Comparison Review

Akamai vs Incapsula

Website Security, Acceleration and High Availability

It's been almost two years since I last blogged about Incapsula - a security and acceleration CDN-based service for websites and applications. Since then, the company has made a lot of progress, going from a security focused CDN to a full-fledged cloud-based ADC (Application Delivery Controller).

With these new features in place, it looks like Incapsula is moving to challenge the legacy CDNs, both with its unique cloud-enabled technologies and with a competitive price point, which tries to pull the rug from under the industry veterans.

But can Incapsula really cause a shift in this, very much consolidated, online industry? To answer this question I decided to put Incapsula to the test by comparing it with Akamai – a globally recognized leader of the CDN space.

For those of you who want to skip to the chase, here's what I think about Incapsula in a nutshell:

Akamai vs Incapsula: In a Nutshell

Incapsula simply offers more for less. You get all of the essentials you would expect, including a robust CDN, PCI compliant Web Application Firewall, DDoS protection and integrated high availability features (both load balancing and failover), all at very reasonable price point.

Not only that, but when compared with Akamai it looks like most of Incapsula features actually offer more, both in terms of their functionality and in term of their overall synergy. One great example is Incapsula's Real Time view which complements its custom security rules engine and load balancing features by providing instant feedback on every action taken.

In fact, when looking at value for money, Akamai does not offer any tangible benefits – at least not for those who are looking beyond a CDN-only option.

Read on for my full comparison.

Web Application Security

Incapsula's WAF utilizes proprietary, non-open source technology. This is important because it enables Incapsula to offer a higher level of security, flexibility and compliance.

For example, as a proprietary solution, Incapsula's WAF is immune to counter-intelligence, while Akamai's Mod_Security (Open Source) firewall's core is exposed to investigation by potential adversaries. This is also why Incapsula's WAF can also comply with PCI DSS 6.6, which Akamai's OS-based solution does not.

Beyond the generic security rule sets, both Akamai and Incapsula offer custom rule engines, which allow their users to implement additional security policies. The difference here, however, is in the implementation.

Custom security rules are needed most in case of emergency, where rapid rule implementation is key to countering an ongoing attack. Here, Incapsula has a significant advantage by offering instant rule implementation via user-side scripting, assisted by a GUI that allows you to generate and test new rules on the fly and real time view that provides instant feedback once the rules are in place.

In Akamai's case things are much more complex because custom rule generation requires users to contact the support team. So the propagation process can take anywhere from days to weeks just for the initial activation, with every additional tweak further extending the implementation cycle.

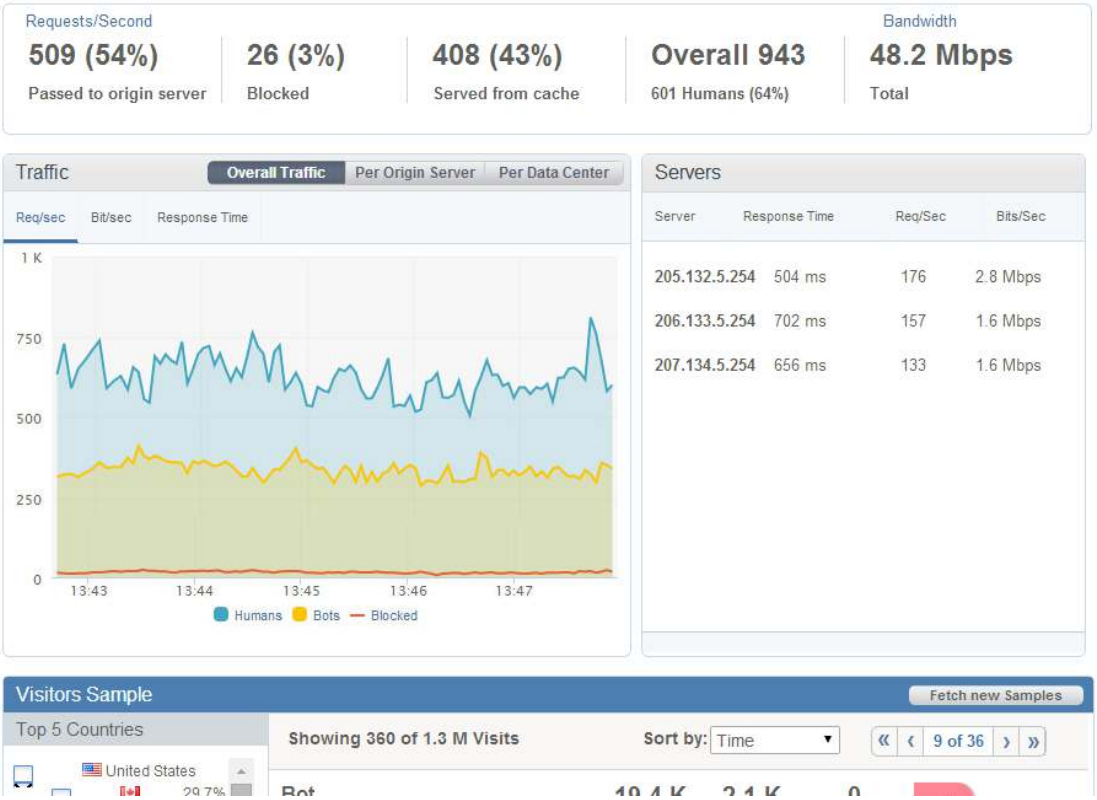
Another Incapsula security feature that impressed me is their two-factor authentication (2FA). This feature lets you control access to any website or application, deploying the 2FA protection on a URL of your choosing. Akamai's users who need second level of authentication must rely on third-party solution, which translates into additional costs, separate database integration and management, additional coding, and etc.

DDoS Protection

Incapsula is already known for its classification engine and proprietary bot filtering capabilities, which enable it to mitigate advanced and highly evasive Layer 7 DDoS attacks with a very low rate of false positives. These capabilities set Incapsula apart from other DDoS mitigation solutions, Akamai included.

When it comes to Network DDoS protection, Akamai's high-capacity CDN with ~1000 POPs around the world gives it more than enough network muscle to handle the largest network DDoS attacks. Incapsula's always-on DDoS mitigation solution is also proven to handle volumetric network attacks with minimal impact on user experience. With over 650GBps of capacity, and new data centers popping up every month, Incapsula also ranks among the "brawniest" DDoS protection providers.

In terms of monitoring and response options, both companies provide premium 247 support from a dedicated NOC, which is crucial for those who come under DDoS-fire. On top of that, Incapsula provides a dashboard that displays traffic data in real-time, enabling immediate response to DDoS attacks and fast feedback regarding the effect of newly propagated rules. Having this level of live visibility, and the ability to provide real-time response, scores another point for Incapsula.



Incapsula's Real Time View (Source: www.incapsula.com)

Load Balancing and Failover

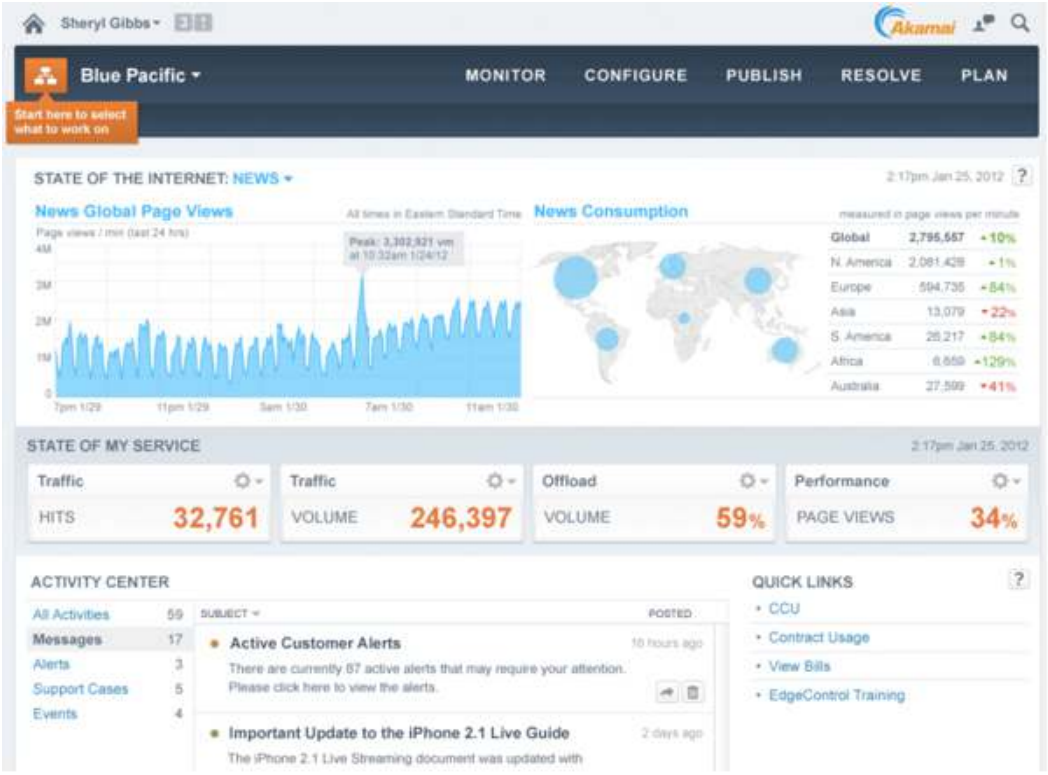
Akamai's availability solutions are all DNS-based and, as a result, are prone to TTL-related issues, which result in uneven performance and delayed propagation. Incapsula, on the other hand, relies on its own global network of reverse proxy servers for all failover and load balancing functions, which ensures instant propagation and zero TTL reliance.

This is actually a pretty big deal because TTL/DNS cache delays are notoriously bad for businesses that need to stay operational, even in the event of multiple server failure. I believe that Incapsula's ability to provide instant failover is what makes the platform so popular with Bitcoin exchanges and other online trading platforms, for which any downtime is not an option.

In terms of settings, both Akamai and Incapsula offer a very similar set of choices: geo-location and connection based distribution algorithms for cross-data center load balancing and several randomized and non-randomized algorithms for in-data center, including "least pending request", which is the one you want to have for optimal load distribution.

The CDN Designed a decade ago to address network latency issues, Akamai's massive network of ~1000 POPs, with coverage in every region of the world, provides a very powerful acceleration solution. Incapsula offers a more up-to-date architecture, with a smaller number (currently 16) of large data centers, each of which delivers much more server power. This efficient architecture provides for better management options, allowing for instant response to security threats (e.g., instant aggregation of custom security rules) and swift deployment cycles.

If your main focus is extensive geographic coverage, Akamai is still your best bet. That being said, both CDNs provide very similar levels of service in key regions, including US, Europe, UK, and APAC.



Akamai's Dashboard (Source: www.behance.net)

Pricing

One of Incapsula's most attractive features is its price. A typical Application Delivery bundle from Akamai – "Kona" WAF and DDoS protection included - starts at over $15K/month. A comparable offer from Incapsula will only cost you $4K/month. Beyond that Akamai also charges 0.4$/GB for overages, while Incapsula charges about one-third of that cost for additional bandwidth.

If you are looking for CDN-only option, Akamai's price will be in the neighborhood of $1800/month for 5Mbps worth of traffic. With Incapsula you can get the same deal for $500/month, with Load Balancing, Real Time view and PCI compliant Web Application Firewall thrown in at no extra cost.