DDoS Defense in a Hybrid Cloud World

Table of contents

DDoS continues to evolve 3

The growing threat 5

The consequences of a DDoS attack 7

Hybrid and multicloud continue to complicate security 8

All DDoS mitigation is not created equal 10

Purpose-built DDoS mitigation with Akamai 13

Akamai Prolexic is world-class DDoS protection tailored for an organization's proactive and positive security posture 14

Akamai Edge DNS and **Akamai Shield NS53** secure and fortify critical DNS infrastructure 17

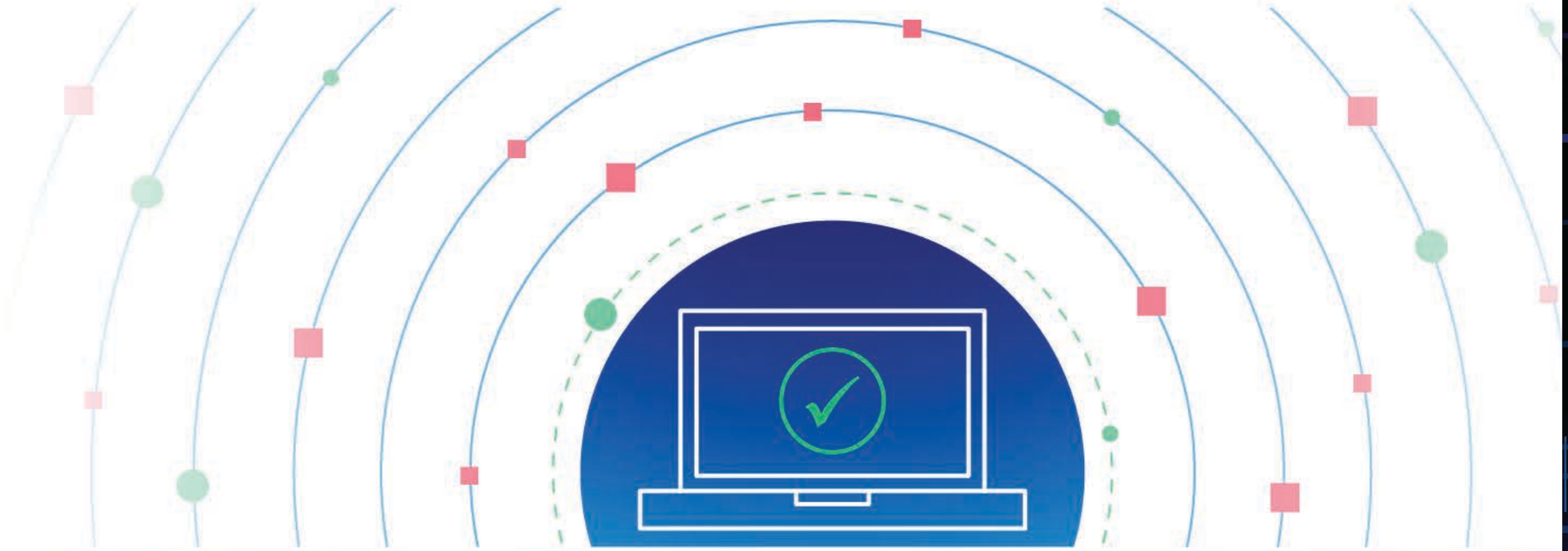
Akamai App & API Protector secures applications and APIs from DDoS attacks 18

Why Akamai? 19

DDoS continues to evolve

Distributed denial of service (DDoS), one of the oldest types of cyberthreats, continues to evolve and has now become a highly sophisticated tool in the hands of cybercriminals and ideologically motivated hacktivists. Indeed, DDoS attacks pose security risks not only to large and small enterprises, but also to critical public infrastructure in areas like healthcare, energy and utilities, and education.

Further complicating this dynamic is the increased adoption of cloud computing resources by both public and private institutions. When these organizations combine cloud with their preexisting on-premises resources, the resulting hybrid environment becomes significantly more complex. Applications, application programming interfaces (APIs), data, microservices, and workloads must now travel through a fragmented environment. The different architectures of these environments create new vulnerabilities and a fractured attack surface that can be exploited by cybercriminals to launch increasingly sophisticated and debilitating DDoS attacks.



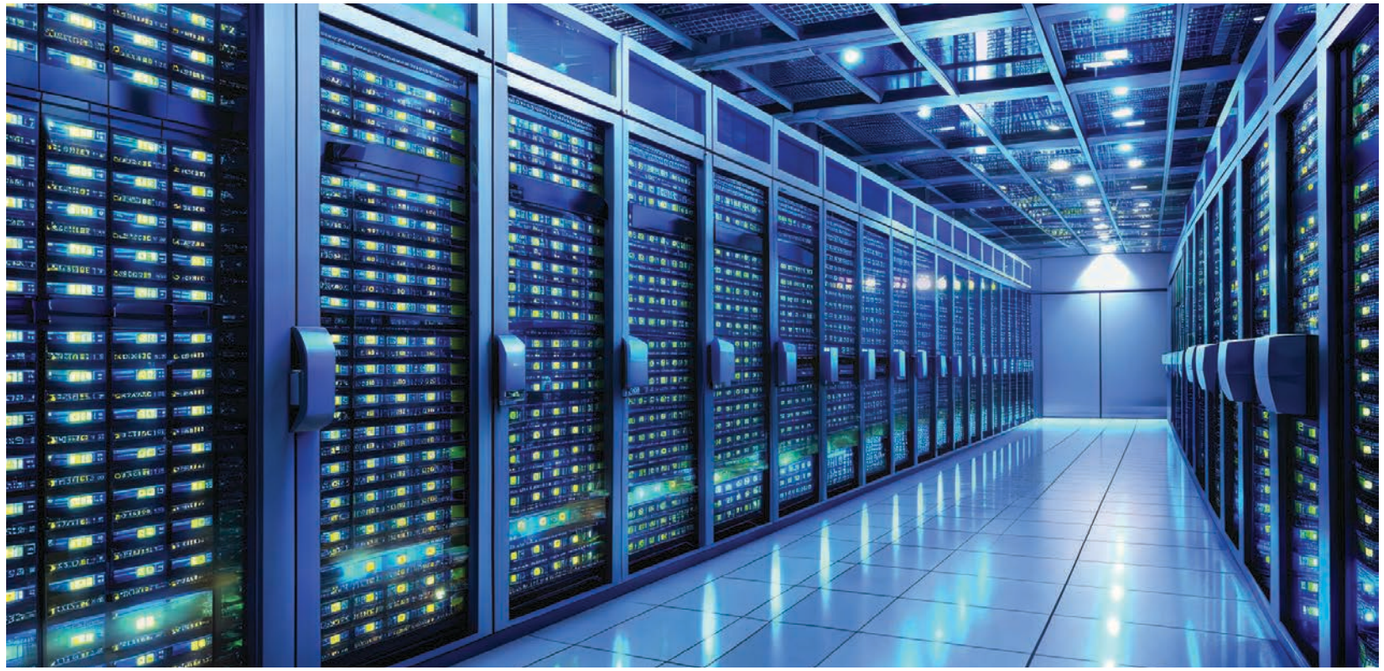
Organizations are scrambling to ensure that their digital infrastructure is protected. They need an integrated and hybrid DDoS protection platform that can protect their on-premises (private cloud) infrastructure from short but sharp DDoS attacks, but also take advantage of the scale and capacity of cloud scrubbing for large volumetric DDoS attacks.

Trends suggest that DDoS attacks will continue to be more powerful and more frequent. In February 2023, Akamai mitigated the largest DDoS attack ever launched against an Akamai Prolexic customer based in the Asia-Pacific (APAC) region, with attack traffic peaking at 900.1 gigabits per second and 158.2 million packets per second (Mpps). That was just a few months after the largest-ever DDoS attack against an Akamai Prolexic customer in Europe in which traffic abruptly spiked to 704.8 Mpps in an aggressive attempt to interrupt the organization's business operations. This is on top of the largest DDoS attack Akamai has mitigated to date: a 1.44 terabits per second (Tbps) and 385 Mpps globally distributed attack lasting for nearly two hours. In fact, based on our insight into traffic and attack patterns, Akamai determined that throughout 2023, DDoS attacks became more frequent, longer, highly sophisticated (with multiple vectors), and focused on horizontal targets (attacking multiple IP destinations in the same attack event).

The growing threat

Most DDoS attacks today are multi-vector attacks, often employing more than 10 attack vectors to overwhelm rudimentary DDoS protection systems and platforms. Indeed, according to Akamai's internal threat intelligence, the number of multidestination or horizontal DDoS attacks doubled from 2022 to 2023. Meanwhile, the overall size, scale, and duration of volumetric DDoS attacks in 2023 were the highest on record.

Further complicating security planning for organizations is the evolution of a number of different tactics attackers are using in conjunction with traditional volumetric attacks.



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

DNS infrastructure

DDoS attacks on an organization's DNS infrastructure have become increasingly common — particularly NXDOMAIN attacks (also known as pseudo-random subdomain attacks, DNS water torture attacks, or DNS resource exhaustion attacks). More than 60% of the DDoS attacks mitigated by Akamai in 2023 had a DNS component, with NXDOMAIN attacks constituting approximately half of those DNS DDoS attacks. These attacks represent a significant risk to a company's bottom line and reputation, because if a company's DNS goes down, their online presence disappears.

Application-layer attacks

Application-layer (Layer 7) DDoS attacks have become more sophisticated as attackers are evolving their tactics to exploit seemingly benign logic and workflows. An HTTP/2 vulnerability discovered in 2023 led to the largest recorded Layer 7 DDoS attack ever.

DDoS as a service

Organized cybercriminal groups like Anonymous Sudan and Killnet are offering DDoS as a service. In this scenario, groups offer their services, typically a botnet, for a fee and will carry out attacks on behalf of a client. These DDoS-for-hire services can be extremely profitable for motivated groups.

Ransomware + DDoS = RDDoS

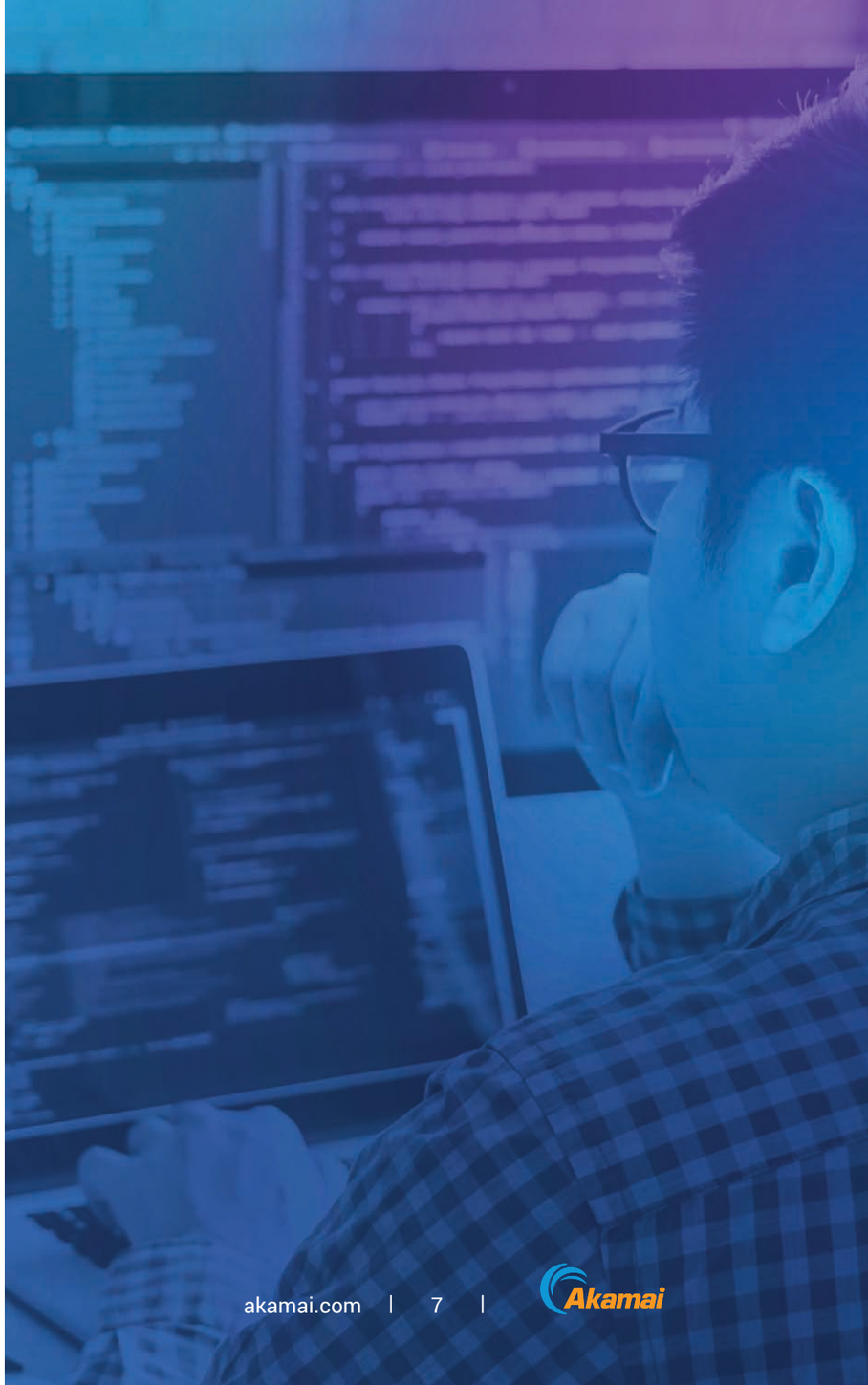
The availability of tactics like DDoS as a service also makes it easier for attackers to use DDoS attacks as a smokescreen to distract security teams. Meanwhile, they launch a concurrent ransomware attack or triple extortion attack. These are called ransom DDoS (RDDoS) attacks.

The consequences of a DDoS attack

With network (Layer 3) and transport (Layer 4) layer DDoS 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 Layer 7 attacks, threat actors aim to disrupt web performance and user experience through vectors like low and slow attacks and HTTP floods to produce downtime that impacts the bottom line. DDoS attacks on DNS can be a bit more complex — depending on the type of the attack, it could affect different layers of an organization's network. For example, DNS reflection and amplification DDoS attacks may produce traffic on Layers 3 and 4 of a company's network, whereas NXDOMAIN or DNS flood types of DDoS often attack the application layer of a network.

The repercussions of downtime affect more than just the cost of targeted services and unavailable applications. According to Ponemon Institute, the average cost of a DDoS attack on an organization is US$1.7 million per year, driven by increased technical support, consumption of incident response resources, internal escalations, legal costs, operational disruption, and that loss of employee productivity. Additionally, for consumer-facing businesses such as financial services institutions, gaming and media companies, and ecommerce organizations, going offline can not only inflict financial damages, but, more important, it can inflict irreparable reputational damages.

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

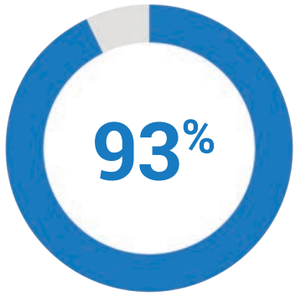


Hybrid and multicloud continue to complicate security

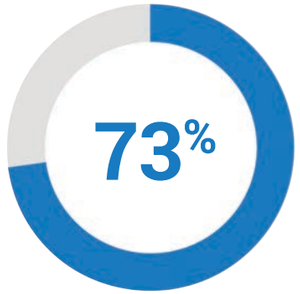
As organizations maintain some workloads in on-premises data centers or private clouds, and move other applications to publicly cloud-hosted environments, this hybrid approach to infrastructure makes ensuring robust security extremely complex. Similarly, companies often have a hybrid DNS infrastructure in which some of their authoritative DNS zones are managed in the cloud, with remaining zones managed by on-premises nameservers and global server load balancers (GSLBs). There are reasons why organizations might continue to maintain some on-premises DNS infrastructure. For example, they may have already invested significant capital in setting up on-premises infrastructure to meet compliance requirements. The complexity of migrating all DNS to the cloud might not be financially viable.

Threat actors are well aware of the vulnerabilities that arise from such a fragmented environment. They are eager to exploit the weaknesses in an organization's security architecture and posture that are created by inconsistent security policies and requirements. They seek to take advantage of the difficulties in troubleshooting across disparate and fragmented cloud-hosted infrastructure.

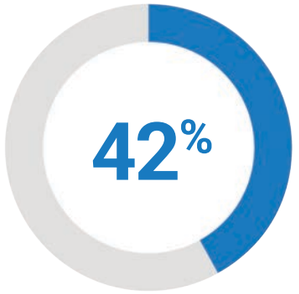
Unfortunately, the responsibility for security within public cloud environments can be inconsistent from provider to provider, with many organizations making false assumptions that could leave them exposed. For example, 73% of enterprise respondents in an IBM survey believe public cloud service providers (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 knowledge about security control responsibility can lead to compromise — a risk no organization should be willing to accept.



Employ a multicloud strategy



Believe public CSPs are responsible for securing SaaS



Believe CSPs are responsible for securing cloud IaaS

Organizations are turning to DDoS security providers that offer an integrated, highly scalable, and comprehensive DDoS protection platform that can protect their applications, APIs, DNS, and the underlying infrastructure that powers it all.

All DDoS mitigation is not created equal

As companies continue to invest in cloud infrastructure, ensuring consistent controls that span hybrid environments will be a challenge for security teams. And as applications deployed across multiple back-end cloud infrastructures become more difficult to protect, many organizations are seeking a single control point to orchestrate defenses.

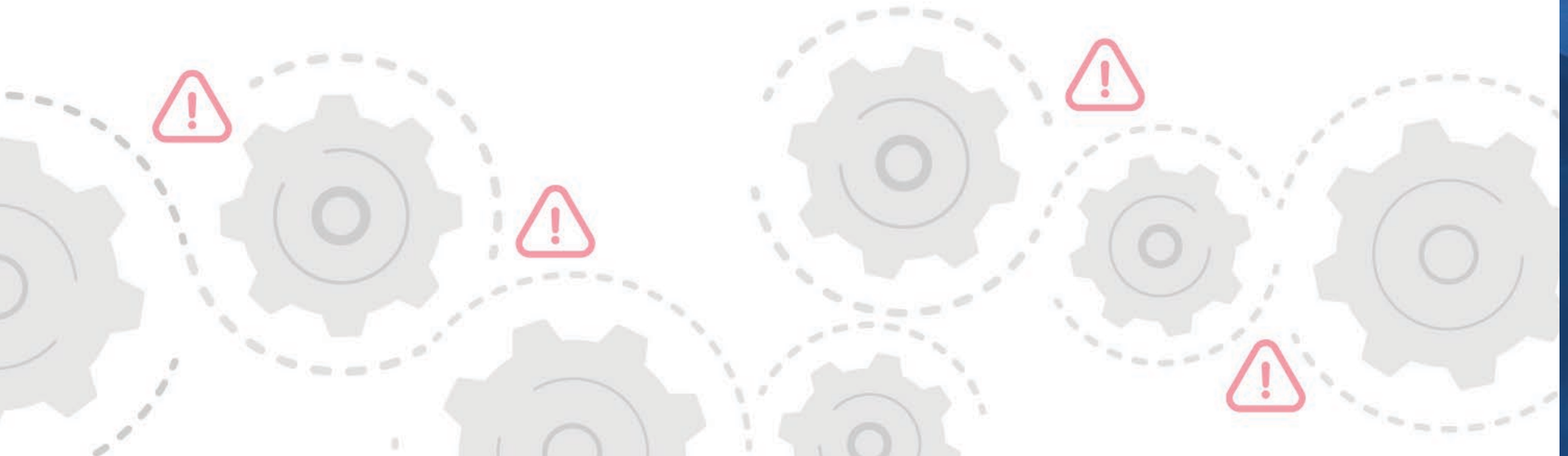
As the security technology stack grows more complex, many want a consolidated view of their environment — not only for optimized visibility, but also for streamlined reporting that can be fed via APIs into event data correlation systems.

To solve this problem, organizations are turning to DDoS security providers that offer an integrated, highly scalable, and comprehensive DDoS protection platform that can protect their applications, APIs, DNS, and the underlying infrastructure that powers it all. They want scalable, responsive defenses — regardless of where enterprise services may reside — on-premises, in the cloud, or in a hybrid environment. This is in direct response to the increase in operational complexity that is required to integrate, deploy, and manage DDoS defenses within a CSP's unique environment. And with many internet-facing assets located across multiple private and public clouds, things get complex quickly.

Adding to the pressure, many CSP in-house DDoS mitigation solutions fall short in key areas: visibility, service-level agreements (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 teams refer to CSPs as the black box of analytics and reporting. While some CSPs allow an organization's security team to set controls and maintain sovereignty over client-specific environments, they typically reject any liability for DDoS traffic and end up charging customers for the astronomical volume of malicious traffic that comes with a DDoS attack — whether or not it is an application-layer attack, a network-layer attack, or a DNS DDoS attack.

Additionally, some CSPs and security vendors don't offer a clear time-to-mitigate (TTM) SLA and instead offer service credits to the impacted organization. It is important to understand whether the TTM clause includes the time to identify an attack. If it takes several minutes or even hours for a platform to identify a DDoS attack before their mitigation protocols kick in, a victim organization could stay offline for a prolonged period. When seconds count, organizations need assurance that their provider will commit to maintaining uptime and availability without compromising performance.



Furthermore, it is equally (if not even more) important for security teams or buyer organizations to identify whether DDoS security vendors and CSPs offer **dedicated DDoS defense capacity** or if the defense capacity is shared with their CDN network. Dedicated DDoS defense is like a SWAT team that is exclusively focused on fighting DDoS attacks and does not share resources or infrastructure with other aspects of a business, like content delivery, thus ensuring minimal impact even during a record-breaking DDoS attack. Organizations that are evaluating DDoS protection need to understand that the vendors themselves will sometimes face DDoS attacks and should heavily factor in whether the vendor offers an uptime/availability SLA.

Finally, many CSPs and security vendors 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. If they do, it comes at a premium cost that is oftentimes more expensive than a specialized hybrid DDoS mitigation solution from a best-in-class provider. With a fully managed hybrid 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 threat landscape, it's clear modern businesses are turning to DDoS mitigation partners that support a streamlined security experience across hybrid environments and reduce attack surface complexity. Your DDoS protection partner should be an enabler of, not a hindrance to, your hybrid or multicloud strategy and be aligned with your business goals.

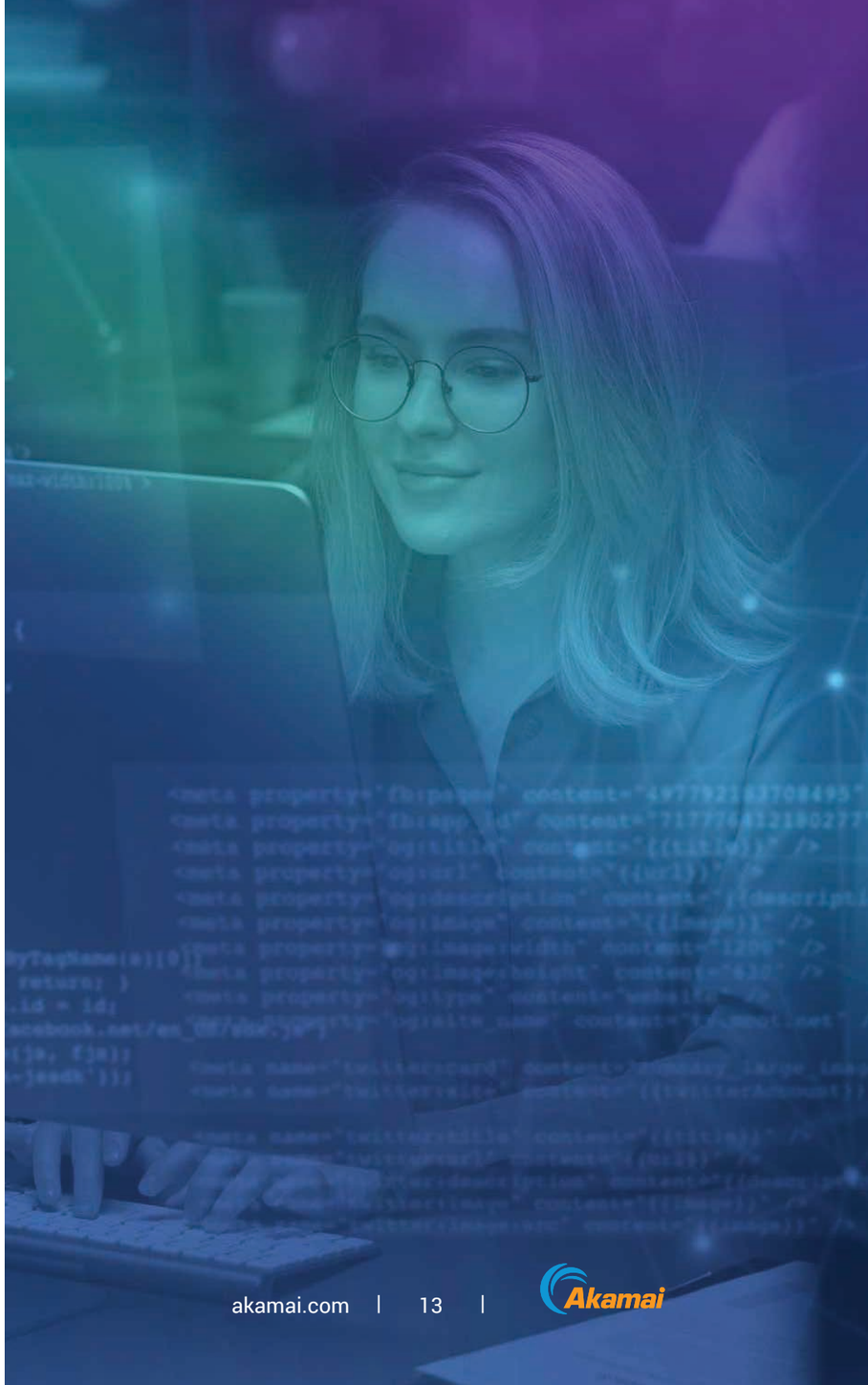
Purpose-built DDoS mitigation with Akamai

Just as organizations need an end-to-end digital infrastructure strategy that includes hybrid and multicloud environments, they also need to consider end-to-end DDoS protection. By taking a comprehensive approach, Akamai acts as a first line of defense, providing protection with dedicated edge, distributed DNS, and hybrid mitigation strategies designed to prevent collateral damage and single points of failure. As opposed to other CSP architectures — built as an all-in-one solution — Akamai's purpose-built DDoS solutions offer increased resiliency, dedicated DDoS defense capacity, and a higher quality of mitigation that is fine-tuned to the specific requirements of web applications or internet-based services. Akamai's DDoS defense is available to customers where they need it: on-premises, in cloud, hybrid — and how they need it: always-on or on demand. This comprehensive protection extends across three core products.

Dedicated DDoS defense capacity

Distributed DNS

Hybrid mitigation



Akamai Prolexic is world-class DDoS protection tailored for an organization's proactive and positive security posture

A modern and scalable architecture

Akamai Prolexic uses a fully software-defined architecture that can adapt to changing network trends related to edge computing, 5G/6G, and network virtualization. With the transition to virtualized software environments, Prolexic removed all dependencies on specialized hardware. This standardized deployment empowers Akamai to serve evolving customer needs faster, facilitate modular deployments for capacity extension, provide better regional coverage with low-latency links, and improve redundancy on the platform. Additionally, the architecture helps accelerate Prolexic's advanced behavioral learning capabilities to learn from attack signatures, adapt to emerging threat vectors, and proactively build DDoS-resilient postures for customers. Prolexic cloud is powered by multiple **scrubbing centers across 32 global metro areas and a total of more than 20 Tbps of dedicated defense capacity**. To put Prolexic's defense capacity in perspective, even the largest known Layer 3 and Layer 4 DDoS attacks don't make up 10% of the capacity available to Prolexic customers.

DDoS protection that is comprehensive, flexible, and reliable

Akamai Prolexic is available as Prolexic Cloud, Prolexic On-Prem, and Prolexic Hybrid.

Prolexic Cloud is the industry pioneer in cloud-based DDoS protection and offers customers zero-second mitigation and 100% platform availability SLAs. Mitigation controls dynamically scale capacity to stop attacks across IPv4 and IPv6 traffic flows. Compute resources can be dynamically allocated to whatever mitigation controls need to be scaled up.

Prolexic On-Prem provides always-on, physical or logical, inline, and datapath DDoS protection that natively integrates with edge routers to automatically stop more than 98% of the attacks at the edge of a customer's network without requiring traffic backhaul. This is ideal for the vast majority of the small and fast attacks and for businesses that require ultra-low-latency DDoS protection.

Prolexic Hybrid combines the power, automation, and performance of Prolexic On-Prem with the industry-leading scale and capacity of Prolexic Cloud on demand to protect customer origins from the largest volumetric DDoS attacks.

Taking security beyond DDoS

Akamai Prolexic comes with Prolexic Network Cloud Firewall — a fully self-serviceable and user-configurable capability that empowers customers to easily define, deploy, and manage their own access control lists (ACLs) and the rules that they want enforced at the very edge of their network. It's a firewall in front of all other firewalls. Network Cloud Firewall also recommends ACLs for the best proactive defense posture based on Akamai's threat intelligence data and delivers actionable analytics of existing rules. As a next-generation firewall as a service, Network Cloud Firewall empowers customers to:

- Define proactive defenses to block malicious traffic instantly
- Alleviate local infrastructure by moving rules to the edge
- Quickly adapt to network changes via a new user interface

Akamai Edge DNS and **Akamai Shield NS53** secure and fortify critical DNS infrastructure

Akamai Edge DNS provides you with comprehensive protection from a wide range of DNS attacks on your DNS infrastructure, whether it be on-premises, in cloud, or hybrid. The solution also offers a high level of DNS performance, resiliency, and availability. Built on a globally distributed anycast network, Edge DNS can be implemented as a primary or secondary DNS service, replacing or augmenting existing DNS infrastructure as needed.

Akamai Shield NS53 is a bidirectional DNS reverse proxy solution that protects on-premises and hybrid DNS infrastructure — including GSLBs, firewalls, and nameservers — from DNS resource exhaustion (aka NXDOMAIN) attacks. Customers can self-configure, administer, manage, and enforce their own dynamic security policies in real time. Illegitimate DNS queries and DNS attack floods are dropped at the edge of the Akamai network to protect critical DNS infrastructure from DNS DDoS attacks.

Akamai App & API Protector secures applications and APIs from DDoS attacks

Recognized as a market-leading web application and API protection (WAAP) solution, App & API Protector instantly drops network-layer DDoS attacks at the edge (for properties hosted on Akamai Connected Cloud) and provides thorough defense strategies against application-layer DDoS attacks.

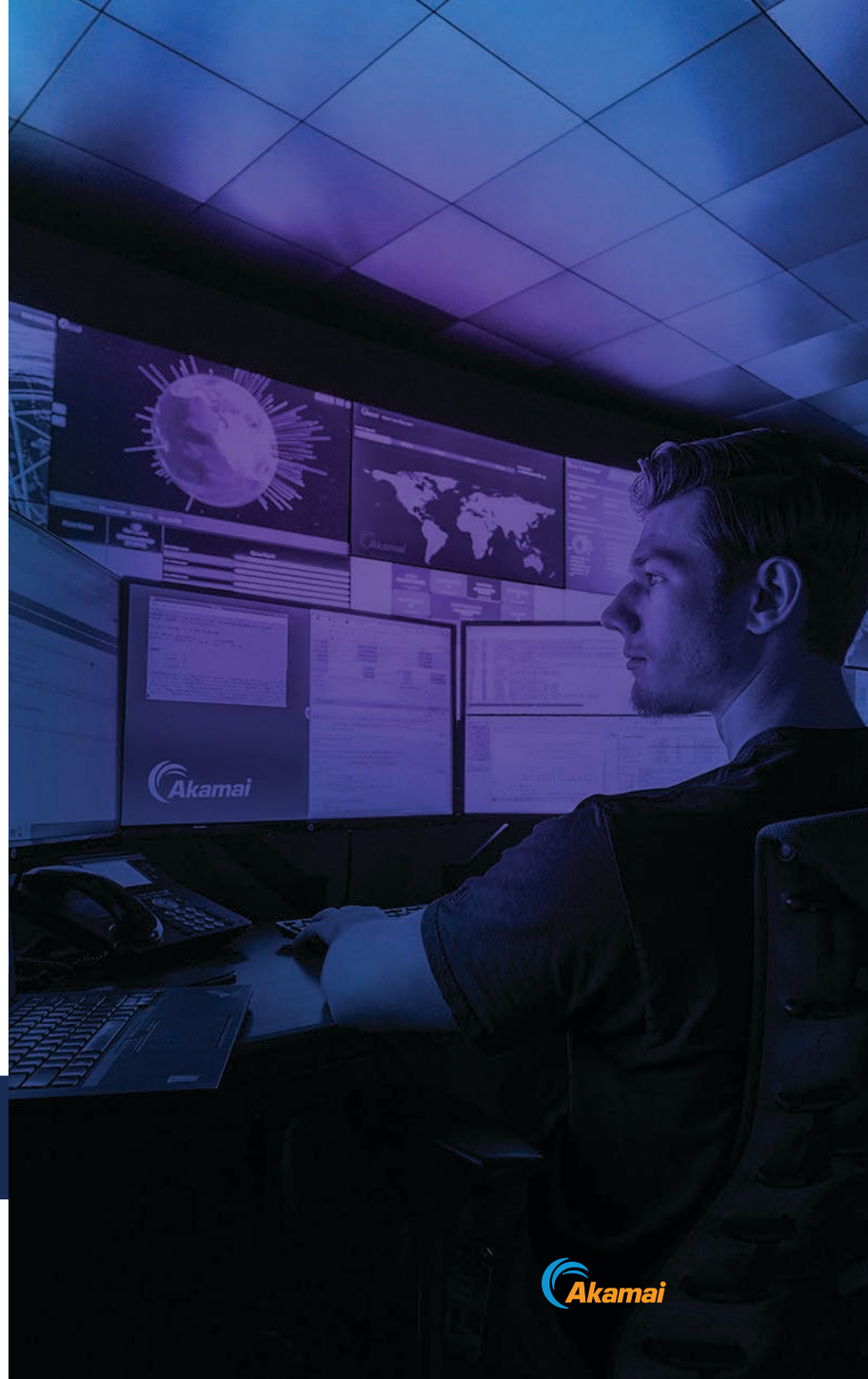
Why Akamai?

Akamai offers the world's most trusted global DDoS mitigation solutions. Whether you're protecting individual applications, entire data centers, or critical DNS infrastructure, 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 and an industry-leading SLA. And we can provide DDoS protection services for multiple clients and fight multiple DDoS attacks at once.

Because DDoS attack vectors keep changing and attack sizes keep getting bigger, a trustworthy DDoS platform must continually innovate, develop, and deploy capabilities to proactively detect threats, orchestrate mitigation strategies, and minimize impacts. Akamai is dedicated to staying ahead of threats by mitigating attacks before they start.

Your DDoS mitigation strategy should empower your hybrid and multicloud strategy. Akamai's next-generation DDoS solutions protect your digital network infrastructure, applications, and DNS on-premises, in cloud, or both, and offer the combined advantages of machine intelligence and human intelligence.



Learn more

 | Support | | Published 10/24