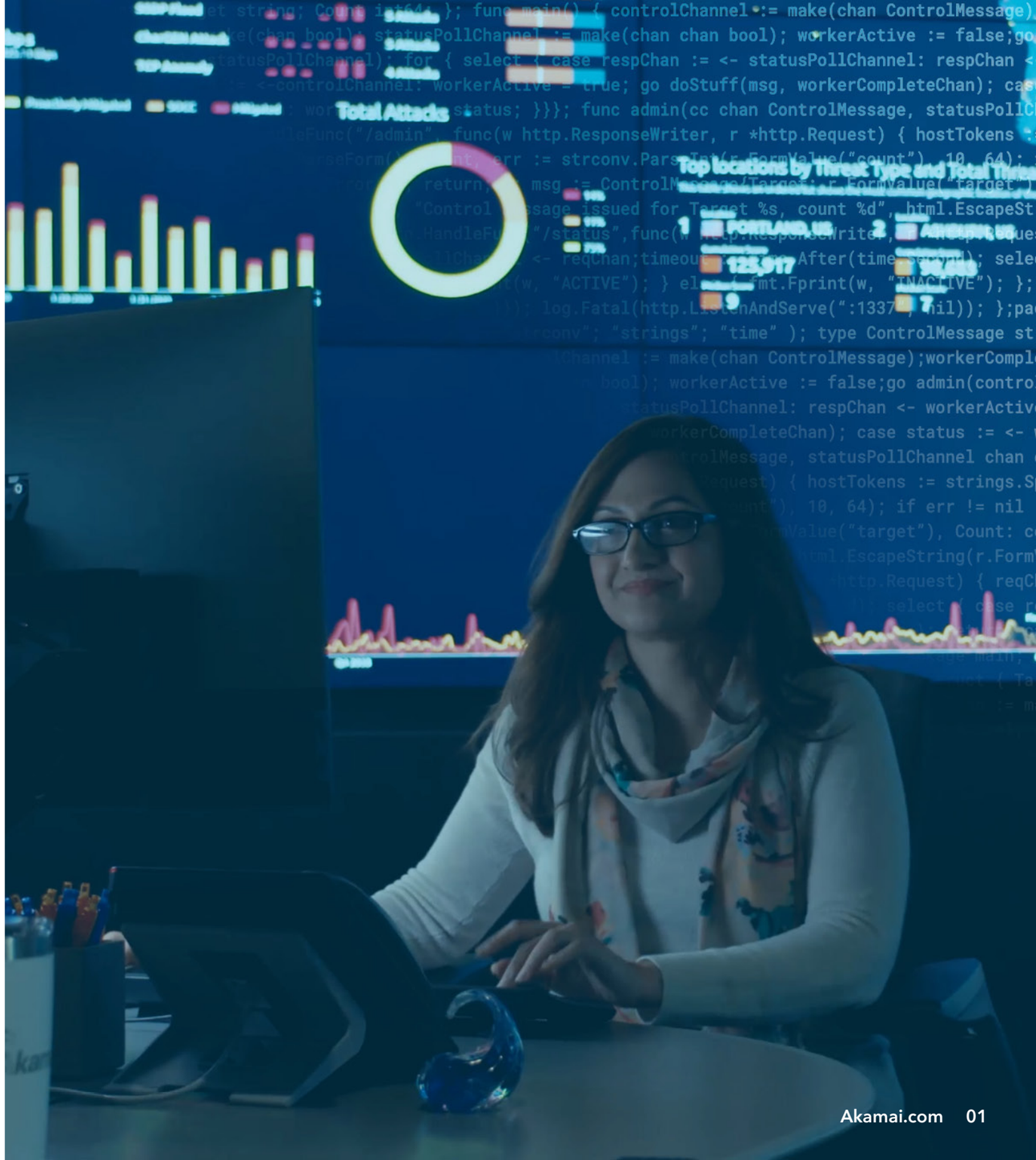
Difesa dagli attacchi DDoS nel cloud ibrido

E-BOOK

Difesa dagli attacchi DDoS nel cloud ibrido

Gli attacchi DDoS (Distributed Denial of Service), uno dei primi tipi di minacce informatiche, continuano a rappresentare un comune strumento di distruzione di massa, ponendo rischi alla sicurezza praticamente per qualsiasi tipo di azienda, dalle piccole imprese a quelle di grandi dimensioni. In realtà, secondo IDC, per gli attacchi DDoS si prevede un aumento del CAGR del 18% fino al 2023: ciò indica chiaramente che è il momento di investire in solidi controlli di mitigazione. Benché alcune organizzazioni ritengano che il rischio di subire un attacco DDoS sia basso, la crescente dipendenza dalla connessione a Internet per utilizzare applicazioni e servizi business-critical sottopone tutti al rischio di incorrere in problemi di downtime e riduzione delle performance, se la propria infrastruttura non è adeguatamente protetta.



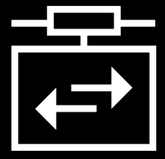
Una **minaccia** in continua evoluzione

La portata degli attacchi DDoS raddoppia ogni due anni e la sua complessità (il numero e la combinazione dei vettori di attacco) ha raggiunto livelli inimmaginabili prima d'ora. Poiché la disponibilità di applicazioni e reti è fondamentale per la continuità operativa, i criminali sono portati a sferrare attacchi DDoS volumetrici, basati su protocolli e a livello di applicazioni per causare problemi ad ogni potenziale point of failure, impedendo agli utenti finali l'accesso a beni e risorse su Internet.

NEL MIRINO DEGLI AUTORI DEGLI ATTACCHI DDoS RIENTRANO TUTTI I POTENZIALI POINT OF FAILURE, AD ESEMPIO:

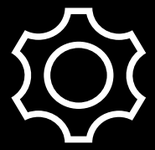
Siti web

Applicazioni web e altri servizi aziendali



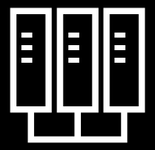
Concentratori VPN per un accesso remoto alle risorse aziendali

Controller SD-WAN



API (Application Programming Interface)

DNS (Domain Name System) e server di origine



Data center e infrastruttura di rete

Conducendo una fase di ricognizione degli spazi IP, delle applicazioni e degli ambienti da attaccare, gli autori degli attacchi possono determinare quali vettori DDoS saranno in grado di apportare il massimo danno potenziale alle infrastrutture di origine e ai servizi presenti in Internet. In presenza di una barriera facilmente raggirabile, i criminali si avvalgono di tutta una serie di strumenti e tecniche di attacco (pensiamo ai booter, agli attacchi DDoS su commissione, ecc.) come ausilio per rilevare i punti deboli o le vulnerabilità presenti nei sistemi di difesa aziendali.

> I criminali hanno diverse motivazioni, tra cui l'estorsione e la manipolazione finanziaria. Akamai sta osservando che gli attacchi sferrati a scopo di estorsione si stanno espandendo oltre il settore finanziario per colpire i servizi aziendali, nonché i settori gaming, viaggi e hospitality, high tech, logistica e retail.

- Roger Barranco, Vice President, Global Security Operations, Akamai

Le ripercussioni di un attacco DDoS si intensificano man mano che le organizzazioni cercano di scalare e proteggere le funzionalità di accesso remoto per garantire la produttività dei dipendenti e lo svolgimento delle consuete attività aziendali.

Le **conseguenze** di un attacco DDoS

Negli attacchi sferrati a livello di rete (livello 3) e trasporto (livello 4), gli attacchi volumetrici e quelli basati su protocolli tentano di congestionare la struttura Internet, sovraccaricare i server ed esaurire le voci delle tabelle di stato per rendere reti e servizi non disponibili. Negli attacchi basati sulle applicazioni (livello 7), i criminali tentano di interrompere web performance e user experience sferrando attacchi "nascosti e lenti", nonché flood HTTP per provocare problemi di downtime con conseguenze sui profitti.

Tuttavia, le ripercussioni sul downtime non influiscono solo sul costo associato alla mancata disponibilità delle applicazioni e dei servizi soggetti all'attacco. ***Secondo il Ponemon Institute, il costo annuo di un attacco DDoS per un'organizzazione corrisponde a 1,7 milioni di dollari***, una cifra determinata dall'aumento dell'assistenza tecnica necessaria, dall'utilizzo delle risorse richieste per risolvere i problemi, le escalation interne, le spese legali, le interruzioni operative e la perdita di produttività da parte dei dipendenti.

È chiaro che la posta in gioco è alta e può solo aumentare, visto l'incremento della migrazione alle infrastrutture del cloud ibrido.

Il cloud continua a rendere sempre più complessi i **sistemi di sicurezza**

Man mano che le organizzazioni smantellano i tradizionali data center spostando le applicazioni in ambienti sul cloud, le architetture di sicurezza diventano sempre più complesse. Molte organizzazioni si sforzano di capire come proteggere le risorse su Internet con lo stesso livello di difesa dagli attacchi DDoS utilizzato per le risorse che si trovano nel data center. Oltre alla complessità, molti IP gestiti sul cloud non rientrano nel controllo diretto di un'azienda, il che li lascia vulnerabili agli attacchi DDoS se non adeguatamente protetti.

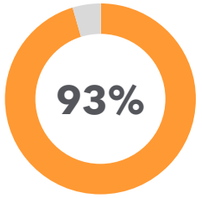
Inoltre, ben consapevoli di questa migrazione accelerata verso strutture di colocation e sul cloud pubblico, i criminali cercano in tutti i modi di sfruttare le vulnerabilità del sistema e dell'architettura di un'organizzazione, causate dalle incoerenze nei requisiti e nelle policy di sicurezza, nonché dalle difficoltà di risoluzione dei problemi legati alla separazione e alla frammentazione delle infrastrutture sul cloud.

IL PUNTO

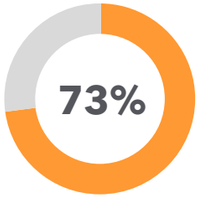
Le aziende moderne hanno bisogno di sistemi di difesa adattivi in grado di proteggere vari servizi e risorse sul web, indipendentemente dalla loro posizione. Inoltre, visto che più del 93% delle imprese (< 1.000 dipendenti) hanno adottato una strategia multicloud, questo è il momento adatto per chiudere una volta per tutte le falle dei sistemi di difesa causate dalle complessità dell'infrastruttura.[1]

[1] *https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020*

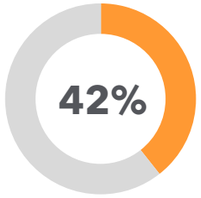
La responsabilità della sicurezza negli ambienti basati sul cloud pubblico può risultare incoerente da un fornitore all'altro, poiché molte organizzazioni suppongono erroneamente di poterli lasciare sguarniti. Ad esempio, il 73% delle aziende che sono state sottoposte ad un sondaggio condotto da IBM ritiene che i fornitori di servizi sul cloud pubblico (CSP) sono i principali responsabili della sicurezza dei servizi SaaS (Software-as-a-Service), mentre il 42% pensa che i CSP siano principalmente responsabili della sicurezza dei servizi IaaS (Infrastructure-as-a-Service) sul cloud. Questa mancanza di chiarezza circa le responsabilità relative al controllo della sicurezza può condurre ad una violazione: un rischio che nessuna organizzazione è disposta ad accettare.



Percentuale di aziende che hanno adottato una strategia multicloud



Percentuale di partecipanti al sondaggio secondo cui i CSP sono responsabili della sicurezza dei servizi SaaS



Percentuale di partecipanti al sondaggio secondo cui i CSP sono responsabili della sicurezza dei servizi IaaS sul cloud

In un recente articolo, Forrester ha sottolineato il fatto che la maggior parte delle organizzazioni scelgono attualmente una strategia ibrida, che si basa cioè sia su fornitori di servizi sul cloud pubblico che sulla gestione dei carichi di lavoro in sede. Di conseguenza, la società di analisi consiglia di scegliere un fornitore di soluzioni per la mitigazione degli attacchi DDoS in grado di garantire una protezione in caso di architetture ibride.

Non tutte le soluzioni di mitigazione degli attacchi DDoS sono **progettate in modo uguale**

Poiché si continua ad investire nell'infrastruttura sul cloud, i team addetti alla sicurezza si trovano ancora di fronte alla sfida di garantire controlli coerenti in ambienti ibridi. Inoltre, visto che diventa sempre più difficile proteggere le applicazioni implementate in diverse infrastrutture di back-end sul cloud, molte organizzazioni cercano un unico punto di controllo in grado di gestire i sistemi di difesa. Poiché lo stack tecnologico dedicato alla sicurezza diventa sempre più complesso, molte organizzazioni desiderano gestire tutto da un'unica posizione, non solo per una migliore visibilità, ma anche per una generazione semplificata dei rapporti da poter trasmettere tramite le API ai sistemi di correlazione dei dati degli eventi.

Per risolvere questo problema, le organizzazioni ora si rivolgono a fornitori di soluzioni per la sicurezza DDoS sul cloud che facilitano, senza ostacolare, le loro strategie di migrazione sul cloud ibrido. Le organizzazioni hanno bisogno di sistemi di difesa scalabili e reattivi, indipendentemente dalla posizione in cui risiedono i servizi aziendali, per rispondere direttamente all'aumento della complessità operativa richiesta per integrare, implementare e gestire i sistemi di difesa DDoS nell'ambiente di un CSP. Inoltre, la situazione si fa ancora più complessa se consideriamo le numerose risorse dislocate su più cloud.

A complicare ulteriormente le cose, molte soluzioni per la mitigazione degli attacchi DDoS in sede fornite dai CSP sono prive di alcune aree chiave (visibilità, SLA e generazione dei rapporti), tutte fondamentali per l'utilizzo da parte degli esperti di sicurezza aziendale di oggi.

Per i team addetti alla sicurezza, la chiave è come ottenere visibilità e informazioni utili per ottimizzare la preparazione e la risposta ai problemi. Alcune soluzioni DDoS offerte dai CSP offrono una trasparenza minima (se non nulla) in termini di generazione di rapporti, visibilità e analisi post-attacco, pertanto non meraviglia il fatto che molti si riferiscano ai CSP come alla "scatola nera" dell'analisi e della generazione di rapporti.

Inoltre, alcuni CSP non offrono SLA time-to-mitigate, ma invece offrono crediti di servizio all'organizzazione che ha subito un attacco. Nei casi in cui il fattore tempo è fondamentale, le organizzazioni devono avere la certezza che il loro fornitore si assumerà l'impegno di mantenere la disponibilità e i tempi di attività richiesti senza compromettere le performance.

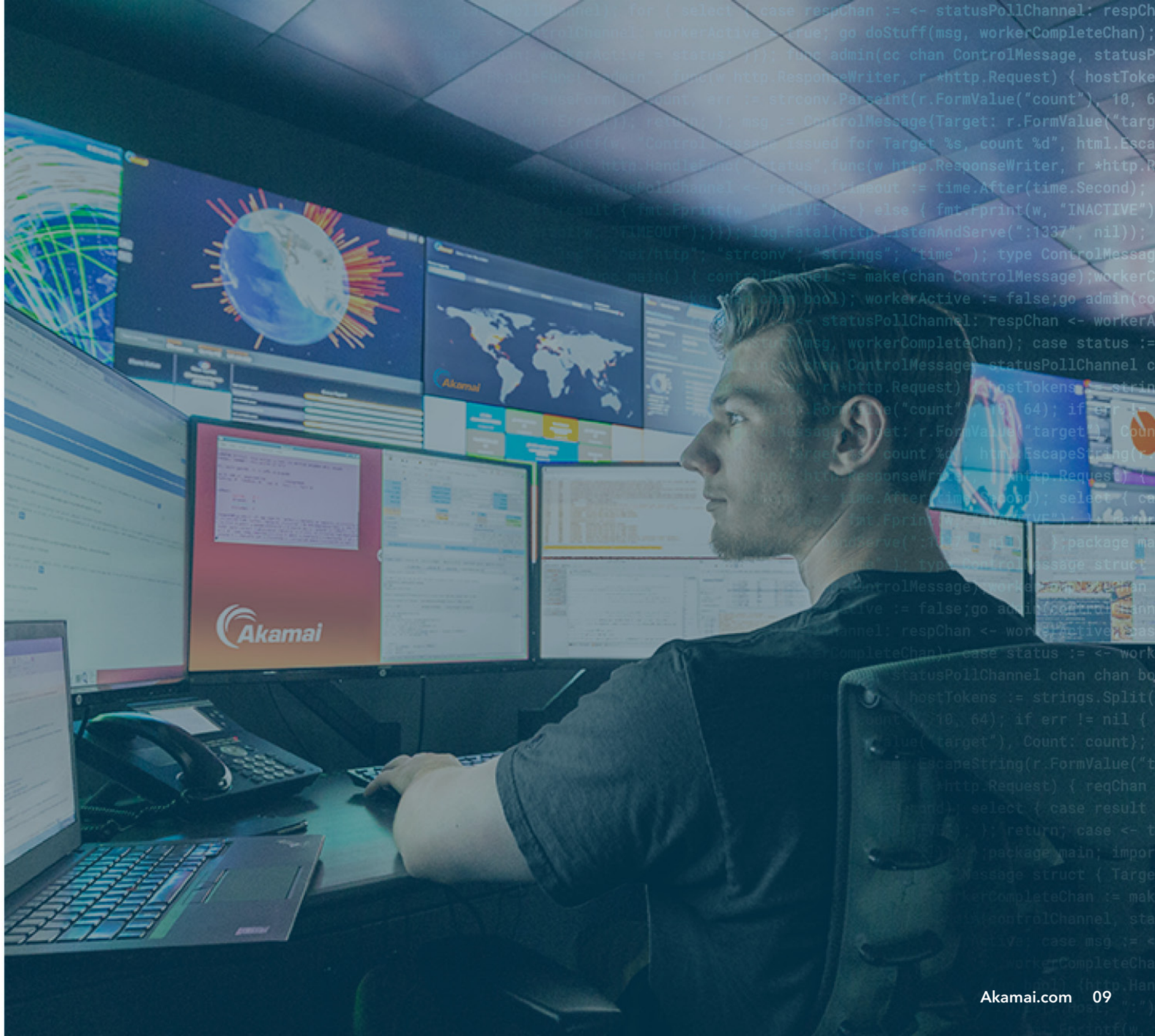
Infine, molti CSP non forniscono un accesso on-demand al SOC (centro operativo per la sicurezza) globale 24/7 oltre all'assistenza prima, durante e dopo l'attacco, che viene fornita come standard dai principali fornitori di soluzioni per la mitigazione degli attacchi DDoS basati sul cloud. Se fornito, questo servizio aggiuntivo risulta spesso più costoso rispetto ad una soluzione per la mitigazione degli attacchi DDoS offerta dai principali fornitori del settore. Con una soluzione per la protezione dagli attacchi DDoS completamente gestita, i fornitori di servizi agiscono come un'estensione del team addetto alla risoluzione dei problemi di un'organizzazione, offrendo, al contempo, le competenze degli esperti necessarie per rispondere rapidamente agli eventi DDoS.

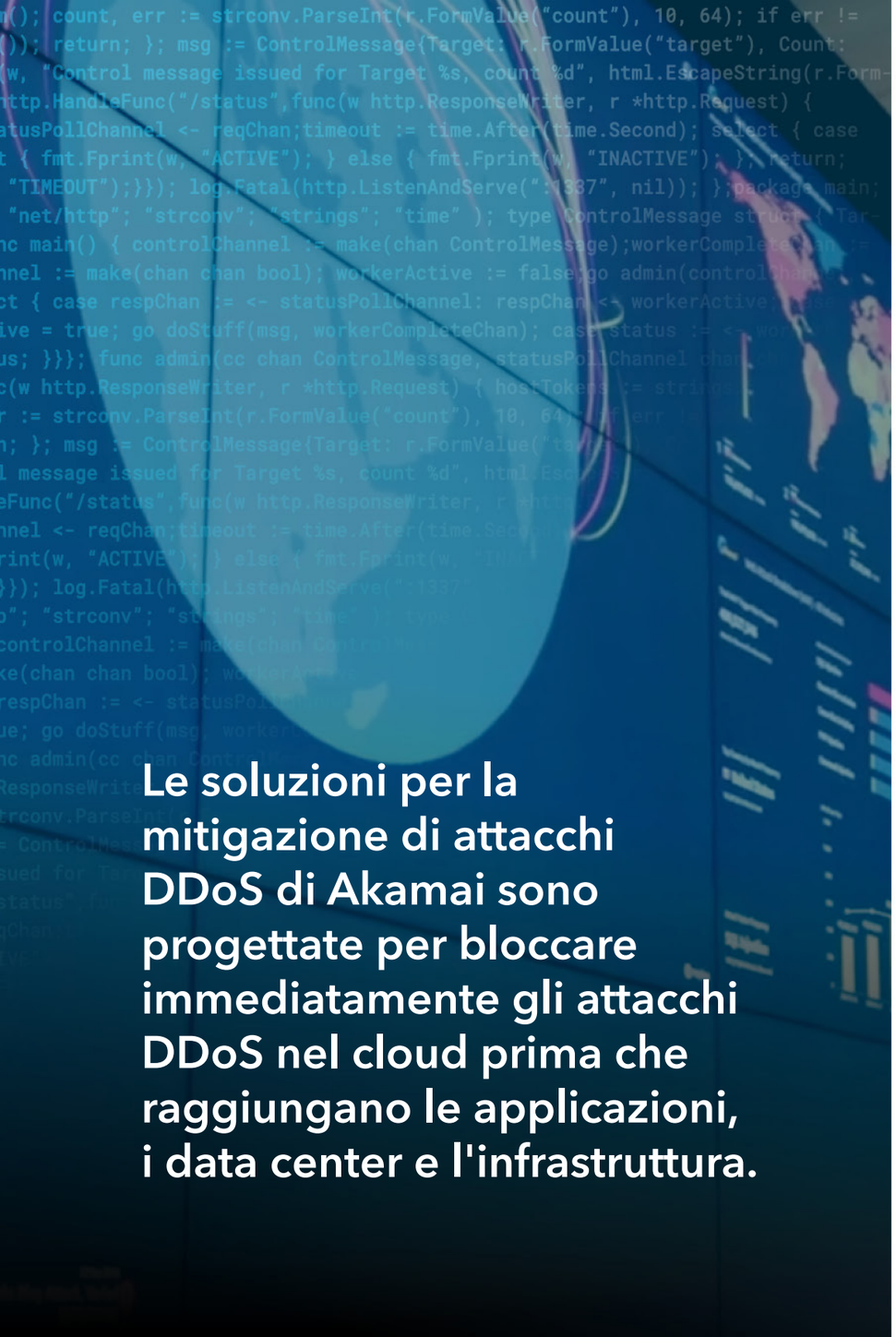
Nell'attuale panorama delle minacce, è chiaro che le aziende moderne si rivolgono a partner per la mitigazione degli attacchi DDoS in grado di supportare un'agevole experience di sicurezza in ambienti ibridi, il tutto riducendo anche la complessità della superficie di attacco.

Un partner per la mitigazione degli attacchi DDoS deve facilitare, non ostacolare, l'adozione di una strategia per il cloud al fine di aiutare a risolvere i problemi legati alla sicurezza.

Mitigazione degli attacchi DDoS **appositamente progettata** con Akamai

Così come le organizzazioni hanno bisogno di una strategia per il cloud end-to-end, devono anche considerare l'adozione di un adeguato sistema di protezione dagli attacchi DDoS. Adottando un approccio olistico, Akamai agisce come una prima linea di difesa, fornendo la protezione richiesta con strategie che si avvalgono di un edge dedicato, un DNS distribuito e la mitigazione sul cloud nell'intento di prevenire danni collaterali e single point of failure. A differenza di altre architetture di fornitori di soluzioni per la sicurezza nel cloud, concepite come prodotti "all-in-one", i cloud DDoS appositamente progettati di Akamai offrono un miglior livello di resilienza, una capacità di scrubbing dedicata e una qualità di mitigazione superiore per soddisfare gli specifici requisiti delle applicazioni web o dei servizi basati su Internet.





Le soluzioni per la mitigazione di attacchi DDoS di Akamai sono progettate per bloccare immediatamente gli attacchi DDoS nel cloud prima che raggiungano le applicazioni, i data center e l'infrastruttura.

DIFESA SULL'EDGE

L'edge di Akamai (CDN) distribuisce e accelera il traffico web tramite i protocolli HTTP e HTTPS. Ogni edge server di Akamai funge da proxy inverso, inoltrando il traffico HTTP/S legittimo sulle porte 80 e 443 e bloccando il resto del traffico sull'edge della rete. In tal modo, ogni cliente Akamai usufruisce automaticamente di una mitigazione immediata di tutti gli attacchi DDoS sferrati a livello della rete come funzione integrata nella web delivery.

DIFESA SUL DNS

La stessa tecnologia viene applicata al servizio DNS autoritativo di Akamai (Edge DNS), che blocca immediatamente tutto il traffico non presente sulla porta 53. A differenza di altre soluzioni DNS, Akamai ha progettato specificamente Edge DNS per la disponibilità e la resilienza contro gli attacchi DDoS, in aggiunta alle performance, con ridondanze delle architetture a livelli multipli, inclusi server dei nomi, punti di presenza, reti e anche i cloud IP Anycast segmentati.

DIFESA DELLO SCRUBBING SU CLOUD

In quanto servizio di scrubbing su cloud collaudato sul campo, Prolexic protegge tutti i data center e l'infrastruttura basata su Internet dagli attacchi DDoS su tutte le porte e tutti i protocolli. Instradando il traffico legittimo e quello dannoso tramite Prolexic, vengono costruiti modelli di sicurezza positivi e negativi in grado di mitigare in modo proattivo e immediato gli attacchi DDoS con un'elevata accuratezza. Gli esperti del SOCC (Security Operations Command Center) di Akamai agiscono come un'estensione del team addetto alla risoluzione dei problemi di un cliente per bilanciare le operazioni automatizzate di rilevamento e risposta con l'engagement dell'utente.

Perché Akamai

Akamai dispone dei cloud per la mitigazione degli attacchi DDoS più grandi e avanzati al mondo. Sia per la protezione di singole applicazioni, di interi data center o del DNS autoritativo, Akamai ha progettato la mitigazione degli attacchi DDoS con i massimi livelli di capacità, resilienza e mitigazione disponibili.

Siamo riusciti a mitigare alcuni dei più vasti attacchi DDoS al mondo. I nostri controlli di mitigazione proattivi offrono una reale mitigazione immediata con uno SLA leader del settore. Inoltre, siamo in grado di fornire servizi di protezione dagli attacchi DDoS per più clienti e contrastare più attacchi DDoS contemporaneamente.

Akamai

Poiché i vettori di attacco DDoS continuano a cambiare con una portata sempre maggiore, un fornitore deve continuamente investire, sviluppare e implementare strumenti e regole tali da rilevare, gestire e mitigare gli attacchi. Akamai si impegna nell'intento di stare un passo avanti rispetto alle minacce mitigando gli attacchi tempestivamente.

La mitigazione degli attacchi DDoS deve potenziare la strategia per il cloud. A tal proposito, l'Akamai Intelligent Edge Platform offre sistemi di difesa dagli attacchi DDoS, aiutando i clienti a estendere la protezione alle loro attività principali, al cloud e sull'edge, minimizzando i rischi e fornendo, al contempo, flessibilità per le future evoluzioni nelle strategie per il cloud.

Contattateci per scoprire come possiamo **proteggere** le vostre attività aziendali

Ulteriori informazioni

*Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24/7/365. Per scoprire perché i principali brand del mondo si affidano ad Akamai, visitate il sito **www.akamai.com** o **blogs.akamai.com** e seguite **@Akamai** su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo **www.akamai.com/locations**. Data di pubblicazione: 11/20.*