

ComputerWeekly – Building IT Security for Flexible Working

By Clive Longbottom, Service Director, Quocirca Ltd

In the dark ages of five years ago, we had suppliers selling us standalone security systems based on securing this platform, this data, this application, these PCs and so on.

We ended up with many different security IDs, different passwords, a lack of inherent interoperability - in essence, a mess that increased the hassle to users, who would then spend as much time as they could trying to circumvent the security.

But that is all changing. The new mantra is federated security, where we bring all the different security systems together, underpin the whole thing with a common architecture and enable people to roam around based on their in-the-round security profile.

All well and good to those who are going down this route. The problem is that federated security is solving a problem that existed some time back, and it is not particularly looking at solving the problem we have today.

The problem today is that each person is not a single security entity - it is not possible to just bundle them up into nicely aggregated groups such as "manager" or "financial department" or whatever, and assign profiles accordingly. Neither can we easily utilise hierarchical systems where we start at the bottom - the person's name - to see what the base security is and then work up through the various groups until we find the maximum security level that the person has.

The main reason for this is that the work/life partition has been ruptured. We now have people working at 11pm from home, and we have people wanting to carry out personal actions while at work, such as buying tickets for an event that evening, or remembering to add chocolate gateau to their Tesco shopping list.

The knee-jerk reaction to this from companies is to use mass enforcement - if you are coming in to the organisation from outside, then a virtual private network has to be used. However, once you are in, you are in, and the standard security policies take over.

If you are starting from inside, then personal stuff is forbidden - you are employed by the company, and we expect you to only do our work during our time. Oh - you are also doing work for us in your own time? Oops - how do we counter this?

What we need is partitioning of security profiles - once we have federated them. First, we need to pull together all the existing corporate security profiles we have for the person and sort them all out. Then we need to layer on top locational/device awareness -

where is the person coming in from, with what device, with what capabilities?

This helps to define not only what they are allowed to do, but also what makes sense for them to do - trying to download a computer-aided design drawing to a GPRS phone isn't too clever.

Then we need to layer on the contextual information - what type of function is the person trying to do, and whether this is likely to be work or leisure related. If work, are they allowed access to this type of information? If leisure, do our corporate policies allow this?

For example, a bit of online shopping is OK, whereas downloading MP3s isn't. As we move more into a virtualised world, it may well be that when a user starts to carry out this type of action, you want to shunt them off from the main corporate network on to a "guest" partition of the network for that specific action, using a virtualised partition of their machine, so sealing off any possibility of any external action disrupting the corporate network.

Because we are essentially dealing with different entities when a person is working in the office for the company, when they are carrying out personal activities within the confines of the office, and when the person is out on the road, traditional federated security comes up against problems.

Far better to have a new set of coupled, but distinct, partitions of the person's identity, enabling the security to be highly granular depending on the task in hand.

Enforcement of company mandates has shown itself to be nigh on impossible time after time. By accepting that people now work during leisure time and play during work, we can create systems that allow for this - and keep the workers happier, less stressed and - hopefully - more effective to us overall.

About Quocirca

Quocirca is one of Europe's leading independent industry analyst firms. One of its biggest assets is the core team of highly experienced analysts drawn from both the corporate and the vendor communities. This team prides itself on maintaining a bigger picture view of what's going on in the IT and communications marketplaces. This allows all of Quocirca's activities to be carried out in the context of the real world and avoids distractions with fads, fashions and the nuts and bolts of specific technologies. Quocirca's focus has always been the point of intersection at which IT meets "the business".

Quocirca Services

The insight and experience that comes from working as an industry analyst as well as a practitioner allows the Quocirca team to contribute significantly to IT Vendors, Service Providers and Corporate clients. To this end, it provides a range of consulting and advisory services. Details of these, along with some of Quocirca's latest analysis, may be obtained by visiting <http://www.quocirca.com>

Quocirca also provides bespoke primary research services through its daughter company QNB Intelligence. This involves interviewing thousands of senior decision makers on a quarterly basis.