Akamai

ホワイトペーパー

ハイブリッドおよびマルチクラウド環境でのワークロードの保護

ハイブリッドおよびマルチクラウド環境でのワークロードの保護

イノベーション、競争優位性、効率性を追求する中で、エンタープライズ組織は DevOps ベースのクラウド・インフラ・モデルへと移行しています。そのため、これまでとはまったく異なる方法で、エンタープライズ IT のスピードとアジリティが向上しています。多くの組織では、パブリック・クラウド・インフラや、コンテナおよびサーバーレステクノロジーなどの新しい展開アプローチが続々と導入されています。この新しいモデルを採用することで、最新のクラウド・コンピューティング・テクノロジーは変化のペースを劇的に加速させています。これらのプラクティスにより、ワークロード、アプリケーション、さらには環境までもが、自動化、自動スケーリング、移行の対象となります。その結果得られる競争上の優位性は強力です。

同時に、従来のデータセンターインフラのような一部のレガシーサービスやシステムも使用され続けています。これらは企業で除外または最新化の過程にあるかもしれませんが、ビジネスクリティカルなアプリケーションやワークフローを保持しているということが、これらのシステムがまだ使用されている本質的な理由です。

さらに、従来のセキュリティ技術では変化のペースに対応できていませんでした。ここから、新しいハイブリッドクラウド環境とマルチクラウド環境でクラウドワークロードをどのように保護すればよいかという課題が生じます。変化の速さという問題以外にも、トラフィックの大部分が外部から受信する垂直方向（North ／ South）のトラフィックではなく、クラウドまたはデータセンター内で移動する水平方向（East ／ West）のトラフィックとなっているため、境界を守るというセキュリティ方式は効果的ではなくなっています。この変革により、IT 管理者はセキュリティプレイブックの見直しも迫られています。

ハイブリッド環境やマルチクラウド環境では従来のセキュリティ技術は効果を発揮できません

実際、従来のサイバーセキュリティモデルはどれも、Infrastructure as a Service（IaaS）を考慮して構築されていません。パブリッククラウドには、独自の課題に基づいた新しい戦略が必要です。

新たなビジネス環境をサポートするためには、エンタープライズセキュリティを進化させる必要があります。組織は、ビジネス要件を満たし、アジャイルな業務遂行方法を取り入れるために、大きな変化を遂げています。ところが、大規模な投資が行われているにもかかわらず、セキュリティは取り残されたままです。

実際のところ、クラウドを考慮せずに開発されたソリューションにコストをかけるのは間違いなのです。そのようなソリューションは、今日の、あるいは将来のセキュリティ侵害の検知や防止には役立ちません。では、重要なデータの保護を犠牲にすることなく、パブリック・クラウド・サービスを利用し、スピードとアジリティのメリットを享受するためにはどうすればよいでしょうか。

最新のハイブリッド・クラウド・データセンター

最新のデータセンターの構成や、細分化の進むワークロード、開発スピード。このすべてが、急速に変化しています。一般に、最新のハイブリッドデータセンターは、オンプレミスとパブリッククラウド／ IaaS の両方で実行されるワークロードで構成され、複数のベンダーが使用されています。また、Platform as a Service（PaaS）がオンプレミスまたはクラウドで利用されています。パブリッククラウドで実行されるワークロードの量は増え続けています。同時に、オンプレミスのデータセンターもしばらくは使い続けられます。具体的な数字で見てみましょう。テクノロジー担当の経営幹部を対象に行われた最近の調査によると、最新の IT 環境に関して、約 59% が「一部がクラウドに展開されているものの、大部分がオンプレミスに展開されている」と回答しており、34% が「ほとんどがクラウドに展開されているが、一部はオンプレミスに展開されている」と回答しています。「すべてクラウド」という回答はわずか 7% ですが、今後大幅に増加すると予想されます。[1.]

ご存じのとおり、エンタープライズ組織は DevOps のプラクティス導入を推進し、アジリティを向上させています。ネイティブ・クラウド・サービスとサーバーレステクノロジーをかつてないほど容易に導入できる環境が整ってきています。コンテナ、VM、サーバーレスのワークロードをクラウドで組み合わせて使用することにより、戦略的な観点からコスト効率の向上と変革を推進できます。

このようなハイブリッドクラウドのパラダイムに合ったセキュリティが求められています。企業は、新機能のテスト、構築、計画から監視、運用、展開、リリースまで、DevOps プロセスのあらゆる段階でセキュリティに対処する必要があります。クラウドへの移行が、成功を妨げる障害となることは許されません。

分散ワークロードが十分に保護されないため、新しいクラウドテクノロジーの使用が制限されます

今日の多くのエンタープライズ組織では、オンプレミス、コロケーション、および複数のパブリッククラウド／ IaaS プラットフォームに分散しているワークロードを保護する必要に迫られています。従来のオンプレミスのネットワーク・セキュリティ・モデルを使用していたのでは、これらのワークロードのセキュリティを確保することは困難です。

新しいクラウドテクノロジーを保護するために新しいクラウドベースのツールとテクニックを導入しようとすると、問題はさらに困難になります。企業がさまざまな環境に異なるセキュリティ制御を適用し、適切な可視性を持たずにこれらの制御を導入するとリスクがもたらされ、複雑さのレベルが増大します。

つまり、本来はエンタープライズ組織にダイナミクスを与え、アジリティと俊敏性を高めるとともに、イノベーションを推進する役割を担うはずのクラウドによって、多くの組織にリスクがもたらされています。エンタープライズ組織がこのクラウドという新しいテクノロジーを導入するためには、クラウドに特化した適切なセキュリティツールが必要です。このようなツールがなければ、盲点を生じさせることなく全体をセキュリティで保護し、新たな課題の発生を防ぐことが困難です。

そこで必要となるのが適応型のワークロード保護です。

IaaS への移行による、適応型ワークロード保護の必要性の高まり

ライフスパンの短いワークロードをきめ細かく保護するための最善の方法は、ワークロードが使用され始めたらすぐに動的な保護を適用することです。パブリック・クラウド・インフラにおいてセキュリティポリシーを適用するためには、ワークロード中心のソリューションを使用するほうが、従来のネットワーク・セキュリティ・モデルを使用するよりもはるかにシンプルです。

クラウドワークロード保護プラットフォームは、プラットフォームに依存しないワークロード中心のセキュリティソリューションをサポートします

このモデルでは、基盤となるインフラから独立したワークロードに沿ってポリシーが適用されるため、ハイブリッド・クラウド・データセンター環境全体のすべてのワークロードに適用することができます。その結果、プラットフォームに依存しない一貫したセキュリティ制御アプローチが実現します。

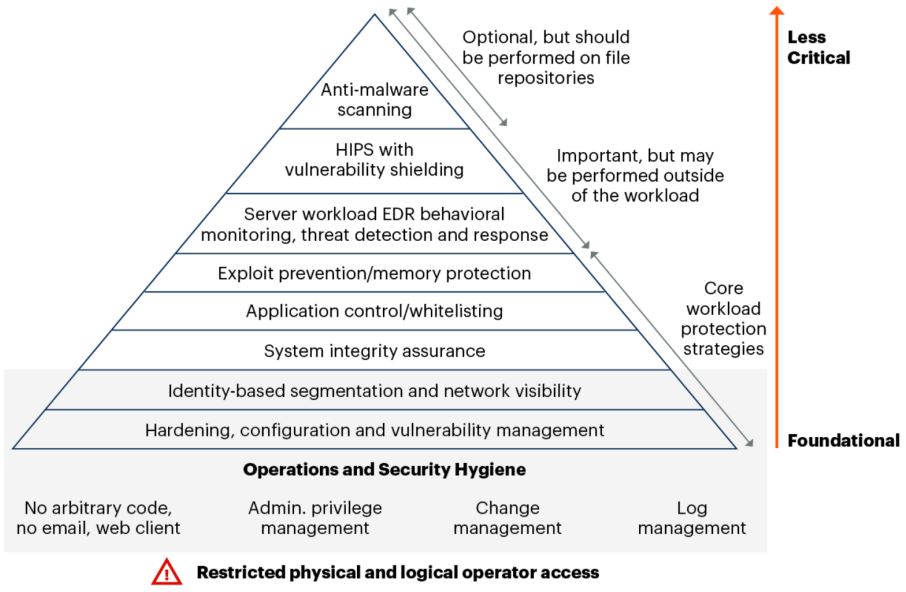
ネイティブなクラウド・セキュリティ・ツールは存在しますが、適応型クラウドワークロード保護プラットフォーム（CWPP）では、プロセス、ユーザー、完全修飾ドメイン名レベルでより包括的できめ細かな制御が提供されます。また、CWPP は複数のクラウドプロバイダーとオンプレミスで機能し、VM、コンテナ、サーバーレスワークロードをより強力かつ包括的に保護します。

実用的なワークロード保護のコア戦略：Gartner のクラウドワークロード保護ガイドラインへの制御のマッピング

クラウドワークロード保護に関して最も活用されているガイドラインの 1 つに、Gartner の業界専門家が作成したガイドラインがあります。Gartner によると、クラウドワークロードを保護する際には、明確な制御階層が存在します。

以下のピラミッドは、基本から重要度の低いものの順に、Gartner がコアと考えている戦略と、重要であるがオプションである戦略を示しています。理想的には、これらの手順を各ワークロードに含める必要があり、クラウド上のアクションごとにセキュリティが組み込まれていることを確認します。

ワークロード保護制御のリスクベースの階層 [2]



Source: Gartner
716192_C

Gartner

Gartner のクラウドワークロード保護ガイドラインは、エンタープライズ組織のセキュリティ制御の明確な階層を示します

ハイブリッドまたはマルチクラウドのデータセンター保護プログラムにこれらの戦略をどのように組み込むのが最善かを判断するために、当社のソリューションが提供するコア戦略の詳細な説明を以下に示します。

- **強化、設定、脆弱性管理**
  Gartner によると、適切なシステムの設定によりリスクを軽減することが、最も基礎的なワークロード保護戦略です。脆弱性管理ツールを使用すると、攻撃ベクトルを手作業で削除していた状態から大きく前進し、このプロセスを自動化することができます。これにより、悪意のある意図的な活動を招き入れる可能性のあるソフトウェアの問題を見つけて解決できます。

- **アイデンティティベースのセグメンテーションとネットワークの可視性**
  Gartner は、クラウド保護のコア戦略としてネットワークのセグメンテーションと可視性を強調しています。ほとんどの組織ではオンプレミスで次世代ファイアウォールを使用していますが、多くの組織ではクラウドに移行する際に安全性の低いソリューションを受け入れています。

  セキュリティチームでは、次世代ファイアウォールがクラウド保護に不十分であることを認識してはいるものの、動的なハイブリッドデータセンターにおいて異機種混在環境についてどのように知見を手にし、制御すればよいか、十分に理解できていません。そのための適切な方法について説明します。

  まず、可視性を確立します。迅速に可視化ができると、すべてのステークホルダーがただちに同じ状況を難なく把握できるため、短時間で価値を創出することにつながります。

  ネイティブなクラウドツールでは、スナップショットのマップやテキストログが提供されますが、これらは理解するのが難しかったり、あるいは不完全または不十分であることが一般的です。最適なソリューションは、ネットワーク内のすべてのアプリケーション、トラフィック、依存関係を自動的に検出できなければなりません。これにより、エンタープライズ組織がハイブリッド方式で分散していても、IT エコシステム全体を一目で把握することができます。

  また、ソリューションには、データセンターで発生している状況を正確に把握できる強力なコンテキストも含まれている必要があります。セキュリティの運用や問い合わせを大規模に管理したいと考えているエンタープライズ組織では、すべてのフローにこのようなコンテキストが必要で、個々のプロセスやサーバー通信にまでドリルダウンできる機能を備えている必要があります。これにより、ポリシー作成を支援するデータ主導型の意思決定が可能になります。

  可視性とコンテキストを確立できたら、ビジネスにおけるベストプラクティスに適合するセグメンテーションルールを作成します。たとえば、本番環境と開発環境を分離したり、顧客データを分離してコンプライアンスを証明したりすることができます。また、より詳細なマイクロセグメンテーションポリシーを作成して、特定のビジネスコンテキストに適した方法で高度なセキュリティと制御を実現することもできます。

- **アプリケーションの制御／許可リスト**
  セキュリティチームがポリシーを設定し、どこでも確実に実行できるという確信を持てれば、クラウドへの移行があらゆる段階でさらにシンプルになり、安全になります。

  ポートや IP だけに依存していては、クラウドワークロードの完全な保護に必要なレベルの可視性は得られません。アプリケーションコンポーネント間のトラフィックの厳密な制御が、強力なマイクロセグメンテーションソリューションの中核となります。最適なテクノロジーは、ハッシュ値、チェックサム、フルパス、解決、ID ストア認証などの詳細を使用して、アプリケーションプロセス、ユーザー、および完全修飾ドメイン名まで詳細に可視化し、制御します。

  アプリケーション制御を強化できる追加機能には、次のようなものがあります。

  - 同じアプリケーションクラスター内でもクラウド上のラテラルムーブメント（横方向の移動）を制限できるマイクロセグメンテーション
  - 「単一画面」のアプローチによるセキュリティの強化
  - 許可リストおよび拒否リストの両方のモデルを作成できる機能（いずれも不正なアプリケーションやトラフィックを防止し、重要な接続が妨げられずに実行できるようにするために必要な機能です）

- **脆弱性攻撃の防止／メモリ保護**
  Gartner が提供する CWPP 向けガイドのサーバー保護におけるコア戦略の最後は、脆弱性攻撃の防止です。セキュリティ侵害の検知と対応を提供するマイクロセグメンテーション・セキュリティ・ツールを取り入れましょう。これにより、冗長なツールを置き換えて、データセンターの複雑さを軽減できます。

  さらに、前述のように、可視性とマッピングは基本です。ネットワーク全体の完全なマップを作成すると、パッチ未適用の脆弱性や、標準とは違うふるまいの悪性の通信を簡単に見抜くことができます。エンタープライズ組織において、正規のトラフィックのベースラインを確立しておけば、許可されていないふるまいを即座に見分けられます。

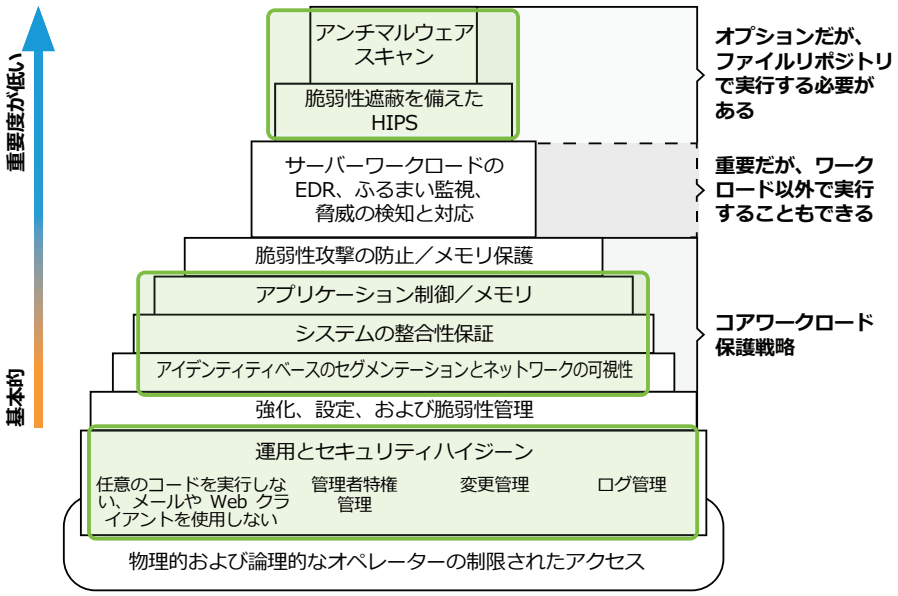
その他の重要な保護戦略

上記のコアサーバー戦略は、クラウドにおけるセキュリティの基礎となります。同時に、Gartner は、サーバーワークロードのエンドポイント検知と対応（EDR）、ふるまい監視、脅威の検知と対応（TDR）など、ハイブリッドまたはマルチクラウド環境のセキュリティ強化に役立つその他のいくつかの戦略も明らかにしています。

EDR、ふるまい監視、TDR は、セキュリティ侵害の検知とインシデント対応の重要な部分を占めています。セキュリティのこれらの側面をカバーするためには、レピュテーション分析を含むソリューションを検討します。このソリューションにより、攻撃に関するより詳しい情報を特定できるようになるうえ、攻撃者をおびき寄せてその手口を明らかにする高度なディセプション機能も利用可能になります。このようにして、今後のポリシーとセキュリティ手順を強化することができます。

過去のイベントに関する情報を明確に把握するためには、可視化データが必要になることがあります。優れたプロバイダーはデータを数か月間にわたって保存しているため、ユーザーは特定のアプリケーション、プロセス、期間に絞り込んで調査を実施できます。セキュリティチームは、このデータをフォレンジック調査やインシデント対応の改善に使用することもできます。

Akamai Guardicore Segmentation：CWPP 階層に基づくハイブリッド・クラウド・ワークロードの保護



強調表示されている領域は、当社のソリューションが CWPP 要件を満たしている部分を示しています

Akamai Guardicore Segmentation は、ネイティブのクラウド・セキュリティ・ツールに足りない部分を補うことで、CWPP に規定されている基本原則の多くを満たすことができます。さらに、このソリューションは、ハイブリッドおよびマルチクラウドデータセンター全体の可視性、ポリシー作成、適用をインテリジェントにサポートします。

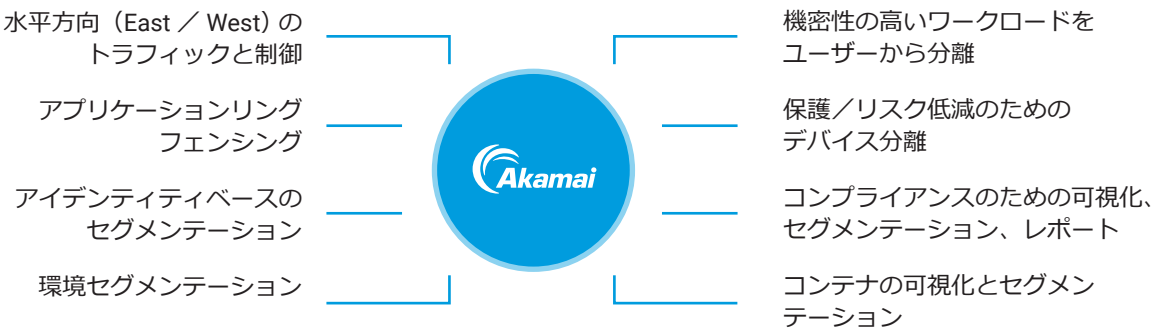
Akamai のソリューションでは、単一の画面でデータセンター全体の状況を確認し、詳細な可視性を得られます。ハイブリッドデータセンターが全体として可視化されるため、アプリケーションの依存関係や、任意のポリシーがネットワークに与える影響を確実に把握できます。これはクラウド移行に大きな影響を与え、ネイティブの可視化ツールよりもクラウドの移行をはるかに迅速に進められます。

この詳細な可視性により、次のことが可能になります。

- クラウド内のネットワーク用の To Do リストを作成する
- あらゆるインフラやアプリケーションの依存関係でアプリケーションを迅速に検出する（移行を成功させるための重要な機能）
- インフラと運用にかかるコストを事前に把握する
- 移行計画の段階からリスクを軽減するための最適なポリシー作成についての洞察を得る
- クラウドに関するビジネス目標を、最もシンプルで安全な最短のパスをたどって達成する

Akamai Guardicore Segmentation の詳細なコンテキストベースの可視性により、自社の環境を迅速かつ完全に把握できます

Akamai が提供する包括的な可視性には、各通信とフローのコンテキストも含まれているため、ミスを減らすとともに、全体的な複雑性を低減できます。情報をグループ化およびフィルタリングして、ステークホルダーによる状況の把握をサポートし、必要な情報を簡単に提供できます。このようにコンテキストに基づいて状況を把握できるため、サードパーティーのベンダーやポリシー作成者によるサポートが不要になり、自社環境を迅速に把握して、適切なポリシーを作成し、改良または修正できるようになります。



Akamai Guardicore Segmentation のユースケース例

Akamai のソリューションでは、その他に以下のような重要な機能が提供されます。

- プロセスおよびサービスレベルのポリシー。FTP や Spark などのダイナミックプロトコルを処理する際に、セキュリティがよりシンプルで強力になります。
- アイデンティティベースのマイクロセグメンテーションポリシー。接続を行うユーザーに基づいて接続ポリシーが適用されます。
- 完全修飾ドメイン名ベースのポリシー。これにより、動的 IP アドレスを持つ自動スケーリングリソースに到達できます。
- 既存のパブリック・クラウド・タグをラベルとして使用する。ハイブリッドまたはマルチクラウドデータセンターを簡単に可視化できます。
- 観察されたトラフィックからのポリシーの自動構築。マイクロセグメンテーションの導入に着手する際に、専門的なガイダンスをすばやく利用できます。

Akamai のソリューションはプラットフォームやインフラに依存しないため、インフラ全体で可視性とポリシー適用を管理できます

ハイブリッドデータセンターのセキュリティを確保する場合に最終的な目標となるのが、複雑さの低減です。Akamai Guardicore Segmentation は、このニーズに対応するため、プラットフォームやインフラに依存しない仕組みとなっており、ワークロードの場所に関係なく、ワークロードに沿った、アプリケーションとポリシー全体の一元化されたビューを参照できます。各ルールは、vCenter およびパブリッククラウド（AWS、Azure、GCP）からベアメタルサーバーおよびコンテナまで、すべてのワークロードに適用されます。

複雑さを低減することは、より強固なセキュリティ体制につながるだけでなく、IT およびセキュリティチームの負担軽減にもつながります。クラウドベースのセキュリティグループの場合、各ベンダーのネイティブクラウドのエキスパートが必要となります。一方、1 つのセキュリティソリューションでインフラ全体の可視性およびポリシー適用を管理する場合、必要なのはその 1 つのテクノロジーの認定ユーザーのみです。

将来に備えたクラウドワークロード保護プラットフォーム

アジャイルの手法や DevOps の基礎の 1 つは、すばやく早期に失敗することで、「次のブーム」に簡単に乗り換えられる点です。しかし残念ながら（そして皮肉なことに）異なるクラウドプロバイダー間でワークロードを移行すると、非常に多くの手間がかかってしまいます。また、セキュリティを適切に維持することが困難な場合もあります。

あらゆる選択肢の可能性を維持できることが必要になります。マルチクラウドのインフラに移行する場合や、ワークロードを新しいクラウドプロバイダーに完全に移行する場合でも、セキュリティに悪影響を及ぼしたり、セキュリティが原因で移行できなかったりすることがあってはなりません。

Akamai Guardicore Segmentation を使用すると、柔軟性を維持しながら、ビジネスのペースに合わせて、セキュリティポリシーの効果はそのままにワークロードを移行できます。DevOps プロセスやアジリティを妨げることも、あらゆる段階で再設定が必要になることもありません。代わりに、信頼できるクラウドワークロード保護プラットフォームの基礎を提供し、ハイブリッドデータセンターやマルチクラウドデータセンターのセキュリティを維持できます。

Akamai Guardicore Segmentation により、クラウドへの移行およびクラウド間の移行を安全に実行でき、コンテキストに応じた比類のない可視性が提供されます。Akamai のソリューションにより、プロセスやユーザーのレベルまでポリシーを適用し、展開されている場所にかかわらずワークロードを保護できます。

これで、DevOps プロセスの各段階にセキュリティが組み込まれ、アジリティを高め、ビジネスをサポートできるようになります。セキュリティをその中心に据えつつ、最先端のクラウド機能を活用することができるのです。

業界をリードするマイクロセグメンテーションでクラウド環境を保護する方法の詳細をご覧ください。今すぐ akamai.com/guardicore をご覧ください。

1 2022 年、Foundry（旧 IDG）による Cloud Computing Study.

2 Market Guide for Cloud Workload Protection Platforms、Gartner のアナリスト Neil MacDonald および Tom Crow 著、2020 年 4 月 14 日発行

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 5 月。