# Security has 3 C&rsquo;s

**Robert Haynes, 2011-08-12**

Yesterday I was having a meeting with one of our global System Integrator Partners on the subject of their information security portfolio and how F5 might fit into it.  These things generally follow a similar format: ideally they first  tell me about their business, how they go to market, what services they offer and why they are successful. This has the twin advantages of helping me understand them better and, more importantly, work out what it is that I'm going to say.  I've broadly given up rehearsing 'pitches' as they generally sound, well, like pitches. What I  do try to do is spend time to understand the solutions we offer, their usefulness to customers and how they can best be deployed. Next I listen to the customer and try to engage them about F5 in a way that has some resonance with them and their business.

This does have the potential, however, to all go horribly wrong. If inspiration fails to strike there is a good chance that I'm going to look like an incoherent, bumbling and badly prepared fool. Just to add a bit of spice,  this particular meeting had lots of the F5 leadership team in the room making it the perfect stage for a career limiting performance. Fortunately the explanation of this partners methodology, services and capability, was both insightful and interesting and it got me thinking. In another piece of good luck, and with some great questions from my esteemed colleagues, it was also long enough to allow me to assemble my thoughts.

For those of you thus far feeling mightily cheated that a security-titled blog post seems to be mainly about me and my oh-so-interesting life in pre-sales, I am getting to the point.

It seems to me that this Integrator is  successful in offering security services because of three key features, and that these are exactly the same for a useful security device:-

**Context** – my SI partner provided their customers with a range of assessment tools and had the advantage of also providing networking and application services, giving them a really good insight into the context of the customer's traffic. At a smaller scale, a network security device has to understand the context of the traffic it inspects: Where is the traffic from? What was the device type? Who is the user? What is the status of the destination services? What does this traffic mean to the application? This level of awareness of a customer or an application is a huge advantage in creating a security service or appliance.

**Control** – understanding the context of  traffic or a whole IT organisation gives you the ability to take action when required. Having a range of actions you can take makes it possible to respond to threats in the most appropriate way. At a service level you can achieve this with a range of security offerings, at an appliance level you need to have a spread of responses. Simply denying traffic might not be appropriate. You might want instead to redirect traffic, rate shape it or strip away malicious parts. Applying the right controls to match the context of a threat gives an organisation the flexibility to respond to a variety of events.

**Capacity** – with many hundreds of security professionals and a presence in nearly 50 countries, my F5 partner has the capability to successfully take on huge projects for the largest of organisations. Security devices also need to scale to meet massive levels of throughput and millions of connections  that are  increasingly part of  distributed attacks. Devices flat-lining at only a few hundred thousand connections is not going to help you when you are under attack from a $9/hour botnet.

So when you're reviewing a security partner  or device, maybe you should take a look at what it offers in terms of the three C's.

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com