クラウド・セキュリティ・ソリューション・プロバイダーに関して確認すべき事項**トップ 10**

クラウド・セキュリティ・プロバイダーを見つける作業はとても面倒です。一見しただけではプロバイダーの違いはわからず、どこも同じような数値や機能を宣伝しています。正確に比較するために必要な情報を得るには、クラウド・サービス・ベンダーに質問し、必ずしも自主的に提供するわけではないクラウドサービスの詳細を確認する必要があります。

以下のリストを、組織を悪意あるサーバー攻撃から保護してくれる最適なクラウド・セキュリティ・プロバイダーを選択するために必要な項目を確認するための資料としてお役立てください。

1. **経験：**そのプロバイダーはクラウド・セキュリティ・ビジネスにどれくらいの期間、携わっていますか？そのプロバイダーは、現在、世界で何社のクラウドセキュリティの顧客を擁していますか？（グローバルな攻撃ベクトルに関する有用な知見があります。）お望みの方法でビジネスをサポートしてくれますか？

2. **容量と規模：**クラウド・セキュリティ・ベンダーの多くは、十分な規模があることを示唆しますが、重要なのは規模の測定方法です。プロバイダーが必要に応じて、規模を拡大できるかどうかを確認する必要があります。次のように質問してみましょう。実際には、最大でどれくらいの規模の分散型サービス拒否（DDoS）攻撃に対応できますか？プロバイダーは自社ネットワークに対する実際の攻撃を例に対処方法を示すことが出来ますか？

3. **パフォーマンス、分散、可用性：**そのプロバイダーは、データ主導アルゴリズムと自動化によってサポートされたグローバルなサーバーネットワークを擁する、完全統合型のクラウド・セキュリティ・ソリューションを提供していますか？貴社では、DDoS スクラビング、CDN ネットワーク、またはその両方を選べますか？

4. **コレクティブインテリジェンス：**そのクラウド・セキュリティ・プロバイダーは、意味のあるインテリジェンスを生み出せるだけの、大規模かつグローバルなトラフィック量を処理していますか？攻撃を受けたとき、あるいは攻撃を受ける前に、蓄積した専門性を活用して、カスタマーベース全体にメリットをもたらす準備はできていますか？包括的なビッグデータ分析エンジンを使用して、他のクライアントに影響を及ぼす可能性のある単独の攻撃者を特定できますか？

5. **IP レピュテーション：**そのクラウド・セキュリティ・プロバイダーは、IP アドレスにレピュテーションスコアを割り当てるために、どんなソースを使用していますか？ IP レピュテーション製品は、品質レベルに幅があり、経時的な悪意あるアクティビティに基づいてスコアを出すのではなく、バイナリ・リスク・スコア（攻撃者か、そうでないか）を使用するものもあります。

6. **正確度：**異なる Web Application Firewall（WAF）の正確度の判定は簡単ではありません。ベンダー 2 社の正確度を比較する場合、同じテストを行わない限り意味はありません。テスト内容、テスト対象となったプロバイダー、最終結果が何件のテストに基づいているかについて確認しましょう。常に同一条件で比較しましょう。

7. **継続的な改善：**正確度を向上させるには、日々進化するトラフィックに合わせて、ルールを定期的に調整することが重要です。クラウド・セキュリティ・ベンダーは、セキュリティインフラストラクチャをどれくらいの頻度でテストしていますか？毎月、毎週、それとも毎日ですか？どれくらいのトラフィックでテストしますか？

8. **緩和所要時間：**クラウド・セキュリティ・プロバイダーのサービスレベル契約（SLA）は、緩和のスピードや品質についてもコミットしていますか、あるいは応答時間のみですか？ほとんどのベンダーは数分以内での応答を保証しますが、調査するだけの場合もあります。具体的で、契約として保証された緩和 SLA は、保護レベルを正確に比較するための明確な基準となります。

9. **人的要因（セキュリティ・オペレーション・センター／ SOC）：**ほとんどのベンダーが、週 7 日／ 24 時間体制の SOC による保護を打ち出しています。ただし、そのクラウド・セキュリティ・ベンダーが保有する設備の数、設備の場所、配備される人員数を確認することが重要です。一度に何名の人員を動員できますか？攻撃を受けている最中にシフト交代が行われても対応できるようにするために、どのようなプロトコルを使用していますか？

10. **マルチレイヤー型防御／多層防御：**単独のセキュリティソリューションですべての脅威を防ぐことは不可能です。ただし、併用しているツールが、同様の基本テクノロジーやハードウェアに基づいて構築されている場合、各層に同じ弱点が存在することとなり、攻撃者にその弱点を突かれてしまう可能性があります。最良のアプローチは、複数の高水準のテクノロジーを相互に積み重ねた層を形成することです。

インターネットセキュリティを確保するために、クラウドを利用する組織は増えつつあります。クラウドベースのセキュリティは、オンプレミスのソリューションのみに比べて、より大規模で、より正確で、より優れたパフォーマンスを企業に提供します。既存のセキュリティインフラストラクチャとも問題なく連携するクラウド・セキュリティ・ソリューションを選ぶには、プロバイダーが提供するサービスのを、確実に把握する必要があります。

詳しくは Akamai の無料 e ブック「なぜクラウドか？クラウド・セキュリティ・バイヤーズ・ガイド（Why Cloud The Buyer's Guide to Cloud Security）」をご覧ください。