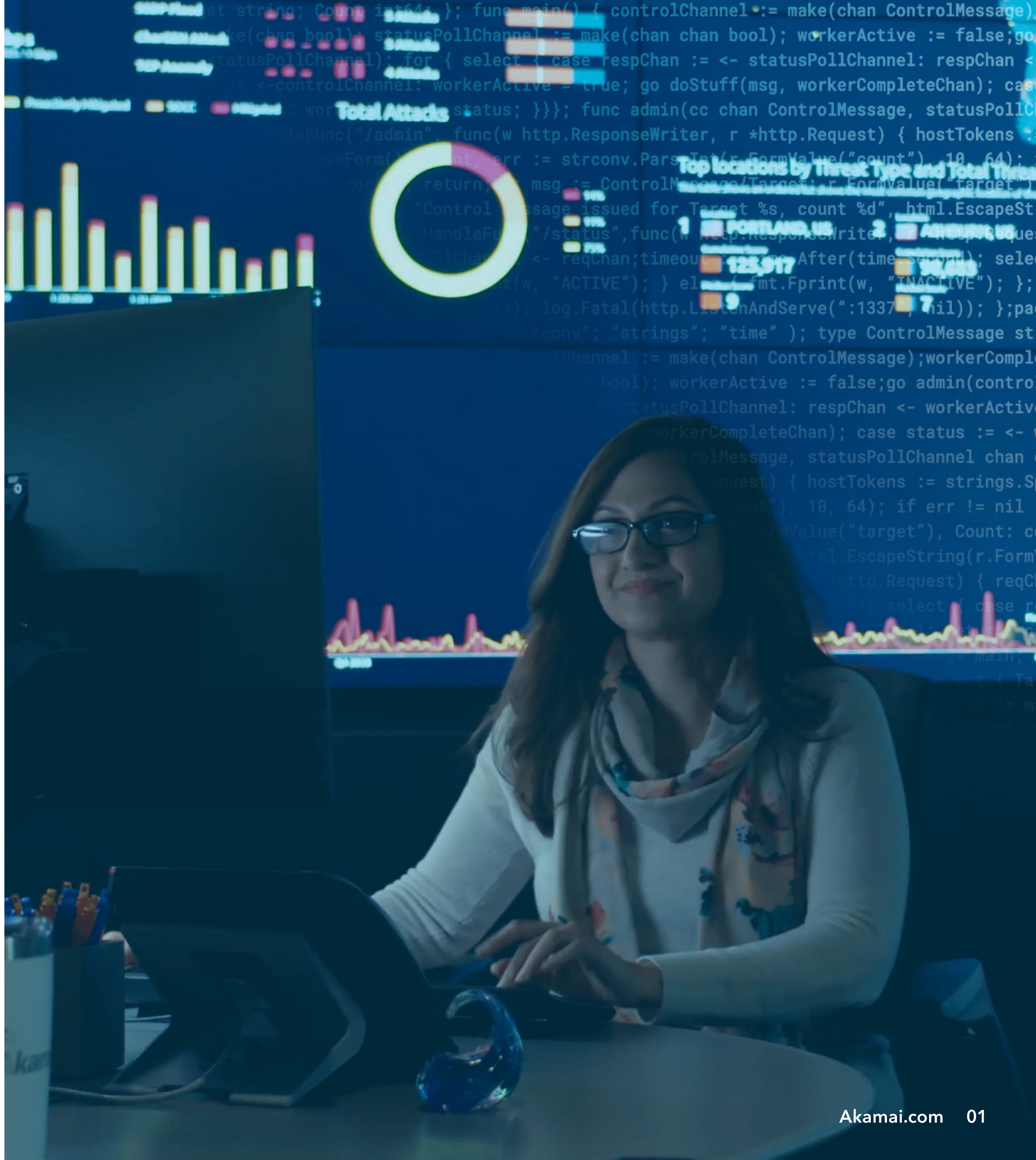
Akamai

# DDoS Defense in a Hybrid Cloud World

E-BOOK

# DDoS Defense in a Hybrid Cloud World

Distributed denial of service (DDoS), one of the oldest types of cyberthreats, continues to be a popular instrument of mass disruption, posing security risks for virtually every type of enterprise – small and large alike. In fact, according to IDC, DDoS attacks are expected to grow at an 18% CAGR through 2023, a clear indicator that it's time to increase investment in robust mitigation controls. And while some organizations may believe they're low-risk targets for a DDoS attack, the growing reliance on internet connectivity to power business-critical services and applications leaves everyone exposed to downtime and diminished performance – if infrastructure isn't protected.



# An Evolving Threat

The size of DDoS attacks has been doubling every two years, and the complexity – the number and combination of attack vectors – is unprecedented. With application and network availability essential to business continuity, threat actors are incentivized to launch volumetric, protocol, and application-layer DDoS attacks to disrupt any potential point of failure, making internet-facing resources and assets unavailable to end users.

**DDoS ATTACKERS WILL TARGET ANY POTENTIAL POINT OF FAILURE, SUCH AS:**

- Websites
- Web Applications and Other Enterprise Services
- VPN Concentrators for Remote Access to Corporate Resources
- SD-WAN Controllers
- Application Programming Interfaces (APIs)
- Domain Name System (DNS) and Origin Servers
- Data Center and Network Infrastructure

By conducting reconnaissance of these victim environments, applications, and IP spaces, attackers can determine which DDoS vectors will inflict the most potential damage on internet-facing services and origin-hosting infrastructures. With a low barrier to entry, these threat actors have no shortage of attack techniques and tools (think booters, DDoS for hire, etc.) to help discover weaknesses or vulnerabilities in enterprise defenses.

> “Threat actors have different motivations, including extortion and financial manipulation. Akamai is observing extortion campaigns expanding beyond the financial sector, targeting business services, gaming, travel and hospitality, high tech, logistics, and retail.”
>
> – Roger Barranco, Vice President of Global Security Operations, Akamai

The repercussions of a DDoS attack intensify as organizations work to scale and protect remote access capabilities to ensure employee productivity and business as usual.

# The Consequences of a DDoS Attack

For network (layer 3) and transport (layer 4) layer attacks, volumetric and protocol-based attacks attempt to fill up internet pipes, overwhelm servers, and exhaust state table entries to make networks and services unavailable. With application-based (layer 7) attacks, threat actors aim to disrupt web performance and user experience through vectors like low and slow attacks, as well as HTTP floods to produce bottom-line-impacting downtime.

But the repercussions of downtime affect more than just the cost of targeted services and applications being unavailable. ***According to Ponemon Institute, the average annual cost of a DDoS attack to an organization is $1.7 million***, driven by increased technical support, consumption of incident response resources, internal escalations, legal costs, operational disruption, and loss of employee productivity.

It’s clear the stakes are high and only getting higher with the increased migration to hybrid cloud infrastructures.

# The Cloud Continues to Complicate **Security Postures**

As organizations decommission traditional data centers and move applications to cloud-hosted environments, security architectures become more complex. Many organizations struggle with how to keep internet-facing assets protected with the same level of DDoS defenses as those located within the data center. Adding to the complexity, many cloud-hosted IPs fall outside of an enterprise's direct control, leaving them vulnerable to a successful DDoS attack if not properly protected.

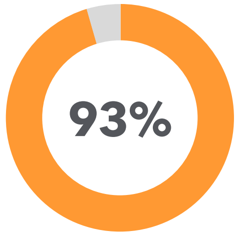
And threat actors are well aware of this accelerated migration to colocation facilities and the public cloud. They are eager to exploit weaknesses in an organization's security architecture and posture created by inconsistent security policies and requirements, as well as difficulties troubleshooting across disparate and fragmented cloud-hosted infrastructure.

## THE BOTTOM LINE:

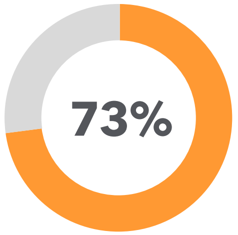
Modern enterprises need adaptive defenses to keep a variety of web-facing assets and services protected, regardless of where they are located. And with more than 93% of enterprises (<1,000 employees) employing a multi-cloud strategy, the time to close defensive gaps driven by infrastructure complexity is now.[1]

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

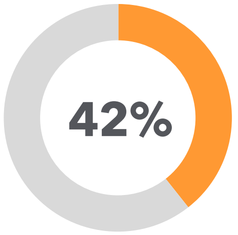
Responsibility for security within public cloud environments can be inconsistent from provider to provider, with many organizations making false assumptions that could leave them exposed. For example, 73% of enterprise respondents in an IBM survey believe public cloud service providers (CSPs) are the primary party responsible for securing software as a service (SaaS), while 42% believe CSPs are mainly responsible for securing cloud infrastructure as a service (IaaS). This lack of ownership around security control responsibility can lead to compromise – a risk no organization should be willing to accept.



of enterprises employ a multi-cloud strategy



of survey respondents believe public CSPs are responsible for securing SaaS



of respondents believe CSPs are responsible for securing cloud IaaS

In a recent paper, Forrester noted that most organizations are choosing a hybrid strategy approach, utilizing multiple public cloud providers as well as hosting on-premises workloads. As such, the analyst firm recommends choosing a DDoS mitigation provider that can enable protection across hybrid architectures.

Threat actors only have to be right once. Companies need responsive mitigation controls to fight back.

# All DDoS Mitigation Is **Not Created Equal**

As investments in cloud infrastructure continue, security teams remain challenged with ensuring consistent controls spanning hybrid environments. And as applications deployed across multiple back-end cloud infrastructures become more difficult to protect, many organizations desire a single control point to orchestrate defenses. With the security technology stack growing more complex, many also desire this single pane of glass – not only for optimized visibility, but also for streamlined reporting that can be fed via APIs into event data correlation systems.

***In order to solve this problem, organizations are turning to cloud-based DDoS security providers that can enable, not inhibit, their hybrid cloud migration strategies. They want scalable, responsive defenses – regardless of where enterprise services may reside.*** This is in direct response to the increase in operational complexity required to integrate, deploy, and manage DDoS defenses within a CSP's unique environment. And with many internet-facing assets located across multiple clouds, complexity is quickly compounded.

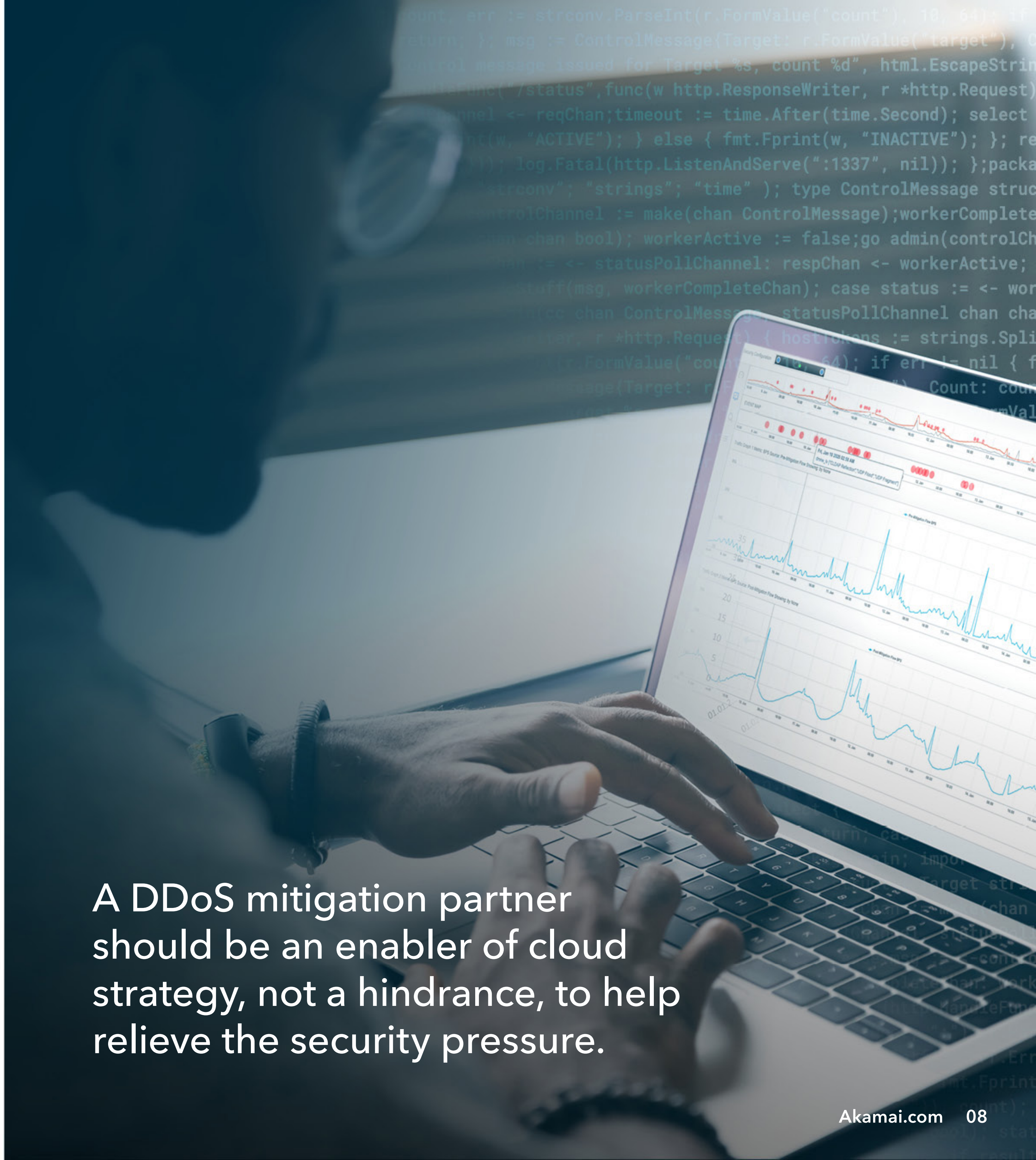
Adding to the pressure, many CSP in-house DDoS mitigation solutions fall short in key areas: visibility, SLAs, and reporting – all critical to empowering today's enterprise defenders.

For security teams, it's all about visibility and attaining actionable insights to optimize incident response and preparedness. Some CSP DDoS solutions offer little to no transparency in terms of reporting, visibility, and post-attack analysis – no wonder many refer to CSPs as the black box of analytics and reporting.

Additionally, some CSPs don't offer a time-to-mitigate SLA and instead offer service credits to the impacted organization. When seconds count, organizations need assurance that their provider will commit to maintaining uptime and availability without compromising performance.

And finally, many CSPs don't provide on-demand access to 24/7 global security operations center SOC support in addition to the pre-attack, during, and post-attack assistance that's standard with leading cloud-based DDoS mitigation providers. If they do, it's at a premium, oftentimes more expensive than a specialized DDoS mitigation solution from a best-in-class provider. With a fully managed DDoS protection solution, service providers act as an extension of an organization's incident response team and offer the expert knowledge to quickly respond to DDoS events.

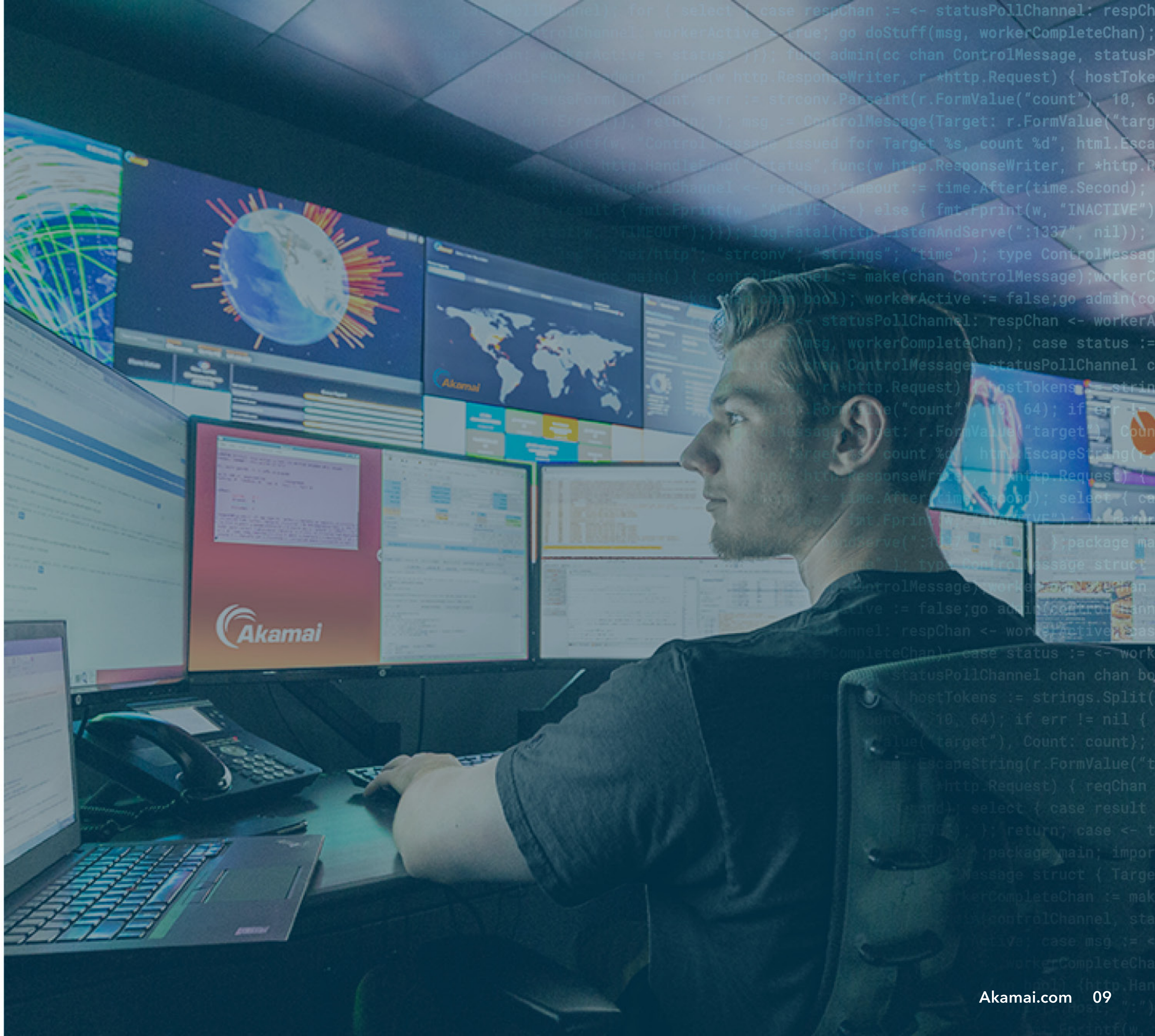
In today's threatscape, it's clear modern businesses are turning to DDoS mitigation partners that support a streamlined security experience across hybrid environments, all while reducing attack surface complexity.

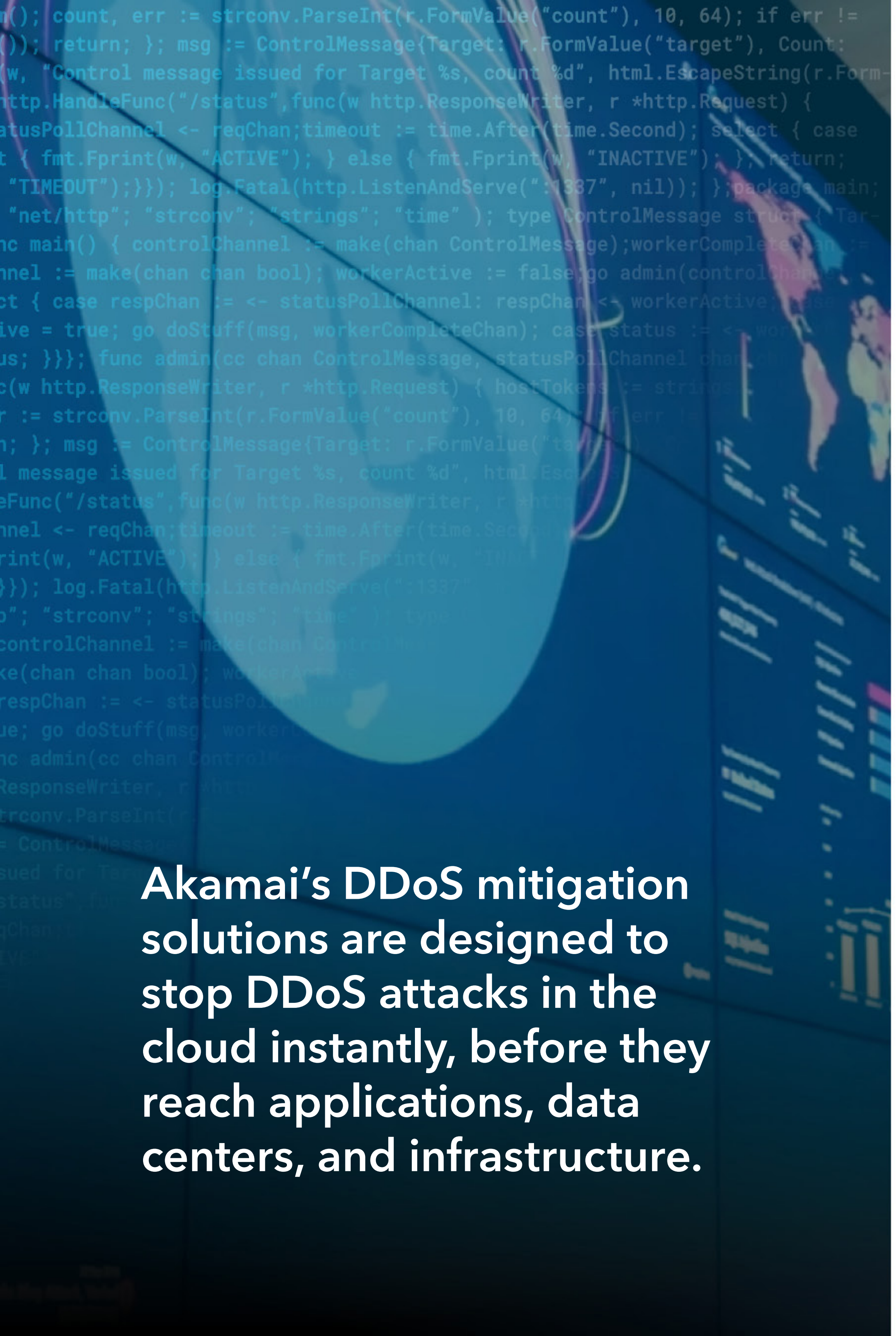


A DDoS mitigation partner should be an enabler of cloud strategy, not a hindrance, to help relieve the security pressure.

# Purpose-Built DDoS Mitigation with Akamai

Just as organizations need an end-to-end cloud strategy, they also need to consider end-to-end DDoS protection. By taking a holistic approach, Akamai acts as a first line of defense, providing protection with dedicated edge, distributed DNS, and cloud mitigation strategies designed to prevent collateral damage and single points of failure. As opposed to other cloud security provider architectures – built as an "all in one" solution – Akamai's purpose-built DDoS clouds offer increased resiliency, dedicated scrubbing capacity, and higher quality of mitigation, fine-tuned to the specific requirements of web applications or internet-based services.





Akamai’s DDoS mitigation solutions are designed to stop DDoS attacks in the cloud instantly, before they reach applications, data centers, and infrastructure.

## EDGE DEFENSE

The Akamai edge (CDN) delivers and accelerates web traffic using HTTP and HTTPS protocols. Every Akamai edge server operates as a reverse proxy, forwarding legitimate HTTP/S traffic on ports 80 and 443, and dropping all other traffic at the network edge. This means that every Akamai customer inherently gets instant mitigation of all network-layer DDoS attacks – built into their web delivery.

## DNS DEFENSE

The same technology applies to Akamai’s authoritative DNS service, Edge DNS, which instantly drops all traffic not on port 53. Unlike other DNS solutions, Akamai specifically architected Edge DNS for availability and resiliency against DDoS attacks, in addition to performance, with architectural redundancies at multiple levels, including name servers, points of presence, networks, and even segmented IP Anycast clouds.

## CLOUD SCRUBBING DEFENSE

As a battle-tested cloud scrubbing service, Prolexic protects entire data centers and internet-facing infrastructure from DDoS attacks – across all ports and protocols. By routing both legitimate and malicious traffic through Prolexic, we are able to build both positive and negative security models that proactively and instantly mitigate DDoS attacks with high accuracy. Akamai Security Operations Command Center (SOCC) experts act as an extension of a customer’s incident response team to balance automated detection and response with human engagement.

# Why Akamai

Akamai has the world's largest mature global DDoS mitigation clouds. Whether you're protecting individual applications, entire data centers, or authoritative DNS, Akamai has architected DDoS mitigation with the highest capacity, utmost resiliency, and fastest mitigation in mind.

We have mitigated some of the largest DDoS attacks launched in the world. Our proactive mitigation controls enable true zero-second mitigation, an industry-leading SLA. And we can provide DDoS protection services for multiple clients and fight multiple DDoS attacks at once.

**2,400**

globally distributed edge and cloud scrubbing centers

MORE THAN **170 Tbps**

of capacity

**PROVEN**

history of mitigating record-setting attacks in zero seconds

**200+**

SOCC experts available 24/7/365 to balance automated detection and response with human intelligence

24/7 emergency DDoS mitigation and protection.

Call us or complete the form below.

s should contact their Account

Technical Support is an important part of the Akamai experience. Our team provides unrivaled expertise and support to keep your online business running smoothly 24/7.

Because DDoS attack vectors keep changing and attack sizes keep getting bigger, a provider must continually invest in, develop, and deploy tools and rules to detect, orchestrate, and mitigate attacks. Akamai is dedicated to staying ahead of threats by mitigating attacks before they start.

Your DDoS mitigation strategy should empower your cloud strategy. The Akamai Intelligent Edge Platform offers DDoS defenses to do so, helping customers extend protection across their core, to the cloud and to the edge, minimizing risk, while providing flexibility around future evolutions in cloud strategies.

# Contact Us to Find Out How We Can Protect Your Business

Learn more

*Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit **www.akamai.com**, **blogs.akamai.com**, or **@Akamai** on Twitter. You can find our global contact information at **www.akamai.com/locations**.*

*Published 11/20.*