Change Auditor

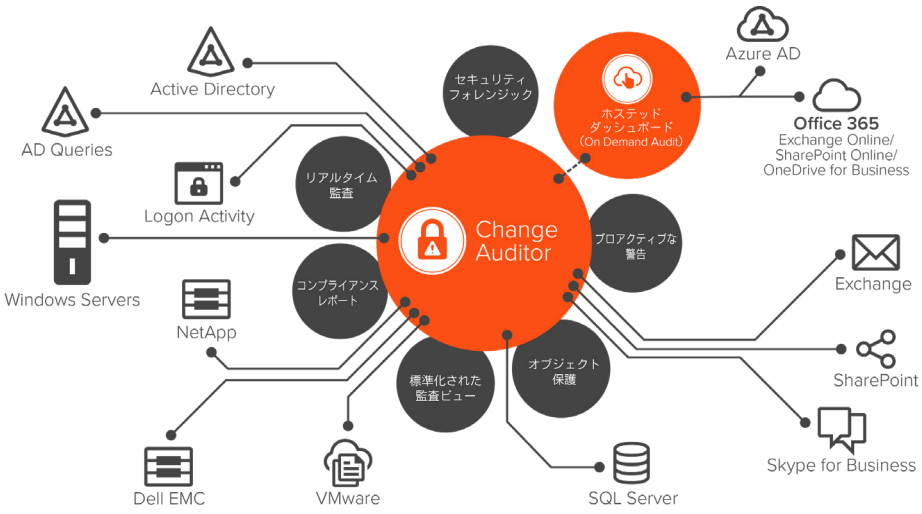
Microsoftプラットフォーム環境の変更監査をリアルタイムに

企業のアプリケーションおよびサービスに関するイベントロギングや変更レポートは、面倒で時間がかかり、場合によってはネイティブ監査ツールでは不可能なこともあります。中央コンソールがないため、サーバごとにプロセスを繰り返す必要があり、その結果、コンテキストのない膨大なデータと無数のレポートを抱えることになります。

つまり、コンプライアンスを証明したり、イベントに迅速に対応したりする作業に絶えず追われるのです。データセキュリティもリスクにさらされます。ネイティブイベントの詳細が不足しており、解釈が困難だからです。その結果、手遅れになるまで問題を見つけることができない可能性があります。ネイティブツールは、特権ユーザがイベントログを消去することを防止できないため、ログデータを失う可能性があり、そもそもの監査目的を果たせなくなります。

しかし、ご安心ください。Quest® Change Auditorがあります。この製品ファミリーを使用すると、Active Directory（AD）、Azure AD、Exchange、Office 365、SharePoint、Skype for Business、VMware、EMC、NetApp、SQL Server、およびWindowsファイルサーバに対するすべての変更と、ADに対するLDAPクエリについて、監査、警告、およびレポートすることが可能です。すべてリアルタイムで行われ、ネイティブ監査を有効にする必要もありません。

1つの中央コンソールから、環境を簡単にインストール、展開、および管理できます。作成、削除、変更、およびアクセスの試行を追跡することは、これ以上ないほど簡単で、何が起きたかも簡単に理解できます。各イベントとすべての関連イベントが簡単な表現で表示され、必須の5つのW（いつ、誰が、どこで、何を、どのワークステーションで）に関する情報に加えて、過去と現在の設定が表示されるからです。



Change Auditor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:

- 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、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。
- 暗号化データおよびその重大度を自動的に解釈することにより、ストレスと複雑さを軽減して、より迅速で適切な意思決定を実現。
- 社内外のあらゆるデバイスにリアルタイムで警告を送信して瞬時の対応を可能にし、セキュリティのリスクを数秒程度で緩和。
- 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制。
- SOX、PCI DSS、HIPAA、FISMA、SAS 70など、内部ポリシーおよび外部規制から分離されたコンプライアンスレポート作成を合理化。
- マネージャと監査人に、適切なIT制御の証拠を提供して安心感をもたらす。

この幅広いデータ分析により、問題が発生した場合に、特定のユーザまたはワークステーションからどのようなその他の変更があるかを特定するなど、ただちにアクションを実行できるので、推測を重ねる必要がなく、セキュリティに関する未知の懸案事項を排除できます。増大するコンプライアンスの要求を満たす場合でも、内部セキュリティポリシーを満たす場合でも、Change Auditorは頼りになるソリューションです。

「以前は問題の調査に1時間はかかっていましたが、Change Auditorによって、たったの5〜10分に短縮されました。」

Dennis Persson氏（Region Halland、ITシステム技術者）

製品
Change Auditor for Active Directory
Change Auditor for Active Directory Queries
ChangeAuditor for EMC
ChangeAuditor for Exchange
Change Auditor for Logon Activity
ChangeAuditor for NetApp
Change Auditor for SQL Server
ChangeAuditor for SharePoint
Change Auditor for Skype for Business
ChangeAuditor for VMware vCenter
Change Auditor for Windows File Servers

特長

相関関係を示すビューによるハイブリッド環境の監査 — AD/Azure AD、Exchange/Exchange Online、SharePoint/SharePoint Online/OneDrive for Businessなどのハイブリッド環境のほか、ADログオンおよびAzure ADサインインを監査します。ネイティブ監査と異なり、Change Auditorでは、ハイブリッド環境全体のアクティビティの相関関係を単一のビューで確認できるため、オンプレミスかクラウドサービスかを問わず、発生したすべての変更を把握することができます。

変更防止 — ADやExchangeおよびWindowsファイルサーバ内の、特権グループ、グループポリシーオブジェクト、機密のメールボックスなどの重要データに対する変更から保護します。

監査人対応のレポート作成 — SOX、PCI DSS、HIPAA、FISMA、GLBA、GDPRなどの法令を順守し、ベストプラクティスに基づいた包括的なレポートを生成できます。

On Demand Auditと統合されたホステッドダッシュボード — 応答性の高い検索、インタラクティブなデータの可視化、および長期間のイベントストレージを備えたホステッドSaaSダッシュボードから、ハイブリッドADおよびOffice 365のアクティビティを同時に表示します。

ゴールデンチケットの検知 — ゴールデンチケット/Pass-the-ticket攻撃中に使用される一般的なKerberos認証の脆弱性を検知して、警告します。

高性能な監査エンジン — 監査上の制約を解消し、ネイティブの監査ログに頼ることなく変更内容を把握できます。これにより、より早く結果を得ることができ、ストレージリソースを大幅に削減できます。*

アカウントのロックアウト — ロックアウトイベントでは元のIPアドレスとワークステーション名を取得し、関連するログオンやアクセスの試みをインタラクティブなタイムラインで表示します。これは内部および外部のセキュリティ脅威の調査と検知をシンプル化するのに役立ちます。

移動中も可能なリアルタイム警告 — 重大な変更やパターンが検出された場合に、至急の対応を促す警告をEメールやモバイルデバイスで受け取ることができます。これにより、現場にいないときでも、セキュリティの脅威に迅速に対応できます。

統合イベントの転送 — 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。

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。

*SharePoint、EMC、NetApp、およびVMwareには適用されません。

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-ChangeAuditor-US-LR-JA-WL-59232