Controlling Application Access

A network security and QoS checkpoint

Freeform Dynamics Ltd, January 2014

A great deal of attention is focused on the quality of service and risk aspects of cloud computing. But with hosted offerings still only accounting for a relatively small part of IT delivery, a bigger concern for most organisations should be the way in which application performance, availability and security challenges are quietly creeping up in the context of internal systems, sometimes without anyone even noticing.

Key Points

The pressure is growing on the corporate network and the systems it supports

When asked about their network and application access infrastructure in a recent research study, the 404 respondents who participated highlighted a range of escalating pressures. Organisations of all sizes are seeing greater demands as a result of core business growth and a general increase in the use of technology and information within the business. Overlaid on this is the additional pressure arising from home and mobile working, BYOD, and greater access of IT systems by customers, partners and suppliers.

Difficulties keeping up are negatively impacting the business

With no sign of the growth in traffic or the appetite for broader access diminishing, keeping up with the trends is proving hard. Challenges reported include poor/unpredictable application performance and unplanned outages which undermine productivity and even interrupt the business. Changing access patterns, a range of external threats, and the unintended consequences of virtualisation are all then hampering the management of security in particular. Many also call out excessive costs to the business.

Many problems stem from shortcomings in the access infrastructure

The trends being highlighted shine a spotlight on the corporate access infrastructure and the components within it for dealing with performance, availability and security. Piecemeal growth means that many are struggling with a complex and disjointed network environment containing lot of old technology requiring an excessive amount of manual administration to keep it running. Furthermore, the majority report significant shortfalls in capability in relation to a range of specific performance and security management functions.

Moving forward successfully has a philosophical as well as a practical dimension

From a philosophical perspective, two mind-set shifts are required. The first is from an infrastructure to a services view of performance and availability management, and the second is to focus less on the 'network perimeter' approach to security and think more in terms of multi-layered protection accompanied by effective analytics. From a practical perspective, there is then a need to analyse and prioritise requirements more objectively, and make sure that the right knowledge, skills and tooling are applied appropriately.

A concerted effort must be made to break the 'reactive investment' habit

Most investment intentions currently revolve around tactical requirements such as the replacement of obsolete equipment or implementation of new applications. When making architectural and technology decisions a conscious effort must be made to think of the bigger picture, and move progressively and proactively towards a more coherent access infrastructure capable of dealing with future needs.

The study upon which this report is based was designed, executed and interpreted independently by Freeform Dynamics Ltd. The research was sponsored by Barracuda Networks, and responses from 404 IT and business professionals representing a range of organisation sizes and industries were gathered via an online survey hosted on a popular IT news site.

Study sponsored by

Barracuda

Introduction

IT and business people are often guilty of applying dual standards when it comes to the use of technology. Encryption of business data on smartphones and tablets is regarded as critical, while laptop users have carried around sensitive information with no such protection for years. Meanwhile everyone throws their arms up in horror when a cloud service provider experiences an outage or security attack, even though frequent downtime, wild fluctuations in performance, and the occasional leakage of confidential information are simply accepted as facts of life in relation to internal systems and data.

Such dual standards are generally not the result of deliberate doublethink. New solutions are always considered in the context of the then current requirements, and are implemented using technology and techniques available at the time. The trouble is that both requirements and technology evolve continuously, and we often forget (or don't have the time) to revisit older systems and infrastructure to make sure they are still current from a technology perspective and are still meeting business needs effectively. The result is that systems gradually fall behind in terms of fitness for purpose and operational efficiency.

This phenomenon is frequently observed in relation to the corporate access infrastructure that deals with many of the important aspects of application performance, availability and security. The chances are that in your organisation, the fundamentals of this were designed into your network five, ten or even fifteen years ago. Since then, modifications and extensions are likely to have been implemented in a piecemeal manner to deal with individual application requirements on a case by case basis. It has probably been a while, however, since you stood back, looked at the state of your access infrastructure as a whole, and asked yourself not just how well it is coping with requirements today, but how ready it is for the future.

With application and network loads increasing, access patterns evolving, and new security threats emerging almost daily, these are highly pertinent questions. In this report, with the help of input gathered from over 400 participants in a recent research study, we therefore examine the way in which requirements and expectations are changing in relation to application access and how well infrastructures are coping. Along the way, we also take a look at some of the imperatives for future proofing your environment.

The pressure is growing and it's hard to keep up

It will probably not come as a surprise to many people that the majority of participants in our study are either experiencing or anticipating an increased load on systems as a result of core business growth and the increased use of technology and information within the business (Figure 1).

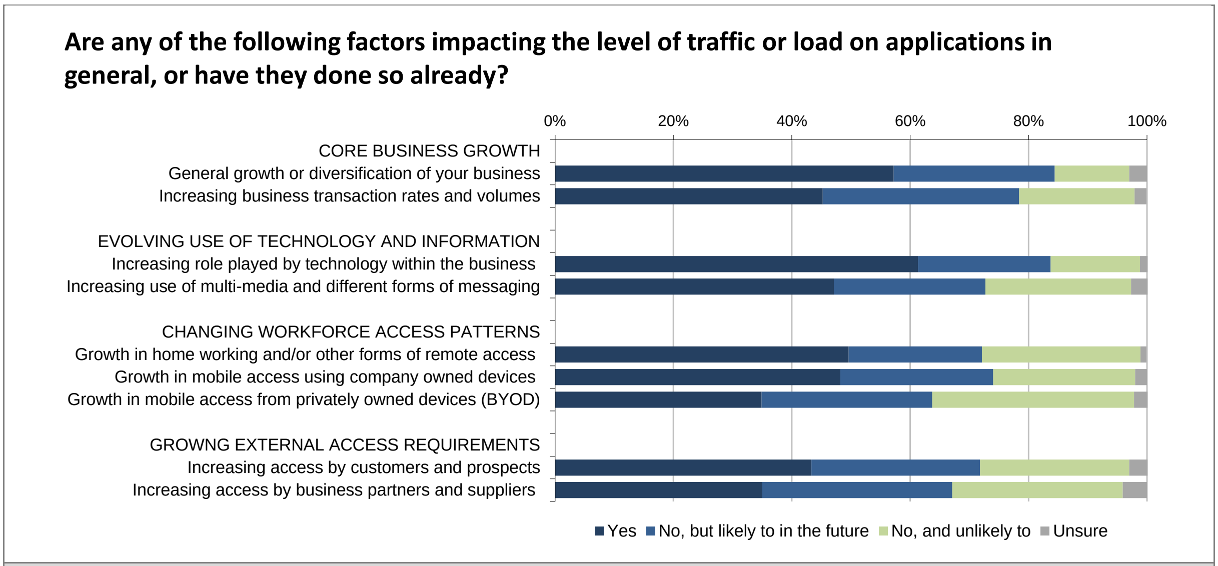


Figure 1 The pressures on systems and network are wide and varied.

Beyond these fundamentals, we can also see the impact of changing access patterns. This not only includes remote and mobile access by employees as a result of trends in home working, mobility and BYOD, but also the additional load arising from systems being opened up to the outside world.

Security is also becoming more challenging as internal and external users access the corporate infrastructure in new and different ways, and data becomes fragmented across departmental and workgroup systems, laptops and mobile devices, and various forms of cloud storage (Figure 2).

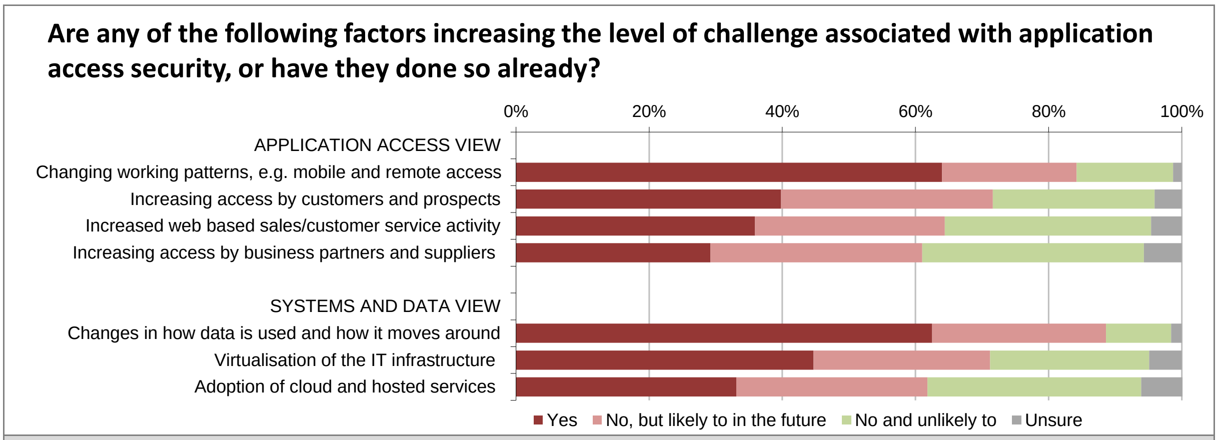


Figure 2 Changes in access patterns and IT delivery models are creating security challenges.

As we can see, even the adoption of something as well-accepted as server virtualisation frequently has security implications, leading to a broad range of concerns and distractions (Figure 3).

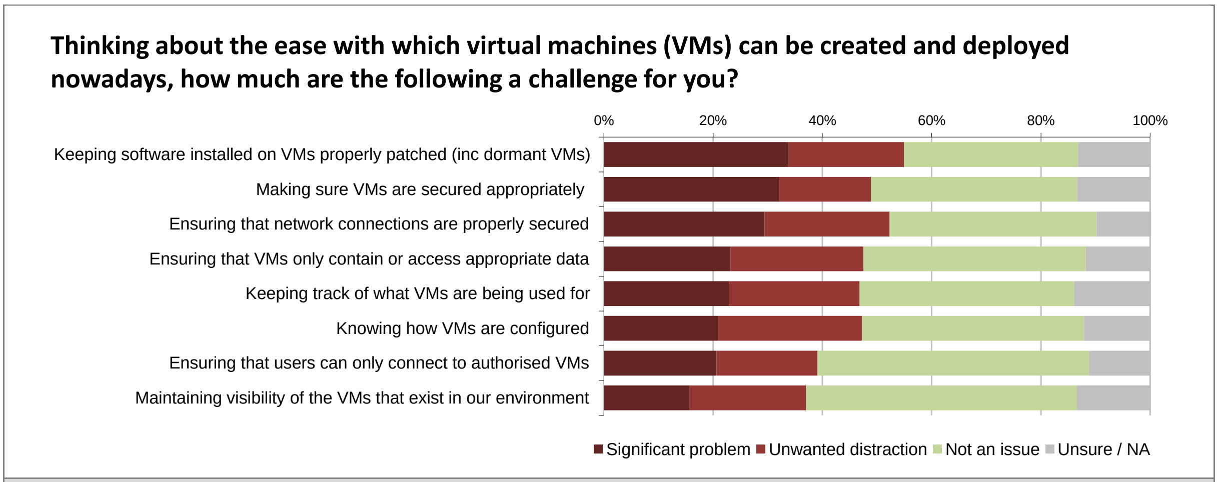


Figure 3 Virtualisation is a double-edged sword when you consider the security implications.

With all this going on, it’s understandable that many are finding it difficult to keep up, resulting in performance, availability and security problems that often have a direct impact on the business (Figure 4).

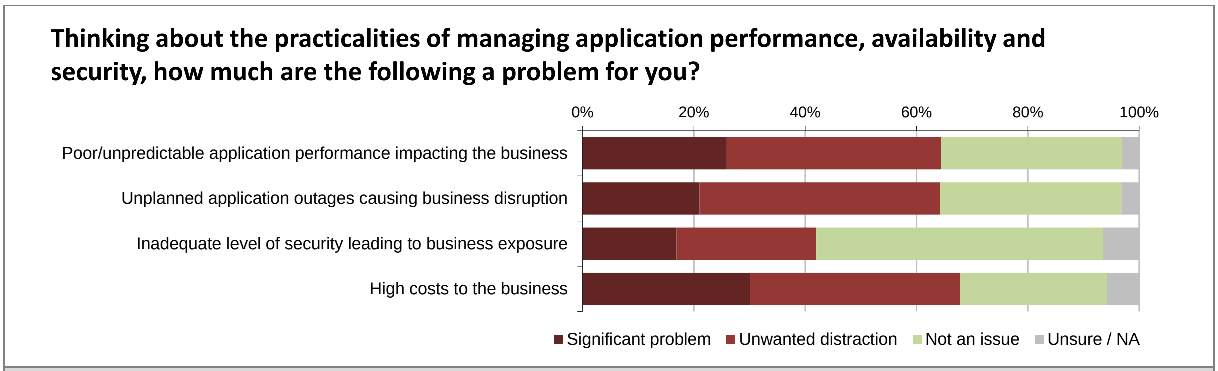


Figure 4 The direct and indirect impact on the business can be significant.

Things are likely to get even more challenging

When IT professionals are asked to compare activity today with what's likely to unfold over the next three years, responses suggest that the level of pressure is only going to increase. As of today, most of the load on systems is typically from employees working in fixed office locations, but looking to the future, growth is anticipated across all forms of internal and external access (Figure 5).

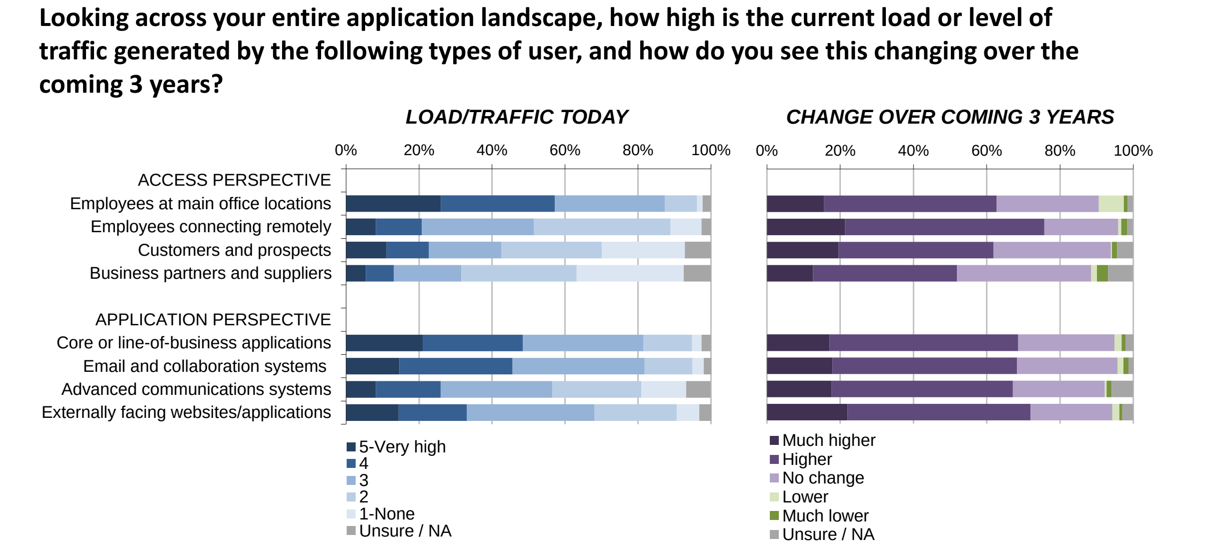


Figure 5 Most are anticipating growth in demand to continue.

On the bottom half of this chart, the application perspective is consistent with the anticipated changes in access. Additional demands stemming from the use of more advanced communications systems, e.g. web conferencing, social networks, interactive video, and so on, will add to the load already associated with more traditional solutions. Layered on this will be even more traffic associated with externally facing web applications accessed by customers, partners and suppliers.

Turning to security, the fallout from the ongoing access trends in the form of 'friendly fire' from within the workforce is as we would expect and as has always been the case. Though as business becomes increasingly connected the growth in external threats, including from national government agencies, is creating more concern for many (Figure 6).

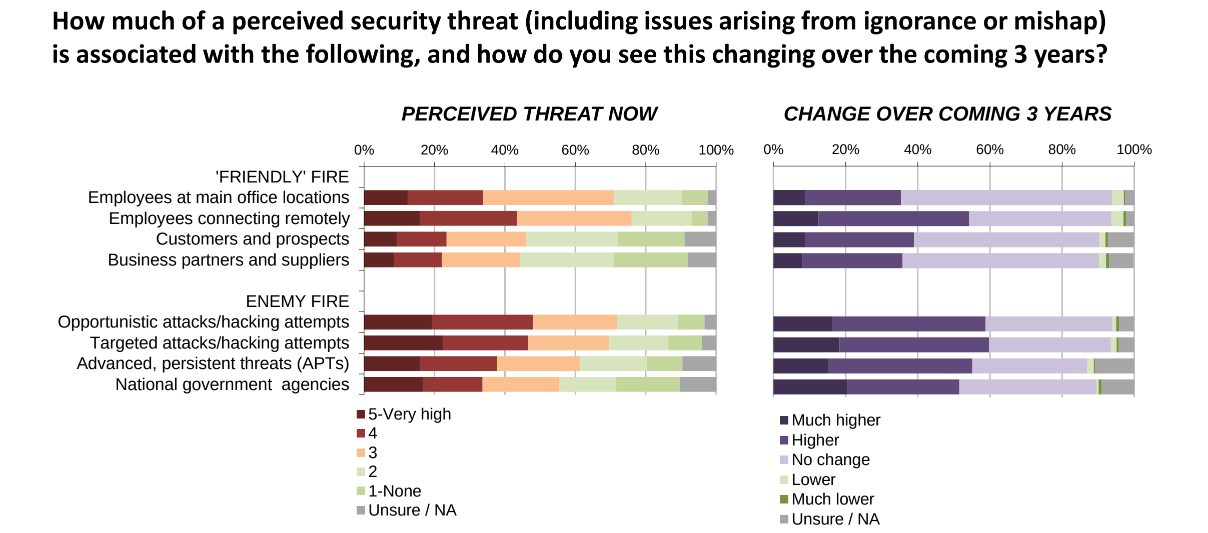


Figure 6 Security challenges are set to continue escalating.

More attention must be paid to the access infrastructure

The dynamics and associated challenges we have been discussing shine a spotlight on the corporate access infrastructure and the components within it for dealing with performance, availability and security requirements. This includes things like load balancers, data transport optimisation devices, firewalls and other solutions that help to optimise access, enable resilience and protect applications.

Such capabilities have been around for many years and most networks have something in place in the relevant areas, so why are IT professionals reporting so many challenges and issues? This comes back to the phenomenon we discussed right at the beginning. As elements of infrastructure and process have accumulated over the years, the most common situation reported is a complex and disjointed environment containing a lot of old technology, with a high reliance on manual administration (Figure 7).

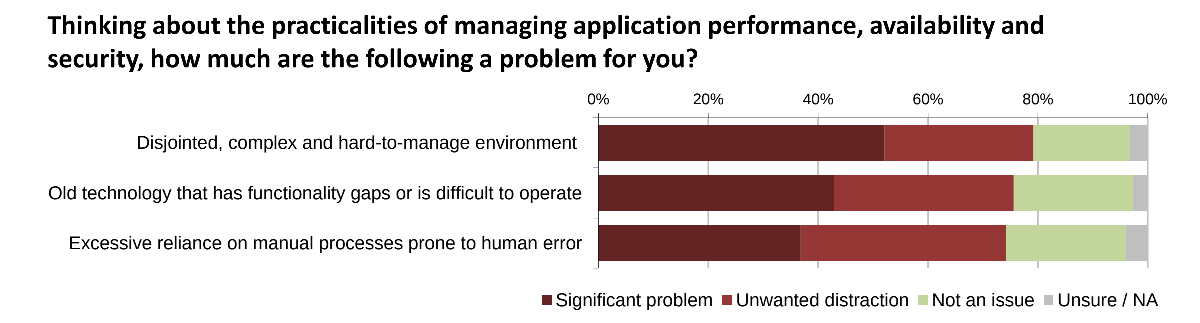


Figure 7 The root causes of application access control problems are clear.

Drilling into specifics we see a capability shortfall in many areas of QoS and security management, with most highlighting a need for improvement across key functions. This confirms a general sentiment that more attention needs to be paid to modernising and strengthening the access infrastructure (Figure 8).

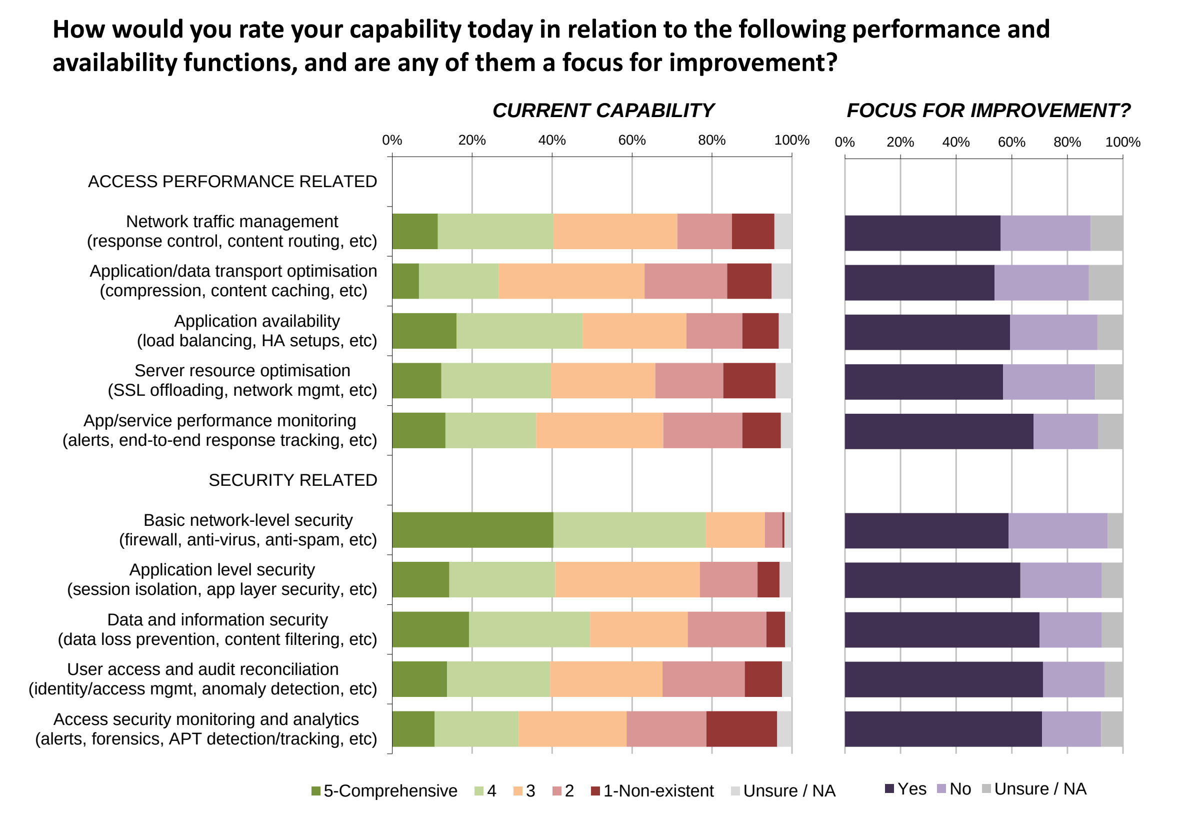


Figure 8 Shortfalls in capability are evident across many key areas of QoS and security management.

Need to switch mind-sets on security

When considering security in particular, improving the access infrastructure is not just about incremental extensions or like-for-like replacement of old kit with the latest equivalent. The trends in application access that are evident from our study suggest that a new way of thinking is also required. In particular, the traditional notion of an organisational boundary, or network perimeter, is directly challenged as the primary way of dealing with security requirements going forward. This comes through in a couple of different ways from the research, with a general consensus that it is necessary to focus more on establishing perimeters around applications and data sets. Most, however, have yet to act on this mind-set shift (Figure 9).

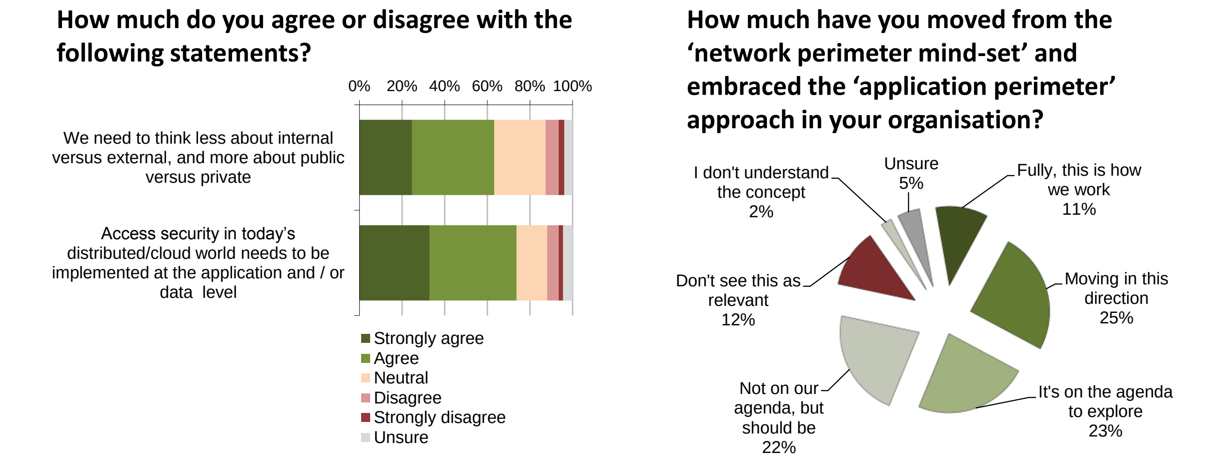


Figure 9 General consensus exists on the way forward, but it is still early days for most organisations.

In practice, moving down the application perimeter route involves defining application-aware policies in the network that are applied regardless of the source of traffic and the physical location of the application and data. This has two main advantages over the network perimeter approach. Firstly, if one application is compromised, others are not automatically exposed as they are each protected individually. Secondly, the network level protection measures in place guard against internal dangers as well as external threats.

A joined up approach is important

Turning to specific types of technology, we typically see the use of separate components for dealing with QoS and security, with integrated solutions such as application delivery controllers (ADCs) exhibiting a more modest level of penetration (Figure 10).

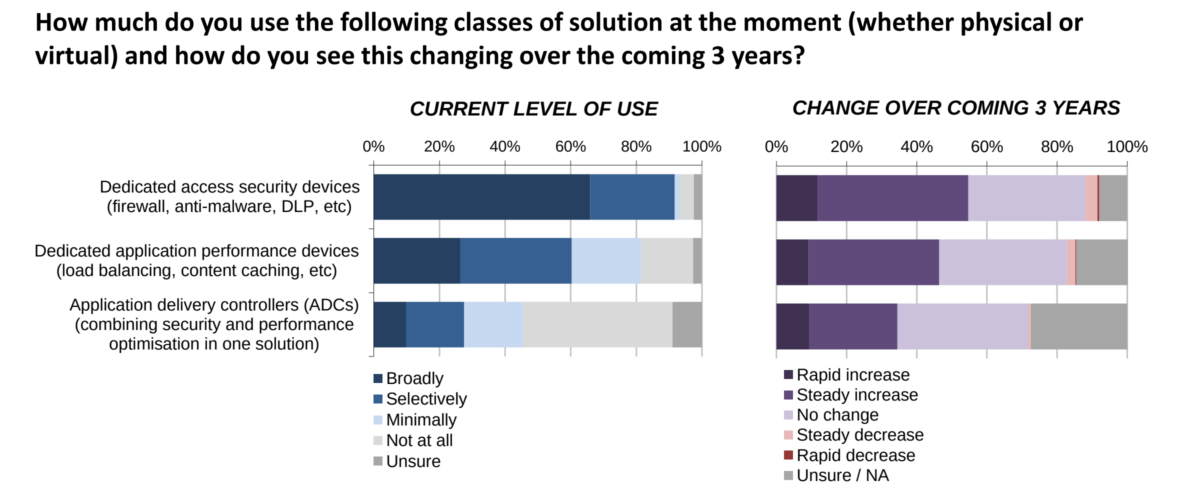


Figure 10 Most activity is associated with dedicated appliances, but ADCs are beginning to find their place.

The relatively low level of current use and future attention on ADCs probably reflects a general lack of awareness and understanding of the potential value offered by multi-function appliances. This is not surprising given that this type of solution is a comparatively new entrant in the market and is often associated with complex and demanding environments. However, as ADCs become more 'mainstream', those with experience confirm the associated benefits they deliver in terms of infrastructure simplification and lowering of overheads, as well as reducing the risk of things falling through the cracks (Figure 11).

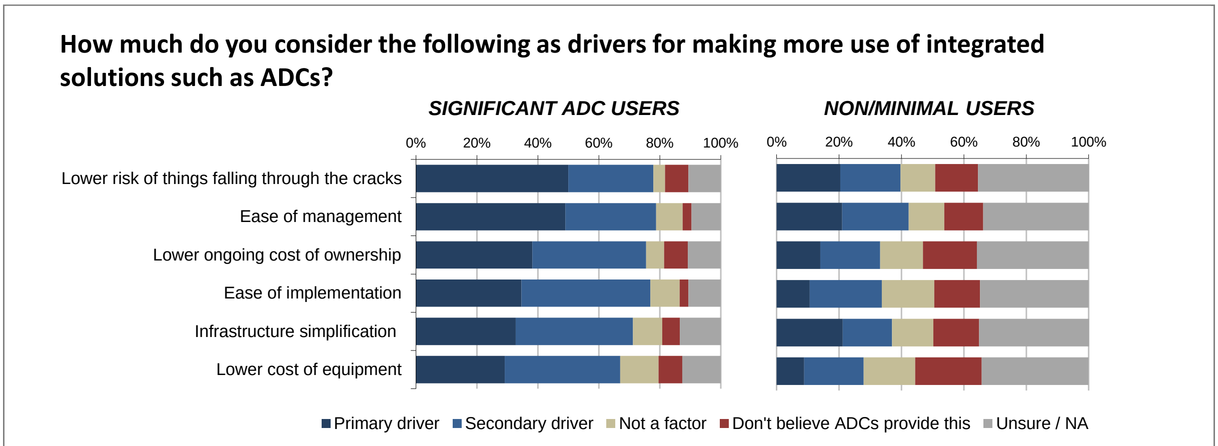


Figure 11 While lack of ADC awareness is commonplace, adopters confirm the key benefits.

As an aside, it is interesting that those more familiar with ADCs also see a role for such solutions to be delivered as virtual appliances to better fit with alternative architectures and emerging IT delivery models (Figure 12).

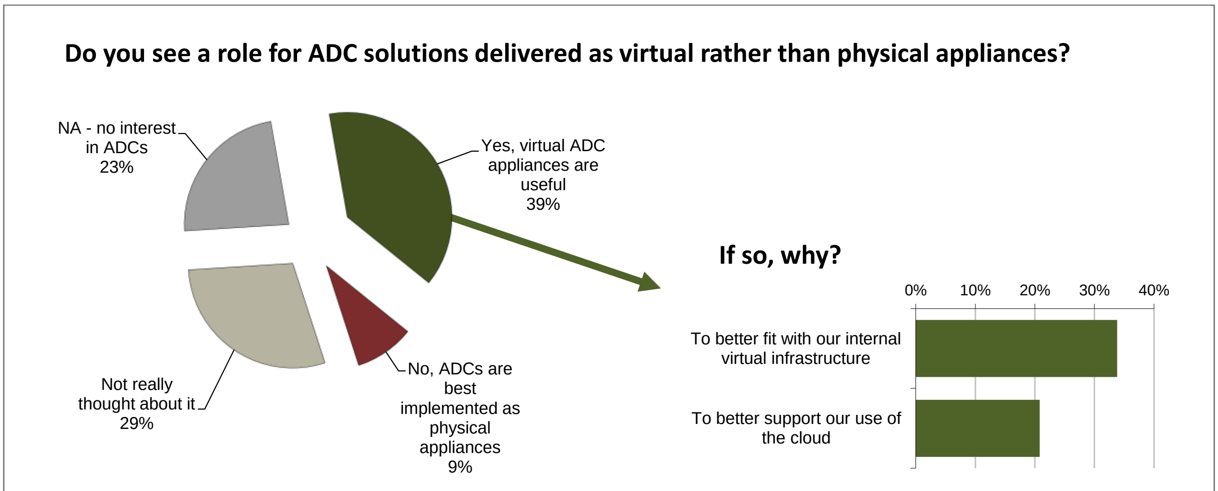


Figure 12 Those with experience acknowledge the need for virtual appliances.

The logic here is reinforced when we consider some of the cloud-related challenges (Figure 13).

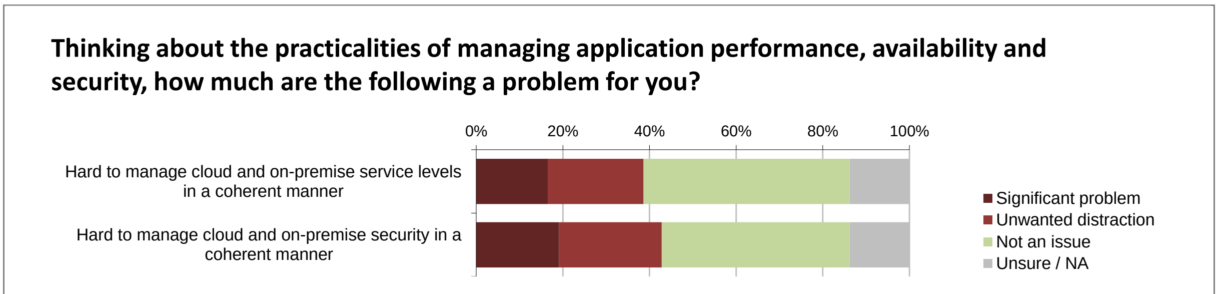


Figure 13 Some are already experiencing cloud-related delivery challenges.

When we stand back and consider these findings alongside some of the other challenges highlighted earlier to do with infrastructure fragmentation, the clear message is that a more joined-up approach is an important part of future-proofing the application access infrastructure. Integrated multi-function appliances can help with this, but if you prefer not to put all your eggs in one basket with ADCs, modern dedicated components need to be implemented as part of a coherent architectural framework.

But moving from the disjointed world of today's communications landscape to a joined up future-proof application access infrastructure is easier said than done, especially as making structural changes to the corporate network is akin to re-engineering an aeroplane mid-flight. So what's needed in practical terms to drive the improvement that is clearly needed?

Putting the theory into practice

In order to move forward successfully, it is first necessary to appreciate that there's a philosophical as well as a practical dimension to consider (Figure 14).

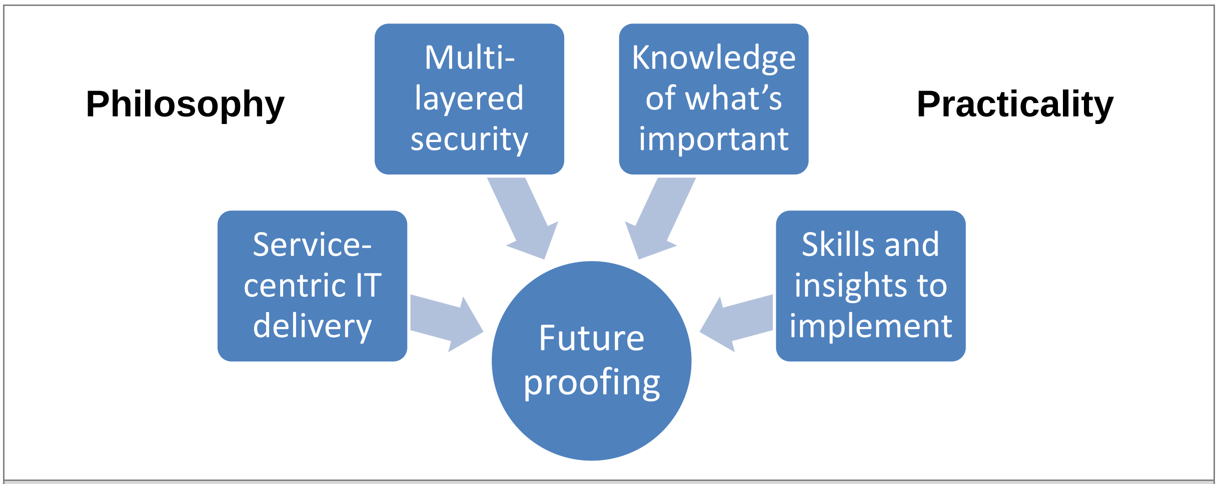

Philosophy
Multi-layered security
Knowledge of what's important
Practicality
Service-centric IT delivery
Skills and insights to implement
Future proofing

Figure 14 Success is dependent on adopting the right approach in the right way.

Let's look at what this translates to in terms of specifics.

Service-centric IT delivery

As of today, service level management is mostly centred on infrastructure elements, e.g. a typical SLA might relate to the uptime of a given server or cluster of servers. All business users care about, however, is whether a specific IT service or system is available to them and is operating at an acceptable level of performance when they need it. A healthy cluster underpinning a key application is no good to them if access is impaired because the network is overloaded or a storage array is underperforming.

The first philosophical shift that needs to take place is therefore from an infrastructure view of delivery to more of a user focused, service-centric view.

Multi-layered security

The second philosophical shift is one we have already discussed, which is from an overall perimeter view of network security to thinking more in terms of a multi-layered approach which incorporates the concept of application and data set level protection embedded in the network. When we talk about creating 'application perimeters', however, this does not mean that protecting the outside edge of the corporate network is no longer important or useful, it's simply that you cannot rely on this alone given the changes in access patterns we are seeing.

While the concept of multi-layered security is by no means a new idea, it's clear from the research that many don't have the pre-requisite capability in their network at the moment. Modernisation and the introduction of both more functionality and additional control is therefore going to be required in the majority of cases in order to keep up with changing demands and the evolving threat land scape.

Knowledge of what's important

The service-centric approach helps a lot with requirements definition as conversations to do with performance and availability are much more meaningful to business stakeholders than discussions about servers and other infrastructure components. What you are ultimately aiming for is a clear and unambiguous definition of how critical or important individual services are to the business, whether they are workforce or customer/partner/supplier facing. You can then define requirements and expectations with regard to uptime, response times, recovery times, and so on much more objectively, and make sure your investments and efforts are prioritised accordingly.

Requirements and expectations to do with security can be analysed and prioritised in a similar manner, except that here you need to also define the level and nature of potential threats, which may vary depending on the service, how the user is connecting to it, and the type of data being accessed. If we think back to shortfalls that currently exist (as we saw previously in Figure 8), the aim in most cases will be to move beyond basic network-level security and introduce more in the way of granular 'application and data-aware' control of security.

It is also likely that you will need to pay more attention to monitoring and security analytics, especially given the increased threat respondents in our study are anticipating from targeted attacks and advanced persistent threats (APTs). Indeed, many now argue that it is unrealistic to expect that you can prevent all intrusion. The aim should therefore be to detect and deal with suspicious activity as quickly as possible, and when a breach occurs, limit the scope of penetration. This again highlights the value of protecting applications and data sources individually as much as possible.

Skills and insights

It's important to stay current from an awareness and skills perspective. With both requirements and technology evolving so rapidly, a knowledge base that is even six months out of date is arguably inadequate. Whether it's the way in which integrated solutions like ADCs are maturing and becoming more widely accessible, or the advances that are taking place in security monitoring, analytics and forensics, it is well worth taking the time to get up to speed and maintain your level of awareness.

Of course you may not have the bandwidth or inclination to maintain lots of detailed specialist knowledge in house, but unless you are outsourcing completely, it is necessary to at least understand the requirements and principles at the kind of level presented in this report. You can then make better judgements about the kind of outside expertise to bring in to help with detailed planning, design and implementation work. You'll also, obviously, be in a better position to deal with IT vendors and put their offerings into perspective.

Final thoughts

An encouraging finding from the research is that most respondents anticipate investing in their application access infrastructure for a wide and varied set of reasons in the next three years (Figure 15).

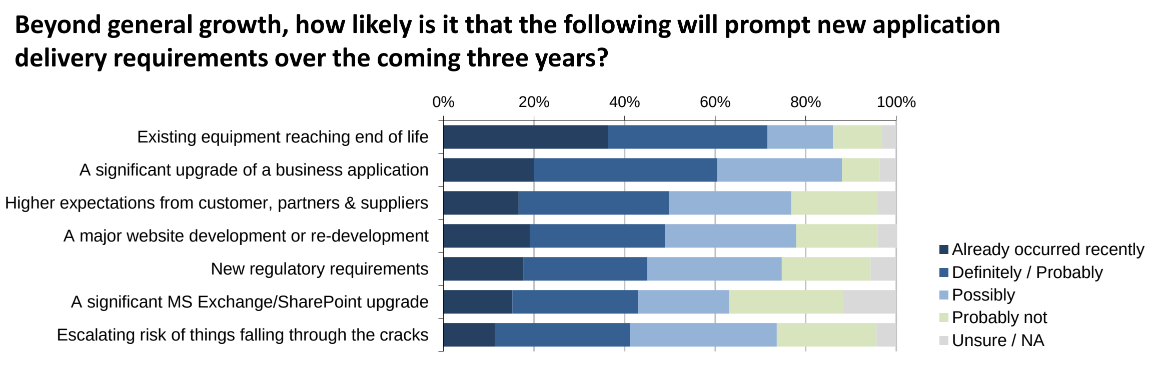


Figure 15 Many of the prompts for investment are tactical in nature.

This is good at one level in that funds are likely to be made available to acquire the necessary equipment, software and services, but it is telling that last on the list of prompts is "Escalating risk of things falling through the cracks".

The big danger is that the list of investment prompts we see is perpetuating the tactical and reactive approach to expanding and implementing new capabilities. While this way of moving forward often deals with immediate requirements, it tends to aggravate a broader set of problems that have their roots in infrastructure fragmentation and disjointed operations that many are already reporting. And this is only likely to get worse with the trends that are unfolding.

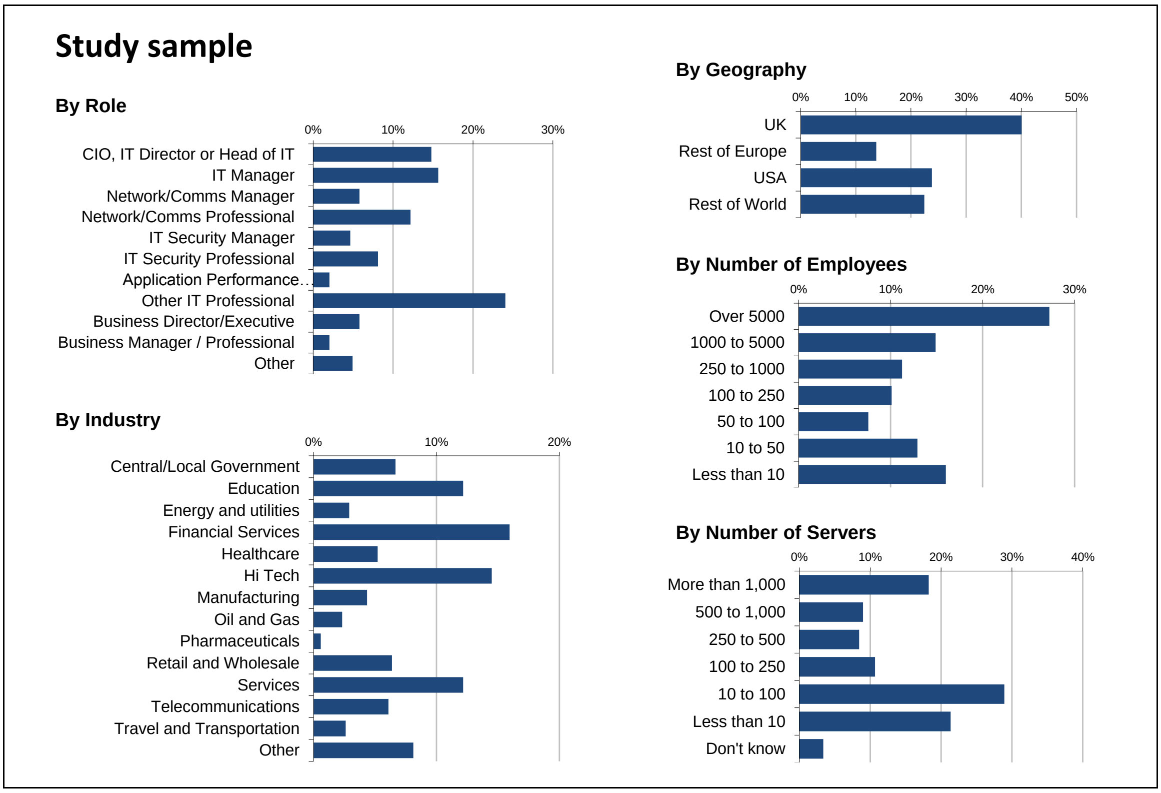
With this in mind, if we were to leave you with a single message from the research discussed in this report, it would be that the world is changing and that this is driving a need to re-think the performance, availability and security aspects of application access. Status quo in terms of architecture, technology and process is not a viable option for the future, so it’s better to start moving in the right direction now, than waiting until your hand is forced.

We hope the insights we have presented will help you as you act on this imperative.

Appendix A: Study sample

The study upon which this report is based was designed, executed and interpreted on an independent and objective basis by Freeform Dynamics Ltd. Data was gathered from 404 respondents via an online questionnaire hosted on a popular IT news and information website. The study was completed in November 2013.

The sample distribution was as follows:



Study sample

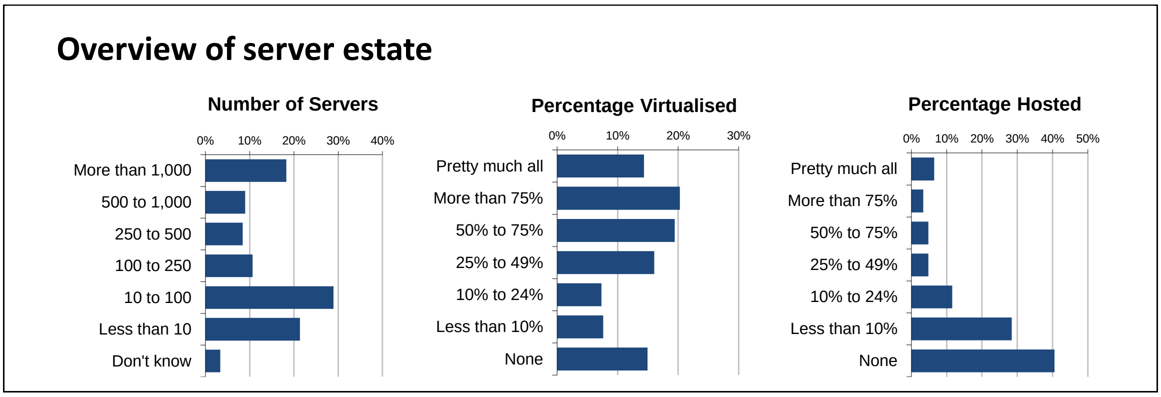
By Role

By Industry

By Geography

By Number of Employees

By Number of Servers



Overview of server estate

Number of Servers

Percentage Virtualised

Percentage Hosted

Limitations of research data

As with all online surveys, the sample in this research is likely to be skewed towards those with more of an interest in the topic under investigation due to the self-selection of respondents into the study. Furthermore, given the medium used to gather information (an IT news site), this research will not have reached smaller organisations with little or no internal IT resource (the bulk of small businesses). The upshot of this is that the results presented may not be representative of the broader business population.

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 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.

About Barracuda Networks, Inc. (NYSE: CUDA)

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security.

For additional information, please visit www.barracuda.com.

Terms of Use

This report is provided for your general information and use only. Neither Freeform Dynamics Ltd nor any third parties provide any warranty or guarantee as to the suitability of the information provided within it for any particular purpose.