アプリのセキュリティを第一に考える

クラウドフレンドリなセキュリティの隠れたROI

概要

もし以前に聞いたことがあるのならこの言葉を遮ってください：
規模を問わずすべての企業は、生産性の向上とイノベーションの加速を実現するためアプリケーションやサービスをクラウドに移行して、デジタル トランスフォーメーションを実施しています。

IoT、ビッグ データ分析およびクラウド アーキテクチャに関する記事、そしてこのデジタル時代を勝ち抜こうとしている企業に対してこれらがもたらす無限の可能性は毎日のように目にしています。企業がデジタル トランスフォーメーションを実施している最中であれば（恐らくそうだと思いますが）、コスト削減、つまり事前に設定されていて数回のクリックで拡張できるソリューション、従量課金など、パブリック クラウドによる何らかの恩恵をすでに実感していることでしょう。しかし、パブリック クラウドの共有セキュリティ モデルが利用側のセキュリティに関する責任にどのような影響を与えるか、また、どのように利用すればマルチクラウド環境のメリットとなるかはご存じないかもしれません。

クラウド プロバイダは通常、その物理的なデータ センタ、インフラストラクチャおよび企業に提供されるシステムのセキュリティの管理については素晴らしい働きをしますが、アプリケーション、サービス、データなど、企業がクラウドで開発、導入または配置することについては何もできません。F5 Labsの調査によると、情報漏洩の53%では、アプリケーション レイヤが最初の標的にされています。[1] クレジット カードの所有者なら誰でも、セキュリティへの影響を理解しているかどうかに関係なく、クラウド サービスを利用してデータを保管または管理できることを踏まえれば、これは重要な事実です。[2]

53%

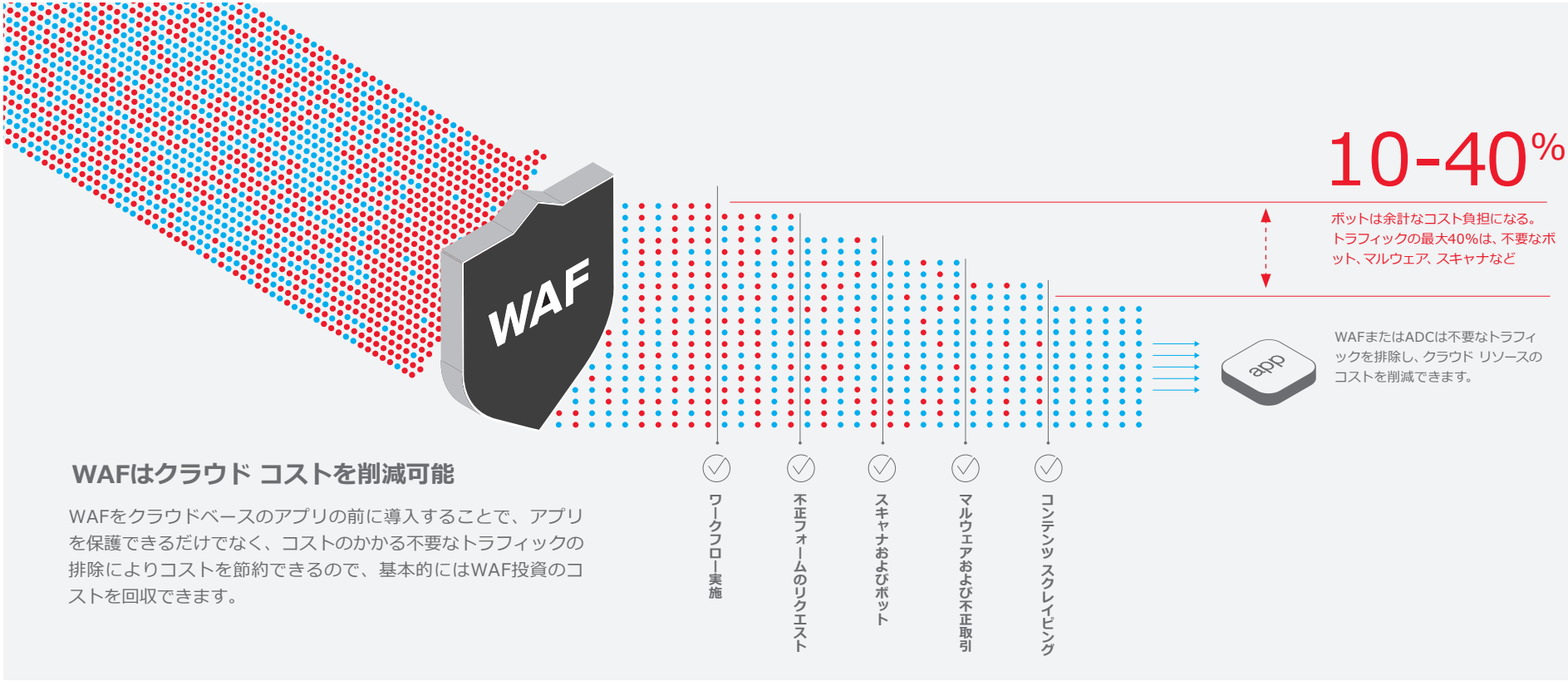
F5 LABSの調査によると、情報漏洩の53%ではアプリケーション レイヤが標的[1]

どう考えても、クラウドのセキュリティが従来のデータ センタのセキュリティと同様に重要であることは明らかです。これらの環境が複雑であるということだけでなく、クラウドにおけるアーキテクチャが一意で、セキュリティ コントロールがさまざまにあることから、クラウドベースの資産を保護するには慎重なアプローチが必要です。幸いなことに、クラウドでのプロアクティブなセキュリティは実際、ビジネス プロセスの最適化に役立ち、最終的な収益に好影響を与えることができます。さらに、さまざまなセキュリティ ソリューション プロバイダが提供するクラウド サービスにより、企業は、顧客の期待するセキュリティおよびサービスを継続的に提供しながら、その開発プロセスを加速することができます。

[1] https://f5.com/labs/articles/threat-intelligence/cyber-security/lessons-learned-from-a-decade-of-data-breaches
[2] https://www.theregister.co.uk/2017/10/10/accenture_amazon_aws_s3/

クラウド セキュリティ ソリューションは **利益を生み出す**

クラウド プロバイダのネットワークは十分に計画および立証されています。つまり、ボットおよび自動化されたスキャナが、クラウドにおけるアプリケーションのトラフィックの大部分を占めています。従量課金制の場合、ボットがクラウド アカウントに関連するリソースをリクエストするたびに、実際の定量化できるコストがかかります。そのため、顧客以外のトラフィックから生じる多額の料金をすでに支払っている可能性があります。しかし、Application Delivery Controller（ADC）やWebアプリケーション ファイアウォール（WAF）などの優れたセキュリティ ツールをクラウドベース アプリの前に導入することで、これらのアプリを保護できるだけでなく、不要なトラフィックを排除して、ボットやスキャナへのサービスのために割り当てられるリソースを削減することもできます。多くの従来のオンプレミス型セキュリティ導入とは対照的に、ADCまたはWAFをクラウドで使用することで、サービスの利用可能性およびセキュリティを保持できるだけでなく、測定可能な投資収益率をもたらすことができます。



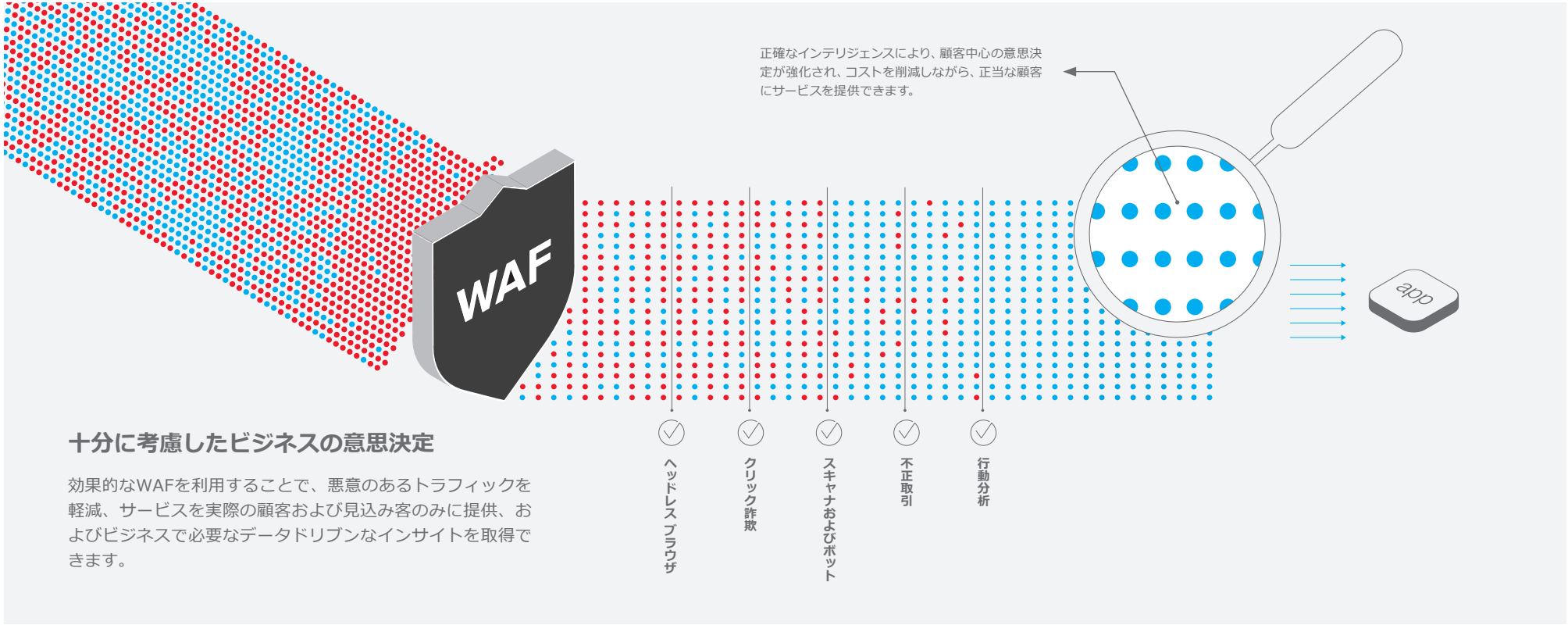
WAFはクラウド コストを削減可能

WAFをクラウドベースのアプリの前に導入することで、アプリを保護できるだけでなく、コストのかかる不要なトラフィックの排除によりコストを節約できるので、基本的にはWAF投資のコストを回収できます。

クラウド セキュリティ ソリューションは
ビジネス インテリジェンスを向上できる

セキュリティ ツールは、効果的に情報を提供し、ビジネス インテリジェンスを実現できます。優れたWAFまたはADCは、クラウドベースのWebアプリとの間で受け渡しされるトラフィック パターンやデータの分析を簡素化できます。このインテリジェンスを手にすることで、リソース管理の意思決定が強化され、正当な顧客に確実にサービスを提供しながらコストを削減できます。

可用性はアプリケーション セキュリティの柱です。顧客がアプリを利用できなければ、セキュリティを確保する必要は何もありません。クラウドでADC技術を利用することで、高可用性を実現できるだけでなく、ますます複雑化するアーキテクチャを簡素化し、強力なマルチクラウド戦略を最大限利用できます。適切なパートナであれば、ADCとセキュリティサービスの両方をパブリックとプライベートのクラウドで一貫してシームレスに提供でき、最もコスト効率に優れた方法で適切にトラフィックを管理および最適化できます。



十分に考慮したビジネスの意思決定

効果的なWAFを利用することで、悪意のあるトラフィックを軽減、サービスを実際の顧客および見込み客のみに提供、およびビジネスで必要なデータドリブンなインサイトを取得できます。

開発しやすいセキュリティ
の恩恵を受ける

セキュリティは誰もが気にすることですが、アプリケーションの所有者および開発者は、必ずしも、WAFポリシー、レイヤ7 DDoS対策またはWeb不正行為対策について詳しく知る必要はありません。必要なことは、アプリに関わるデータの機密性、完全性および可用性の保証だけです。事前に組み込まれているコード ライブラリおよびサードパーティ製ツールチェインを使用する方が一般的に簡単かつ効率的であるように、高度なセキュリティ サービスおよびソリューションを利用して、開発にかかる時間や労力を軽減することは、開発上非常に大きな意味をもたらします。これを踏まえて、効果的かつ実用的なセキュリティ ポリシーは、それを一番理解している人、つまりセキュリティの専門家から簡単に受け継ぎ、管理できます。

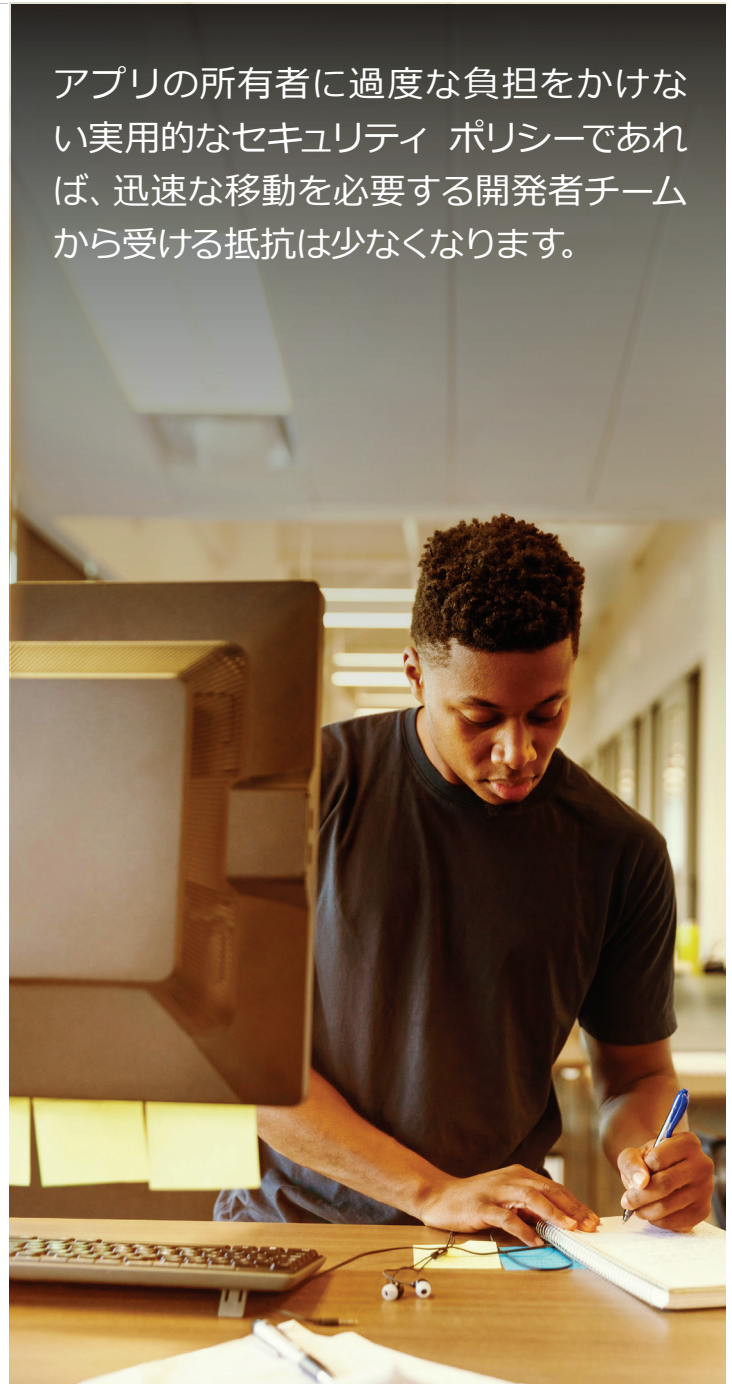
しかし、ビジネスのセキュリティについては、簡単かつ信用できるものでなければなりません。また、開発者と同じ方法で、開発プロセスに統合できなければなりません。アプリの所有者に過度な負担をかけない実用的なポリシーであれば、迅速な移動を必要する開発者チームから受ける抵抗は少なくなります。これは重要なことです。ポリシーが開発を可能にするのではなく、その妨げになるのであれば、開発チームはクレジット カードを取り出し、自らパブリック クラウドのアプリをスピンアップするかもしれません。積極的なスケジュールに取り組む場合や、競争力のある柔軟性を求めるニーズに応えようとする場合はこれが魅力的に感じるかもしれません。

50%

シャドーITは現在、大規模な組織の支出の最大50%を占めている[3]

アプリの所有者および開発者が、API、テンプレートおよびInfrastructure as Codeなどの慣れ親しんだ方法でセキュリティおよびADCソリューションとやり取りできることも重要です。クラウドに導入するソリューションは、アプリの所有者およびDevOpsチームが求め必要とするプログラム上の俊敏性を促進できるように、REST APIを適切にサポートする必要があります。これらの協力とサポートは、戦略的セキュリティ プログラムの成功に不可欠です。

[3] https://www.cio.com/article/3188726/it-industry/how-to-eliminate-enterprise-shadow-it.html



迅速な開発サイクルに要求される **強力なセキュリティ ツール**

セキュリティ ポリシーを整備しても、Webアプリを保護することは、難しく、コストも時間もかかります。クロスサイト スクリプティング（XSS）およびSQLインジェクションなどのリスク領域は、十分に理解されていますが、アプリを提供するたびにこれらに対する防御を確立することは難しいため、あらゆるところに存在しています。また、開発チームが、安全なコーディングおよび包括的なリスク保護を確実にするために必要な専門的知識を手に入れることがますます難しくなっています。『2017 WhiteHat Security Application Security Report』によると、ほとんどのアプリケーションには3つ以上の脆弱性があり、それらの約50%は危機的な状況にあります。つまり、すぐに修復しないと、データ損失、盗難またはサービス拒否のリスクが高まります。[4]

アプリ保護は簡単になってはいませんが、クラウドベースのWAFなどのツールを利用することができます。開発チームは、強力なWAFの機能を利用することで、OWASP Top 10のリスク領域への対処、レイヤ7 DDoS攻撃の軽減、ボットの検知および管理、ゼロデイ攻撃の阻止といったすべてを、通常の開発サイクル外で、これに影響を与えることなく実現できます。行動分析も、パターンを識別して、クラウドベースのWebアプリケーション間のトラフィックを管理する上で非常に有用です。また、これらの機能を自ら構築および管理するのは難しいことですが、信頼できるセキュリティ ソリューション プロバイダは、これらのサービスの実装を簡単かつ効果的にできます。

最後に、ハッキングが関連する情報漏洩の81%では、盗まれたパスワードまたは簡単に破られるパスワードが利用されているため、IDの管理をアプリケーション セキュリティ ポリシーの基盤にする必要があります。[5] フェデレーテッド アイデンティティ/シングル サインオンを使用することで、開発チームの認証インフラストラクチャのコーディング、監査および保守における負担を軽減できるだけでなく、アプリがどんなに素晴らしくても複数のユーザ名とパスワードを管理したくないユーザにとってもメリットがあります。

[4] https://info.whitehatsec.com/rs/675-YBI-674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

3

ほとんどのアプリケーションには3つ以上の脆弱性がある[4]

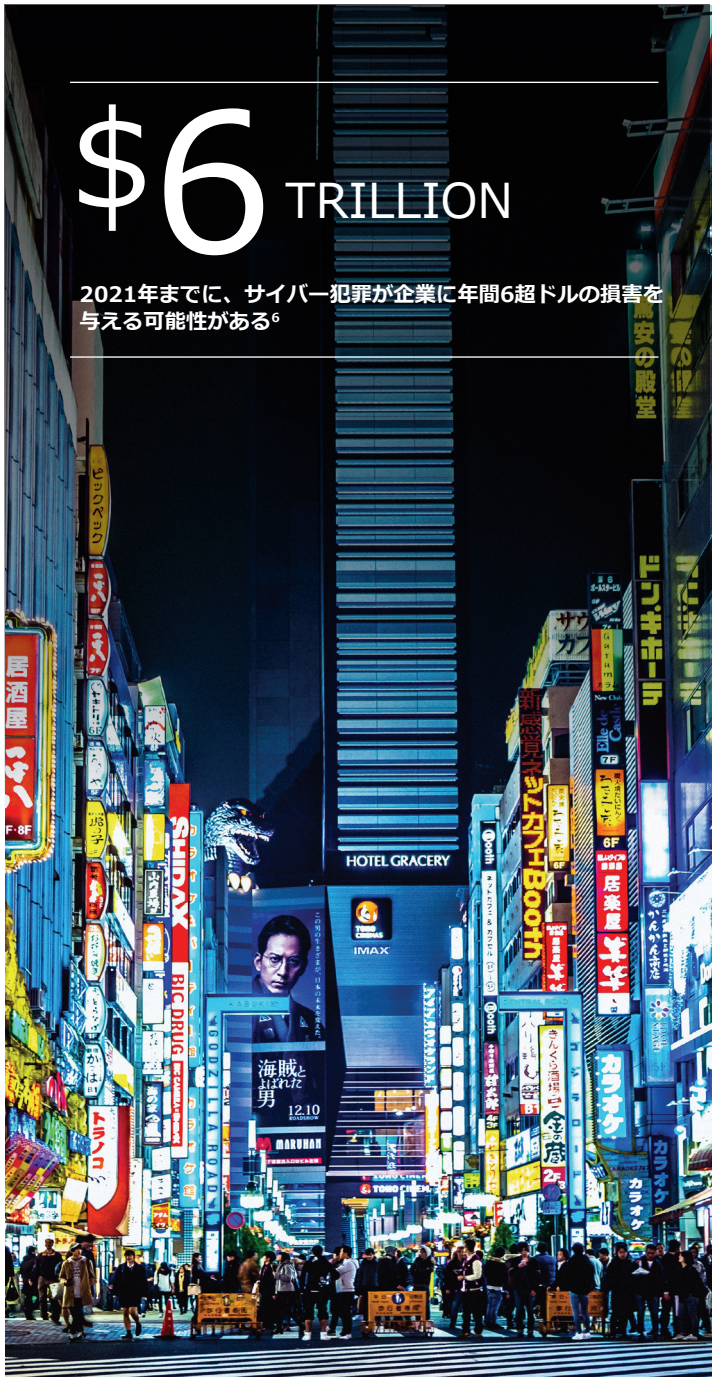
クラウドの俊敏性を向上する

信頼できるパートナー

クラウド プロバイダは、開発チームが選択できる多種多様なユーティリティ サービスおよびツールを導入することで、顧客を獲得しようと活発に競争しています。あるプロバイダは長期保存用のストレージを手頃な価格で提供し、またあるプロバイダは高度なビデオ ストリーミング体験を提供しているので、特定のアプリケーションでさまざまなクラウドのサービスを利用することは理に適ったことです。ポータブル セキュリティ ポリシーは、異なるクラウド プロバイダ間でインフラストラクチャをより柔軟に移動して必要な機能を利用できるようにするだけでなく、コスト削減を実現できます。高度なポータブルADCは、これらのますます一般的になるマルチクラウド導入環境からの恩恵を受けるために必要な流動的な負荷分散および管理を可能にします。

ここで注意すべきことは、クラウド プロバイダは、可能な限り多くの顧客のニーズを満たすようにその基本構造を設計しているため、ニーズによってはアーキテクチャおよびプロセスが最適でない場合もあります。ビジネスに合わせてクラウドを最適化するのは利用者側の責任です。ここで助けになるのが、信頼できるサードパーティ ソリューション プロバイダです。

任意のアプリケーションを一貫したセキュリティで任意の環境に導入するには、使用するセキュリティ ソリューションがマルチクラウドに対応し、高度にプログラム可能で、APIドリブンである必要があります。サードパーティ パートナの専門的知識を利用することで、各クラウド環境に一意な専用ツールを管理する必要なく、すべてのアプリケーションで一貫したセキュリティ サービスを利用できるポータビリティとユーティリティを得ることができます。



マルチクラウド セキュリティ プログラム

のための実用的なソリューション

2016年の調査では、技術CFOの4分の3近くが、クラウド コンピューティングは将来のビジネスにおいて最も測定可能な影響を与えると答えていました。[6] ビジネスがクラウドから最大の恩恵を受けるには、アクセスおよびアイデンティティを制御し、重要なサービスをいつでも利用できるようにして、管理下のクラウド インフラストラクチャの各所の脆弱性を管理するための戦略が必要になります。

クラウドのセキュリティを向上することは、今後もさらに重要になります。2021年までに、サイバー犯罪は企業に年間6兆ドルの損害を与える可能性があります。これは、違法か合法かに関係なく、歴史上最大となる経済的な富の譲渡です。[7] 17世紀フランスの貴族であり文学者でもあるフランソワ・ド・ラ・ロシュフコーの格言「大きな罪を犯すことができない人は、他人が大きな罪を犯すとは簡単には疑わない。」にあるように、ほとんどの人は自分がハッキングによる情報漏洩の被害者となるなど予期していません。[8] そのため、誰かに狙われていると疑うことがなくても、攻撃者は、ビジネスおよびアプリの所有者のお人好しの性格を喜んで利用します。そして悲しいことに、あまりにも多くの人がその標的にされています。

適切なツールを利用すれば、コストの削減につながるだけでなく、適切なレベルの保護を提供して、クラウドベースのアプリを円滑に運用し成功することができます。セキュリティに対する誤った知識を身に着けるのではなく、マルチクラウドの時代の未開の地でアプリケーションを保護するプロアクティブな方法を選んでください。

アプリケーション保護の詳細については、f5.com/security をご覧ください。

[6] https://www.bdo.com/getattachment/022227f4-aa2e-4a8b-9739-b0ad6b855415/attachment.aspx?2017-Technology-Outlook-Report_2-17.p
[7] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[8] https://books.google.com/books?id=D5B2BelDhOQC&printsec=frontcover#v=onepage&q&f=false

アプリのセキュリティを第一に考える

常時稼働、常時接続のアプリは、ビジネスを強化および変革する一方、ファイアウォールに保護されないデータへのゲートウェイにもなり得ます。ほとんどの攻撃はアプリ レベルで発生しているため、ビジネスを推進する機能を保護することは、攻撃を受けるアプリを保護することにつながります。

F5ネットワークスジャパン合同会社

東京本社
〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ19階
TEL 03-5114-3210 FAX 03-5114-3201

西日本支社
〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838

お問合わせ先：https://f5.com/jp/fc/

EBOOK-SEC-176514946 12.17