CROWDSTRIKE

主要なクラウド攻撃テクニック

それらをどう防御するのか

クラウドは拡大と進化を続ける攻撃対象領域です。この環境を増加の一途をたどるクラウド攻撃から防御するためには、脅威アクターの活動に関する詳細な知識が必要となります。このインフォグラフィックでは、クラウドストライクによって観察されたクラウドの攻撃トレンドの上位 3 つとその防御方法をご紹介します。

脅威アクターはより頻繁にクラウドを標的にしています

クラウド環境は拡大を続けています：

41.4%
クラウドベースのサービスや製品の使用が増加していると回答したグローバルトップ企業の割合[1]

33.4%
レガシーエンタープライズソフトウェアをクラウドベースのツールに移行することを計画している割合[1]

32.8%
オンプレミスのワークロードをクラウドに移行している割合[1]

そして、脅威アクターも注目しています。

2022年、クラウドストライクは以下のことを観察しました：

95%
クラウドエクスプロイトケースの増加割合

3倍
クラウドを意識した脅威アクターが関与したケース数

71%
マルウェアフリーの攻撃の割合

クラウド環境を標的にする理由とは？

マルチクラウド環境は複雑であるため、
保護がより困難

迅速なソフトウェア配信プロセスにより、クラウドネイティブなアプリケーションは
脆弱性や設定ミスの影響を受けやすい

ローグクラウドやシャドークラウド環境には
セキュリティ制御と監視が欠けている

サイロ化されたセキュリティポイント製品は
攻撃者が気付かれずにすり抜けられる死角を残す

脅威アクターはクラウドに精通しており、クラウドサービスを悪用し、クラウドの脆弱性を悪用するための戦術を改善し続けています。CrowdStrike Intelligence が昨年、200 以上の脅威アクターを追跡することで観察した上位 3 つのクラウド攻撃手法は次のとおりです。

IT インフラストラクチャ間のラテラルムーブメント

脅威アクターは、従来のエンドポイントを活用してクラウドインフラストラクチャに軸足を移すことが増えています。そして、その逆も同様で、クラウドインフラストラクチャは、エンドポイントにアクセスするためのゲートウェイとして使用されています。しかし、組織が、この活動を停止するために必要な可視性を備えていることはほとんどありません。オンプレミス環境に対処するため、そして最近ではクラウド環境に対処するために、多数の個別のソリューションを導入しているのが理由です。

ラテラルムーブメントを阻止するには、オンプレミスとクラウド両方のITインフラストラクチャ全体を完全に可視化する必要があります。

侵害につながるクラウドの設定ミス

クラウドストライクは、クラウドセキュリティ設定が正しく設定されていれば、早期に検知または防止できた可能性のあるクラウド侵害を調査することが多々あります。設定ミスは、単に侵害のリスクを高めるだけでなく、組織がクラウドインフラストラクチャを拡張するにつれて、ますます蔓延し、問題になります。

No. 1
クラウド環境で発生する脆弱性の第1位は設定ミス

60%
クラウドストライクが観察したコンテナのうちセキュリティ保護が適切に設定されていなかったものの割合

36%
クラウドサービスプロバイダーの安全とは言えないデフォルト設定を使用していたクラウド環境の割合

新しい境界としてのクラウドアイデンティティ

新しい境界であるアイデンティティは王国への鍵となっています。脅威アクターは、アンチウイルスやファイアウォールテクノロジーの無効化ではなく、認証プロセスの変更とアイデンティティの攻撃に重点を置いています。クラウドベースのアプリケーションとサービスの継続的な採用により、攻撃者が標的として都合よく悪用できるアイデンティティの数も増加しています。

クラウド侵入の43%
で、初期アクセスの獲得に正規のユーザーアカウントが使用されました

47%のクラウドの重大な設定ミスは
アイデンティティと権限のハイジーンの不備に関連しています

67%のクラウドセキュリティインシデントで
クラウドストライクはアイデンティティ/アクセス管理（IAM）ロールが必要以上に権限昇格されていたことを発見しました。これは攻撃者が環境に侵入してラテラルムーブメントを行うためにロールを変更した可能性があることを示しています

クラウドセキュリティのためのクラウドストライク

クラウド環境が増加し続けるにつれて、クラウドを標的にする攻撃も増加しています。脅威アクターが使用する進化を続ける TTP（攻撃手口）を理解することは言うまでもなく、クラウドの脆弱性、設定ミス、ユーザーエラーをすべて把握することは不可能です。組織はそれを単独で行うことはできません—脅威アクターの行動とクラウドに関する豊富な知識を持つパートナーが必要です。

クラウドストライクは、世界一のエージェントベースのエンドポイントでの検知と対応プロバイダーとして、単一のプラットフォームで簡単に展開および管理できるスケーラブルで効果的なクラウドセキュリティを設計するための先進的アプローチを採用しています。CrowdStrike Falcon® Cloud Security は、エージェントレスとエージェントベースの両方の保護を提供するためにゼロから構築されました。組織はこれをオンにするだけで、エンドポイントからクラウドに保護を拡張し、シームレスで統合されたエージェントレスおよびエージェントベースの保護で IT インフラストラクチャ全体をカバーできます。Falcon Cloud Security は、クラウドセキュリティポスチャ管理、クラウドワークロード保護、クラウドアイデンティティの権限管理を完全に統合したクラウドネイティブアプリケーション保護プラットフォーム（CNAPP）製品として提供します。

ホワイトペーパー「クラウド防御のためのインサイダーズガイド」をダウンロード

詳細情報 →

CrowdStrike について

CrowdStrike (Nasdaq: CRWD), は、サイバーセキュリティのグローバルリーダーであり、エンドポイント、クラウドワークロード、アイデンティティ、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームにより、現代のセキュリティを再定義しています。

CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud およびワールドクラスの AI を搭載し、リアルタイムの攻撃指標、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリーを活用して、超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けられた脆弱性の可観測性を提供します。

Falcon プラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンスを提供し、複雑さを低減し即座に価値を実現します。

CrowdStrike: We stop breaches

フォローしてください：

CROWDSTRIKE

---

[1] https://cloud.google.com/blog/transform/top-cloud-computing-trends-facts-statistics-2023