MVISION Cloud Security Risk Assessment

無償のクラウドセキュリティ・脆弱性分析で、クラウドサービスの利用から発生するリスクを把握

ビジネス向けクラウドサービスにより、ビジネスに利用できるリソースが増え、ケイパビリティを拡大する新しい機会が生まれています。しかしこういったクラウドサービスの保護はIT環境において大きな課題にもなります。McAfee® MVISION Cloud Security Risk Assessmentは、事業のさらなる成功を目指す組織に対して、組織に存在するクラウドセキュリティリスクを明示し、クラウドサービスの利用に必須の保護策を優先順位付けします。

リスクを過小評価していませんか？

クラウドの利用が広がるにつれ、ビジネス機会だけでなく潜在的な脆弱性も増加しています。2019 Cloud Adoption and Risk Report（2019年クラウドの採用とリスクに関するレポート）では、大半の組織で約1,935のクラウドサービスを利用しているものの、その多くは30程度しか利用していないと考えていることがわかりました。

MVISION Cloud Security Risk Assessmentは、以下のような一般的なビジネスアプリケーションの使用によって組織に発生する脆弱性を分析します。

- **シャドーIT：**未承認のクラウドサービスの利用
- **SaaS：**Microsoft Office 365、Salesforceなど
- **IaaS：**Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform

自社に存在する脆弱性に気付いていますか？

- 企業のデータはどこに保存していますか？
- 誰がそのデータにアクセスしますか？
- 現在、どのようなクラウドサービスが承認されないまま利用されていますか？
- 未承認のクラウドサービスにより、どのようなリスクがあるでしょうか？
- 機密データが社外で共有されていますか？
- クラウドサービス内でDLP違反はありますか？
- アカウント侵害や内部の不正使用のリスクはありますか？
- データの安全はいかなる場合（保管中、移動中、及び使用中）でも確保されていますか？
- 規制は遵守されていますか？（PCI、OFSI、HIPAA、GDPRなど）
- AWS/Azure/GCPはセキュリティのベストプラクティスに沿って設定されていますか？

主な特徴

- Shadow IT Assessmentは高リスクなクラウドサービスを可視化します
- SaaS Assessmentはファイル共有リスクを識別します
- IaaS Assessmentは不適切な設定を検出して修正します
- エグゼクティブサマリと詳細レポートを提供します

詳細

クラウド時代に向けたクラウドネイティブのデータセキュリティの詳細はこちらをご覧ください。
www.mcafee.com/cloud-security

McAfeeにアクセス

Shadow IT Assessment

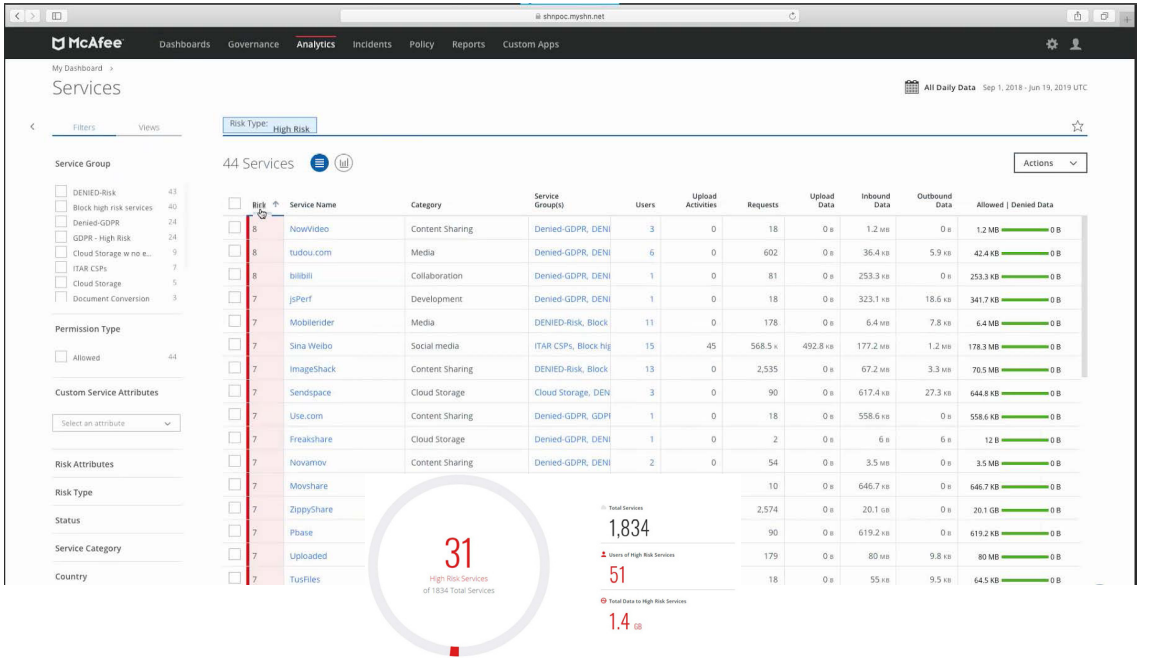
高リスクなクラウドサービスの可視化

Stratecastの調査によると、企業のIT部門が自社内のクラウドサービスの利用状況を評価したところ、ほとんどの企業で当初想定数の10倍のクラウドサービスが利用されており、今まで聞いたこともないようなアプリケーションやサービスも多く使われていたことがわかりました。各サービスのリスクとセキュリティコントロールを評価することで、ITチームはどのサービスを推奨または利用可にすべきかについてインフォームドチョイスができるようになります。

主要調査結果のサマリーには以下のような内容が含まれます。

- 利用中のクラウドサービス数
- 高リスクのクラウドサービス
- どのサービスがIPのオーナーシップを得るか
- 各サービスにアクセスしているユーザー
- 各サービスでアップロード及びダウンロードされるデータ量
- サービスの地理的ロケーション
- 高リスクの地理的ロケーション
- アクセスされているクラウドストレージサービス数
- プロキシ漏えいの識別

クラウド時代に向けたクラウドネイティブのデータセキュリティの詳細はこちらでご覧ください。www.mcafee.com/cloud-security



SaaS Security Assessment

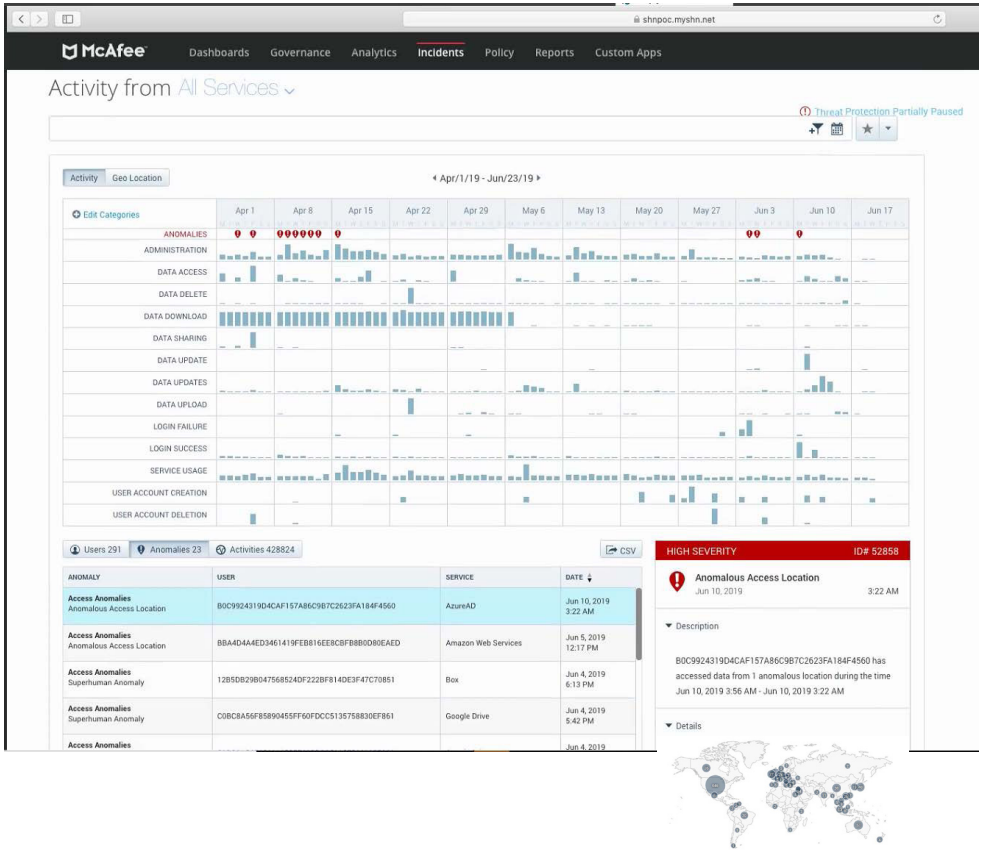
ファイル共有リスクの識別

従業員が利用するアプリはますます多様化しています。調査対象となった従業員のうち、80%はSoftware-as-a-Service（SaaS）アプリケーションを、多くの場合IT部門の承認なく使用していました。IT部門が承認したアプリでも課題はあります。例えば、Office 365での脅威は過去2年間で63%増加しました。

主要調査結果サマリーには以下のような内容が含まれます。

- OneDriveとSharePointに保管されている、機密情報を含むドキュメント数
- 管理者権限を持ったユーザー
- 脅威の存在を暗示するような、変則的な使用イベント
- 「パスワード」というキーワードを含むファイル
- 誰とでも共有できる追跡不可能なリンクを含む機密データのファイル
- すべてのデータへのアクセス権限を持つユーザー
- 過剰なユーザーアクテビティのリスト
- 不審な地域からのログイン試行
- 不審行動分析

クラウド時代に向けたクラウドネイティブのデータセキュリティの詳細はこちらでご覧ください。www.mcafee.com/cloud-security



IaaS Security Assessment

不適切な設定の検出と修正

AWSのようなInfrastructure-as-a-Service (IaaS) は生産性やアジリティの向上に役立つため、ますます頻繁に利用されるようになっています。しかしこれは同時に、組織におけるサイバーセキュリティを複雑にしています。平均的な組織では、不適切な設定をされたIaaSインスタンスが最低でも常時14個実行されており、これが原因となったインシデントは月に平均2,269件発生しています。設定ミスにより重大な問題が発生する前に対処しましょう。

以下の設定ミスを識別します。

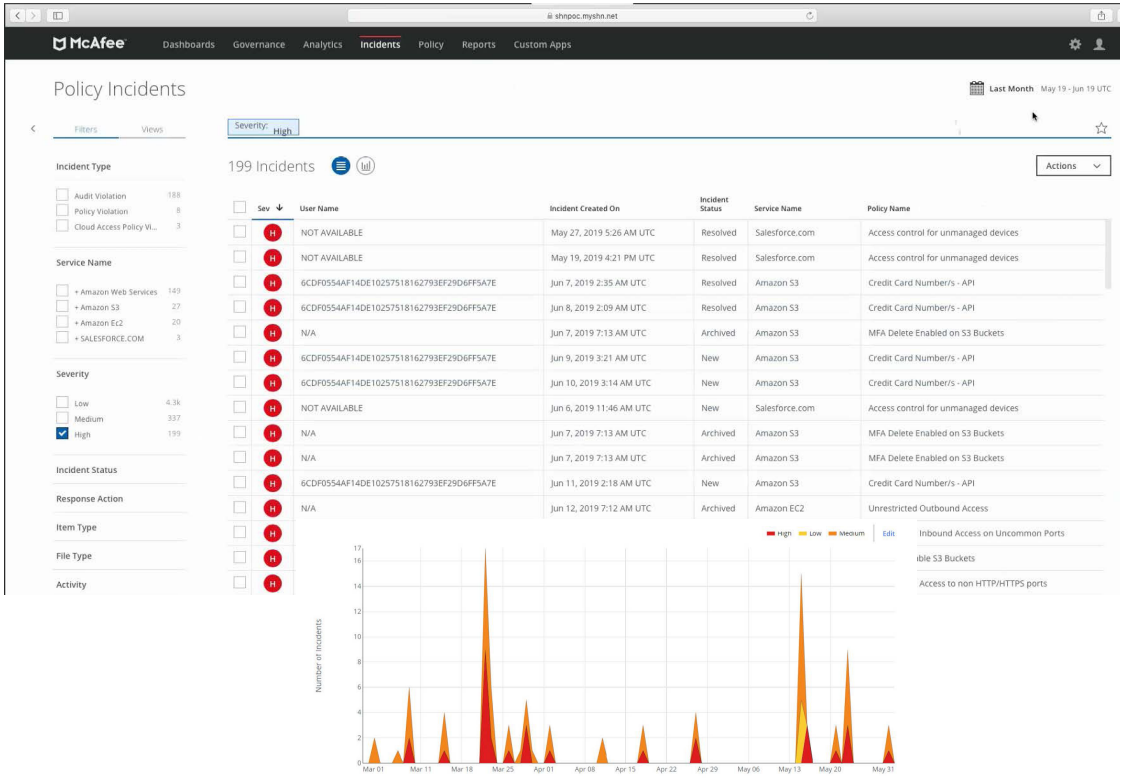
- Elastic Compute Cloud (EC2) インスタンス
- Amazon Machine Images
- S3バケット、EBS、RDSなどのストレージサービス
- Identity and access management (IAM)
- CloudTrailのようなログ記録および監視シリーズ
- ネットワークセキュリティグループおよびバーチャルプライベートクラウド (VPC)ネットワーク

以下を使用して不適切に設定されたサービスを修正します。

- Center for Internet Security (CIS) ベンチマークの推奨レベル1および2
- HIPAA-HITECH、ISO、FedRAMP、ITAR、PCI DSS、または内部コンプライアンスポリシーなどの規制順守の推奨

アクティビティレポート：

- 管理された、及び管理されていないAWSアカウントのリスト
- 誰がどのサーバーにアクセスしているか
- 実行されたアクテビティのリスト
- 地理的ロケーション及びIPアドレス
- アクティブでない、または元従業員のユーザーアカウントによるログインの成功／失敗の記録



クラウド時代に向けたクラウドネイティブのデータセキュリティの詳細はこちらでご覧ください。www.mcafee.com/cloud-security

わずかな労力で大きな見返り

MVISION Cloud Security Risk Assessmentのプロセス

MVISIONプラットフォームのスムーズなアーキテクチャのため、非常に簡単にMVISIONクラウドセキュリティリスク評価のメリットを享受いただけます。評価プロセスの5つのステップをご覧ください。

ステップ 1: MVISION Cloudセキュリティチームと一緒に、必要なアセスメントのスコープを決定します。

ステップ 2: MVISIONチームがシャドーITへのプロキシ（ファイアウォール）ログを収集またはプロキシとの接続をセットアップします。

ステップ 3: MVISIONチームはSaaS、PaaS、IaaS環境との接続用にAPIインテグレーションを確立します。

ステップ 4: MVISIONチームがMVISIONトリートメントへのアクセスをお客様に提供します。

ステップ 5: MVISIONチームがMVISION Cloud Security Risk Assessmentレポートを提供します。

次のサービスをご利用いただけます

- エグゼクティブサマリ及び詳細な調査結果レポート。
- 評価期間中の、MVISIONのテナントクラウドサービスの情報とレポートへのアクセス。

詳細

Cloud Securityの詳細についてはこちらにアクセスしてください。
www.mcafee.com/cloud-security

マカフィー株式会社　www.mcafee.com/jp
東京本社　〒150-0043　東京都渋谷区道玄坂 1-12-1　渋谷マークシティウエスト 20F　TEL：03-5428-1100（代）　FAX：03-5428-1480
西日本支店　〒530-0003　大阪府大阪市北区堂島 2-2-2　近鉄堂島ビル 18F　TEL：06-6344-1511（代）　FAX：06-6344-1517