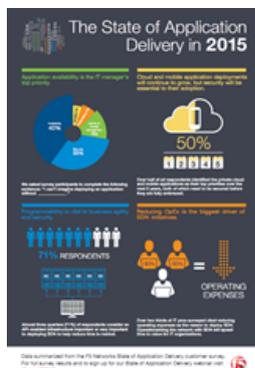# State of Application Delivery in 2015: Availability is a Coat of Many Colors

Lori MacVittie, 2015-11-02

One of the more interesting data points to come out of our State of Application Delivery 2015 was the overwhelming importance placed on availability - even over security. When respondents were asked which service they would not deploy an application without, they chose availability. Security came in a close second.

This caused a great deal of discussion. After all, one of the most often cited impediment to adopting, well, everything has been and remains security. One would think, then, that security is top of mind and clearly a priority for everyone.

Yet availability beat it out for what amounts to the "most important application service."

OTOH there's some logic to that, if you think about it. If an application isn't available, well, security's kind of not all that important is it?

OTOH the definition of "available" is increasingly not a binary one. A site is not simply "on" or "off", "available" or "unavailable". Usability in terms of performance characteristics is increasingly considered part of the definition of "available." Again, if the application is responding so slowly that you can drink an entire cup of coffee in between page loads, well, that's not really all that available and the result is the same as being "off" - users or consumers simply abandon the application.

Availability today really means that a site is both usable and available. That implies that a whole lot of application services disguised as performance and security have at their core the goal of maintaining availability.

Let me illustrate with an example: DDoS protection.

Consider for a moment that traditional definitions of security services have a core focus of protecting data and systems from intrusion, exfiltration, infection and corruption*.

Application Services

- Reside in the data path between an end user device and the application
- Are fluent in a wide range of application and network protocols (L4-7)
- Execute actions on application data and protocol based on their specific focus

DDoS attacks are not attempting intrusion. They are not attempting exfiltration of data. They are not trying to infect or corrupt data or systems.

They are simply trying to deny availability. The name says it all - it's about denying service, i.e. making a service unavailable.

DDoS protection services, then, are really about maintaining availability by detecting and mitigating attacks against the availability of services. Attackers do this in a variety of ways, but increasingly they're about chewing up resources. Bandwidth on the incoming pipes or compute on the systems serving up the applications.

But what they aren't doing is trying to steal, destroy or otherwise infiltrate systems and data, which is typically what we consider security services to be protecting against.

Yet no one** would argue against DDoS Protection services being categorized as "security services" (we do, and I've not seen anyone who offers said services categorize them differently).

Of course, one could *also* argue that if a system is corrupted, it makes it unusable or potentially brings it down and therefore it, too, is supporting the overarching requirement that an application be available.
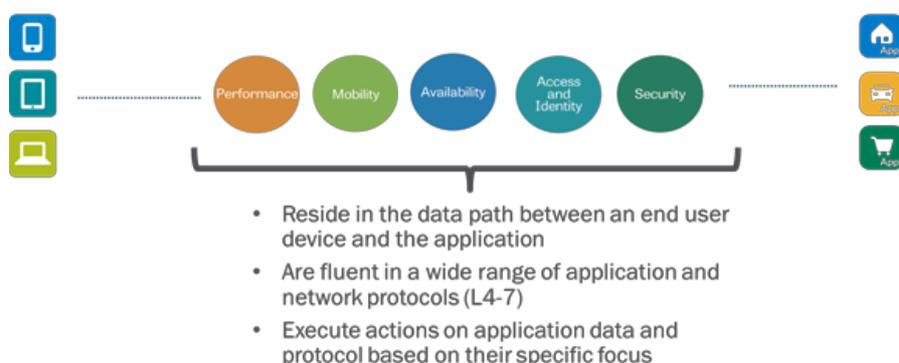
Which pretty much makes my point for me, I think: availability is not just a service but about many services working in concert to mitigate those conditions and situations that might negatively impact availability.

We categorize our portfolio of application services into colorful categories representing availability, performance, security, mobility and identity and access. But these are not binary, either. Services are not necessarily only in one category, because there are secondary and even tertiary benefits to each of them that fall into other categories. The goal of performance services are to make apps go fast, yes, but that also means contributing to the perception of availability. Some performance services are specifically targeting mobile applications and devices, making them also a part of "mobility" services.

The first step is putting into place the services that enable availability (load balancing, global load balancing, DNS). The second is to put into place those services that maintain availability such as performance and, yes, security like DDoS protection.

That's likely why we see the emphasis on availability as the "primary" service. DDoS protection and other security (and performance) services don't *provide* availability. They *maintain* it. They play as critical a role in availability as they do in their respective service "categories." That's proven out by other results in our report, such as the indication that application performance is the *last* thing folks will give up to make their networks more secure.

But enough of my philosophical and existential (and potentially pedantic) arguments about how to categorize services. We'll be diving into more detail about the results in our State of Application Delivery in 2015 report again next week, with a focus on availability as a goal and in particular how to achieve that in a hybrid data center architecture.

> **Availability: Ensure Application Availability Between Hybrid Data Centers**
>
> Multi–data center deployments allow organizations to minimize downtime, increase the ability to deliver new applications and functionality, and scale dynamically. To achieve this, companies are looking to bolster and consolidate their infrastructure with cloud services. Learn real-world strategies for building a hybrid infrastructure to support your on- and off-premises applications.

If you haven't gotten the report yet or signed up for the webinar, you can do that by visiting http://f5.com/SOAD

* I'm sure arguments against this view of "security" will be forthcoming.

** Okay, no one but me, perhaps, but I'm not really arguing that they should be re-categorized, I'm just waxing philosophical about it and looking at this existentially and a more top-down, "business goal" perspective.