Qualys

クラウドセキュリティ導入のための5ステップガイド

自信を持ってクラウドへの
取り組みを開始するために

目次

はじめに

クラウドの俊敏性とセキュリティへの確信――そのギャップを埋める

変革の途上にある組織のセキュリティ責任者が直面する極めて困難な課題の一つは、イノベーションのためにクラウドの俊敏性を活用することと、同時に強固なセキュリティ対策を確保すること、という二つの要請を両立させることです。4社に1社がクラウドやSaaS環境に関連するデータ侵害の被害に遭っているという最近の分析結果は、この取り組みを成功させることが急務であることを浮き彫りにしています。しかし、複雑なクラウド環境を適切に管理し、絶えず変化するこの環境の安全性を維持することは、クラウド特有の課題にまだ十分に通じていないセキュリティ専門家にとって、圧倒されるような難題に感じられるかもしれません。

本書は、クラウドの俊敏性とセキュリティへの確信を両立させるための5つのステップを提示するガイドです。クラウドセキュリティへの取り組みを始めたばかりのリーダーから、セキュリティ体制の強化を目指すリーダーまで、あらゆるリーダーが成功を収めるために必要な知見とツールを提供します。

この複雑なプロセスを、セキュリティリーダーが実践しやすい明確かつ管理可能なステップへと、以下のように体系化しています。

1. **責任共有モデル:** 自社が負うべき責任と、クラウドサービスプロバイダーが担う範囲を理解する。
2. **インベントリ管理と可視性の確保:** リソース、構成、アクセス権限を確実に把握する。
3. **最小権限の原則:** アクセス権を適切に制御し、セキュリティリスクを最小限に抑える。
4. **データ暗号化のベストプラクティス:** E機密データを確実に保護する。
5. **継続的なクラウド監視:** セキュリティの脅威をリアルタイムかつ能動的に検知し、対処する。

これらの実践的なステップを活用し、クラウドによるイノベーションとセキュリティの要件を両立させ、課題を戦略的な優位性へと転換する方法について見ていきましょう。

1 責任共有モデルを理解する

クラウドは「**責任共有モデル**」に基づいて運用されており、セキュリティに関する責任はクラウドプロバイダーと顧客の間で分担されています。この責任分担についての理解が不足していると、不必要なリスクを招く恐れがあります。

組織によっては、クラウドプロバイダーが実際よりも広範な範囲を管理していると思い込み、その結果、データ、アプリケーション、ワークロードが潜在的な脅威にさらされたままになってしまうことがあります。

知っておくべきこと

「責任共有モデル」は、クラウドサービスプロバイダー（CSP）と顧客との間におけるセキュリティ上の責任分担を明確にするものであり、双方がセキュアなクラウド環境の実現に向けて効果的に役割を果たすことを可能にします。

クラウドサービスプロバイダー（CSP）の責務

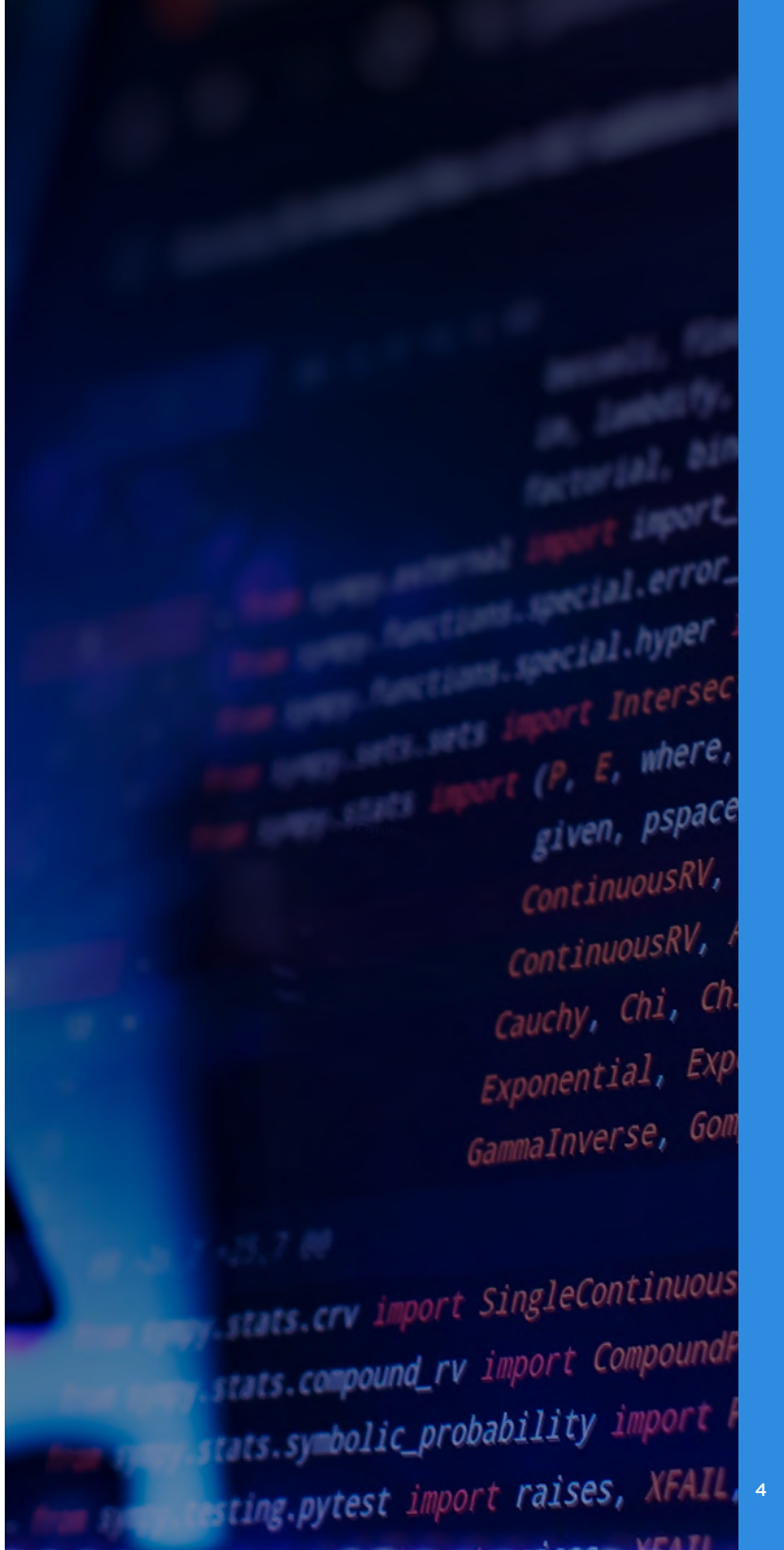
CSPは、クラウドの基盤となるインフラストラクチャを保護する責務を担っています。これには、物理的なデータセンター、ネットワークハードウェア、そしてクラウドサービスを支える仮想化レイヤーが含まれます。具体的には、物理施設の安全確保、ハードウェアの健全性維持、さらには潜在的な脅威に対して強固な耐性を持つ仮想化プラットフォームの維持・管理などが求められます。こうした取り組みを通じて、CSPは、顧客がアプリケーションやサービスを構築・展開するための、安全かつ堅牢なプラットフォームを提供しています。

クラウドにおけるお客様の責任

CSP（クラウドサービスプロバイダー）がインフラストラクチャを管理する一方で、クラウド環境に導入する要素のセキュリティを確保する責任はお客様にあります。これには、アプリケーション、データ、ユーザーアクセス制御、および設定などが含まれます。お客様には、アクセス権の適切な管理、クラウドサービスの安全な設定、そして不正アクセスや情報漏洩からのデータ保護を行う責任があります。

結論

クラウドセキュリティは共同の取り組みであり、安全なクラウド環境を構築するためには、自らの責任を理解し、それを受け入れることが重要です。



2 インベントリと可視性という重要な柱を優先する

クラウド環境において、アイデンティティは新たなセキュリティ境界となっています。攻撃者もこの変化を認識しており、そのため、盗用された認証情報は依然としてクラウド・セキュリティ・インシデントの最も一般的な侵入経路の一つであり続けています。こうした現状を踏まえ、組織はあらゆるアクセスポイントを積極的に保護し、検証済みかつ承認されたアイデンティティのみがクラウド・リソースにアクセスできるようにする必要があります。

AWS、Microsoft Azure、Google Cloud Platform (GCP)、Oracle Cloud Infrastructure (OCI) といったクラウド環境は、スピードと拡張性を重視して設計されていますが、その柔軟性ゆえに、全体像の把握が困難になることが少なくありません。数千ものサービスやIDが稼働する中で、組織は「何が動いているのか」「誰がアクセス権を持っているのか」「どこにリスクが潜んでいるのか」を把握しきれなくなってしまうのです。
だからこそ、クラウドセキュリティにおいて、インベントリ（資産）の把握と可視化は不可欠なのです。

知っておくべきこと

1. インベントリはすべての基本

主要なCSP（クラウドサービスプロバイダー）は、複数のリージョンやアカウントにわたり、数十、時には数百ものサービスを提供しています。統合されたインベントリがなければ、以下のような状況を正確に把握することはほぼ不可能です。

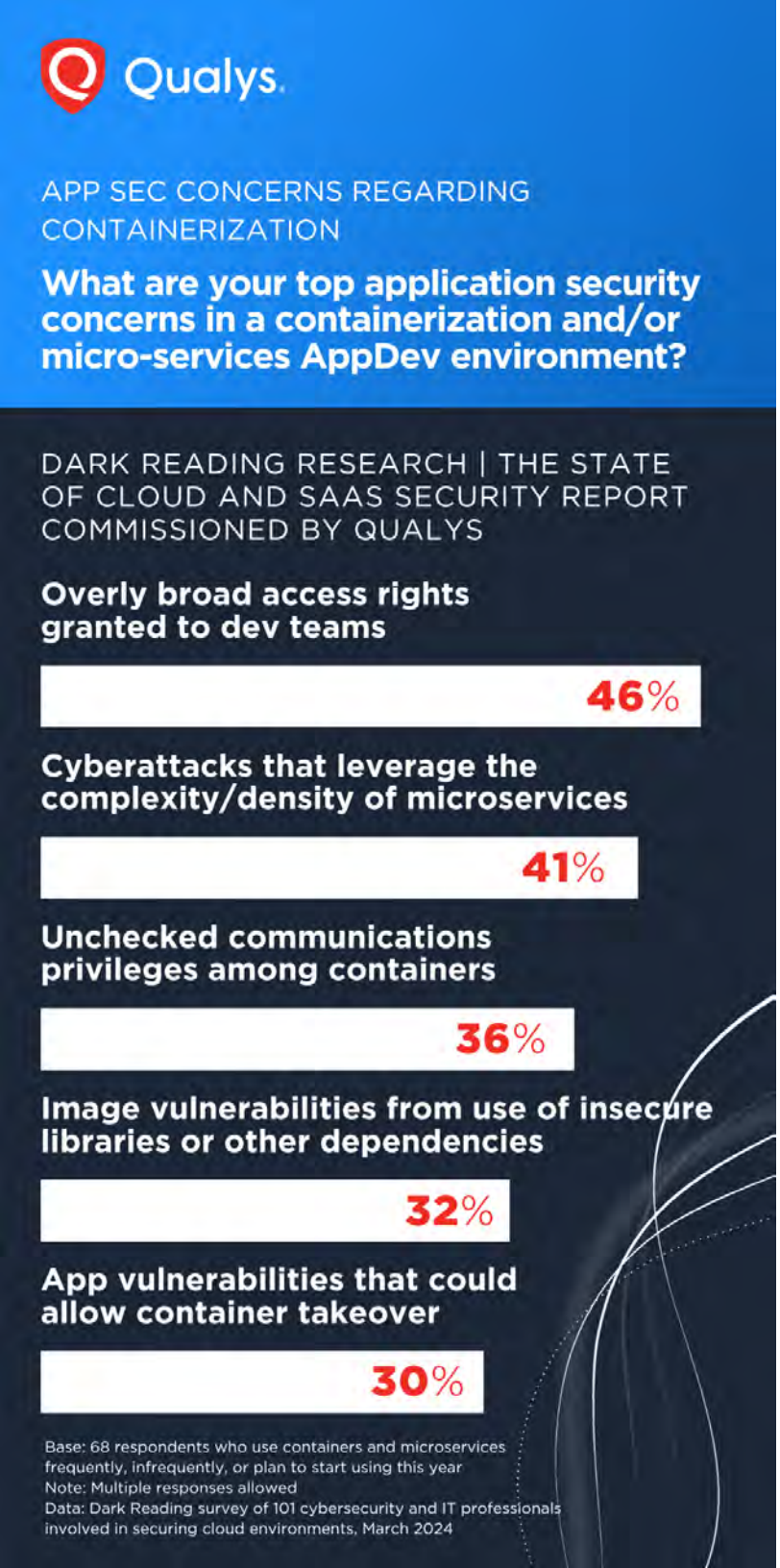
- どのようなEC2インスタンス（AWS）、Compute Engine VM（GCP）、Azure VM、あるいはOCIコンピュートシェイプが稼働しているか
- どのストレージバケット、ロードバランサー、APIがパブリックにアクセス可能になっているか
- 孤立したリソース（オーファンリソース）、タグ付けされていない資産、あるいはシャドー環境で稼働しているサービスが存在するかどうか

一元化されたクロスクラウドのインベントリは、セキュリティチームに「信頼できる唯一の情報源」を提供します。

2. IDの可視性は極めて重要

各CSP（クラウドサービスプロバイダー）は独自のIDシステムを採用しています（AWSのIAMロールやポリシー、GCPのIAMおよびサービスアカウント、Azure Active Directory、OCI IAMなど）。これらすべてにおいて、以下の点には「可視性」の確保が不可欠です。

- ユーザー、ロール、サービスアカウントを、それらがアクセス可能な特定のリソースと関連付けること
- 過剰な権限を付与したアクセス・ポリシーや、使用されていない権限を特定すること
- クラウドプロバイダー全体にわたり、「最小権限の原則」を実装・徹底すること



3. コンテナとKubernetesの可視性が重要

多くの企業は、Amazon EKS、Azure AKS、GKEといったサービスや、自己管理型クラスター上でコンテナワークロードを運用しています。そのため、以下の点を把握することが不可欠です。

- クラスター内部の状況（Pod、Service、Deploymentなど）
- S3、Pub/Sub、Azure Blob Storageなどのクラウドネイティブサービスとワークロードとの相互作用
- セキュリティグループ、Kubernetesネットワークポリシー、クラウドファイアウォールなどのツールを用いたネットワークの公開範囲とセグメンテーション

4. AIインフラストラクチャとワークロードの可視化が進展

AWS SageMaker、Azure Machine Learning、GCP Vertex AI、OCI Data Scienceなどのサービスを利用してAI/MLワークロードを導入する際、可視化の対象は以下にまで及ぶ必要があります。

- どのAIワークロードがGPUやその他の特殊なコンピュートリソースを消費しているか
- どのようなモデルが使用され、それらがどのように学習・提供（サービング）され、どのデータにアクセスしているか
- インフラストラクチャのプロビジョニング、モデルへのアクセス、コンプライアンスの追跡に関して、どのようなセキュリティ制御が適用されているか

結論

特にマルチクラウド環境において、インベントリと可視性は、クラウドセキュリティを支える重要な要素です。AWS、Azure、GCP、OCIのいずれを利用している場合でも、あるいはこれらを組み合わせて利用している場合でも、どのようなリソースが存在し、それらがどのように設定され、誰がアクセスできるのかを把握することが、環境を安全に保つための基盤となります。利用環境が複雑化するほど、リスクを低減し、大規模な環境で適切な制御を行うためには、リアルタイムかつコンテキストに富んだ可視性が不可欠となります。

コンテナやアプリケーションの可視性は不可欠です。それがなければ、こうした環境に新たに伴うリスクに対して、大きな死角が生じてしまいます。

3 最小権限の原則（PoLP）を遵守する

クラウドセキュリティにおいて、権限の付与は諸刃の剣です。権限が少なすぎれば、チームは不可欠な業務を遂行するのに支障をきたす恐れがあります。逆に権限が多すぎれば、攻撃者に悪用されかねない脆弱性を生み出すことになります。人間であれマシンであれ、過剰な権限を与えられたIDは、サイバー犯罪者を招き入れる格好の標的となってしまいます。

従来のアクセスモデルからの脱却

これまで多くの組織は、運用の利便性や従来の慣行を理由に、広範かつ過剰なアクセス権限に依存してきました。こうした時代遅れのモデルは、不要な脆弱性を生み出しています。過剰な権限を持つアカウントが侵害されると、攻撃者は組織のデジタルインフラ内を自由に移動できるようになり、サイバーインシデントによる被害が拡大する恐れがあります。

クラウドセキュリティにおける最も基本的な原則の一つである「**最小権限の原則（PoLP）**」を採用するには、静的かつ役割（ロール）ベースの権限設定から、変化するリスク指標に応じて継続的に調整される、きめ細かく動的に適用されるアクセス制御へと移行する必要があります。

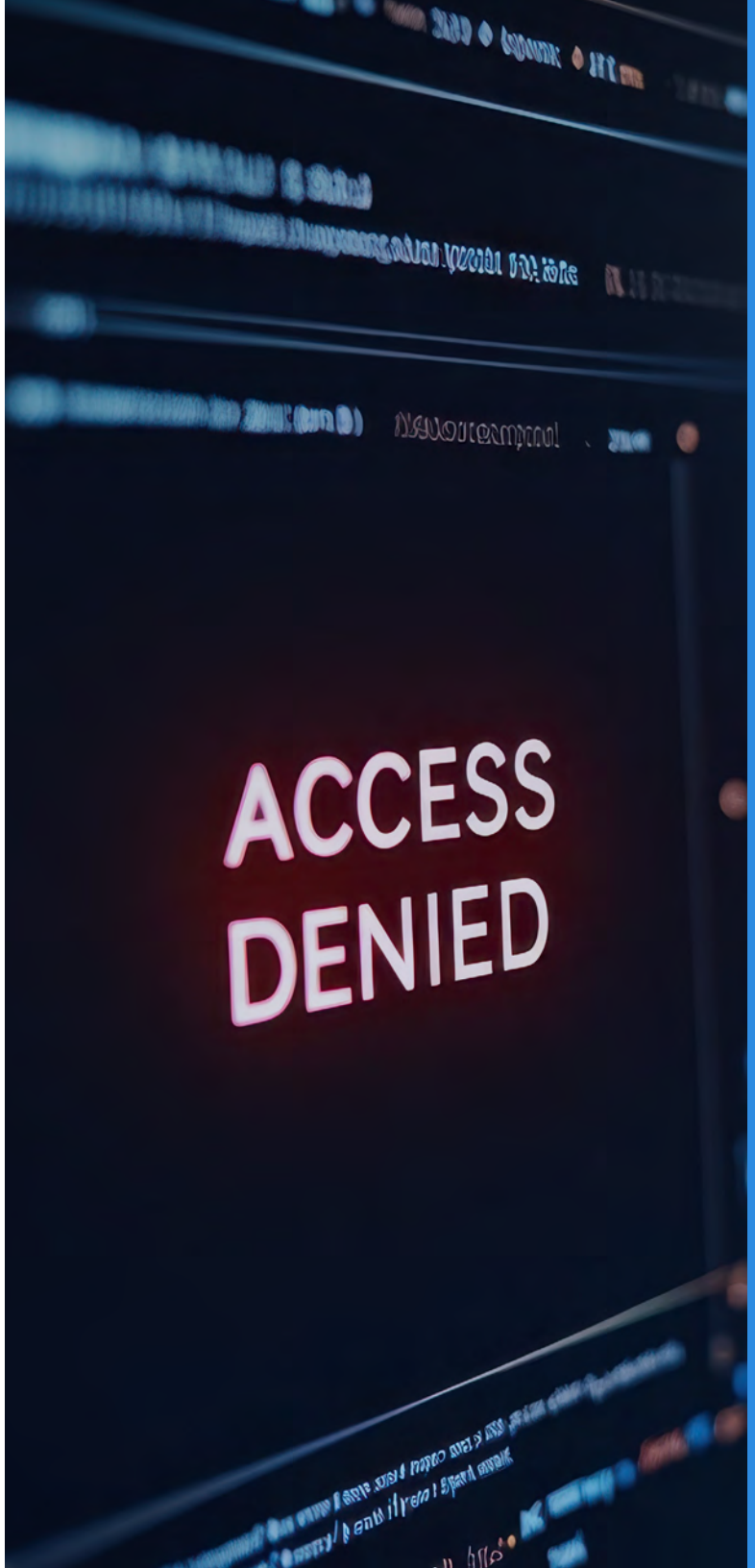
知っておくべきこと

「**最小権限の原則（PoLP）**」は、ユーザー、アプリケーション、およびサービスに対し、それぞれの役割を遂行するために必要な最小限のアクセス権限のみを付与することを保証する、セキュリティの基本原則です。クラウドセキュリティを強化するために、組織がどのようにPoLPを効果的に導入・運用できるかを見ていきましょう。

クラウド環境における「最小権限の原則」を導入するための重要なステップ

1. きめ細かな制御を伴う明確なアクセス・ポリシーを策定する: アクセス権は、「業務上知る必要性（need-to-know）」および「業務上使用する必要性（need-to-use）」に基づいて付与されるべきです。役割ベースのアクセス制御（RBAC）を導入し、職務内容に応じて権限を割り当てます。また、必要な時にのみ一時的に権限を付与し、一定期間経過後に取り消す「Just-in-Time（JIT）アクセス」の利用も検討してください。

2. 包括的な管理者権限の付与を避ける: セキュリティ上の最も一般的な落とし穴の一つは、必要のないユーザーに過剰な管理者権限を与えてしまうことです。その代わりに、限られた担当者のみに高い権限を付与する、段階的なアクセス管理のアプローチを採用してください。



3. 強固な認証と「最小権限」の原則に基づくサービスアカウントの運用: アクセス制御を必要とするのは人間だけではありません。サービスアカウント、API、ワークロードも「最小権限」のモデルに従う必要があります。クラウドのリソースには固有かつ最小限の権限を持つIDを割り当て、多要素認証（MFA）を強制することで、不正アクセスを防止してください。

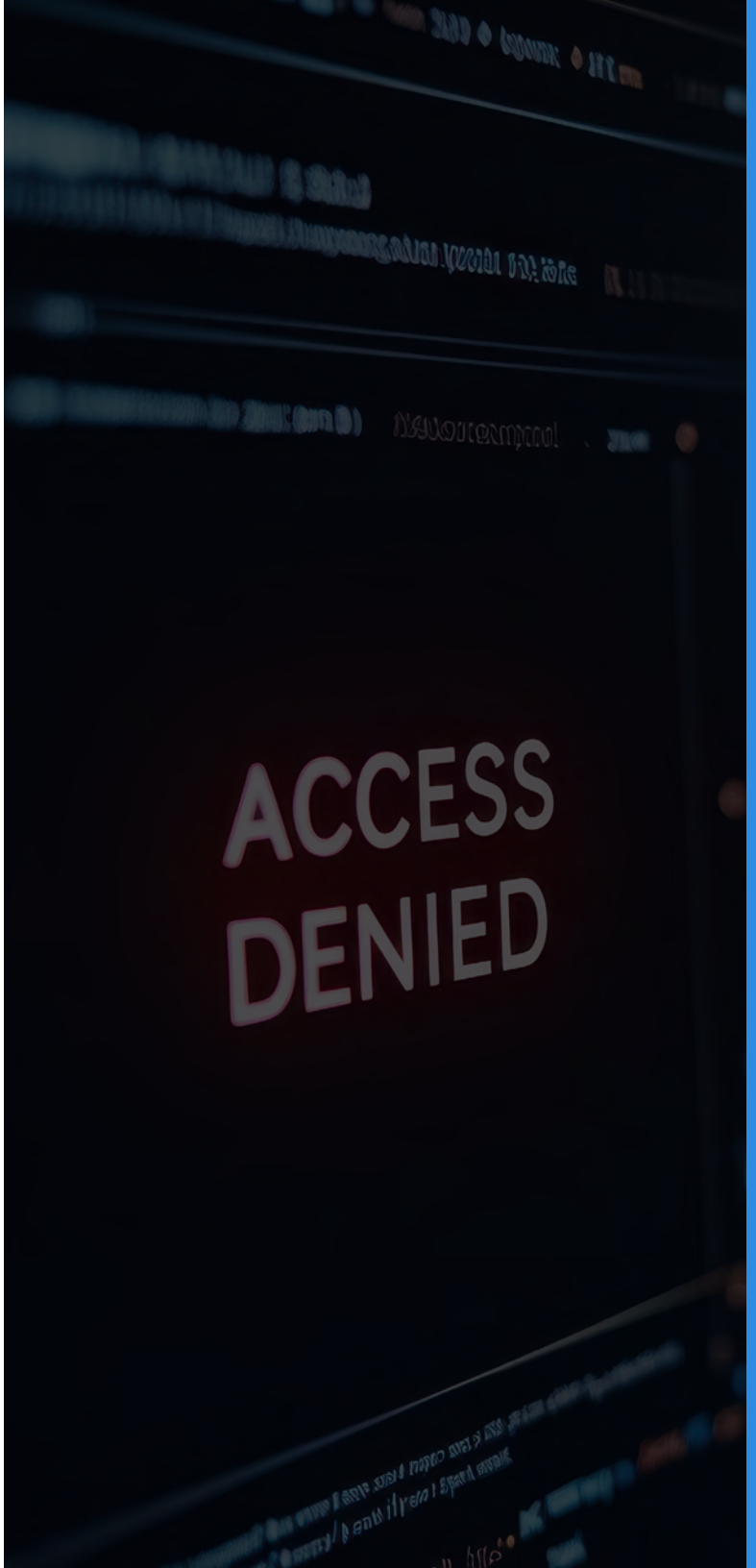
4. 定期的な監査と権限の見直し: 時間の経過とともに、ユーザーやサービスアカウントには不要になった権限が蓄積されることがあります。定期的にアクセス権限を見直し、使用されていない権限（オーファン権限）や過剰な権限を特定して取り消してください。CIEM（Cloud Infrastructure Entitlement Management：クラウドインフラ権限管理）などの自動化ツールを活用すれば、リスクのある権限割り当てを検出し、アクセスガバナンスを効率化できます。

5. 権限昇格の試行に対する監視と対応: 不審な権限昇格を検知するために、継続的な監視を導入してください。ユーザーが通常の行動パターンから逸脱し、突然重要なリソースへのアクセスを要求した場合には、自動化された対応策を講じて、潜在的な侵害を未然に防ぐようにします。

結論

設定ミスや過剰な権限を持つアカウントが主要な脅威となっているクラウドセキュリティの現状において、「最小権限の原則（PoLP）」の遵守は単なる選択肢ではなく、不可欠な要件です。

PoLPを導入し、継続的に改善していく組織は、進化し続けるサイバー脅威から自社のデジタル資産を保護する能力を大幅に高めることができるでしょう。



4 暗号化で機密性の高いクラウドデータを保護する

暗号化はクラウドセキュリティの根幹を成すものであり、機密データを不正アクセス、盗難、改ざんから確実に保護します。クラウドストレージに保存されているデータ（保存データ）であれ、転送中のデータであれ、暗号化は機密性と完全性を守るために不可欠なセキュリティ層を提供します。

クラウドにおける暗号化の重要性

クラウド環境は、その分散型構造、マルチテナンシー、リモートアクセスの容易さといった特性ゆえに、特有のセキュリティ課題を抱えています。設定ミスや内部関係者による脅威、あるいは高度なサイバー攻撃によって、機密データが権限のない第三者に流出する恐れがあります。暗号化は、適切な暗号鍵がなければデータを読み取り不可能な状態にすることで、こうしたリスクを低減し、攻撃者にとって無価値なものにします。

さらに、GDPR、HIPAA、PCI DSSといったコンプライアンスや規制要件においても、機密データの暗号化が義務付けられています。

知っておくべきこと

多くのクラウドプロバイダーは、組み込みの暗号化機能を提供しています。以下に一般的な概要を記載しますが、利用するクラウドプロバイダーが提供する具体的な暗号化機能について理解しておくことが重要です。

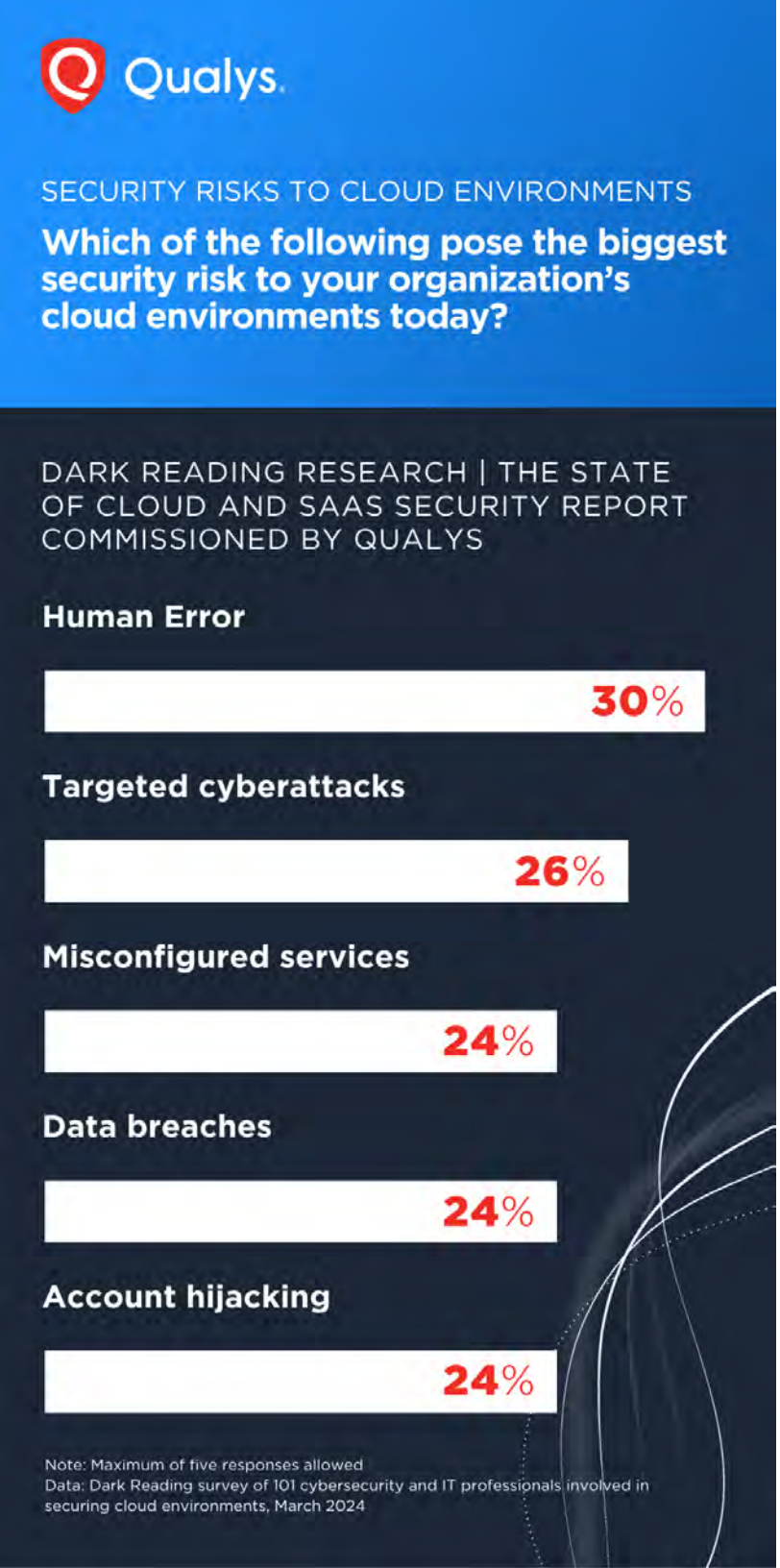
保存データの暗号化

「保存データ（Data at Rest）」とは、クラウド上のデータベース、ファイルシステム、オブジェクトストレージ、またはバックアップアーカイブなどに格納されているデータを指します。保存データを暗号化することで、攻撃者がクラウドストレージにアクセスした場合でも、復号キーがなければ情報を読み取ることができなくなります。

クラウドプロバイダーは通常、保存データの暗号化として、主に以下の2つの方式を提供しています。

1. **サーバーサイド暗号化（SSE）**：この方式では、クラウドプロバイダーがデータの保存前に自動的に暗号化を行い、データの取得時に復号を行います。

2. **クライアントサイド暗号化**: SSEとは異なり、クライアントサイド暗号化では、クラウドへアップロードする前にローカル環境でデータを暗号化します。この方式は暗号化プロセスをより詳細に制御できるほか、万が一クラウドプロバイダーのセキュリティが侵害された場合でもデータは暗号化されたまま維持されるため、セキュリティの層をさらに強化できます。ただし、暗号化キーを組織側で安全に保管・管理する必要があります。



転送中のデータの暗号化

「転送中のデータ（Data in transit）」とは、クラウドアプリケーション間、クラウドストレージ、あるいはクラウドサービスにアクセスするエンドユーザー間など、ネットワーク上を移動している最中の情報を指します。転送中のデータを暗号化することで、データの傍受や中間者攻撃を防ぎ、データの機密性と完全性を確保します。主な対策は以下の通りです。

- **セキュアなプロトコルの使用**: HTTPS、SSL/TLS、セキュアなVPNなどを導入して通信経路を暗号化し、不正な傍受を防止します。
- **エンドツーエンド暗号化（E2EE）**: 送信前にデータを暗号化し、最終的な宛先に到達した時点でのみ復号を行う方式です。これにより、サービスプロバイダーであってもデータにアクセスできない状態が保たれます。

暗号化キー管理のベストプラクティス

暗号化の強度は、その暗号化キーのセキュリティに依存します。強固な暗号化セキュリティを維持するためには、以下の点に留意してください。

- **適切な鍵管理システム（KMS）の選択**: クラウドプロバイダーが提供する、鍵の生成・保管・ローテーションを自動化する組み込み型KMSを利用するか、あるいは自前で管理するかを選択します。
- **鍵の定期的なローテーションと廃棄**: 鍵を定期的にローテーションすることで、万が一侵害された場合でも、鍵が長期間にわたって危険にさらされるのを防ぎます。
- **鍵の安全な生成と保管**: 鍵生成プロセスの安全性を確保し、暗号化鍵を安全な場所に保管してください。

結論

暗号化はクラウドセキュリティの極めて重要な要素であり、機密データを不正アクセスから保護し、規制要件への準拠を確保する役割を果たします。保存データと転送中のデータの双方に暗号化を適用することで、組織はデジタル資産の管理を維持しつつ、セキュリティリスクを大幅に低減できます。

データ侵害は主要なリスクの一つであり、人的ミスがデータ流出につながるケースも少なくありません。暗号化は、こうしたリスクへの対策として有効です。

5 クラウド環境での継続的な監視を有効にする

企業によるクラウド導入が加速する中、セキュリティ責任者は根本的な課題に直面しています。それは、動的かつ分散型の環境において、いかにして可視性を維持するかという点です。
先進的な企業は、クラウド上のアクティビティをリアルタイムで可視化することが、規制への準拠に不可欠であるだけでなく、競争上の差別化要因にもなることを認識しています。これにより、対応の迅速化や運用の俊敏性向上が実現し、進化し続けるサイバー脅威に対するレジリエンス（回復力）が強化されます。

「可視化」から「アクション」へ: インテリジェントなクラウド監視の台頭

極めて動的な今日のクラウド環境において、可視化とは単にどのような資産が存在するかを把握することではありません。それは、リスクを予測し、的確に対処することを意味します。静的なダッシュボードや定期的な監査では、現代のクラウド運用が持つスピードや複雑さには太刀打ちできません。ワークロードがわずか数分で立ち上げられ、変更され、廃棄されるというクラウド特有の「一時性」は、受動的な監視から、インテリジェントかつリアルタイムなセキュリティの可視化へと、根本的な転換を求めています。

知っておくべきこと

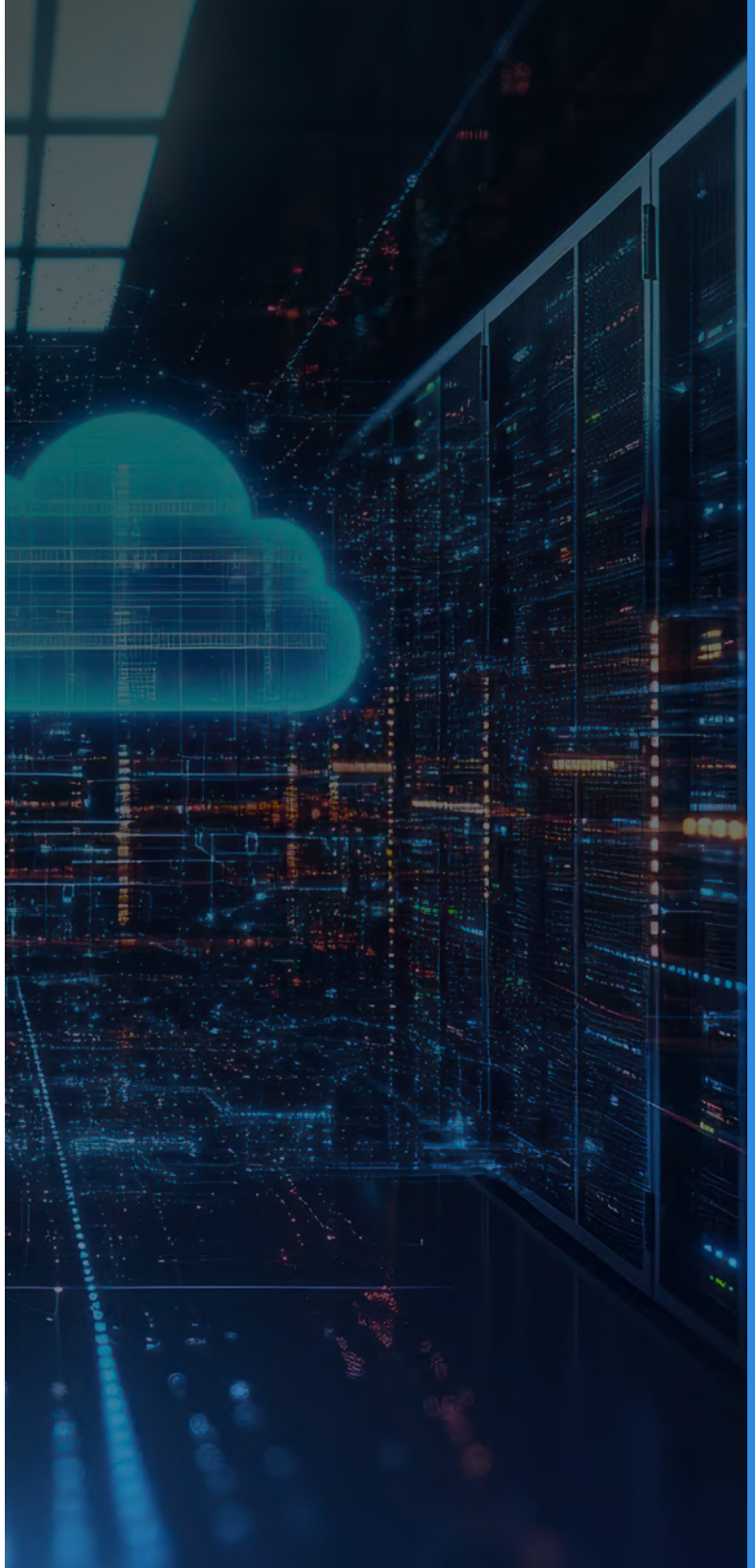
強固なクラウドセキュリティポスチャーは、クラウド上のアクティビティをリアルタイムで可視化する、堅牢な監視およびログ記録ソリューションから始まります。継続的な監視を行うことで、組織は異常なパターンや予期せぬ挙動、不審な動きを、本格的なセキュリティインシデントへと拡大する前に検知することが可能になります。

効果的な監視戦略の重要な要素は以下の通りです。

1. 重要イベントのログ記録 – クラウド環境におけるすべての重要なアクションを記録する必要があります。これには以下が含まれます。

- ユーザー認証およびログインの試行
- API呼び出しおよび管理者による変更
- ネットワークトラフィックおよびデータ転送
- セキュリティ設定の変更

これらのログは、クラウドエコシステム内で発生したイベントの記録として機能し、セキュリティチームがインシデントの経緯を再構築したり、異常を検知したりする際に役立ちます。



2. ログの一元管理 – 複数のクラウドサービスやプラットフォームにまたがるログの管理は、複雑になりがちです。**ログの一元管理ソリューション**は、さまざまなソースからのログを集約し、セキュリティチームが効率的にデータを分析できる単一の統合ビューを提供します。ログ管理ツールを導入することで、組織はクラウドインフラ全体にわたるイベントを関連付けて分析できるようになり、脅威の検知能力を向上させることができます。.

3. 異常検知とアラート通知 – 単にログを収集するだけでは不十分です。組織は**高度な分析や機械学習**を活用し、異常なパターンや潜在的なセキュリティインシデントを特定する必要があります。

例:

- 通常とは異なる地理的場所からのログイン試行の失敗が繰り返される場合、ブルートフォース攻撃の可能性があります。
- 送信トラフィックの急激な増加は、データの外部流出を示唆している可能性があります。
- セキュリティグループ設定への不正な変更は、アカウントが侵害されたことを示唆している可能性があります。

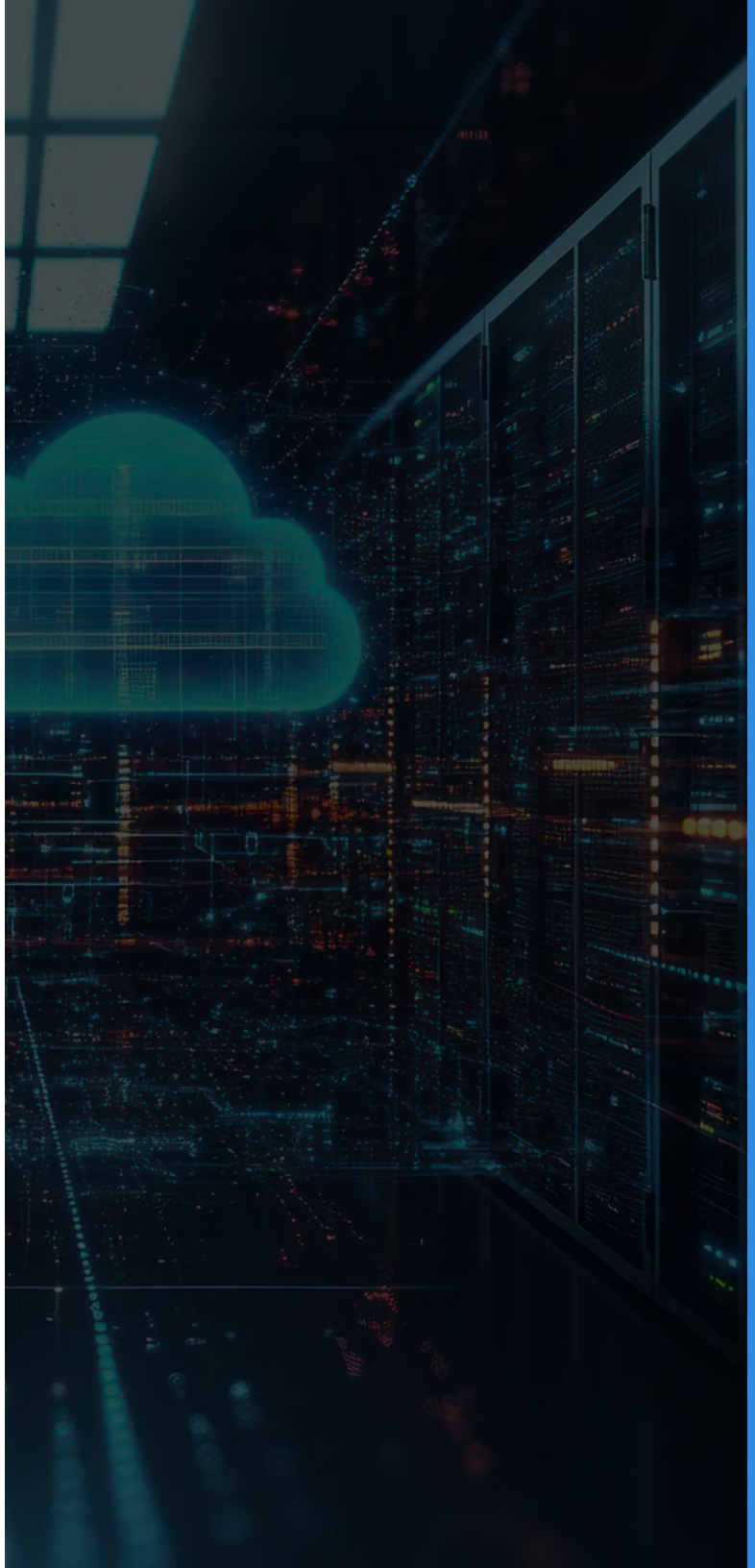
重要なイベントに対する**アラートや通知**を設定しておくことで、セキュリティチームは不審なアクティビティを迅速に調査できるようになり、対応時間の短縮と影響の最小化が可能になります。

クラウドの可視化による規制コンプライアンスの確保

脅威の検知にとどまらず、クラウドの可視性を維持することは、規制や業界のコンプライアンス要件を満たす上で極めて重要です。**HIPAA、PCI DSS、GDPR、NIST、CIS**といった規制ガイドラインはいずれも、ログの記録、監視、および監査証跡の維持の重要性を強調しています。

結論

流動的なクラウド環境を継続的に監視することは、規制要件への適合や業界のベストプラクティスの遵守において不可欠であるだけでなく、より大きな脅威の予兆となり得る異常な活動を迅速に特定し、攻撃者の一歩先を行くためにも極めて重要です。



Qualys, Inc. (NASDAQ: QLYS) is a leading provider of disruptive cloud-based security, compliance and IT solutions helping organizations measure, communicate and eliminate cyber risk. Over 10,000 subscription customers worldwide, including most of the Forbes Global 100 and Fortune 100, utilize the Qualys Enterprise TruRisk Platform.

This platform enables companies to streamline and automate their security and compliance processes into a single, comprehensive view, resulting in increased agility, improved business outcomes, and significant cost savings.

 V250505

おわりに

強靭なクラウドセキュリティ戦略の基盤

今日のクラウドアーキテクチャは動的であり、ワークロードは急速に拡張し、脅威アクターは絶えず戦術を高度化させています。ここで示した5つの重要なステップを実践し、主体的にセキュリティを管理する組織は、デジタルファーストの経済環境において成功を収める体制を整えることができます。これを実現するには、セキュリティをクラウド運用の根幹に組み込む必要があります。そうすることで、企業は保護を犠牲にすることなく、イノベーションを加速させることが可能になります。

重要なポイント:

- **責任共有モデルの理解**: クラウドプロバイダーが保護する範囲と、自社が責任を負う範囲を把握する。
- **インベントリと可視性の確保**: どのようなリソースが存在し、どのように構成され、誰がアクセスできるかを確実に把握する。
- **最小権限の原則の適用**: 権限を制限し、攻撃対象領域を最小限に抑える。
- **適切なデータ暗号化**: 強力な暗号化と鍵管理によって機密情報を保護する。
- **継続的な監視**: 自動化されたセキュリティツールを活用し、脅威をリアルタイムで検知・対応する。

クラウドセキュリティの成熟に向けた取り組みは、現在進行形で続いています。適切なツール、プロセス、そして専門知識があれば、組織は複雑な状況を確実に乗りこなし、リスクを低減し、クラウド技術の可能性を最大限に引き出すことができます。今こそクラウドセキュリティ戦略を高度化させましょう。サイバーセキュリティにおいて、常に一歩先を行くことこそが、安全を確保する唯一の道だからです。

Qualysは、リスクの可視化、優先順位付け、および修復を大規模かつ自動化することで、これら5つの重要なステップを「クラウド・レジリエンス（回復力）」へと高め、お客様のマルチクラウド戦略を強力に支援します。

詳しくはこちらをご覧ください。

こちらからご確認ください。