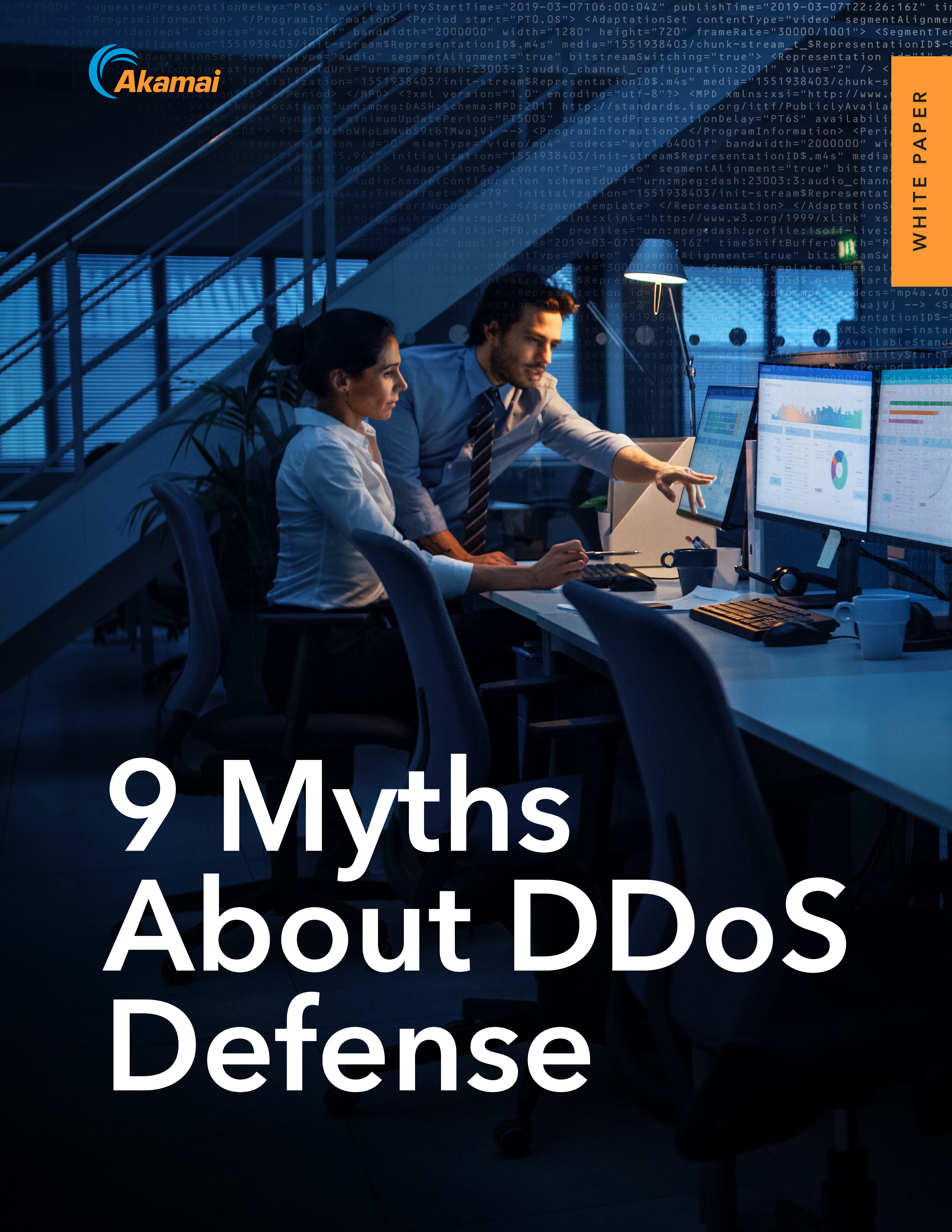
Akamai

WHITE PAPER



9 Myths About DDoS Defense

Over the past two years, the size of distributed denial-of-service (DDoS) attacks doubled, and the number and combination of attack vectors increased significantly. In 2020, an 809 million packets per second (Mpps) attack hit an organization, making the event the largest packet per second attack ever recorded. While some organizations may believe they're low-risk targets for a DDoS attack, business-critical services and applications in every industry are rich targets, and leave every business exposed to downtime and diminished performance if infrastructure isn't protected.

DDoS protection must be a key tenet of your overall security strategy, so being aware of the myths can be critical to your DDoS defensive posture.

There are a lot of myths about DDoS protection – some of them are even encouraged by security vendors.

Myth 1. Total capacity indicates available mitigation resources

A simple network capacity number leaves out important details. Questions that need to be answered include: How much network capacity is dedicated for consuming attack traffic? How many of the mitigation system's resources are dedicated to stopping attacks? How many of the network and system resources are available to deliver clean traffic to all customer origins on that platform? And capacity isn't just limited to technology. At some point, if technologies are not working effectively or optimizing mitigation, what dedicated human capacity can be leveraged for escalations, handling incident response and fine-tuning mitigation?

Tip: Look deeper into differences between a provider's total network capacity and platform stability, capacity available for attack mitigation, and clean traffic delivery utilization.

Myth 2. All time-to-mitigate SLAs are created equal

Time to mitigate should mean how quickly malicious traffic is stopped or blocked, without impacting legitimate traffic and users. It turns out that there's a lot of room for interpretation. For example, one vendor might not consider a surge in traffic a DDoS attack until it has lasted at least five minutes. So the SLA timer may not start until you're already five minutes into the attack. That means an advertised 10-second time to mitigate could really be five minutes or more. Other vendors define time to mitigate as how quickly a mitigation rule can be deployed. At the end of the day, what you care about is the time to get internet-facing assets back up and running. Be sure to carefully read the fine print for your vendor's SLA.

Tip: Dig into the details of time to mitigate listed in an SLA. It should represent the equation: Time to Detect Attack + Time to Apply Mitigation Controls + Time to Block Attack + Quality of Mitigation = The Real Time to Stop the Attack.

Myth 3. Blackholing and rate limiting are acceptable defenses

Blackholing is a common defensive response from some DDoS mitigation providers. If an asset is under attack and putting other customers at risk, the provider may try to prevent collateral damage by discarding that resource's traffic in a virtual black hole. Does that really help you? From an attacker's perspective, blackholing means mission accomplished – the targeted asset is effectively offline. Depending on the provider's infrastructure, other customers may end up going offline or experience degraded performance. As another response, many providers also rate limit customer traffic as a countermeasure within shared environments. But dropping 20%–40% of legitimate traffic to give the perception the asset or service is still up and running is not a successful outcome for the customer under attack.

Tip: Ask your provider how often they blackhole or rate limit traffic during peacetime or when under attack. Determine under what conditions a provider will blackhole traffic and what criteria you'll need to meet to have your services restored.

Myth 4. It doesn't matter who shares the cloud platform

Every organization needs security. Controversial businesses that attract frequent attacks, such as gray markets like gambling and porn websites, need security defenses, too. Even organizations promoting criminal activity and terror attacks have purchased cybersecurity from legitimate cloud vendors. It's easy to think that it doesn't matter to you. However, if your business shares a cloud security platform with an illegal or frequently attacked enterprise, the potential for collateral damage is high. The vendor's resources may already be tied up or overwhelmed, leaving your organization exposed.

> *If your business shares a cloud security platform with an illegal or frequently attacked enterprise, the potential for collateral damage is high.*

Tip: Read a cloud security vendor's acceptable use policy carefully to confirm that you won't be sharing security platform resources with high-risk targets.

Myth 5. An all-in-one security platform = better security experience

Some providers offer a variety of services stacked on top of a single-cloud platform, which might mean reduced technical complexity for deploying and integrating security controls in the short term. But multiple services sharing the same back-end infrastructure and networks are vulnerable to platform outages, collateral damage, and resiliency issues if other parts of the environment are disrupted. Oftentimes, one-stop-shop vendors sacrifice feature functionality due to limitations of designing a single-platform approach. A transparent mesh of purpose-built CDN, DNS, and DDoS scrubbing clouds, designed to solve specific technical and security challenges, means higher quality of mitigation and performance at scale to optimize defensive postures.

Tip: Keep in mind, you don't have to share the same infrastructure to achieve a unified security experience. Diverse underlying architectures can deliver both seamless user experience and high-performance mitigation.

Myth 6. An on-premises solution offers more control

While an on-premises solution allows organizations to turn the knobs and pull the levers themselves, the control can be illusory. The weakest link for any on-premises solution is often the size of the internet link. As DDoS attacks get bigger and more complex (multi-vector), even a typical attack of less than 4 Gbps can saturate the internet link and cause denial of service for even those data centers that include the best on-premises hardware. For on-premises deployments, you're essentially buying minutes to move serious attack mitigation to the cloud. With security talent not only scarce, but strained, organizations are outsourcing DDoS mitigation to cloud-based platforms vs. developing internal DDoS mitigation expertise.

Tip: You can't be in control if your network, IT, and incident response staff are overwhelmed. DDoS is an attack vector best handled by the mitigation experts. Double down on what you can do in-house and outsource to the experts.

Myth 7. You don't need multiple layers of defense

Most organizations don't actually believe this, but sometimes they build their defense strategy as if it were true. For example, consider the hybrid approach. An organization looking to bolster its on-premises security solution may upgrade by adding a cloud-based solution from the same vendor. One-stop shopping may be convenient, but it doesn't necessarily provide defense in depth. If multiple layers of defense are built on the same underlying technology, those layers will have the same gaps and weaknesses, leaving you just as exposed.

Tip: Layer best-of-breed technologies with different strengths and weaknesses, so gaps in one layer will be covered by defense in another.

Myth 8. Every SOC offers the same level of support

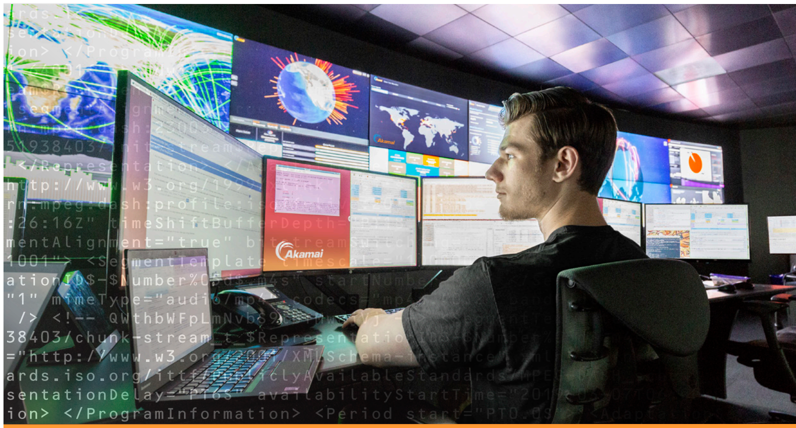
Many vendors advertise security operations center (SOC) support on their data sheets. But having a 24/7 SOC isn't what matters most. What's important is the level of service and expertise you can expect to receive when your assets are under attack. Some key considerations when evaluating DDoS mitigation providers should include: What type of support and analysis would you receive before, during, and after an attack? How is the SOC staffed to ensure continuity of defense? If you contact the SOC, is the person you call the actual analyst performing mitigation, or only the escalation point? Does your provider have security professionals trained on mitigation, or are they "traffic cops" routing traffic to off-the-shelf mitigation gear? Do they offer a custom runbook? Your security provider's SOC should act as an extension of your incident response team to drive real value.

Tip: Evaluate the expected quality of support you would receive from the service provider's SOC. Aside from attack detection and mitigation, determine if they offer integration and testing, incident troubleshooting, post hoc analysis (lessons learned), and design support to help reduce your attack surface.

Myth 9. DDoS protection is all-inclusive

While a lower price may seem attractive, there could be hidden costs. Some vendors offer a low price but restrict the number or size of attacks that they'll mitigate. If you are targeted with too many attacks, or too large an attack, they will ask you to upgrade to a higher (and more costly) tier of service before stopping the attack – all while you're trying to get your business back online. When comparing vendors and prices, make sure you understand the trade-offs and their impact on your risk posture.

Tip: Understand what's included in the price you're quoted before you sign.



If you are targeted with too many attacks, or too large an attack, some vendors will ask you to upgrade to a higher (and more costly) tier of service before stopping the attack – all while you're trying to get your business back online.

DDoS security is complex, time-consuming, and ever-changing. Staying connected to your clients, customers, and employees is the basis of your business. There's no room for error here – and there's no need to bear the high cost of trying to go it alone. As the largest, most trusted cloud delivery platform for web security, Akamai can help. Learn more at www.akamai.com/secureapps.