Change Auditor for Active Directory

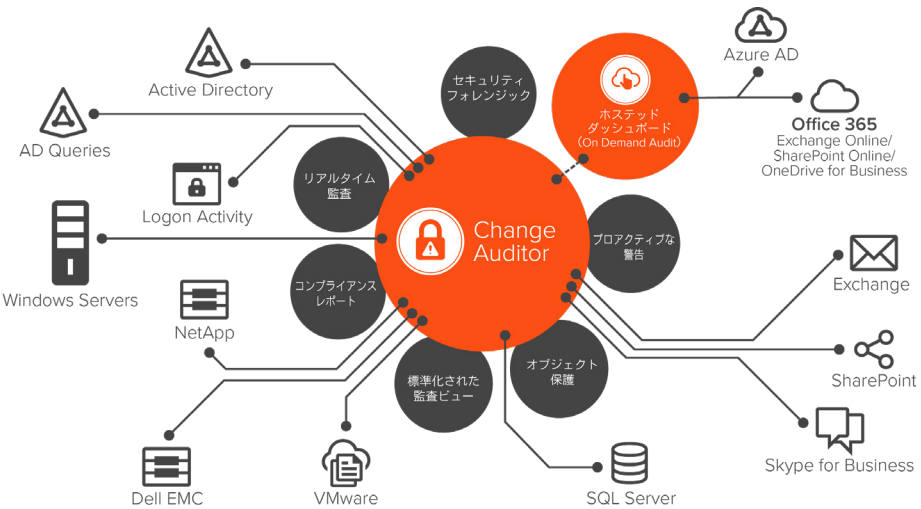
Active DirectoryおよびAzure Active Directoryのリアルタイム監査

Active Directory（AD）に関する問題は、サービス中断という予想外の手痛い損害を招くほか、業務に大きな影響を与えるネットワークのダウンタイムも引き起こすおそれがあります。また、有害なデータ漏洩が発生したり、SOX、PCI、HIPAA、GDPRなどのコンプライアンスに違反したりした場合も、大きな損害を被ることがあります。そこで必要なのが、Active Directoryの監査とセキュリティです。これによって、AD、Azure ADを問わず、重要な変更が行われた場合に通知をリアルタイムで受け取れるようになります。

Quest® Change Auditor for Active Directoryは、ADとAzure ADのセキュリティと制御を促進するために、すべての重要な設定変更を追跡し、単一のコンソールに統合します。Change Auditorは、オンプレミスおよびクラウド環境に影響を及ぼす変更について追跡、監査、報告、および警告を行います。その際に、ネイティブの監査機能実行によるオーバーヘッドは生じません。Change Auditor for ADを使用すると、すべての変更および関連するイベント詳細が標準化されて表示されます（例: 変更前後の値や関連するオンプレミスおよびクラウドIDなど）。また、監査要件を満たすために特定の変更が行われた理由を説明するコメントを追加することもできます。Change Auditor for ADを使用すると、あらゆる重要な変更を素早く効率的に監査して、貴重なデータやリソースの安全性を確保できます。

重要な変更をすべて監査

ADおよびAzure ADのあらゆる重要な変更に関する広範かつカスタマイズ可能な監査およびレポートを取得できます（例えば、グループポリシーオブジェクト（GPO）、ドメイン・ネーム・システム（DNS）、サーバ構成、ネストされたグループ、その他多数に対して行われた変更）。ネイティブ監査と異なり、ADおよびAzure AD環境のオンプレミス、クラウド、およびハイブリッドADのすべての変更アクティビティが、期間中のその他のイベントに関連する詳細なフォレ



Change Auditor for Active Directoryを使用すると、誰が、何を、いつ、どこで変更したか、どのワークステーションで変更が行われたかに関する情報を時系列順に取得できます（関連するオンプレミスおよびクラウドIDなど）。

「私たちが依頼したペンテスターも、Change Auditorのオブジェクト保護を通過できなかったことにとても驚いていました。」

大手小売チェーン、
エンタープライズ管理者

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即座に分析
- 1つのクライアントで全社規模、オンプレミスとクラウドサービスの監査とコンプライアンスが可能
- 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セキュリティに関する未知の懸案事項をなくし、アプリケーション、システム、およびユーザへの継続的なアクセスを確保
- デバイスを問わないリアルタイムの警告で即座に対応し、セキュリティリスクを低減
- 望ましくない変更の防止によって社内の制御を強化し、認定ユーザの制御権限を制限
- アカウントのロックアウトをプロアクティブにトラブルシューティングすることにより、可用性を向上
- 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
- 企業のポリシーやGDPR、SOX、PCI DSS、HIPAA、FISMA、SAS 70など政府が定める規制法令へのコンプライアンスを合理化
- 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

「全体的に見て、Change Auditorは非常に役立っています。当校が検討した製品の中で、Active Directoryのすべての変更に対してWindowsの監査機能を有効にする必要なく、これほどのレベルのリアルタイム監査と保護機能を提供するものは、他にありませんでした。」

*Patrick Rohe*氏
シニア*IT*アーキテクト
タウソン大学

システム要件

最新のシステム要件の詳細な一覧については、quest.com/products/change-auditor-for-active-directoryをご覧ください。

ンジックと共に時系列順に統合ビューに表示されます。また、プロアクティブなアラートを受け取ることができるため、常に状況を把握できます。重要なポリシー変更やセキュリティ侵害が発生した際には、場所やデバイスを問わず対処できるため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て望ましくない変更を防止

アカウントのロックアウトと重要なレジストリ設定へのアクセスに関するユーザと管理者のアクティビティを追跡することによって、全社規模の変更および制御ポリシー強化に役立ちます。重要な変更の発生を最初の段階でプロアクティブに制御し、24時間365日アラートを発行します。また、詳細な分析、変更前の値のリストア機能、およびレポート作成機能により、ADおよびAzure AD環境が不正アクセスを狙った疑わしい行動にさらされることを防止して、常に企業と政府が定める規則に準拠した状態を維持します。

ON DEMAND AUDITと統合されたホステッド監査ダッシュボード

On Demand Audit Hybrid Suite for Office 365にアップグレードして、Change Auditor for Active DirectoryおよびOn Demand Auditの両方も利用できるようになりました。数回のクリックで組み合わせるだけで、AD、Azure AD、Exchange Online、SharePoint Online、およびOneDrive for Business全体に及ぶすべての変更が単一のホステッドビューに表示されます。応答の速い検索とインタラクティブなデータの可視化によって調査を簡素化し、監査履歴を最長10年間保存します。

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

重要な変更を追跡し、生データを意味のある情報へと変換することで、お客様の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ちます。Change Auditor for ADを使用すると、誰が、何を、いつ、どこで変更したか、どのワークステーションで変更が行われたかに関する情報を、関連するイベント詳細（例: 変更前後の値）と共に取得できます。したがって、素早くセキュリティ関連の意思決定を行えます。また、Change Auditorのハイパフォーマンスな監査エンジンを使用すれば、監査の制限がなくなります。ネイティブ監査ログを必要とせずに、より短時間で結果が得られ、ストレージを節約できます。

統合イベント転送

SIEMソリューションと簡単に統合でき、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、および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

組み込みのコンプライアンスライブラリとカスタマイズ可能なレポートを使用すれば、GDPR、SOX、HIPAA、PCI DSS、FISMA、SAS 70などの政府の規制へのコンプライアンスの証明は極めて容易です。

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。

Quest
quest.com/jp
世界各地のオフィスの情報については、(quest.com/jp-ja/locations)をご覧ください。

DataSheet-ChangeAuditor4AD-US-KS-JA-WL-59235