INSTART

How to migrate from Akamai to Instart

SOLUTION BRIEF

Contents

Introduction

Instart provides a modern approach to delivering and protecting exceptional web experiences. We have a large number of customers moving to our platform from legacy CDNs such as Akamai. Through our discussions with them, we have discovered that they are upgrading to our cloud services because they are looking for faster, more reliable performance, better security that offers advanced bot protection, and the ability to manage not only their own code and content, but the third-party tags or scripts they are using to build their website experiences.

As a result, one of the most common questions we hear is: Is it difficult to convert from Akamai to Instart? Our team has a lot of experience with helping customers upgrade from their former CDNs. Even better, it's a very simple process — here are the five steps you need to know to move your website or web app over to Instart.

Step 1: Send us your Akamai configuration — we'll do the heavy lifting

The good news is that you can export your existing Akamai configuration easily, including all your routine delivery and security rules as well as any custom configurations and logic specific to your website or web app. From there, we'll take over. Our team of experts will assess your configuration and convert everything for Instart — shifting over rules that are still currently in use and helping you to identify legacy configurations that are no longer used on your site. We also take a look at any automated log delivery configurations you have set up and duplicate them within Instart, even matching the log format your systems expect.

Think your configuration is too complex? Not a problem. Our team has taken on configurations with thousands of lines and easily migrated them over to Instart. We've seen it all and have taken customers with thousands of lines of configuration onto our service.

Step 2: Give our service access to your origin web infrastructure

Many customers will lock down their origin infrastructure so that only the Akamai service can make incoming connections. It's a smart move that prevents the bad guys from getting around your security layer to attack your backend infrastructure. This is generally done using a default deny rule on your networking infrastructure and allowing specific IP addresses from Akamai in. We will provide you with our IP blocks which you can add to your allow rules so that our service can make incoming connections as well.

Step 3: Test your site and your systems running on our infrastructure

Once we get everything setup and complete an initial round of testing, we will do a handover to your teams so you can test to make sure everything is ready for launch. Generally customers just run their normal QA process against our service. Your testing teams can route requests through our service using a simple DNS override. It's likely the same process you are already using for your own internal development environment testing. And you can also use third-party synthetic testing tools, such as Catchpoint or WebPageTest, to check out the performance of your website on our system as well. During this testing, if you have a log ingestion system setup, our team will ensure we are feeding you all the right data.

Step 4: Go live with a percent of traffic and do a controlled migration over a few days

After testing, you are ready to go live and improve the performance and security of your website. We have a variety of approaches to easily and safely shift traffic onto our system. The most popular approach is to start by sending a percent of DNS requests to Instart. You can start by sending 5 percent of the traffic to our system — After that,and then we ramp up the traffic to 100 percent over a few hours or days. This ensures you can do a controlled migration over to Instart with the ability to roll-back on the off chance any issues arise.

Step 5: Security tuning

Since security configuration must address real world situations, our security experts continue to monitor live traffic after your website is migrated. Instart provides ongoing WAF and bot defense tuning to ensure our services are

defending your website against nuisance and malicious visitors while allowing legitimate traffic to flow undisturbed.

We have successfully moved thousands of sites over to Instart from Akamai and other legacy CDN platforms, and we are professionals at doing it safely with minimal impact to you and your teams. And then once you are migrated we have a great set of security, support, and customer success teams that will ensure you continue to have a great experience and get access to the latest tools to improve the protection and security for your site.

Security comparison

	INSTART	Akamai
Web app firewall	●	●
Advanced bot protection	●	◑
3rd party javascript protection	●	○
Advanced security analytics	●	◔
Request blocking/throttling	●	●
Custom security rules	●	●
Networks lists	●	●
Managed security	●	●

Performance and availability comparison

Image optimization	●	◕
Image adaptation	●	●
Dynamic HTML performance	●	◔
Javascript performance	●	◑
Network acceleration	●	●
3rd party javascript performance	●	◔
App network acceleration	●	○
Shopper prioritization	●	●