

# 見付ける。安全を確保する。簡素化する。Forcepoint Data Security Posture Management

## 貴社のデータリスクを認識していますか？

デジタル時代は、あらゆるところにデータをもたらします。組織は、複数のクラウドプラットフォーム、オンプレミス環境、そして今日では ChatGPT、Copilot、Gemini などの GenAI アプリに広がるデータに対応するのに苦労しています。この複雑な状況により、重大な課題が生じています。見えないものを保護することはできません。多くの組織では、機密データがどこに保存されているか、誰がアクセスできるか、どのように使用されているかについての洞察が不足しています。大量の未知の「ダークデータ」(組織のデータの最大 80%) がシステムに残っている場合、特にデータ侵害は大きな問題となります。さらにデータプライバシー規制はますます厳しくなっています。組織は、罰則や評判の低下を回避するために、コンプライアンスを実証できる必要があります。



## Forcepoint Data Security Posture Management (DSPM) –データリスクへのソリューション

Forcepoint DSPMは、これらの課題に取り組み、企業のデータセキュリティ体制を管理するために役立ちます。保護されたデータプロアクティブなデータリスク検出とリアルタイムモニタリングを提供し、攻撃者がダークデータを利用する前に、ダークデータに関連するリスクを特定して対処できるようにします。AIメッシュや GenAI Small Language Model (SLM) などの最新のイノベーションを活用した Forcepoint DSPM は、優れたデータ分類精度で組織を支援します。Forcepoint DSPM により、次のことが可能になります。

- データ内容を判別して分類し、セキュリティポリシーをより正確かつ効率的に定義し、自動化します。
- データアクセス管理を簡素化し、データの所有権と場所を明確に把握し、適切なアクセス権限の付与プロセスを合理化します。
- DSPMを特定の業界セクター、規制要件、およびユーザーの好みに合わせてカスタマイズすることで、コンプライアンスを合理化。組織はプライバシー規制により適切に準拠できます。調整可能な感度設定とユーザー固有の detectors (検出器)により、正確なデータ処理が可能になり、コンプライアンスリスクが軽減されます。プライバシー規制により適切に準拠できます。調整可能な感度設定とユーザー固有の detectors (検出器)により、正確なデータ処理が可能になり、コンプライアンスリスクが軽減されます。
- データセキュリティリスクを事前に特定することにより、コストのかかるデータ侵害のリスクを軽減します。

Forcepoint DSPMは、攻撃者に悪用される前に、データセキュリティのリスクを特定して修復することで、データセキュリティを強化します。コンプライアンス報告を簡素化することで、コンプライアンスにかかるコストを削減し、データプライバシー侵害関連の罰則を回避するのに役立ちます。他の DSPM ソリューションとは異なり、マルチノードの接続された AI アーキテクチャを提供し、GenAI SLM と高度なデータおよび AI コンポーネントのネットワークを活用し、迅速かつ正確なデータ分類を実現します。

完全なデータセキュリティ実現に [Forcepoint DSPM](#) がどのように役立つか、詳細を今すぐお問い合わせください。