Juggling Performance, Availability and Security

Factors driving data centre evolution

By Tony Lock, February 2014

Originally published by

datacentre solutions DCS UK
IT OPTIMISATION FOR MAXIMUM BUSINESS EFFICIENCY

A recent report from Freeform Dynamics[1] illustrates that many corporate networks are facing serious challenges to application performance consistency, service availability and enterprise data security. The importance of the network has never been so high, as more and more business processes depend implicitly and explicitly on the corporate network functioning well to deliver IT services when and where required.

The pressures on the network are ramping up as changes to working patterns, mobility, infrastructure virtualisation and escalating security threats all combine to leave many existing networks in need of modernisation. When you understand that so many enterprise networks are built utilising equipment of various ages, often technological generations apart, it should not surprise that existing access infrastructure is fragmented and is difficult to manage.

Thus there is no escape from a reality where the demands on networks and systems continue to grow relentlessly, with increased loads resulting from a wide variety of factors. (Figure 1).
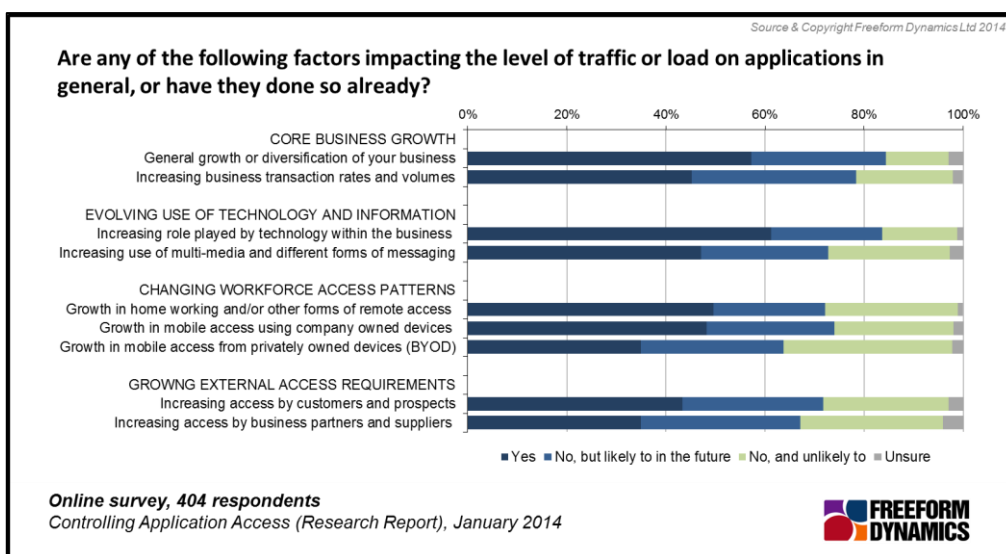

Figure 1

Some of the changes, including general business growth and an increasing use of IT technologies and services, originate inside the enterprise. Other changes arise externally, as organisations seek to offer IT access to customers, suppliers and business partners.

In addition there is a third element which impacts traffic loads on the network as well as places pressure on IT security. This encompasses the changes needed in order to provide the workforce with access core IT systems. In particular Freeform Dynamics's research documents the high level impact of users employing mobile devices, whether owned by the organisation or personally, which access IT systems from outside the firewall.

In this context mobile access from tablets and smartphones grabs most of the headlines. In reality staff members working from home actually generate a significant volume of network traffic. Our research shows that the same types of usage changes and evolving workforce access patterns also have an impact on application and data security. (Figure 2)
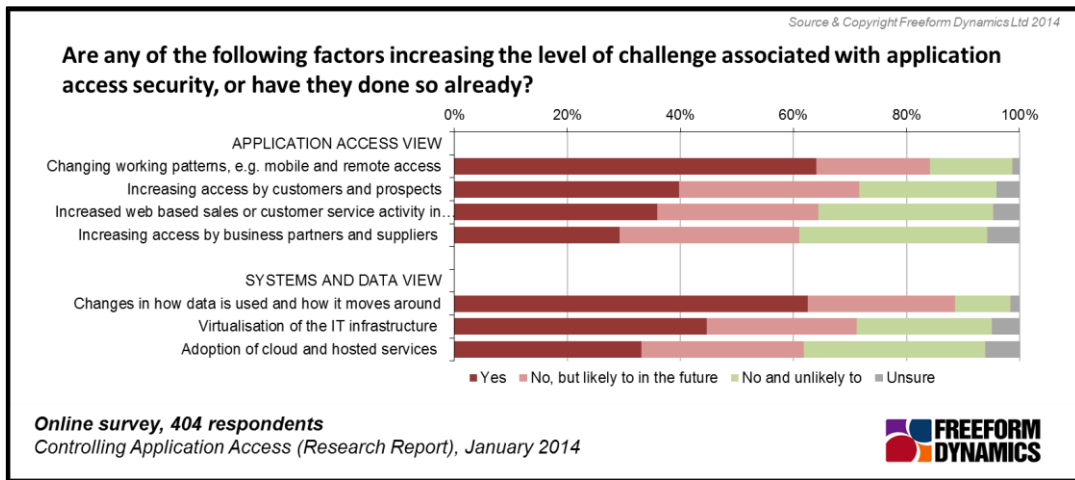

Figure 2

This reveals a second set of dynamics impacting security. Figure 2 shows that trends going on behind the scenes in IT, in particular how data is used and moved around along with the rise of virtualised IT systems, are expanding the security challenge.

The combined pressures on application performance, availability and security are now perceived as problems for a significant proportion of those responding. (Figure 3)
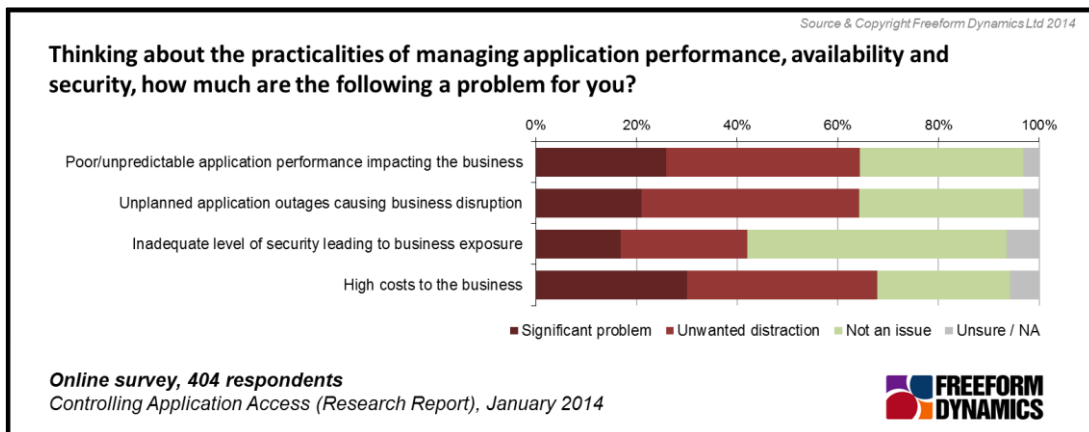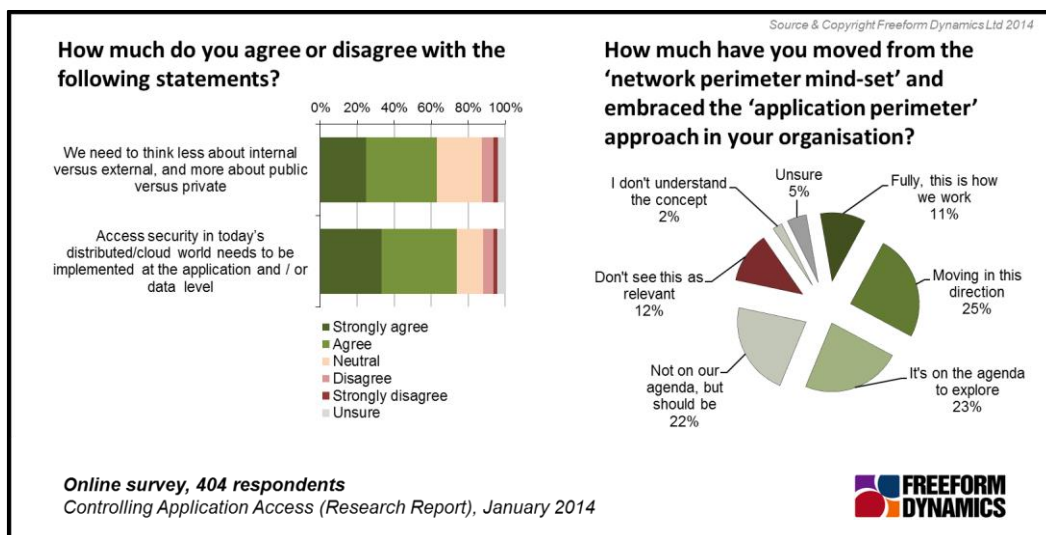

Figure 3

The majority of respondents openly confirm challenges with regards to application performance and availability. Fewer, though still a significant proportion, acknowledge having significant security challenges.

When analysing these returns it is important to understand peoples' natural disinclination to admit to security problems. That said, more respondents report problems or distractions caused by application performance or service disruption than security, something that has not been the case in previous years. Until now 'security' has usually been regarded as more important a problem than either application availability or performance. This may reflect the expectation of users to have access to ever available IT systems delivering excellent performance using whichever device from any location, inside or outside the business,

While not shown here directly, the research highlights that inadequate application delivery control leads to excessive costs to the business. Some of this will be direct (for example, overhead on IT and operations). Yet it is important to not forget the indirect costs incurred as a result of business interruption, reduced productivity and lost business. In this context it is even more important to understand the potential impacts of any IT security breach, in both financial terms and brand damage.

The challenge of trying to manage fragmented networks composed of technology components that were installed over long periods is difficult at the best of times. The task becomes even harder when business requirements demand ever improving availability, security and application performance, especially when there is little additional budget made available.

While the technology challenges are indubitably considerable, there is another, potentially more important 'philosophical' evolution which data centre professionals today recognise as needing to be made (Figure 4).

Figure 4

Our research confirms that the changing user access patterns (as mentioned earlier) challenges the long-established security assumption that the corporate 'internal' network and the 'external' world remain separate. As Figure 4 reveals, the majority of respondents believe it is necessary to move away from security ideas based on 'internal versus external' and instead need to address application and data level security at a granular level.

While acceptance of the need for change is high, those disagreeing amounting to less than ten percent, few organisations have made the change. Only about 1 in 10 in the survey state they have made the transition fully from a 'network boundary mind-set and security regime' to one based on 'application and data perimeter' ideas. The vast majority, some seventy percent, see this shift as necessary even they have yet to even start on the transition.

Taking such a data/application centric approach to security has the advantage that it is more straight-forward to handle performance and availability issues in the dynamic IT infrastructures which many organisations are looking to implement This makes the fact that so few have yet embarked down this road somewhat surprising, even given the huge time pressure under which every data centre routinely functions.

Changing technology - even with the adoption of solutions now becoming available which actively combine security, availability and performance capabilities - will not meet escalating business requirements and ever-more demanding user expectations. It is essential that those who run data centres take steps to adopt the data/application centric view of the world widely recognised as required.

This philosophical modification will need significant changes to how data centre staff think and the operational processes they use every day. The time to start this journey is now.

[1] Controlling Application Access. A network security and QoS checkpoint.
http://www.freeformdynamics.com/fullarticle.asp?aid=1738

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.