ホワイトペーパー

リスク緩和、防止、キルチェーンの切断

Akamai Guardicore Segmentation で
ランサムウェアの影響を最小限に抑える

概要

ランサムウェアは、これまで、サイバー犯罪者がファイルやデータを暗号化してアクセスできなくするために使用する迷惑なマルウェアの 1 つにすぎませんでしたが、現在ではより大きな問題を引き起こす存在へと変貌を遂げています。永久的なデータ損失の脅威だけでもやっかいですが、サイバー犯罪者や国家ぐるみのハッカーたちは、ランサムウェアを使用してエンタープライズ、連邦政府、グローバルインフラ、ヘルスケア組織に侵入して機能を麻痺させてしまうほど高度なものになっています。

2017 年に被害をもたらした WannaCry クリプトワームは、Microsoft Windows の脆弱性を悪用して全世界の 23 万台におよぶコンピューターに感染しましたが、これはランサムウェアがどのような脅威をもたらすかを示す格好の例となりました。それ以来、攻撃者はますます巧妙になり、攻撃はますます広汎になっています。ハッカーがランサムウェアをサービスとして販売する RaaS（Ransomware as a Service）のようなものまで登場しています。Akamai のランサムウェア脅威レポート（2022 年上半期）では、2020 年に最初に検知された悪名高い RaaS グループで、ロシアを拠点としていると思われる Conti の攻撃パターンを評価しました。この分析により、ラテラルムーブメント（横方向の移動）に対する強力な保護の必要性、そしてそのような保護がランサムウェアに対する防御において重要な役割を果たす可能性があることが示唆されています。さらに、Conti の被害を受けた企業の圧倒的多数が、1,000 万米ドルから 2 億 5,000 万米ドルの収益規模であることがわかりました。

> **マイクロセグメンテーションは、ポリシーに明示的に定義された接続のみを許可することで、ネットワーク内における暗黙的な信頼を一掃します。これにより、さまざまなアプリケーションにおけるマシン間トラフィックに対して、最小限のアクセス権のみを付与できます。**
>
> **— Forrester、「Best Practices For Zero Trust Microsegmentation」、2022 年 6 月 27 日**

このことは、時代遅れのテクノロジーの使用、境界とエンドポイントのみに重点を置いた「そこそこ効果のある」防御戦略の導入、トレーニング不足（不十分なセキュリティエチケット）、「特効薬」となるソリューションが存在しないといった原因が重なり、あらゆる規模の組織がリスクにさらされていることを明確に示しています。実際、サイバーセキュリティベンチャーが発行した「Who's Who In Ransomware」レポート 2023 年版によると、2031 年までに、2 秒に 1 回の頻度でランサムウェアが企業、消費者、デバイスを攻撃するようになると予測されています。

ラテラルムーブメントを利用するランサムウェア

ランサムウェア攻撃では、まず攻撃者の実際の意図を悟られ、防御されないよう用心しながら、フィッシングメール、ネットワーク境界の脆弱性、総当たり攻撃などによりセキュリティが侵害されます。マルウェアがデバイスまたはアプリケーションに到達すると、権限の昇格とネットワークおよび複数のエンドポイントのラテラルムーブメントを経て、感染および暗号化のポイントを最大化します。攻撃者は通常、ドメインコントローラーの制御を奪い、認証情報を侵害し、バックアップを見つけて暗号化することで、凍結されたサービスをオペレーターが復元できないようにします。

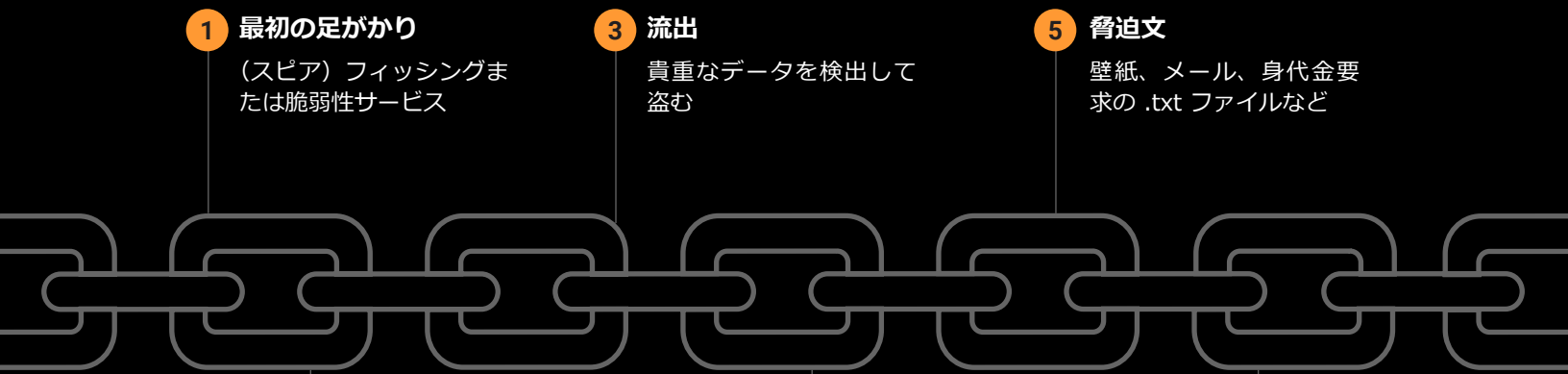
攻撃を成功させるためには、ラテラルムーブメントがきわめて重要です。マルウェアが最初にセキュリティを侵害したポイントから拡散できなければ、その攻撃は成功しません。したがって、ラテラルムーブメントの防止が不可欠となります。Akamai Guardicore Segmentation などのソリューションの可視化機能およびセグメンテーション機能により、迅速にポリシーを設定して初期侵害を防ぎ、封じ込めることができます。また、マルウェアを早期に検知してすぐに対応できるように、ラテラルムーブメントやその他の疑わしいふるまいについてアラートを受け取ることもできます。

第 1 部：ランサムウェアのキルチェーンの切断 - リスクの緩和と防御

ランサムウェアは1 台のマシンやデバイスの侵害では終わりません。サイバー犯罪者は、ランサムウェアを利用して、ネットワークのできるだけ多くのシステムを暗号化し、確実に身代金を手に入れます。

ランサムウェアは多面的な攻撃であるため、複数の防御層を実装することで、広範囲にわたる被害、データの損失、およびダウンタイムを防ぐことができます。防御の最初の層で行うことは、ランサムウェアの初期感染を防ぐことです。

ランサムウェアのキルチェーン



1 **最初の足がかり**
（スピア）フィッシングまたは脆弱性サービス

2 **ラテラルムーブメント**
ネットワーク全体に拡散して最大のインパクトを与える

3 **流出**
貴重なデータを検出して盗む

4 **暗号化**
PKI を利用した暗号化により、クラッキングを防ぐ

5 **脅迫文**
壁紙、メール、身代金要求の .txt ファイルなど

6 **影響**
データ、財務、ブランドなど

初期感染を防ぐ

ネットワークにおいて最初の脆弱な場所となるのはインターネットとの接点です。多くのランサムウェア攻撃はスピアフィッシングに依存していますが、インターネットに公開されているサービスへの侵入を妨げるものは何もありません。

Akamai Guardicore Segmentation の可視化機能を使用すると、インターネットに公開されているサービスを監視し、以下のためのポリシーを通じて公開範囲を制限できます。

- リモート・アクセス・サービス（RDP、SSH、TeamViewer、AnyDesk、VPN）
- 脆弱な可能性のあるサービス（Apache、IIS、Nginx）
- 脆弱な可能性のあるマシン（追加の Insight 機能を使用して、パッチ未適用のオペレーティングシステムを使用しているマシンを検知）
- 不要な公開サービス（データベース、ドメインコントローラー、内部の Web またはファイルサーバー）

セグメンテーションによってキルチェーンを切断

ネットワークがいずれかのポイントで侵害されることは避けられません。これは、スピアフィッシング、人為的エラー、または脆弱なサービスを実行しているサーバーなどに対する緩和が適切に行われなかった場合に発生する可能性があります。適切なリスク緩和戦略を実施することが重要なのはこのためです。

マシンが侵害されると、ネットワーク内での伝播を制限する必要があります。これを行うには、次の 3 つの方法があります。

1. アプリケーションのリングフェンシングによるセグメンテーション

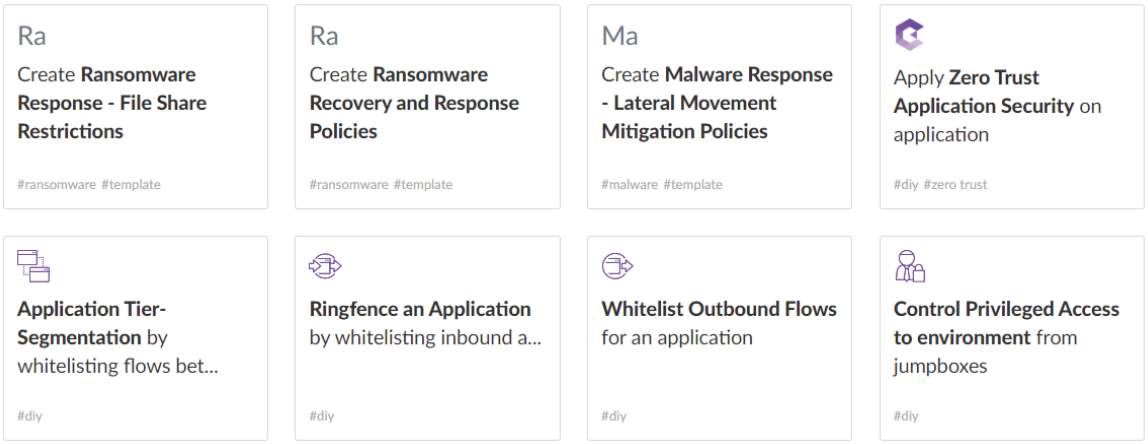
ネットワークを、アプリケーション、使用方法、または環境によって運用セグメントに分割し、それらのセグメント間およびセグメント内での不要な接続を許可しないようにします。

以下がセグメンテーションについて考慮すべき 4 つのガイダンスとなります。

- ノートパソコン／ワークステーションの間でのあらゆる通信をブロックする。
- ドメイン管理者などの「強力」なドメインユーザー権限で実行されているプロセスからの通信をブロックする。
- プロセスをサーバーで実行できるユーザーを制限する。
- ノートパソコン／ワークステーションからデータセンターサーバーおよびクラウドインスタンスへのアクセスを制限する。

Akamai Guardicore Segmentation を使用することで、ネットワークをランサムウェアから簡単に保護できます。あらかじめ用意されたテンプレートを使用すると、以下の 3 つの簡単な手順でポリシーを設定し、攻撃を緩和できます。

1. **目標を選択する：**重要なアプリケーションのリングフェンス、ランサムウェア緩和ポリシーの策定、または Active Directory のセキュリティの保護など。
2. **保護する関連アセットを特定する：**リングフェンスの実行を考えている E コマース・アプリケーション・アセット、データセンター内のすべての Active Directory ワークロード、またはランサムウェアの拡散から防御したいエンドポイントなど。このステップは、多くの場合、Akamai の AI ラベリングによって自動的に実行されます。
3. **ポリシーを作成することでアセットを保護する：**Akamai Guardicore Segmentation の AI が、環境内の実際のトラフィックに基づいてポリシーを自動的に提案および推奨するとともに、数百のネットワークにわたるアプリケーションの通信パターンを学習します。

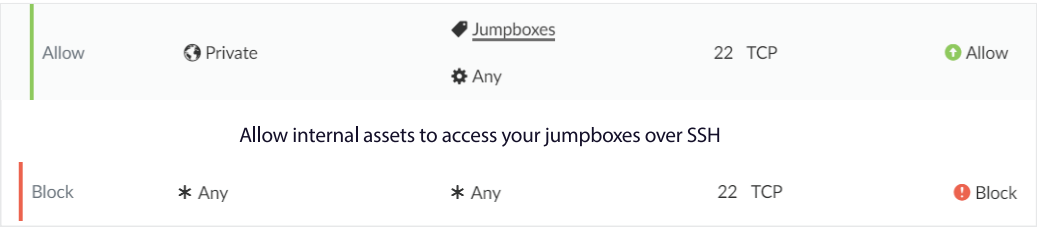


お客様事例：Akamai Guardicore Segmentation テンプレート

2. プロトコル制限ルールによるラテラルムーブメントの防止

特定のプロトコルとふるまいについて、一般的なガイドラインがあります。通常の日常業務に組み込まれて使用されているプロトコルもあるため、それらを細かく確認して制限する必要があります。Akamai Guardicore Segmentation を使用することで、すべてのトラフィックを可視化し、WinRM、SMB、RPC、RDP、SSH などのリスクの高いプロトコルに関して、環境向けの最も正確なルールを作成できます。

たとえば SSH は、リモート管理に役立つとともに他のプロトコル（sFTP など）のセキュリティにも役立ちますが、攻撃者がマシンを侵害してネットワークに伝播するために使用するツールでもあります。許可されたユーザー用のジャンプボックスを作成して、ネットワーク全体の SSH を可能な限り制限する必要があります。



Akamai Guardicore Segmentation で作成されたルール

3. バックアップと重要なデータサービスの保護

ランサムウェア攻撃は通常、与える損害を最大限高めるため、組織のバックアップサーバーをターゲットにして、保存されているデータを暗号化します。データサービスとファイルサーバーも同様にランサムウェアのターゲットとなります。

Akamai Guardicore Segmentation を使用することで、バックアップサーバー、データベース、ファイルサーバーへのアクセスを制限し、ネットワークの外部およびアクセスを必要としないネットワーク内のリージョンからのアクセスを制限できます。また、重要なバックアップサーバーとの間の通信を最小限まで抑えるために、Akamai Guardicore Segmentation を使用してアプリケーションをリングフェンスし、アプリケーションとの通信をプロセスレベルおよびユーザーレベルまでロックダウンできます。データサービスの公開を運用において最小限必要なもののみに制限することで、それらのサービスのリスク要因が軽減され、ランサムウェアにさらされる機会と伝播につながる可能性が緩和されます。

第 2 部：ランサムウェアの検知と対応

ランサムウェアなどのサイバー脅威に対処するためには、高度な計画と警戒が重要です。侵害に迅速に対応することで、ネットワークへの被害を最小限に抑えることができます。Akamai Guardicore Segmentation は、脅威の検知と対応の両方に役立つ機能を備えています。

Akamai Guardicore Segmentation による脅威検知

以下はインシデントの一例です。

- **ディセプション** – 疑わしいラテラルムーブメントの試みを検知および阻止し、そのアクションを監視および分析できるように動的なハニーポットにリダイレクトします。ディセプションにより、インシデントをハニーポットで忠実に再現することができるため、悪性のアクティビティについて詳細なデータを得ることができるとともに、サイバー犯罪者が次の段階としてどのような攻撃を行うかを把握することができます。
- **ネットワークスキャン** – サイバー犯罪者は、ネットワーク内に侵入した後、これを実行して情報を集めます。偵察方法としてこれを使用し、他のサーバーがリッスンしている、開いたままのポートまたはサービスを検出します。Akamai Guardicore Segmentation は、ネットワークスキャンを自動的に検知し、ユーザーに即座にアラートを送信します。
- **ポリシーベースの検知** – ネットワークおよびプロセスレベルのセキュリティポリシーにより、不正な通信や非準拠のトラフィックを即座に認識できます。

Akamai Guardicore Segmentation の Insight 機能

Akamai Guardicore Segmentation では、osquery に基づく追加機能を利用することで、個々のアセットを可視化することができます。Akamai Guardicore Segmentation が提供するクエリーフレームワークを使用して、ランサムウェアによる暗号化前の最も一般的なアクションであるボリューム・シャドウ・コピーなど、異常なアクティビティをすばやく検知できます。Akamai Guardicore Segmentation は、正規の Windows プロセスである svchost.exe の下にマルウェアを隠す一般的なハロウイング（空洞化）テクニックを検索することにより、ランサムウェアの配信に使用されるトロイの木馬を検知することもできます。

マネージド型脅威ハンティング

Akamai Hunt マネージド型脅威ハンティングサービスは、ネットワーク内の異常なふるまいについてユーザーにアラートを送信します。これは、着信および発信のインターネット接続とそれに関連する GeoIP の分析や、ネットワークプレゼンスが増加している新しい実行可能ファイルの検索（伝播を示している可能性がある）、アセット接続の分析による隣接カウントの異常の検知（ラテラルムーブメントの兆候となる）などの手法によって行われます。

即座に対応

ネットワーク内でランサムウェアなどの脅威を検知したら、プロセスおよびユーザーレベルでポリシーを適用し、悪性のアクティビティの発生を積極的に拒否および隔離することで緩和策を迅速に展開できます。

さらなる感染の可視化

最初の糸口や脅威の痕跡情報（IoC）を基に、通信パターン、プロセス、使用されたポート、感染したアセットなど、追加の兆候を探し始めることができます。Akamai Guardicore Segmentation を使用すると、そのような兆候のあるすべてのアセット（C2 と通信するすべてのアセット、一意のポートと通信するすべてのアセット、または悪性のプロセスを実行しているすべてのアセット）を検索できます。また、環境ビジュアルマップで、感染したマシンにわたってその他の類似点や伝播の痕跡を探すことができます。

第 3 部：駆除と復旧

感染したすべてのマシンと IoC のリストを取得したら、駆除を開始できます。マシンを**隔離済み（Isolated）**、**監視中（Monitored）**、**クリーン（Clean）**の 3 つのラベルグループに分けます。

隔離済み

- マルウェアに**感染**しているアセット
- マルウェアが削除されるまで、これらのアセットの**隔離**を維持

監視中

- **感染**している可能性があるアセット
- マルウェアが**削除**されたことが確認されるまで**監視**

クリーン

- **感染していない**ことが確認されたアセットで、**通常運用**が可能

復旧に関するセグメンテーションガイドライン

3 つのラベルグループを設定した後は、以下の 4 つの通信段階を作成することで、ネットワークをセグメント化するためのポリシーの追加を開始できます。

- **隔離済み**のマシンからの着信および発信のすべての通信を**ブロック**。
- **監視中**のマシンからの着信および発信のリモート管理プロトコル通信を**ブロック**。
- **クリーン**なマシンへのあらゆるリモート管理プロトコル通信に関して**アラート**。
- ラベルグループ間のすべての通信を**ブロック**。

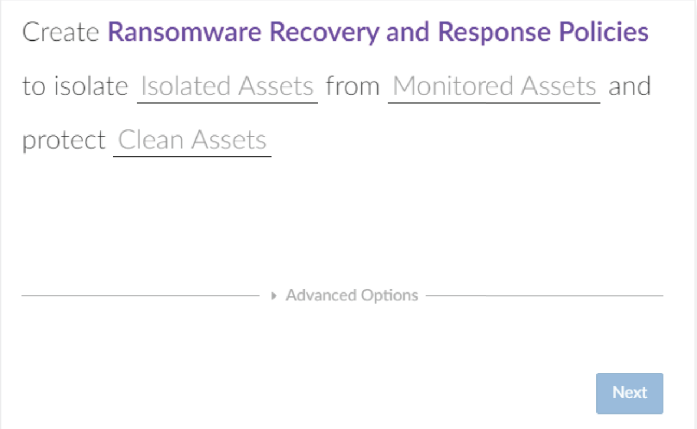
	Override Alert	✶ Any	Clean Any	5985, 5986 ... TCP | UDP
	Override Block	Monitored Any	Clean Any	Any TCP | UDP
	Override Block	Clean Any	Monitored Any	Any TCP | UDP
	Override Block	Monitored Any	✶ Any	5985, 5986 ... TCP | UDP
	Override Block	✶ Any	Isolated Any	Any TCP | UDP Any ICMP
	Override Block	Isolated Any	✶ Any	Any TCP | UDP Any ICMP

Akamai Guardicore Segmentation **でのブロックおよびアラートルール**

ランサムウェアからの復旧および対応のテンプレート

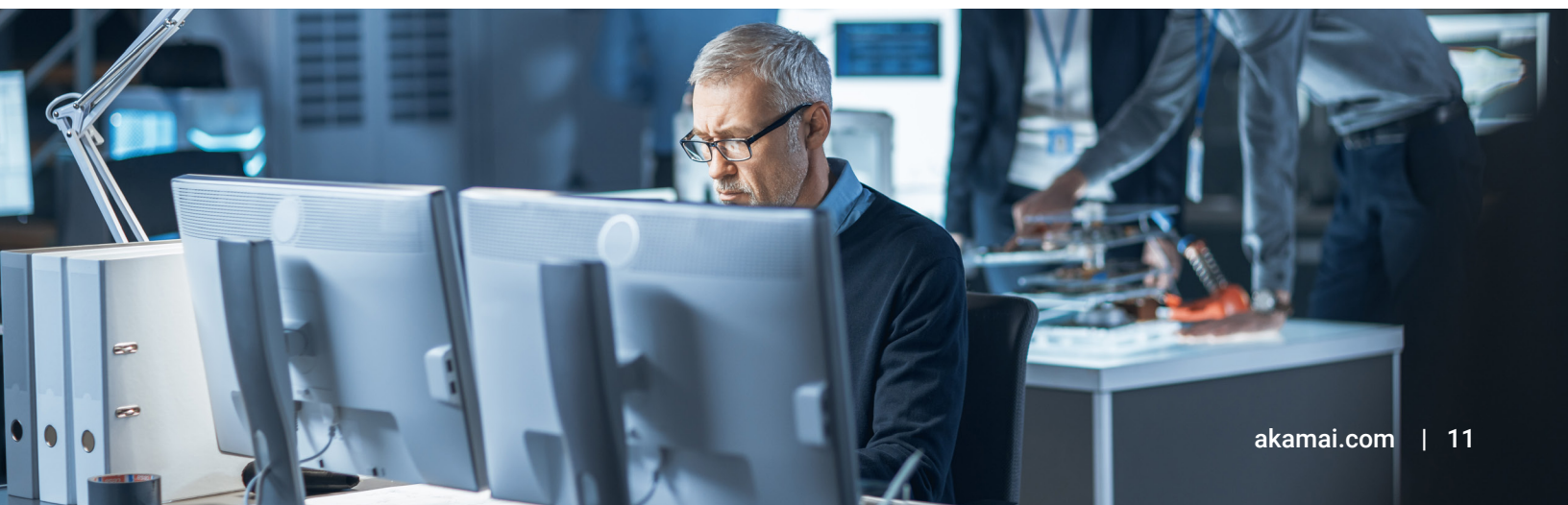
Akamai Guardicore Segmentation に含まれているランサムウェアからの復旧および対応のポリシーテンプレートは、使いやすい構築済みのポリシーを提供します。これにより、**隔離済み**、**監視中**、および**クリーン**のラベル全体へのアクセスを制限することができます。

このテンプレートを使用すると、**隔離済み**のマシンからの（再）感染を恐れることなく、**クリーン**なマシンの運用継続性を簡単に維持できます。



結論

いまだにレガシーファイアウォールや境界のみの防御に依存している場合は、ネットワークでのランサムウェアの拡散や、重要なアプリケーションとインフラのロックダウンを防ぐことはできません。侵害を受けることは避けられないというのが現実であり、そのために準備しておくことが必要です。Akamai Guardicore Segmentation は、水平方向（East ／ West）のデータセントートラフィックに潜む脅威を検知し、ランサムウェアが重要なアセットを暗号化し、人質にとる際に利用するラテラルムーブメントをブロックするのに役立ちます。



Akamai Guardicore Segmentation でランサムウェア攻撃の影響を緩和するための 5 つのステップ

準備のために特定する：IT 環境で実行しているすべてのアプリケーションやアセットを特定することで侵害に備えます。

阻止するために作成する：一般的なランサムウェア拡散手法を阻止するルールを作成します。

検知のために受信する：セグメント化されたアプリケーションやバックアップへのアクセスを検知すると、アラートが送信されます。

修復のために開始する：攻撃を検知したときの脅威の封じ込めと隔離対策を開始します。

回復のために可視化する：段階的な回復戦略をサポートします。

ネットワークでのランサムウェアのラテラルムーブメントを阻止しませんか。信じられませんか？ぜひご自身でご確認ください。akamai.com/guardicore

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、セキュリティポスチャ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。