

ソフォスと Veeam の統合

重要なバックアップデータを標的とする脅威を阻止

攻撃者は、過去1年間のランサムウェア攻撃の75%¹でバックアップリポジトリに影響を与え、バックアップを改ざんし、データを削除して回復を阻止しました。このたび、ソフォス製品と Veeam は、バックアップデータに対する脅威の発生時にセキュリティ情報をシームレスにやりとりできるようになりました。これにより、可視性を拡張してアクティブな攻撃の検出、調査、対応を行うことで、サイバーレジリエンスを簡素化します。

ユースケース

1 | ランサムウェア攻撃に対する防御

期待される結果:ランサムウェア攻撃の最強の防止策を入手してください。

対策:ソフォスは、新しい亜種やローカル/リモートの暗号化攻撃など、ランサムウェアがシステムに影響を与える前に、ランサムウェアを幅広く検出して阻止する、業界をリードしたテクノロジーを提供しています。ソフォスの高度な検出、保護機能と Veeam が提供する揺るぎないバックアップおよびバージョン機能を組み合わせることで、バックアップを安全で復旧可能な状態に維持することが可能となります。

2 | 脅威の可視性を拡張

期待される結果:バックアップデータに影響を与える可能性のある潜在的な脅威を特定します。

対策:ソフォスと Veeam の統合は、Sophos MDR (Managed Detection and Response) サービスおよび Sophos XDR (Extended Detection and Response) ソリューションで利用できます。バックアップリポジトリの削除、多要素認証の無効化、暗号化パスワードの変更など、バックアップに影響を与える悪意のあるアクティビティを可視化します。

3 | バックアップの整合性と可用性の確保

期待される結果:バックアップデータはいつでも利用可能で保護されているため、安心できます。

対策:ソフォスの強力な統合により、脅威の検出、疑わしいアクティビティの調査、そして最終的にはデータの迅速な回復を可能にし、ビジネスを継続することができます。Sophos と Veeam を組み合わせて使用すれば、バックアップの整合性および可用性を確保し、マルウェアはもちろん、意図せぬデータ削除や、内部のセキュリティ脅威など、さまざまな原因によるデータ消失のリスクを減らすことができます。

4 | 脅威への対応時間を短縮

期待される結果:ダウンタイムを最小限に抑え、ビジネス継続性を確保します。

対策:Sophos MDRは、人間主導の24時間年中無休の脅威防止、検出、および対応サービスで、組織を最も高度な攻撃から保護します。ソフォスの専門家は、脅威ハンティングを実行して、防御ツールをバイパスしようとする攻撃者の手法を特定し、確認した脅威を阻止するための対応アクションを実行します。平均対応時間は38分と業界トップで、これは業界ベンチマークを96%上回ります。



MDR サービスで Gartner の「Customers' Choice」を獲得

Gartner®

2023 Magic Quadrant for Endpoint Protection Platforms のレポートでは14回連続でリーダーに選出

MITRE ATT&CK.

マネージドセキュリティサービスの MITRE ATT&CK 評価でトップパフォーマンスを発揮するベンダー

詳細情報:

www.sophos.com/mdr
www.sophos.com/xdr

¹Veeam 2023 ランサムウェアトレンドレポート