Protección frente a DDoS en un mundo de nube híbrida

Tabla de contenido

Los ataques DDoS siguen evolucionando

Los ataques distribuidos de denegación de servicio (DDoS), uno de los tipos de ciberamenazas más antiguos, siguen evolucionando y ahora se han convertido en una herramienta muy sofisticada en manos de los ciberdelincuentes y hacktivistas que tienen una motivación ideológica. De hecho, los ataques DDoS plantean riesgos de seguridad no solo para las grandes y pequeñas empresas, sino también para la infraestructura pública esencial en ámbitos como la atención sanitaria, la energía y los servicios públicos, y la educación.

Esta dinámica se complica aún más debido a que las instituciones públicas y privadas están adoptando más recursos de cloud computing. Cuando estas organizaciones combinan la nube con sus recursos locales previos, el entorno híbrido resultante se vuelve mucho más complejo. Las aplicaciones, las interfaces de programación de aplicaciones (API), los datos, los microservicios y las cargas de trabajo deben moverse ahora por un entorno fragmentado. Las diferentes arquitecturas que se combinan en ese tipo de entornos crean nuevas vulnerabilidades y una superficie de ataque fracturada que los ciberdelincuentes pueden aprovechar para lanzar ataques DDoS cada vez más sofisticados y dañinos.

Las organizaciones se esfuerzan por garantizar la protección de su infraestructura digital. Necesitan una plataforma de protección contra DDoS integrada e híbrida que pueda defender su infraestructura local (nube privada) frente a ataques DDoS breves pero intensos, y que también aproveche la escala y la capacidad de barrido en la nube para ataques DDoS volumétricos de gran tamaño.

Las tendencias apuntan a que la potencia y la frecuencia de los ataques DDoS seguirá en aumento. En febrero de 2023, Akamai mitigó el mayor ataque DDoS lanzado hasta la fecha contra un cliente de Prolexic con sede en la región de Asia-Pacífico (APAC), con un tráfico de ataque pico de 900,1 gigabits por segundo y 158,2 millones de paquetes por segundo (Mpps). Ocurrió solo unos meses después del mayor ataque DDoS de la historia contra un cliente de Akamai Prolexic en Europa, en el que el tráfico se disparó bruscamente hasta los 704,8 Mpps en un agresivo intento por interrumpir las operaciones empresariales de la organización. A ello hay que sumar el mayor ataque DDoS que Akamai ha mitigado hasta la fecha: un ataque distribuido en todo el mundo, de 1,44 terabits por segundo (Tbps) y 385 Mpps que duró casi dos horas. De hecho, según nuestra información sobre el tráfico y los patrones de ataque, Akamai determinó que, a lo largo de 2023, los ataques DDoS se volvieron más frecuentes, largos y sofisticados (con diferentes vectores), y que se centraron en objetivos horizontales (es decir, que atacaron varios destinos IP en el mismo evento).

La amenaza creciente

La mayoría de los ataques DDoS actuales son ataques multivectoriales, que a menudo emplean más de 10 vectores de ataque para saturar los sistemas y plataformas de protección contra DDoS rudimentarios. De hecho, según la inteligencia interna antiamenazas de Akamai, de 2022 a 2023, el número de ataques DDoS horizontales o multidestino se duplicó. Por otro lado, el tamaño, la escala y la duración generales de los ataques DDoS volumétricos en 2023 fueron los más altos registrados.

La planificación de la seguridad para las organizaciones se complica aún más debido a la evolución de varias tácticas diferentes que los atacantes utilizan en conjunto con los ataques volumétricos tradicionales.

Los atacantes DDoS aprovecharán cualquier posible punto de fallo, como:

- Sitios web
- Aplicaciones web y otros servicios empresariales
- Concentradores de VPN para acceso remoto a recursos corporativos
- Controladores SD-WAN
- Interfaces de programación de aplicaciones (API)
- Sistema de nombres de dominio (DNS) y servidores de origen
- Infraestructura de red y centro de datos

Infraestructura de DNS

Los ataques DDoS a la infraestructura de DNS de las organizaciones se han vuelto cada vez más comunes, especialmente, los ataques NXDOMAIN (también conocidos como ataques de subdominio pseudoaleatorios, ataques "DNS Water Torture" o ataques de agotamiento de recursos del DNS). Más del 60 % de los ataques DDoS mitigados por Akamai en 2023 tenían un componente DNS, y los ataques NXDOMAIN constituían aproximadamente la mitad de esas ofensivas DDoS al DNS. Estos ataques representan un riesgo significativo para los resultados y la reputación de las empresas, porque si su DNS se cae, su presencia online desaparece.

Los ataques a la capa de aplicación

Los ataques DDoS a la capa de aplicación (capa 7) se han vuelto más sofisticados, ya que los atacantes están desarrollando sus tácticas para aprovechar la lógica y los flujos de trabajo aparentemente benignos. Una vulnerabilidad HTTP/2 detectada en 2023 dio lugar al mayor ataque DDoS de capa 7 registrado hasta la fecha.

DDoS como servicio

Hay grupos cibercriminales organizados, como Anonymous Sudan y Killnet, que ofrecen servicios de DDoS. En tal contexto, los grupos prestan esos servicios, que normalmente consisten en una botnet, a cambio de una tarifa, y llevan a cabo ataques en nombre de un cliente. Estos servicios contratados de DDoS pueden ser extremadamente rentables para grupos con determinadas motivaciones.

Ransomware + DDoS = RDDoS

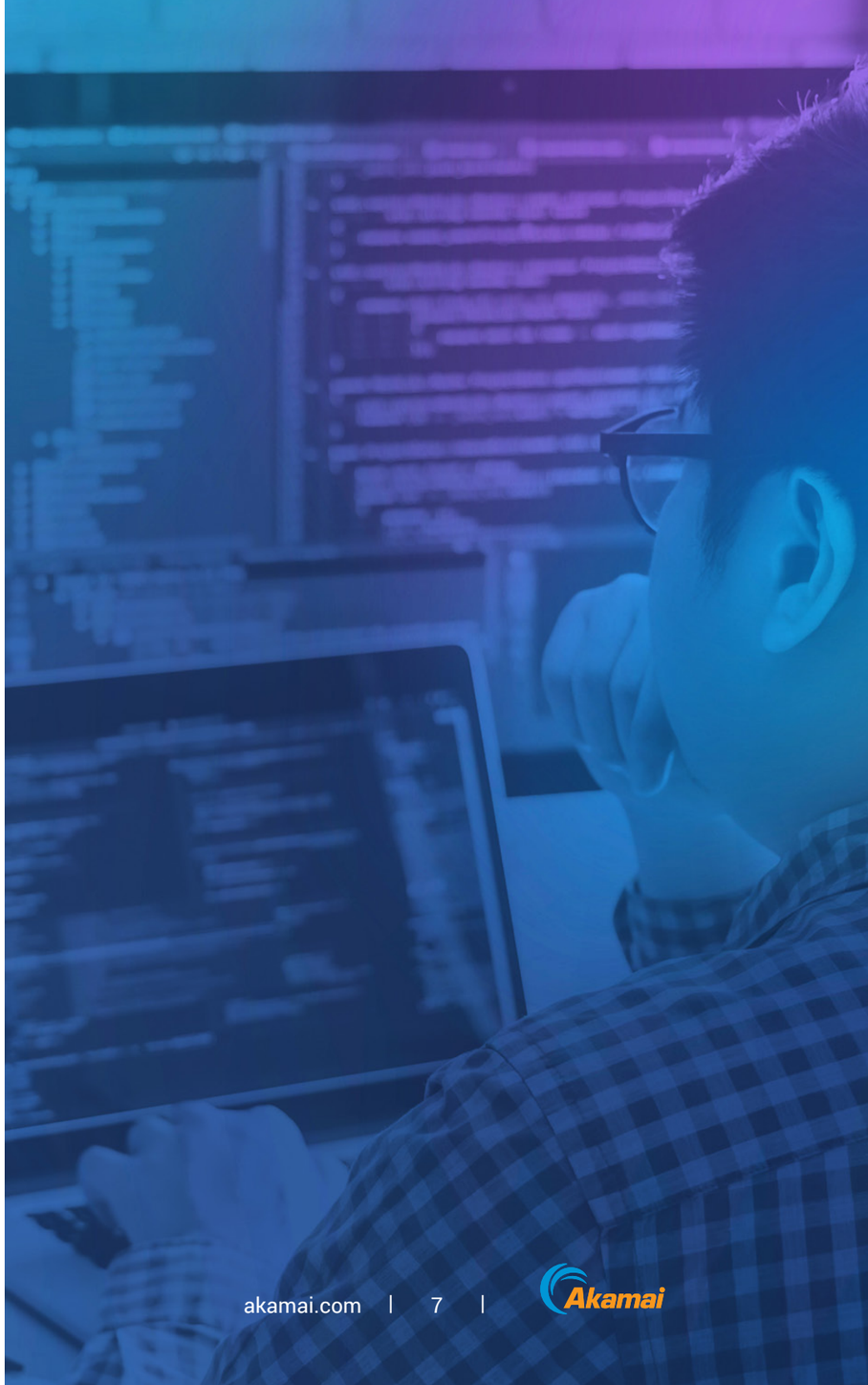
La disponibilidad de tácticas como los ataques DDoS como servicio también facilitan a los atacantes el uso de este tipo de ataques como cortina de humo para distraer a los equipos de seguridad. Mientras tanto, lanzan simultáneamente un ataque de ransomware o triple extorsión. Estos ataques se denominan DDoS de rescate (RDDoS).

Las consecuencias de un ataque DDoS

En los ataques DDoS a la capa de red (capa 3) y de transporte (capa 4), los ataques volumétricos y basados en protocolos intentan llenar los canales de Internet y saturar los servidores y las entradas de la tabla de estado para que las redes y los servicios no estén disponibles. Con los ataques de capa 7, los atacantes tienen como objetivo interrumpir el rendimiento web y la experiencia del usuario a través de vectores como los ataques bajos y lentos y las inundaciones HTTP para producir un tiempo de inactividad que afecte a los resultados. Los ataques DDoS al DNS pueden ser un poco más complejos, ya que, en función del tipo de ataque, podrían afectar a diferentes capas de la red de una organización. Por ejemplo, los ataques DDoS de reflexión y amplificación de DNS pueden producir tráfico en las capas 3 y 4 de la red de una empresa, mientras que los tipos de inundación NXDOMAIN o DNS de DDoS suelen atacar la capa de aplicación de una red.

Las repercusiones del tiempo de inactividad van mucho más allá de que se inhabiliten los servicios y las aplicaciones dejen de estar disponibles. Según Ponemon Institute, el coste promedio de un ataque DDoS a una organización es de 1,7 millones de USD al año por un incremento de la carga de trabajo para los servicios de soporte técnico, el uso de recursos de respuesta a incidentes, las derivaciones internas, los costes legales, las interrupciones operativas y la pérdida de productividad de los empleados. Además, para las empresas orientadas al consumidor, como las instituciones de servicios financieros, las empresas de juegos y medios de comunicación y las organizaciones de comercio electrónico, el hecho de estar fuera de línea no solo puede producir daños financieros, sino que, lo que es más importante, puede infligir daños irreparables a la reputación.

Está claro que hay mucho en juego, y cada vez más, con el aumento de la migración a las infraestructuras de nube híbrida.

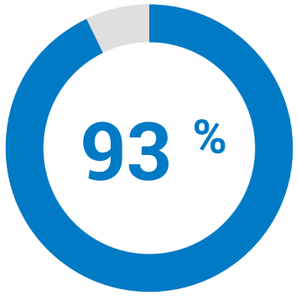


Los entornos híbridos y multinube siguen complicando la seguridad

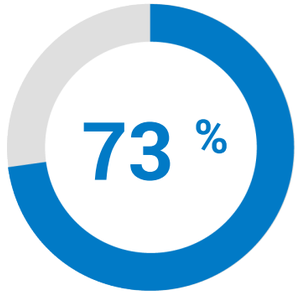
A medida que las organizaciones mantienen algunas cargas de trabajo en centros de datos locales o nubes privadas y trasladan otras aplicaciones a entornos alojados en la nube pública, este enfoque híbrido de la infraestructura hace que garantizar una seguridad sólida sea extremadamente complejo. Del mismo modo, las empresas suelen tener una infraestructura de DNS híbrida en la que algunas de sus zonas de DNS autoritativas se gestionan en la nube, mientras que las zonas restantes se administran mediante servidores de nombres locales y balanceadores de carga de servidores globales (GSLB). Hay razones por las que las organizaciones podrían seguir queriendo mantener cierta infraestructura de DNS local. Por ejemplo, es posible que ya hayan invertido un capital considerable en la configuración de una infraestructura local para satisfacer ciertos requisitos de cumplimiento. La complejidad de migrar todo el DNS a la nube puede no ser económicamente viable.

Los atacantes son muy conscientes de las vulnerabilidades que surgen de un entorno tan fragmentado y buscan, por todos modos, formas de explotar los puntos débiles de la arquitectura y la estrategia de seguridad de las organizaciones que tienen políticas y requisitos de seguridad incoherentes. Su objetivo es aprovechar las dificultades a la hora de solucionar problemas en infraestructuras alojadas en la nube dispares y fragmentadas.

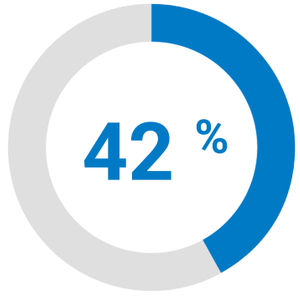
Lamentablemente, la responsabilidad de la seguridad en los entornos de nube pública puede ser contradictoria entre proveedores, y muchas organizaciones hacen falsas suposiciones que podrían dejarlas expuestas. Por ejemplo, el 73 % de las empresas entrevistadas en una encuesta de IBM cree que los proveedores de servicios en la nube pública (CSP) son los principales responsables de proteger el software como servicio (SaaS), mientras que el 42 % considera que los CSP son los responsables principalmente de proteger la infraestructura como servicio (IaaS). Esta ausencia de conocimiento en torno a la responsabilidad del control de la seguridad puede dar lugar a un riesgo que ninguna organización debería estar dispuesta a aceptar.



Usa una estrategia multinube



Cree que los CSP públicos son responsables de proteger el SaaS



Cree que los CSP son responsables de proteger la IaaS en la nube

Las organizaciones recurren a proveedores de seguridad frente a DDoS que les ofrezcan una plataforma integrada, altamente escalable y completa de protección contra este tipo de ataques, capaz de defender sus aplicaciones, API y DNS, así como la infraestructura subyacente en la que se apoyan.

No todos los sistemas de mitigación de DDoS son iguales

Dado que las empresas siguen invirtiendo en infraestructura de nube, garantizar controles coherentes que abarquen los entornos híbridos será un desafío para los equipos de seguridad. Además, a medida que las aplicaciones implementadas en diversas infraestructuras de nube de back-end se vuelven más difíciles de proteger, muchas organizaciones buscan tener un único punto de control para organizar las defensas.

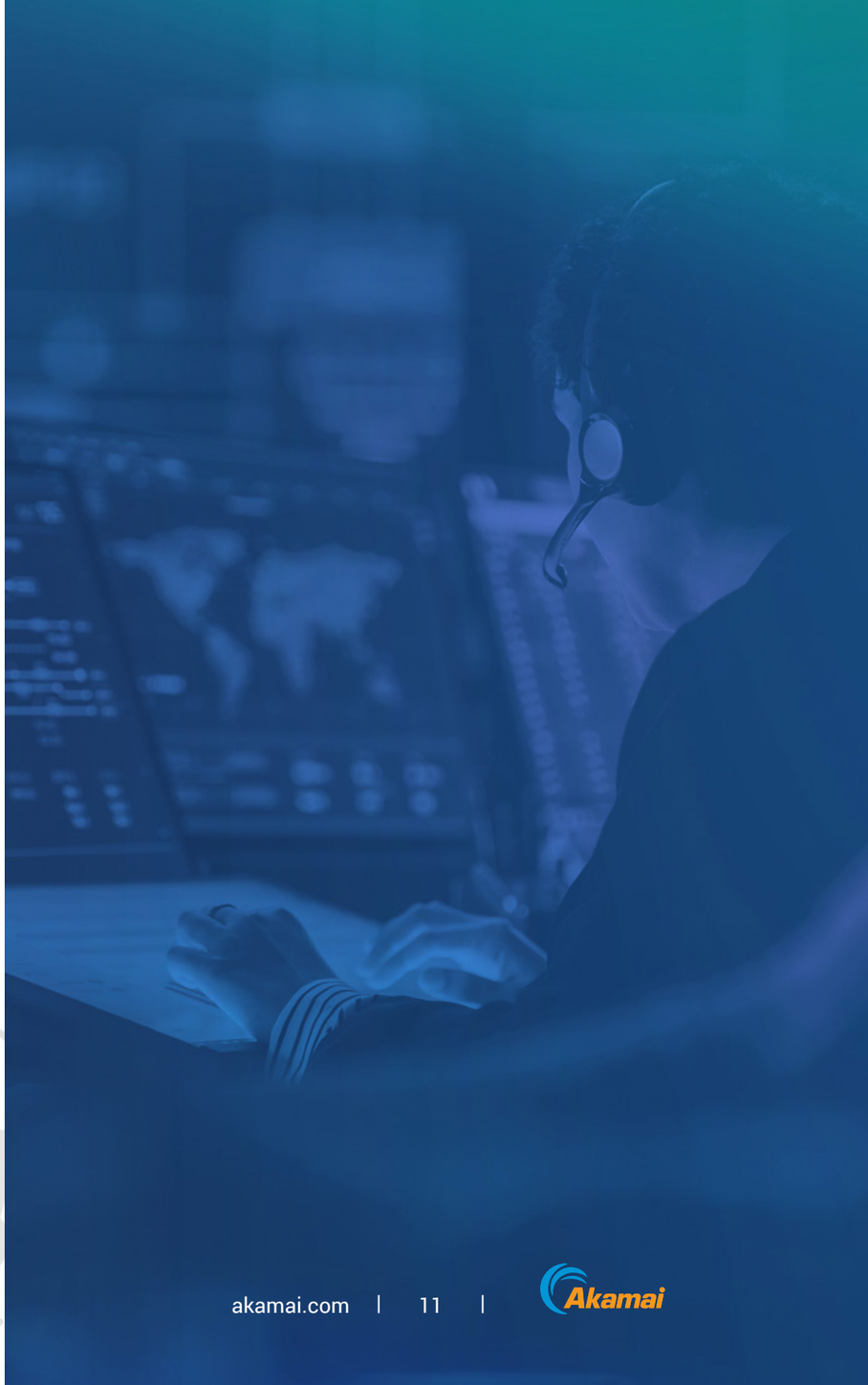
Con la creciente complejidad de la pila tecnológica de seguridad, son muy numerosas las que quieren tener una visión consolidada de su entorno, no solo para optimizar la visibilidad, sino también para generar fácilmente informes que puedan transferirse a través de las API a sistemas de correlación de datos de eventos.

Para resolver este problema, las organizaciones recurren a proveedores de seguridad frente a DDoS que les ofrezcan una plataforma integrada, altamente escalable y completa de protección contra este tipo de ataques, capaz de defender sus aplicaciones, API, y DNS, así como la infraestructura subyacente en la que se apoyan. Quieren tener defensas escalables y adaptables sin importar dónde se encuentren los servicios empresariales, ya sea en la nube, en un entorno híbrido o en uno local. Se trata de una respuesta directa al aumento de la complejidad operativa necesaria para integrar, implementar y gestionar la protección frente a DDoS en el entorno de un único CSP. Al tener muchos activos web ubicados en distintas nubes privadas y públicas, las cosas pueden complicarse muy rápido.

Para aumentar aún más la presión, muchas soluciones de mitigación de DDoS que ofrecen los CSP se quedan cortas en áreas clave: visibilidad, acuerdos de nivel de servicio (SLA) y generación de informes, todas ellas fundamentales para los expertos en protección de hoy en día.

Para los equipos de seguridad, todo gira en torno a la visibilidad y la obtención de información útil para optimizar la preparación y la respuesta ante incidentes. Algunas soluciones contra DDoS de los CSP ofrecen poca o ninguna transparencia en términos de informes, visibilidad y análisis posterior al ataque. No es de extrañar que muchos equipos se refieran a los CSP como la caja negra de los análisis e informes. Aunque algunos CSP permiten al equipo de seguridad de una organización establecer controles y mantener la soberanía sobre los entornos específicos del cliente, normalmente rechazan asumir cualquier tipo de responsabilidad por el tráfico DDoS y terminan cobrando a los clientes por el volumen astronómico de tráfico malicioso que conlleva un ataque de este tipo, tanto si va dirigido a la capa de aplicación, a la de red o al DNS.

Además, algunos CSP y proveedores de seguridad no ofrecen un SLA de tiempo de mitigación (TTM) y, en su lugar, ofrecen créditos de servicio a la organización afectada. Es importante comprender si la cláusula del TTM incluye el tiempo necesario para identificar un ataque. Si una plataforma tarda varios minutos o incluso horas en identificar un ataque DDoS antes de que se activen sus protocolos de mitigación, la organización víctima del ataque podría permanecer sin conexión durante un periodo prolongado. Cuando cada segundo cuenta, las organizaciones necesitan asegurarse de que su proveedor se compromete a mantener el tiempo de actividad y la disponibilidad sin sacrificar el rendimiento.



Además, es igual de importante o más que los equipos de seguridad o las organizaciones compradoras comprendan si los proveedores de soluciones de protección contra DDoS y los CSP ofrecen **capacidad de defensa específica contra DDoS** o si la capacidad de defensa se comparte con su red CDN. La defensa específica contra DDoS es como un equipo de operaciones especiales que se centra exclusivamente en combatir los ataques DDoS y no comparte recursos ni infraestructura con otros aspectos de una empresa, como la distribución de contenido, lo que garantiza un impacto mínimo incluso en caso de que se produzca un ataque sin precedentes. Las organizaciones que están considerando la protección frente a DDoS deben comprender que, en ocasiones, los propios proveedores se enfrentarán a ataques DDoS, y es preciso que tengan muy en cuenta si esos proveedores ofrecen un SLA de tiempo de actividad o disponibilidad.

Por último, muchos CSP y proveedores de seguridad no proporcionan acceso ininterrumpido y bajo demanda a la asistencia de un centro de operaciones de seguridad (SOC) global junto con la ayuda previa, durante y después del ataque. Si lo hacen, es por un precio elevado, lo que suele resultar más caro que contratar una solución de mitigación de DDoS especializada de un proveedor de calidad. Con una solución de protección híbrida contra DDoS totalmente gestionada, los proveedores de servicios actúan como una extensión del equipo de respuesta a incidentes de una organización y ofrecen conocimientos especializados para responder rápidamente a estos ataques.

En el panorama de amenazas actual, es obvio que las empresas modernas recurren a partners de mitigación de DDoS que ofrecen una experiencia de seguridad optimizada en todos los entornos híbridos, al tiempo que reducen la complejidad de la superficie de ataque. Su partner de protección contra DDoS debe facilitar y no obstaculizar su estrategia híbrida o multinube, además de estar en consonancia con sus objetivos empresariales.

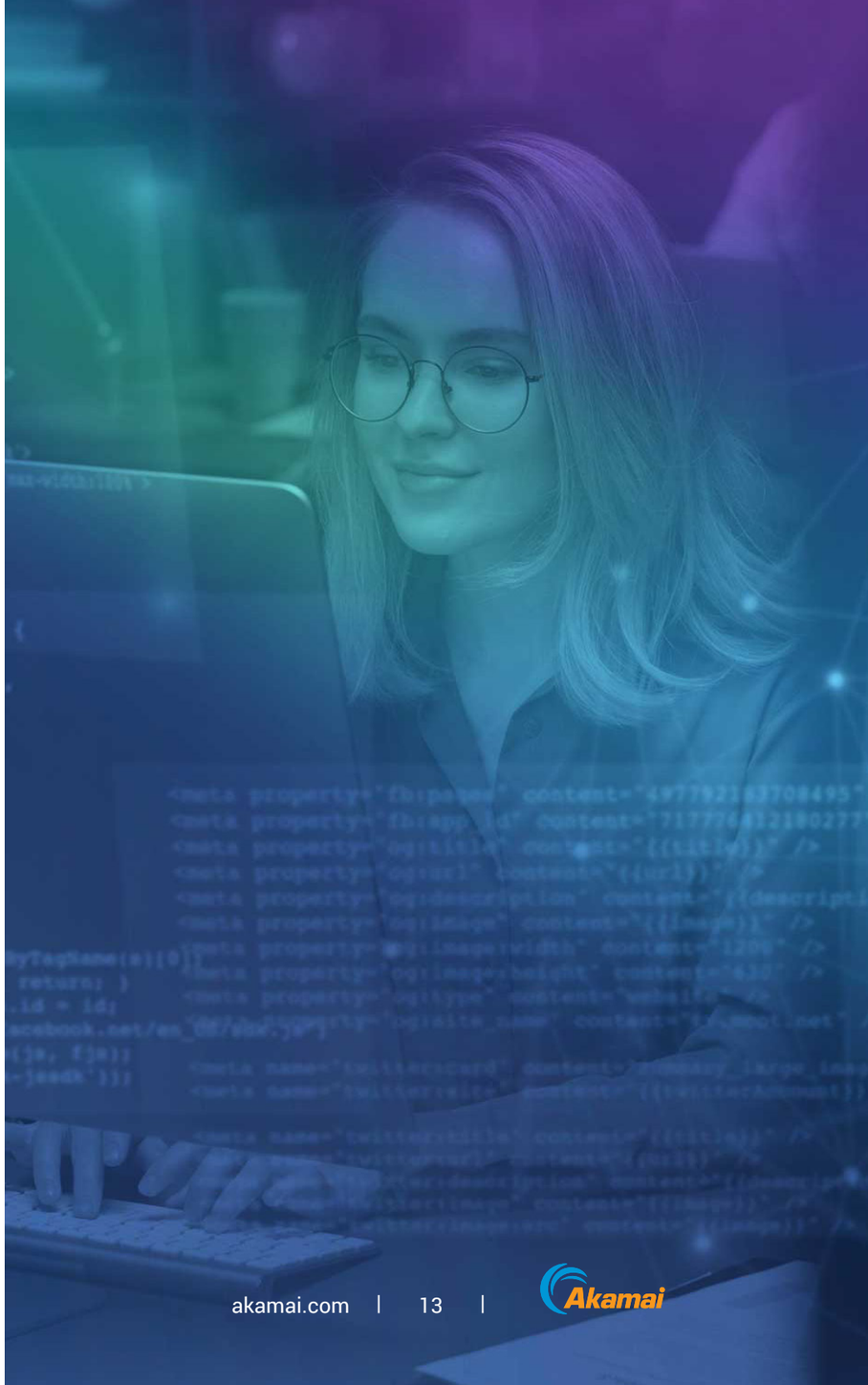
Mitigación de DDoS específica con Akamai

Al igual que necesitan una estrategia integral de infraestructura digital que incluya entornos híbridos y multinube, es recomendable que las organizaciones adopten también la protección integral contra DDoS. Akamai aplica una perspectiva integral, ya que actúa como primera línea de defensa y ofrece protección con estrategias de mitigación específicas de entornos híbridos, de DNS distribuido y en el Edge para evitar daños colaterales y puntos únicos de fallo. A diferencia de las arquitecturas de otros CSP, diseñadas como una solución "todo en uno", las soluciones con protección expresa frente a DDoS de Akamai ofrecen mayor resiliencia, capacidad de defensa frente a DDoS específica y una mitigación de mayor calidad y optimizada según los requisitos particulares de las aplicaciones web o los servicios basados en Internet. La defensa contra DDoS de Akamai está disponible para los clientes donde la necesiten —en entornos locales, en la nube o híbridos— y cuando la necesiten —siempre activa o bajo demanda—. Esta protección integral abarca tres productos principales.

Defensa contra DDos específica

DNS distribuido

Mitigación híbrida



Akamai Prolexic ofrece una protección contra DDoS de primera clase y adaptada a la estrategia de seguridad proactiva y positiva de una organización

Una arquitectura moderna y escalable

Akamai Prolexic usa una arquitectura completamente definida por software que es capaz de adaptarse a los cambios en las tendencias de red relacionados con el edge computing, el 5G/6G y la virtualización. Con la transición a entornos de software virtualizados, Prolexic eliminó todas las dependencias del hardware especializado. Esta estandarización de la implementación permite a Akamai satisfacer las necesidades cambiantes de los clientes con mayor rapidez, facilitar las implementaciones modulares para ampliar la capacidad, proporcionar una mejor cobertura regional con enlaces de baja latencia y mejorar la redundancia en la plataforma. Además, la arquitectura ayuda a acelerar las capacidades avanzadas de aprendizaje conductual de Prolexic para aprender de las firmas de ataque, adaptarse a los vectores de amenaza emergentes y crear de forma proactiva estrategias resistentes a los ataques DDoS para los clientes. Prolexic Cloud se apoya en **múltiples centros de barrido situados en 32 áreas metropolitanas de todo el mundo, con un total de más de 20 Tbps de capacidad defensiva específica**. Para poner en perspectiva la capacidad de defensa de Prolexic, los ataques DDoS de capa 3 y capa 4 más grandes conocidos no representan ni el 10 % de la capacidad disponible para los clientes de Prolexic.

Una protección contra DDoS completa, flexible y fiable

Akamai Prolexic está disponible como Prolexic Cloud, Prolexic On-Prem y Prolexic Hybrid.

Prolexic Cloud es la solución pionera del sector en materia de protección frente a DDoS basada en la nube y ofrece a los clientes SLA de mitigación de cero segundos y disponibilidad permanente. Los controles de mitigación escalan dinámicamente la capacidad para detener los ataques en los flujos de tráfico IPv4 e IPv6. Los recursos informáticos se pueden asignar dinámicamente a cualquier control de mitigación que los necesite.

Prolexic On-Prem ofrece una protección contra DDoS constante, física o lógica, en línea y de la ruta de datos que se integra de forma nativa con enrutadores del Edge para detener automáticamente más del 98 % de los ataques en el Edge de la red de un cliente sin tener que redirigir el tráfico. Es una solución ideal contra la gran mayoría de los ataques pequeños y rápidos y para las empresas que requieren una protección frente a DDoS de latencia ultrabaja.

Prolexic Hybrid combina la potencia, la automatización y el rendimiento de Prolexic On-Prem con la escala y la capacidad líderes del sector de Prolexic Cloud para proteger los orígenes de los clientes frente a los mayores ataques DDoS volumétricos.

Seguridad más allá de los ataques DDoS

Akamai Prolexic incluye Prolexic Network Cloud Firewall, una función de autoservicio totalmente configurable por el usuario que permite a los clientes definir, implementar y gestionar fácilmente sus propias listas de control de acceso (ACL) y las reglas que desean que se apliquen en el Edge de la red. Se trata de un firewall que se coloca por delante de todos los demás. Network Cloud Firewall también recomienda las ACL para aplicar la mejor estrategia de defensa proactiva basada en datos de inteligencia de Akamai sobre amenazas, y ofrece análisis prácticos de las reglas existentes. Network Cloud Firewall es un firewall como servicio (FWaaS) de última generación que permite a los clientes:

- Establecer defensas proactivas para bloquear el tráfico malicioso al instante
- Aligerar la infraestructura local trasladando las reglas al Edge
- Adaptarse rápidamente a los cambios en la red mediante una nueva interfaz de usuario

Akamai Edge DNS y **Akamai Shield NS53** protegen y fortalecen la infraestructura de DNS esencial

Akamai Edge DNS le proporciona una protección integral frente a una amplia variedad de ataques contra la infraestructura local, en la nube o en un entorno híbrido. La solución también ofrece un alto nivel de rendimiento, resistencia y disponibilidad del DNS. Basada en una red Anycast distribuida globalmente, se puede implementar como un servicio DNS primario o secundario, que puede sustituir la infraestructura de DNS actual o complementarla, según sea necesario.

Akamai Shield NS53 es una solución de DNS de proxy inverso que protege la infraestructura de DNS híbrida y local, incluidos los GSLB, los firewalls y los servidores de nombres, de los ataques de agotamiento de recursos del DNS, también conocidos como NXDOMAIN. Los clientes pueden configurar, administrar, gestionar y aplicar por sí mismos sus propias políticas dinámicas de seguridad en tiempo real. Las consultas de DNS ilegítimas y los ataques de inundación del DNS se neutralizan en el Edge de la red de Akamai para proteger la infraestructura de DNS esencial frente a los ataques DDoS.

Akamai App & API Protector protege las aplicaciones y las API frente a los ataques DDoS

App & API Protector, reconocida como una de las soluciones de protección de API y aplicaciones web (WAAP) líderes del mercado, neutraliza instantáneamente los ataques DDoS dirigidos a la capa de red que se producen en el Edge (en el caso de las propiedades alojadas en Akamai Connected Cloud) y proporciona estrategias de defensa completas contra aquellos que tienen lugar en la capa de aplicación.

¿Por qué Akamai?

Akamai ofrece las soluciones de mitigación de DDoS más fiables del mundo. Tanto si quiere proteger aplicaciones individuales como si busca defender centros de datos completos o infraestructuras esenciales de DNS, Akamai ha diseñado la mitigación de DDoS con la capacidad más elevada, la máxima resistencia y la ejecución más rápida.

Hemos mitigado algunos de los ataques DDoS más grandes del mundo. Nuestros controles proactivos ofrecen mitigación en cero segundos y un SLA líder en el sector. Además, podemos ofrecer servicios de protección contra DDoS a distintos clientes y combatir muchos ataques DDoS al mismo tiempo.

Debido a que los vectores de ataque DDoS cambian constantemente y la envergadura de esos ataques va en aumento, es preciso que las plataformas de lucha contra DDoS innoven, y que desarrollen e implementen capacidades continuamente para detectar las amenazas de forma proactiva, trazar estrategias de mitigación y minimizar el impacto. Akamai tiene como objetivo anticiparse a las amenazas para mitigar los ataques antes de que comiencen.

Su estrategia de mitigación de DDoS debe potenciar su estrategia de nube. Las soluciones DDoS de última generación de Akamai protegen su infraestructura de red digital, sus aplicaciones y su DNS, tanto en la nube como en el entorno local, y ofrecen las ventajas combinadas de la inteligencia artificial y la inteligencia humana.

Más información

| Publicado en: 10/24