EU GDPR への準拠に向けた取り組みをサポートする

Enterprise Mobility + Security

2017 年 5 月版

Microsoft

目次

免責事項

このホワイト ペーパーでは、GDPR について説明しており、発行時点におけるマイクロソフトの解釈を表しています。マイクロソフトは、GDPR の意図と意味について、長い時間を費やしてじっくりと考えてきました。しかしながら、GDPR の適用は事実特定的であるうえ、GDPR のあらゆる側面と解釈が確定されているわけではありません。

そのため、このホワイト ペーパーは、情報の提供のみを目的としており、法律上の助言として、あるいはお客様およびお客様の組織が GDPR を適用する方法を決定するために利用することはできません。法的に資格のある専門家と協力し、GDPR がお客様の組織に具体的にどのように適用されるのか、また法令を遵守するための最善の方法は何かなど、GDPR について議論することをお勧めします。

明示、黙示または法律の規定にかかわらず、このホワイト ペーパーの情報についてマイクロソフトはいかなる責任も負わないものとします。このホワイト ペーパーは "現状有姿" で提供され、このホワイト ペーパーに記載されている情報や見解 (URL 等のインターネット Web サイトに関する情報を含む) は、将来予告なしに変更されることがあります。

2017 年 5 月公開

バージョン 1.0

概要

2018 年 5 月 25 日に、欧州でプライバシーに関する法律が発効となる予定ですが、これによって、プライバシーの権利、セキュリティ、コンプライアンスに関する世界的な新しい基準が設けられることになります。

この一般データ保護規則 (GDPR) は、基本的に個人のプライバシーの権利の保護と確立を目的としています。GDPR によって、データの送信、処理、保存を行う場所にかかわらず、個人の選択を尊重しながら、個人データを管理および保護する方法を制御するための厳格で世界的なプライバシー要件が確立されます。

マイクロソフトとお客様には、GDPR のプライバシーに関する目標を達成するために尽力することが求められます。マイクロソフトでは、プライバシーを基本的な権利ととらえており、GDPR は個人のプライバシーの権利を明確にして確立するための重要な一歩であると考えます。しかしながら、GDPR によって、世界中の組織に大きな変更が必要となることも認識しています。

GDPR へのマイクロソフトの対応とお客様のサポートについて、次のブログに概要が記載されています。最高プライバシー責任者 Brendon Lynch のブログ「Get GDPR compliant with the Microsoft Cloud」(Microsoft Cloud を使用して GDPR への準拠を実現) および Microsoft コーポレート バイス プレジデント兼次席法務顧問 Rich Sauer のブログ「Earning your trust with contractual commitments to the General Data Protection Regulation」 (一般データ保護規則に対する契約責任の履行による信頼の獲得)。

GDPR に対する取り組みは困難だと思われるかもしれませんが、マイクロソフトがお手伝いいたします。GDPR、マイクロソフトの対応、およびお客様の取り組みの開始に関する具体的な情報については、Microsoft Trust Center の GDPR のセクションを参照してください。

GDPR の影響

GDPR は、複雑な規制であり、個人データの収集、使用、および管理の方法に大幅な変更が必要になる可能性があります。マイクロソフトは長年にわたり、お客様による複雑な規制への準拠を支援してきました。もちろん、GDPR に対する準備もマイクロソフトがお手伝いいたします。

GDPR によって、欧州連合 (EU) 圏内の個人に商品やサービスを提供する組織、または EU 加盟国の居住者に関連するデータを収集および分析する組織には、その所在地にかかわらず、新しい規則が課されます。GDPR の主要な要素は次のとおりです。

- **個人のプライバシーの権利の強化** - EU 居住者が自分の個人データに関して、データへのアクセス、データの不正確さの修正、データの削除、データの処理に対する異議申し立て、およびデータの移動を行う権利を守ることにより、これら EU の居住者に関するデータ保護が強化されます。

- **データ保護の義務の厳格化** - 個人データを処理する企業や公的機関のアカウンタビリティが強化され、これによってコンプライアンスの確保における責任がより明確になります。

- **侵害のレポートの義務化** - 企業は遅滞なく、通常は 72 時間以内に、監督当局に個人データの侵害をレポートすることが義務付けられます。

- **非準拠に対する巨額の罰金** - 意図的であるか不注意によるものであるかにかかわらず、組織が法令を遵守しなかった場合は、多額の罰金を科すなどの厳しい制裁措置があります。

お客様も予想されているとおり、GDPR はビジネスに多大な影響を与えるおそれがあり、プライバシー ポリシーの更新、データ保護制御と侵害通知手順の実装と強化、透明性の高いポリシーの展開、および IT とトレーニングにおけるさらなる投資が必要になる可能性があります。
Microsoft Enterprise Mobility + Security (EMS) は、これらの要件に効果的かつ効率的に対処できるよう支援します。

1995 年に確立された EU データ保護指令の地域的な範囲の拡大に加えて、EU 内の管理者と処理業者、および EU の居住者に商品やサービスを提供し、それらの居住者を監視する、EU 外の管理者と処理業者を管理下に置くことで、GDPR は保護するデータの種類の定義を明確にすると同時に拡張します。

はじめに

「Beginning your General Data Protection Regulation (GDPR) Journey」 (一般データ保護規則 (GDPR) に対する取り組みの開始) では、GDPR の概要、GDPR がお客様に与える影響、取り組みをすぐに開始するためにできることなどのトピックを取り上げています。このドキュメントでは、GDPR に準拠するための取り組みを開始するときに、次の 4 つの重要なステップに焦点を当てることもお勧めしています。

GDPR に準拠するための重要なステップ

- **把握する** — どのような個人データがどこにあるかを把握します。
- **管理する** — 個人データの使用方法とアクセス方法を管理します。
- **保護する** — セキュリティ制御を確立して、脆弱性とデータ侵害に関する防御、検出、および対応を行います。
- **報告する** — データの要求に対応し、データ侵害を報告して、必要なドキュメントを保管します。

これらの各ステップについて、そのステップの要件に対応するために使用できるマイクロソフトのさまざまなソリューションのツール、リソース、および機能の例の概要が示されています。このドキュメントは包括的な "手引書" ではありませんが、詳細を入手できるリンクが Microsoft.com/GDPR に記載されています。

どれほどたいへんな作業になるかを考えると、GDPR の施行が開始してからの準備では間に合いません。すぐにプライバシー保護とデータ管理の実施方法を見直す必要があります。

このホワイト ペーパーでは主に、Microsoft Enterprise Mobility + Security (EMS) が GDPR への準拠を支援するしくみ、そして GDPR への準拠に向けたお客様の取り組みを支援するためのアプローチ、推奨プラクティス、および手法に焦点を合わせています。

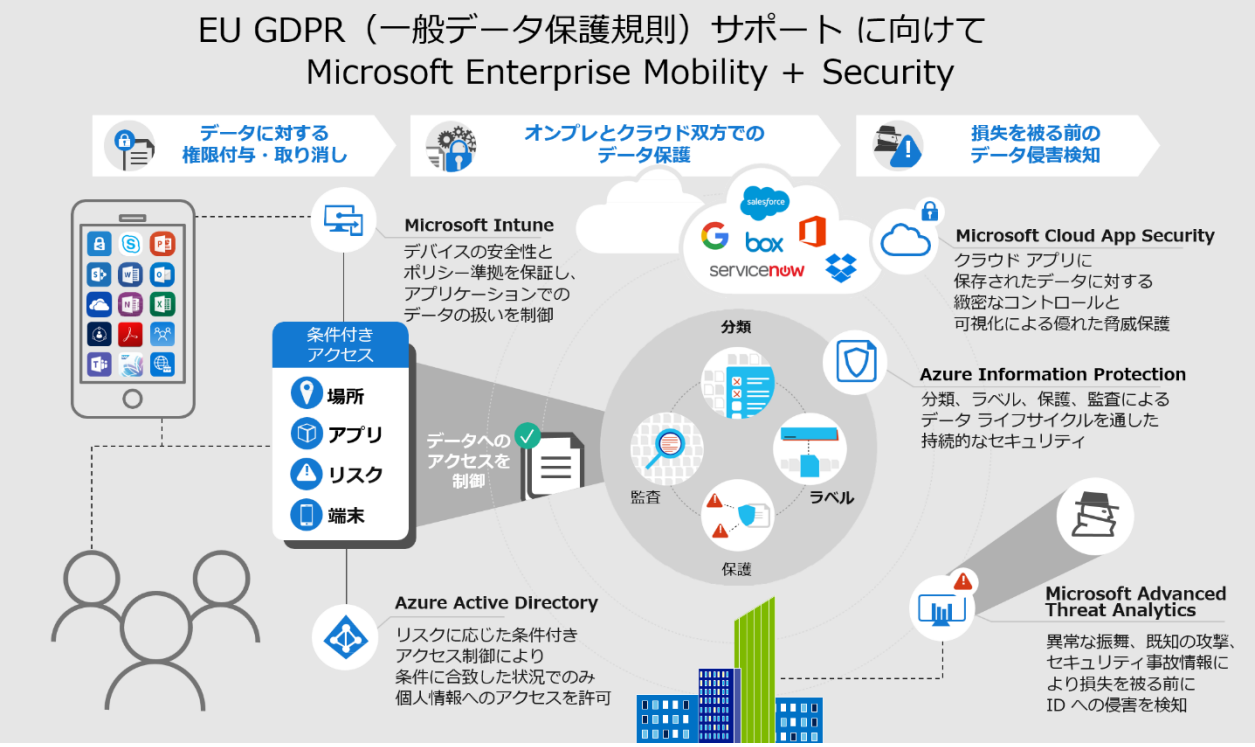
モバイル ファースト、クラウド ファーストの世界における課題への Microsoft EMS での対処

GDPR は明確です。データ管理者またはデータ処理業者は、その活動が GDPR の範囲に含まれるときは、個人データがオンプレミスに存在するのか、その他のクラウドやモバイル環境に存在するのかにかかわらず、この規制の要件を満たす責任があります。

かつてセキュリティは、もっぱらオンプレミス環境の境界に限られていました。しかし、モビリティおよびクラウドへの移行に伴い、従業員によるデバイス、アプリ、およびデータの操作、そしてデータの処理と保存に関連した他のユーザーとのやりとりは、ますます複雑になってきています。この新しい世界では、境界を管理しても、企業の境界外に移動されるデータの保護を保証することにはなりません。

環境が複雑化しているだけでなく、サイバーセキュリティの脅威は進化するという特性を備えており、その数は増大しているということを考えたとき、GDPR に従ったデータの保護において直面する困難が見えてきます。ユーザーに最高のエクスペリエンスを提供する一方で、GDPR などの規制への準拠を維持できるよう、バランスをとらなければならないのです。

それを実現するのが Microsoft EMS です。モビリティおよびクラウドの最新のイノベーションを適用することで、企業のデータ、ID、デバイス、およびアプリを脅威から保護し、GDPR の要件を満たすために取り組む必要のあるさまざまな種類の業務上および技術上の管理を可能にする、包括的なソリューション セットを提供します。



EMS の各製品の概要は以下のとおりです。また、このホワイト ペーパーの GDPR について詳しく説明しているセクションでも、これらの製品について触れています。

- **Azure Information Protection** - 永続的なデータ分類と保護を提供します。また、組織の内外でデータを安全に共有できるようになります。共有データに対するアクティビティを監視して、不測のイベントが発生したときに対応するためのオプションも用意されています。

- **Azure Active Directory Premium** - 多要素認証 (MFA)、デバイスの正常性とユーザーの場所に基づくアクセス制御、および包括的なセキュリティ レポート、監査、警告の機能を提供します。

- **Microsoft Intune** - iOS、Android、および Windows の PC をすべて 1 つのコンソールからより簡単にセキュリティで保護して管理できるようになります。Office 365 との緊密な統合により、Office モバイル アプリの企業データを保護します。

- **Microsoft Cloud App Security** - クラウド アプリケーション内のデータの可視化と制御を強化します。また、脅威からも保護します。

- **Microsoft Advanced Threat Analytics** - 機械学習、行動分析、および決定論的検出を使用して、持続的標的型攻撃や悪意のある攻撃からの保護を支援します。

EMS 内のソリューションは従業員が毎日使用している生産性ツール (Office や Office 365 など) と緊密に統合されるので、従業員に複雑な処理や作業方法の変更を課することなく制御とセキュリティを強化できます。

Microsoft EMS が EU GDPR への準拠に向けた取り組みをサポートするしくみ

モビリティおよびクラウド サービスの導入により、データはこれまでよりも多くの場所に移動するようになっています。これらのサービスの導入はユーザーの生産性と共同作業の向上に役立っていますが、データのセキュリティ保護と監視がより難しくなってきています。

このモバイル ファースト、クラウド ファーストの世界でデータを保護するには、データのライフサイクルについて一歩離れたところから全体的に考えることが重要です。データが作成または変更されてから、ユーザーがそのデータにアクセスするまで、あるいはデータがモバイル アプリやクラウド アプリに移動するまで、さらにはデータが侵害されるまでの間にとるべき保護対策について考える必要があります。

このホワイト ペーパーでは、Microsoft Enterprise Mobility + Security のテクノロジが、データのライフサイクルを通して考慮する必要のある重要な使用事例のシナリオに対処できるよう支援するしくみを説明します。これらのシナリオは、GDPR の要素に焦点を置いており、以下の方法を知るために役立ちます。

- オンプレミスおよびクラウドで永続的なデータ保護を提供する
- データへのアクセスを許可および制限する
- モバイル デバイスおよびモバイル アプリケーションでデータを保護する
- クラウド アプリでデータの可視性と管理を確保する
- 被害をもたらす前にデータ侵害を検出する

これらのシナリオについて説明した後、EMS ソリューションを試してみるだけでなく、マイクロソフトの FastTrack プログラムのサポートを得ながら EMS ソリューションを展開するための、有用なリソースを示します。

GDPR の義務を履行するには、個人データと機密データを把握して分類すること、そしてそれらのデータを保護するための適切なセキュリティ対策を講じることが不可欠です。まずは、GDPR に対する取り組みの対象となるデータの種類を確認することから始めましょう。

個人データと機密データ

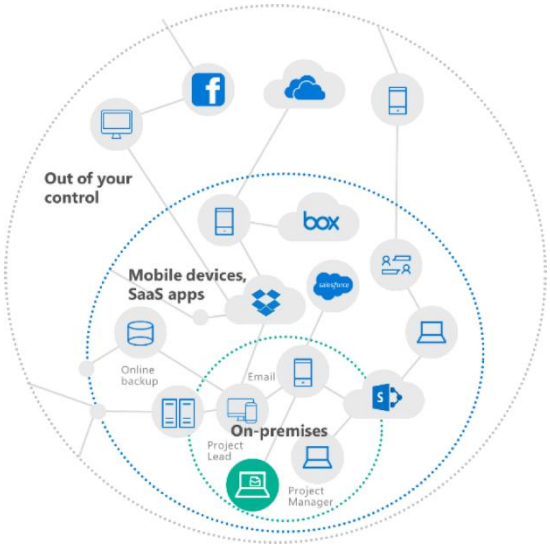
GDPR への準拠に向けた取り組みの一環として、この規制で個人データと機密データがどのように定義されているか、またそれらの定義がお客様の組織で保有しているデータにどのように関係するかを理解することが必要になります。そうしたことを理解したうえで、お客様のデータがどこで作成、処理、管理、および保存されているのかを把握できるようになるのです。

> 自然人として識別された、または識別可能な個人（つまりデータ主体）に関連する情報 – 例:
>
> - 名前
> - ID 番号（SSN など）
> - 場所データ（自宅住所など）
> - オンライン識別子（電子メール アドレス、スクリーン ネーム、IP アドレス、デバイス ID など）
> - 遺伝的データ（個人の生体サンプルなど）
> - 生体認証データ（指紋、顔認識など）

GDPR では、個人データは、自然人として識別された、または識別可能な個人に関連するあらゆる情報と見なされます。こうしたデータには、直接的な ID (実名など) と間接的な ID (データが参照する個人が明確になる特定の情報など) の両方が含まれます。これまで EU データ保護指令ではあいまいになっていましたが、GDPR ではオンライン識別子 (IP アドレス、モバイル デバイスの ID など) や場所データも個人データと見なされることが明確になりました。

GDPR では遺伝的データ（個人の遺伝子配列など）と生体認証データ（指紋、顔認識、網膜スキャンなど）について詳しく定義されています。GDPR では遺伝的データや生体認証データが、個人データのその他のサブカテゴリ（人種的または種族的出身、政治的見解、宗教上または哲学上の信念、あるいは労働組合員であることが明らかになる個人データ、健康状態に関連するデータ、個人の性生活や性的指向に関連するデータ）と共に、機密性のある個人データと見なされています。機密性のある個人データは保護が強化され、通常はそれらの個人データを処理するときに、個人の明示的な同意が必要となります。

オンプレミスおよびクラウドで永続的なデータ保護を提供する方法



境界、ユーザー、またはデバイスを管理しても、企業の境界外に移動されるユーザー データの保護を保証することにはなりません。保護が必要なデータを単純に識別することが非常に困難な場合もあります。では、さまざまな場所に保存されているデータを境界を越えて共有するときに、それらのデータを永続的に識別および保護するにはどうすればいいでしょうか。

データの保存場所や共有相手、あるいはデバイスで iOS、Android、または Windows が実行されているかどうかにかかわらず、データを常に保護するには、分類と保護の機能をファイル自体に組み込んで、データをどこに移動するときにも、それらのデータが保護されるようにする必要があります。Microsoft Azure Information Protection (AIP) は、オンプレミスとクラウドの両方で、この永続的なデータ保護を提供するよう設計されています。

Azure Information Protection を使用すると、データを作成または変更するときにそれらのデータを分類してデータにラベルを付けることができます。そうして、個人データと機密データに保護を適用することができます。分類ラベルと保護は永続的であり、データが移動するときにも維持されるため、保存場所や共有相手にかかわらず、常にデータが識別され、保護されるようになります。インターフェイスはシンプルかつ直感的で、ユーザーの通常の業務を妨げません。また、共有データの可視化と管理が強化されます。

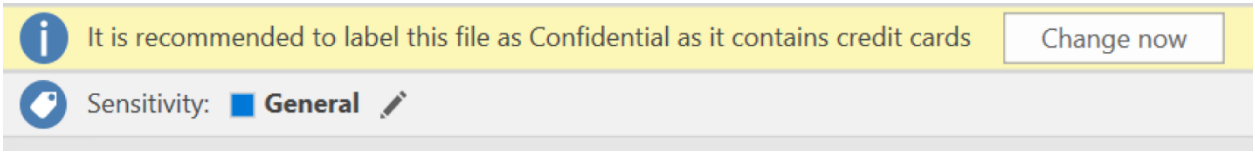
分類とラベル付け

データの分類は、あらゆるデータ ガバナンス計画における重要な部分です。企業全体に適用される分類スキームの採用は、GDPR でデータ主体 (つまり、企業の EU 圏内の従業員または顧客) の要求であると見なされているものに対応するときに特に有用です。このような分類スキームによって、企業は個人データに関する要求をより迅速に特定して処理できるようになるからです。

Azure Information Protection を、データを作成または変更するときの分類やラベル付けに役立てることができます。これにより、GDPR で場合によって適切であると見なされている暗号化の形式、または視覚的なマーキングによる保護を、保護が必要なデータに適用することができます。

Azure Information Protection を使用すると、機密度ラベルでマーキングされているデータを照会することも、ファイルまたは電子メールの作成/変更時に機密データをインテリジェントに識別することもできます。識別されたデータは、企業が選択したポリシーに基づいて自動的に分類またはラベル付けすることができます。

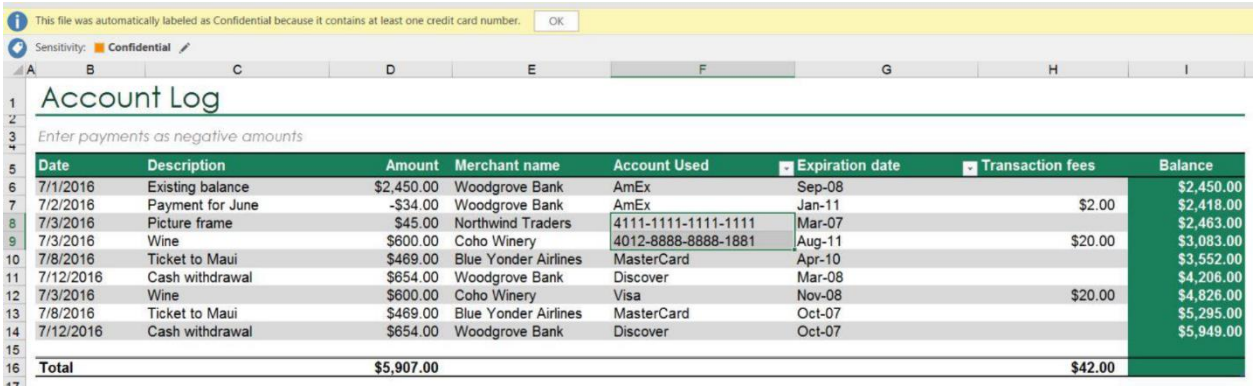
次のスクリーン ショットは、Azure Information Protection がドキュメント内の特定のコンテンツを識別し、このファイルを "社外秘" としてラベル付けするよう推奨する通知をユーザーに送信したケースを示しています。これは、ユーザーが作業しているドキュメント内の特定のコンテンツ (クレジット カード番号など) を検索して、そのドキュメントに適切なラベルを付けることを推奨するよう構成されている、企業ポリシーに基づいて実行されました。



Azure Information Protection – 推奨された分類

管理者およびデータ所有者は、ファイル ストアに保存されているラベルの付いたファイルを照会することもできます。1 つの例として、リスク管理者は、Shared フォルダーに配置されている "極秘" のラベルが付いたすべてのファイルを照会および調査することができます。

次のスクリーン ショットは、実行中の Azure Information Protection の例を示しています。管理者は機密データ (この場合は、クレジット カード情報) を検出するようルールを構成しており、機密データが含まれるこのファイルには "社外秘" のラベルが自動的に付けられました。ユーザーがクレジット カード情報を含む Excel ドキュメントを保存するときには、ファイルが "社外秘" としてラベル付けされていることを示す通知がそのユーザーに表示され、ファイルのラベルが "設定なし" から "社外秘" に変更されます。



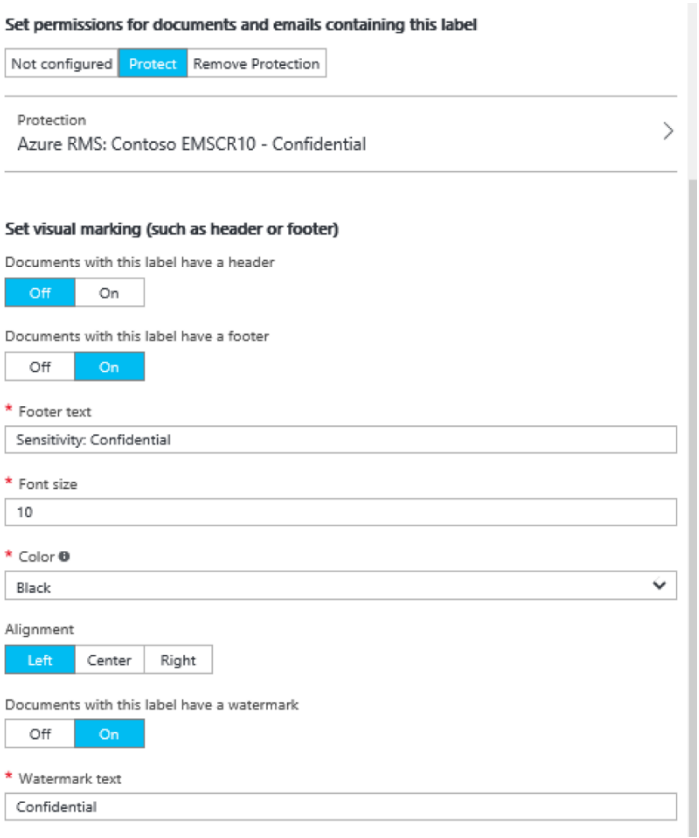
Date	Description	Amount	Merchant name	Account Used	Expiration date	Transaction fees	Balance
7/1/2016	Existing balance	$2,450.00	Woodgrove Bank	AmEx	Sep-08		$2,450.00
7/2/2016	Payment for June	-$34.00	Woodgrove Bank	AmEx	Jan-11	$2.00	$2,418.00
7/3/2016	Picture frame	$45.00	Northwind Traders	4111-1111-1111-1111	Mar-07		$2,463.00
7/3/2016	Wine	$600.00	Coho Winery	4012-8888-8888-1881	Aug-11	$20.00	$3,083.00
7/8/2016	Ticket to Maui	$469.00	Blue Yonder Airlines	MasterCard	Apr-10		$3,552.00
7/12/2016	Cash withdrawal	$654.00	Woodgrove Bank	Discover	Mar-08		$4,206.00
7/3/2016	Wine	$600.00	Coho Winery	Visa	Nov-08	$20.00	$4,826.00
7/8/2016	Ticket to Maui	$469.00	Blue Yonder Airlines	MasterCard	Oct-07		$5,295.00
7/12/2016	Cash withdrawal	$654.00	Woodgrove Bank	Discover	Oct-07		$5,949.00
Total		$5,907.00				$42.00	

Azure Information Protection – 機密データの自動分類

保護

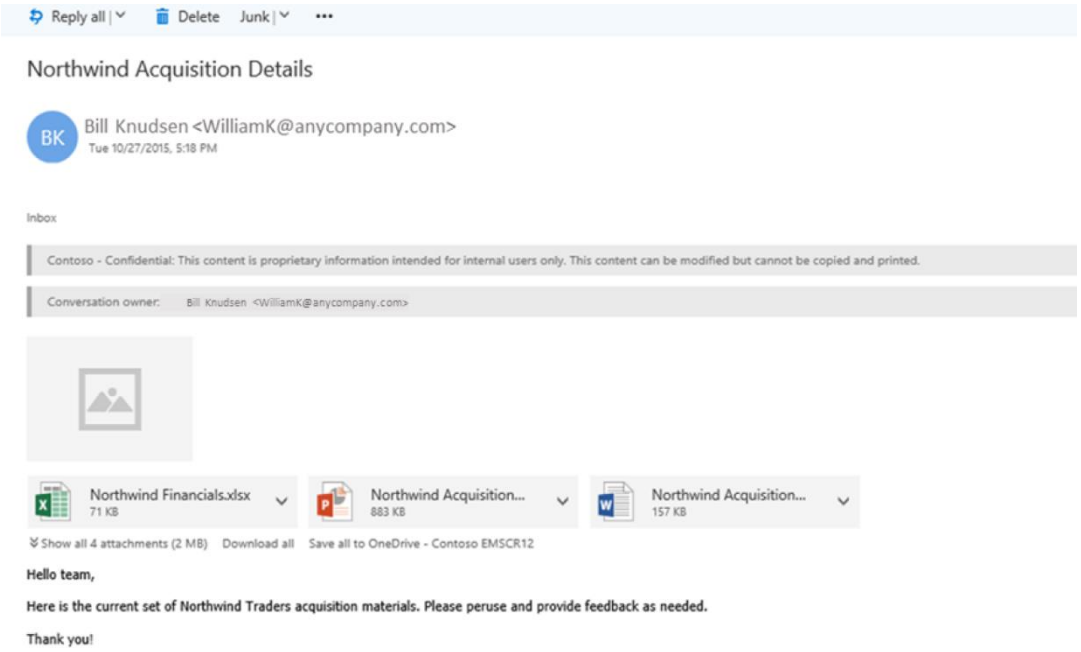
データを適切に分類およびラベル付けしたら、次のステップはデータをセキュリティで保護して管理することです。Azure Information Protection には、そのために使用できる ID ベースのセキュリティ アプローチが用意されています。

Azure Information Protection では、管理と保護を行うためのポリシーを柔軟に定義できます。ポリシーを定義したら、個人データが含まれるファイルを AIP を使用して暗号化して、GDPR を満たす適切なポリシーに従ってアクセス権を管理することができます。右のスクリーン ショットは、"社外秘" のラベルが付いているすべてのデータを自動的に保護する管理者ポリシーを示しています。フッターや透かしなどの視覚的なマーキングも、これらのデータに適用されます。



Azure Information Protection – ドキュメントのアクセス許可の設定

さらに、Azure Information Protection を使用すると、ユーザーが機密データを安全な方法で共有できるようになります。次の例では、機密の買収に関する情報が暗号化され、情報に対するアクセスが特定のユーザー グループのみに制限されています。それらのユーザーには、その情報に対する限定された一連のアクセス許可のみが付与されており、ユーザーはコンテンツを変更できますが、コピーしたり印刷したりすることはできません。



Azure Information Protection – ドキュメントへのアクセスの制御

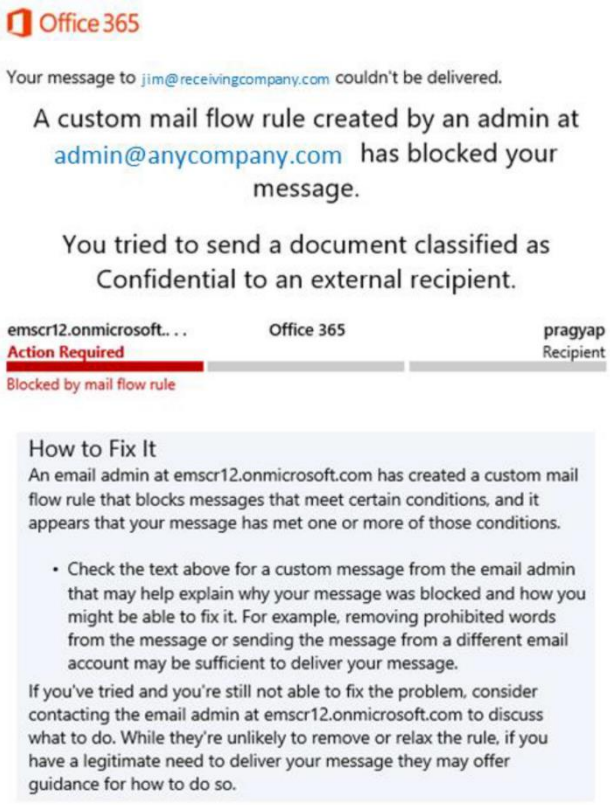
暗号化解除は、アクセス ポリシーによって許可されているユーザーのみという条件付きで認められます。これにより、個人データが意図されたとおりに保護されます (つまり、許可されていないユーザーはアクセスできません)。権限ベースの暗号化を設定することによって、共有の煩雑さが軽減されます。監査ログを使用して各アクセスを追跡することにより、許可されていないユーザーへの個人データの漏えいを防止できます。

データの保護には、データ フローの制御も必要です。Azure Information Protection によって設定される分類ラベルと保護は永続的であり、データが移動しても有効なので、データ損失防止 (DLP) システムおよびクラウド アクセス セキュリティ ブローカー (CASB) ソリューションをこのフローで利用して、警告、暗号化、通知、ブロック、検疫、アクセス無効化などのアクションによりポリシーを実施することができます。

次の例では、DLP ポリシーは、"社内用" のラベルが付いているデータが含まれるすべての電子メールについて、外部での共有をブロックするよう構成されています。

DLP ルール - 社内データの外部共有をブロック

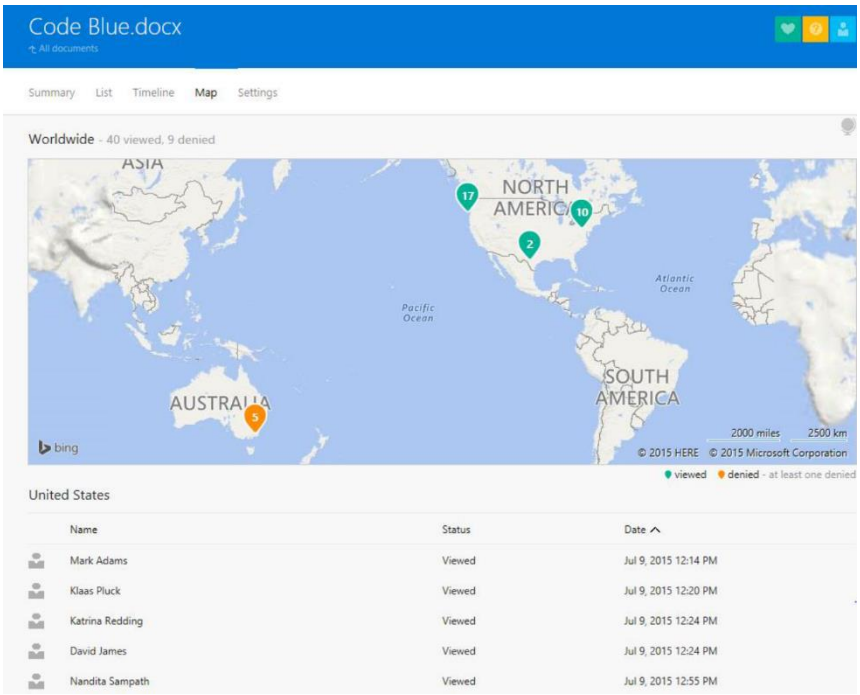
次のスクリーン ショットは、ユーザーが社外に機密情報を送信しようとしたときに受け取る通知を示しています。管理者が構成した DLP ルールによって、このような電子メールがブロックされ、ユーザーに通知が送信されます。これは、重要な企業データを保護するだけでなく、ユーザーに適切な行動を教育するという意味でも優れています。



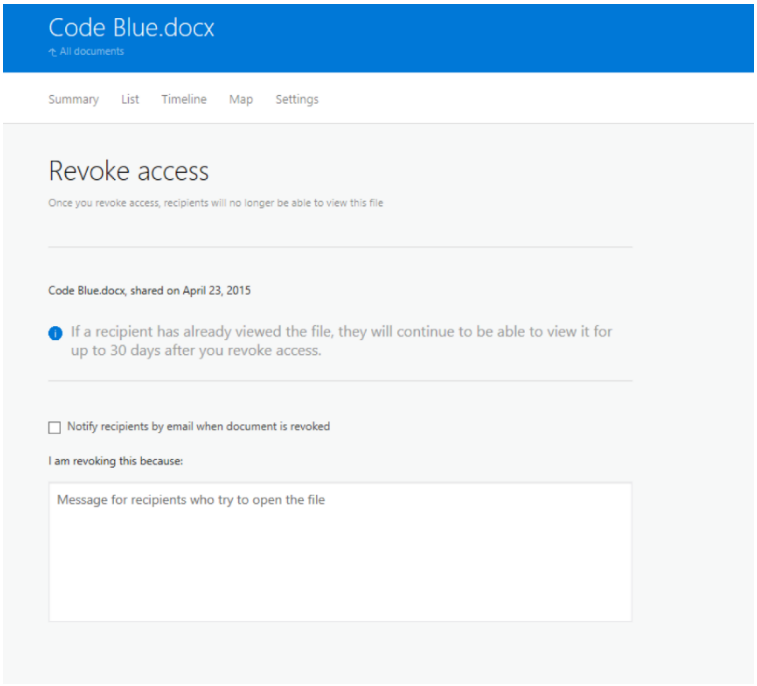
Azure Information Protection – DLP ユーザー通知

監視

コンテンツを分類した（また、オプションで保護した）後は、コンテンツの使用状況を監視できます。次の 2 つの画像で示しているように、データ フローを分析することにより、社内の状況を把握する、危険な行動を検出する、是正措置（アクセス無効化など）を講じる、ドキュメントへのアクセスを追跡する、データの漏えいや誤使用を防ぐ、といったようなことが可能になります。



Azure Information Protection – 地図によるデータの追跡



Azure Information Protection – データへのアクセス無効化

データへのアクセスを許可および制限する方法

各企業は情報のセキュリティの重要性を認識しつつありますが、GDPR ではさらなる対策が求められます。GDPR では、企業が適切な技術的および組織的な対策を講じて、個人データの損失や未承認のアクセスまたは開示を防ぐことが求められます。これらの対策を講じなければ、セキュリティの侵害が発生したときに、企業に多額の罰金が科せられる可能性があります。

個人データへのアクセスを許可および制限し (ロールベースのアクセスや職務分掌など)、製品に適切な技術的セキュリティ対策を実装して、個人データと処理システムの機密性、整合性、および可用性を常に確保できるようにするメカニズムによって、この要件を満たすことができます。

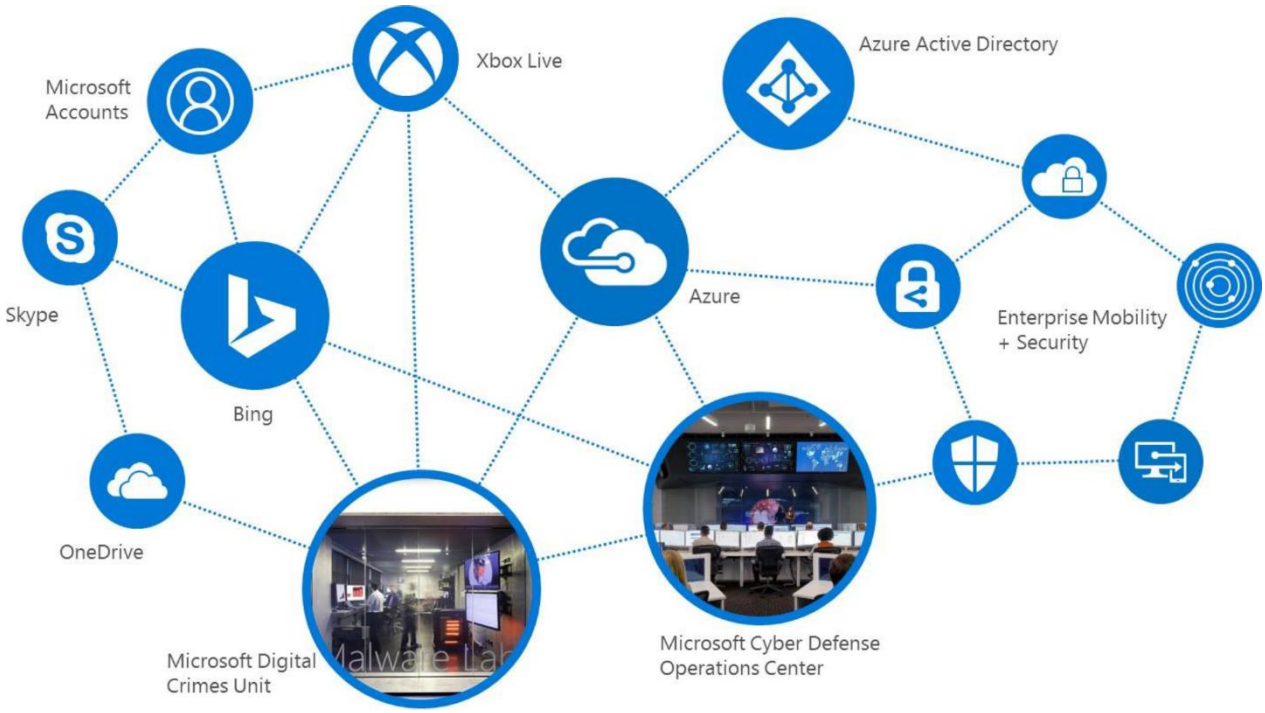
Azure Active Directory は、マイクロソフトの "ID とアクセス管理" ソリューションであり、組織がユーザー ID および関連するアクセス特権を管理できるよう支援することを目的としています。Azure Active Directory は、条件付きアクセス、ユーザーおよびサインインのリスク計算、多要素認証、特権 ID 管理などの機能によって、データへのアクセスの保護と制限を支援します。

条件付きアクセス ポリシーは、デバイスの状態、アプリケーションの機密度、場所、およびユーザーの各ルールに基づいて適用できます。また、Microsoft Enterprise Mobility + Security では、アクセス要求ごとおよびユーザーごとにリスクを計算し、自動化された修復アクションを必要に応じて適用する ID 保護機能によって、最も高度な脅威からリアルタイムでデータを保護することができます。リスクの計算は、Azure Active Directory Identity Protection が提供する機能です。

Identity Protection のリスク計算は、マイクロソフトの製品、グローバル クラウド サービス、サイバー セキュリティ チーム、およびその他のマイクロソフト以外のソースから収集するシグナルである一連のインテリジェンスをベースとしています。マイクロソフトは、脅威をプラットフォームの強化とお客様の保護に役立つ有用なインテリジェンスに転換してきました。マイクロソフトでは現在、クラウドがもたらすコンピューティングの大きなメリットを活かしつつ、脅威インテリジェンス主導型の機能豊富な分析エンジンを使用してお客様を保護するための新たな方法を探し続けています。

機械学習と人間の専門家という自動プロセスと手動プロセスを組み合わせることにより、リアルタイムで自ら学習して進化するインテリジェント セキュリティ グラフを作成して、製品で生じた新たなインシデントの検出とその対応に要する全体的な時間を削減することが可能になりました。マイクロソフトのセキュリティ チームは、このグラフを使用して、大規模かつ重要なセキュリティ イベントの相互関係を調べます。このとき、革新的なクラウド ファーストの機械学習と、行動分析および異常検出に基づいた検索クエリを使用して、実施可能なインテリジェンスを明確にします。

マイクロソフト インテリジェント セキュリティ グラフで扱われる範囲は、まさに数十億ものデータ ポイントに及びます。毎月 4,000 億のメッセージのスパムとマルウェアがスキャンされ、毎月 10 億を超える企業およびお客様のデバイスが更新されており、毎月 180 億を超える Bing スキャンと 4,500 億の認証がマイクロソフトのクラウド サービスで実行されています。



マイクロソフト インテリジェント セキュリティ グラフ

きめ細かな条件指定と制御に基づいて、個人データや機密データへのアクセスを許可することができます。次に例を示します。

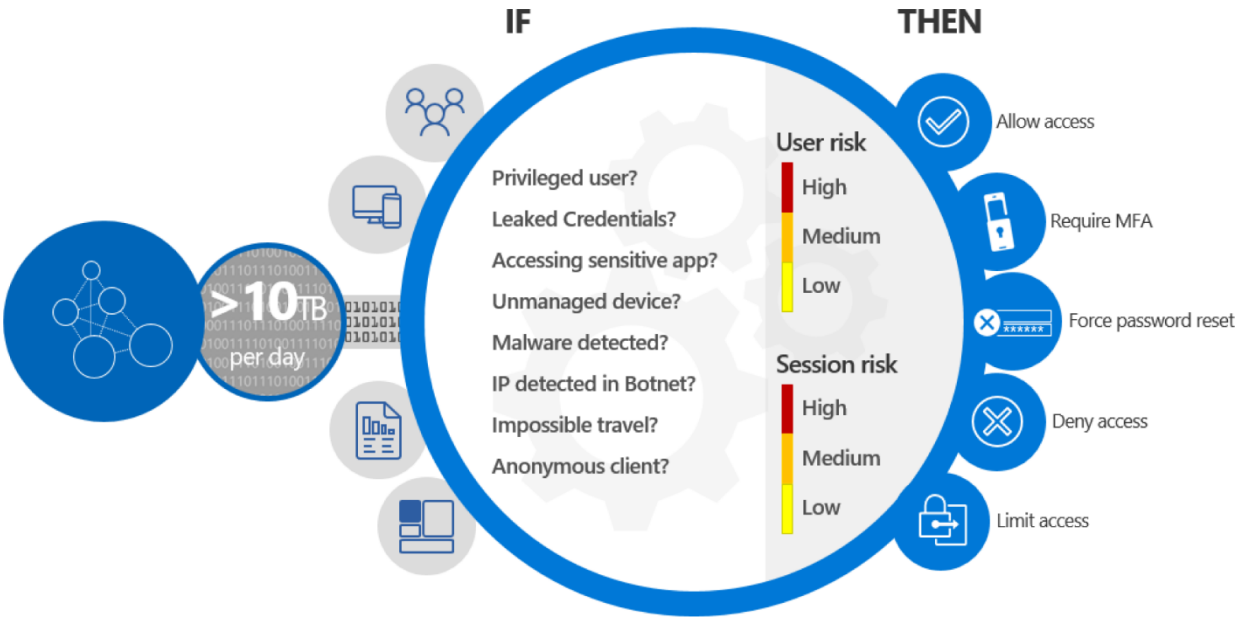
- **グループ メンバーシップ。**グループのメンバーシップに基づいてユーザーのアクセスを制御します。

- **場所。**ユーザーの場所を使用して、多要素認証をトリガーします。また、ユーザーが信頼できるネットワーク内にいない場合にブロック制御を使用します。

- **デバイス プラットフォーム。**iOS、Android、Windows Mobile、Windows などのデバイス プラットフォームをポリシー適用の条件として使用します。

- **デバイス。**デバイスの状態 (法令を遵守しているかどうか) を、デバイス ポリシーの評価時に検証します。紛失したり盗難にあったりしたデバイスをディレクトリで無効にすると、そのデバイスではポリシーの要件を満たすことができなくなります。

- **サインインとユーザー リスク。**条件付きアクセス リスク ポリシーに、Azure AD Identity Protection を使用できます。条件付きアクセス リスク ポリシーにより、リスク イベントおよび異常なサインイン アクティビティに基づいた高度な保護を組織で適用できるようになります。



マイクロソフト インテリジェント セキュリティ グラフによって強化される条件付きアクセス機能

条件付きアクセス ポリシーでは、ある条件が満たされなかったときにアクセスをブロックしたり、追加の認証形式 (多要素認証など) を要求したりすることができます。

多要素認証 (MFA)

多要素認証とは、複数の検証方法を必要とし、重要な 2 つ目のセキュリティ レイヤーをユーザーのサインインとトランザクションに追加する認証方法のことです。これは、以下の検証方法のうち 2 つ以上を要求することにより機能します。

- ユーザーが知っているもの (通常はパスワード)
- ユーザーが持っているもの (電話などの、簡単に複製できない信頼できるデバイス)
- ユーザーに関するもの (生体認証)

Azure Multi-Factor Authentication (MFA) は、マイクロソフトの多要素認証ソリューションです。Azure MFA は、シンプルなサインイン プロセスというユーザーの要望を満たしながら、データやアプリケーションへのアクセスを保護するのに役立ちます。Azure MFA では、電話の呼び出し、テキスト メッセージ、モバイル アプリなどによるさまざまな検証方法を使用して、強力な認証を実現できます。

Azure Multi-Factor Authentication は、クラウドとサーバーの両方に対する、選択可能な検証方法を提供します。つまり、音声通話、テキスト メッセージ、アプリでの通知、アプリからの確認コードなど、ユーザーに使用可能な方法を選択することができます。詳細については、「選択可能な検証方法」を参照してください。

データに対する特権アクセスの管理

特権アカウントへのアクセスを安全に管理することは、組織における以前からの課題となっていました。気が付けば、組織の環境では高度な特権を持つ永続アカウントが増えすぎてしまっていたのです。この結果生じる脅威の例として、悪意のあるまたは不正な管理者、フィッシング攻撃による管理者の資格情報の漏えい、侵害されたシステムでの管理者の資格情報のキャッシュ、永続アカウントを得るための一時的に昇格された特権を付与されたユーザー アカウントなどがあります。これは、GDPR によって期待されるセキュリティを揺るがすおそれがあります。

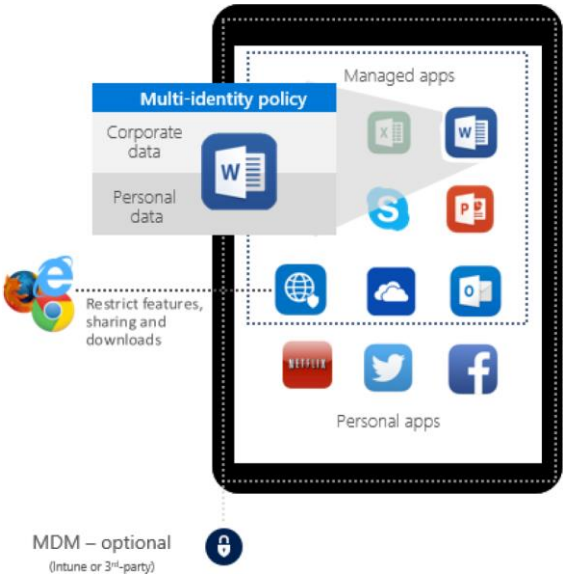
それを防ぐには、特権アカウントの悪用に関連するリスクであることを踏まえたうえで、特権アカウントを管理して、そのアクティビティを監視することが重要になってきます。

これは、Azure AD Privileged Identity Management が役立つ領域です。Azure AD Privileged Identity Management を使用すると、Azure Active Directory の特権付き管理者ロールとそれらの管理者の割り当て先のユーザー アカウントを検出できます。また、永続的な特権アクセスを無効にしたうえで、Azure Active Directory の特権アカウント向けの、オンデマンドの期限付きアクセス権を管理するメカニズムを使用できます。これにより、管理者および管理者からリソースへのアクセスを、検出、制限、および監視することができるようになります。管理者アクセス権が必要なユーザーは、多要素認証で ID が証明された後、事前に構成された期間内に使用できるアクセス権 (Just-In-Time アクセス) を取得できます。

モバイル デバイスおよびモバイル アプリでデータを保護する方法

モビリティは新たな標準です。このため、モバイル デバイスやモバイル アプリに移動するデータの保護が、データのライフサイクルにおいて考慮する必要のある重要なシナリオの 1 つとなります。

Microsoft Intune は、クラウドからのモバイル デバイス、モバイル アプリケーション、および PC の管理機能を提供します。Intune を使用すると、組織は企業データのセキュリティを確保しながら、従業員がほぼどこからでも、ほぼあらゆるデバイスで会社のアプリケーション、データ、およびリソースにアクセスできるようにすることが可能です。iOS、Android、Windows、Windows Mobile、および Mac OS X の各デバイスがサポートされる Intune では、安全な統合された方法で多様なモバイル環境を管理できます。



Intune のモバイル デバイス管理機能およびデバイス コンプライアンス ポリシーにより、まずは組織のデータや機密性の高いアプリにアクセスしようとするデバイスが、企業の特定の要件または標準を満たすよう徹底されます。管理者は、デバイスの登録、ドメインへの参加、強力なパスワード、および暗号化を実施するポリシーを設定できます。フル アクセスを付与する前に、デバイスのオペレーティング システムとアプリが、最新のパッチが適用されて最新の状態になっているよう、ポリシーで要求することもできます。

Microsoft Intune のコンプライアンス ポリシーの設定を使用して、従業員のデバイスが、作成した一連のルールに準拠しているかどうかを評価できます。デバイスがポリシーに設定されている条件を満たしていない場合、Intune はエンド ユーザーがデバイスを登録して (まだ登録されていない場合)、コンプライアンスの問題を修正することができるようガイドします。

Microsoft Intune は、以下の方法で、モバイル デバイス、アプリ、および PC に対する高度なセキュリティ ポリシーが実施されるようにします。

- iOS、Android、Windows、MacOS などのモバイル デバイスおよび PC に対する包括的な設定管理を実現する。

- モバイル デバイスおよび PC から特定のアプリケーションまたは URL アドレスにアクセスできないようにする機能を提供します。

- パスコードのリセット、デバイスのロック、リモート ワイプなどのリモート アクションを実行できるようにします。

- 管理対象 iOS デバイス、キオスク モードを使用している Android デバイス、および割り当てられたアクセスを使用している Windows 10 デバイスに対して、より厳格な "ロックダウン" ポリシーを実施できるようにします。

機密性の高い企業データまたは顧客データが保存されている可能性があるモバイル アプリへのアクセスを制御できるようになったら、次はデータがアクセスされた後に生じることの制御が重要になります。Microsoft Intune のモバイル アプリケーション管理機能およびアプリ保護ポリシーでは、アプリ レベルの認証、コピー/貼り付けの制御、名前を付けて保存の制御などにより、アプリ レベルでデータを保護できます。

Intune のアプリケーション ポリシーを使用すると、ユーザーがアプリでアクセスするデータを使用して実行できることをきめ細かく制御できます。また、マイクロソフトのアプローチではユーザー ID を利用するため、アプリの複数 ID の使用が可能になります。その場合、アプリのポリシーは十分にインテリジェントであるため、会社のアカウントに適用されるデータのみに適用することができます。

Intune のアプリケーション管理機能によって、iOS および Android デバイスにおける Microsoft Office モバイル アプリのデータのきめ細かな制御が可能となり、Exchange Online、Exchange On-Premises、SharePoint Online、および Skype for Business に条件付きアクセス ポリシーを実施できるようになります。

Intune では、以下を可能にすることにより、GDPR への準拠を支援します。

- 従業員がモバイル アプリを使用して企業データに安全にアクセスできるようにし、コピー/切り取り/貼り付け/名前を付けて保存などの制限されたアクションによってアクセスされた後も企業データが引き続き保護されるようにします。

- 管理のためにデバイスを登録して、または登録せずに、データの保護ポリシーをアプリケーションに適用し、ユーザーの私生活に立ち入ってしまうことのないようにしながら企業データを保護できるようにします。

- Intune アプリ ラッピング ツールを使用して、同じモバイル アプリケーション管理ポリシーを、コードを変更せずに、既存の基幹業務 (LOB) アプリケーションにも適用します。

- Managed Browser および Azure Information Protection ビューアーを使用して、管理されたアプリ エコシステム内のデバイスでユーザーが安全にコンテンツを表示できるようにします。

- iOS および Android が提供する最高レベルのデバイス暗号化を使用して、アプリ内の企業データを暗号化します。

- PIN または資格情報ポリシーを実施して、企業データを保護します。

Intune を使用すると、個人のデータを残したまま、ユーザー デバイスとアプリから企業のデータ (アプリ、電子メール、データ、管理ポリシー、ネットワーク プロファイルなど) を選択して削除することもできます。

Intune のモバイル デバイスの管理機能およびモバイル アプリの管理機能を使用すると、GDPR で定義されている個人データまたは機密データであると見なされる可能性のあるデータへのアクセスを保護できるようになり、データがユーザーからアクセスされた後でも引き続き保護されるようになります。

クラウド アプリでデータの可視性と管理を確保する方法

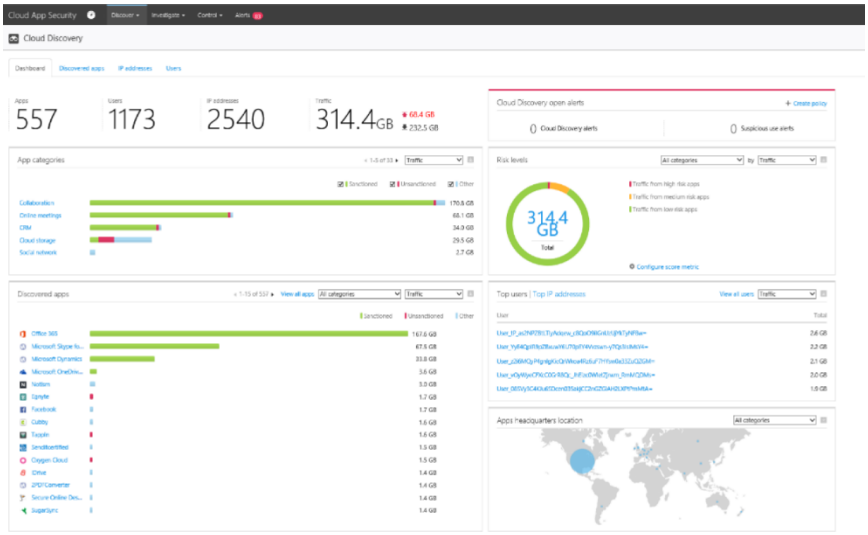
GDPR で定義されているデータ管理者である場合、個人データを処理する目的、条件、および方法を決定する責任があり、その責任は手配したデータ処理業者の監督にまで及びます。お客様は、組織の環境で使用されるサービスとしてのソフトウェア (SaaS) アプリの数の増加に伴い、承認されているクラウド アプリと承認されていないクラウド アプリの両方で個人データを保存および処理してきた可能性があります。クラウドに保存されたデータの検索は複雑な場合が多々あります。

80% を超える従業員が、"承認されていない" SaaS アプリを使用していることを認めていました。また、未承認のソフトウェアの使用がデータ損失を招く可能性があることに懸念を抱いている従業員は半分以下でした[1]。それでもなお組織には、一般に "シャドウ IT" と呼ばれるものにより使用されるアプリで作成、処理、管理、および保存される可能性のある個人データに対して責任を持つ必要があります。組織の環境に対する可視性と管理を強化するほど、その環境をより安全に保護して、GDPR のセキュリティ要件をより確実に満たすことができるようになります。

[1] The Hidden Truth Behind Shadow IT」 (シャドウ IT の背後に隠された真実)、2013 年 11 月発行、Frost & Sullivan の Stratecast 部門による

Microsoft Cloud App Security は、クラウド アプリケーションに高度な可視性、きめ細かい制御、および脅威に対する保護の強化を提供する包括的なサービスです。Microsoft Cloud App Security は、ネットワーク内のすべてのデバイスの 13,000 を超えるクラウド アプリケーションを識別し、リスク スコアリングおよび継続的なリスクの評価と分析の機能を提供します。エージェントは不要です。情報は、ファイアウォールとプロキシから収集され、クラウドの使用やシャドウ IT に対する完全な可視性とコンテキストが提供されます。

マイクロソフトのログ匿名化の機能によって、SaaS アプリの検出時に従業員のプライバシーを保護することもできます。Cloud Discovery のデータ匿名化によって、ユーザーのプライバシーを保護できます。データ ログが Cloud App Security ポータルにアップロードされると、そのログはサニタイズされ、ユーザー名の情報はすべて暗号化されたユーザー名に置き換えられます。



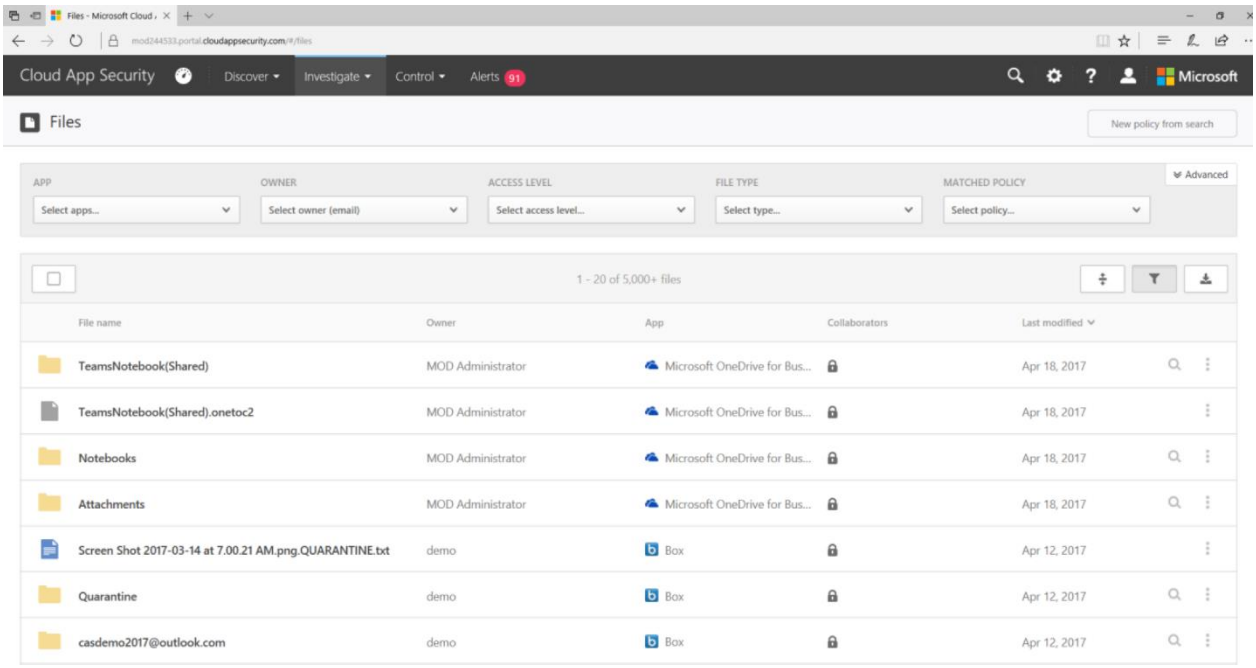
Cloud App Security – Cloud Discovery のダッシュボード

特定のユーザーに対して疑いを持つ理由が管理者にある場合、管理者は既知のユーザー名がどう暗号化されているかを調べて、その暗号化されたユーザー名を使用して調査を開始することができます。ユーザー名の変換はすべて、ポータルのガバナンス ログで監査されます。

リスク評価。Cloud App Security は、個人データが存在する可能性のあるクラウド アプリケーションを検出するだけでなく、検出された各サービスを 60 を超えるパラメーターに照らして評価し、サービス プロバイダー、セキュリティ メカニズム、およびコンプライアンス証明書を評価することによってリスクスコアを出力します。これらの詳細によって、検出された各クラウド サービスの信頼性が特定および評価され、リスク評価によって表されます。Cloud App Security は、リスク スコアと使用状況の組み合わせに基づいて各サービスの総合的なリスク評価を実施するためのツールとなります。

強力なレポートおよび分析機能。組織全体で使用中のアプリケーションを検出することは、データを確実に保護するための最初のステップにすぎません。ユース ケースの把握、トップ ユーザーの識別、各アプリケーションに関連付けられたリスクの特定はすべて、組織の全体的なリスクの状況を把握するために重要なことです。Cloud App Security は、ユーザー、使用パターン、トラフィックのアップロード/ダウンロード、トランザクションについての継続的なリスク検出、分析、強力なレポートの機能を提供し、異常をすぐに特定できるようにします。

調査。組織のクラウド環境についてより詳しく把握するために、Cloud App Security の調査機能では、承認済みの管理されているアプリに関するすべてのアクティビティ、ファイル、アカウントに対する高度な可視性が提供されます。ファイル レベルで詳細な情報を取得し、データがクラウド アプリ内のどこを移動しているのかを検出することができます。



Cloud App Security – ファイルの調査

Cloud App Security を使用して、使用中の SaaS アプリを組織全体から検出することは、可視性と管理を実現するための最初のステップです。また Cloud App Security では、きめ細かなポリシーとガバナンス アクションによって、これらのアプリ内のデータも保護されるうえ、異常検出と行動分析によって、潜在的な脅威も検出されます。

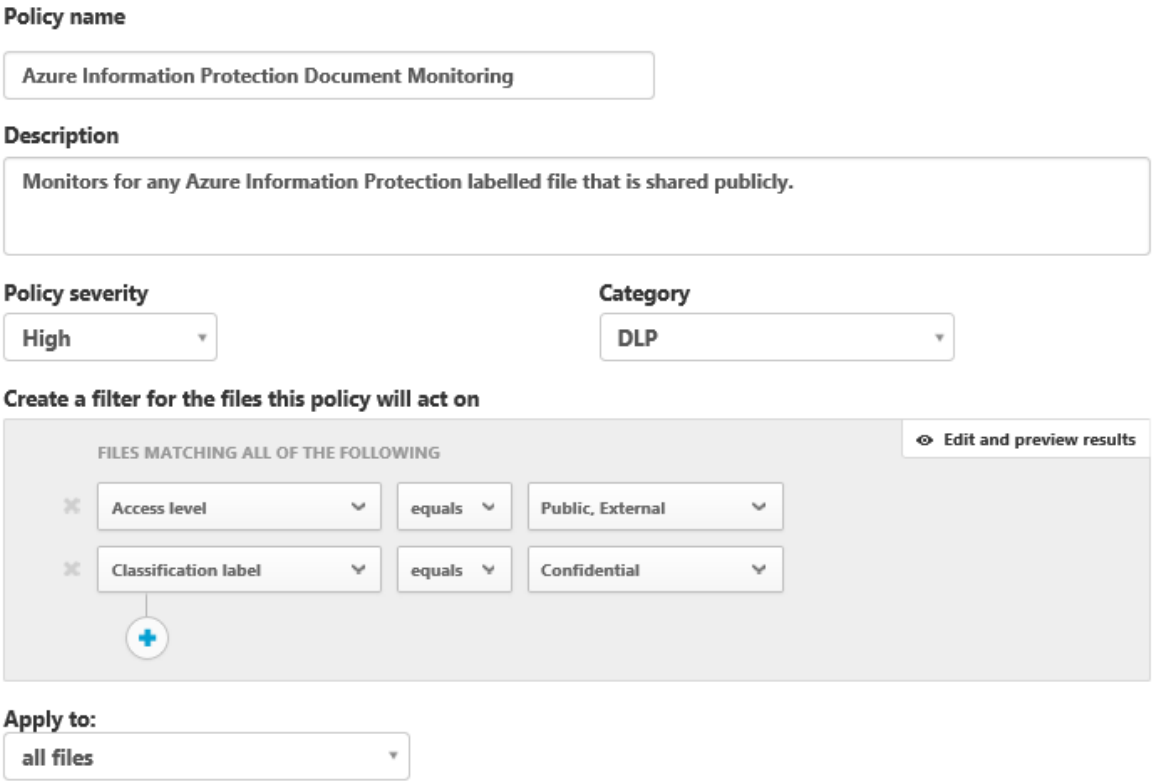
GDPR で個人データと見なされるデータが含まれるクラウド アプリが検出されたら、それらのアプリを適切なポリシーと制御で管理する必要があります。Cloud App Security では、データ コントロール ポリシーの設定と実施が可能です。きめ細かい制御が可能なセキュリティ ポリシーを簡単に構築できます。既定のポリシーを使用することも、独自のポリシーを作成してカスタマイズすることもできます。以下のものを作成できます。

- アクティビティ ポリシー
- 異常検出ポリシー
- アプリ検出ポリシー
- Cloud Discovery 異常検出ポリシー

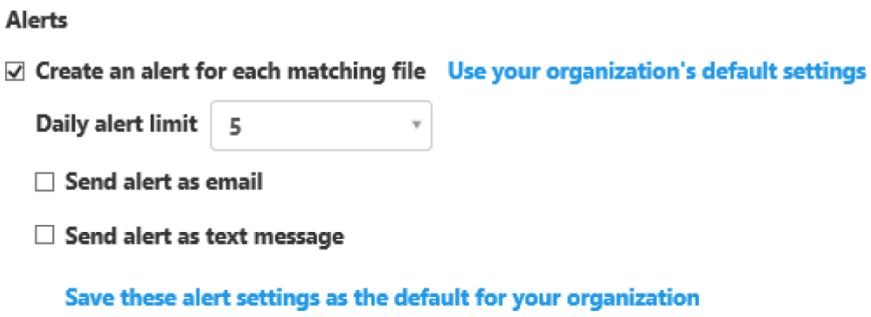
- ファイル ポリシー

さらに、Azure Information Protection との統合を通じ、Azure Information Protection によって設定されたビジネス上の機密度レベルに基づいて、Cloud App Security ポータルを使用してファイル共有ポリシーを設定できます。

Azure Information Protection と Cloud App Security の統合により、クラウドの場所に移動した機密データにまで可視性が拡大されます。次に示すように、Cloud App Security の管理者は、Azure Information Protection のラベルを読み取って適切な措置を講じたりアラートを発したりするポリシーを構成できます。



Azure Information Protection – ポリシーの構成



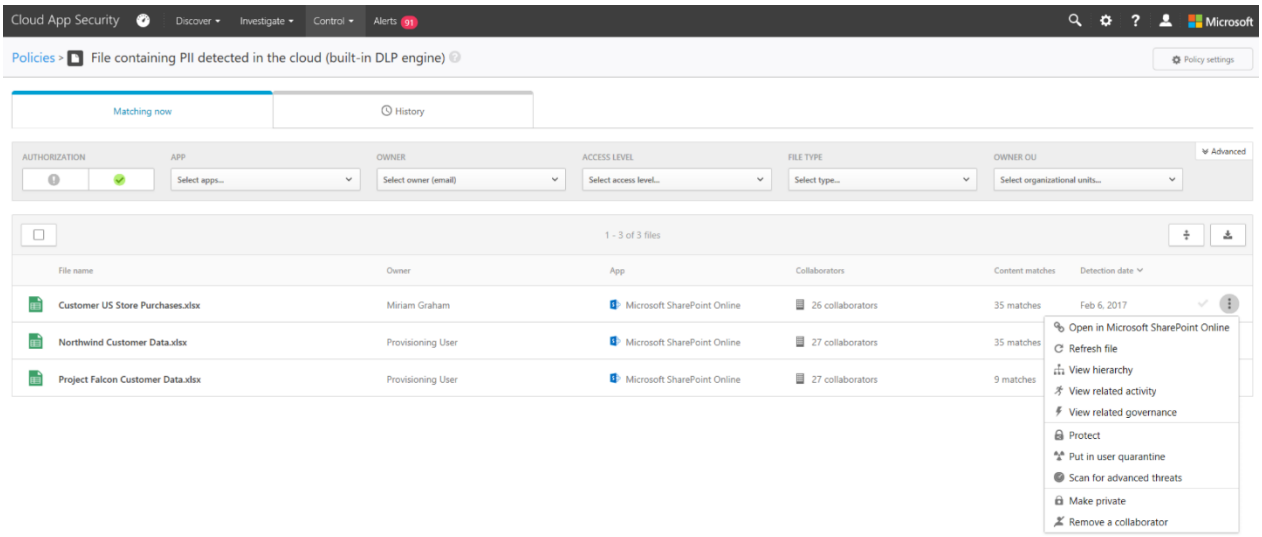
Azure Information Protection – アラートの構成

ポリシー違反があったときは、アラートが送信されてきます。この違反について徹底的に調査し、把握し

た後は、ガバナンス アクションを使用してクラウド アプリ内のデータをすぐに保護することができます。洞察はすべてアクションにつながり、シングル クリックするだけで修復したり、データ共有ポリシーやきめ細かい使用ポリシーを実装したりできます。

たとえば、以下が可能です。

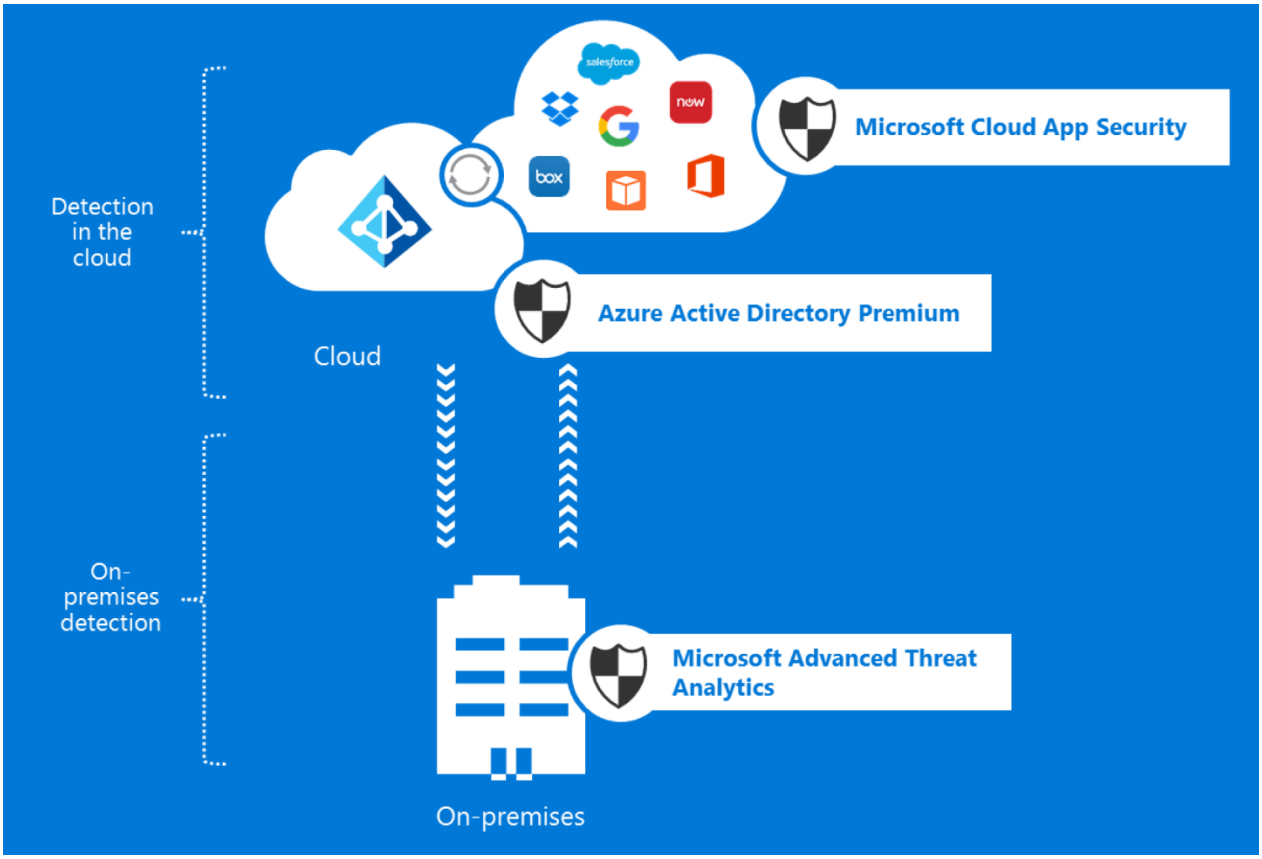
- ファイルの検疫を実行して、管理者のみがそのファイルにアクセスできるようにする。
- 共有を制限する (つまり、リンクをプライベートに設定する)。
- これらの機密ファイルを共有していたユーザーに通知を送信する。
- Rights Management を使用してファイルを保護する。



Cloud App Security – ポリシー違反に対するガバナンス アクション

被害をもたらす前にデータ侵害を検出する方法

GDPR では、個人データの侵害を管理者 (お客様が処理業者の場合)、関連する監督当局、および影響を受けたデータ主体に通知する必要があるときに従うべき期限と条件が定義されています。マイクロソフトの革新的で高度なソリューション セットは、この要件を満たせるよう支援します。Microsoft EMS ソリューションでは、最先端の行動分析と異常検出テクノロジを使用して、オンプレミスおよびクラウド上での疑わしいアクティビティを発見し、脅威を指摘します。それには、ご使用のシステムの既知の悪意のある攻撃 (Pass the Hash、Pass the Ticket など) やセキュリティの脆弱性が含まれます。



オンプレミスとクラウドでの検出

従来の IT セキュリティ ツールは、ユーザーの資格情報が盗まれたときの高度なサイバーセキュリティ攻撃に対する保護機能が十分ではありません。初期セットアップ、ルールの作成、微調整が面倒であり、これらの作業に年単位の時間がかかる場合もあります。毎日、誤検知でいっぱいになったレポートをいくつも受信することもあります。

ほとんどの場合、この情報を確認するためのリソースがなく、確認できたとしても、回答が見つからないことがあります。これらのツールは、境界を保護するよう設計されており、主として、攻撃者がアクセスできないように阻止することを目的としているからです。

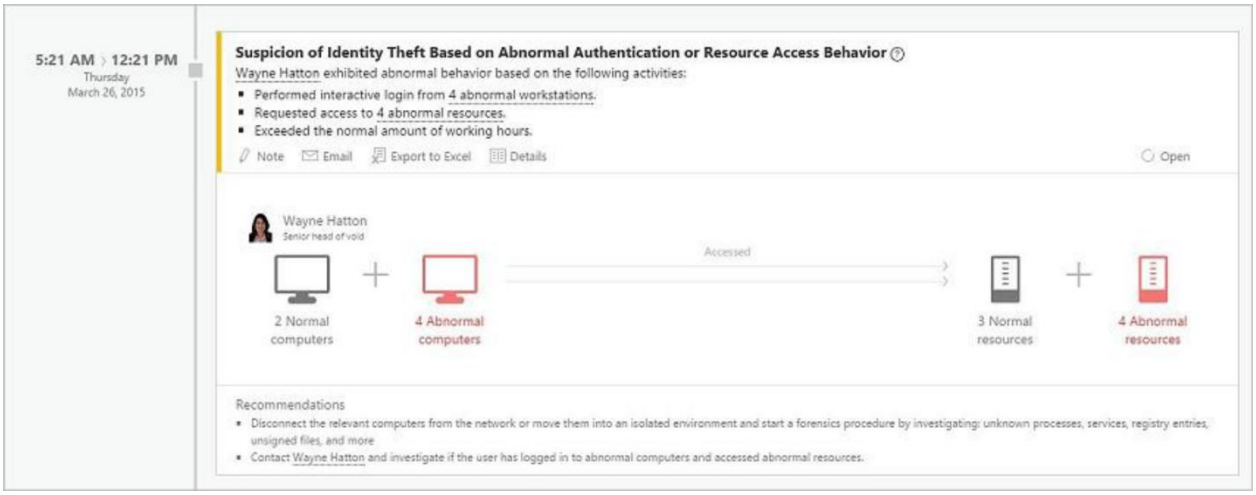
ネットワーク ログは、脅威の検出には不十分です。ログ分析から攻撃者を見つけることは、干し草の山の中から針を見つけるようなものです。手がかりが見つかったとしても、実際にいつ、どのようにして、どこで発生したのかを解明することは困難です。今日の複雑なサイバーセキュリティ攻撃には、別のアプローチが必要です。

Microsoft Advanced Threat Analytics (ATA) は、オンプレミスの非割り込み型ソリューションであり、ディープ パケット インスペクション (DPI) テクノロジを利用して、Active Directory 関連のネットワーク トラフィック、およびセキュリティ情報/イベント管理 (SIEM) と Active Directory からの情報を分析します。

ATA では、この情報を分析して、組織内のエンティティごとに動的な行動プロファイルが作成され、組織のセキュリティ グラフ (ユーザー、デバイス、およびリソースのコンテキストとアクティビティを表したエンティティ相互関係マップ) が構築されます。

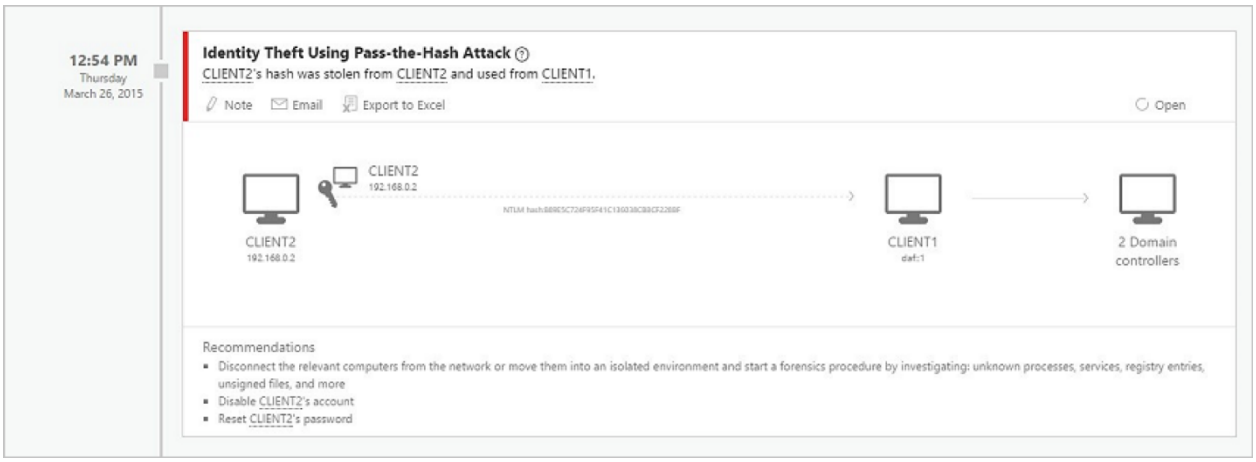
この相互関係マップの構築後、ルールやポリシーを作成したりデスクトップ エージェントやサーバー エージェントをインストールしたりする必要なく、エンティティの**異常な行動**、**高度な攻撃**、**およびセキュリティ リスク**が識別されます。Microsoft Advanced Threat Analytics では、次の異常の検出に焦点が当てられています。

- **異常な行動**: ATA では、Machine Learning アルゴリズムを使用して、通常のエンティティ行動と異常なエンティティ行動を識別し、異常なログイン、異常なリソース アクセス、さらには通常とは異なる稼働時間を検出します。



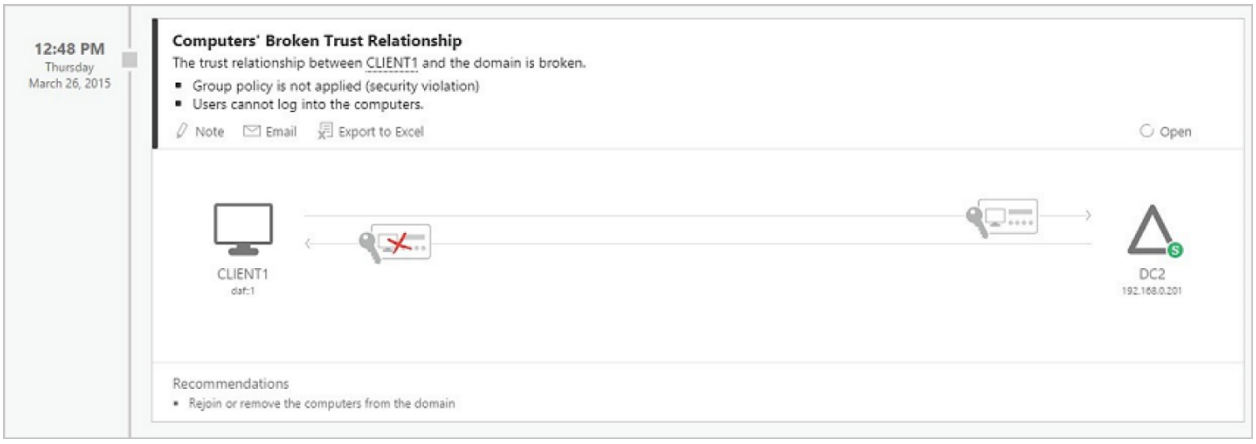
Advanced Threat Analytics – ユーザーの異常な行動のアラート

- **TTP に基づいたほぼリアルタイムの高度な攻撃**: ATA では、ディープ パケット インスペクション テクノロジおよび他のソースからの情報を使用して、Pass-the-Hash、Pass-the-Ticket、Overpass-the-Hash、偽造 PAC、ゴールデン チケット、ドメイン コントローラーでのリモート実行、スケルトン キー マルウェア、ハニー トークン アクティビティなどの高度な攻撃を識別します。



Advanced Threat Analytics – 既知の悪意のある攻撃の検出

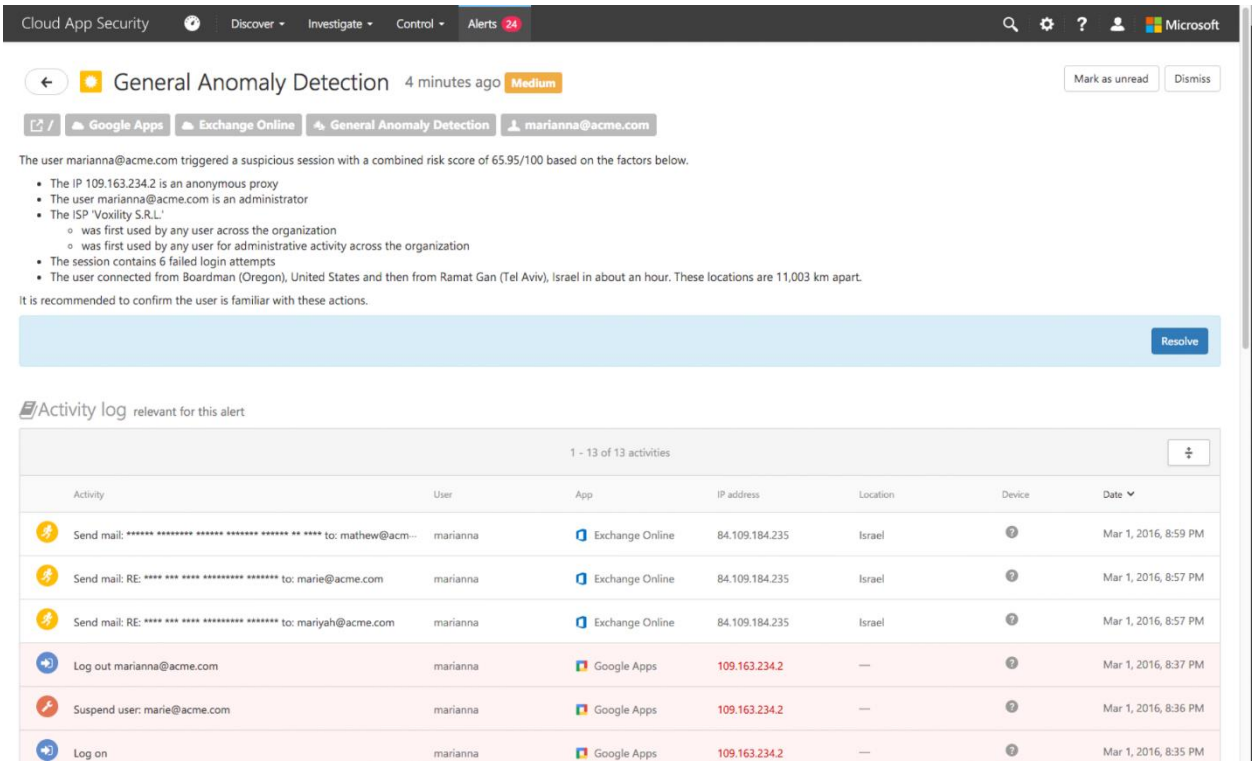
- **既知のセキュリティの問題とリスク**: ATA では、ネットワークでのクリアテキストによるサービス アカウントのパスワードの公開、信頼の消失、弱いプロトコル、プロトコルの脆弱性など、既知のセキュリティの問題とリスクを識別します。



Advanced Threat Analytics – 既知のセキュリティの問題の検出

従来のセキュリティ ツールでは、レポートが途切れることなく作成されます。それらのレポートをふるいにかけて重要な関連アラートを特定するには膨大な処理が必要となり、対処しきれなくなる場合があります。ATA では、攻撃タイムラインが提供されます。これは、わかりやすい、効率的で、便利なフィードであり、タイムライン上の的確な情報を見つけ出して、"誰が、何を、いつ、どのように" したのかを把握できるようになります。また、ATA では、疑わしいアクティビティごとに、調査と修復に関する推奨事項が提案されます。

クラウド アプリのシナリオで各機能を使用して可視性とデータの管理性を確保する方法について、概要を説明してきましたが、そのほかにも、Cloud App Security は、クラウド アプリのデータをサイバーセキュリティの脅威から保護するのに役立ちます。データ侵害の兆候と考えられるクラウドの使用状況の異常を特定できます。Cloud App Security の高度な機械学習ヒューリスティックは、各ユーザーが各 SaaS アプリケーションと対話する方法を学習し、動作分析によって各トランザクションのリスクを評価します。これには、2 か国からの同時ログイン、テラバイト単位のデータの突然のダウンロード、またはブルートフォース攻撃の可能性を示す複数回のログインの失敗が含まれます。



Cloud Add Security – 一般的な異常検出

異常検出は、マイクロソフトの膨大な脅威インテリジェンスおよびセキュリティ調査データに基づいたものです。Cloud App Security は、マイクロソフトの包括的でアジャイルなセキュリティ プラットフォームを利用して、マイクロソフトのインテリジェント セキュリティ グラフの洞察による情報を得ます。

Azure Active Directory の監視とレポート

満たす必要がある GDPR の主要素の 1 つに、実施されている管理と保護に関連する監査の要件があります。Azure AD では、重要な監査レポートが提供されます。たとえば、疑わしい行動や高度な攻撃から保護するための詳細なセキュリティ レポートがあります。

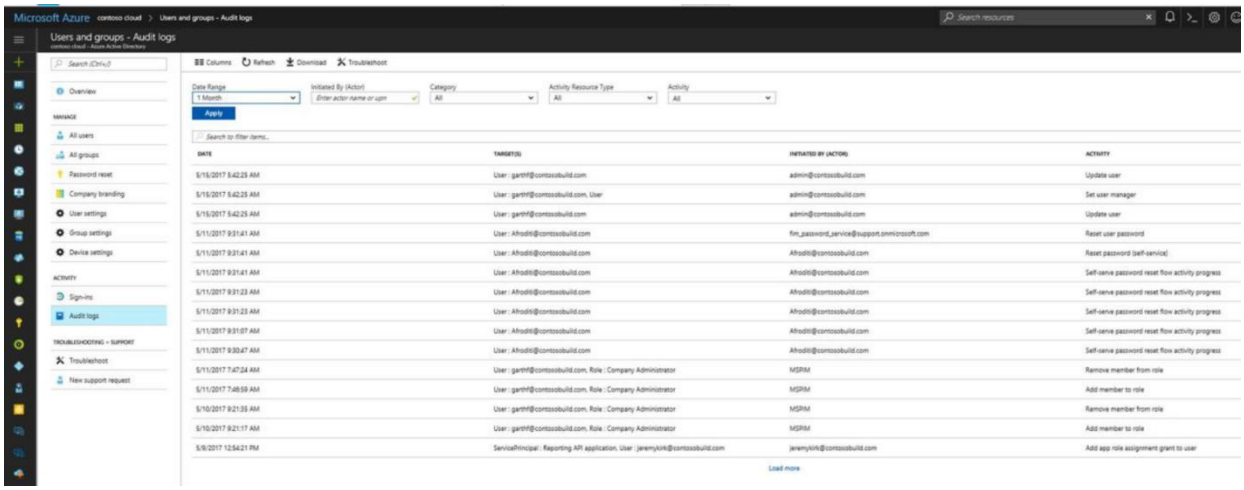
Azure Active Directory のアクセス、使用状況、およびセキュリティの各レポートを使用すると、組織のディレクトリの整合性とセキュリティに対する可視性を確保できます。ディレクトリ管理者は、この情報を使用して、潜在的なセキュリティ リスクのある場所をより的確に判別し、それらのリスクを軽減するための適切な計画を立てることができます。

Azure の管理ポータルでは、レポートは次のように分類されます。

- **セキュリティ レポート** - リスクのフラグ付きユーザー、およびリスクの高いサインイン (匿名の IP、ありえない移動、未知の場所、および感染しているデバイスからのサインイン) の 2 種類のレポートがあります。

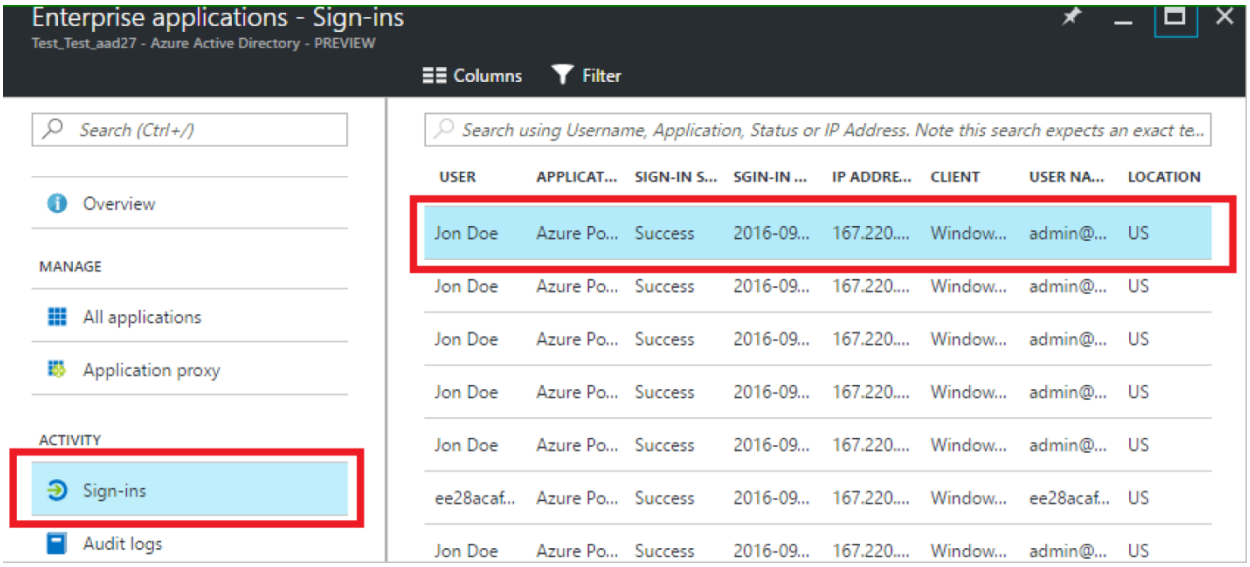
- **ユーザー固有レポート** – 特定のユーザーのデバイス/サインイン アクティビティのデータが表示されます。

- **アクティビティ ログ** – 過去 24 時間、過去 7 日間、または過去 30 日間のすべての監査イベントの記録、グループのアクティビティの変更、およびパスワードのリセットと登録のアクティビティが含まれます。



Azure Active Directory – 監査ログ

アクセスおよび使用状況レポートによって、組織のディレクトリの整合性とセキュリティが可視化されます。[サインイン] オプションを使用すると、個人データおよび機密データが含まれるアプリケーションへのサインイン イベントすべての完全な概要を表示できます。



Azure Active Directory – サインインの分析

使用を開始する方法

EMS 無料試用版

マイクロソフトは、テクノロジを直接体験することによって、ビジネスに適した購入を決断できることを理解しています。このため、マイクロソフトは、90 日間無料試用版を用意しました。Enterprise Mobility + Security ソリューションを試用して、このソリューションがお客様のビジネスの課題にどのように対応するか評価していただけます。また、マイクロソフトの経験豊富な専門家による 1 対 1 のデモを要求して、お客様はオフィスから出ることなく、EMS を体験していただくこともできます。使用を開始する方法については、試用版のページを参照してください。

展開のサポート

マイクロソフトの FastTrack サービスが、EMS サブスクリプションの一環として含まれています。FastTrack との連携により、展開の成功を加速できます。FastTrack は、成功プランを使用して、それぞれの専門分野の担当エンジニアによる無料の展開サービスを提供します。ビジネス価値とコンプライアンスをより迅速に実現するために必要なリソースおよび専門知識を提供することによって、EMS 製品をスムーズに展開できるよう支援します。ほかにはないマイクロソフトの FastTrack プログラムのサポートの利用については、こちらを参照してください。

GDPR の詳細が必要な場合は、以下のリンクを参照してください。

- GDPR に関するマイクロソフトのサイト
- マイクロソフトと GDPR に関するホワイトペーパー
- GDPR に向けたマイクロソフトの取り組みに関するビデオ

ライセンス

EMS のライセンスの詳細については、EMS のライセンスのページを参照してください。ご質問がある場合は、0120-41-6755 までお問い合わせください。