

Change Auditor for Exchange

ExchangeおよびExchange Onlineのリアルタイム監査

Eメールは、組織内および組織間のコミュニケーションの主要なビジネスツールになっています。その結果、Eメールは情報のリポジトリとして機能していますが、情報の一部は機密性が高く、誤用に対して脆弱です。ほとんどのセキュリティアクションは監査されていないため、多くの組織ポリシー違反は検出されずにいます。これにより、生産性が失われ、システム停止が発生する可能性があります。これは、どんな組織も避けなければならないリスクです。

今日、企業は、法令遵守を証明し、効率を促進するために、Microsoft Exchange ServerとOffice 365のセキュリティおよびコンプライアンスについての詳細な監査とレポート作成を必要としています。

Quest® Change Auditor for Exchangeは、お客様のExchange環境内で発生したアクティビティをプロアクティブに監査し、重要なメールボックスへのアクセスを防止し、重要な変更があった場合には詳細なアラートをリアルタイムで提供します。継続的に情報を把握することは、Exchange ServerおよびExchange Onlineの構成および権限

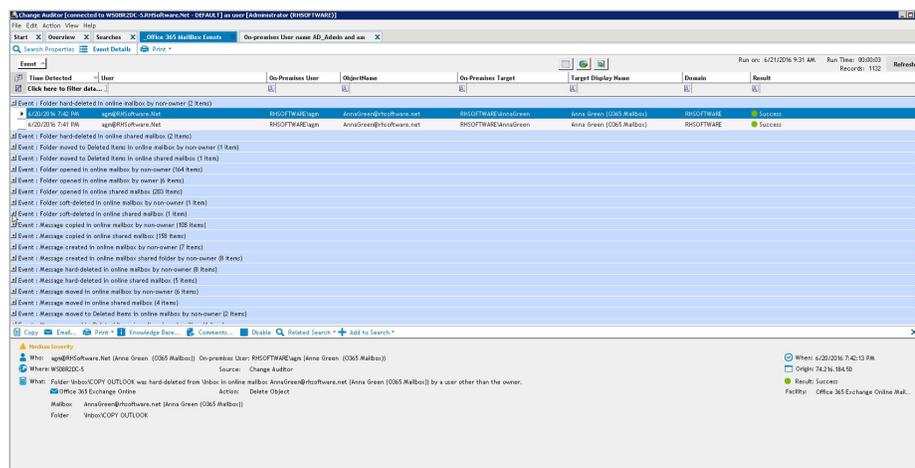
に対する変更をプロアクティブに監査しながら、コンプライアンスを証明し、セキュリティを促進し、稼働時間を向上させるために役立ちます。ExchangeおよびExchange Onlineのセキュリティおよびポリシー設定における、追跡、警告、およびレポートの機能を利用できるほか、元の値と現在の値を含む、主要な変更に関連するすべての情報を自動的に収集することで、その他の問題も迅速にトラブルシューティングできます。

重要な変更をすべて監査

Change Auditor for Exchangeは、Exchange ServerおよびOffice 365のホストされたExchangeコンポーネントに対するすべての重要な変更に適した広範かつカスタマイズ可能な監査とレポート作成を提供します。これには、管理グループ、メールボックスポリシー、パブリックおよび個人情報ストアの監査や、ActiveSyncメールボックスポリシーの変更、配布リストの変更などの組織的な変更が含まれます。時間の経過とともに完全な可視性を時系列順に得ることが可能です。すべての変更について、いつ、誰が、何を、どこで、なぜ、

メリット:

- 数分程度でインストールでき、迅速なイベント収集でExchangeおよびExchange Online環境を即座に分析
- 1つのクライアントで全社規模の監査とコンプライアンスが可能
- 機密性の高いメールボックスや重要なメールボックスへのアクセスを阻止することで内部制御を強化し、アクセス権限のあるユーザを制御
- デバイスを問わないリアルタイム通知で即座に対応し、セキュリティリスクを低減
- すべてのイベントおよび特定のインシデントに関する変更を追跡して未知のセキュリティの問題をなくし、ExchangeおよびExchange Onlineの構成、メールボックス、およびユーザへの継続的なアクセスを確保
- ポリシーおよびExchangeパブリックフォルダに対する変更のプロアクティブなトラブルシューティングを有効にすることにより、可用性を促進
- ネイティブの監査機能を使用せずにイベントを収集することにより、サーバ上でのパフォーマンスの低下を抑えてストレージリソースを節約
- GDPR、SOX、PCI DSS、HIPAA、FISMA、SAS 70など、内部ポリシーおよび外部規制のコンプライアンスレポート作成を合理化
- 情報に基づいて、監査人や経営陣に役立つインテリジェントで詳細なフォレンジックを実現



Change Auditor for Exchangeの概要画面

Exchangeユーザは数か月でROIを獲得

調査した、Change Auditor for Exchangeを選択したIT組織の69パーセントが、6~9か月以内に投資を回収しています。

TechValidate調査

システム要件

詳細な要件の完全なリストについては、リリース・ノート・ガイドをご覧ください。

どのワークステーションで行ったのか、その詳細なフォレンジック、その他の関連イベントの詳細、およびイベント前後の値も確認できます。また、すべてのデバイスに対する警告をリアルタイムで受け取ることができるため、常に状況を把握でき、重要なポリシー変更が発生すれば、どこからでもそうした事態に対処して日常の変更に伴うリスクを軽減できます。

ユーザのアクティビティを追跡し、機密性の高いメールボックスを保護

Change Auditor for Exchangeは、ユーザアカウントおよび配布制限の変更に対するユーザおよび管理者のアクティビティを追跡することで、企業全体の監査およびコンプライアンスのポリシーの強化に役立ちます。また、Change Auditorは、権限のないユーザがメールボックスにアクセスすることを防止し、別のユーザのメールボックスにアクセスした管理者およびユーザに関する情報を提供します。そのメールボックスから誰がアクセス、削除、コピー、移動、および作成したEメールかを正確に知ることができます。24x7のリアルタイムの警告、詳細な分析、およびレポート作成機能により、ExchangeおよびExchange Onlineインフラストラクチャは、不審な行動または不正なアクセスから保護され、常に企業および政府の標準に準拠します。

ACTIVESYNCによるモバイルデバイスの監査

MicrosoftのActiveSyncテクノロジーを使用して、モバイルデバイスを監査し、Eメールおよびカレンダーへのアクセス、デバイスの登録などを追跡します。

無関係なデータを意味のある情報に変換してセキュリティとコンプライアンスを促進

Change Auditor for ExchangeはExchangeおよびExchange Online環境における重要な変更を追跡し、生データを意味のあるインテリジェントなデータに変換することで、インフラストラクチャのセキュリティとコンプライアンスを保護しま

す。Change Auditorのハイパフォーマンスな監査エンジンによって監査上の制約は過去のものとなりつつあります。ネイティブの監査ログは不要で、より迅速に結果を得られ、ストレージリソースも節約できます。

統合イベント転送

SIEMソリューションと簡単に統合して、Change AuditorイベントをSplunkやArcSight、QRadarに転送できます。さらに、Change AuditorはQuest® InTrust®と統合して、20:1に圧縮されたイベントストレージおよび一元化されたネイティブまたはサードパーティのログ収集、アラート機能による解析と分析、不審なイベントに対する自動応答アクションを実現します。

企業と政府の規制に合わせてレポート作成を自動化

Change Auditor for ExchangeではMicrosoftのSQL Reporting Service (SRS)を使用して、意味のあるセキュリティおよびコンプライアンスレポートを瞬時に作成します。内蔵のコンプライアンスライブラリと独自のカスタムレポートを作成する機能により、EU一般データ保護規則 (GDPR)、サーベンスオクスリー法 (SOX)、PCIデータセキュリティ基準 (PCIDSS)、医療法典の携行性と責任に関する法律 (HIPAA)、連邦情報セキュリティマネジメント法 (FISMA)、米国監査基準第70号 (SAS 70) などの標準への準拠を簡単に証明できます。

QUESTについて

Questは、急速に変化するエンタープライズITの世界にソフトウェアソリューションを提供しています。データの爆発、クラウドサービスへの拡張、ハイブリッドデータセンター、セキュリティ脅威、規制上の要件によって生じる課題のシンプル化を支援します。Questのポートフォリオは、データベース管理、データ保護、統合エンドポイントの管理、IDおよびアクセス管理、Microsoftプラットフォーム管理などのソリューションで構成されます。