FileAudit® ホワイトペーパー

オンプレ＆クラウドに点在するファイルの一元的な監査に数クリックで対応？更に不正アクセス対応も！

OCEANBRIDGE

ファイルサーバー・クラウドストレージの一元的なファイル監視とデータ侵害の検出と阻止を実現する

データ侵害の現在地

機密性の高い企業のデータは、不適切なアクセスや潜在的な盗難リスク、改ざんまたは削除といったアクションから保護する必要があります。このような不適切なアクティビティを迅速に検出、対応、さらには停止する手段としてのファイル監視ツールは企業のIT部門にとって、必要不可欠なものになりつつあります。

データ侵害を目的とした外部からのサイバー攻撃は、企業が現在直面している最もポピュラーな脅威の1つです。組織的にサイバー攻撃を行う集団は、ブラックマーケットにおいて高額で取引されるアカウント情報や個人情報、健康データなどを狙っています。このようなデータを保管している企業のデータベースがターゲットの１つとなっており、データ侵害の脅威にさらされていると言えます。

2017年に確認できているだけで、1億7,400万件を超えるデータが盗難被害に合いました。非常に大きな数のように見えますが、これは判明している数であり、全体の一部にすぎません。さらに発見を困難にしているのは、データ漏えいの場合、ほとんどが数分程度で特定されているのに対し、データ侵害の特定には月または年単位で時間がかかる場合が多いという事実です。このような背景から不適切なアクセスやアクティビティを迅速に検出する手段が必要とされています。

大切なデータはどこに保管されているのか？

ほぼすべての業界で、依然としてファイルサーバーは主要なデータ資産であり、企業のセキュリティにとって重要なポイントであるのは明確です。さらにクラウドストレージは数年前から、特に企業間での使用が増加しています。いまだに古い認識に基づいた、クラウドストレージに対する懸念は根深く残っていますが、現在では中小企業を含む、数多くの企業がクラウドのメリットを享受しています。

しかし、オンプレミスのファイルサーバーとクラウドのハイブリッド環境では、企業にとって重要な資産が点在することになり、両方のセキュリティをまとめて管理する難しさもあります。課題を認識するためにサイバー攻撃のターゲットとなるような、価値のあるデータやファイルとはどのようなもので、どこに保管されているかを把握する必要があります。注意すべきなのは下記のような情報です。

- クレジットカードまたは銀行口座情報
- 個人の健康情報（PHI）
- 個人を特定できる情報（PII）
- 企業機密情報
- 知的財産
- 資格情報

OceanBridge

企業によって違いはありますが、標的となるようなデータはデータベースやオフィスドキュメントだけでなく、データ転送操作の一部として使用されるファイルなどにも点在している可能性があります。ファイルアクセスがデータ侵害のポイントになります。

クラウドの不正アクセスの検出はオンプレミスより難しい？

従業員のアカウントの誤用と不適切なアクセス制御により、不正アクセスの検出は、今日のクラウドセキュリティ上の最大の懸念事項の1つです。中小企業の31%は、ストレージのためにクラウドに移行して以来、不正アクセスを検出するのが難しいと答えています。

従来、企業がオンプレミスのファイルサーバーにデータを保存する場合、データは不正使用から「比較的」安全です。ネイティブセキュリティでは、企業内の特定のユーザーか、またはユーザーグループのデータへのアクセスのみが許可されます。オフィスからのみファイルアクセスを許可する場合、社外からの不正アクセスに対して有効性がある境界を作ることができます。

この境界外からのアクセスに仮想プライベート ネットワーク (VPN) を使用する従業員やパートナーでも、IT部門は特定のデバイスへのアクセスのみを制限できるため、データは比較的安全です。

従業員の不正アクセスを止めるのは難しい？

確かに、オンプレミスのファイルサーバーとPCだけの環境では、誰かが機密情報を盗もうとした場合、発見されるリスクがはるかに高くなりますが、従業員がノートPCや、スマートフォンやタブレット(個人端末を含む)を使用してクラウド内の情報にアクセスできる場合、どこからでもアクセスできるため、辞める前に情報を盗むのは簡単に行うことができてしまいます。

実際、以前行ったIS Decisionsの調査によると、元従業員の3分の1は退社後も会社のデータにアクセスできることがわかりました。さらに22%が漏えいした従業員のログイン情報により、外部の悪意のある第三者により、システムにアクセスされたことがあるということがわかりました。

侵害の結果は非常に大きな損害となっており、15%がクラウドネットワークに保存されている機密性の高い企業データに不正にアクセスされたことにより、著しい風評被害を受けたと考えています。

データ侵害の特定に重要なポイントはファイル監視

データ侵害を特定して保護するためには、エンドポイント検出、ファイアウォール、脆弱性保護、データ損失防止、SIEMソリューションなどといった、大がかりなセキュリティソリューションのパッケージが必要だと思われるかもしれません。

確かに、これらはセキュリティ戦略全体では重要なものです。しかし、結局のところ、ファイルシステム自体が、悪意のあるアクティビティを進行するためのターゲットや、資産として利用されるため、ファイル監視をしっかりと行うことがデータ侵害のセキュリティ戦略の重要なポイントになるのです。

ファイル監視を活用してデータ侵害を検知、阻止するにはどうすればよいか？

基本的にファイル監視自体は、ファイルシステムに対して実行された、すべてのアクションログの記録にすぎません。コピー、移動、読み取り、削除、名前、権限、所有権の変更などは、すべてログに記録され、分析、レポートが可能です。このような複数のファイルアクティビティを単一のアクションとして表示するためには、サードパーティのソリューションを使用する必要があります。

また、オンプレミスとクラウドのハイブリッド ストレージ環境で運用している場合、特にセキュリティ面で苦労しています。双方に対応できる一元化したセキュリティが確保できていないことが要因となっており、オンプレミス、クラウド、両方のストレージ環境のセキュリティを一元化できるツールが必要です。

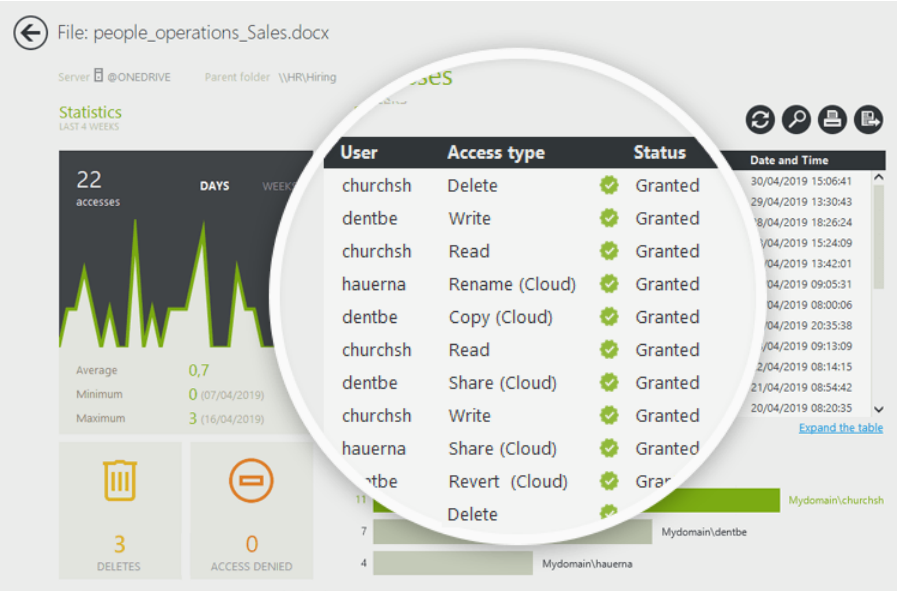
FileAudit がハイブリッド環境のセキュリティを支援

FileAuditは、ファイルやフォルダへのすべてのアクセスを事前に追跡、監査、レポートし、その発生した時点で、疑わしいファイルアクティビティを 担当者に警告します。従来、FileAuditはWindows Active Directoryベースのサーバー上のファイルとフォルダを監視しましたが、現在、FileAuditの監視機能はGoogleDrive、box、OneDrive、Dropboxまで拡張しています。

オンプレミスとクラウドストレージのハイブリッド環境のストレージを管理する場合、FileAuditを活用することで、一元化された管理画面から、すべてのストレージ、サーバー上のデータのセキュリティを確認することができます。

FileAuditを使用すると、委任を通じてファイルアクセスの監視を簡単にすることもでき、生産性とセキュリティの両方に役立ちます。IT担当者が、ユーザーがどのアクセスを必要としているか、またファイルの使用が適切か、といった詳細を確認するために毎回連絡を行うことは難しいです。

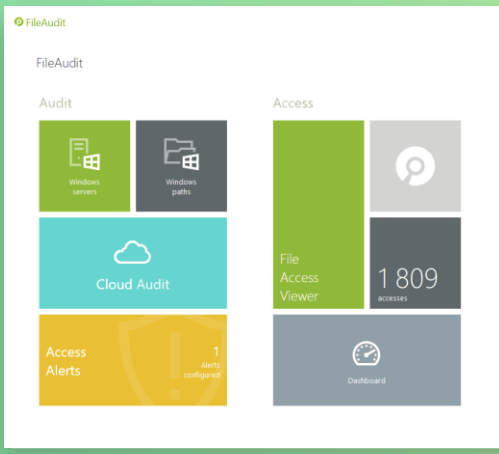
企業に積極的に関与している人々にファイルアクセスを管理する権限を委任することにより、管理者は「通常の」アクセスであれば、どのように見えるかという判断が可能となり、異常を迅速に発見することを容易にして負担を軽減します。



OceanBridge

FileAudit®

FileAuditはクラウドストレージのログにも対応したファイルサーバーログ管理ツールです。ファイル サーバー監査をより速く、よりスマートに、より効率的に行います。すべてのアクセスを追跡、監査し、レポーティングや不正アクセス検知を実現。



FileAuditの主な機能とメリット

主な機能

- ファイルとフォルダのリアルタイム監視
- ファイルアクセス操作への警告と自動対応
- クラウドデータを含めた統合的な監視
- ファイルとフォルダのアクセス監査
- NTFS権限とプロパティのレポート
- スケジュールレポートと長期的なアーカイブ

主な導入メリット

- 機密性の高いファイルやフォルダへのアクセス監視の作業負荷を大幅削減
- 不適切なアクセス、潜在的な漏洩リスク、変更、削除操作に対する保護
- 緊急事態で即座に、自動的に対応
- 正確なIT上の法的立証を実現
- オンプレとクラウド上のファイルを保護
- 法令遵守（GDPR, HIPAA, SOX, FISMAなど）

対応サーバー・クラウドストレージ

Windows Server / OneDrive / SharePoint Online / Google Drive / Dropbox / Box

フル機能を無料で20日間お試しいただける体験版もご用意しております。
下記サイト、またはfileaudit@oceanbridge.jp (FileAudit担当)まで
お気軽にお問い合わせください。

■製品情報サイト　：https://www.isdecisions.jp/fileaudit/
■体験版お申込み　：https://www.isdecisions.jp/trial
■製品お問い合わせ：https://www.isdecisions.jp/contact

OCEANBRIDGE
つかえるITを、世界から。

株式会社オーシャンブリッジ
〒 107-0051 東京都港区元赤坂1-5-12 住友不動産元赤坂ビル7F
https://www.isdecisions.jp/
fileaudit@oceanbridge.jp