CHECKLIST

クラウド上で重要なアプリケーションをセキュアに実行するための検討事項 TOP4

今では、ほとんどすべての企業がクラウドを導入して、業務をモダナイズし、迅速なイノベーションを実現し、成長を加速しています。823 人のサイバーセキュリティプロフェッショナルを対象に、Fortinet が行ったグローバル調査、2022 年版クラウドセキュリティレポートでは、企業の40% 近くが自社のワークロードの半分以上をクラウドで実行していると報告されています。

さらに、この数字は2024 年までに60% 近くまで増加すると予想されています。[1] このような企業の多くは、複数のセキュリティソリューションをバラバラに導入しており、そのほとんどが統合されていません。

さらに、それぞれのクラウド環境ごとに、リスクの状況がサイロ化されていて、また修復機能に制限があるため、管理の複雑性が増大することになります。

重要なアプリケーションを「スマートかつ強固に」保護する

また同じ調査で、セキュリティスキルの不足が多くの企業にとっての最重要課題（61%、前年度の57% から上昇）であることが明らかになりました。これに続いて、データ保護（53%）、異なるソリューションがどのように組み合わされるかを把握すること（51%）、可視性と制御性の不足（47%）が挙げられました。[2]

そのため企業は、セキュリティ戦略を進化させ、運用上の効率性を改善することに力を入れ、クラウドリスクを積極的に管理する必要があります。ワークロードの保護に関していえば、これは、組織がクラウドデプロイの効果的な保護を「スマートかつ強固に」することを可能とする、適切なクラウドネイティブなプラットフォームを選択することを意味します。

- ソリューションの価値と効果を最大化します。クラウドネイティブな、統合型のセキュリティソリューションであれば、デプロイや管理が容易です。また、クラウドに加わる急な変更にも柔軟に対応でき、変更の必要性に応じて迅速にスケーリングできます。このような統合でソリューションの実装、集約を検討し、セキュリティアーキテクチャを簡素化し、アプリケーションやワークロード全体を幅広く可視化する機能を獲得し、投資の価値を最大化します。
- 対処すべき最も重要なリスクに集中します。複数のセキュリティテクノロジーから来るセキュリティデータを、クラウド環境をまたいで相互に関連付けて標準化することが可能な、統合型のクラウドネイティブソリューションを検討します。そのようなクラウドネイティブソリューションには、最も重要なリスクに集中できるようにするためにリスクの優先順位付けを行う機能も求められます。
- セキュリティオペレーションを簡素化して、対応を加速し、リスクを管理します。単一のダッシュボードから一貫性のあるポリシーやワークフローをモニタリングして適用でき、複数のクラウドにまたがり有効化できるソリューションを検討することで、セキュリティチームがセキュリティカバレッジのギャップを最小限に抑えられるようにするとともに、生産性を改善してクラウドフットプリントを一貫した形で保護できるようにします。

クラウドで重要なアプリケーションを実行する際のリスクを管理するためのソリューションを選択する際には、以下の重要な点について検討します。

☑ **そのソリューションは、他のクラウドネイティブセキュリティソリューションや、すべてのクラウドに統合されますか?**

クラウドリソースの保護において、導入が容易で迅速に実装できる、クラウドサービスプロバイダー（CSP）の幅広いセキュリティサービスが使用されることがよくあります。そのため、すでに導入しているCSP のクラウドネイティブセキュリティサービスやテクノロジーとも統合できるソリューションを検討して、統合の摩擦を最小限に抑え、価値を最大化するようにすべきです。

また、主要なクラウドを網羅する、最も広範な統合を実現できるソリューションを模索すべきです。これにより、単一のプラットフォームでワークロードを管理できるようになり、すべてのクラウドで一貫性のあるセキュリティとエクスペリエンスを達成できます。プラットフォームがひとつであるということは、専門知識の学習、構築が一度ですむということであり、結果を予測可能なものにするとともに、クラウドセキュリティオペレーションを効率化できます。

☑ **そのソリューションに、着目すべき最も重要なセキュリティリスクを優先付けて表示する機能はありますか?**

クラウドリスクの管理はダイナミックなプロセスです。潜在的な新しいリスク、進展するリスクを単に幅広く可視化するだけではなく、軽減が必要な最も重要なリスクを詳細に分析できる機能や、管理可能なリスクを受け入れるための機能も必要です。

他のセキュリティツールやサービスと統合でき、クラウド環境をまたがるさまざまなセキュリティテクノロジーから生成されるセキュリティに関する情報をリアルタイムで相互に関連付けて標準化できるとともに、セキュリティポスチャ、脆弱性、権限、脅威シグナルを織り込み、標準化されたリスク分析を実行できるソリューションが理想です。

☑ **そのソリューションで、セキュリティオペレーションを簡素化し、リスクを効果的に管理できますか?**

セキュリティの簡素化についてですが、他のセキュリティソリューションやサービスとの統合を活用するソリューションは、簡単にアクティベートでき、クラウドに依存しない、広範なセキュリティテクノロジーの専門知識を必要としないものであるべきです。

主要なクラウド環境すべてにおいてセキュリティカバレッジのギャップを最小限に抑えるための、一貫性のあるワークフローを実現するソリューションが不可欠です。このようにすることで、各クラウドプラットフォームとそれぞれのセキュリティサービスに関する詳細な項目をセキュリティチームが覚える必要性が低減されます。

☑ **そのソリューションは、サイバーセキュリティメッシュプラットフォームの一部として機能しますか?**

アプリケーションやワークロードがクラウド上で実行されるようになり、複雑性が増し、可視性が損なわれるという問題が発生しました。これにより、オンプレミスとクラウドの両方を管理するうえでの盲点が発生することとなりました。そのような問題に対応するには、クラウドネイティブな統合と調和して機能するサイバーセキュリティメッシュプラットフォームが必要不可欠です。

サイバーセキュリティプラットフォームであれば、広範で自動化された、統合型の機能が利用でき、エンタープライズセキュリティとクラウドデプロイを連携させる際にこれを役立てることができます。このような強力な組み合わせで、一元化された管理機能や可視性、一貫性のあるポリシーに加え、デプロイ全体を対象とした、自動化された対応、オペレーション能力を獲得し、その恩恵を得ることができます。

また、人工知能や機械学習を使用して脅威に迅速かつ効率的に対応できるようになるため、究極的には、多くの組織が直面している、サイバーセキュリティスキルとリソースギャップの対応にもこれを役立てることが可能です。

まとめ

フォーティネットは、クラウド環境全体にわたるクラウドアプリケーションとワークロードのデジタルアクセラレーションをセキュアに行うことをサポートします。フォーティネットは、Fortinet Security Fabric とともに主要なクラウドプラットフォームやセキュリティテクノロジーで統合可能な、摩擦のないクラウドネイティブなソリューションを提供することで、これを実現します。フィーティネットは、企業によるクラウドネイティブなセキュリティへの投資や、Fortinet Security Fabric での投資で得られる価値の最大化に貢献し、クラウドセキュリティを運用可能にする中で多大なメリットが得られるよう後押しします。

これらをFortiGuard の脅威インテリジェンスと組み合わせて使用することで、複雑性を低減し、アプリケーションやワークロードの保護に役立つ優れた可視性を獲得して、あらゆるクラウド環境で有効化してリスクを管理し低減する一貫性のあるワークフローを始めとした機能を実現する、包括的なクラウドネイティブセキュリティソリューションを構築することができます。

[1] 2022 年クラウドセキュリティレポート
[2] Ibid.

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木7-7-7 Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ