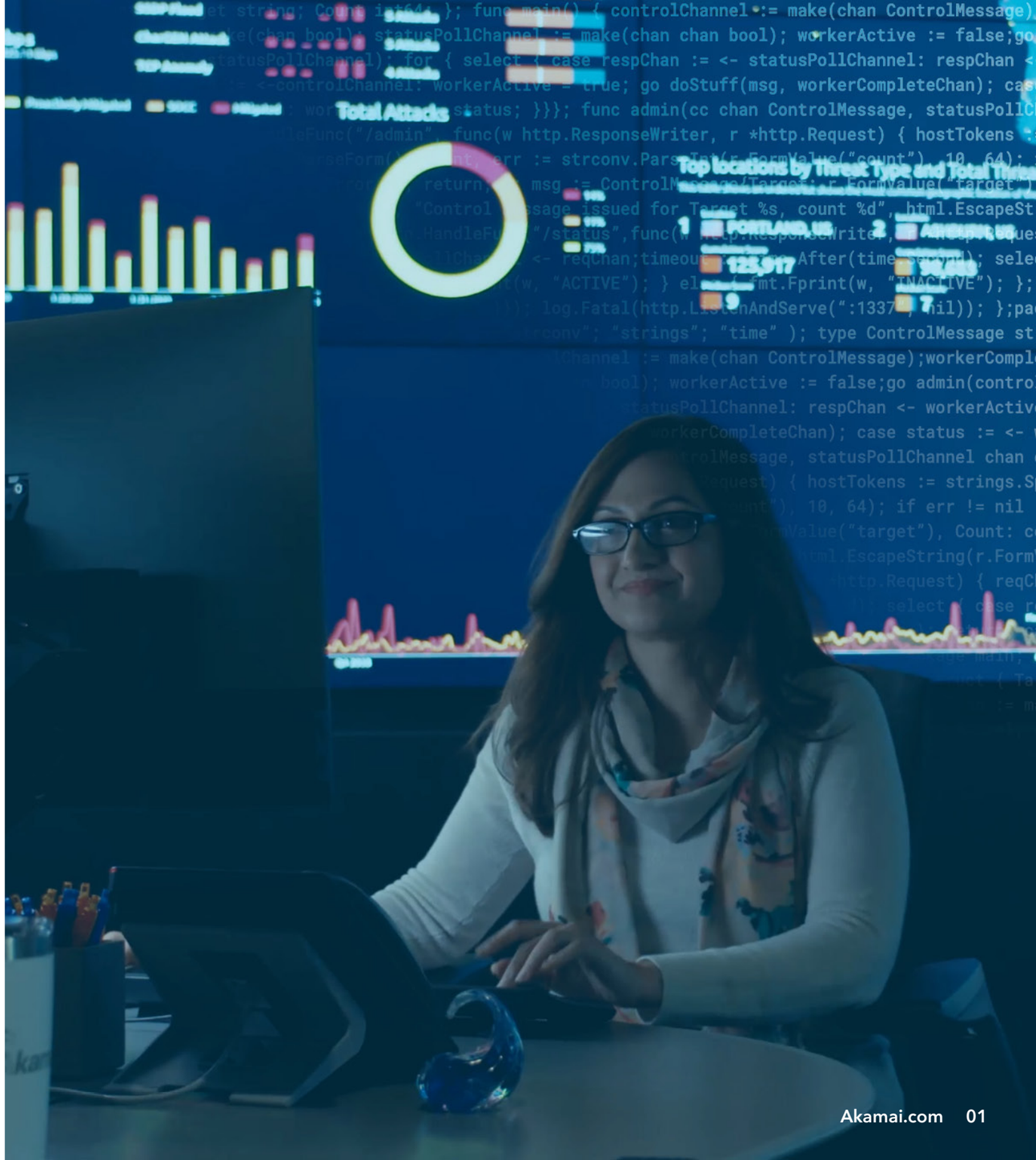
Protección frente a DDoS en un mundo de nube híbrida

LIBRO ELECTRÓNICO

Protección frente a DDoS en un mundo de nube híbrida

Los ataques distribuidos de denegación de servicio (DDoS), uno de los tipos de ciberamenaza más antiguos, siguen siendo un instrumento popular de interrupción masiva y plantean riesgos de seguridad para prácticamente cualquier empresa, tanto pequeña como grande. De hecho, según IDC, se prevé que los ataques DDoS aumenten con una tasa de crecimiento anual compuesta (TCAC) del 18 % hasta 2023, un claro indicador de que es hora de aumentar la inversión en controles sólidos de mitigación. Aunque algunas organizaciones pueden creer que son objetivos de bajo riesgo para un ataque DDoS, la creciente dependencia de la conectividad a Internet para potenciar los servicios y las aplicaciones esenciales para las empresas deja a todo el mundo expuesto al tiempo de inactividad y a una reducción del rendimiento si la infraestructura no está protegida.



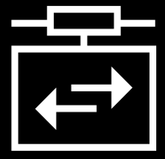
Una amenaza **en constante evolución**

El tamaño de los ataques DDoS se ha ido duplicando cada dos años y la complejidad (el número y la combinación de vectores de ataque) no tiene precedentes. La disponibilidad de las aplicaciones y las redes es esencial para la continuidad del negocio. Esto incentiva a los atacantes a lanzar ataques DDoS volumétricos y de protocolo a la capa de aplicación para aprovechar cualquier posible punto de fallo, haciendo que los recursos y activos orientados a Internet no estén disponibles para los usuarios finales.

LOS ATACANTES DDoS APROVECHARÁN CUALQUIER POSIBLE PUNTO DE FALLO, COMO:

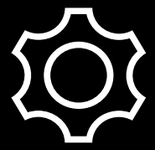
Sitios web

Aplicaciones web y otros servicios empresariales



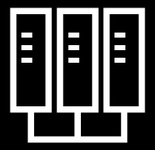
Concentradores de VPN para acceso remoto a recursos corporativos

Controladores SD-WAN



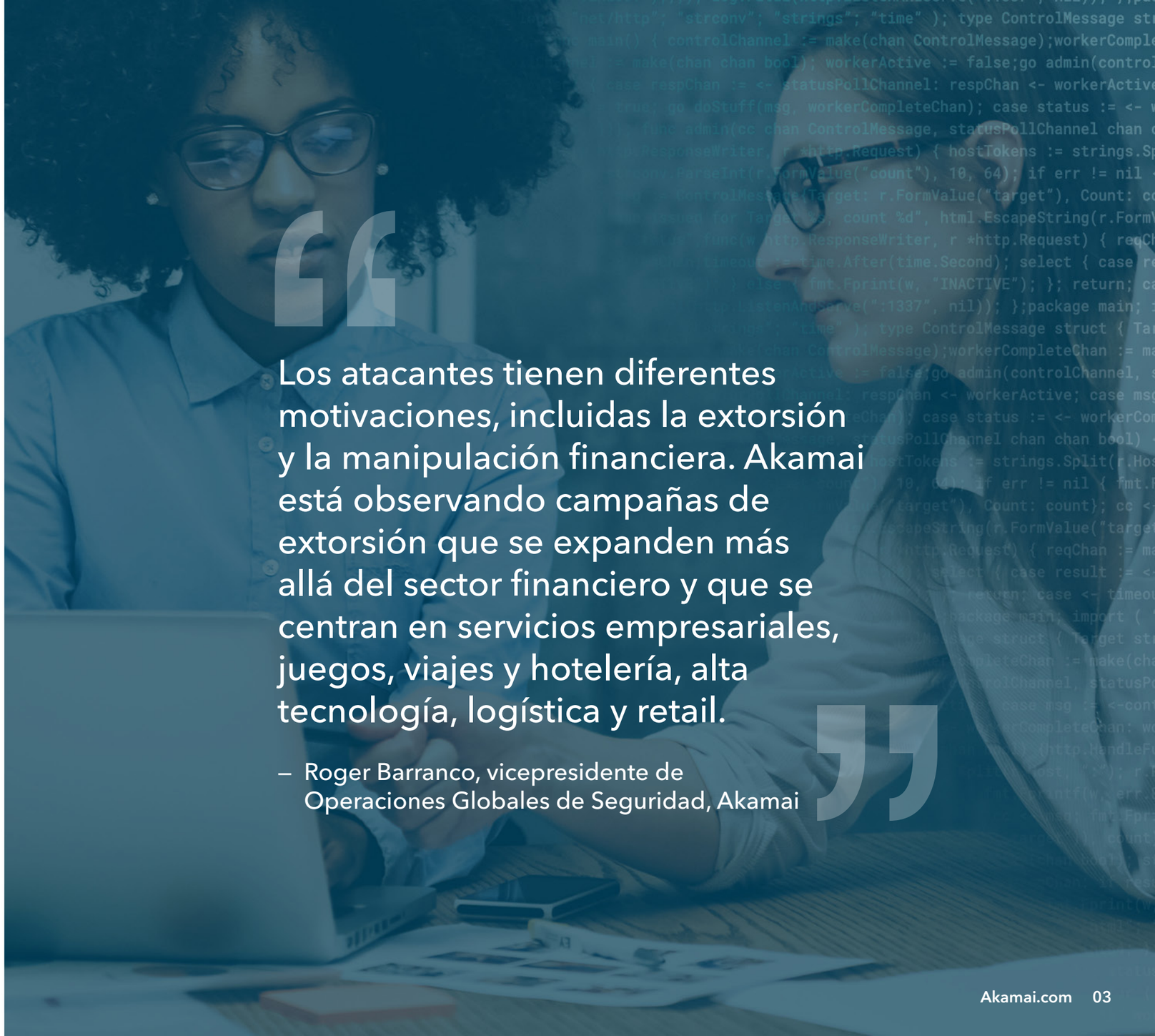
Interfaces de programación de aplicaciones (API)

Sistema de nombres de dominio (DNS) y servidores de origen



Infraestructura de red y centro de datos

Mediante el reconocimiento de estos entornos, aplicaciones y espacios de IP de las víctimas, los atacantes pueden determinar qué vectores DDoS causarán más daños en los servicios de Internet e infraestructuras de alojamiento de origen. Con fácil acceso, a estos atacantes no les faltan técnicas ni herramientas de ataque (booters, DDoS de alquiler, etc.) para ayudar a descubrir debilidades o vulnerabilidades en las defensas de la empresa.



> Los atacantes tienen diferentes motivaciones, incluidas la extorsión y la manipulación financiera. Akamai está observando campañas de extorsión que se expanden más allá del sector financiero y que se centran en servicios empresariales, juegos, viajes y hotelería, alta tecnología, logística y retail.
>
> — Roger Barranco, vicepresidente de Operaciones Globales de Seguridad, Akamai

Las repercusiones de un ataque DDoS se intensifican a medida que las organizaciones trabajan para escalar y proteger las capacidades de acceso remoto a fin de garantizar la productividad de los empleados y la normalidad del negocio.

Las **consecuencias** de un ataque DDoS

En los ataques 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 a la capa de aplicación (capa 7), los atacantes pretenden interrumpir el rendimiento web y la experiencia del usuario a través de vectores como ataques lentos y sigilosos, además de inundaciones HTTP para producir un tiempo de inactividad que afecte a los resultados económicos de la empresa.

Sin embargo, las repercusiones del tiempo de inactividad van mucho más allá de la inhabilitación de los servicios y aplicaciones objeto del ataque. ***Según Ponemon Institute, el coste anual promedio de un ataque DDoS a una organización es de 1,7 millones de USD*** 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.

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

La nube sigue complicando las **estrategias de seguridad**

A medida que las organizaciones retiran centros de datos tradicionales y migran las aplicaciones a entornos alojados en la nube, las arquitecturas de seguridad se vuelven más complejas. Muchas organizaciones tienen dificultades para proteger los activos orientados a Internet con el mismo nivel de eficacia frente a DDoS que los que se encuentran en el centro de datos. Además de la complejidad, muchas IP alojadas en la nube se encuentran fuera del control directo de una empresa, lo que las deja en una posición vulnerable a un ataque DDoS si no cuentan con la protección adecuada.

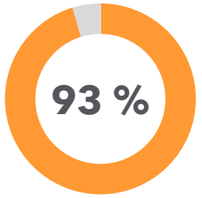
Y los atacantes son conscientes de esta migración acelerada a instalaciones de coubicación y a la nube pública. Están ansiosos por aprovechar las debilidades en la arquitectura y la estrategia de seguridad de una organización creadas mediante políticas y requisitos de seguridad incoherentes, así como las dificultades para la solución de problemas en una infraestructura fragmentada alojada en la nube.

CONCLUSIÓN:

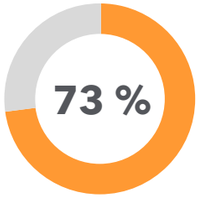
Las empresas modernas necesitan defensas adaptables para mantener una variedad de servicios y activos orientados a la web protegidos, independientemente de dónde se encuentren. Y con más del 93 % de las empresas (<1000 empleados) utilizando una estrategia multinube, ha llegado el momento de subsanar las brechas en seguridad generadas por la complejidad de la infraestructura.[1]

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

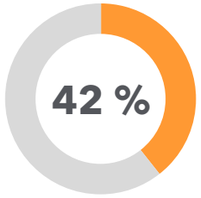
La responsabilidad de la seguridad en los entornos de nube pública puede ser contradictoria entre proveedores, y muchas organizaciones hacen falsas suposiciones que podrían dejarlos expuestos. Por ejemplo, el 73 % de las empresas entrevistadas en una encuesta de IBM cree que los proveedores de servicios 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 de nube como servicio (IaaS). Esta ausencia de titularidad en torno a la responsabilidad del control de la seguridad puede dar lugar a un riesgo que ninguna organización debería estar dispuesta a aceptar.



de las empresas utilizan una estrategia multinube



de las empresas encuestadas considera que los CSP públicos son responsables de proteger el SaaS



de las empresas encuestadas cree que los CSP son responsables de proteger la IaaS en la nube

En un documento reciente, Forrester puso de manifiesto que la mayoría de las organizaciones están escogiendo un enfoque de estrategia híbrida, utilizando varios proveedores de nube pública, así como albergando cargas de trabajo locales. Por eso, la empresa de análisis recomienda elegir un proveedor de mitigación de DDoS que pueda facilitar protección en las arquitecturas híbridas.

No todos los sistemas de mitigación de DDoS **son iguales**

A medida que continúan las inversiones en infraestructura de nube, los equipos de seguridad se siguen enfrentando al desafío de garantizar controles coherentes que abarquen los entornos híbridos. Además, a medida que las aplicaciones implementadas en varias infraestructuras de nube de back-end se vuelven más difíciles de proteger, muchas organizaciones desean un único punto de control para organizar las defensas. Con la creciente complejidad de la pila de tecnología de seguridad, muchas también desean este único panel, no solo para optimizar la visibilidad, sino también para obtener informes simplificados que se pueden alimentar a través de las API en sistemas de correlación de datos de eventos.

Para resolver este problema, las organizaciones están recurriendo a proveedores de seguridad frente a DDoS basados en la nube que puedan habilitar, no inhibir, sus estrategias de migración a la nube híbrida. Quieren contar con defensas escalables y eficaces, independientemente de la ubicación de los servicios empresariales. Se trata de una respuesta directa al aumento de la complejidad operativa necesaria para integrar, implementar y administrar las protecciones frente a DDoS en un entorno único de CSP. Y con tantos activos orientados a Internet ubicados en múltiples nubes, la complejidad se intensifica rápidamente.

Para aumentar la presión aún más, muchas soluciones de mitigación de DDoS internas de CSP se quedan cortas en áreas clave: visibilidad, acuerdos de nivel de servicio (SLA) e informes, todas ellas fundamentales para capacitar a 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 de DDoS de CSP ofrecen poca o ninguna transparencia en términos de informes, visibilidad y análisis posterior al ataque. No es de extrañar que muchos se refieran a los CSP como la caja negra de los análisis e informes.

Además, algunos CSP no ofrecen un SLA de tiempo de mitigación y, en su lugar, ofrecen créditos de servicio a la organización afectada. 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.

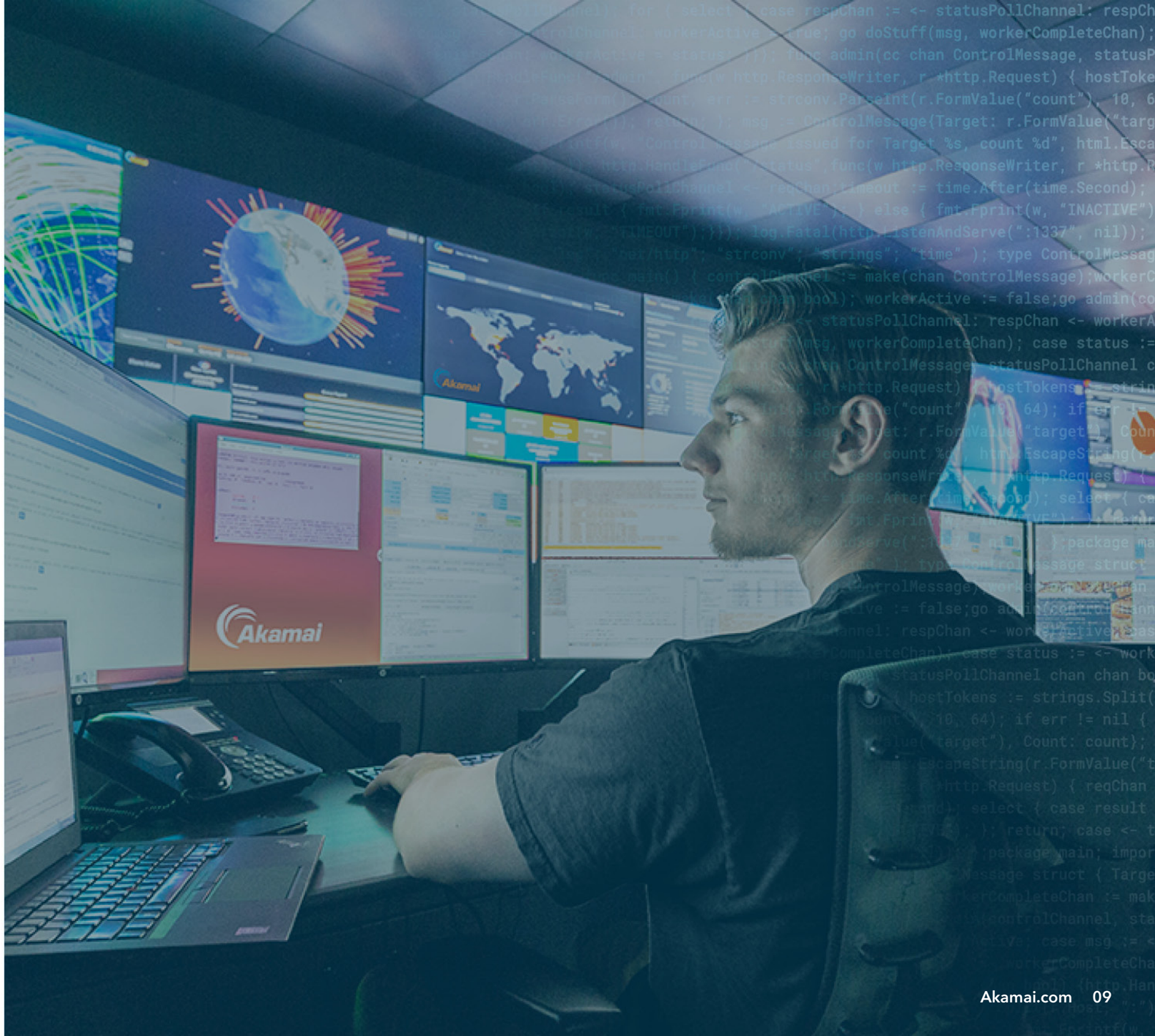
Por último, muchos CSP no ofrecen acceso a la carta a la asistencia del centro de operaciones de seguridad (SOC) global ininterrumpida, además de la asistencia previa, durante y después del ataque que está disponible con los principales proveedores de mitigación de DDoS basados en la nube. Si lo hacen, tiene un precio elevado que, muchas veces, es más caro que una solución de mitigación de DDoS especializada de un proveedor de calidad. Con una solución de protección 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 eventos DDoS.

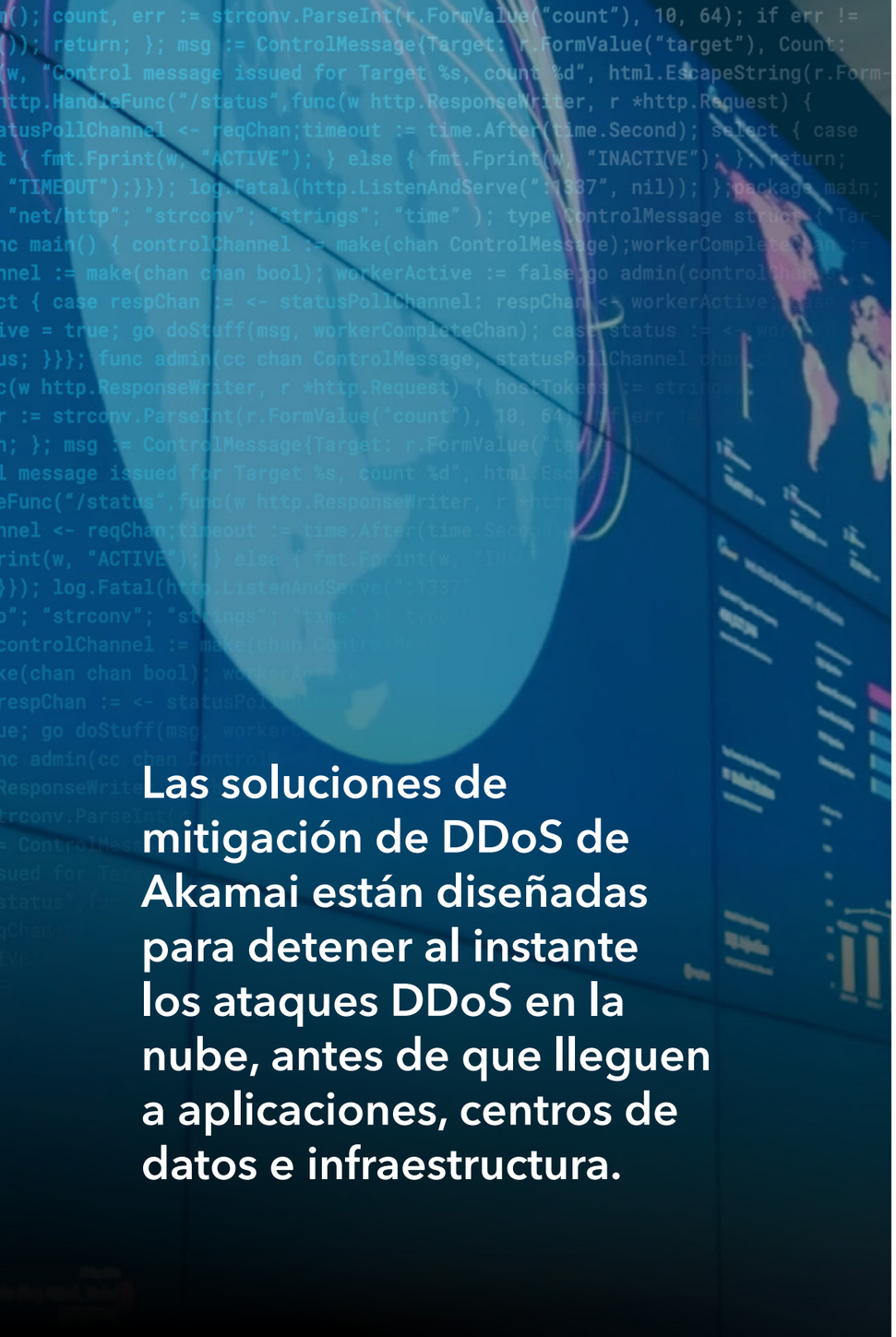
En el panorama actual de amenazas, es obvio que las empresas modernas recurren a partners de mitigación de DDoS que ofrecen una experiencia de seguridad optimizada en todos los entornos híbridos, al tiempo que reducen la complejidad de la superficie de ataque.

Un partner en la mitigación de DDoS debe poder facilitar una estrategia de nube, y no ser un obstáculo, a fin de ayudar a aliviar la presión asociada a la seguridad.

Mitigación de DDoS **específica** con Akamai

Al igual que las organizaciones necesitan una estrategia de nube integral, también deben plantearse la protección frente a DDoS integral. Al adoptar un enfoque holístico, Akamai actúa como primera línea de defensa y ofrece protección con estrategias de mitigación específicas en la nube, de DNS distribuido y en el borde de Internet para evitar daños colaterales y puntos únicos de fallo. A diferencia de las arquitecturas de otros proveedores de seguridad en la nube, diseñadas como una solución "todo en uno", las nubes con protección expresa frente a DDoS de Akamai ofrecen mayor resistencia, capacidad de barrido específica y mayor calidad de mitigación, optimizadas según los requisitos particulares de las aplicaciones web o los servicios basados en Internet.





Las soluciones de mitigación de DDoS de Akamai están diseñadas para detener al instante los ataques DDoS en la nube, antes de que lleguen a aplicaciones, centros de datos e infraestructura.

PROTECCIÓN EN EL BORDE DE INTERNET

La red de distribución de contenido (CDN) en el borde de Internet de Akamai ofrece y acelera el tráfico web mediante los protocolos HTTP y HTTPS. Cada servidor en el borde de Internet de Akamai funciona como un proxy inverso, reenviando tráfico HTTP/S legítimo en los puertos 80 y 443 y dejando el resto en el borde de Internet. Esto significa que todos los clientes de Akamai obtienen, intrínsecamente, mitigación instantánea de todos los ataques DDoS dirigidos a la capa de red, incorporada en su distribución web.

PROTECCIÓN DE DNS

La misma tecnología se aplica al servicio DNS autoritativo de Akamai, Edge DNS, que descarta al instante todo el tráfico que no pasa por el puerto 53. A diferencia de otras soluciones de DNS, Akamai ha diseñado específicamente Edge DNS para ofrecer disponibilidad y resistencia frente a los ataques DDoS, además de rendimiento, con redundancias de arquitectura en varios niveles, incluidos servidores de nombres, puntos de presencia, redes e incluso las nubes de IP Anycast segmentadas.

PROTECCIÓN DE BARRIDO EN LA NUBE

Como servicio de barrido en la nube certificado, Prolexic protege todos los centros de datos y la infraestructura orientada a Internet de los ataques DDoS, en todos los puertos y protocolos. Mediante el enrutamiento del tráfico tanto legítimo como malicioso a través de Prolexic, podemos crear modelos de seguridad positivos y negativos que mitigan de forma proactiva e instantánea los ataques DDoS con alta precisión. Los expertos del centro de control de operaciones de seguridad (SOCC) de Akamai actúan como una extensión del equipo de respuesta a incidentes de un cliente para equilibrar la detección y la respuesta automatizadas con la participación humana.

¿Por qué Akamai?

Akamai tiene las nubes globales de mitigación de DDoS más avanzadas del mundo. Ya quiera proteger aplicaciones individuales, centros de datos completos o DNS autoritativo, 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 de mitigación proactivos ofrecen un SLA de mitigación de cero segundos líder en el sector. Además, podemos ofrecer servicios de protección contra DDoS a varios clientes y combatir muchos ataques DDoS al mismo tiempo.

Akamai

Debido a que los vectores de ataque DDoS siguen cambiando y la envergadura de los ataques continúa aumentando, un proveedor debe invertir continuamente en el desarrollo e implementación de herramientas y reglas para detectar, combatir y mitigar los ataques. 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. Akamai Intelligent Edge Platform proporciona mecanismos de defensa frente a DDoS para ello, lo que ayuda a los clientes a extender la protección en todo su núcleo, en la nube y en el borde de Internet, minimizando el riesgo y ofreciendo, al mismo tiempo, la flexibilidad necesaria para adoptar futuras evoluciones en las estrategias de nube.

Póngase en contacto con nosotros para averiguar cómo podemos **proteger** su negocio

Más información

*Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite **www.akamai.com**, **blogs.akamai.com**, o siga a **@Akamai** en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en **www.akamai.com/locations**. Publicado el 20 de noviembre.*