Akamai

LIVRE BLANC

Protéger les charges de travail dans les environnements hybrides et multicloud

Protéger les charges de travail dans les environnements hybrides et multicloud

En quête d'innovation, d'avantages concurrentiels et d'efficacité, les entreprises ont adopté un modèle d'infrastructure cloud basé sur DevOps. Elles ont ainsi gagné en vitesse et en agilité dans leurs opérations informatiques. Du jamais vu. De nombreuses entreprises continuent d'adopter une infrastructure de cloud public et de nouvelles approches de déploiement (conteneurs et technologies sans serveur, par exemple). En appliquant ce nouveau modèle, la toute dernière technologie de Cloud Computing accélère considérablement le rythme du changement. Ces pratiques permettent, entre autres, d'automatiser, de mettre à l'échelle automatiquement et de migrer les charges de travail, les applications et même les environnements. Les avantages concurrentiels qui en résultent sont particulièrement intéressants.

Dans le même temps, certains services et systèmes existants (infrastructure de centre de données traditionnelle, par exemple) sont toujours utilisés. Il se peut que les entreprises soient en passe de les supprimer ou de les moderniser, mais ces systèmes existent toujours en soi car ils contiennent des applications et des flux de travail stratégiques.

De plus, les techniques de sécurité traditionnelles n'ont pas su s'adapter aux changements, ce qui pose la question de savoir comment protéger les charges de travail cloud dans ces nouveaux environnements de cloud hybride et multicloud. Au-delà de la vitesse, la sécurité basée sur le périmètre n'est plus efficace lorsque la grande majorité du trafic se fait à l'intérieur du cloud ou du centre de données (est-ouest), au lieu de provenir de l'extérieur du réseau (nord-sud). Cette transformation oblige également les responsables informatiques à repenser leur stratégie de sécurité.

Les techniques de sécurité traditionnelles ne sont pas efficaces dans les environnements hybrides et multicloud

En fait, aucun modèle de cybersécurité traditionnel n'a été élaboré pour une infrastructure en tant que service (IaaS). Le cloud public a besoin de nouvelles stratégies basées sur les défis uniques qui lui sont propres.

La sécurité d'entreprise doit évoluer pour prendre en charge le nouvel environnement d'entreprise. Les entreprises ont déjà apporté des changements radicaux pour répondre aux exigences métiers et suivre la méthodologie de travail agile. La sécurité n'a pas évolué au même rythme, malgré d'importants investissements.

En réalité, investir dans des solutions qui n'ont pas été développées pour le cloud est une erreur. Cela ne permet pas de détecter et de prévenir les violations actuelles ou futures. Alors, comment utiliser des services de cloud public et profiter de leurs avantages en matière de vitesse et d'agilité, le tout sans compromettre la protection des données critiques ?

Centre de données contemporain dans le cloud hybride

La composition d'un centre de données contemporain, la granularité accrue des charges de travail et la vitesse de développement évoluent rapidement. Un centre de données hybride contemporain classique est composé de charges de travail exécutées sur site et dans un cloud public/une IaaS, utilisant plusieurs fournisseurs et une plateforme en tant que service (PaaS) sur site ou dans le cloud. Le nombre de charges de travail exécutées dans le cloud public ne cesse de croître. Simultanément, les centres de données sur site ne sont pas prêts de disparaître. Par exemple, une récente enquête menée auprès de cadres du secteur des technologies a montré qu'environ 59 % d'entre eux ont « quelques environnements informatiques contemporains sur le cloud, mais la plupart sur site », et 34 % « principalement sur le cloud, mais quelques-uns sur site. » Seulement 7 % ont « tout sur le cloud », mais ce nombre devrait considérablement augmenter.[1]

Comme nous pouvons le constater, les entreprises adoptent de plus en plus de pratiques DevOps et améliorent leur agilité. Les services cloud natifs et la technologie sans serveur sont plus faciles que jamais à mettre en œuvre. En utilisant une combinaison de conteneurs, de machines virtuelles et de charges de travail sans serveur dans le cloud, vous pouvez gagner en rentabilité et en capacité de transformation d'un point de vue stratégique.

La sécurité doit s'intégrer à ce paradigme de cloud hybride. Les entreprises doivent gérer la sécurité à chaque étape du processus DevOps : test, création, planification, surveillance, exploitation, déploiement et lancement de nouvelles fonctionnalités. Migrer vers le cloud ne devrait pas être un obstacle à la réussite.

Aujourd'hui, de nombreuses entreprises doivent protéger des charges de travail distribuées sur site, dans une installation de colocation et sur plusieurs plateformes de cloud public/IaaS. Elles peinent à sécuriser ces charges de travail avec les modèles de sécurité réseau sur site traditionnels.

> Les charges de travail distribuées ne sont pas bien sécurisées, ce qui limite l'utilisation des nouvelles technologies cloud

La situation est d'autant plus difficile lorsque vous tentez de déployer de nouveaux outils et techniques basés sur le cloud pour sécuriser les nouvelles technologies cloud. Et elle se complique encore davantage lorsque les entreprises essaient d'appliquer différents contrôles de sécurité dans différents environnements. Déployer ces contrôles sans visibilité adéquate présente des risques.

En d'autres termes, le cloud, censé rendre les entreprises plus dynamiques, agiles, rapides et innovantes, en met beaucoup en danger. En raison d'un manque d'outils de sécurité pertinents axés sur le cloud, elles sont limitées dans leur capacité à adopter cette nouvelle technologie sans créer d'angles morts et de nouveaux défis.

C'est là qu'intervient la protection adaptative des charges de travail.

La migration vers une IaaS rend la protection adaptative des charges de travail nécessaire

Le meilleur moyen de sécuriser des charges de travail granulaires de courte durée est d'y appliquer une protection de manière dynamique dès qu'elles sont utilisées. En matière d'infrastructure de cloud public, les solutions centrées sur les charges de travail sont beaucoup plus simples que les modèles de sécurité réseau traditionnels pour appliquer une règle de sécurité.

> Les plateformes de protection des charges de travail dans le cloud prennent en charge des solutions de sécurité indépendantes de la plateforme et centrées sur les charges de travail

Étant donné qu'une règle suit la charge de travail, indépendamment de l'infrastructure sous-jacente, il est possible d'appliquer le modèle à toutes les charges de travail dans tout l'environnement de centre de données dans le cloud hybride. Il en résulte une approche cohérente et indépendante de la plateforme pour les contrôles de sécurité.

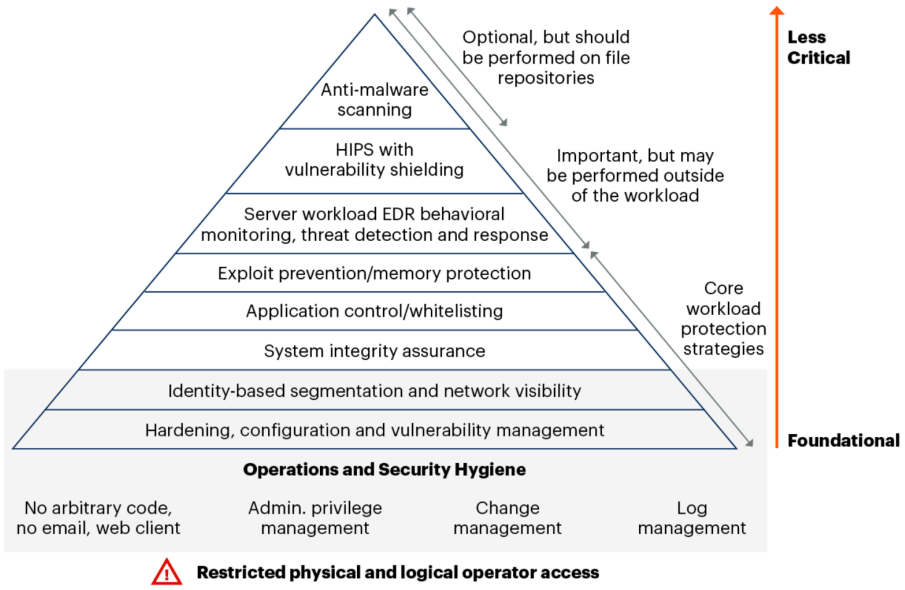
Bien qu'il existe des outils de sécurité cloud natifs, les plateformes de protection adaptative des charges de travail dans le cloud (CWPP) offrent un contrôle plus complet et granulaire au niveau des processus, des utilisateurs et des noms de domaine complets. Elles fonctionnent également avec plusieurs fournisseurs de cloud et sur site, offrant une protection renforcée et plus complète pour les machines virtuelles, les conteneurs et les charges de travail sans serveur.

Principales stratégies concrètes de protection des charges de travail : mapper les contrôles conformément aux directives de Gartner en matière de protection des charges de travail dans le cloud

L'une des directives les plus suivies pour la protection des charges de travail dans le cloud a été rédigée par des experts du secteur chez Gartner. Selon Gartner, il existe une hiérarchie claire des contrôles à effectuer afin de protéger les charges de travail dans le cloud.

La pyramide ci-dessous classe, de la plus fondamentale à la moins critique, les stratégies que Gartner considère comme essentielles, ainsi que celles qui sont importantes mais facultatives. Dans l'idéal, ces étapes doivent être incluses dans chaque charge de travail pour veiller à ce que la sécurité soit intégrée pour chaque action sur le cloud.

Hiérarchie des contrôles de protection des charges de travail, basée sur les risques[2]



Les directives de Gartner en matière de protection des charges de travail dans le cloud fournissent une hiérarchie claire des contrôles de sécurité pour les entreprises

Pour vous aider à comprendre comment intégrer au mieux ces stratégies dans votre programme de protection des centres de données hybrides ou multicloud, voici une explication détaillée des principales stratégies que notre solution applique :

- **Renforcement, configuration et gestion des failles de sécurité**
  Selon Gartner, la stratégie de protection des charges de travail la plus fondamentale consiste à configurer vos systèmes et paramètres de manière appropriée afin de réduire les risques. Les outils de gestion des failles de sécurité poussent la suppression manuelle des vecteurs d'attaque plus loin et automatisent ce processus. Vous pouvez alors détecter et résoudre les problèmes logiciels susceptibles d'ouvrir la porte à des intentions malveillantes.
- **Segmentation basée sur l'identité et la visibilité du réseau**
  Gartner présente la segmentation et la visibilité du réseau comme des stratégies essentielles pour la protection du cloud. La plupart des entreprises utilisent des pare-feu nouvelle génération sur site mais, lorsqu'elles migrent vers le cloud, bon nombre d'entre elles acceptent une solution moins sécurisée.

  Les équipes de sécurité comprennent que les pare-feu nouvelle génération sont insuffisants pour la protection dans le cloud, mais elles ne savent pas comment obtenir un contrôle ou une visibilité hétérogène dans un environnement de centre de données hybride dynamique. Prenons un moment pour voir comment s'y prendre.

  Il faut tout d'abord établir la visibilité. Une visibilité rapide réduit les délais de rentabilisation, car toutes les parties prenantes sont immédiatement et automatiquement sur la même longueur d'onde.

  Les outils cloud natifs peuvent fournir des cartes instantanées ou des journaux textuels, mais ceux-ci sont généralement denses, incomplets ou insuffisants. La meilleure solution doit identifier automatiquement l'ensemble des applications, du trafic et des dépendances de votre réseau. Ainsi, vous verrez en un coup d'œil tout votre écosystème informatique, même lorsque votre entreprise est distribuée de manière hybride.

  Votre solution doit également inclure un contexte efficace, avec une vision claire de ce qui se passe dans votre centre de données. Pour toute entreprise cherchant à gérer ses requêtes et opérations de sécurité à grande échelle, chaque flux doit disposer de ce contexte et pouvoir analyser tous les processus et les communications avec le serveur. Cela permet une prise de décision basée sur les données qui favorise la création de règles.

  Une fois la visibilité et le contexte établis, créez des règles de segmentation conformes aux meilleures pratiques de votre entreprise. Par exemple, vous pouvez séparer les environnements de production et de développement ou isoler les données client pour en prouver la conformité. Vous pouvez également développer des règles de microsegmentation plus granulaires pour assurer une sécurité et un contrôle approfondis en fonction du contexte spécifique de votre entreprise.

- **Contrôle des applications/Liste blanche**
  Lorsque votre équipe de sécurité est en mesure de définir une règle tout en étant sûre qu'elle s'exécutera partout, votre transition vers le cloud est plus simple et plus sécurisée à chaque étape.

  Utiliser uniquement les ports/adresses IP ne vous permettra pas d'obtenir le niveau de visibilité dont vous avez besoin pour assurer une protection complète des charge de travail dans le cloud. Un contrôle strict du trafic entre les composants applicatifs est un élément essentiel d'une solution de microsegmentation efficace. Les meilleures technologies offrent une visibilité et un contrôle granulaires au niveau des processus, des utilisateurs et des noms de domaine complets, avec des détails tels que les valeurs de hachage, la somme de contrôle, le chemin complet, les résolutions et les authentifications des systèmes d'identification.

  Les fonctionnalités suivantes supplémentaires sont susceptibles d'améliorer le contrôle des applications :

  - Microsegmentation, capable de limiter les mouvements latéraux sur le cloud même au sein d'un même cluster d'applications
  - Environnement de surveillance unique, se traduisant par une sécurité accrue
  - Possibilité de créer des modèles de liste blanche et noire pour empêcher les applications ou le trafic non autorisés et veiller au bon fonctionnement des connexions importantes
- **Prévention des exploits/Protection de la mémoire**
  La dernière stratégie essentielle de protection des serveurs du guide de Gartner pour les plateformes CWPP est la prévention des exploits. Recherchez un outil de sécurité de microsegmentation qui assure la détection et le traitement des violations. Vous pourrez ainsi remplacer les outils redondants et simplifier votre centre de données.

  De plus, comme mentionné précédemment, la visibilité et le mappage sont essentiels. Une fois l'ensemble de votre réseau mappé, vous pouvez facilement voir les failles de sécurité non corrigées ou les communications malveillantes inhabituelles. Une fois que votre entreprise a établi une base de référence pour le trafic légitime, les mouvements non autorisés ressortent.

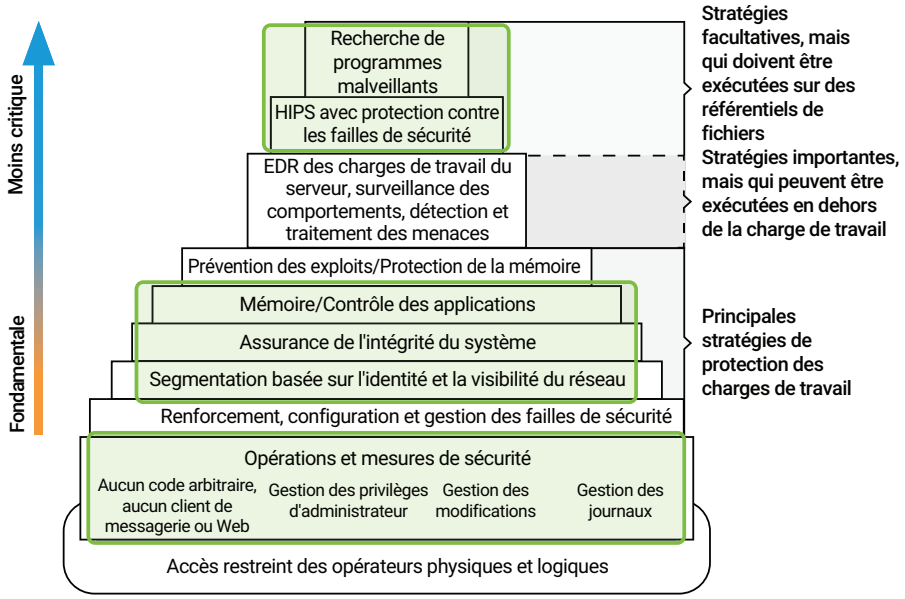
Autres stratégies de protection importantes

Les principales stratégies de serveur mentionnées ci-dessus sont fondamentales pour la sécurité dans le cloud. Dans le même temps, Gartner identifie plusieurs autres stratégies qui peuvent renforcer votre environnement hybride ou multicloud, notamment la détection et le traitement des points de terminaison (EDR) des charges de travail des serveurs, la surveillance des comportements et la détection et le traitement des menaces (TDR).

Les stratégies EDR, de surveillance des comportements et TDR sont des éléments importants de la détection des violations et de la réponse aux incidents. Pour couvrir ces aspects de la sécurité, recherchez une solution qui inclut l'analyse de la réputation. Cela vous permettra non seulement d'identifier plus d'informations sur une attaque, mais aussi de profiter de capacités de leurres avancées pour inciter les attaquants à dévoiler leurs méthodes. De cette façon, vous pourrez durcir votre règle et votre procédure de sécurité à l'avenir.

Des données de visibilité peuvent être nécessaires pour établir des informations sur un événement passé. Les meilleurs fournisseurs stockent vos données pendant des mois, ce qui permet aux utilisateurs de se concentrer sur des applications, processus et périodes spécifiques. Les équipes de sécurité peuvent également utiliser ces données pour mener des enquêtes et assurer une meilleure réponse aux incidents.

Akamai Guardicore Segmentation : protéger les charges de travail dans le cloud hybride conformément à la hiérarchie CWPP



Les zones en surbrillance indiquent où notre solution répond aux exigences des CWPP

Akamai Guardicore Segmentation comble les lacunes inhérentes aux outils de sécurité cloud natifs, en respectant bon nombre des principes fondamentaux définis dans la hiérarchie CWPP. De plus, la solution prend en charge intelligemment la visibilité, la création de règles et leur application dans les centres de données hybrides et multicloud.

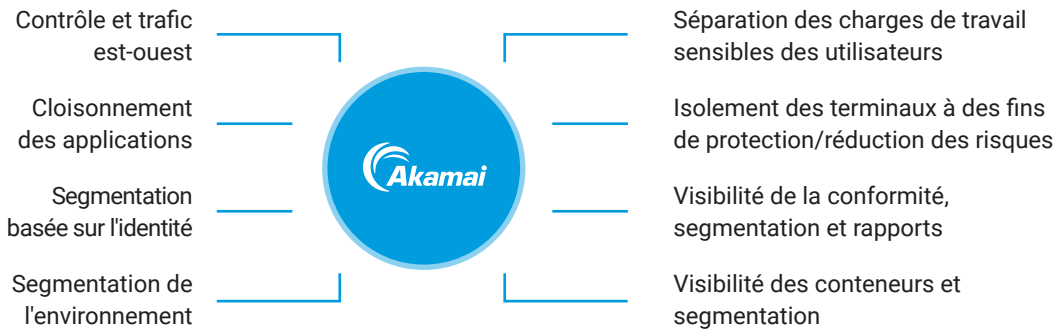
Notre solution offre une visibilité profonde, avec un environnement de surveillance unique qui donne un aperçu de l'ensemble du centre de données. En visualisant votre centre de données hybride dans son intégralité, vous pouvez comprendre parfaitement les dépendances des applications et l'effet que toute règle aura sur votre réseau. Cela a un fort impact sur la migration vers le cloud, permettant aux clients d'y accéder beaucoup plus rapidement qu'avec des outils de visualisation natifs.

Grâce à cette visibilité exceptionnelle, vous pouvez :

- créer une liste des tâches à réaliser pour votre mise en réseau dans le cloud ;
- détecter rapidement les applications dans toutes les dépendances des infrastructures et des applications, une capacité indispensable pour réussir votre migration ;
- comprendre à l'avance votre infrastructure et vos coûts opérationnels ;
- obtenir un aperçu du meilleur processus de création de règles pour réduire les risques dès les étapes de planification de la migration ; et
- emprunter le chemin le plus court, le plus simple et le plus sécurisé pour atteindre les objectifs de votre entreprise en matière de cloud.

La visibilité approfondie et contextuelle offerte par Akamai Guardicore Segmentation assure une compréhension rapide et approfondie de vos environnements

Notre visibilité complète s'accompagne également d'un contexte pour chaque communication et flux, ce qui vous permet de réduire les erreurs et de simplifier l'intégralité du processus. Vous pouvez regrouper et filtrer les informations pour aider les parties prenantes à lire la carte, en leur fournissant facilement les informations exactes dont elles ont besoin. Cette vue basée sur le contexte réduit le nombre de fournisseurs tiers et de créateurs de règles nécessaires, vous permettant de comprendre rapidement vos environnements pour pouvoir créer, affiner ou modifier les règles applicables.



Exemples de cas d'utilisation d'Akamai Guardicore Segmentation

Les autres fonctionnalités stratégiques de notre solution sont les suivantes :

- Règles au niveau des processus et des services, qui permettent de simplifier et de renforcer la sécurité en cas de protocoles dynamiques tels que FTP ou Spark
- Règles de microsegmentation basée sur l'identité, qui appliquent les connexions en fonction de l'utilisateur à l'origine de la connexion
- Stratégies basées sur les noms de domaine complets, qui vous permettent d'atteindre les ressources de mise à l'échelle automatique dont les adresses IP sont dynamiques
- Utilisation de balises de cloud public existantes en tant qu'étiquettes, simplifiant ainsi la visualisation de votre centre de données hybride ou multicloud
- Création automatique de règles à partir du trafic observé, pour vous fournir des conseils rapides et avisés dès le début de votre parcours de microsegmentation

Notre solution est indépendante de la plateforme et de l'infrastructure, et gère la visibilité et l'application des règles dans l'ensemble de l'infrastructure

Réduire la complexité est l'objectif ultime lorsque l'on cherche à sécuriser un centre de données hybride. Pour cela, la solution Akamai Guardicore Segmentation est indépendante de la plateforme et de l'infrastructure, ce qui vous donne un aperçu de l'ensemble de l'application et des règles qui suivent la charge de travail, quel que soit son emplacement. Chaque règle est appliquée à toutes les charges de travail, de vCenter et des clouds publics (AWS, Azure, GCP) aux serveurs dédiés physiques (bare metal) et aux conteneurs.

Non seulement la réduction de la complexité renforce la stratégie de sécurité de l'entreprise, mais elle allège également la charge de travail des équipes informatique et de sécurité. Avec des groupes de sécurité basés sur le cloud, vous avez besoin d'experts cloud natifs pour chaque fournisseur. En revanche, avec une seule solution de sécurité qui gère la visibilité et l'application des règles dans l'ensemble de l'infrastructure, vous avez seulement besoin d'utilisateurs certifiés pour une technologie unique.

Une plateforme pérenne de protection des charges de travail dans le cloud

L'une des pierres angulaires de la méthodologie Agile et du DevOps est la capacité à échouer et à passer facilement et rapidement au « prochain grand défi ». Malheureusement, et quelque peu ironiquement, la migration de vos charges de travail entre différents fournisseurs de cloud peut ralentir considérablement votre activité. Il peut également s'avérer difficile de réussir avec la sécurité en place.

Vous devez être en mesure de garder votre libre-choix. Si vous souhaitez migrer vers une infrastructure multicloud, ou même migrer des charges de travail vers un nouveau fournisseur de cloud, cela ne doit pas avoir d'effet négatif sur la sécurité, et la sécurité ne doit pas non plus vous empêcher de procéder à cette migration.

Akamai Guardicore Segmentation vous assure une certaine flexibilité et vous permet de suivre le rythme de votre activité, en migrant vos charges de travail sans toucher aux règles de sécurité. Cette solution ne nuit pas à l'agilité et au processus DevOps, et ne nécessite pas de reconfiguration à chaque étape. Au lieu de cela, elle fournit les bases d'une plateforme fiable de protection des charges de travail dans le cloud, pour que vous puissiez sécuriser votre centre de données hybride ou multicloud.

Akamai Guardicore Segmentation assure une migration sécurisée vers le cloud et entre les clouds, et offre une visibilité inégalée assortie de contexte. Grâce à notre solution, vous pouvez appliquer des règles au niveau des processus et des utilisateurs, et suivre vos charges de travail quelle que soit leur destination.

Vous pouvez désormais intégrer la sécurité à chaque étape du processus DevOps, favorisant ainsi l'agilité et les activités de l'entreprise, qui pourra être en mesure d'adopter des capacités cloud de pointe tout en privilégiant la sécurité.

En savoir plus sur la sécurisation des environnements cloud avec notre solution de microsegmentation leader du marché. Consultez le site akamai.com/guardicore dès aujourd'hui.

1 2022. Étude menée par Foundry (anciennement IDG) sur le Cloud Computing.

2 Market Guide for Cloud Workload Protection Platforms ; rédigé par Neil MacDonald et Tom Crow, analystes chez Gartner ; publié le 14 avril 2020

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de sécurité, de traitement et de diffusion d'Akamai, consultez les sites akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn. Publication : 05/23.