クラウド・コンピューティングで セキュリティ機能をサポートする 6 つの方法

クラウド・コンピューティングを取り入れるには、クラウド環境の使用によるコスト効率、スケーラビリティ、利便性と、データとアプリケーションを自前のサーバー上で安全にホストし続ける安心感の、どちらかをとるか決める必要があります。しかし、オンプレミスはクラウド・コンピューティングよりも本当に安全なのでしょうか。多くのエキスパートがそうではないと考えています。以下は、クラウド・コンピューティングに安心して移行できることを示す 6 つの要因です。

1 セキュリティは高価

セキュリティにはコストがかかります。自社の現実的なセキュリティ予算の規模を考えてみましょう。オンプレミス・データセンターに必要なセキュリティをデプロイするには極めて高いコストがかかり、特に中小規模の企業にとっては厳しい額に上ります。ハイパースケーラーが顧客に提供するものに近いレベルのセキュリティを達成するのは、現実的ではありません。

2 セキュリティには 多大な人的リソースが必要

同様に、セキュリティには人的リソースの増員も必要となります。大規模なクラウドプロバイダーは年中無休のチーム体制と完全なセキュリティ運用センターを導入し、IT インフラストラクチャと物理的なハードウェアを継続的に監視しています。たとえば Microsoft Azure は、3,500 名を超えるサイバーセキュリティのエキスパートのチームによって保護されています。ほとんどの組織では、ハイパースケーラーと同レベルのセキュリティを提供できるスタッフ数を備えていません。

3 クラウドプロバイダーの重点は セキュリティビジネス

セキュリティは確かに重要です。しかし貴社の本業ではありません。貴社にとってセキュリティは多くの懸念事項の 1 つですが、クラウドプロバイダーにとっては最優先事項の 1 つです。クラウドプロバイダーがビジネスを継続し、競争力を維持するには、可能な限り最高レベルのセキュリティを顧客に提供しなければなりません。たとえば Google Cloud は組み込みの保護と暗号化をデフォルトで搭載した「セキュアバイデザイン・インフラストラクチャ」を提供しています。[1]

また Microsoft Azure は、Microsoft Intelligent Security Graph の一環として「180 億件の Bing Web ページ、4,000 億件のメール、10 億件の Windows デバイスの更新、毎月 4,500 億件の認証など、幅広いソースを分析」することで脅威の特定に役立てています。[2]

また、クラウドプロバイダーは、さまざまな厳格なプログラムを通じて、セキュリティに関わる人、プロセス、テクノロジーに対する国際的に認知された独立した認定や監査など、最高レベルの基準に準拠しなくてはなりません。 たとえば Amazon Web Services (AWS) は、数千ものグローバル・コンプライアンス要件に対するサードパーティ検証を定期的に達成しています。ほとんどの組織には、このレベルのセキュリティ保証を満たすための時間、リソース、予算がありません。[3]

1 「信頼とセキュリティ」、Google、2022 年 4 月にアクセス。
2 「Azure でセキュリティ体制を強化」、Azure、2022 年 4 月 29 日にアクセス。
3 「AWS cloud security」、Amazon、2022 年 4 月 29 日にアクセス。

4 高度なセキュリティツール

クラウドプロバイダーは、多岐にわたる高度なセキュリティツールをデプロイして、顧客のアプリケーションとデータを保護しています。AWS は、きめ細かな ID およびアクセス制御、継続的な監視、脅威検出、ネットワークおよびアプリケーションの保護、複数の暗号化レイヤー、自動インシデント応答およびリカバリーなどを提供しています。ハイパースケーラーのパートナーマーケットプレイスでは、数百の追加セキュリティ・ソリューションが提供されています。この広範にわたる高度なセキュリティツールと同じことを自社のネットワークおよびデータセンターで行うことは、実質的に不可能です。セキュリティを専門としない企業にとって、必要となるコスト、人員、時間、作業量は重すぎる負担です。

5 ネットワーク・セグメンテーション

クラウド環境特有のセキュリティ上のメリットとは、ユーザーのワークステーションから分離されていることです。一般的なサイバー攻撃の手法は、E メールや Web サイトを介してシステム上の特定のユーザーを標的にするというものです。このような場合、ユーザーのワークステーションを通じてシステムに侵入します。それに対してクラウド環境では、ユーザーワークステーションはユーザーが自分の業務を実行するのに必要な接続性しか持ちません。ワークステーションは企業ネットワークに直接アクセスできません。つまり、ワークステーションが侵害されても、攻撃者は企業やそのアプリケーションおよびデータにアクセスできないのです。

6 物理的なセキュリティ

物理的なセキュリティは、依然として重要な要因です。ハードウェアに物理的に直接アクセスできる状態は、セキュリティ上の重大なリスクとなりかねません。しかし、データとアプリケーションがクラウド環境にあれば、不満を持った従業員や、このサイトで作業し、偶発的に危害を及ぼす可能性があるその他の人物は、このような資産に近づけません。クラウド環境ではデータを見つけることがはるかに困難だからです。

さらに、ハイパースケーラーは、セキュリティガード、サーバー用鍵付きケージ、その他の最新の物理的セキュリティ制御など、大半の組織にはない、データの物理的な盗難を防ぐリソースを用意しています。

関連情報

「クラウドサービスを通じた開発者の能力強化」をお読みになり、Red Hat® Cloud Services がクラウドネイティブ・アプリケーションへの移行に役立つ方法の理解にお役立てください。

Red Hat について

Red Hat は、受賞歴のあるサポート、トレーニング、コンサルティングサービスを通じて、組織の環境全体の標準化、クラウドネイティブ・アプリケーションの開発、複雑な環境の統合、自動化、保護、および管理を支援します。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
0120 266 086
03 5798 8510

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
#F31540_0522