

AVEPOINT COMPLIANCE GUARDIAN

全方向的リスク マネジメント

AvePoint Compliance Guardian を利用してできること



データ
ディスカバリー



データ分類



データ損失
防止 (DLP)



インシデント
管理

監視ツールを活用してプライバシーポリシー違反とアクセス許可ルール違反に対して警告を発生し、継続的に疑わしいデータを検知・レビューすることにより、インシデントの深刻化を未然に防ぎます。

ファイルレベルおよびコンテンツレベルでファイルをスキャン・分析することにより、組織が持つ全ファイルの分類およびセキュリティ対策・不適切なコンテンツのブロック・情報資産の保護を実行します。

組織内で統一されたデータ分類基準に従い、既存のコンテンツと新規データの両方を対象に、コンテキストと所有者情報に基づいた自動タグ付けを実行します。

これにより、ITリソースへの時間的負荷と人的負担を取り除くとともに、アクセス許可および情報ガバナンスポリシーが自動的に守られる環境づくりが可能になります。

エンドユーザー同士のコラボレーション促進を阻害することなく、データに関する問題の発生を先回りして防止することを可能にするアクションプランを導入します。

自動的なタグ付け・リスク要因の高いドキュメント対策・アクセス許可違反およびポリシー違反の発生を防ぐ環境の構築・位置情報を基準としたモバイルアクセスコントロールなどの機能を備え、コンテンツレベルまでを対象とした粒度の細かいスキャンを実行します。

セキュリティトリミング・優先順位付けを組み込んだレポート出力機能で、コンテンツオーナーやコンプライアンス担当部署に、最優先に取り組むべき問題を分かりやすく提示することにより、迅速かつ効果的な問題の解決が可能になります。

SharePoint・ファイルサーバー・データベース・OFFICE 365、すべての環境で情報セキュリティを守る

スキャン・レポート作成・問題解決機能のすべてが組み込まれた AvePoint Compliance Guardian は、データが作成された瞬間からライフサイクルの終了までの全段階において、プライバシー・セキュリティ・コンプライアンス上の問題を未然に解決し、データセキュリティ上の問題発生リスクを抑制します。

また、AvePoint Compliance Guardian は、関連する問題を限定して表示するレポート作成機能とダッシュボード機能を備えています。発生した問題に応じ、適切な担当者に自動的に対策を促すため、迅速な問題の解決が可能になります。

Microsoft Partner

Gold Application Development
Gold Collaboration and Content
Gold Cloud Platform

www.AvePoint.jp

主要機能紹介

データ ディスカバリー

- ファイル タイプ・作成からの経過時間・サイズ・所有者・ファイルの置き場所・機密度等の指標を使用してマッピングし、場所別・違反タイプ別のリスク指標を算出
- 組織のファイルで発生するプライバシー／情報セキュリティ ポリシーへの違反を検出し、ロール (役割) もしくは所有者別にアサインを実行することにより、責任区分の明確化とデータの見える化を実現
- セキュリティ トレーニングや危険度・場所別の集中度を組み入れたレポートを生成し、リスクのヒートマップを作成。最も適切な人員が問題解決に的確な情報を得、迅速に問題に対処することができるような環境を構成

データ分類

- 情報ガバナンス チェック ファイルを使用して、組織の保有する環境を、リアルタイムと定期的からタイミングを選択できるスキャンで確認。平文検索・正規表現・レポート条件などを含むチェック ファイルは、デフォルトのまま使用することもカスタマイズして使用することも可能
- メタデータ分類エンジンで、コンテンツの分類を自動的に、もしくは担当者の確認を経てから実行
- コンテンツの分類に基づき、アクセス許可の割り当てや適切な場所への移動、ブロック・消去・検疫・暗号化・墨消しなどのアクションで機密情報対策を実行し、組織の情報ガバナンス ポリシーが遵守される環境を維持

データ損失防止 (DLP)

- スキャン画像・AutoCAD ファイル・zip ファイルなど数百種類のファイル タイプを、プライバシー・情報セキュリティの観点から査定可能
- 規定の数式とカスタマイズ可能なアルゴリズム数式を活用した高度なロジックにより、対象となるコンテンツの潜在的なリスクを算出することが可能に
- メタデータ分類エンジンを使用して、埋め込み型のメタデータにタグ付けを実行・コンテンツを分類
- コンテンツの分類に応じて、組織の情報ガバナンス ポリシー違反となるコンテンツの消去・検疫・適切な場所への移動を実行

インシデント管理

- 機密情報が含まれるファイルをスキャンし、自動実行可能なブロック・検疫・墨消し・暗号化・消去などのアクションを活用して対策を実行。スキャン実行のタイミングはファイルのアップロード時点・スケジュール設定・オンデマンドから選択可能。適切なユーザーもしくはユーザー グループに通知を送信し、詳細の確認・適切な対策の実行を推奨
- ロールに基づいたインシデント管理マップを活用し、コンテンツ作成者・コンテンツ 所有者・コンプライアンスおよび法務担当部門・ユーザー グループなどのロール別にコンテンツをマッピング。ポリシー違反の発生時に、適切な担当者に自動で警告を送信
- 明快なリスク計算システムに基づき、優先度順位付けされたインシデント レポートをソート。直観的に現況を把握できるヒート マップを表示し、違反が最も頻繁に発生する場所・最も頻繁に起こるポリシー違反を表示
- 自動実行可能なタグ付けに、担当者が誤検知の有無を確認するプロセスを加え、コンテンツへのタグ付けと分類を正確に実行

Compliance Guardian
に関するお問い合わせ

電話: (03) - 6853 - 6300
E-mail: SalesJP@AvePoint.com

AvePoint Japan 株式会社
〒108-0074
東京都港区高輪 4-10-18
京急第一ビル 11F

アポイントジャパン ブログ www.avepoint.co.jp/community/ をご覧ください。

その他ご希望の方はお問い合わせください。