セキュリティと生産性を向上させた政府関連機関

テキサス州北部中央自治体評議会（NCTCOG: North Central Texas Council of Governments）は、QuestのMicrosoft Platform Managementソリューションによって、ハイブリッドIT環境全体における変更に対してリアルタイム制御を実現しました。

「以前のソリューションでは、消えてしまったフォルダについて、翌日まで何が起きたか説明できませんでした。でも今はChange Auditorのおかげで、そのフォルダに何が起きたか即答することができます。もし誰かが不注意で移動した場合であれば、その人物に元の場所に戻すよう伝えるか、手早く自分で戻すこともできます」

テキサス州北部中央自治体評議会、情報セキュリティオフィサー、Brett Ogletree氏

お客様のプロファイル

North Central Texas Council of Governments

会社名	テキサス州北部中央自治体評議会
業種	政府機関
国	米国
従業員数	400
Webサイト	nctcog.org

ビジネスニーズ

テキサス州北部中央自治体評議会では、ADの変更を監査する機能を備えておらず、ファイルシステムの監査も、夜間プロセス後にのみ行われるサードパーティソリューションを利用していたため、監査要求や問題発生時へのタイムリーな対応が限られていました。

ソリューション

同評議会は、AD、Windowsファイルサーバ、EMC向けのChange Auditorのソリューションを利用することで、必要としていた包括的なリアルタイム監査ができるようになりました。アラートは重大なイベントへの迅速な対応を可能にし、レポートのスケジュール設定は、ビジネスオーナーが定期的なレビューを行うのに役立っています。また、IT Security Searchの統合により、調査の合理化が実現されています。さらに評議会は、SharePointおよびSQL用のChange Auditorモジュール、そしてEnterprise ReporterとSecurity Explorerにも投資しました。

メリット

- リアルタイムの監査、レポート作成、環境全体にわたるアラート機能を実装
- 統合クロスシステム検索による合理化された問題調査を実現
- 以前のソリューションよりはるかに多くの機能を備えながら金額はそのまま

ソリューションの概要

- Microsoftプラットフォーム管理

政府関連機関は効率的な運用のために、中小企業や大企業と同様にテクノロジーを必要としています。そして、ITスタッフは最小限に留められており、それが一般的になっています。テキサス州北部中央自治体評議会は、例えば、EメールやVOIPシステムのような基本的なテクノロジーだけでなく、地理情報システム、文書管理システム、車道モデリングアプリケーションなどの専門的なシステムも運用の大部分に活用しています。同評議会のITセキュリティチームは、変更監視の自動化およびセキュリティ調査のスピードアップのため、QuestのWindows管理ソリューションのスイートを利用しています。

「Change Auditorはセキュリティだけでなく、業務の生産性も向上するため、かなりの時間節約にもなります。その機能には、お金に換算できないほど大変貴重な価値があります」

テキサス州北部中央自治体評議会、情報セキュリティオフィサー、Brett Ogletree氏

リスクが急増するのは、ADおよびFILE SYSTEMSへのリアルタイムなインサイトが不十分なときです。

同評議会は、ダラスとフォートワース内および周辺の16の郡と複数の町、学区、特別自治で構成される組合です。同評議会は各メンバーが、共通のニーズについて計画し、各地域における機会を認識し、不必要な重複を排除できるようにサポートします。例えば、運輸部門は地域の政府事業体と組んで車道プロジェクトに優先順位をつけ、資金をこれらの優先順位に従って割り当てます。一方、人事部門はトレーニングの機会を提供し、保育サービスの利用を促進し、その他の部門は地域利益のためのパートナーシップづくりに携わります。

同評議会のITチームは、これらすべてのアプリケーションのセキュリティと可用性に対して、Active Directory（AD）が重要であることを認識しています。なぜならユーザ、グループ、権限などの重要な情報が保存されるからです。例えば、グループ権限に対するたった一つの不適切な変更によって、そのグループメンバー全員が重要なリソースにアクセスできず、重要な業務プロセスが損なわれかねません。さらには、そのグループの全メンバーが閲覧許可のない極秘データにアクセスできるようになる可能性もあり、組織をセキュリティ違反とコンプライアンス不履行のリスクに追い込まれることにもなりかねません。

実は同評議会は、数年前まさにこのような状況に陥ったことがあったのです。「そのときはActive Directoryに何が起きているのか知る由もありませんでした」とテキサス州北部中央自治体評議会の 情報セキュリティオフィサーであるBrett Ogletree氏は言います。「例えば、誰かがアカウントを削除したり、グループポリシーオブジェクトを変更しても、誰の責任なのか、不注意からなのか、故意によるものなのか知るすべがありませんでした。そのため、変更を行った人が誠実に話してくれることを望むしかありませんでした」

しかしそれは問題のたった一部だったのです。ITチームはファイルシステムとADのリアルタイム監査が必要です。重要なファイルが変更または削除された場合、例えば、それを誰が実行したのか、そしてその人物がアクセスしたネットワーク上に他にどのようなリソースがあるのか、すぐに特定できる必要があります。同評議会のITチームは、ADよりも高い可視性をファイルサーバに備えていましたが、それでも十分とは言えませんでした。

製品とサービス

ソフトウェア
Change Auditor for Active Directory
ChangeAuditor for EMC
ChangeAuditor for SharePoint
ChangeAuditor for SQL Server
ChangeAuditor for Windows File Servers
Enterprise Reporter Suite
Security Explorer

「当初、ファイルシステムへの変更を誰が行ったかを特定するためにネイティブツールの使用を試みましたが、扱いにくく、何が起きたかを解明するのに大変な作業量を必要としていました」とOgletree氏は当時を振り返ります。「そのため、ファイルの変更または削除を誰が実行したのか、そして特定のユーザまたはグループのユーザがネットワーク上で何にアクセスしたのかがわかるソリューションを購入したのです」

しかしながら、その情報は24時間までしか保存できなかったため、実用性が限られていました。「そのツールはリアルタイムのファイルサーバ監査ではなく、毎夜定時にファイルサーバ内をクロールして重要なデータを調べるものだったので、情報は常に古いものでした」とOgletree氏は付け加えます。「例えば、見つけられなくなったフォルダに何が起きたのか尋ねるリクエストが午後にあっても、次の朝まで回答できなかったのです。これでは生産性の損失につながり、ファイルシステムのセキュリティもリスクにさらしてしまいます」

QUESTの包括的なリアルタイム監査

同評議会のITチームは、まずAD監査機能を充足させることに取り組むことにしました。複数のソリューションを入念に検討した結果、評議会はQuest® Change Auditor for Active Directoryを選択しました。このソリューションは、ADへの変更すべてをリアルタイムで追跡するため、ユーザはセキュリティまたは業務の継続性を脅かす潜在的な内部攻撃および不注意による変更を、迅速かつ簡単に検知することができます。頭を抱えるたくなるような複雑なネイティブツールなしにすべてできるのです。ITチームは、未承認の変更またはボタンのクリックによる不適切な変更を削減することができます。さらに、特定の組織単位（OU）やグループポリシーオブジェクト（GPO）などの最も重要なADオブジェクトへの変更をプロアクティブに防止することもできます。

このソリューションが大変役立ったため、同評議会はファイル監査用にその姉妹アプリケーションを検討することにしました。それらはChange Auditor for Windows File ServersとChange Auditor for EMCです。特に同評議会では、ADで取得できるようになったリアルタイムのインサイトを、ファイルシステムでも取得する必要がありました。現行ソリューションではその機能がなかったからです。同評議会ではすでにChange Auditor for Active Directoryのためのインフラストラクチャが導入されていたため、評価用に2つのアプリケーションを追加するのは簡単なことでした。トライアルキーを導入するだけでよかったからです。

Change Auditor for Windows File ServersおよびChange Auditor for EMCによって、ITチームはリアルタイムの追跡、監査、レポート作成、アラート機能を利用できるようになり、セキュリティの脅威、可性の問題、ユーザからの要求に速やかに対応できるようになりました。さらにChange Auditorでは「誰が、何を、いつ、どこで、どのワークス

> 「Questから多数の製品を購入しましたが、年間メンテナンス費用は以前のソリューション用の費用と同じ金額です」
>
> *テキサス州北部中央自治体評議会、情報セキュリティオフィサー、Brett Ogletree氏*

テーションで変更が行われたか」に関する詳細と、変更前後の値を取得できます。これらは迅速なトラブルシューティングに不可欠です。加えて、重要なファイルとフォルダが変更されたり不注意から削除されないように保護することもできます。

Questのソリューションに切り替えると、これらの機能的優位性に加えて、さらに2つのメリットを受けることができます。1つは、Change Auditorファミリーのソリューションで統合を行うことで メンテナンスと操作がシンプル化されることです。2つ目ははるかに高い価値を提供するということです。「Questに求めるすべてがパッケージングされており、出費以上の価値がありました」とOgletree氏は言います。「Questから多数の製品を購入しましたが、年間メンテナンス費用は以前のソリューション用の費用と同じ金額です」

「重要度の高いイベントが発生した場合、Change AuditorがEメールでアラートしてくれるため、変更が変更管理プロセスに従って適切に行われたものか、またはハッカーによる悪意のある行為なのかを判断できます」

テキサス州北部中央自治体評議会、情報セキュリティオフィサー、Brett Ogletree氏

リアルタイムのアラート機能が脅威に迅速に対応

同評議会のITチームは、Change Auditorアプリケーションを導入してから、重要な変更を即座に把握できるようになりました。以前のように1日もかかることはありません。「重要度の高いイベントが発生した場合、Change AuditorがEメールでアラートしてくれるため、変更が変更管理プロセスに従って適切に行われたものか、またはハッカーによる悪意のある行為なのかを判断できます」とOgletree氏は説明します。「例えば、私たちは保護された医療情報を扱うグループなど、慎重に扱うべき特定グループのメンバーシップに対する変更に関してアラートが行われるようにChange Auditor for Active Directoryを設定しています」

Change Auditorは、同じようなリアルタイムアラートを同評議会のファイルシステムにも提供します。「マネージャの中には、セキュアなフォルダに権限を持たない人物がアクセスした場合にアラート通知を希望する人もいます」とOgletree氏は言います。「以前のソリューションにはこの機能はありませんでした。でも今ではアラートを簡単に設定し、不審なアクティビティはChange Auditorの自動監視に任せることができます」

合理化された問題調査

テキサス州北部中央自治体評議会は、Change Auditorの包括的で柔軟性のあるレポート作成を活用して、不審な変更およびその他のユーザの行動に対する詳細なインサイトを取得しています。「問題に対するフォレンジック調査が簡単で、システム内で起きたことを正確に把握できます」とOgletree氏は説明します。「例えば、以前のソリューションでは、消えてしまったフォルダについて、翌日まで何が起きたか説明できませんでした。でも今はChange Auditorのおかげで、そのフォルダに何が起きたか即答することができます。もし誰かが不注意で移動した場合であれば、その人物に元の場所に戻すよう伝えるか、手早く自分で戻すこともできます。フォルダが削除された場合は、以前であれば、オフサイトからテープを注文して届くのを待ち、それから復元プロセスを実施しなければなりませんでした。しかし今では
フォルダを即座に復元できます」

レポートは自動的に作成され、関係者に配信されます。このレポート作成のスケジュール設定は、各ビジネスオーナーがデータおよびシステムへの変更に対するレビューを定期的に行うことを促進し、誤った変更を速やかに検知するのに役立ちます。「複数のレポートを設定して、ファイルシステム内の特定領域への変更が表示されるようにしました。そしてそのデータの所有者に毎週配信しています」とOgletree氏は言います。「例えば、ある部門にたまにしか使用しないファイルがいくつかあるとします。Change Auditorを利用する前は、これらのファイルのいくつかが変更またはなくなっていることに気づいた場合、最後にそれらのファイルを使用してからシステムに起こったことを再現するのに、私に依頼する必要がありました。Change Auditorであれば、ファイルに何が起きているか毎週レビューすることができるので、後になって突然問題が発覚することはありません」

さらに、すべてのChange Auditorアプリケーションとその他の複数のQuest Windows管理ソリューションは、高性能でインタラクティブなサーチエンジンを備えています。IT Security Searchは、多数のシステムやデバイスのさまざまなITデータを単一コンソール内で関連付けるため、セキュリティ問題の対応とフォレンジック分析が高速化されます。

企業全体に可視性を拡大

Active Directoryおよびファイルシステムに対してリアルタイムにインサイトを取得する

ことは、さまざまな面で同評議会に利点をもたらします。「Change Auditorでは、セキュリティだけでなく業務の生産性も向上するため、かなりの時間節約にもなります」とOgletree氏は言います。「その機能には、お金に換算できないほど大変貴重な価値があります」 Change AuditorソリューションによるActive Directory、Windowsファイルサーバ、EMCの監査が成功したため、同評議会は2つのChange Auditorアプリケーションを追加することにしました。それらはChange Auditor for SQL ServerとChange Auditor for SharePointです。

「AD、EMC、ファイルサーバへの可視性が向上されて大変役立っていることから、SharePointとSQL Serverにも同様の可視性があればと感じていました」とOgletree氏は言います。「例えば、SQL Server環境内のデータベーススキーマの変更およびその他の変更を監視することで、これらのシステムの継続的な稼働と、システム内のデータの安全確保に役立ちます」

同評議会では最近、Enterprise Reporter Suiteも導入しました。その包括的なアクセス評価とビルトインのレポート作成機能は、Microsoft環境全体のユーザ、グループ、権限、その他の設定について詳細な可視性を提供します。Ogletree氏は「以前は、多数あるSQL Serverそれぞれについてデータベース所有者（DBO）ロールは誰が持っているかという質問に答えるのは困難であり、各サーバを確認しなければなりませんでした」と振り返ります。「Enterprise Reporterがあれば、このような質問に簡単に答えることができます」。さらに、Enterprise Reporter Suiteへ投資すること で、同評議会にはSecurity Explorerの全機能を利用できるようになり、そのレポート作成および修復機能を組み合わせることで、ITチームはMicrosoftプラットフォーム全体におよぶアクセス制御、権限、セキュリティを単一コンソールから管理することができるようになります。

クラウドに対応

同評議会の成長と、そのIT環境がクラウドへと拡大するにつれ、 評議会が有するQuestソリューションの価値はさらに上がります。例えば、Change Auditor for Active Directoryは、Azure Active Directoryに対して監査を行います。これにより、クラウドのみのオブジェクトや属性に対する変更が確実に追跡され、アラートが生成されるようになります。同様に、Change Auditor for SharePointはSharePoint OnlineおよびOneDrive for Businessをサポートし、Enterprise ReporterはAzure Active Directory、Exchange Online、OneDrive for Businessに対応します。

QUESTについて

Questでは、複雑な問題をシンプルなソリューションで解決することを目的としています。当社は、優れた製品と優れたサービスを大切にし、シンプルにビジネスを行うという全体的な目標を重視する哲学をもって、これを達成しています。当社のビジョンは、効率性と有効性のどちらかを選ばなければならないような状況をつくらないテクノロジーを提供することです。これにより、お客様と組織はIT管理の時間を短縮し、より多くの時間をビジネスの革新に費やすことができます。

「以前は、多数あるSQL Serverそれぞれについてデータベース所有者（DBO）ロールは誰が持っているかという質問に答えるのは困難であり、各サーバを確認しなければなりませんでした。Enterprise Reporterがあれば、このような質問に簡単に答えることができます」

テキサス州北部中央自治体評議会、情報セキュリティオフィサー、Brett Ogletree氏

その他の導入事例: Quest.com/Customer-Stories

CaseStudy-NCTCOG-US-GM-JA-WL-34291