IBM Security

IBM

データの場所に関係なく、クラウドでセキュリティーを購入し導入する

クラウド・モデルまたはハイブリッド・モデルに移行している組織は、コンプライアンス用レポートと高度な脅威検知の効率性を達成することが可能になりました

IBM Security ホワイト・ペーパー

IBM QRadar がネットワークを可視化

組織の規模に関係なく、データとネットワークのセキュリティーは今日、手ごわい作業です。新しい脆弱性がほぼ毎日発見され、旧マルウェア用の検出スクリプトが作成されるとすぐに新種のマルウェアが開発され、サイバー犯罪者は、プロのサポート・チームがバックアップする Darknet で事前パッケージ済みエクスプロイト・キットを購入できます。セキュリティー・アナリストの担当者は、ネットワーク末端を保護するために設計されたポイント・ソリューションを複数必要としています。可 視性、全体像、何かがおかしいときに感じる生来の勘が必要です。

IBM® QRadar® はこれらの課題を解決します。誰がいつどこで何をしているのかを示すことができる幅広い機能でデータとネットワークを保護します。ダッシュボードと高度な視覚化機能を使って、数千あるいは数百万の個々のインシデントをまとめ合わせて、疑わしい問題としてシンプルに示し、疑わしいアクティビティの詳細な記録を保持して将来の分析に対応します。それと同時に、その高度なログ機能とレポート生成ツールによって、レポート作成義務などの基本要件に素早く対応できます。

また、IBM QRadar on Cloud の登場により、ハードウェアとソフトウェアの導入と維持を回避でき、QRadar が収集する情報の活用に集中することが可能になりました。チームが状況を監視しているので、常にコントロールを維持できます。自社の環境を調査し、検知機能を微調整し、同僚と連携してすべての脅威検知機能と対応スキルを深化させましょう。

QRador クラウド・ソリューションは毎秒最大

80,000

のイベントを処理できます。[1]

▸ 詳細を見る: IBM QRadar on Cloud の Web ページ

1 “IBM Security Intelligence on Cloud onboarding,” *IBM Knowledge Center*

規制とセキュリティーの要件を同時に満たす

単純な攻撃を防ぐためにネットワークの境界に基本的なセキュリティー対策を講じてはいるけれども、ほとんどのエンドポイントのセキュリティーは不十分で、一部のユーザーはつい怪しいリンクをクリックしてしまうというのが貴社の状況ではないでしょうか。デバイスと資格情報のセキュリティーが侵害されることがあまりにも多く、データ損失と潜在的なビジネス中断の可能性が生じてしまいます。

まず、規制要件について考えてみましょう。これらの要件では、すべてが保護されていることを証明するために、システムとデータ、そして文書を適切にロックダウンすることが求められます。セキュリティー分析システムを導入すると、セキュリティー・チームに課せられるワークロード・コンプライアンス・レポートの負担を軽減することができます。これらのシステムによって、適切にフォーマットされた包括的なレポートを準備すること、ネットワークに関する情報を監査に適したフォームで収集、キュレート、検証することが容易になるからです。

では、重要データが作成、保存、送信される内部環境の複雑さについて考えてみましょう。現代のネットワークには多くのアセットが詰め込まれており、それぞれのアセットに悪用可能なセキュリティーの欠陥があるのが一般的です。それらのアセットには、ネットワークの多様なオペレーティング・システム、サーバーからルーター、スイッチからファイアウォールまでの各種ハードウェア、Web ベースなどのアプリケーション・ソフトウェアが挙げられます。各エレメントの存在がネットワーク全体を保護することを困難にし、サイバー犯罪者は最も脆弱なリンクを利用してアクセスします。

データ保護およびコンプライアンス・レポート・システムの導入はごく簡単ですが、監査員を満足させ、組織の重要データを保護することは容易ではありません。IBM Sense Analytics Engine™ がバックアップする QRadar など、システムが高度になるほど、日常的な作業、および調査とインシデント対応を必要とする非日常的なネットワーク侵害の両方の管理に徹底的に備えることができます。

2015 年、ハッキング事象は過去 9 年で最高数に達し、2014 年よりも

8.4%

増加しました。[1]

- もっと多くを学ぶ: IBM X-Force® が提供する、今日の企業への脅威に関する知見

1 “Identity Theft Resource Center Breach Report Hits Near Record High in 2015,” *Identity Theft Resource Center*、2016 年 1 月

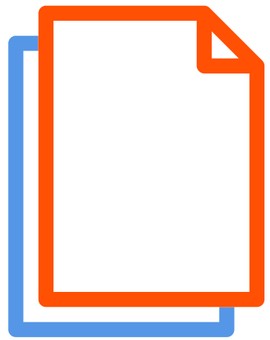
コンプライアンスとセキュリティーをサポートするための詳細な知見を入手

マルウェアを検知、根絶し、ファイアウォール・ルールを確立してサブネットを保護するのは重要なことです。だから、貴社では境界を守るセキュリティーに資金を投じていることでしょう。しかし、セキュリティー分析ソフトウェアは、インターネットに接続された周辺機器は完全に安全ではなく、組織は行動の変化と異常を検出できなければならないという基本的なコンセプトの上に成り立っています。

セキュリティー分析を追加する 1 つの方法は、多額の予算を組み、データセンターのスペースを空け、数週間から数カ月かけてオンプレミス・ソリューションを導入することです。その間、チームは自動更新サービスをスケジューリングし、脅威に関する情報フィードを構成し、ネットワーク・スキャンのスケジュールを作成し、データ保持期間を定義します。セキュリティーへの投資から大きな成果を上げるにはこれらすべてを実施しなければなりません。

もう 1 つの方法は、セキュアなデータ・ゲートウェイを導入して、毎月の運用費が予測可能な、プロの手で導入、管理されたクラウド環境にセキュリティー・データを送信する方法です。このクラウド・モデルの場合、コントロールは企業の手にあり、スタッフはソフトウェア・パッチの適用やデータ・バックアップの実行ではなく、環境の監視、脅威検知ルールの調整、規制または管理レポートのカスタマイズに多くの時間を費やすことができます。

スタッフは数日もすれば、単純なログ・イベント (Jackie Jones がシカゴから午後 2:32 にログインした) に煩わされることがなくなり、代わりに行動の変化 (Jackie Jones が東南アジアから今週後半午前 3:07 にログインした)が通知されます。不要な中断をなくすことで、行動の違い (Jackie は旅行中) または何か別の事態が進行中なのかを調べる時間ができます。



QRadar は規制コンプライアンスから脆弱性管理まで、

1,500

ただの定義済みレポート・タイプ以上のレポートを作成できます。[1]

ホワイト・ペーパーを読む: QRadar の詳細

1 Lee Bell “IBM builds QRadar Security Intelligence in the cloud,” *The Inquirer*、2015 年 4 月

規制コンプライアンスへの工程の着手

QRadar on Cloud は、主要なビジネス主導型機能を実行します。データを保護し、保護を実現するセキュリティー・プラクティスとイベントの記録を監査対応フォームで保持することで、行政機関と産業の規制への準拠を支援します。

これらの規制に従わない場合、マルウェアでデータ損失を招いて多額のお金を失うように、多額の刑罰が科せられるおそれがあります。

消費者の個人情報と財務情報を保護し、企業による顧客データと組織データの管理の透明性を高めるように設計された、多数の要件とベスト・プラクティス基準が収集、保存、保護されます。サーベンス・オクスリー法 (SOX)、クレジットカード業界データセキュリティー基準 (PCI DSS)、医療保険の携行性と責任に関する法律 (HIPAA)、EU の一般データ保護規則 (GDPR)、およびその他の規制により、企業は民事罰則と刑事罰則、決済カードの使用禁止、基準に準拠していないプラクティスのためにビジネスが中断して壊滅的な打撃を受けるなどその他のリスクに直面するおそれがあります。

たとえ罰則のプレッシャーがなくても、規制コンプライアンスを確実に遵守するプロセスによって、データ保管、暗号化、ネットワーク・ノードの保護のベスト・プラクティスが促進されます。規制コンプライアンス・ワークフローとストレージ・アーキテクチャーを組み込むインフラストラクチャーの設計と維持を行えるソフトウェアはありませんが、QRadar on Cloud は不適合プラクティスを見つけて、データとアプリケーションの正常性を証明できるように支援します。

HIPAA 違反は刑罰の対象となることがあり、違反 1 件につき最大

米ドル50,000

になり、年間最大 150 万米ドルになります。[1]

- 詳細情報: このホワイト・ペーパーで取り上げられている規制コンプライアンスの注意事項

1 “HIPAA Violations and Enforcement,” *American Medical Association*. 、2016 年 7 月 26日にアクセス

データをよく監視することで、新たに進化した脅威に対処

一部のセキュリティーの脅威には、セキュリティーの個々の面に対処する専用ツールを使って戦術的にアプローチできます。これらはのツールは、定義済みの脅威や既知の問題の対処で役立つことがあり、ネットワーク・ポートを選択的にブロックしたり、マルウェアのインスタンスを削除したり、特定された脆弱なアセットにパッチ適用したりしてシンプルに対応できる場合があります。

しかし、QRadar ソフトウェアは、すべてのセキュリティー情報モジュールで共有されたもっと広範なセキュリティー・データを収集するので、ポイント・ソリューションよりもはるかに有効に活用できます。ネットワークのデータ・フロー基準のしきい値を観察、計算したら、これらのしきい値に違反するイベントを自動的に感知し、セキュリティー・スタッフに通知します。しきい値ルールを設定すると、異常に大きいアウトバウンド・データ転送、アプリケーションにおける帯域幅使用の変化、あるいは予期しない IP アドレスからの不自然に多いログイン試行回数などを検知できます。

QRadar は接続されたイベントも監視して、ユーザー ID、発信元および宛先 IP アドレス、アクティビティが発生した地理情報を比較します。リンクされたこれらのイベントのコンテキストを調べ、本物の攻撃と新しい行動の 1 回限りのインスタンスをより正確に区別します。特定のサービスやアセットが突然消えた場合の　のパターンも探します。これは、アセットがオフライン (マルウェアが原因の可能性) になっているか、QRadar がユーザー行動基準の逸脱を検出したことを意味する場合があります。

医療業界において、セキュリティー攻撃が医療記録データ

漏洩

の主な原因です。[1]

- 詳細情報: IBM X-Force が収集するセキュリティーの詳細な知識

1 “Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data,” *Ponemon Institute*、2016 年 5 月

クラウドベースのセキュリティー・ソフトウェアで新しい費用モデルを採用

ソフトウェアは、IT と企業の運営を実現する上で非常に重要かもしれませんが、ほとんどの組織では、セキュリティー・ソフトウェアを社内で維持することでワークロードが増え、実質的に主要セキュリティー・タスクの妨げになる可能性があります。セキュリティー・スタッフが兼任する必要があるいくつもの役割を減らして簡素化できるのであれば、クラウドベースのソリューションを採用する動機付けになるかもしれません。

さらに、初期仕様から最後の廃棄処分まで、オンサイトでホストするハードウェアのライフサイクルによってさらに負担が増す可能性があります。これはほとんどの場合、十分なスペア・パーツを手元に保持すること、メンテナンスを念頭にハードウェアを選ぶことを意味します。また、これらすべてがすでに多忙な現場スタッフの責任になるのが一般的です。

セキュリティーの改善には必ず、ある程度のレベルの人的および技術的資源が必要になりますが、ホストされたクラウドベースのソリューションならば、セキュリティー・スタッフがルーチン作業に費やす時間と関連費用を分析と計画策定に割り当てることができます。システム・アップグレードとアプリケーションの修正はスペシャリストがリモートで対処でき、現場の IT インフラストラクチャーを中断せずにこれらの作業を遂行できます。クラウド・アプリケーションを定義するリモート・アクセスにより、現場のスタッフ・メンバーは物理的にサーバーを設置し、プロビジョニングしなくても、新しいソフトウェア機能を利用できます。これらのことから、オンサイト・リソースをオーバープロビジョニングすることなく、クラウドベース・ソリューションを迅速なスケジュールで、通常は数日か数週間で入手し、拡張できます。

QRadar on Cloud インフラストラクチャーは、信頼できる IBM プロフェッショナルによって、

24 時間年中無休

で監視されます。[1]

- この IBM ホワイト・ペーパーを読む: クラウド・ソフトウェアの採用によって達成する費用の調整に関する詳細

1 “IBM QRadar on Cloud,” *IBM Corp.*、2015 年 4 月

セキュリティーへの投資で変化と成長に向けて準備する

他のあらゆるテクノロジーと同様に、セキュリティー・ツールが単独で動作することはめったにありません。他の機能と連携するツールは、変化する脅威の環境により適切に対処したり、特定に機能を追加したりすることができ、その中には、すでに投資した境界防御ツールが含まれます。

QRadar on Cloud は、過去 10 年にわたって開発された 500 超の既存のインテグレーションを継承して、オンプレミスのお客様からの要求に対応し、セキュリティー情報プラットフォームを補完する他社製ソリューションと連携します。クラウドを展開する経験豊富なプロフェッショナルはほとんどの場合、新しいサポート・モジュールを開発しなくても、貴社のアセットとアプリケーションからのデータの受信を開始できます。ほとんどのお客様は、契約締結後わずか数日で価値を実感し始めます。

たとえば、IBM X-Force Threat Intelligence の調査を通じて収集されたセキュリティー・データもシームレスかつ継続的に QRadar on Cloud 環境に統合されて、進化する脅威のベクトルと確認された攻撃、およびこれまで報告されなかった脆弱性に関する数百テラバイトもの情報を利用します。

IBM Security App Exchange からの、ネットワーク監視機能を強化する新しい拡張機能やアプリをダウンロードおよびインストールできます。また、IBM クラウド・メンテナンス・チームがテクノロジーの拡張をサポートします。このようなサポート対象の拡張機能はすでに数十もあり、その中には新しい仮想化機能、統合機能、パッチ、カスタム・ルールがあり、IBM QRadar User Behavior Analytics アプリなどの新しいアプリを補完します。サイトの全コンテンツは *Ready for IBM Security Intelligence* 検証プロセスを通じて IBM Security によって検証されます。

QRadar はログ・イベントとネットワーク・フローを

500+

のアプリケーションとデバイスから収集できます。[1]

- 詳細情報: IBM Knowledge Center からの QRadar プラグインと拡張機能

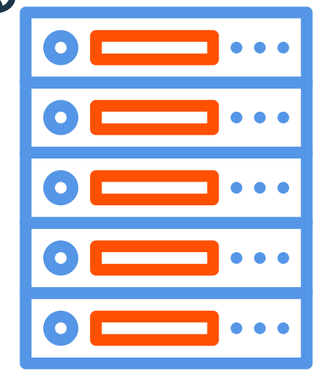
1 “Introducing the IBM Security App Exchange,” *IBM Corp.*、2015 年 12 月

スケーラブルで柔軟なインフラストラクチャーを必要なときに機能させる

サービス型ソフトウェアを購入すると、拡張性と柔軟性のメリットを得られます。容量を変更する場合、オンサイトのインフラストラクチャーに制約されないし、社内スタッフの有無に左右されることがはるかに少ないからです。クラウドに展開したセキュリティー分析ソフトウェアの長所を理解するには、2 つのタイプの規模の変更について考えてみればわかります。

季節性: ほとんどの企業の作業負荷には繁忙期と閑散期がありますが、その一部は、正確なタイミングは無理でも範囲ならかなりの確率で予測できます。従来のソフトウェア購入だと、通常の使用時よりも多くのハードウェア容量に資金を費やすことになっても、最悪のシナリオのとき (つまり、繁忙期) に購入せざるをえないことがあります。

企業の成長: 同様に、合併、買収、または他の成長を計画している組織はほとんどの場合、必要な容量が増えると予測して「不必要に」大きな買い物をする必要に迫られます。しかし、クラウドベースの導入なら、必要に応じて少しずつ容量を購入またはリリースすることができます。インフラストラクチャーはクラウド内にあり、容量の変更を念頭に設計されているので、ソフトウェアをローカルで変更する必要がありません。容量はすぐに増減でき、お客様の関与は最小限で済みます。



多くの企業は、安定したビジネス・サイクルに必要なデータセンターのスペースより

5 倍

多くのスペースを採用しています。[1]

▸ アナリストの見解を読む: ビジネス・データをクラウドに移行した場合の財務事例について

1 David Linthicum “Cloud Economics – Are You Getting the Bigger Picture?” *Cloud Technology Partners、2016 年 5 月*

IBM QRadar on Cloud の実世界の機能を利用する

クラウドベースのソフトウェアを使用すると、社内スタッフやコンサルタントから派生するスコーピング、プロビジョニング、テスト時間といった相当な額になりがちな、オンプレミス環境で要求されるインフラストラクチャー・コストを省くことができます。IBM QRadar on Cloud は、数千ものオンプレミスの QRadar 環境から得た経験を適用して、お客様の環境のニーズを満たします。これはクラウドでのジャンプスタートです。

QRadar on Cloud を導入することで、既に開発したモニタリング機能を維持または拡張することができる一方で、アナリストは脅威に関する情報データの理解により多くの時間をかけたり、スキルを既存アセットの保護に利用することができます。オンプレミスのセキュリティー・ソフトウェアを維持または微調整する必要はありません。自動ソフトウェアの更新とオンデマンドの拡張性により、QRadar on Cloud は予測可能な月次運用費を組織に提供できるので、IT セキュリティー・スタッフの作業が従来よりもシンプルになります。
QRadar on Cloud を導入すれば、必要な専門知識、パワー、拡張性を得ることができます。このシステムは、エンタープライズ級の分析を実行でき、次のような機能を備えています。

- Web ブラウザーのアクセス性
- データ収集、相関付け、およびレポート生成機能によって規制コンプライアンスを達成
- 大規模な Event Per Second (EPS) により、数百ものグローバルな場所にいるお客様のニーズに最大限に対処
- 可用性の高いシステム構成により、ほぼ継続的な可用性を実現
- IBM Security App Exchange を介したアプリ、アドオン、拡張機能
- X-Force Threat Intelligence が開発状況をフィード

セキュリティー・スタッフが提供できる以上の時間または専門知識が必要な場合は、オプションの追加管理サービスもご利用いただけます。

クラウド戦略を採用した企業は、採用しない企業に比べて支出を

22%

低減しています。[1]

▸ 動画を見る: QRadar on Cloud の詳細情報

1 “Buying Intentions Survey:Security,” *Nucleus Research*、2016 年 2 月

IBM が選ばれる理由

IBM Security ソリューションは、統合されたハードウェア、ソフトウェア、サービス製品でセキュリティーの脅威と脆弱性を防止、検知、対応できるように企業を支援します。詳細分析と信頼できる IBM Security の専門知識で支えられた IBM ポートフォリオの業界をリードするスケーラブルなツールは、幅広いセキュリティー情報を提供します。

QRadar セキュリティー情報インフラストラクチャーの購入、導入、管理のアウトソーシングを求めているあらゆる規模の組織のために、QRadar on Cloud は同じ基盤テクノロジーを使用して、ログ管理、ネットワーク・フロー分析、リアルタイムおよび履歴分析、脆弱性管理を実行します。このソリューションは IBM Cloud Data Center 内でホストされており、世界中で提供されています。国固有のデータ保管要件のある地域については、現在、米国 (テキサス州ダラス)、カナダ (オンタリオ州トロント)、EU (ドイルのフランクフルト)、ラテンアメリカ (ブラジルのサンパウロ) で QRadar on Cloud をご利用いただけます。その他の地域もサポート予定です。

さらに、QRadar On Cloud のオープン・フレームワークにより、IBM Security App Exchange に掲載されたソリューションとの統合が容易です。IBM Security App Exchange では、パートナー企業がアプリケーション、セキュリティー・アプリケーション拡張機能、IBM Security 製品の拡張機能を共有できます。QRadar on Cloud を使用するセキュリティー・チームは、既存のホスト契約を変更することなく (基本ライセンス条件を超えない限り)、セルフサービス・モデルを使い、必要に応じてソリューションをダウンロードし、インストールすることができます。

詳細情報

クラウド内の IBM QRadar Security Intelligence Platform の詳細については、日本 IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。**ibm.com**/software/products/en/qradar-on-cloud

IBM Security について

IBM Security は、企業セキュリティー製品とサービスの最先端且つ包括的ポートフォリオを提供します。世界中で高い評価を受けている IBM X-Force 研究がサポートするこのポートフォリオは、組織のインフラストラクチャー、データ、アプリケーションの包括的な保護を支援するセキュリティー情報を提供し、ID とアクセス管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、ネットワーク・セキュリティーなどのソリューションを実現します。

これらのソリューションにより、組織はリスクを効果的に管理できると共に、モバイル、クラウド、ソーシャル・メディア、他企業のビジネス・アーキテクチャーに対応する統合セキュリティーを実装できます。IBM は世界で最も幅広くセキュリティーの研究、開発、提供組織を運営しており、130 か国で一日当たり 150 億ものセキュリティー・イベントを監視し、3,000 以上のセキュリティー特許を保持しています。

また、IBM グローバル・ファイナンシングは多数の決済方法をご用意して、ビジネスの成長に必要なテクノロジーの購入をご支援しています。ご購入から廃棄まで、IT 製品とサービスの完全なライフサイクル管理を提供します。詳細については、次の Web サイトをご覧ください。**ibm.com**/financing

IBM

© Copyright IBM Corporation 2017

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2017

IBM、IBM ロゴ、ibm.com、QRadar、Sense Analytics Engine、および X-Force は、世界の多くの法域で登録されている International Business Machines Corp., の商標です。その他の製品名とサービス名は、IBM または他の企業の商標である場合があります。現時点での IBM の商標リストについては、次の Web サイトをご覧ください。www.ibm.com/legal/copytrade.shtml の「Copyright and trademark information」の項目をご覧ください。

本資料は最初の発行日の時点において最新の内容であり、IBM によって予告なしに変更される場合があります。掲載されている製品・サービスは IBM がビジネスを行っているすべての国・地域でご提供できるとは限りません。

顧客事例は、説明目的のみのために提示しております。実際の性能結果は特定の構成と動作条件によって異なる場合があります。

本資料の情報は「現状のまま」提供され、商品性、特定目的への適合性に対する保証、および非侵害の保証または条件を含め、いかなる明示的または黙示的な保証も行いません。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

適用されるすべての法令と規則の順守は、お客様の責任範囲とします。IBMは法律上の助言を提供することはいたしません。また、IBMのサービスまたは製品が、お客様がいかなる法規も遵守されていることの裏づけとなると表明するものでも、保証するものでもありません。

確実なセキュリティー体制への取り組みについて:IT システムのセキュリティーでは、社内外の不適切なアクセスの防止策、検出、対応に取り組むことで、システムと情報を保護しています。不適切なアクセスにより、情報が改ざん、破壊、不正流用、または悪用される可能性があり、システムへのダメージが生じたり、他者への攻撃のための使用など、システムの悪用が生じることがあります。IT システムまたは製品によってセキュリティー対策が万全になると考えることは危険であり、1 つの製品、サービスまたはセキュリティー対策で不正使用や不正アクセスを完全に有効に防ぐことはできません。IBM のシステム、製品、およびサービスは、合法的で包括的なセキュリティー・アプローチの一部として設計されています。そのため、運用手順を追加することがどうしても必要となり、効果を最大限に高めるには、他のシステム、製品、サービスが必要になることがあります。IBM は、システム、製品、またはサービス、あるいは貴社が、他者による悪意のある行為または不法行為を受けないことを保証するものではありません。

WGW03245-JPJA-01