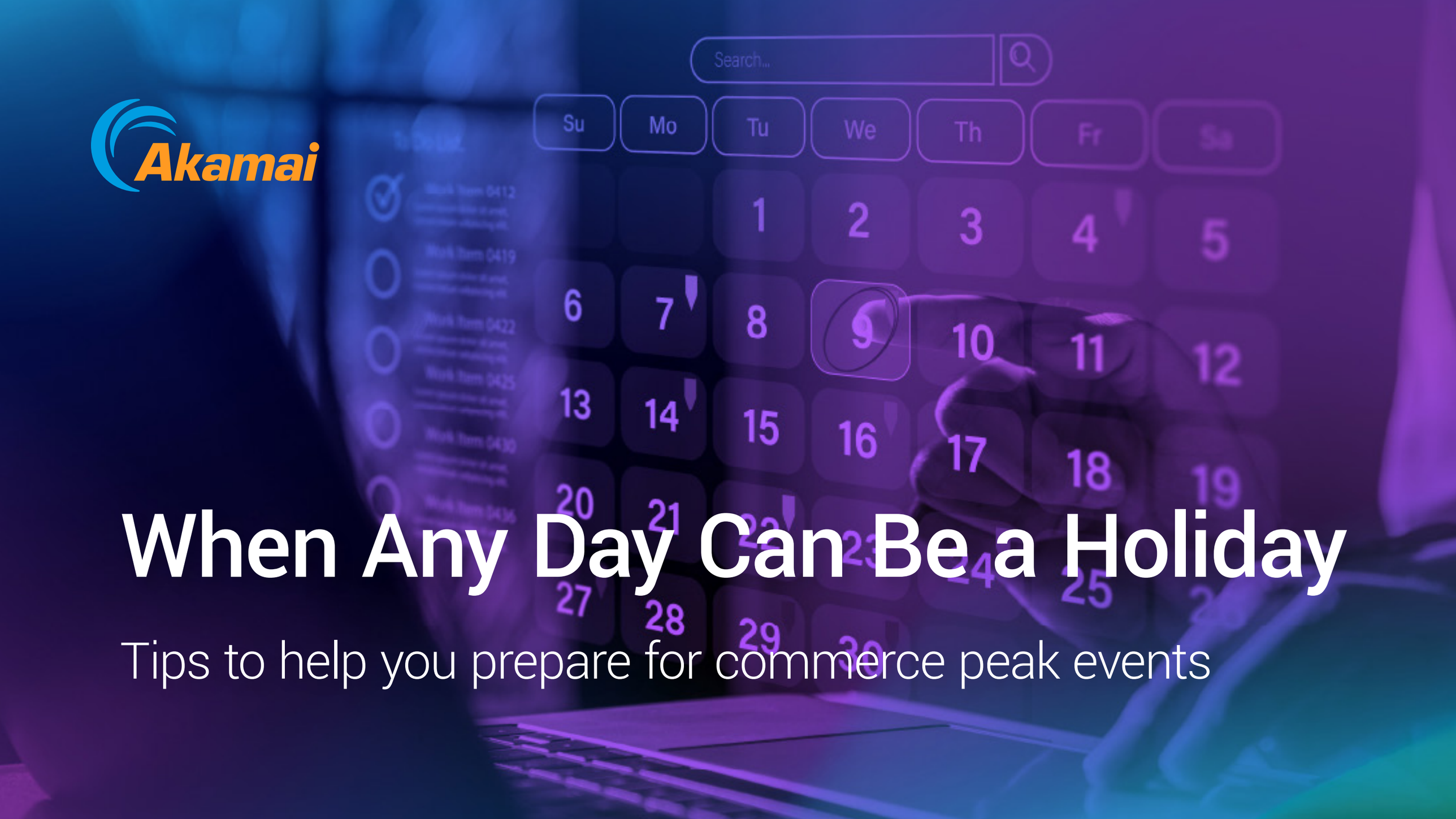

When Any Day Can Be a Holiday

Tips to help you prepare for commerce peak events

Introduction

The traditional “big three” American shopping holidays — Thanksgiving, Black Friday, and Cyber Monday — aren’t the only peak events for commerce companies, which include retail, travel, and hospitality organizations. Any day may be a peak event, depending on your business or industry. For example, Valentine’s Day is the biggest day of the year for a florist, while summer vacation looms large for travel and hospitality companies. A health insurance company will see spikes in visitors during open enrollment, while a retail company will get a rush whenever a new product goes viral or back-to-school shopping starts. If we expand beyond the United States, peak events could arise because of the Olympics, the World Cup, or holidays such as Diwali, Lunar New Year, and Oktoberfest.

Lessons learned from managing performance needs and security risks on traditional peak days can apply to any peak or high traffic event. In each case, you must successfully handle single-day bursts in traffic and risk well above your typical levels. And in every case, the stakes are high: Failure to successfully manage these moments can result in revenue loss and reputational harm. Success in managing these events means increased revenue and happy customers.

After reflecting on 2024, when 4 of the top 10 largest distributed denial-of-service (DDoS) attacks ever recorded against Akamai customers took place, we have a clear indication that the stakes are higher than ever in 2025. Akamai has observed that the number of attacks targeting multiple destinations — known as horizontal attacks — has nearly doubled over the last several quarters. It’s not just that modern DDoS attacks are multidestination and multi-vector — they’re also extending in length, often unfolding as well-orchestrated campaigns that span hours, days, or even weeks. This combination of scale, complexity, and duration underscores the shift from volume to sophistication in today’s threat landscape.

Preparing for peak events requires optimizing performance of your platform, preparing for worst-case scenarios, updating your security posture, and conducting an after-action review to learn how to ensure that your next peak event goes off without a hitch.

In the following four chapters, we provide best practices that will help you prepare for any peak event — whenever and however often those events occur.

Insight

Peak events are changing. Your peak strategy needs to change, too.

Today’s customers expect the holiday season to start earlier and last longer — often stretching over weeks or months. Akamai data shows that while U.S. events like Black Friday and Cyber Monday remain major traffic peaks, online activity now ramps up earlier, beginning around Thanksgiving week.

Globally, peak periods vary — driven by regional holidays and shopping events like Singles’ Day in China, Diwali in India, or Boxing Day in the United Kingdom and Canada. With shifting consumer behavior and broader macroeconomic uncertainty, peak readiness is no longer about a single event. It requires a sustainable, agile approach that enables your teams to respond to multiple high-demand moments without disrupting operations or customer experience.

CHAPTER 1

Getting ahead of the performance curve

Planning ahead is key to optimizing your website's performance at higher-than-normal traffic loads. It goes without saying that a good content delivery network (CDN) is an essential component of your strategy. But you also need to plan out how to ensure that your site will function well as more visitors interact with it — and how to respond when your system needs help under stress. There are three content types that are part of this picture, and each should be treated differently to maximize performance and increase offload.

HTML page structure that makes up your base website content (target offload should be 50%)

Other static content such as **JavaScript, CSS, images, and videos** (target offload of 80%, but we recommend striving for 90% and above)

API traffic such as mobile apps, pricing, logins, and checkouts (optimal offload varies depending on the nature of API calls and the data being retrieved)

Here are five best practices to ensure that your system's performance is optimized and tuned for a peak event.

Tip 1: Review caching settings beforehand

Assess what you are caching and where, to make sure that your caching strategy is the best it can be for everyday purposes, before you even add a peak event into the equation. The goal is to optimize how your site looks and feels, and to deliver your desired web experience as fast as possible with maximum personalization. Cache settings primarily apply to static content and assets, which should be cached as much as possible for your business requirements. It's better to cache an image on your load balancer at origin or on your CDN — or even to push it to your user's device — than to pull it from your web server.

With HTML, there is a lot more cacheable content than at first glance. It's possible to structure your site and make decisions to fragment the content to get a higher HTML offload. For example, if users on the site are not logged in (dynamic personalization of content is not available to be served), then content can be cached and reused for this group. The bottom line: If a large percentage of users are not logged in, then cache for them accordingly. For other types of static content, you should strive for 90% offload and above. We recognize that you are probably already spending a lot of effort optimizing this type of site content, but just double-check to make sure you are hitting your targets. Finally, although some API data is so dynamic it can't be cached, consider which API calls *could* be cached, like shipping quotes, store locations, or pricing. If inventory updates every 60 seconds, why not cache for 30 seconds? If pricing updates once a day at midnight, then cache all API calls every 12 hours. During your peak event when every dollar counts, every second that can be cached will increase your offload when it matters most.

Tip 2: Increase offload during the event

Next, look for advantages you might be able to gain by caching certain content only during your event. If you cache pricing or shipping quote responses for a few minutes, for example, you could free up your servers so you can scale higher at a reduced cost. Some other ideas include caching redirects like dynamic page assembly, pre-render, and image optimizations — and you should be caching redirects at the edge. During the event and even after, there may be a lot you can offload, including business logic, user experience, redirects, search engine optimizations, and bot management.

Tip 3: Optimize images and video

Images and video may be static content, but there's a lot you can do to help serve them to your customers in a simplified *and intelligent* manner. It's essential to work on image and video optimization prior to your peak event for the best user experience. You will most likely need to work with an image optimization provider to ensure that you serve the right size, format, and viewpoint of your image or video assets at the right time to each customer. This process also requires you to consider all the combinations of devices, browsers, operating systems — and even network connections — that your customers may use or have. By optimizing your images and videos, you can:

- Make your pages lighter and faster (reducing bytes without degrading quality)
- Enhance load time and site responsiveness
- Streamline asset management to reduce work for your creative and design teams

Tip 4: Identify and manage bots

Research indicates that 42% of overall web traffic is composed of bots, and 65% of these bots are malicious. It's crucial to have a strategy for bots to avoid surprises during peak events. Serving bots during a peak event diminishes your capacity to serve paying customers at a time when you need as much of that capacity as possible. You can use toolsets to identify what kind of user is making a request and the intent of that transaction, which can allow you to prioritize certain bot interactions and deprioritize others.

Managing the "good" or "known" bot transactions is critical. Imagine a bot problem funnel where the top is broad and relatively easier to deal with from a detection perspective. The further you go down that funnel, the more expensive and more difficult it is to deal with the evasive nature of the bot activity. So having a holistic approach to bot management is imperative. One strategy to reduce bot load is to serve bots pre-rendered and cached content from a different origin. Another strategy is to turn off all site crawlers during peak hours and suffer the short-term SEO consequences to maximize revenue. Within the bot population, you should be equipped to make more granular decisions about how to handle different types of bots during your peak event, especially if you don't want to pay to serve them.

Tip 5: Embrace "graceful degradation"

You should be able to lose a portion of your functionality while still keeping your site running. In fact, you're probably never running without some functionality shortfall; that is, you're likely always in some state of "graceful degradation," which is a concept from complex systems. You can architect your system to strategically run in a "degraded" state during peak loads to enable better performance. An example is a large online retailer suspending its recommendations function during peak shopping days because the function's business value isn't worth the load it puts on the system. This boils down to the concept of resilience. Over the past two years, this has been the number one topic in the C-level playbook. Simply put, how well can you weather the storm, even when you don't know when the storm will strike? You need to not just stay online, but ensure the business continues to thrive even while under duress.

CHAPTER 2

Preparing for the worst

Now that you've designed your system to successfully handle the loads you expect during peak events, think about what you'll do if your expectations of success go awry.

Peak-traffic moments throw your operational constraints and vulnerabilities into high relief because you're already strained. In the pressure of a peak event, you may not have time to identify problems — much less respond to them — before it's too late. That's why it's critical to prepare for potential problems before they impact your customers or your revenue. Spend time before your event to gain a solid understanding of your anticipated load and its possible effect on your security, performance, and reliability. Verify where you think you can run, and create contingencies in case you can't.

Here are four best practices that can help you ensure that you're prepared for every eventuality.

Tip 6: Perform stress and load tests

The first step in this process is identifying an unacceptable result. The goal is to identify the bounds and to have a plan for when those bounds are exceeded. Stress testing and load testing help you establish those bounds and understand what's expected. Run stress tests multiple times in the months leading up to a peak event, with the expectation that your system will fail at first. You'll have time to correct problems and become more confident in your ability to handle the necessary load.

Tip 7: Deploy a waiting room

Your site must have the ability to throttle traffic on demand. A waiting room allows you to maintain your checkout flow during peak times and manage user experience when unexpected issues slow down that flow. This tooling also allows you to employ graceful degradation, such as by time-shifting or offering early exclusive access. And a key benefit of a waiting room is that it can operate as a failback to employ if things go wrong.

Tip 8: Plan for disaster recovery

Disaster recovery is designed to respond to a major natural, cyber, or business disaster, and recovery can often take days or weeks. What if this disaster happens in the middle of your peak event? For example, if it takes you four days to fail over but your event is four hours long, you don't have an effective disaster recovery plan. Match your disaster recovery planning and exercises to the likelihood that you're going to need them, and make sure that your time frame and ability to execute are compatible with that likelihood. Ultimately, moving toward an active-active approach (with multiple systems employed) and away from a disaster recovery stance can help ensure that no single disaster damages your operations.

Tip 9: Maximize observability

Monitoring lets you know how your system is performing during a peak event. It's important to monitor technical measures as well as business measures. Half your dashboard might be dedicated to technical metrics like CPU, throughput, and page load time, while half is tracking business measures like click-through rates, cart abandons, and conversions. You need both because the technical metrics may tell you why something's broken but won't tell you the impact the issue is having on real users. For that, you need the associated business metrics. Maximizing observability of these measures helps you detect anomalies, which can trigger automated actions to repair harm.

Insight

What does an increased load look like?

Increased load on your system can range from a modest bump during a regional promotion to a massive surge driven by a global event or coordinated attack. Between Q1 2023 and Q4 2024, Akamai observed over 230 billion web attacks targeting commerce organizations, underscoring how traffic spikes are no longer just about customer demand — they're also about defending against increasingly aggressive and automated threats.

CHAPTER 3

Bolstering your security framework

Security is always discussed in terms of risk — risk identification, risk mitigation, risk impact, risk likelihood — and it's critical to decide how you will respond to that risk. It's essentially a balancing act. You could choose to be more aggressive against potential risks during peak events, for example, but that could affect your user experience. Best practices for security include ensuring that your platform has well-tuned controls, setting traffic thresholds, determining how to consume alerts, and having a plan for how to act when problems arise.

Check out these six best practices.

Tip 10: Review your runbook

Your runbook should detail all pertinent information about people, processes, and prerequisites in your security strategy. For people, list on-shift schedules, knowledge base and gaps, and training required. For processes, create a protocol or flowchart so everyone knows what to do and who to contact for every eventuality. For prerequisites, describe the dependencies and communication requirements for security escalations. The runbook should also list emergency protocols aimed at protecting origin as much as possible. And finally, make sure you put this runbook to the test on a regular basis. Only through careful analysis of what goes wrong during your "test scenarios" can you make sure that there will be minimal issues and less chance of errors during a real event.

Tip 11: Don’t be caught off guard by DDoS attacks

To mitigate DDoS attacks, make sure your platform has well-tuned rate controls. Deny traffic above certain thresholds and send healthy HTML feedback to deceive bot traffic. Caching is a working weapon against DDoS attacks, so cache as much as you can. Conduct a tabletop exercise to find visibility gaps or inefficiencies in your incident response processes. For the most effective mitigation controls, work with a security vendor that is close to the ground and understands your environment and the nature of your web-facing applications. This means protecting the three main pillars of your online presence: 1. Ensure your website is online, respond to good requests, and have a plan in place for Layer 7 DDoS. 2. If your network IP space was to come under an attack, you need to have a BGP-based DDoS defense solution, which usually involves routing all network traffic through a scrubbing service while under mitigation to keep the attacker traffic far away from your routers and IP-based equipment. 3. And finally, protect the availability of your DNS nameservers and the core function they provide in the event of an attack. DNS-related attack techniques were used in 60% of all DDoS attacks that Akamai mitigated in 2024. DNS will always be a favorite of attackers when your peak days are on the line. After all, if your website cannot be found via DNS, even the good users won’t be able to visit it.

Tip 12: Don’t forget about the customer

With web skimming and Magecart attacks on the rise, it’s essential (and required with PCI DSS v4.0) to manage and monitor all JavaScript execution behavior on your web applications to defend against client-side attacks during your peak event — *and beyond*. The holiday season in particular is also prime time for fraudsters to hijack your brand, creating fake sites and social media accounts designed to steal credentials and credit card information, or sell counterfeit goods or fake reservations. As part of your strategy, make sure you have a monitoring tool in place — and a plan to respond when a fake site or abuse is detected — to protect customer loyalty and trust.

Insight
DDoS attacks are breaking records

DDoS attacks continue to grow in both size and sophistication. In fact, 4 of the 10 largest DDoS attacks ever mitigated by Akamai Prolexic occurred in 2024. One of the most significant DDoS attacks place in August 2024, when Akamai mitigated a 1.3 Tbps attack targeting a major U.S. customer — the third-largest volumetric DDoS attack ever recorded on the platform. The attack used a highly distributed botnet and cycled through multiple vectors in rapid succession, showcasing the increasing complexity of modern DDoS campaigns.

Tip 13: Understand your API attack surface

API sprawl is a challenge for any organization, especially those in commerce. Set up an inventory discovery process for APIs and run the audit. Your security team might not be familiar with newer APIs that your app team is running through the platform, so it's important to register those new APIs to the platform and make sure the inventory is accurate. If your security team doesn't recognize an API, they might block it — but if APIs are registered, the team can protect them. Another best practice is to make sure your web application firewall is up to date and in automatic mode.

Tip 14: Tune alerts to reduce noise

It's important to monitor everything, but there is danger in creating too much noise. Too many alerts essentially means no alerts, as your team may fail to pick out what's important. Tuning your alerts helps you reduce the noise and become more responsive. Perform this step well before a peak event — not at the last minute. And it's important to develop a routing plan for the alerts that conveys the key information so the right people can respond.

Tip 15: Bump up your defense against bad bots

Certain types of bots can be considered benign — but others can be used to launch DDoS attacks, scrape content or inventory, open fake accounts, perform credential stuffing attacks, and worse. Even good bots can slow your site down to unacceptable speeds during your crucial peak event. Make sure your bot strategy allows you to be as aggressive as you need to be to shut down bad bots, focusing on emergency protocols for what to do, how to do it, and who to work with to neutralize them. Tooling can allow you to track bots separately, and accurately account for the impact of an attack that can lead to compromised accounts, outages, and even data breaches.

CHAPTER 4

Capturing your lessons learned

The process of preparing for and carrying out peak events provides a lot of both technical and business-oriented information, making it critical to capture lessons learned to help your team improve. However, finding the time and energy to conduct a formal review can be difficult, especially just after your peak season. For companies that undergo regular or frequent peak events, it can be hard to squeeze reviews between them. However, we think it's an essential best practice to put your post-event review on the calendar so it is more likely to occur.

To support you in doing just that, we're giving you one more tip.

Tip 16: Conduct a formal review

Conduct your post-event review while the event is still fresh in the minds of everyone in your organization. With a clear memory of the event, your team can bring actionable insights to interpret the valuable data you've collected from the event and prioritize activities for next time.

- Did you measure the right things?
- Were there any gaps in your metrics or processes that you want to bridge before the next event?

Preparing well ahead of time for a formal post-event review of your technical and business performance sets you up to gain the most from what you've learned and the data you've gathered.

Transform your approach to peak events

When any day can be a peak day, your goal should be to make peak events less of an exception and more of a standard occurrence that you're always ready for. That's where we come in. Getting support from an expert like Akamai can make the entire process much easier. And as you learn, you can gradually integrate your preparations into your technical architecture, processes, and culture so that they become second nature. At that point, any day could be a holiday, and your team will be well prepared.

Are you ready to elevate your business's performance during peak events?

Learn more about Akamai's retail, travel, and hospitality insights and solutions — or contact an Akamai expert.

Akamai