Forcepoint

Forcepoint Data Security Posture Management

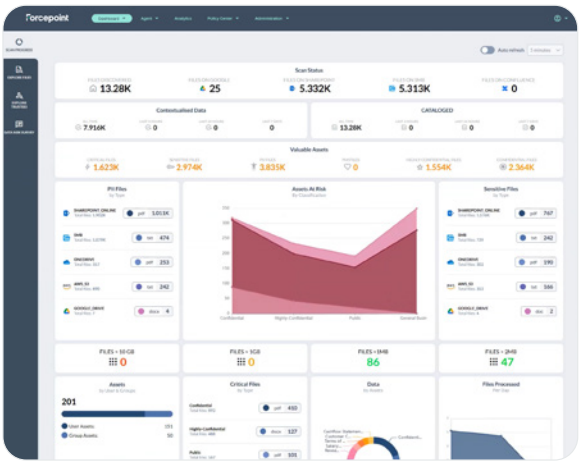
الميزات والفوائد الرئيسة:

- **تصنيف AI Mesh -** معمارية تصنيف شبكي عالية الدقة وفعالة تستخدم إمكانات الذكاء الاصطناعي التوليدي، والذكاء الاصطناعي التنبؤي، وعلوم البيانات.
- **الاكتشاف السريع -** يمكن تشغيل خدمة Forcepoint DSPM في مواقع التخزين السحابية ومواقع تخزين on-prem بقدر ما تريد.
- **اتقييم المخاطر في الوقت الفعلي -** التحقق من أذونات الوصول والمخاطر الأخرى المتعلقة بالبيانات.
- **تنسيق سير العمل -** تنفيذ أولويات الأعمال الخاصة بالجهات المعنية.

لقد تطور التحول الرقمي في العمليات التجارية ليصبح التحول إلى الذكاء الاصطناعي، مدفوعًا بدمج تقنيات الذكاء الاصطناعي، لاسيما تطبيقات الذكاء الاصطناعي التوليدي. وإلى جانب انتشار البيانات الناجم عن المؤسسات التي تقوم بترحيل التطبيقات والبيانات من مواقع الشركة الداخلية إلى الخدمة السحابية وتستفيد من أدوات الذكاء الاصطناعي التوليدي، مثل ChatGPT و Copilot و Gemini، فإنها تجاهد باستمرار لتتبع مكان وجود بياناتها الحساسة، ومعرفة من يمكنه الوصول إليها، وكيف يتم استخدامها. يمثل النمو الهائل "للبيانات المظلمة" ، المخفية داخل مستودعات معتمدة على الخدمة السحابية أو المنتشرة عبر الأجهزة الفردية، وحاليًا تطبيقات الذكاء الاصطناعي التوليدي، مخاطرةً كبيرة. تشير التقديرات إلى أن ما يصل إلى 80 بالمائة من بيانات المؤسسة موجودة في هذه الحالة " المظلمة" الغامضة، حيث لا تخضع لأي رقابة تقليدية.

إن عواقب هذا المشهد المبهم للبيانات وخيمة. وبدون رؤية واضحة وإدارة مستنيرة، سيزداد الخطر الذي تتعرض له المؤسسات بسبب الانتهاكات، مع ما قد يترتب على ذلك من عواقب وخيمة عبر القطاعات التجارية والحكومية وغير الربحية على حدٍ سواء. لقد أصبحت ضرورة استعادة القدرة على التحكم في المعلومات الحساسة في عصر التحول الرقمي الحاضر أكثر إلحاحًا من أي وقت مضى.

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.

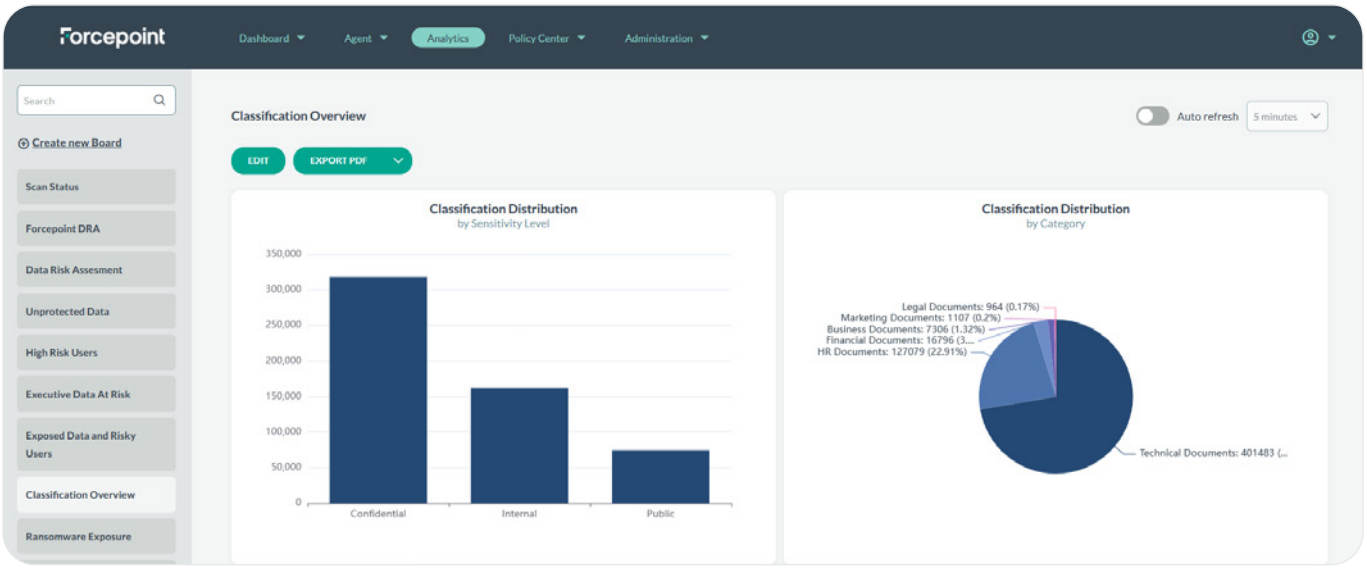


الاكتشاف السريع والشامل

بفضل تعدد الموصلات، يقوم حل Forcepoint DSPM بتحديد مواقع البيانات الحساسة بكفاءة عبر بيئات التخزين المتنوعة، سواء كانت في السحابة أو الأنظمة المحلية، حيث يقوم بالفحص عبر المنصات الرئيسية مثل Amazon (AWS S3 و IAM)، و Microsoft (Azure AD و OneDrive و SharePoint Online) و Google (Google Drive و IAM)، بالإضافة إلى أنظمة LDAP و SharePoint المحلية .

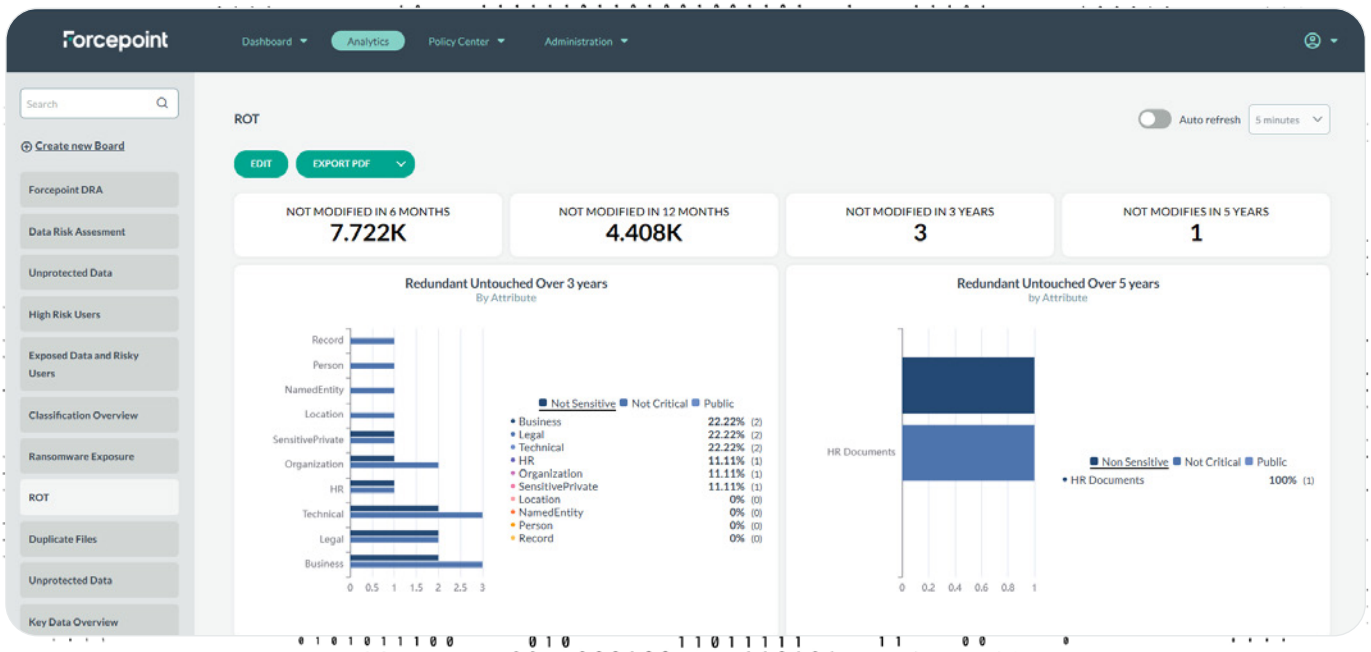
الدقة المزودة بتقنية AI Mesh

تتفوق ميزة AI Mesh في خدمة Forcepoint DSPM في أنها تمكّن المؤسسات اليوم من خلال الدقة الفائقة لتصنيف البيانات. وخلافًا لحلول DSPM الأخرى، فإنها توفر بنية ذكاء اصطناعي متصلة متعددة العُقد، تستفيد من تقنية GenAI SLM وشبكة من مكونات البيانات والذكاء الاصطناعي المتقدمة. تلتقط هذه البنية السياق بكفاءة وتحول النص غير المنظم إلى تصنيفات دقيقة للمستند. تتسم ميزة AI Mesh بأنها قابلة للتخصيص، حيث تتناسب مع احتياجات المجال والبيئات التنظيمية. يتم تشغيلها بكفاءة على موارد الحوسبة القياسية من دون الحاجة إلى وحدات معالجة الرسومات مع توفير تصنيف عالي الأداء. يتم تحقيق الدقة العالية دون تدريب مكثف على تعلم الآلة، ما يقلل من تكاليف الصيانة. تعزز قابلية التفسير الخاصة بميزة AI Mesh الثقة والامتثال للقواعد، ما يضمن وضعًا آمنًا للغاية للبيانات مع الالتزام بلوائح الخصوصية.



المراقبة عالية الأداء وتقييم مخاطر البيانات

نظرًا لأن خدمة Forcepoint DSPM تفحص البيانات وتكتشفها، فإنها توفر معلومات مفصلة مثل عدد الملفات التي تمت مشاركتها داخليًا والتي تحتوي على معلومات مهمة وحجم ملفات PII المعرضة للخطر وعدد ملفات البيانات الزائدة عن الحاجة والقديمة والمهملة (ROT).



تنسيق سير العمل

تبسيط حوكمة أمن البيانات دون عناء باستخدام خدمة Forcepoint DSPM. إن تنسيق سير العمل سهل التنفيذ لدينا يضمن التتبع الفعال لملكية البيانات والمساءلة. ومن خلال تفصيل المنصات وتسهيل التعاون بين الجهات المعنية، فإنها توحد المسؤوليات وتعزز الكفاءة التشغيلية وتعزز الوضوح عبر المؤسسة.

يبعد تنفيذ حل DSPM القوي أمرًا بالغ الأهمية للمؤسسات التي تهدف إلى تأمين وضع البيانات وحماية المعلومات الحساسة في جميع مواقع تخزين البيانات، سواء في الخدمات السحابية أو في الأنظمة المحلية. ومن خلال الاستفادة من حل Forcepoint DSPM، يمكن للمؤسسات تعزيز الإنتاجية من خلال تعزيز موثوقية الوصول إلى البيانات ومشاركتها وتعزيز الابتكار وتشجيع التعاون. وفي الوقت نفسه، يمكنها تقليل المخاطر من خلال تحديد الاستخدام غير السليم للبيانات الحساسة ومعالجته، ما يمنع تسرب البيانات. وفي نهاية المطاف، يمكن للمؤسسات تبسيط جهود الامتثال من خلال الحصول على رؤية حقيقية وتحكم كامل في البيانات الحساسة على مستوى جميع البيئات.

الاكتشاف القوي

الميزة	الفائدة
الاكتشاف والفهرسة السريعان	يتم تشغيله على موارد متعددة لفحص كميات أكبر من الملفات في الثانية/الساعة وتجميع التفاصيل حول مجموعات البيانات غير المهيكلة، وتنظيمها في تنسيق بسيط.
التوصيل بموارد البيانات المهمة	تحقيق رؤية شاملة للبيانات غير المهيكلة من خلال توفير مجموعة من موصلات موارد البيانات.
تحليل البيانات العرضة لخطر زائد	تحديد البيانات التي تم الكشف عنها والتي تتم مشاركتها بشكل عام ومشاركتها خارجيًا مع أطراف ثالثة والتي يتم مشاركتها بشكل زائد داخليًا.
عرض الأذونات ومعالجتها	عرض الوصول لكل ملف ومعالجته من أجل تطبيق مبدأ الحد الأدنى من الصلاحيات (POLP) وأمن انعدام الثقة لتأمين البيانات.
التخلص من المخاطر الناجمة عن البيانات الزائدة عن الحاجة والقديمة والمهملة (ROT)	يمكنك تحديد الملفات الزائدة عن الحاجة والقديمة والمهملة (ROT) والتخلص منها.
الرؤية في الوصول والأذونات	تعزز عمليات التكامل مع Active Directory وحلول IRM الأخرى أمن الوصول داخل المؤسسات.

AI Mesh Data Classification

الميزة	الفائدة
تصنيف AI Mesh للبيانات غير المهيكلة	تصنيف الذكاء الاصطناعي عالي الدقة للبيانات غير المهيكلة.
التدريب على نموذج مخصص	يمكن للمؤسسات تخصيص نموذج AI Mesh ليتناسب مع احتياجات البيانات الفريدة (مثل الملكية الفكرية والأسرار التجارية وغيرها)، بهدف تصنيف البيانات بدقة عالية وتقليل الأخطاء الإيجابية والسلبية في حلول DSPM و DLP.
القدرة على تعيين العلامات إلى علامات Microsoft Purview IP.	توفير طبقة إضافية من دقة التصنيف، ما يكمل علامات MIP. القدرة على تصحيح علامات MIP.
وضع علامات على البيانات	وسم جميع الملفات التي تم فحصها وتصنيفها بعلامات دائمة يمكن لحلول DLP قراءتها، باستخدام الوسوم القياسية (مصنف، مصنف بدرجة عالية، عام)، بالإضافة إلى التصنيف/وضع العلامات الخاص بالأعمال (الموارد البشرية، التسويق، المالية، DevOps مع وسوم فرعية مثل السير الذاتية، أوامر الشراء، وغيرها).
التكامل مع خدمة Forcepoint DLP	إمكانية التكامل مع Forcepoint DLP لاستخدام علامات DSPM AI Mesh للملفات (التصنيف) لبناء سياسات قوية لحماية البيانات.

المراقبة في الوقت الفعلي وتقييم المخاطر

الميزة	الفائدة
تقييمات مخاطر البيانات (DRA)	تتوفر تقييمات مخاطر البيانات المجانية لتحليل الوضع الحالي لأمن البيانات في المؤسسة عبر فئات متعددة.
لوحة معلومات تفاعلية مفصلة	عرض تفاصيل الملف الشاملة على شاشة واحدة. البحث الدقيق عن بيانات الملفات المهمة، مثل مستوى المخاطر والأذونات والمواقع (عنوان IP والمسار).
وظيفة إعداد التقارير	يمكنك إنشاء تقارير تظهر الاستعداد العام للامتثال وللوائح الخصوصية المحددة.
النظام المتقدم للتنبيهات	يوفر عناصر التحكم المتطورة في البيانات والتنبيهات التي يتم العثور عليها في أثناء عمليات الفحص عن أي حالات غير طبيعية أو انتهاكات محتملة.
البحث عن طلب الوصول إلى موضوع البيانات (DSAR)	تبسيط إنشاء طلبات DSAR لسرعة الامتثال إلى طلبات لوائح الخصوصية.
مجموعة أدوات Analytics	جرب مجموعة أدوات التحليل المتقدمة التي تسهل الوصول إلى رؤى الأمان والتصنيف بسرعة. اختر من بين العديد من لوحات المعلومات المحددة مسبقًا أو أنشئ لوحاتك الخاصة، وقم بتصدير لقطات بتنسيق PDF بنقرة واحدة ومن دون عناء. تتضمن لوحات المعلومات المحددة مسبقًا تحليل التعرض المفرط وبرمجيات الفدية، وتكرار البيانات الحساسة، واكتشاف المستخدمين المعرّضين للمخاطر، والاحتفاظ بالبيانات، والبيانات غير الموضوعة في أماكنها الصحيحة، وتقييم مخاطر البيانات، والسيادة، وتتبع الحوادث المتعلقة بانتهاكات التحكم في البيانات، وغير ذلك الكثير.
تحليل التعرض لبرامج الفدية	تحديد البيانات المهمة التي يمكن أن تتعرض لهجوم برمجيات الفدية.
أداة إعداد التقارير والتحليلات من دون ترميز	سهولة إنشاء حالات استخدام مخصصة وإعداد تقارير تحليلية من دون الحاجة إلى مهارات في البرمجة.
تحديد هوية المستخدمين العرضة للمخاطر	تحديد هوية المستخدمين التي ملفاتهم التعريفية عرضة لمخاطر عالية ويمكنهم الوصول إلى كميات كبيرة من المعلومات المهمة.
حادث التحكم في البيانات	يوفر عرضًا واضحًا لأي انتهاكات للتحكم في البيانات وحالة حل الحوادث.

تنسيق سير العمل

الميزة	الفائدة
ملكية البيانات	تحدد المساءلة بكل سهولة وتحقق المواءمة بين الجهات المعنية.
مدير المهام	إسناد المهام إلى أمناء البيانات ومالكيها، مما يسمح بتتبع إحصاءات خدمة DSPM (مثل تذاكر الدعم المفتوحة والتي تم حلها والمغلقة، ووقت الحل).