

# Forcepoint Data Security Posture Management

لقد تطور التحول الرقمي في العمليات التجارية ليصبح التحول إلى الذكاء الاصطناعي، مدفوعاً بدمج تقنيات الذكاء الاصطناعي، لاسيما تطبيقات الذكاء الاصطناعي التوليدية. وإلى جانب انتشار البيانات الناجم عن المؤسسات التي تقوم بتحليل التطبيقات والبيانات من موقع الشركة الداخلية إلى الخدمة السحابية وتستفيد من أدوات الذكاء الاصطناعي التوليدية، مثل ChatGPT و Copilot و Gemini، فإنها تجاهد باستمرار لتبني مكان وجود بياناتها الحساسة، ومعرفة من يمكنه الوصول إليها، وكيف يتم استخدامها. يمثل النمو الهائل للبيانات المظلمة، المحفية داخل مستودعات معتمدة على الخدمة السحابية أو المنتشرة عبر الأجهزة الفردية، حالياً تطبيقات الذكاء الاصطناعي التوليدية، 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 يتعرض له المؤسسات بسبب الانتهاكات، مع ما قد يترب على ذلك من عواقب وخيمة عبر القطاعات التجارية والحكومية وغير الربحية على حد سواء. لقد أصبحت ضرورة استعادة القدرة على التحكم في المعلومات الحساسة في عصر التحول الرقمي الحاضر أكثر إلحاحاً من أي وقت مضى.

تكتشف Forcepoint DSPM البيانات الحساسة وتصنفها بسرعة على نطاق واسع، ما يغطي البيانات المنظمة وغير المنظمة. توفر شبكة AI Mesh الفريدة من نوعها السرعة والقدرة على التفسير من خلال بنية عالية الكفاءة لنموذج اللغات الصغيرة (SLM). كما تتيح AI Mesh التخصيص دون الحاجة إلى إعادة تدريب شاملة للنماذج، كما تضمن تصنيفاً سريعاً ودقيقاً لزيادة الثقة والامتثال.

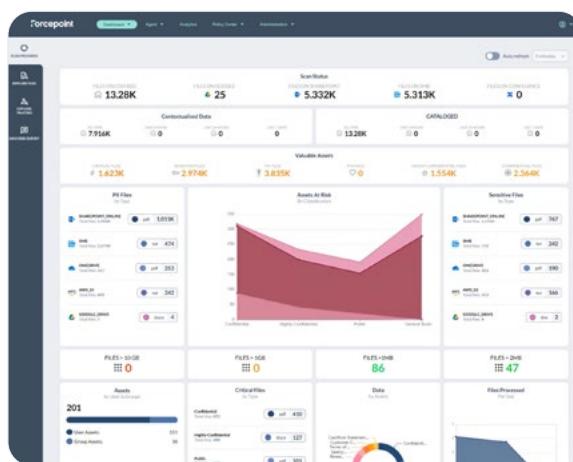
## الميزات والفوائد الرئيسية:

**تصنيف AI Mesh** - بنية تصنيف عالية الدقة والفعالية باستخدام الذكاء الاصطناعي التوليدية والذكاء التنبؤي وقدرات علوم البيانات.

**الاكتشاف السريع** - يمكن تشغيل خدمة Forcepoint DSPM في موقع التخزين السحابية وموقع تخزين on-prem بقدر ما تريده.

**تقييم المخاطر في الوقت الفعلي** - التحقق من أذونات الوصول والمخاطر الأخرى المتعلقة بالبيانات.

**تنسيق سير العمل** - تنفيذ أولويات الأعمال الخاصة بالجهات المعنية.

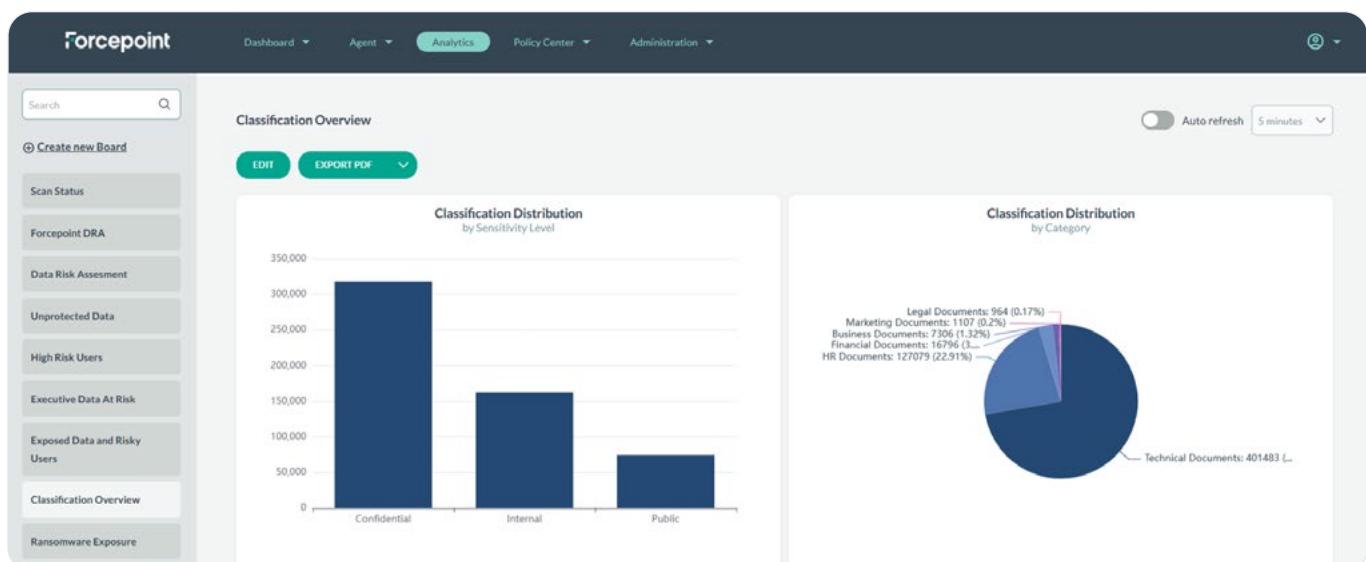


## الدقة المزودة بتقنية AI Mesh

تفوق ميزة AI Mesh في خدمة Forcepoint DSPM في أنها تمكّن المؤسسات اليوم من خلال الدقة الفائقة لتصنيف البيانات. وخلافاً لحلول DSPM الأخرى، فإنها توفر بنية ذكاء اصطناعي متصلة متعددة الغُصُق، تستفيد من تقنية GenAI SLM وشبكة من مكونات البيانات والذكاء الاصطناعي المتقدمة. تلتقط هذه البنية السياق بكفاءة، وتحول النص إلى تصنیفات دقيقة للوئاق. تسمیة ميزة AI Mesh بأنها قابلة للتخصیص، حيث تتناسب مع احتياجات المجال والبيئات التنظیمية. يتم تشغیلها بكفاءة على موارد الحوسبة القياسیة من دون الحاجة إلى وحدات معالجة الرسومات مع توفير تصنیف عالی الأداء. يتم تحقیق الدقة العالیة دون تدرب مکثف على تعلم الآلة، ما یقلل من تکالیف الصيانة. تعزز قابلیة التفسیر الخاصة بميزة AI Mesh الثقة والامتثال للقواعد، ما یضمن وضعاً آمناً للغاية للبيانات مع الالتزام بلوائح الخصوصیة.

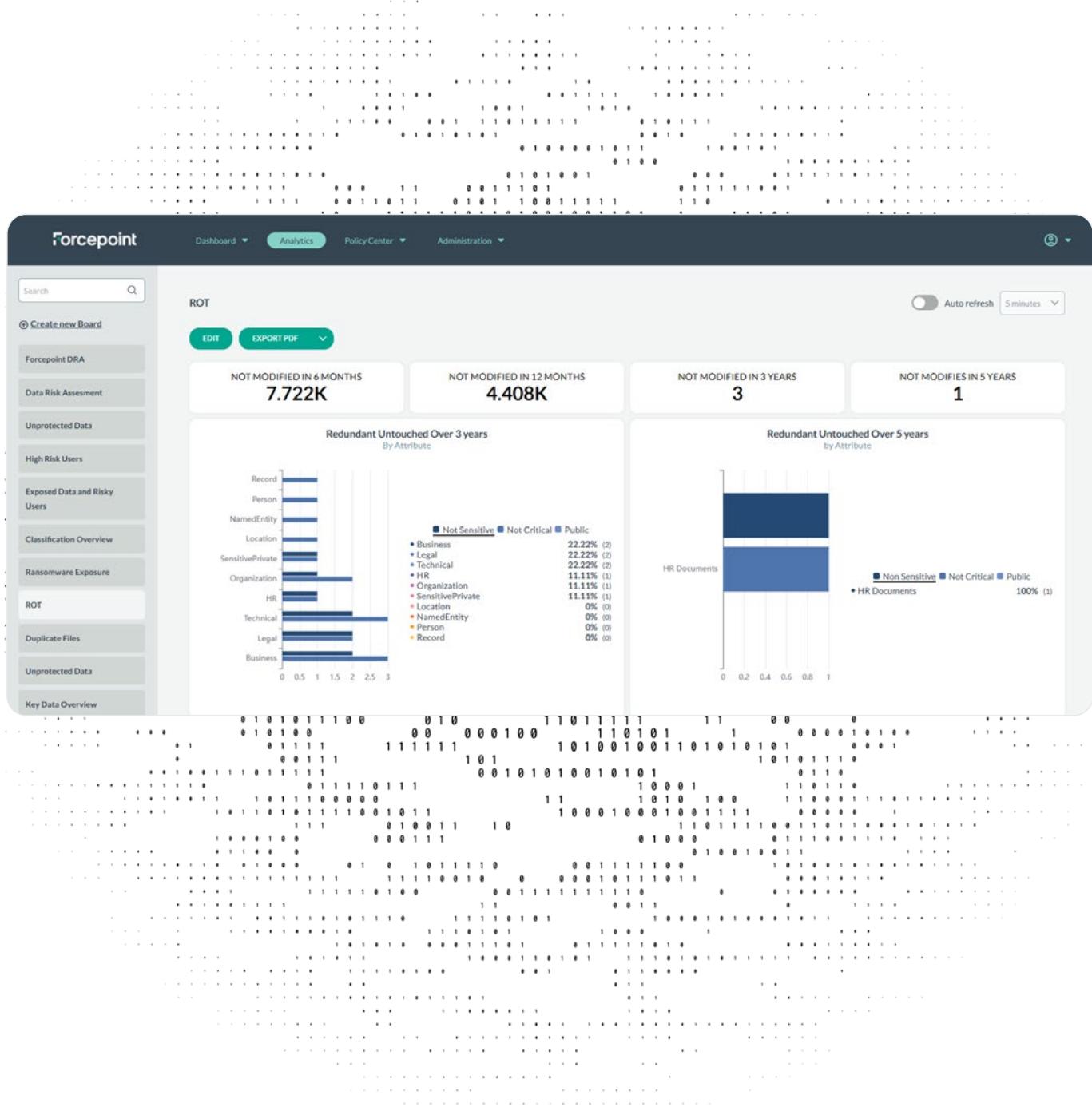
## الاكتشاف السريع والشامل

من خلال عدد كبير من الموصلات، تعمل Forcepoint DSPM على تحديد موقع البيانات الحساسة بكفاءة عبر بیئات تخزين متعددة، سواء كانت في السحابة أو في مكان العمل، سواء كانت البيانات المنظمة أو غير المنظمة، و تقوم بمسح ضوئي عبر المنصات الرئيسية، مثل: AWS S3 (Amazon) و IAM و Microsoft SharePoint Online و OneDrive و Azure AD (Microsoft) و Google Drive (Google) و LDAP و SharePoint المحلية.



## المراقبة عالية الأداء وتقدير مخاطر البيانات

نظرًا لأن خدمة Forcepoint DSPM تفحص البيانات وتكتشفها، فإنها توفر معلومات مفصلة مثل عدد الملفات التي تمت مشاركتها داخلًا 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 أمراً 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 ومعالجتها، ما يمنع تسرب البيانات. وفي نهاية المطاف، يمكن للمؤسسات تبسيط جهود الامتثال من خلال الحصول على رؤية حقيقة وتحكم كامل في البيانات الحساسة على مستوى جميع البيانات.

## الاكتشاف القوي

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

## AI Mesh Data Classification

الفائدة	الميزة
تصنيف عالي الدقة من الذكاء الاصطناعي للبيانات المنظمة وغير المنظمة.	تصنيف البيانات المنظمة وغير المنظمة من خلال AI Mesh
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.	التدريب على نموذج مخصص
توفير طبقة إضافية من دقة التصنيف، ما يكمل علامات MIP. القدرة على تصحيح علامات MIP.	القدرة على تعين العلامات إلى علامات Microsoft Purview IP
وسم جميع الملفات التي تم فحصها وتصنيفها بعلامات دائمة يمكن حلول DLP قراءتها، باستخدام الوسوم القياسية (مصنف، مصنف بدرجة عالية، عام)، بالإضافة إلى التصنيف/وضع العلامات الخاص بالأعمال (الموارد البشرية، التسويق، المالية DevOps مع وسم فرعية مثل السير الذاتية، أوامر الشراء، وغيرها).	وضع علامات على البيانات
إمكانية التكامل مع Forcepoint DLP لاستخدام علامات DSPM AI Mesh للملفات (التصنيف) لبناء سياسات قوية لحماية البيانات.	التكامل مع خدمة Forcepoint DLP

## المراقبة في الوقت الفعلي وتقييم المخاطر

الفائدة	الميزة
توفر <a href="#">تقييمات مخاطر البيانات المجانية</a> لتحليل الوضع الحالي لأمن البيانات في المؤسسة عبر قنوات متعددة.	تقييمات مخاطر البيانات (DRA)
عرض تفاصيل شاملة للملفات وقواعد البيانات في حل واحد. البحث الدقيق عن بيانات الملفات المهمة، مثل مستوى المخاطر والأذونات والموقع (عنوان IP والمسار).	لوحة معلومات تفاعلية مفصلة
يمكنك إنشاء تقارير تظهر الاستعداد العام للامتثال ولوائح الخصوصية المحددة.	وظيفة إعداد التقارير
يوفّر عناصر التحكم المتطرفة في البيانات والتنبيهات التي يتم العثور عليها في أثناء عمليات الفحص عن أي حالات غير طبيعية أو انتهاكات محتملة.	النظام المتقدم للتنبيهات
تسهيل إنشاء طلبات DSAR لسرعة الامتثال إلى طلبات ولوائح الخصوصية.	البحث عن طلب الوصول إلى موضوع البيانات (DSAR)
جرب مجموعة أدوات التحليل المتقدمة التي تسهل الوصول إلى رؤى الأمان والتصنيف بسرعة. اختر من بين العديد من لوحات المعلومات المحددة مسبقاً أو أنشئ لوحاتك الخاصة، وقم بتصدير لقطات بتنسيق PDF بقدرة واحدة ومن دون عناء. تضمن لوحات المعلومات المحددة مسبقاً تحليل التعرض المف躬 وبرمجيات الفدية، ونكرار البيانات الحساسة، واكتشاف المستخدمين المعرضين للمخاطر، والاحتفاظ بالبيانات، والبيانات غير الموضوعة في أماكنها الصحيحة، وتقييم مخاطر البيانات، والسيادة، وتتبع الحوادث المتعلقة بانتهاكات التحكم في البيانات، وغير ذلك الكثير.	مجموعة أدوات Analytics
تحديد البيانات المهمة التي يمكن أن تتعرض لهجوم برمجيات الفدية.	تحليل التعرض لبرامج الفدية
سهولة إنشاء حالات استخدام مخصصة وإعداد تقارير تحليلية من دون الحاجة إلى مهارات في البرمجة.	أداة إعداد التقارير والتحليلات من دون ترميز
تحديد هوية المستخدمين التي ملفاتهم التعريفية عرضة لمخاطر عالية ويمكنهم الوصول إلى كميات كبيرة من المعلومات المهمة.	تحديد هوية المستخدمين العرضة للمخاطر
يوفّر عرضاً واضحاً لأي انتهاكات للتحكم في البيانات وحالة حل الحوادث.	حدث التحكم في البيانات

## تنسيق سير العمل

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

[forcepoint.com/contact](http://forcepoint.com/contact)