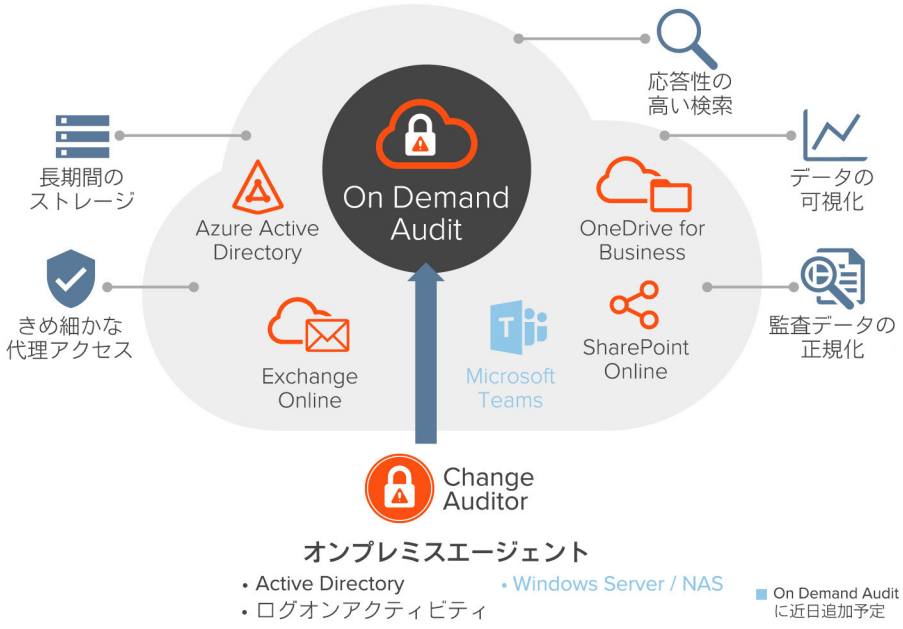
On Demand Audit Hybrid Suite for Office 365

ハイブリッドなMicrosoft環境におけるセキュリティとコンプライアンスの監査

Microsoftによると、Azure ADのユーザアカウントの50パーセント以上がハイブリッドです。[1] 貴社がまだハイブリッドでない場合も、近いうちに移行する可能性があるでしょう。ただし、ハイブリッドなMicrosoft環境に移行したとしても、引き続きレガシーインフラストラクチャを維持する必要があります。つまり、ITチームが管理し、保護する必要がある領域は2倍になります。クラウドに移行するワークロードの増加により、データのフットプリントが拡大するにつれて、インフラストラクチャはますます多くのセキュリティ脅威にさらされます。残念ながら、ネイティブのオンプレミスおよびクラウドサービス監査ツールでは、この新しいハイブリッドのビジネスモデルのセキュリティとコンプライアンスのニーズに対応する能力に限界があります。

単一のダッシュボードから、オンプレミスやクラウドサービスで行われた変更を検索することにより、ハイブリッド環境を保護し、継続的なコンプライアンスを保証できるとしたらどうでしょうか? オンプレミスとOffice 365ワークロード全体で個々の変更の見え方を標準化できるとしたらどうでしょう? 監査データのアクセスを委任して、ユーザが必要なレポートだけを入手し、それ以上のものを入手できないようにできるとしたら? 必要な期間、必要なだけ監査データを保持できるとしたらどうでしょうか?



Change AuditorとOn Demand Auditを組み合わせて、SaaSダッシュボードからハイブリッドアクティビティの単一ホステッドビューを実現します。

Quest® On Demand Audit Hybrid Suite for Office 365を使用することで、ハイブリッドなMicrosoft環境全体のユーザアクティビティを単一のホステッドビューで確認できます。

メリット:

- Change AuditorとOn Demand Auditを組み合わせて、ハイブリッド監査に完全に対応
- 最新の直感的なSaaSダッシュボードから、ハイブリッドアクティビティの単一のホステッドビューを提供
- 応答の早い柔軟な検索ビルダにより、調査時間を短縮
- インタラクティブなデータの可視化によって分析をシンプル化
- 解釈が容易になるように、監査データをシンプルな形式で標準化
- 各変更と関連イベントに関する詳細情報にワンクリックで瞬時にアクセスすることで、調査中の臆測を排除
- 現場にいないときでも、至急の対応を促すリアルタイムの警告をEメールやモバイルデバイスに送信
- きめ細かな代理アクセスにより、ステークホルダーに必要なレポートを提供
- 監査履歴を最大10年間保存できるので、コンプライアンス規制を満たすために必要なだけのデータを保持可能

1 https://www.microsoft.com/en-us/microsoft-365/blog/2017/11/13/how-organizations-are-connecting-their-on-premises-identities-to-azure-ad/

On Demand Auditは監査履歴をすべて最長10年間保存します。固定サブスクリプション料金で、ネイティブの保持期間よりはるかに長期の保存が可能です。

Quest® On Demand Audit Hybrid Suite for Office 365は、ハイブリッドなMicrosoft環境全体のユーザアクティビティの単一のホステッドビューを提供し、オンプレミスのActive Directory（AD）、Azure AD、またはExchange Online、SharePoint Online、およびOneDrive for Businessなどの Office 365ワークロードで行われたすべての変更を視覚化します。

Hybrid Suiteはサブスクリプションサービスとして提供され、Change Auditor for Active Directory、Change Auditor for Logon Activity、およびOn Demand Auditのライセンスを得られます。数回クリックするだけで、これらを簡単に組み合わせることができるようになっています。

CHANGE AUDITOR FOR ACTIVE DIRECTORYおよびLOGON ACTIVITY

Change Auditorは、オンプレミスのMicrosoft環境を詳細かつ忠実に監査するための、業界をリードするソリューションです。グループポリシーオブジェクト（GPO）、DNS、サーバ構成、入れ子グループなどを含め、すべての重要な設定やAD全体のユーザおよび管理者の変更について、リアルタイムの監査、アラート送信、およびフォレンジックを提供します。

ON DEMAND AUDIT

On Demand AuditはAzureホステッドのSaaSで、Azure AD、Exchange Online、SharePoint Online、OneDrive for Business全体におけるすべてのアクティビティを追跡します。Hybrid Suiteの一部として、Change Auditorが収集したオンプレミス監査データと、Azure ADおよびOffice 365ワークロードからのクラウドサービスアクティビティを統合し、相関させます。

ON DEMAND AUDIT HYBRID SUITEの仕組み

Change AuditorとOn Demand AuditをOn Demand Audit Hybrid Suite for Office 365で組み合わせることにより、オンプレミスとクラウドサービスの監査データを単一のビューで表示できます。また、応答性の高い検索とインタラクティブなデータの可視化によって、そのビューからインシデントを素早く調査し、On Demandテナントに最大10年間、監査履歴を保存できます。

ほとんどのクラウド・サービス・ベース製品のオンプレミスアクティビティ、およびSIEMツールなどそれが可能なツールは、ネイティブのイベントログに依存するため、Change Auditorで得られるような監査の忠実性を欠いています。

Change Auditorは、各ドメインコントローラーにインストールされた軽量エージェントからデータを取得します。その結果、ネイティブ監査ツールよりも迅速かつ正確に監査できます。Change Auditorは、すべてのイベントを読みやすい5つのW（who: 誰が、what: 何を、when: いつ、where: どこで、originating workstation: 発生ワークステーション）の標準化された形式で表示します。Change Auditorは、ユーザがこれらの変更を行うネイティブ許可を持っている場合でも、特権グループ、GPO、機密情報を扱うメールボックスなど、重要データの変更を防止することもできます。

On Demand Auditは、オンプレミスのChange Auditorイベントを表面化しながら、Azure ADおよびOffice 365ワークロード全体のアクティビティを監査して、以下について単一のホステッドビューを提供します。

- ADおよびAzure ADのユーザ、グループ、ロール、IDなど
- Kerberos認証およびNTLM認証の両方を含む、ADのログオン/ログオフアクティビティ
- Azure ADのサインインの失敗とその原因
- Exchange Onlineのメールボックスへのログイン、アクティビティ、非所有者によるメールボックスへのアクセス、配布グループなど
- SharePoint OnlineおよびOneDrive for Businessのファイルアクセス、データの外部共有、匿名のリンクなど

ハイブリッドID監査

On Demand Auditを使用すると、オンプレミスIDとクラウドサービスIDの両方で検索できるので、アクティビティが発生した場所に関係なく、すべてのユーザアクティビティを見つけることができます。

移動中も可能なリアルタイム警告

どこにいても一定した可視性を保ち、重要なポリシー変更および不審なイベントに対して、その発生元がオンプレミスまたはクラウドサービスであるかどうかにかかわらず、どこからでも、どのデバイスでも対応できます。On Demand Audit Hybrid Suite for Office 365では、現場にいないときでも、至急の対応を促すリアルタイムの警告をEメールおよびモバイルデバイスに送信することができます。

新しいクラウドファースト機能で、CHANGE AUDITORの機能を拡張

応答の速い柔軟な検索

テナント全体にわたって迅速かつ直感的に操作できるよう設計された検索により、即座に結果が得られるため、調査時間を大幅に削減できます。On Demand Auditでは、あらゆるイベントやフィールドで柔軟な検索をご利用いただけます。例えば、アクター、変更された属性、アクティビティの詳細、クラウドサービス専用オブジェクトによる検索などです。

インタラクティブなデータの可視化

何百または何百万というオンプレミスおよびOffice 365の監査イベントを、わかりやすく視覚的なダッシュボードに変換するため、コンプライアンスレポートの作成がシンプル化され、インシデント調査も迅速化されます。

標準化された監査ビュー

ネイティブ監査と異なり、On Demand Auditは、監査ログの生データを、意味のある正規化された形式に変換します。On Demandはすべてのオンプレミスおよびクラウドサービスの変更イベントから最も重要なイベントの詳細（変更前後の値を含む）を強調表示するので、セキュリティが懸念される場所について迅速に判断できます。

きめ細かな代理アクセス

わずか数回クリックするだけで、セキュリティチーム、コンプライアンスチーム、ヘルプデスクのスタッフ、ITマネージャだけでなく、外部監査人やパートナーに対しても、それぞれが必要とする内容のみのレポートを提供することができます。On Demand Auditはきめ細かな代理アクセスを提供して、設定を変更したり追加のインフラストラクチャをセットアップしたりすることなく、ユーザが安全に必要なインサイトを得られるようにします。

長期間のストレージ

On Demand Auditは監査履歴をすべて最長10年間保存します。固定サブスクリプション料金で、ネイティブの保持期間よりはるかに長期の保存が可能です。これにより、Azureストレージのコストを増加させることなく、セキュリティとコンプライアンスポリシーを満たすのに必要な限りの監査データを保持できます。

セキュアでスケーラブルな信頼性の高いSaaS

On Demand Auditは、受賞歴を誇るグローバルな24/7/365サポートに支援され、必要とするセキュリティスタンダード、サービスレベル、および拡張性を提供します。認証には、ISO/IEC 27001:2013、ISO/IEC 27017:2015、およびISO/IEC 27018:2019が含まれます。

ホステッド監査ダッシュボードの迅速かつ簡単なセットアップ

Quest On Demandへ容易にオンボードし、監査を数分のうちに開始できます。インストール、アップグレード、複雑な設定も不要で、汗だくになることはありません!

迅速な刷新

当社はMicrosoftのアップデートに対応しているため、お客様はアップデートを行う必要がありません。AzureホステッドSaaSプラットフォームとして、Quest On Demandの自動アップデートは、新機能、お客様の要望による機能拡張、セキュリティパッチを迅速に、お客様の手をわずらわせることなく提供します。

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。

Quest On Demand Auditは、ISO/IEC 27001:2013、ISO/IEC 27017:2015、ISO 27018:2019を取得しています。

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-OnDemandAudit-US-LP-JA-WL-58421