WHITE PAPER

Protezione dei carichi di lavoro negli ambienti ibridi e multicloud

Protezione dei carichi di lavoro negli ambienti ibridi e multicloud

Alla ricerca di innovazione, vantaggi competitivi ed efficienza, le aziende sono passate a un modello di infrastruttura cloud basato su DevOps, aumentando la velocità e la flessibilità dell'IT aziendale in modi mai visti prima. Molte organizzazioni continuano ad adottare l'infrastruttura del cloud pubblico e nuovi approcci di implementazione come container e tecnologie senza server. Adottando questo nuovo modello, la più recente tecnologia di cloud computing sta accelerando notevolmente il ritmo del cambiamento. Queste pratiche consentono di automatizzare, scalare automaticamente, migrare carichi di lavoro, applicazioni e persino ambienti e altro ancora. I vantaggi competitivi che ne derivano sono potenti.

Allo stesso tempo, alcuni servizi e sistemi legacy, come l'infrastruttura tradizionale del data center, rimangono in uso. Le aziende potrebbero essere in procinto di rimuoverli o modernizzarli, ma i sistemi esistono ancora intrinsecamente perché contengono applicazioni e workflow business-critical.

Inoltre, le tradizionali tecniche di sicurezza non sono state in grado di stare al passo con il ritmo del cambiamento, aprendo la questione di come proteggere i carichi di lavoro cloud in questi nuovi ambienti cloud ibridi e multicloud. Al di là della velocità, la sicurezza perimetrale non è più efficace quando la stragrande maggioranza del traffico si svolge all'interno del cloud o del data center (est-ovest) anziché provenire dall'esterno (nord-sud). Questa trasformazione costringe anche i dirigenti IT a rivedere la propria strategia di sicurezza.

Le tecniche di protezione tradizionali non sono efficaci in ambienti ibridi e multicloud

In effetti, nessun modello di cybersicurezza è stato creato pensando all'infrastruttura come servizio (IaaS). Il cloud pubblico necessita di nuove strategie basate sulle sue sfide specifiche.

La sicurezza aziendale deve evolversi per supportare il nuovo ambiente aziendale. Le organizzazioni hanno già apportato cambiamenti radicali per soddisfare i requisiti aziendali e la metodologia di lavoro flessibile. La sicurezza è rimasta indietro nonostante gli ingenti investimenti effettuati.

La realtà è che spendere soldi per soluzioni sviluppate senza pensare al cloud è un errore. Non aiuta a rilevare e prevenire le violazioni odierne o future. Quindi, come è possibile utilizzare i servizi di cloud pubblico e usufruire dei vantaggi della velocità e della flessibilità, senza compromettere la protezione dei dati critici?

Il data center cloud ibrido moderno

La struttura del data center moderno, la maggiore granularità dei carichi di lavoro e la velocità di sviluppo stanno cambiando rapidamente. Un tipico data center ibrido moderno è composto da carichi di lavoro in esecuzione sia on-premise che su cloud pubblico/IaaS, utilizzando più fornitori e utilizzando la piattaforma come servizio (PaaS) on-premise o nel cloud. La quantità di carichi di lavoro in esecuzione nel cloud pubblico continua a crescere. Allo stesso tempo, i data center on-premise non scompariranno a breve. Un esempio: un recente sondaggio tra i responsabili della tecnologia ha mostrato che per quanto riguarda gli ambienti IT moderni, circa il 59% ne includono "alcuni sul cloud ma la maggior parte on-premise", con il 34% con data center "principalmente sul cloud ma alcuni on-premise". Solo il 7% è "basato completamente sul cloud", ma si prevede che tale numero aumenterà notevolmente.[1]

Come possiamo vedere, le aziende stanno sempre più adottando pratiche DevOps e migliorando la propria flessibilità. L'implementazione dei servizi cloud nativi e della tecnologia senza server sta diventando sempre più facile. Utilizzando una combinazione di container, macchine virtuali e carichi di lavoro senza server nel cloud, consente una maggiore convenienza e capacità di trasformazione da un punto di vista strategico.

La sicurezza deve adattarsi a questo paradigma di cloud ibrido. Le aziende devono gestire la sicurezza in ogni fase del processo DevOps, dal test, alla creazione e alla pianificazione, al monitoraggio, all'operatività, all'implementazione e al rilascio di nuove funzionalità. Il passaggio al cloud non può essere un ostacolo che impedisce il successo.

I carichi di lavoro distribuiti non sono ben protetti, limitando l'utilizzo della nuova tecnologia cloud

Molte aziende oggi devono proteggere i carichi di lavoro distribuiti in locale, colocation e più piattaforme di cloud pubblico/IaaS. Fanno fatica a proteggere questi carichi di lavoro con i tradizionali modelli di sicurezza di rete on-premise.

Le cose diventano più difficili quando si tenta di implementare nuovi strumenti e tecniche basati su cloud per proteggere le nuove tecnologie cloud. I livelli di complessità si moltiplicano, poiché le aziende tentano di applicare controlli di sicurezza diversi in ambienti diversi e introducono rischi implementando questi controlli senza un'adeguata visibilità.

In altre parole, il cloud, che ha lo scopo di rendere le imprese più dinamiche, flessibili, veloci e innovative, sta ora mettendo a rischio molte organizzazioni. In assenza di strumenti di sicurezza incentrati sul cloud pertinenti, la capacità delle aziende di adottare questa nuova tecnologia senza causare punti ciechi e ulteriori sfide è limitata.

È qui che entra in gioco la protezione adattiva del carico di lavoro.

Il passaggio all'IaaS determina la necessità di una protezione adattiva del carico di lavoro

Il modo migliore per proteggere i carichi di lavoro granulari di breve durata consiste nell'applicazione dinamica della protezione non appena il carico di lavoro è in uso. L'applicazione delle policy di sicurezza è molto più semplice per le soluzioni incentrate sui carichi di lavoro per rispetto ai tradizionali modelli di sicurezza di rete quando si tratta di infrastrutture cloud pubbliche.

Le piattaforme di protezione del carico di lavoro nel cloud supportano soluzioni di sicurezza indipendenti dalla piattaforma e incentrate sul carico di lavoro

Poiché una policy segue il carico di lavoro, indipendentemente dall'infrastruttura sottostante, il modello può essere applicato a tutti i carichi di lavoro nell'intero ambiente del data center cloud ibrido. Il risultato è un approccio coerente e indipendente dalla piattaforma ai controlli di sicurezza.

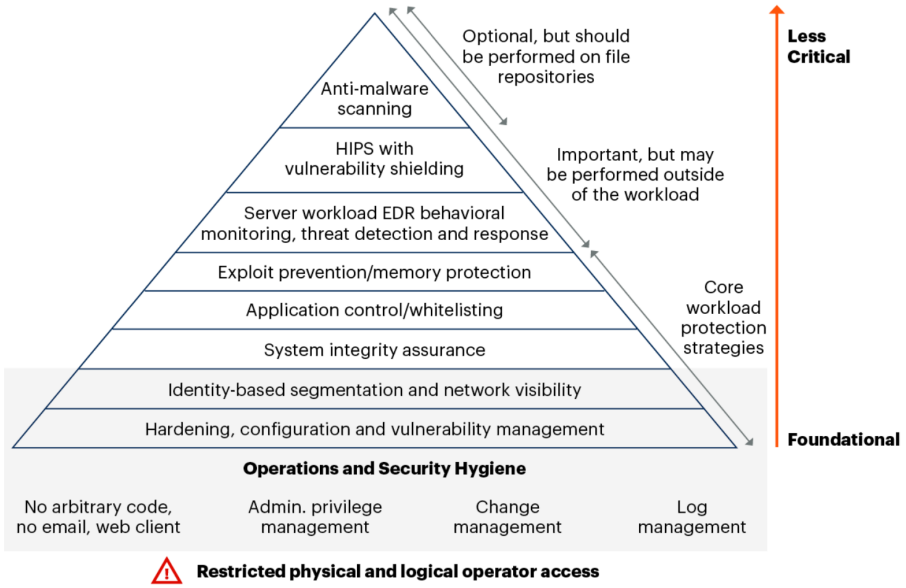
Sebbene esistano strumenti di sicurezza cloud nativi, le piattaforme di protezione dei carichi di lavoro nel cloud (CWPP) adattiva forniscono un controllo più completo e granulare a livello di processo, utente e nome di dominio completo. Funzionano anche su più provider cloud e on-premise, fornendo una protezione più efficace e completa per VM, container e carichi di lavoro senza server.

Strategie funzionali di protezione del carico di lavoro di base: mappatura dei controlli alle linee guida per la protezione del carico di lavoro nel cloud di Gartner

Una delle linee guida più seguite per la protezione dei carichi di lavoro nel cloud è stata scritta dagli esperti del settore di Gartner. Secondo Gartner, esiste una chiara gerarchia di controlli per la protezione dei carichi di lavoro cloud.

La piramide sottostante varia da fondamentale a meno critica, mostrando le strategie che Gartner considera fondamentali, così come quelle importanti ma facoltative. Idealmente, questi passaggi dovrebbero essere inclusi in ogni carico di lavoro, assicurando che la sicurezza sia integrata per ogni azione sul cloud.

Gerarchia basata sul rischio dei controlli di protezione del carico di lavoro[2]



Source: Gartner
716192_C

Gartner

Le linee guida per la protezione dei carichi di lavoro nel cloud di Gartner forniscono una chiara gerarchia dei controlli di sicurezza per le aziende

Ecco una spiegazione dettagliata delle strategie principali soddisfatte dalla nostra soluzione per aiutarvi a comprendere come integrare al meglio queste strategie nel vostro programma di protezione del data center ibrido o multicloud:

- **Rafforzamento, configurazione e gestione della vulnerabilità**
  Secondo Gartner, la strategia di protezione del carico di lavoro più fondamentale consiste nel configurare i sistemi e le impostazioni in modo appropriato per ridurre i rischi. Gli strumenti di gestione delle vulnerabilità migliorano ulteriormente la rimozione manuale dei vettori di attacco e automatizzano questo processo. È quindi possibile individuare e risolvere problemi software che potrebbero aprire le porte a malintenzionati.

- **Segmentazione basata sull'identità e sulla visibilità di rete**
  Gartner evidenzia la segmentazione e la visibilità della rete come strategie fondamentali per la protezione del cloud. La maggior parte delle organizzazioni utilizza firewall di nuova generazione on-premise, ma molte accettano una soluzione meno sicura quando passano al cloud.

  I team di sicurezza comprendono che i firewall di nuova generazione non sono sufficienti per la protezione del cloud, ma non sanno come ottenere informazioni eterogenee o il controllo in un ambiente di data center dinamico e ibrido. Quindi prendiamoci un momento per esaminare come farlo nel modo giusto.

  Innanzitutto, stabilite la visibilità. Una visibilità rapida si traduce in un time-to-value più rapido, poiché tutti gli stakeholder possono agire immediatamente e automaticamente in modo coordinato.

  Gli strumenti cloud nativi possono fornire mappe istantanee o registri testuali, ma questi sono generalmente corposi, incompleti o insufficienti. La soluzione migliore dovrebbe rilevare automaticamente tutte le applicazioni, il traffico e le dipendenze nella vostra rete. In questo modo, puoi visualizzare immediatamente l'intero ecosistema IT, anche quando la vostra azienda è distribuita in modo ibrido.

  La vostra soluzione dovrebbe anche includere un contesto potente, con informazioni approfondite e un quadro reale di ciò che sta accadendo nel data center. Per qualsiasi azienda che desideri gestire le operazioni di sicurezza e le richieste su larga scala, ogni flusso deve avere questo contesto, con la possibilità di eseguire un'analisi dettagliata dei singoli processi e delle comunicazioni del server. Ciò consente il tipo di processo decisionale basato sui dati che rafforza la creazione di policy.

  Dopo aver stabilito la visibilità e il contesto, create regole di segmentazione che si adattino alle best practice per la vostra azienda. Ad esempio, potreste separare gli ambienti di produzione e sviluppo o isolare i dati dei clienti per dimostrare la conformità. Potete anche sviluppare policy di microsegmentazione più granulari per fornire sicurezza e controllo approfonditi in un modo adatto al vostro specifico contesto aziendale.

- **Controllo/inserimento delle applicazioni in elenchi di elementi consentiti**
  Se il vostro team di sicurezza può impostare policy ed essere sicuro che verranno applicate ovunque, la transizione al cloud sarà più semplice e più sicura in ogni fase.

  Affidarsi solo a porte/IP non vi fornirà il livello di visibilità necessario per una protezione completa dei carichi di lavoro nel cloud. Il controllo rigoroso del traffico tra i componenti dell'applicazione è una parte fondamentale di una solida soluzione di microsegmentazione. Le migliori tecnologie offrono visibilità e controllo granulari, fino al processo dell'applicazione, all'utente e al nome di dominio completo, utilizzando dettagli come valori hash, checksum, percorso completo, risoluzioni e autenticazioni dell'archivio di identità.

  Alcune funzionalità aggiuntive che possono aumentare il controllo delle applicazioni includono:

  - Microsegmentazione che può limitare il movimento laterale sul cloud anche all'interno dello stesso cluster di applicazioni
  - Un approccio basato su un'unica posizione, che si traduce in una maggiore sicurezza
  - La possibilità di creare modelli sia di elenchi di elementi consentiti che di elenchi di elementi bloccati, entrambi in grado di impedire applicazioni o traffico non autorizzati e garantire che le connessioni importanti funzionino senza interruzioni

- **Prevenzione degli exploit/protezione della memoria**
  L'ultima strategia di protezione del server principale nella guida di Gartner per CWPP è la prevenzione degli exploit. Cercate uno strumento di sicurezza di microsegmentazione che fornisca il rilevamento e la risposta alle violazioni. Ciò vi consentirà di sostituire gli strumenti ridondanti e ridurre la complessità nel data center.

  Inoltre, come accennato in precedenza, la visibilità e la mappatura sono fondamentali. Disponendo di una mappa completa dell'intera rete, è facile individuare le vulnerabilità senza patch o comunicazioni dannose che agiscono fuori dalla norma. Se la vostra azienda ha stabilito una linea guida per il traffico legittimo, il movimento non autorizzato si distingue.

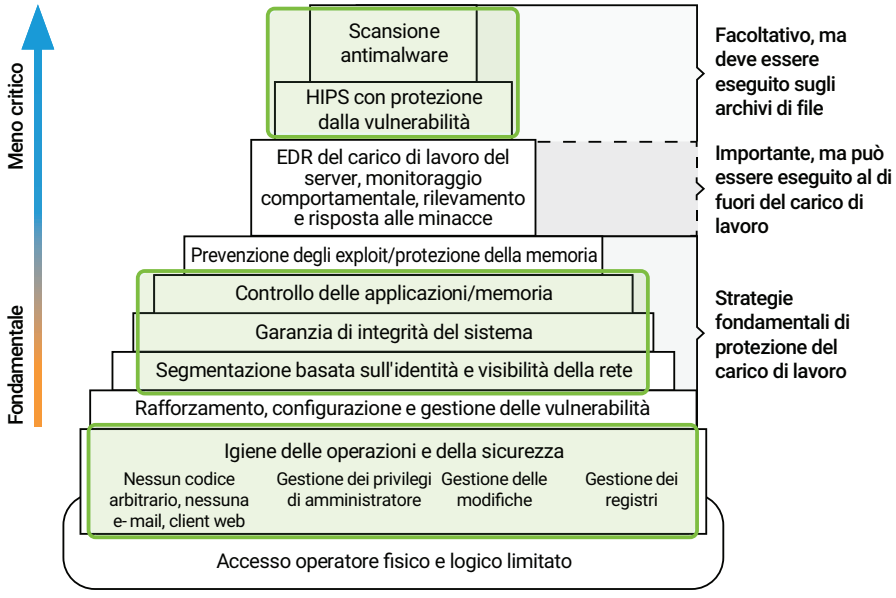
Altre importanti strategie di protezione

Le strategie del server principale sopra menzionate sono fondamentali per la sicurezza nel cloud. Allo stesso tempo, Gartner identifica diverse altre strategie che possono rafforzare il vostro ambiente ibrido o multicloud, tra cui il rilevamento e la risposta dell'endpoint (EDR) del carico di lavoro del server, il monitoraggio comportamentale e il rilevamento e risposta alle minacce (TDR).

EDR, monitoraggio comportamentale e TDR sono parti importanti del rilevamento delle violazioni e della risposta agli incidenti. Per gestire questi aspetti della sicurezza, cercate una soluzione che includa l'analisi della reputazione. Ciò vi consentirà di identificare più informazioni su un attacco, oltre a fornirvi funzionalità di elusione avanzate per indurre gli autori di attacchi a rivelare i loro metodi. In questo modo, potete rafforzare la vostra policy e procedura di sicurezza in futuro.

I dati sulla visibilità possono essere necessari per ottenere informazioni su un evento passato. I migliori provider archiviano i vostri dati per mesi, consentendo agli utenti di concentrarsi su applicazioni, processi e periodi di tempo specifici. I team di sicurezza possono anche utilizzare questi dati per indagini forensi e una migliore risposta agli incidenti.

Akamai Guardicore Segmentation: protezione dei carichi di lavoro del cloud ibrido nella gerarchia CWPP



Le aree evidenziate mostrano dove la nostra soluzione soddisfa i requisiti CWPP

Akamai Guardicore Segmentation colma le lacune inerenti agli strumenti di sicurezza cloud nativi, rispettando molti dei principi fondamentali stabiliti nel CWPP. Inoltre, la soluzione supporta in modo intelligente la visibilità, la creazione di policy e l'applicazione nei data center ibridi e multicloud.

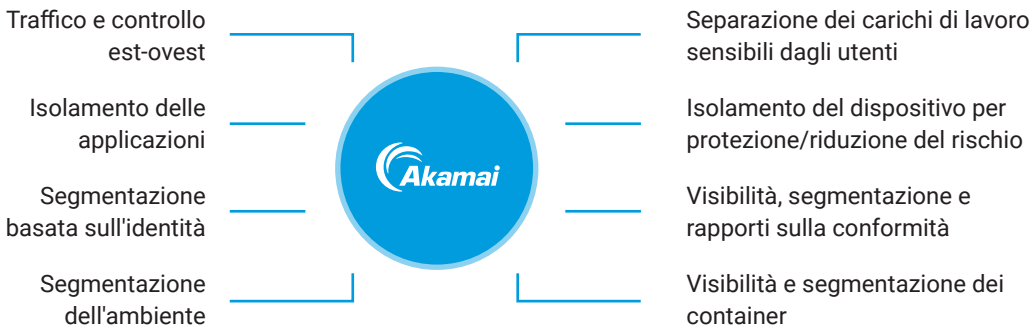
La nostra soluzione offre una visibilità approfondita: un'unica posizione che offre la visibilità sull'intero data center. Visualizzando il vostro data center ibrido nel suo complesso, potete comprendere a fondo le dipendenze delle applicazioni e l'effetto di qualsiasi policy sulla vostra rete. Ciò ha un potente effetto sulla migrazione al cloud, portando i clienti nel cloud in modo molto più rapido rispetto agli strumenti di visualizzazione nativi.

Questa visibilità approfondita vi consente di:

- Creare un elenco di attività da svolgere per il networking nel cloud
- Rilevare rapidamente le applicazioni su qualsiasi infrastruttura e le dipendenze delle applicazioni: una funzionalità fondamentale per una migrazione di successo
- Prevedere in anticipo i costi dell'infrastruttura e operativi
- Ottenere informazioni sulla migliore creazione di policy per ridurre il rischio dalle fasi di pianificazione della migrazione
- Sfruttare il percorso più breve, più semplice e più sicuro verso i vostri obiettivi aziendali per il cloud

La visibilità approfondita e basata sul contesto di Akamai Guardicore Segmentation si traduce in una comprensione rapida e completa dei vostri ambienti

La nostra visibilità completa include anche il contesto per ogni comunicazione e flusso, consentendovi di ridurre gli errori e la complessità generali. Potete raggruppare e filtrare le informazioni per supportare qualsiasi stakeholder che legge la mappa, fornendo facilmente le informazioni esatte di cui necessitano. Questa visibilità basata sul contesto riduce la necessità di fornitori di terze parti e creatori di policy, consentendo una rapida comprensione dei vostri ambienti in modo da poter creare, perfezionare o modificare le policy applicabili.



Esempi di casi di utilizzo di Akamai Guardicore Segmentation

Altre funzionalità critiche fornite dalla nostra soluzione includono:

- Policy di processo e a livello di servizio, che consentono una sicurezza più semplice e più efficace per protocolli dinamici come FTP o Spark
- Policy di microsegmentazione basate sull'identità, che applicano le connessioni in base all'utente che crea la connessione
- Policy basate su nomi di dominio completamente qualificati che consentono di raggiungere risorse a scalabilità automatica con indirizzi IP sono dinamici
- L'uso di tag del cloud pubblico esistenti come etichette, semplificando la visualizzazione del vostro data center ibrido o multicloud
- Creazione automatica di policy dal traffico osservato, in modo da ottenere una guida rapida ed esperta all'inizio del percorso di microsegmentazione

La nostra soluzione è indipendente dalla piattaforma e dall'infrastruttura e gestisce la visibilità e l'applicazione nell'intera infrastruttura

Ridurre la complessità è l'obiettivo finale quando si cerca di proteggere un data center ibrido. In risposta a questa esigenza, Akamai Guardicore Segmentation è indipendente dalla piattaforma e dall'infrastruttura, offrendo una visibilità dell'intera applicazione e della policy che segue il carico di lavoro, indipendentemente da dove risieda. Ogni regola viene applicata a tutti i carichi di lavoro, da vCenter e cloud pubblici (AWS, Azure, GCP) a server e container bare metal.

La riduzione della complessità non solo si traduce in una strategia di sicurezza più solida, ma alleggerisce anche il carico di lavoro IT e di sicurezza. Con i gruppi di sicurezza basati su cloud, necessitate di esperti del cloud nativo per ogni fornitore. Al contrario, con un'unica soluzione di sicurezza che gestisce la visibilità e l'applicazione nell'intera infrastruttura, sono necessari solo utenti certificati per una singola tecnologia.

Una piattaforma di protezione dei carichi di lavoro cloud a prova di futuro

Uno dei capisaldi della metodologia Agile e di DevOps è la capacità di fallire rapidamente e rapidamente e di passare facilmente alla "prossima grande novità". Sfortunatamente, e in qualche modo ironicamente, la migrazione dei carichi di lavoro tra diversi fornitori di servizi cloud può rallentarvi enormemente. Può anche essere difficile da realizzare mantenendo la sicurezza.

Bisogna essere in grado di mantenere aperte le opzioni. Se desiderate passare a un'infrastruttura multicloud o addirittura migrare completamente i carichi di lavoro a un nuovo provider cloud, ciò non dovrebbe avere un effetto negativo sulla sicurezza, né la sicurezza dovrebbe impedire tale passaggio.

Akamai Guardicore Segmentation vi consente di rimanere flessibili e di muovervi al ritmo dell'azienda, migrando i vostri carichi di lavoro con policy di sicurezza intatte. Non ostacola il processo o la flessibilità DevOps né richiede la riconfigurazione in ogni fase. Al contrario, fornisce le basi fondamenti di una piattaforma affidabile per la protezione dei carichi di lavoro nel cloud, per consentire la protezione del vostro data center ibrido o multicloud.

Akamai Guardicore Segmentation consente la migrazione sicura al cloud e tra i cloud e fornisce una visibilità impareggiabile con il contesto. Con la nostra soluzione, potete applicare le policy a livello di processo e utente e seguire i vostri carichi di lavoro ovunque.

Ora potete integrare la sicurezza come funzionalità in ogni fase del processo DevOps, consento la flessibilità e supportando le vostre attività aziendali. La vostra organizzazione sarà in grado di adottare funzionalità cloud all'avanguardia mantenendo la sicurezza al centro.

Per ulteriori informazioni sulla protezione degli ambienti cloud con la microsegmentazione leader del settore, visitate il sito all'indirizzo akamai.com/guardicore oggi stesso.

1 2022. Foundry (formerly IDG) Cloud Computing Study.

2 Market Guide for Cloud Workload Protection Platforms; scritto dagli analisti di Gartner Neil MacDonald e Tom Crow; pubblicato il 14 aprile 2020

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 05/23.