة. يستفيد Forcepoint DDR من الاستجابات التي تعتمد على الذكاء الاصطناعي، فيقدم إمكانية تحديد التهديدات بدقة، مما يساعد المؤسسات في الحفاظ على تدابير أمنية قوية. إن رؤيته الواسعة عبر السحابة ونقطة النهاية، إلى جانب تتبع سلسلة البيانات، تجعله أداة أساسية لحماية المعلومات الحساسة والحد من الخسائر المالية والحفاظ على ثقة العملاء.

تنسيق سير العمل: تحديد الملكية بكل سهولة وتعيين جوانب المساءلة لمجموعات مختلفة من البيانات بهدف تبسيط عملية توفير المعايدة بين الجهات المعنية. وهذا يمكن من رفع كفاءة مهام سير العمل حول الإجراءات التي يتم تنفيذها على كل مصدر وأصل للبيانات. يتطلب الإصلاح الفعال دعماً وتعاوناً واسعاً يتجاوز المؤسسة الأمنية ليشمل مجموعة المديرين التنفيذي للبيانات (CDO)، الحكومة والمخاطر والامتثال (GRC) ، بالإضافة إلى وظائف أخرى، مثل التسويق والتمويل و DevOps وغيرها الكثيرة. يُركز حل Forcepoint DSPM على تأمين وضع البيانات ليس باعتبارها مجرد مسألة أمنية، بل كأولوية تجارية.



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 يتم إدارتها بشكل صحيح. توفر خدمة Forcepoint DSPM نهجاً استباقياً لتأمين بياناتك الحساسة، مما يخفف من مخاطر انتهاكات البيانات ويضمن الامتثال للوائح التنظيمية. يتنفيذ 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 التوليدية. 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 الأمان أن يزودك بعينة من بياناتك الخاصة لمعرفة أنواع مخاطر البيانات التي تواجهها الآن.

Forcepoint حول

Forcepoint

forcepoint.com/contact

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