The End User Security Jigsaw

Completing the puzzle for your organisation

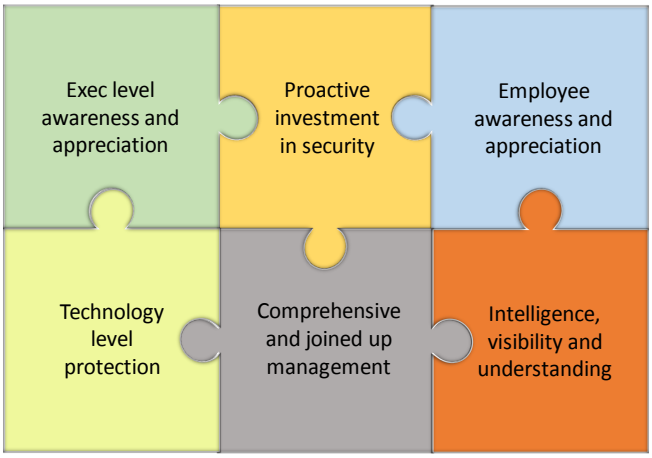
Freeform Dynamics Ltd, August 2013

Security remains a hot topic in both the IT industry and the media. Widespread reporting of breaches experienced by household brands has kept the discussion going, and revelations from high-profile 'whistle-blowers' have added fuel to the fire. Closer to home, organisations of all sizes are trying to understand the security implications of mobile working, device proliferation and BYOD. But with IT vendors offering up a broad range of options, it can be hard to know where to focus your efforts.

Key Points

Stop press: The end user computing environment is becoming more complex and challenging
OK, so this might be an obvious statement, but the reality of it came through strongly in feedback received from 977 respondents during a recent online survey. Specific factors conspiring to increase user-related risks include a growing emphasis on employee empowerment, and a greater reliance on mobile working and information access. Device proliferation and BYOD are then aggravating factors on top of these.

End user security is about much more than technology level protection
Quantitative analysis of data together with extensive commentary from study respondents yielded some great insights. Based on these, we are able to highlight six areas that have a significant impact on how confident organisations are in meeting their immediate and future end user security needs:



This broader picture matters because it's too easy for attention to get sucked into focusing purely on technology level protection, which will only get you so far.

A balanced and holistic approach is required for success
When looking to drive improvements, it is important to deal with all of the pieces of this puzzle. Without a more proactive and holistic approach, the likelihood is you will end up continually fighting fires that will increase in number and become more difficult to put out over time. The right approach, however, will reduce IT overhead and hassle, and reduce costs and risks within the business.

The study upon which this report is based was designed, executed and interpreted independently by Freeform Dynamics Ltd. The research was sponsored by McAfee, and responses from 977 IT and business professionals representing a range of organisation sizes and industries were gathered via an online survey hosted on a popular news site.

CONTENTS

Introduction 3
Defining the problem 3
Assessing current confidence 6
The end user security solution puzzle 6
Technology level protection 7
Comprehensive and joined up management 7
Intelligence, visibility and understanding 9
Employee awareness and appreciation 10
Executive level awareness and appreciation 11
Proactive investment in security 12
Assembling the jigsaw 13
Appendix A: Study sample 14
Limitations of research data 14
Appendix B – Confidence based analysis 15
Appendix C – Technology level protection in more detail 16
Drill down charts on specific solutions 16
About Freeform Dynamics 20
About McAfee 20
Terms of Use 20

Introduction

Risk management is not about absolutes or certainty; it's about playing the odds. This principle is particularly relevant when it comes to securing end user computing activity.

We have no shortage of solutions available to us in this area. Indeed looking at what's available on the market, it's clear that many options exist for tackling the same or similar requirements. The problem, however, is that none of them are 100% effective at what they are supposed to do. But even if they were, the complexity of the environment along with the dynamic nature of the problem means no single technology or service is ever going to be enough. Minimising your exposure is about mixing the right cocktail of solutions and approaches to achieve an 'acceptable' level of protection for your organisation and the situations that arise within it.

In an attempt to understand what this translates to in practice, we conducted an online research study during June and July 2013 in which data was gathered from 977 IT and business professionals. In terms of scope, the questionnaire used was one of the broadest we have ever developed at Freeform Dynamics, and our thanks go out to all of those who had the patience to work through it. The exercise was well worth it, however, as we ended up with a good holistic view of the things that really matter.

Before getting into solutions and approaches, however, it's important to understand the problem. So let's start out by looking at the nature of the end user security challenge.

Defining the problem

Most IT professionals have fantasised at some point about how easy life would be without end users. You build great systems, put what you think are robust policies and procedures in place, then a user comes along and finds some way of messing it all up. As one respondent put it, though:

> *"Without users, all security issues would go away. But without users my job would go away too. So, I need those users, whatever I might think of them".*

Seriously, apart from providing many of us with employment, supporting and protecting the activities of users is more important than ever. This becomes clear when we consider the increasing reliance on information access, mobile working, and the general empowerment of employees to operate effectively in a fast moving business environment (Figure 1).

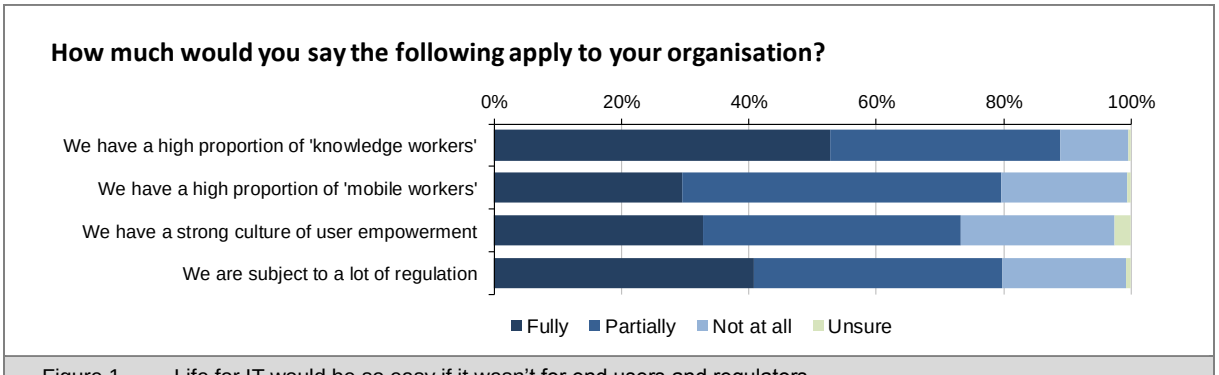


Figure 1 Life for IT would be so easy if it wasn't for end users and regulators.

And the regulators don't help. As we can see from this chart, most organisations need to keep an eye on compliance to one degree or another.

Another complicating factor is the way in which the end user technology landscape is becoming more diverse. Gone are the days when all we had to think about was the Windows PC and perhaps a few BlackBerries. If you look across your workforce today, the chances are you will see a range of form-factors in use running a variety of different operating systems (Figure 2).

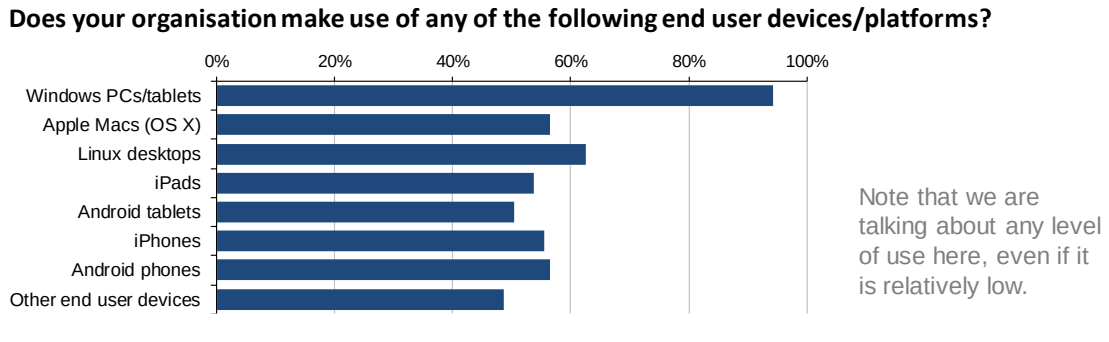


Figure 2 The range of devices in use within the workforce has proliferated significantly in recent years.

Even if it's only a few employees using a particular platform, you still need to pay attention. A basic but important principle is that the overall security of your business is defined by whatever represents the weakest link. In device terms, that could be a handful of users with Android smartphones who are exposed to malware-infected apps without anyone acknowledging their existence or the risks they are running.

The potential for exposure here becomes particularly acute when we consider the use of personal devices for work purposes (Figure 3).

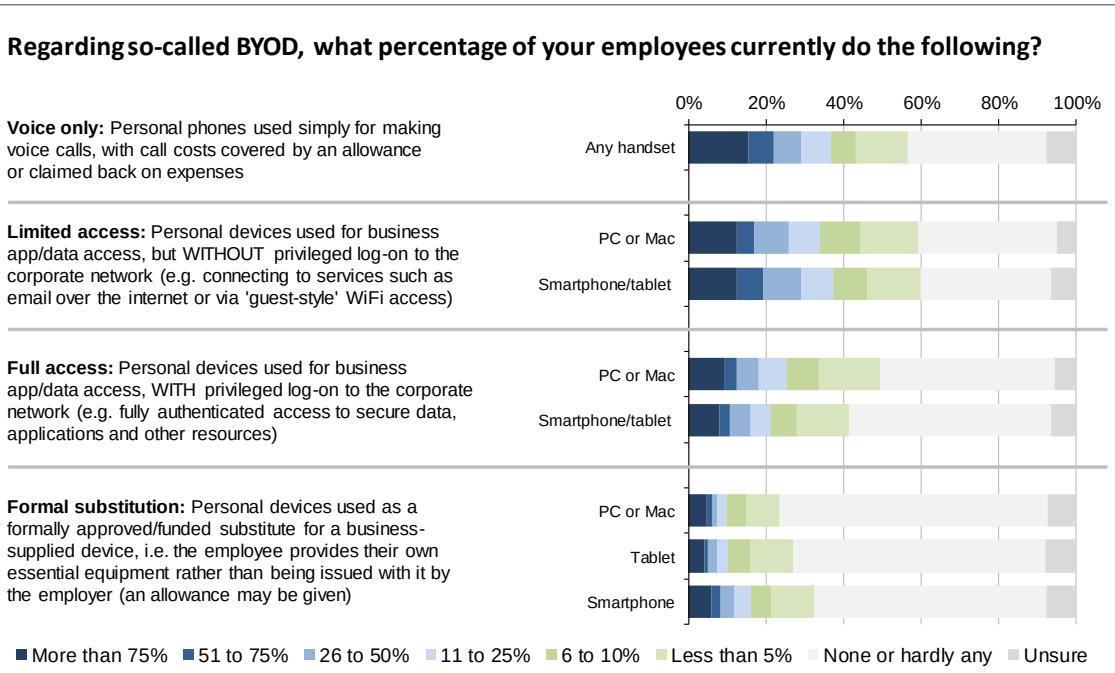


Figure 3 While most BYOD does not involve privileged access to the network, employees are still often handling sensitive business information on personal devices.

We can see from this that most so-called 'Bring Your Own Device' (BYOD) activity doesn't currently involve privileged access to the corporate network. This should not be a source of comfort, however, as employees are still often handling sensitive data on personal equipment. It might just be email access from outside the firewall using a secure ActiveSync connection, but the contents of messages and attachments that end up being stored on the user's device can clearly still be very sensitive.

Beyond email, any connected device is a potential target for attack via the internet. In fact, respondents in our study put the risk of malware infection from the Web ahead of threats relating to email and removable media (Figure 4).

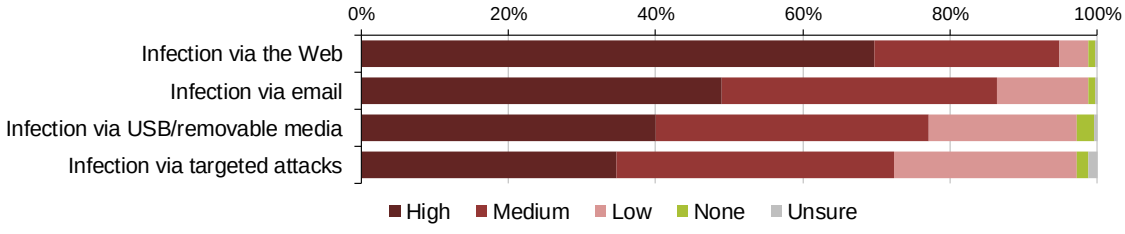


Figure 4 Within our sample, Web related threats are regarded as more prevalent than threats stemming from email and removable storage media/devices. Many also highlight the risks from targeted attacks.

The acknowledgement of targeted attacks that we can also see on this chart highlights the risk of more focused efforts to penetrate business systems. It's not just large organisations that need to be concerned with this. We haven't shown it here but respondents from smaller businesses in our study also often see themselves as potential targets. This is understandable when you consider that a good way to attack a large multi-national is via one of its suppliers.

With this in mind, many security specialists and advisors in the industry are today talking about 'Advanced Persistent Threats' (APTs). These are based on bad guys taking a patient and methodical approach to penetrating systems over an extended period of time. Along the way, all possible entry-points are explored through a variety of techniques until a vulnerability is found. Step-by-step, knowledge of the organisation and its systems is then built up, allowing progressively deeper penetration to be achieved.

Targeting people with trusted access through phishing, social engineering and other types of deception typically plays an important role in such advanced targeted attacks. The reason for this isn't surprising when we look at how our respondents characterise the risks that stem from users themselves (Figure 5).

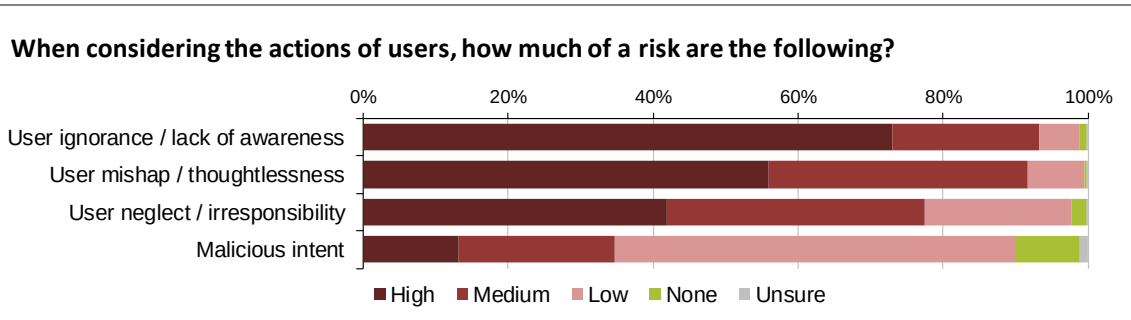


Figure 5 Requirements frequently stem from workforce, working practice and compliance-related factors.

As we can see, malicious intent, while not to be dismissed, is the least of the problems study participants are concerned about. Most of the risks relating to user behaviour are connected with accidents, neglect or users simply not knowing any better. This obviously isn't just relevant to targeted attacks. Probably the bigger risk is of users inadvertently doing things that lead to leakage of sensitive data or malware infection from more opportunistic threats.

So, in summary, we have users doing increasingly risky things in the name of productivity, empowerment and flexibility, utilising a proliferating and constantly changing set of devices, while the threats out there continue to develop in new and challenging ways.

The following respondent quote sums up the result of this quite nicely:

> *"The battle of convenience versus security is ongoing, both with users and management".*

With that, how well do those participating in our study believe they are doing?

Assessing current confidence

It's difficult to get a precise view of threats and exposure when conducting research via surveys. IT and business professionals are often not willing to admit to specific incidents and vulnerabilities, so you can never be sure that what you are told is accurate or complete. In order to form a view of how well participants felt they were doing, we therefore asked some high level questions that were a bit more subjective in nature, but good enough to capture the general level of confidence in meeting current and future needs.

From the responses, we learned that only a few organisations are completely confident in the measures they have in place, though most indicate they are doing 'OK' meeting immediate needs (Figure 6).

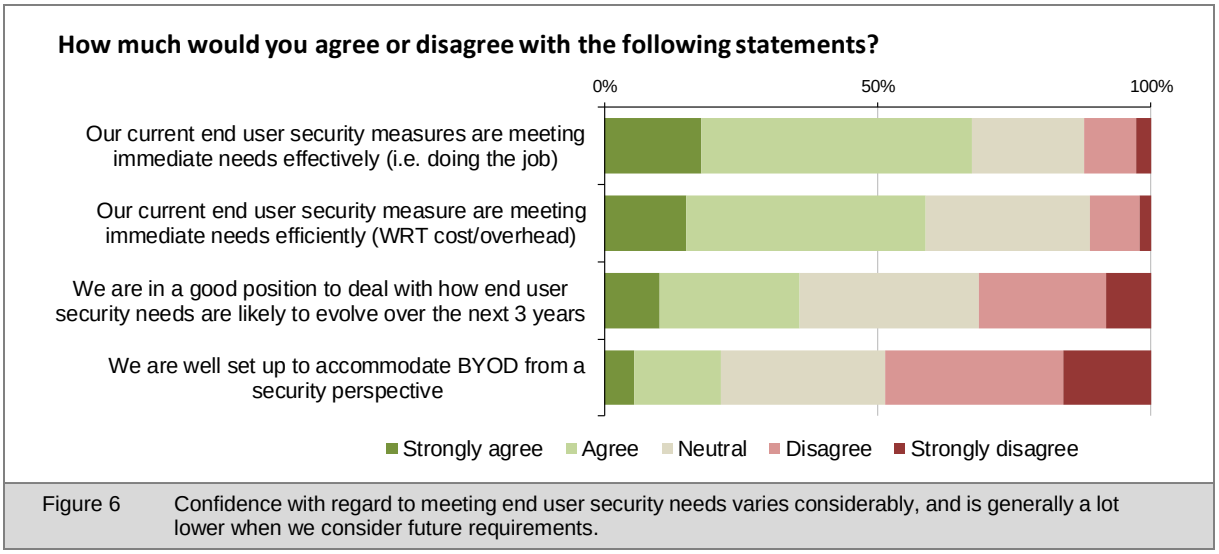


Figure 6 Confidence with regard to meeting end user security needs varies considerably, and is generally a lot lower when we consider future requirements.

What's also clear from this chart, however, is that some organisations have little or no confidence at all in their end user security measures. Furthermore, as we look to the future, and particularly the challenges of dealing with BYOD, the level of confidence falls away considerably.

It's worth nothing that this question came at the very end of our survey, after participants had worked through a lot of detail. Issues and practicalities were therefore front-of-mind at the time, so we can view these responses as being reasonably well considered.

The end user security solution puzzle

The remainder of the results from our study are mainly focused on the solution side of the equation. As we analysed these, we began to form an understanding of the key components of a successful end user security strategy. In many ways, this process was like discovering and assembling the pieces of a jigsaw puzzle. As we did this, a clear picture of what really matters started to emerge.

Along the way, we gained insights from a couple of things in particular:

Confidence based analysis
When we saw the above level of variation in confidence, the obvious question that occurred to us was why some respondents were more confident than their peers. We therefore divided respondents into a '*Confident Group*' and '*Others*' group so we could compare the two (see Appendix B for an explanation of how we did this).

Freeform feedback from respondents
When designing the questionnaire for the study, we deliberately left space for respondents to express themselves freely on certain topics. Some of the quotes you have already seen were captured in this way. This kind of feedback provided additional insights that complemented the more quantitative data.

So let's walk through the pieces of the puzzle one by one in the order we discovered them.

Technology level protection

When considering end user security, it is natural to gravitate to the technology aspects of the discussion. As we said at the outset, however, one of the challenges here is that there are so many options available. It can be hard figuring out which combination is right for your business and the scenarios you are trying to deal with within it.

During the study, we looked at a broad range of the technology level protection options available, across areas such as anti-malware, firewall, encryption, data loss protection (DLP), black-listing, white-listing, and various forms of virtualisation that can be brought to bear in a desktop or mobile computing context.

It would be nice to say that this aspect of the research was conclusive and that we could provide a formula for assembling the optimum mix of technology and services to achieve maximum protection. However, it quickly became clear that this was not going to be possible.

Some organisations, for example, put a heavy emphasis on device-side anti-malware, while some say this kind of protection should live in the network or in the cloud. Meanwhile, others argue that you should attempt to block malware at all levels to provide the best chance of filtering out the threats. Mixed up in all this is then the debate about devices and operating systems. Should you install third party malware protection on Windows machines, Macs, iDevices or Android based equipment? Again, we received lots of different views on this and other forms of protection.

If you are interested in seeing some of the detailed findings in relation to technology level protection you will find them in Appendix C. For now, however, it's probably worth restricting our discussion to the highlights in this area that came out of the confidence-based analysis.

The '*Confident Group*' within our study are generally more likely to:

- Use third party anti-malware and firewall software across all device types
- Implement data loss protection (DLP) technology
- Exploit cloud-based content-filtering services
- Encrypt data on desktops and mobile devices, as well as notebooks
- Lock down mobile devices in particular
- Control application/service access via black-lists and white-lists
- Employ various virtualisation and sand-boxing techniques
- Favour the embedding of device security at a hardware level

It must be stressed, however, that the correlations listed here are far from absolute. This reinforces the notion that it's possible to tackle specific aspects of the end user security problem in different ways. It also tells us that protection technology itself only gets you so far. This brings us onto the next piece of the puzzle.

Comprehensive and joined up management

From the discussion so far, it will be evident that the end user environment and the security solution landscape required to protect it can be very complex. This is therefore an area in which we would expect management tools and processes to be particularly important. During the study, we therefore quizzed respondents on the kind of facilities they have in place from a management perspective.

Not surprisingly, this was an aspect of end user security in which we picked up some very significant differences between more confident organisations and their peers. These are notable across the three key domains of Windows desktop management, management of non-Windows desktops (e.g. Mac and Linux), and looking after mobile devices (i.e. smartphones and tablets). The *Confident Group* are much more likely to have comprehensive and joined up management facilities in place within each of these (Figure 7).

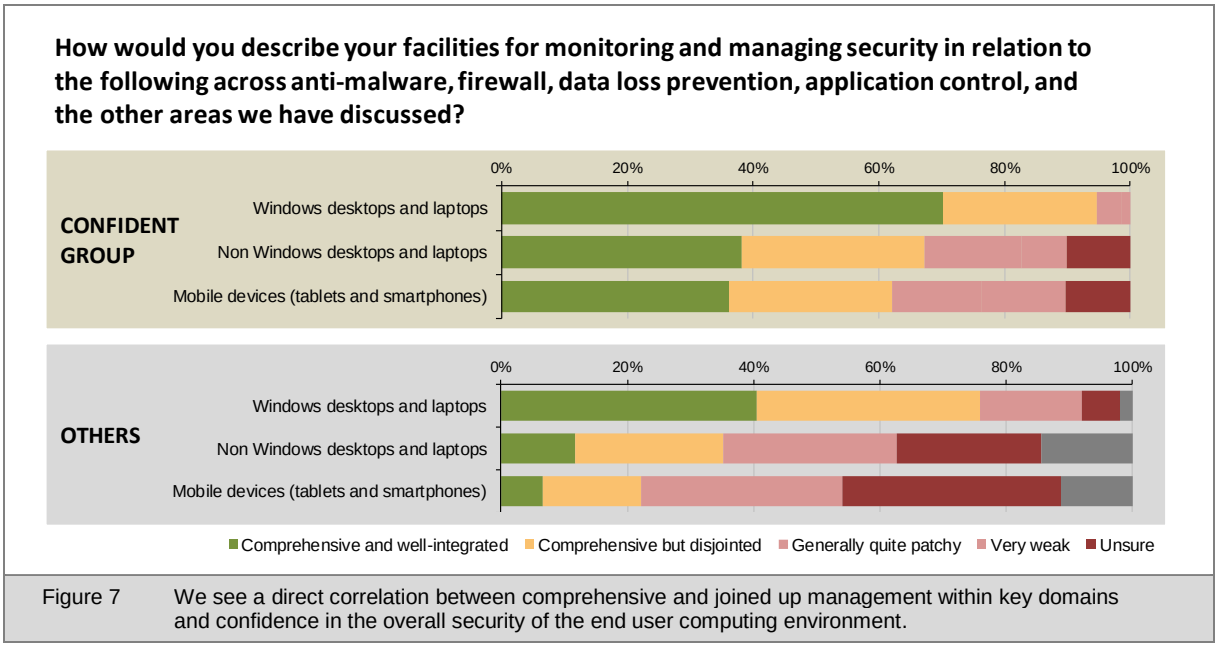


Figure 7 We see a direct correlation between comprehensive and joined up management within key domains and confidence in the overall security of the end user computing environment.

Of course when we look at how things are evolving, it becomes clear that managing different device-types separately may not make sense in the longer term. A number of key trends are important to consider in this respect:

- Individual users are increasingly utilising more than one device to access business systems and data, including non-Windows desktops and notebooks, as well as mobile equipment.
- Virtualisation of desktops, applications, data and user preferences is on the increase, and it is only a matter of time before virtualisation becomes normal to consider for mobile devices too.
- The lines are blurring between device categories, to the point where it is already difficult to draw a hard and fast line between notebooks and tablets, and tablets and smartphones, when it comes to specs, software and general capability.
- Most organisations can expect BYOD to creep into the mix over time if it isn't doing so already, particularly for important user segments such as executives, managers, marketing professionals, sales teams, consultants, and so on.

With this in mind, it is unsurprising to see respondents aspiring to put a device-agnostic management approach in place, with everything being joined up in various dimensions (Figure 8).

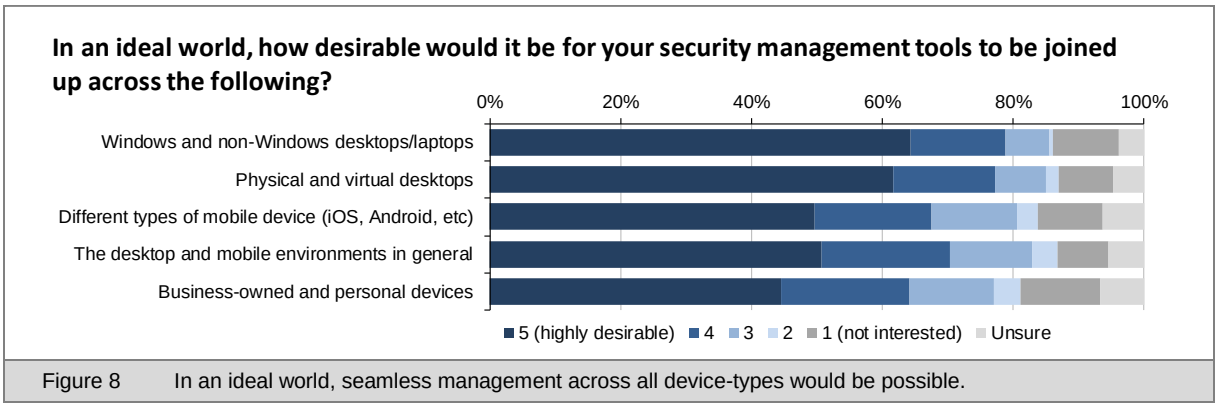


Figure 8 In an ideal world, seamless management across all device-types would be possible.

And when we turn to current capability, we can see that organisations in the *Confident Group* are already taking steps to implement more coordination across traditionally separate domains (Figure 9).

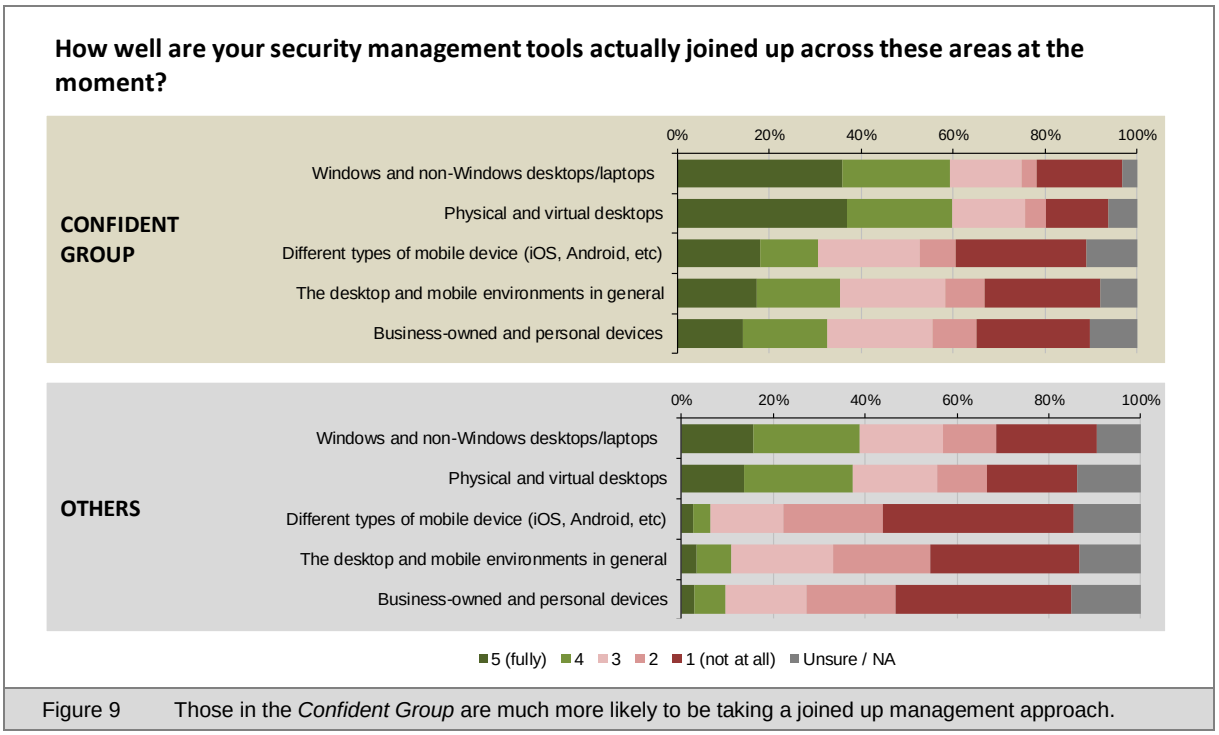


Figure 9 Those in the *Confident Group* are much more likely to be taking a joined up management approach.

As time goes on, the over-arching trend is likely to be towards a more user-centric approach to management so security policy and protection can be defined and applied consistently across devices.

Intelligence, visibility and understanding

The management facilities we have been discussing will provide basic tracking and monitoring of assets, applications and data, and how they are used. Beyond this routine operational visibility, however, a broader and deeper understanding of both threats and activity is also important for effective end user security.

One of the aims is to use insight and automation to detect suspicious activity in real time and react immediately. In addition, accumulated historical data may be exploited to better understand threats and vulnerabilities in order to pre-empt future attacks and allow protection efforts to be targeted more effectively. Given this, the strong correlation we see between confidence and the use of security analytics makes absolute sense (Figure 10).

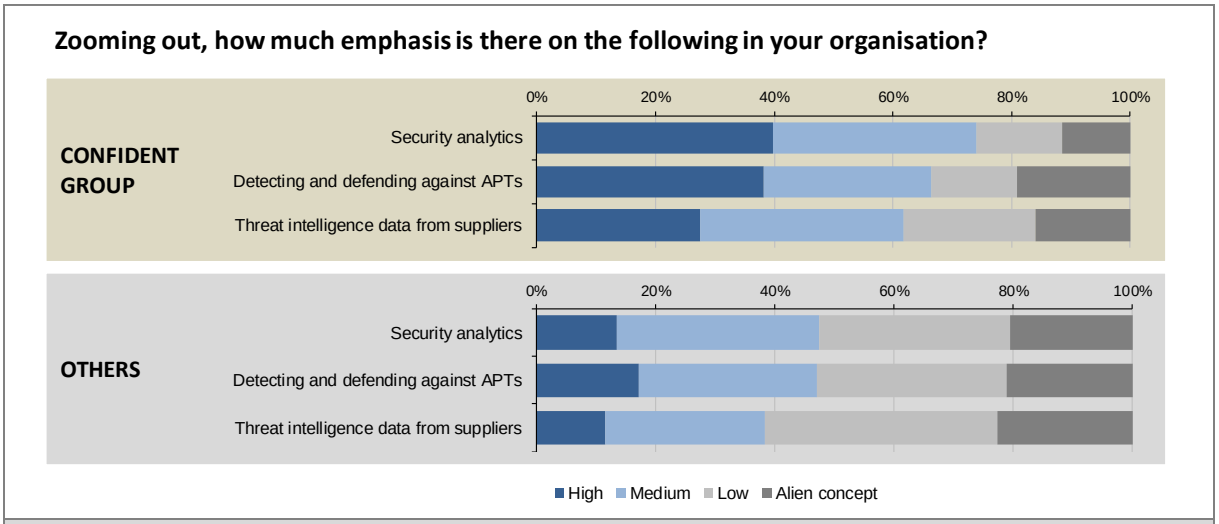


Figure 10 Visibility and understanding are key to both preventative and remedial activity.

Seeing security analytics going hand in hand with an increased focus on detecting and defending against APTs is also understandable, as is exploiting threat intelligence data from suppliers. On this last point, some of the larger security solution vendors and service providers gather a huge amount of data from their customers on the way the threat landscape is evolving. This is again helpful to identify potential vulnerabilities and pre-empt attacks of various kinds.

The value of visibility and understanding in the context of ongoing planning and review or more time-critical incident handling is underlined by the following insightful comments from respondents:

> *"When it comes to end user security, many people are 'doing something' - whether they are doing something that is genuinely useful is a completely different question".*
>
> *"I fully believe that it isn't a case of preventing intrusion; it is naive to assume you can. It is how you detect it and deal with it, and what measures are in place that would limit damage should it happen".*

These are representative of a lot of the freeform feedback we received in this area.

Employee awareness and appreciation

Another area in which freeform feedback was very forthcoming has to do with user behaviour. Building on the results we saw earlier highlighting the problems of ignorance, accidents, thoughtlessness, and neglect, many respondents told us of the importance of end user awareness and appreciation of security matters:

> *"The focus should be on people, not hardware and software".*
>
> *"The technical problems are secondary. The tough bit is getting non-technical users to even accept it is their responsibility to engage with, not work against the IT department".*
>
> *"We have too much emphasis on buying stuff, not enough on teaching users".*

These are just a few of the many comments we received on the challenges of working with users when it comes to security matters. Issues highlighted included how to achieve the right balance between restricting user activity to minimise risks, and providing the freedom, flexibility and convenience necessary for users to do their jobs productively. Many respondents, however, simply referred to how hard it can be to motivate users to take security seriously. As part of this, frustration with ill-thought out BYOD activity came across very strongly. Indeed, BYOD appears to be one of the major preoccupations of IT professionals with whom the buck often stops when it comes to systems and information security.

Looking at the quantitative data, dealing with the challenges of user attitude, awareness and behaviour is clearly a tough area. Even though those in the *Confident Group* are twice as likely to have a high emphasis on user training, we see a general lack of focus in this area across the board (Figure 11).

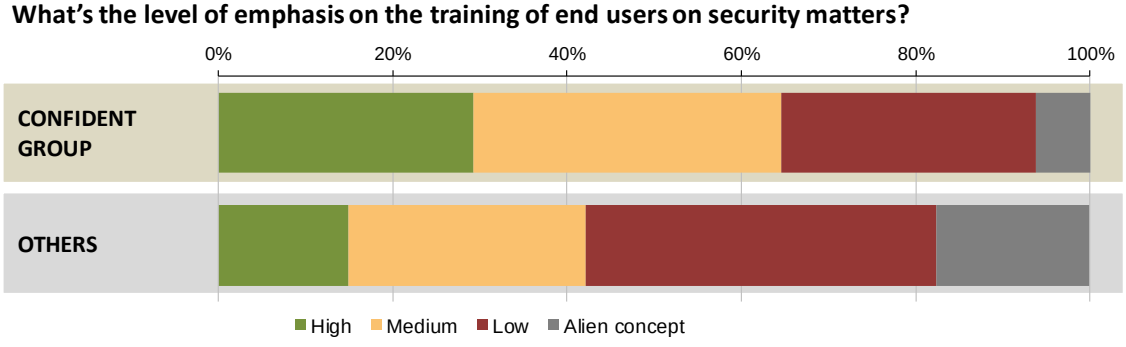


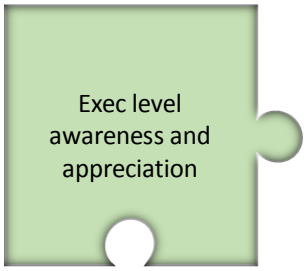
Figure 11 End user training is seen as important by some, but this remains a very challenging area.

As the following comment indicates, lack of security consciousness among users, however, isn't helped by the bad example set by senior managers within the business:

> *"When the boss doesn't care about, think about, or want to know about security, then an organisation's security-conscious personnel are doomed".*

This brings us on to the next important piece of our puzzle, which has to do with leadership and executive responsibility.

Executive level awareness and appreciation



Every senior manager needs to make choices about how to allocate the finite levels of budget and resource under their control.

In this respect, security is just one of the many potential areas for investment competing for attention. Those running the business must therefore have an adequate level of awareness and appreciation for security, otherwise it will not receive the level of attention it deserves:

> *"C-level execs MUST understand and push a change in attitude to the value of information, before security will be seen as standard as seatbelts in cars".*

Given this, it is no coincidence that we see a significant correlation between executive awareness and the level of confidence that exists in organisations with respect to end user security (Figure 12).

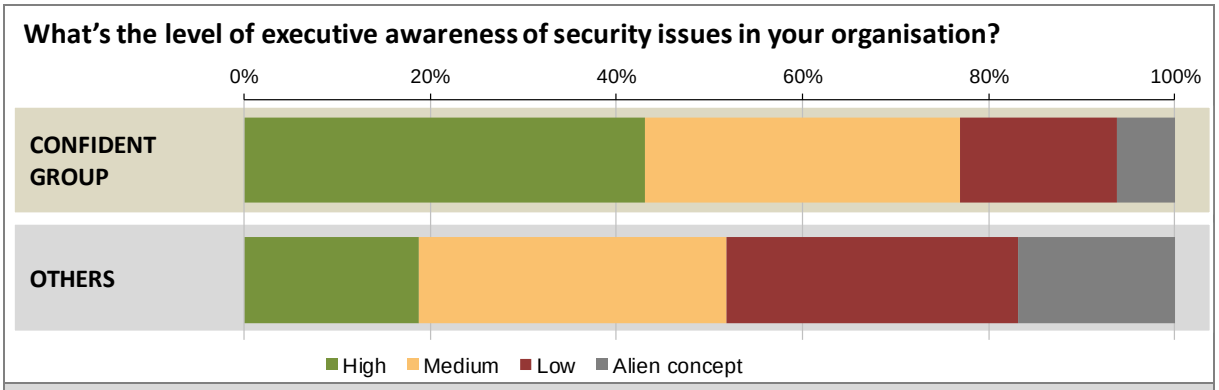


Figure 12 Executives are much more likely to be tuned-in to security matters within the *Confident Group*.

But the freeform feedback gathered during our study suggests that even if executives acknowledge the importance of security in a general sense, they often don't have a good feel for what this translates to in terms of practicality:

> *"Management understand the requirement for security but do not understand the implementation".*

> *"Management has a hard time grasping why good security costs as much as it does, and therefore is reluctant to properly fund it".*

An aggravating factor here is the common belief that because the security discussion usually revolves around systems and information, it's the responsibility of the IT department to take care of it. As far as some senior managers are concerned, the problem has then been delegated, so it's not something they need to spend time thinking about, until, of course, something goes horribly wrong:

> *"Security is never considered a priority for upper management; of course until there is a major breach".*

Breaking this reactive approach to dealing with security requirements is the idea that underpins the last piece in our end user security jigsaw.

Proactive investment in security

The dynamic nature of the end user computing environment and the rapid way in which threats continue to evolve means you stand little chance of staying on top of things with a reactive approach.

If you don't pay attention to requirements until your hand is forced by a technology change, a new type of user behaviour, or a security breach, the result will be unnecessarily high costs and risks. The reactive approach is also a recipe for uncertainty, stress and disruption within the business which you can well do without.

Acting more proactively means you can anticipate and pre-empt challenges to come. At the time of writing, for example, the device proliferation and BYOD trends are clear, and it's only a matter of time before even the most resistant of IT departments is required to take these on board.

Many of those in our *Confident Group* are already taking this need for proactivity on board (Figure 13).

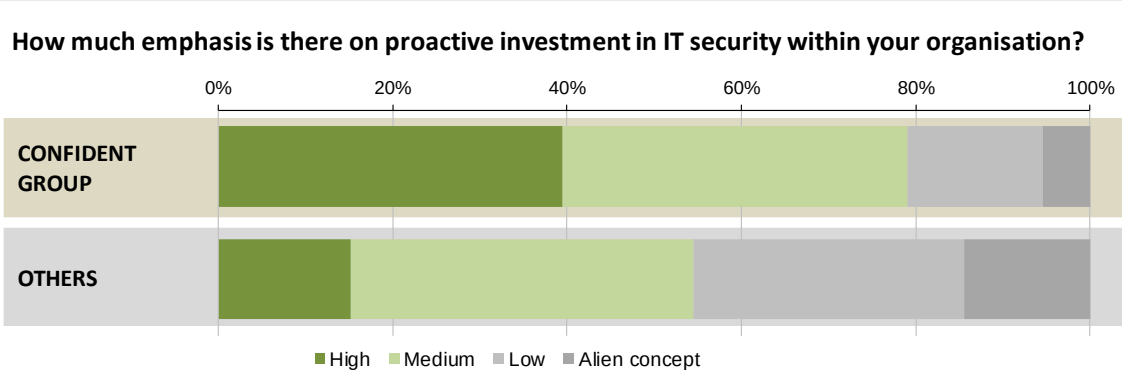


Figure 13 Forward-thinking organisations look to invest more proactively in security related improvements.

Consistent with this, and in line with the general desire for a more joined up approach, a significant number of organisations are looking to reduce the level of fragmentation. This often translates to a greater emphasis on integrated suites (Figure 14).

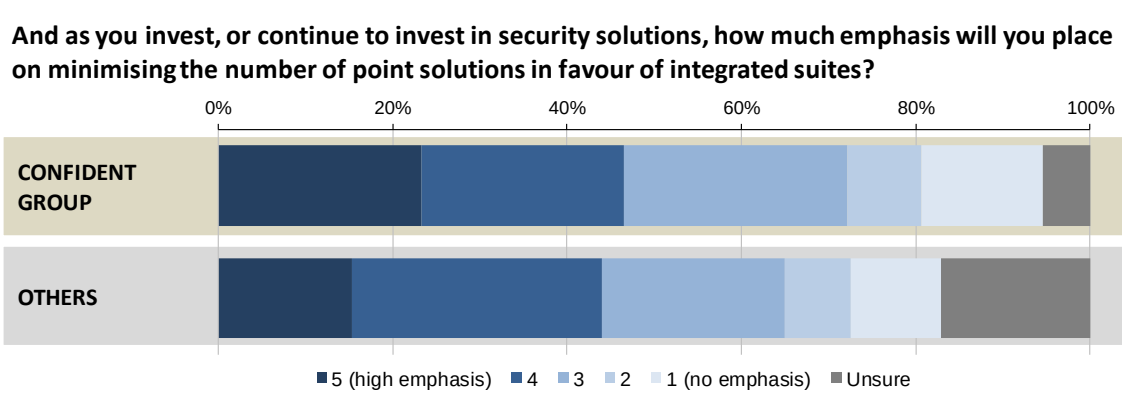


Figure 14 The increased focus on integrated suites is consistent with the need for a more joined up approach.

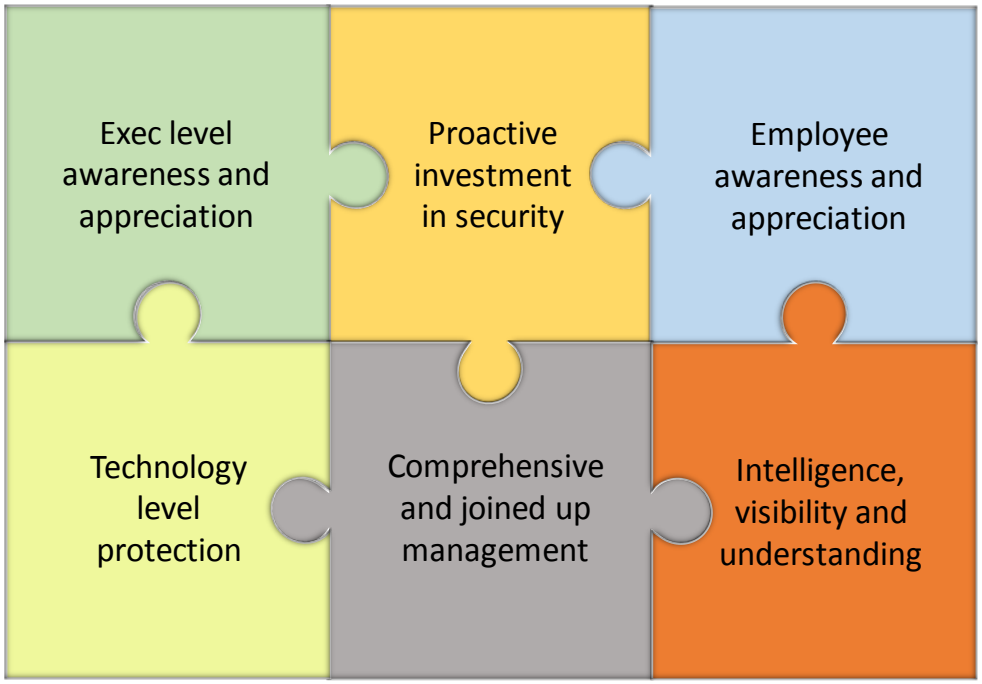
With this last piece of the puzzle defined, let's talk about how to pull it all together.

Assembling the jigsaw

Listening to a lot of the marketing in the IT industry, it's easy to get the impression that a single 'hero' solution is the answer to all of your end user security needs. There are a lot of vendors out there at the time of writing, for example, saying it's all about BYOD and that the answer lies in adopting their 'Mobile Device Management' (MDM) solution. Others argue that all of your challenges will go away if you simply adopt cloud-based options or virtualise everything.

The reality, as we have seen, is that end user security is a complex area that needs a considered and blended approach to handle the risks efficiently and effectively without undermining user productivity and satisfaction.

The pieces of the puzzle are clearly defined, and if we assemble them, we get a pretty good picture of the areas to which attention must be paid:



As you continue to develop your own capability, we encourage you to use this picture to make sure the scope of your improvement activities is broad enough. It's all too easy to get sucked into focusing purely on the technology level protection piece in the bottom left hand corner. It's not that this isn't important, it's just that without executive level air cover, you won't get the investment you need, and without intelligence and visibility you won't know where to invest your money, time and effort anyway.

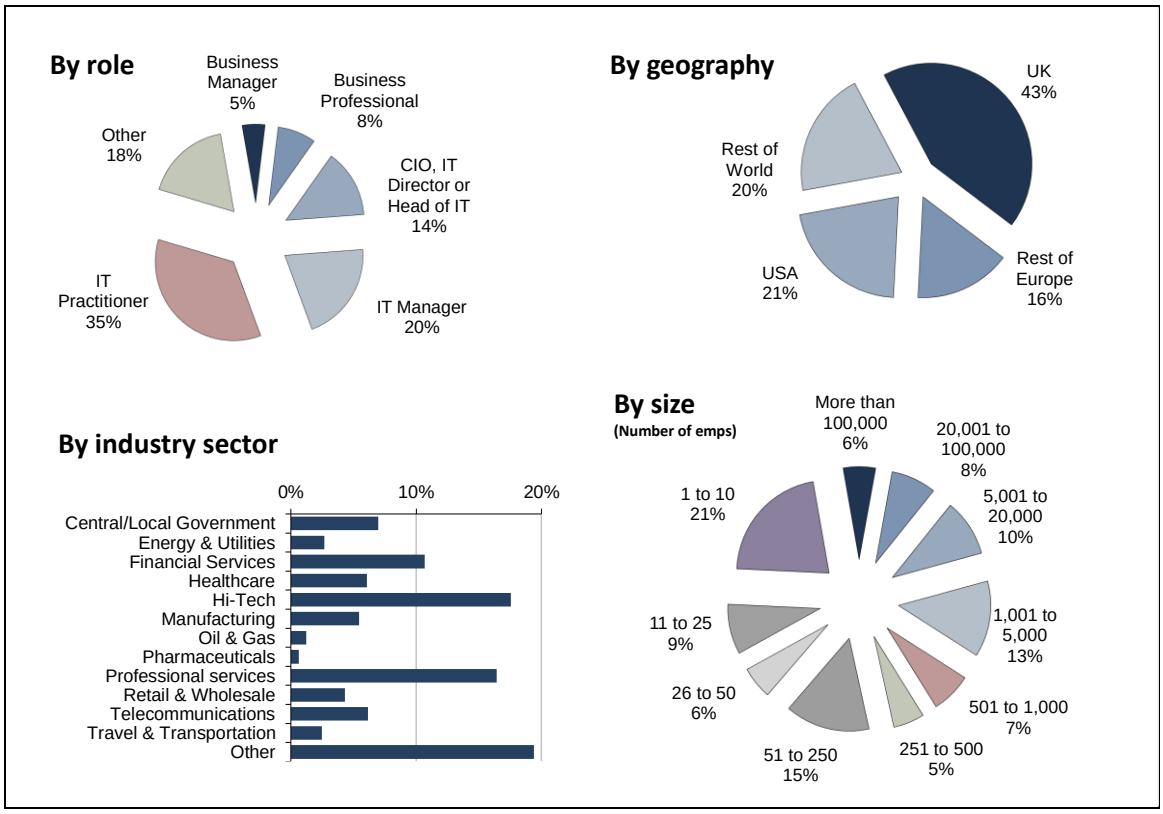
Perhaps the two areas we would really stress the importance of, however, are user education and joined up management. The first is something many tell us they are struggling with at the moment, and as users become increasingly more empowered, the challenges will only get worse. The second is simply a practical reality. Todays fragmented management environments will not cope well with the virtualised, multi-device, BYOD world we are headed for, so better to start thinking about that now if you aren't doing so already.

In the meantime, we hope our discussion in this report has helped to put what really matters into perspective when it comes to securing the end user computing environment.

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 via a Web survey hosted on a popular IT news site (www.theregister.com).

The sample distribution was as follows:



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 will not be representative of the broader business population, so percentages relating to distribution, penetration, activity levels, etc must not be taken literally.

These limitations, however, do not undermine the analysis and insights presented in this report, as we have focused on relative differences in results in order to draw our conclusions. In fact, having a more 'tech savvy' and/or 'security/savvy' sample means the feedback we received is more likely to be 'informed' rather than based on guess-work.

Appendix B – Confidence based analysis

During this report, we make frequent reference to survey sample segments relating to how confident respondents are when it comes to meeting current and future security needs. The segmentation behind this is based on the responses shown in the following chart (Figure 15).

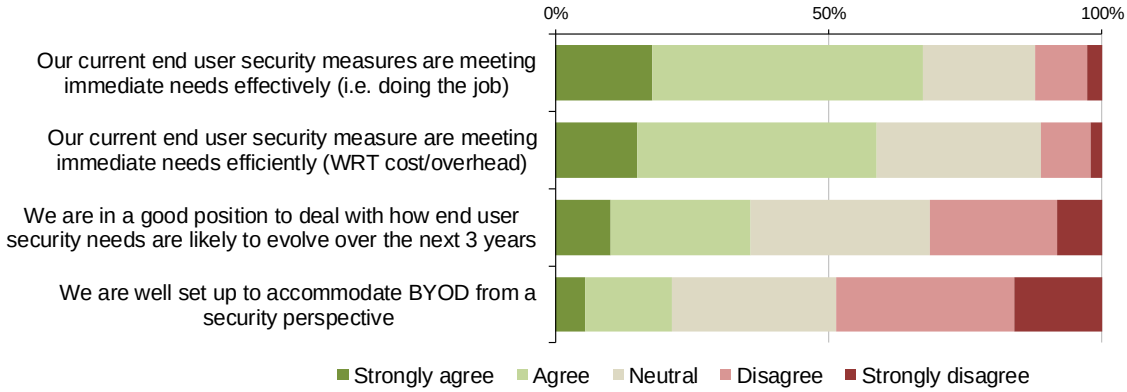


Figure 15 Responses used to segment respondents based on levels of confidence.

To begin with, the responses gathered on the agreement scale were translated into numeric scores ('Strongly agree'=5, 'Agree'=4, and so on). We then took the respondents who had an average confidence score of 4 or above and placed them in a segment we labelled the '*Confident Group*'. The idea was to examine what these organisations were doing differently to the '*Others'* that contributed to their higher level of confidence.

In order to make sense of the data, however, we needed to make one more adjustment as preliminary analysis told us that respondents at the very low end, with less than 10 employees, were confusing the analysis. This was because that part of the respondent base was heavily skewed towards small IT and security services companies whose behaviour bore no relation to the rest of the sample. They had a disproportionately high level of confidence in their end user security measures, and many had a heavy focus on desktop Linux that isn't generally seen beyond this group. For the purposes of confidence-based analysis, we therefore excluded respondents with less than 10 employees. Given that many are clearly very 'security savvy', however, we have taken their feedback on board when interpreting the study data in general.

Following segmentation, we ended up with a '*Confident Group*' containing 133 respondents, and there was no significant difference in the composition of this group compared to the '*Others'* in terms of organisation size, industry and so on.

Appendix C – Technology level protection in more detail

During the study, we gathered a significant amount of information on specific technology-based solutions for enhancing end user security. The charts presented in this appendix lay out some of the more interesting findings. As you look through these, however, please bear in mind the over-arching conclusion of the main report which tells us quite clearly that securing the end user environment effectively is about much more than protection technology.

Drill down charts on specific solutions

Please see the notes at the bottom of each chart for relevant analyst commentary:

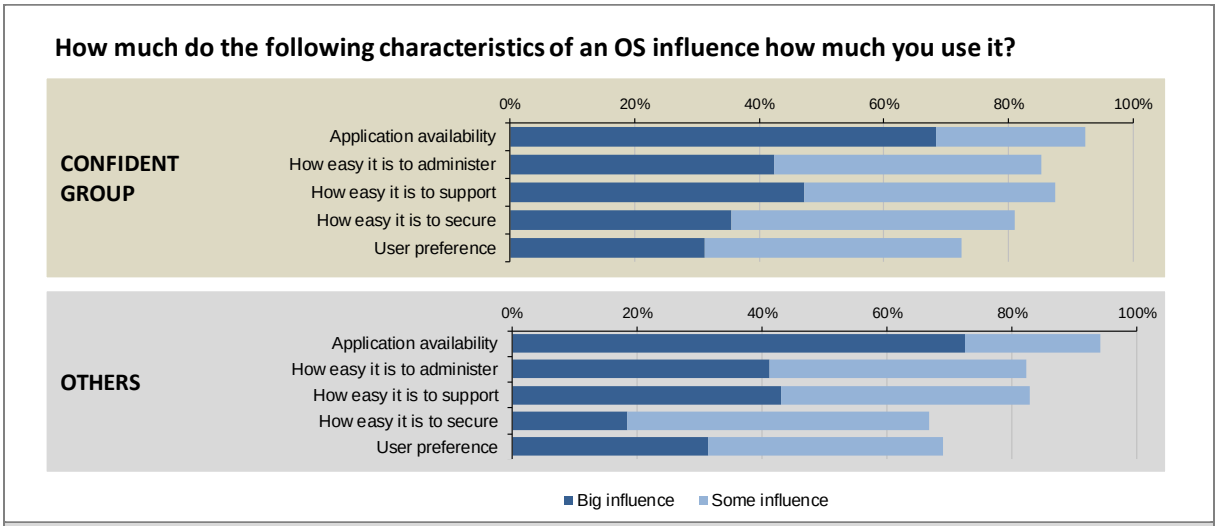


Figure 16 Most don't have the luxury of selecting devices and platforms based on their security characteristics; application availability, operational considerations and sometimes even user preference come first.

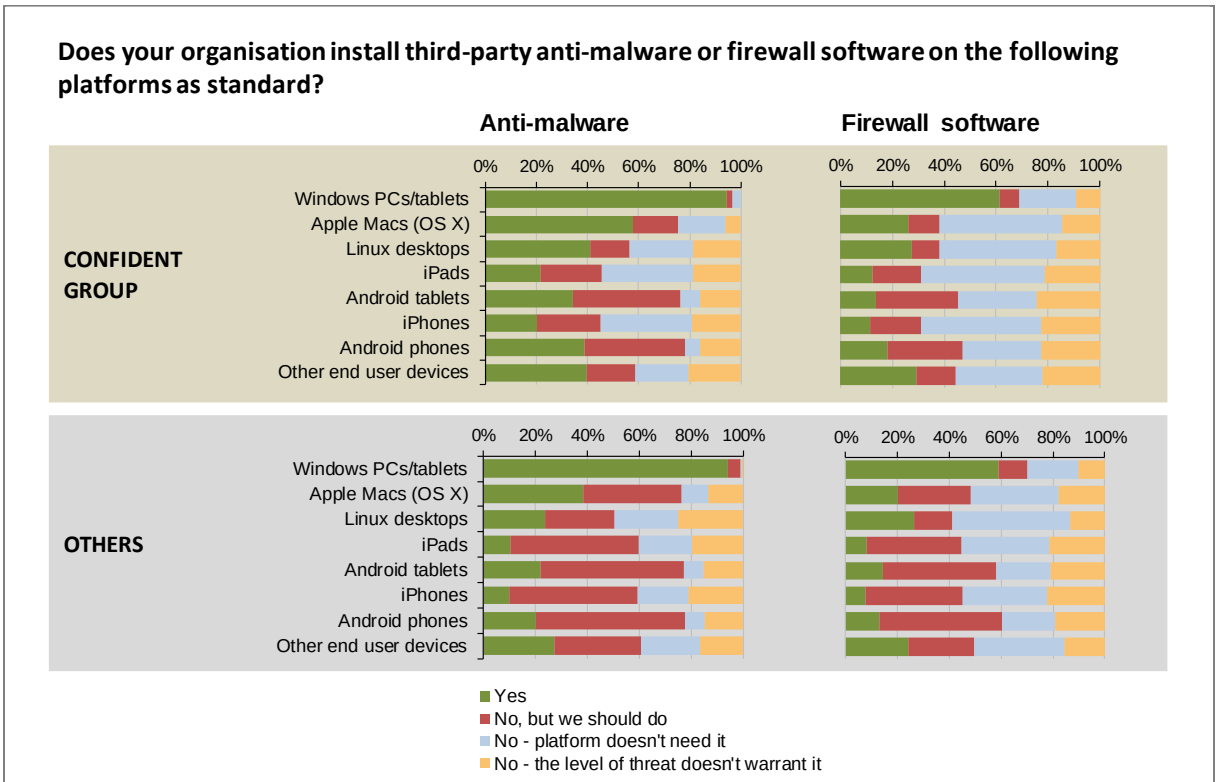


Figure 17 Many acknowledge protection gaps, but there is still debate in some areas over what's required.

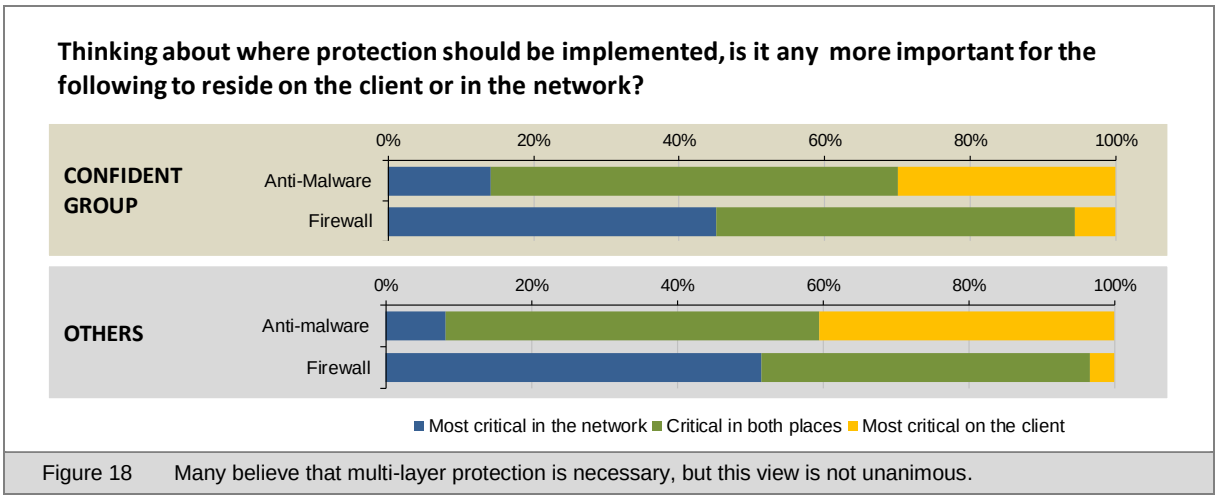


Figure 18 Many believe that multi-layer protection is necessary, but this view is not unanimous.

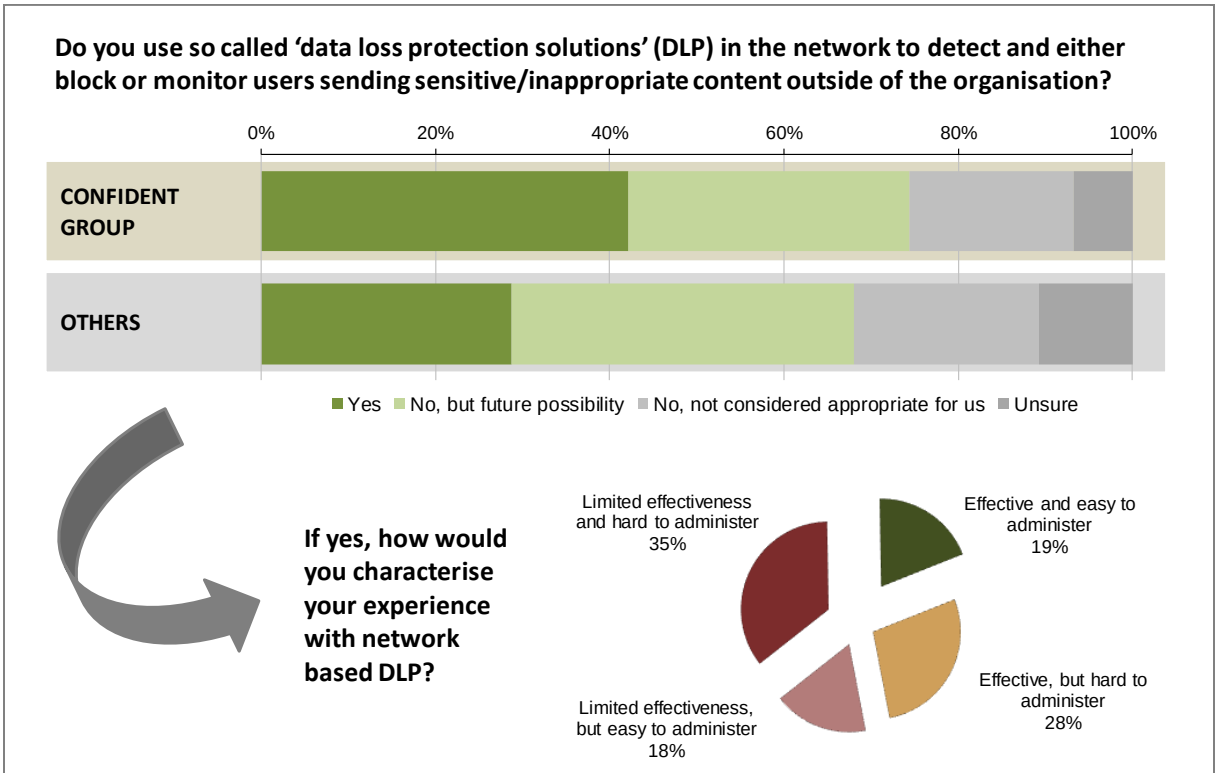


Figure 19 DLP has its place, but many struggle to administer it in a constantly changing business environment.

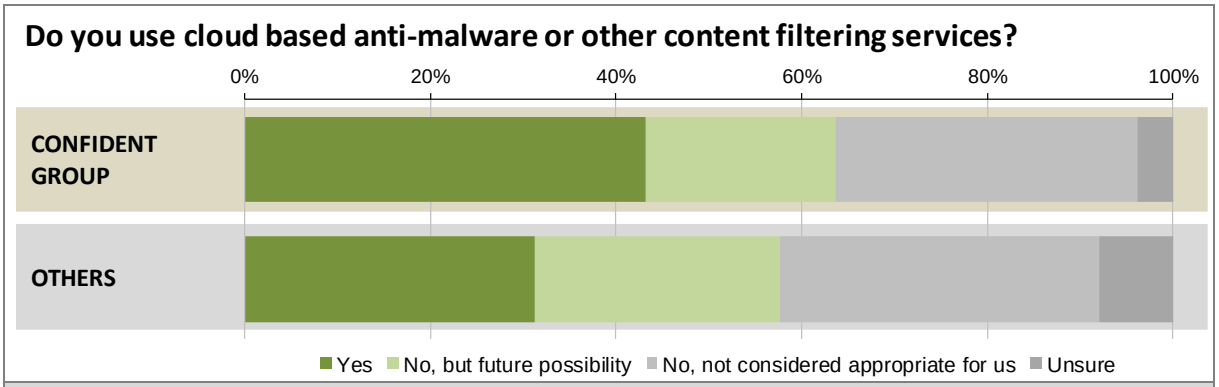


Figure 20 Views of cloud based options are generally pretty positive among those with experience of them.

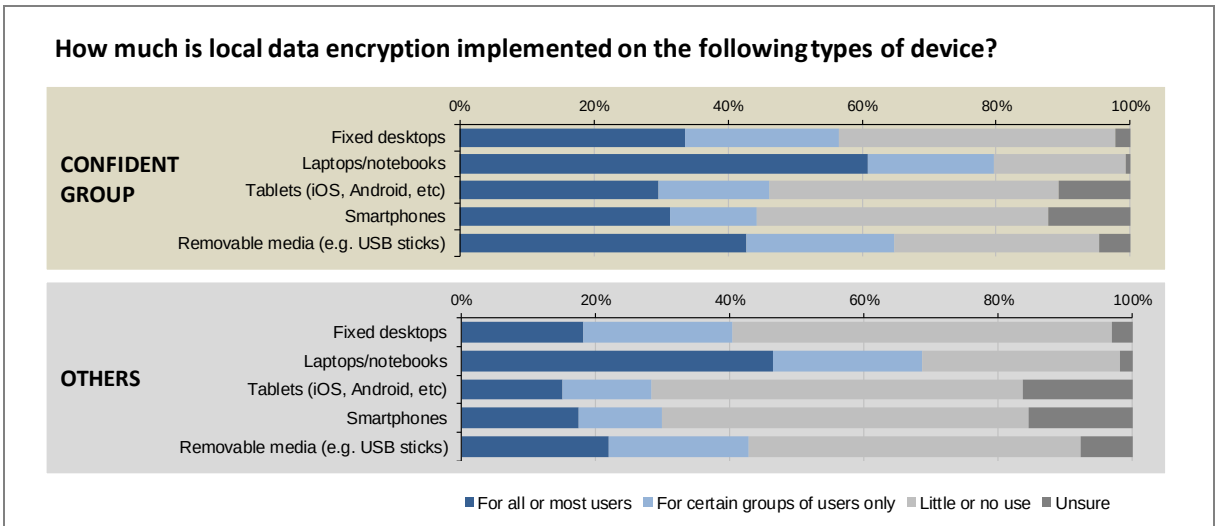


Figure 21 Many see encryption as valuable, but comments highlight challenges such as key management.

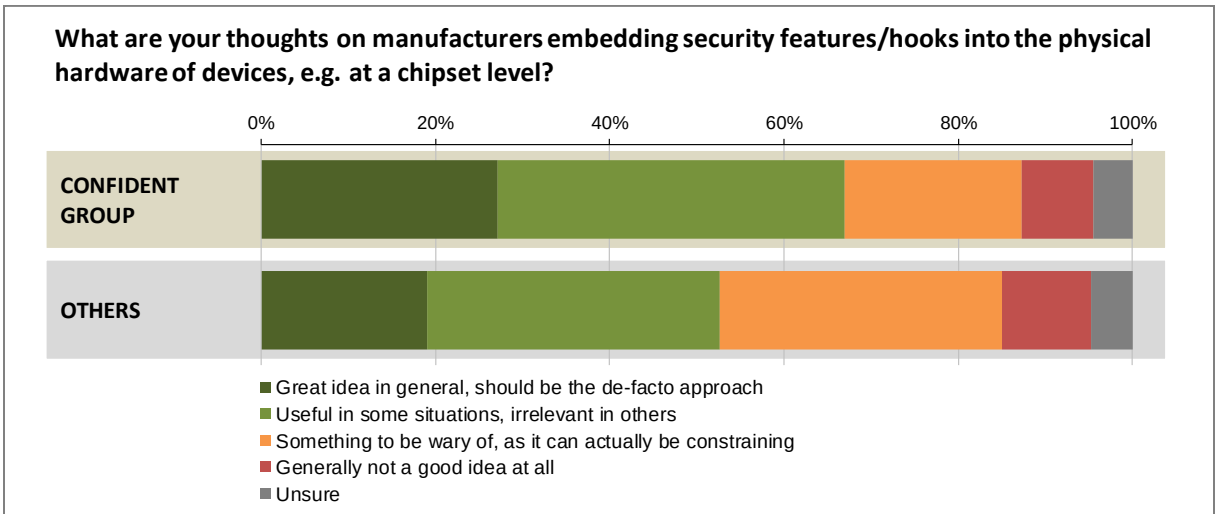


Figure 22 Positive view of hardware level security, though some have concerns about lock-in and obsolescence.

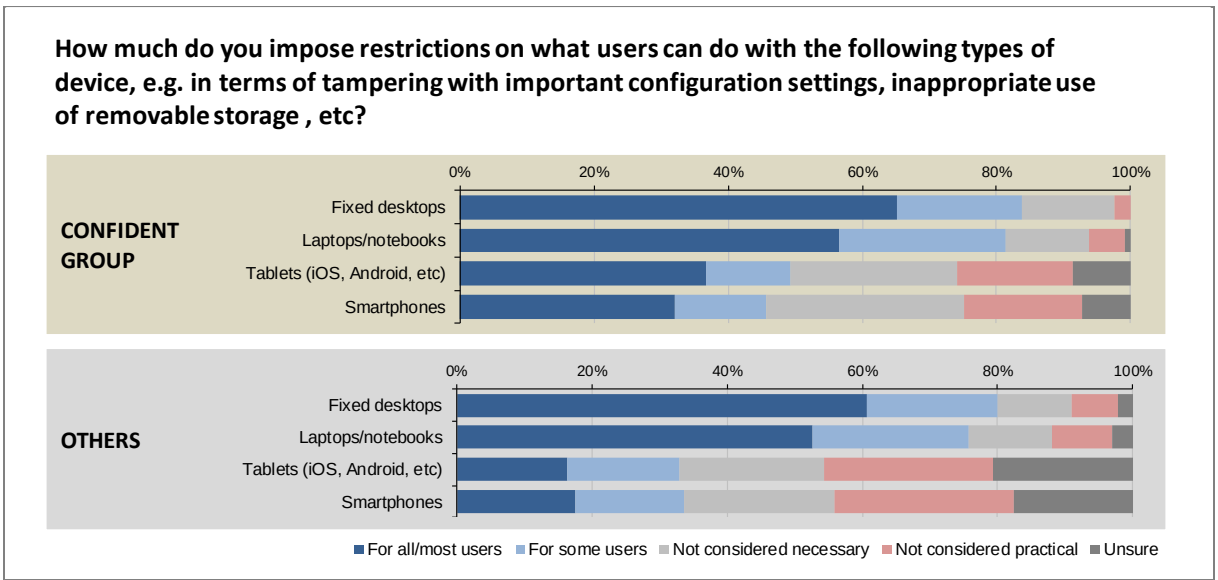


Figure 23 Control is good, but comments stress the need for balance to maintain user productivity and goodwill.

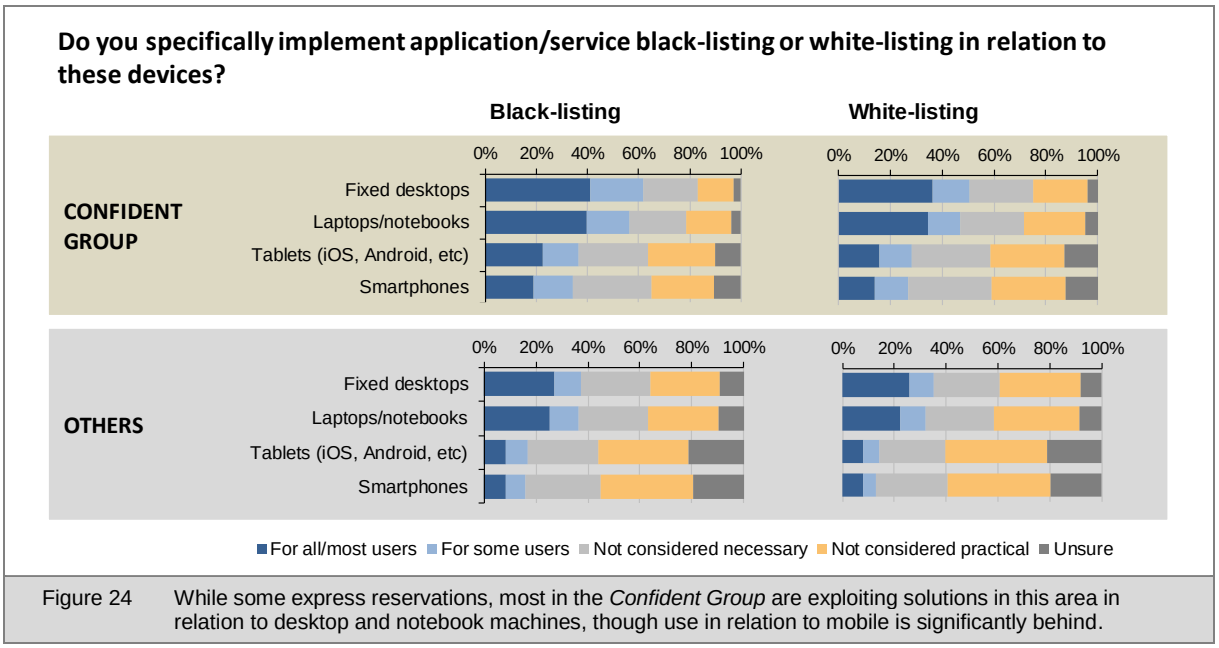


Figure 24 While some express reservations, most in the *Confident Group* are exploiting solutions in this area in relation to desktop and notebook machines, though use in relation to mobile is significantly behind.

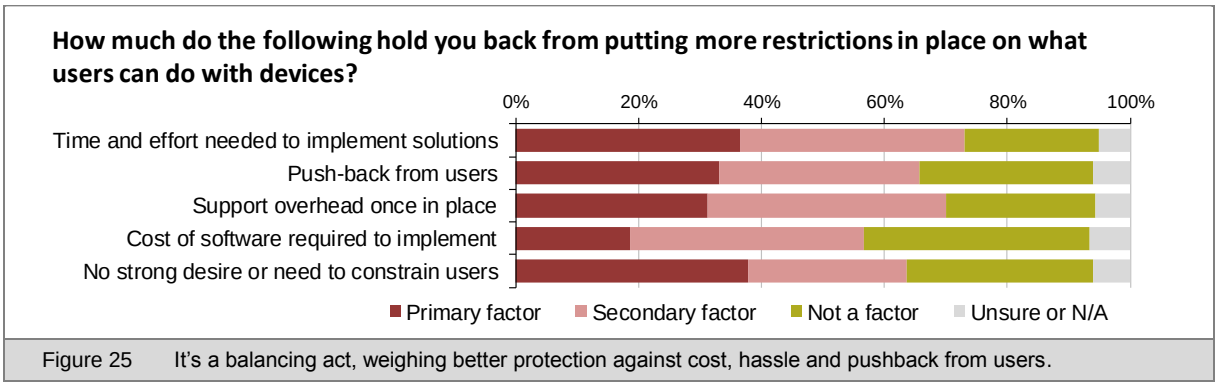


Figure 25 It's a balancing act, weighing better protection against cost, hassle and pushback from users.

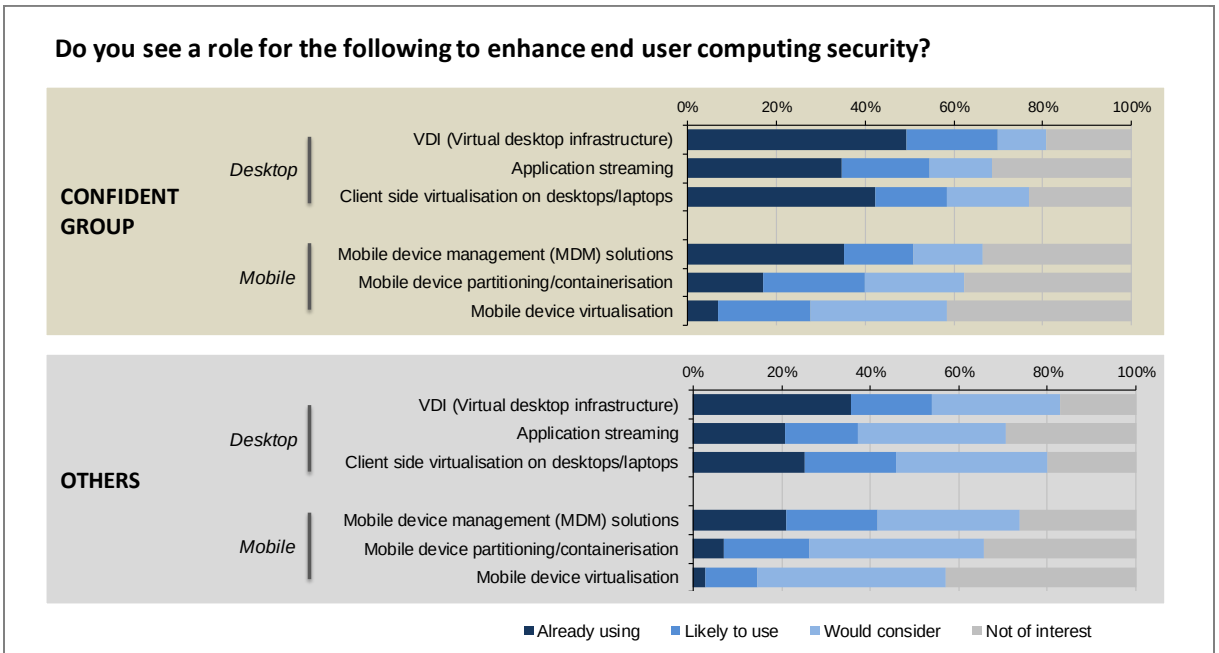


Figure 26 Those in the *Confident Group* are more likely to be exploiting a wide range of delivery and management options to enhance end user security.

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 McAfee

McAfee is the world's largest dedicated security technology company. Delivering proactive and proven solutions and services that help secure systems and networks around the world, McAfee protects consumers and businesses of all sizes from the latest malware and emerging online threats. Our solutions are designed to work together, integrating antimalware, antispyware, and antivirus software with security management features that deliver unsurpassed real-time visibility and analytics, reduce risk, ensure compliance, improve Internet security, and help businesses achieve operational efficiencies.

Backed by an award-winning research team, McAfee security technologies use a unique, predictive capability that is powered by McAfee Global Threat Intelligence — enabling home users and businesses to stay one step ahead of online threats.

McAfee's security products and solutions span the following areas:

- Data Protection
- Database Security
- Email & Web Security
- Endpoint Protection
- Mobile Security
- Network Security
- Risk & Compliance
- Security-as-a-Service (Security SaaS)
- Security Management
- Security Information and Event Management (SIEM)

For more information, please visit www.mcafee.com.

Terms of Use