

The IT profit centre

Delivering measurable value to the business through better IT management

May 2011

The day-to-day job of fixing recurring problems with all the network end-points that constitute a business's IT infrastructure, whether they are in the data centre, the office or out in the field, can make the lives of those in the IT department a repetitive grind. How can they get out of this break/fix cycle to the sunny uplands of creating new value for the users they serve?

The answer lies in having the management tools to automate repetitive tasks and preempt problems. However, the value of end-point management tools goes well beyond this. They also allow the value of IT services to be quantified and for this to be reported to lines-of-business. Wasteful usage of resources can also be identified and curtailed. In short, IT departments demonstrate that they are running profitably and justify new investments to provide incremental value.

For inspiration, IT managers can look to managed service providers who have to achieve this to make sure their own businesses are profitable. This report should be of interest to those who do not yet have effective end-point management or are seeking to improve existing practices. Many mid-market organisations with limited resources will be in this position.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: bob.tarzey@quocirca.com

Clive Longbottom
Quocirca Ltd
Tel: +44 188 9483360
Email: clive.longbottom@quocirca.com

The IT profit centre

Delivering measurable value to the business through better IT management

The day-to-day fixing of recurring problems with the end-points that constitute a business's IT infrastructure, in the data centre, the office and out in the field, can make the lives of those in the IT department a repetitive grind. How can they get out of this break/fix cycle to the sunny uplands of creating new value for the users they serve?

End-point is a generic term for the devices attached to a given IT Network

The rapid growth in the number of devices that constitute any given organisation's IT infrastructure means that many IT departments cannot answer the question '*what end-points are attached to my network at any given time and do I know what they are and who is using them?*' Putting in place the tools for effective end-point management can answer this question and provide the further insight needed to enable the provision of better services for the business and demonstrate that the IT department is a profit centre.

For MSPs this is an everyday challenge

Those that want to keep the management of IT in-house but are daunted by the prospect can look to managed service providers (MSPs) for inspiration. Many MSPs provide services for the management of IT assets both inside and outside of the data centre, providing a single view of all IT usage for each customer. Because they serve many customers from a single platform, MSPs show that the right tools can scale up to manage tens of thousands of end-points and provide granular reporting.

IT departments show they are a profit centre for the business

Successful MSPs must, by definition, ensure that they deliver such services at a profit. Businesses keeping IT management in-house can and should aspire to do the same. Having a pervasive view of end-points and their usage means that better consistency and reliability can be provided and that the service levels achieved can be demonstrated. The IT usage of each line-of-business can be measured and wasteful usage of IT resources can be reported.

End-point discovery is both an initial and on-going process

When pervasive end-point management is first implemented the initial priority is to discover all the end-points on a given network. For on-going management purposes this often involves the installation of a lightweight agent. The agent also makes it easy to quickly identify a device re-attaching to the network, as will often be the case with mobile end-points. End-point management tools must also be able to recognise completely new devices and decide if they should be allowed on to the network and with what level of security.

Management tools enable the automation of a wide range of tasks

There is a long list of tasks that need to be regularly carried out on all end-points. These include ensuring operating, application and security software is up to date; initiating data backups; enforcing usage policy (e.g. around USB devices); ensuring a consistent user experience across multiple devices; power management; and taking action if a device becomes compromised. Effective management must ensure that these tasks can be automated with end-points grouped by device type, job role, line of business etc.

A value proposition can be built to justify the investment required

The cost of procuring end-point management tools must be offset by three factors: cost reductions that are enabled elsewhere; the business and IT risk that is mitigated; and the incremental business and IT value that is created. Quantifying these three factors through a total value proposition allows a powerful business case to be made for the necessary investment to create an IT profit centre.

Conclusions

The imaginative use of IT can drive new value into existing business processes and help create new ones. To achieve this, IT departments need effective management tools. Businesses will only bear the on-going cost of IT if the value being provided is clearly identifiable and demonstrable. Management tools must provide insight at a granular level so that lines of business can see the IT services they are consuming and recognise the value they are receiving. When this has been achieved, the IT department can consider itself a profit centre.



Introduction – Earth’s tens of billions of computers

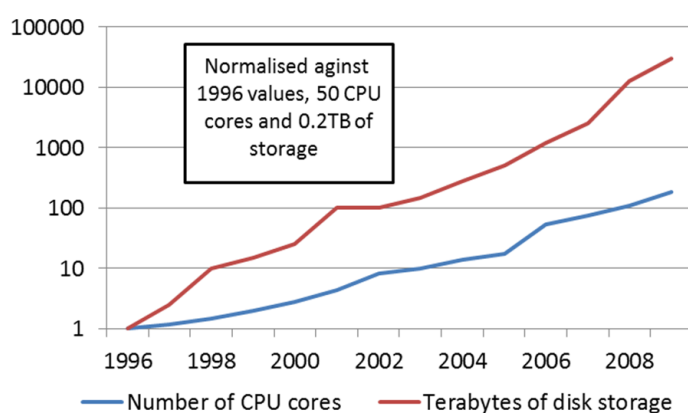
Ask yourself the question ‘*how many computers are there in the world?*’ and you soon find yourself asking another question ‘*what is a computer?*’ Gartner estimated¹ that in 2008 the number of PCs worldwide surpassed one billion and that it would reach two billion by 2014: that is just PCs, what about servers? Some estimates suggest that Google alone has over a million in its data centres; organisations like Rackspace, Akamai and Facebook have tens of thousands². As for mobile phones, are they computers? Apparently there are five billion³ of them, and an increasing proportion of them are looking more like computers than telephones. Then there are point-of-sale terminals (think of the growing number of self-service checkouts), lottery machines, ticket readers, cash-points, printers, network routers, security appliances etc. Given the diversity of all these devices, to avoid debate, many in the information technology (IT) industry use the generic term end-point, rather than computer, to indicate the fact that most are joined together with others on a network of some sort to share, access and process data in some way.

Even if you could race around the world counting all the individual physical end-points you would not have an answer to the original question. Virtualisation means that a physical server might actually be running multiple virtual servers, sometimes owned and managed by different organisations. This is also true of PCs; some users run multiple virtual workspaces on a single device. It is estimated (using a technique similar to that used by the allies in World War II to count German tanks⁴), that about 90,000 new virtual servers per day are currently being created on Amazon EC2, the largest infrastructure-as-a-service (IaaS) platform in the world. User desktops are increasingly being virtualised onto servers in the data centre too, through the use of virtual desktop infrastructure (VDI) software.

“Given the diversity of all these devices, to avoid debate, many in the IT industry use the generic term end-point, rather than computer”

Now ask yourself another question, ‘*how many end-points does the organisation I work for own?*’ It is perhaps more pragmatic to try and find an answer here, but still not straightforward. The growth of processing power and storage capacity in the data centre over the last 15 years has been phenomenal (Figure 1). Even so, you should be able to count the assets in your data centre (although for many that may mean travelling to the premises of one or more co-location providers – companies that many organisations rent data centre space from). You may also have local

Figure 1: Relative increase in CPU and storage since 1996, European Bioinformatics Institute⁵



servers in branches and departments, some parts of the business may be using third party services from hosted infrastructure providers to run some applications and you cannot see and count those so easily. However, the real headache is user end-points; you may know how many PCs and smartphones your organisation has procured over time, but that gives little insight into the actual number of them attaching to your network. Increasingly, the desire for flexible working means more and more employees are using their own devices for work-related activities – a trend dubbed *the consumerisation of IT*. So perhaps you have asked the wrong question: a better one would be ‘*what end-points are attached to my network at any given time and do I know what they are and who is using them?*’



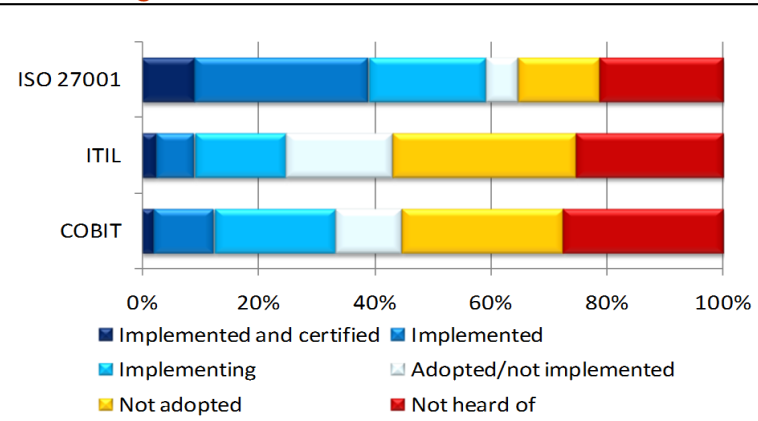
If you can answer that question and go one step further to actually control and manage those end-points, then you can answer some more fundamental questions. ‘What applications and information are end-points being used to access?’ ‘Is access secure and reliable?’ ‘Are appropriate service levels being delivered and can we prove it?’ ‘What departments are using which resources?’ ‘Are they aware of the value they are receiving?’ ‘Are some IT resources being use wastefully?’ ‘Is the use of data compliant with the growing number of regulations that govern my organisation?’ Being able to answer such questions is only possible with the right tools in place to understand and manage all end-points.

The IT profit centre

Management of data centre assets is something the majority of larger businesses will have addressed to a greater or lesser extent. Many do it for themselves, whilst some outsource the task to managed service providers (MSP). Smaller businesses may not have any real controls in place; at first a few servers and other devices in the racks of a co-location provider does not seem to warrant specialist tools to manage them but, as the business grows and its reliance on IT increases, more servers are deployed. Before long things are out of control – and that is just the data centre.

In an ideal world anyone starting a new business would plan their use of IT from the start, but things rarely happen that way. By the time it is realised a more measured approach to IT management is required, the end-points involved have already sprawled far and wide. However, it is possible to get things under control quite quickly. MSPs often do this for customers when they first take on a contract to manage IT infrastructure. In the past, many MSPs focussed on data centre assets but, increasingly, they are extending their services to cover all end-points, proving a single ‘pane of glass’ through which they can view all of a given customer’s assets. MSPs do this for many customers and demonstrate that tens or hundreds of thousands of end-points can be brought under control and managed using a single system, which allows separate reporting and billing for each customer.

Figure 2: Deployment of security standards and methodologies?⁶



End-point diversity

In the data centre

- Servers
- Storage
- Network equipment
- Security appliances

Beyond the data centre

- Branch office servers
- Branch office security and network appliances
- Printers, copiers and scanners – these store data as they produce output

User end-points

- PCs
- Tablets
- Smartphones
- Virtual desktops

Other remote devices

- PoS devices
- ATMs
- Video displays
- Ticket readers
- Lottery machines

“Things”

- Networks of “things” or machine-to-machine (M2M) communication means ever more unexpected devices are being attached to IT networks, from fridges to robots



Successful MSPs must, of course, make sure that their own costs are considerably less than the value of the invoices they send out. As a starting point for IT services management (ITSM), many deploy best practices such as laid down by ITIL (IT Infrastructure Library), a methodology which is yet to be adopted by most businesses (Figure 2).

A typical mid-market organisation that takes on the task of end-point management for itself faces a big challenge. There will likely be hundreds of users and end-points and just a handful of over-stretched IT staff, stuck in a daily break/fix cycle. The example of MSPs shows, however, that the job can be done and, furthermore, it is possible to demonstrate the value IT is providing – given the right tools, processes and standards, any IT department should be able to turn itself into a demonstrable profit centre.

MSP case study – Mirus IT Solutions

Mirus IT Solutions is a UK-based managed service provider. With less than 50 employees, it is a small business but, as an MSP, it manages IT infrastructure to support 7,000 users across 100 different customers. As Mirus's business grew, it struggled to keep up with everyday tasks such as patch management and data backup across the many locations involved. Mirus's problem was that it did not have the tools to automate these tasks, and ensuring they were completed was consuming most of its employees' time, preventing a focus on incremental value.

In 2008, when Mirus had just 2,000 users under management, it felt its plans for future growth were being severely constrained. It was at this stage that it implemented end-point management tools from Kaseya. Following the deployment, Mirus found it had far better visibility into its customers' use of IT, that is was able to automate everyday mundane tasks and growth rapidly resumed, without the need to take on lots of new staff. In fact, Mirus even reduced head count, whilst improving services for, and making more profit from, each customer.

Mirus does not charge for the individual end-points under management but levies a per-user charge agreed at the start of a contract. Of course, that per-user charge has to be understood in terms of supporting all aspects of each customer's IT infrastructure and the Mirus resources to achieve that. Only with the tools to measure this can Mirus ensure that it keeps the cost of supporting each customer as low as possible without compromising service levels and that every contract is a profitable one.

Managing the mundane

Some management tasks apply to all end-points; the first and most fundamental, when end-point management is first applied, is device discovery and classification. This is possible as all devices – real or virtual – have IP addresses. There must be an initial one-off discovery process that allows the management tools database to be populated; with many tools this also involves the installation of a lightweight management agent on each and every end-point.

However, discovery is also an on-going dynamic process that identifies devices attaching to the network. For a known end-point re-attaching to a network there may be management tasks to be carried out, due since it was last online. For previously unknown end-points, a decision needs to be made as to whether the device should be admitted to the network in the first place. The majority of end-points attaching to the network dynamically will be those used by mobile users requesting access from outside the office. These pose an additional problem in that they do not have fixed IP addresses. This means something must be known about the device itself so that it can

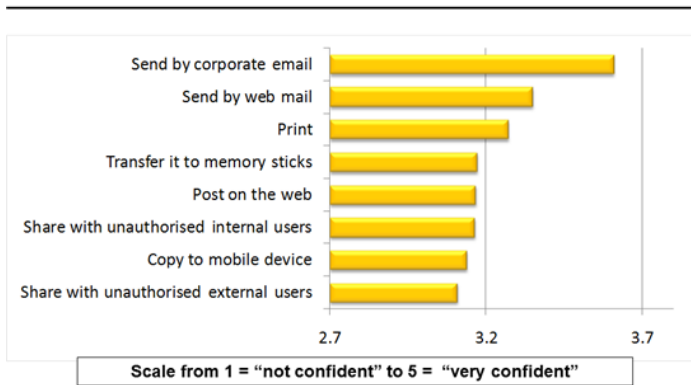
“The management of user end-points is becoming even more problematic with the growing diversity of form factors and operating systems in use”



be recognised whatever IP address it has been allocated. The easiest way to do this is via the previously installed agent. The management of user end-points is becoming even more problematic with the growing diversity of form factors and operating systems in use.

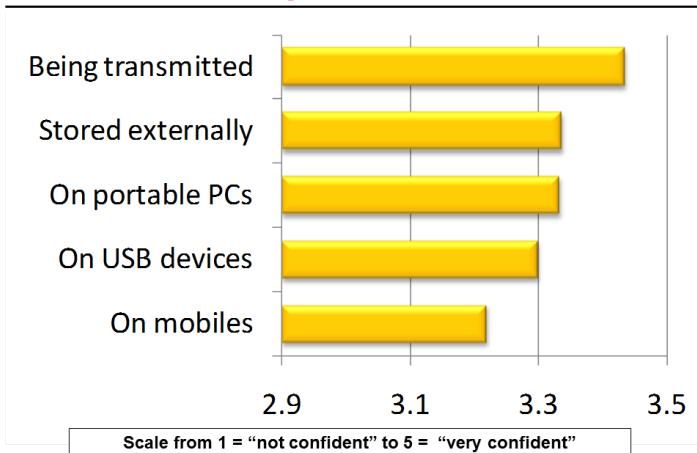
Identity is just one of an agent’s uses. As well as running local management tasks as and when required, if the device is lost or stolen the agent can ‘call home’ and, if GPS software is installed, it may even be able to report its whereabouts. It can also be used to enforce other policies about what users can and cannot do on their end-points; for example the use of USB devices (memory sticks, iPods etc.) can be restricted, which is an area where many IT managers lack confidence that they have control (Figure 3). The storage of certain types of data can also be blocked (e.g. preventing local email storage by blocking the creation of local Exchange PST files). Where it is policy, it can be checked that encryption is turned on. Furthermore, the agent can be used to gather information particular to a given user, for example web browser favourites or personal application settings and be able to migrate them to a new device when it is allocated to them.

Figure 3: When users have legitimate access to data how confident are you that you can control their ability to do the following?⁶



Whatever the device, it needs software installed to be useful. Software patches and updates need to be applied, sometimes urgently. Software licences need to be kept up to date too, ensuring all end-points are running current valid licences and that licences are not being over-used. This is a particular problem in virtual environments, where it is all too easy to invoke new virtual machines, which themselves invoke application and infrastructure software that needs to be licenced. This is a critical part of cost control that end-point management helps to achieve.

Figure 4: How confident are you that access to data is controlled at the following levels?⁶



Keeping software up to date ensures critical vulnerabilities that have been identified by the software vendors are patched, but this is not enough to keep end-points secure. How end-point security is managed will depend on the type of end-point and the security posture of the organisation concerned. For end-points that live permanently behind a firewall, security is less of an issue than it is for mobile end-points. With these, a decision must be made as to whether the end-point itself is kept independently secure or whether the user is forced back via a central resource before being able to access applications and data. The latter can be achieved in a number of ways, for example using network proxies, SSL VPNs, virtual desktops and so on, but this can be problematic depending on the network connection. Whatever the posture, security software and policies must be kept up to date.

Then there is protection of data – there are two aspects to this. First, the data stored on an end-point must be backed up on a regular basis, the management regime must ensure that this is carried out and that no devices are missed, whatever the chosen backup method. The only exception is likely to be personally owned devices where access to data may only be enabled via a central resource, i.e. no confidential data is allowed to be stored locally.

Second, there is the protection of data should a device fall in to the wrong hands. Most obviously this applies to mobile devices where the ability to remotely wipe data is an important feature provided by end-point management



tools. IT managers worry about their ability to protect data on mobile devices more than anywhere else (Figure 4). However, it also applies to an end-point at end of life (an investigation in 2010 found details of sex crimes, social security numbers and medical records on second-hand copiers purchased from a dealer⁷). Some IT security analysts argue that encryption is the only way to protect data in such circumstances, but if the cost of encrypting all data is considered too expensive then end-point management tools must be able to ensure the wiping of stored data when an end-point is disposed of.

There is also an issue of protecting data stored by third parties. What happens if you decide to move from one managed hosting or IaaS provider to another? Can you guarantee they will safely delete all your data? It should at least be in the provider's service level agreement (SLA) but, again, some argue that encryption is the only way to be sure; end-point tools need to ensure that, where it is the agreed policy, encryption is enforced, whether the end-point involved is located in-house or with a 3rd party.

A growing cost for businesses is the amount of power consumed by IT devices. Should this not be costed into the overall provision of IT? When this is the case it is in the interests of the IT department to reduce power usage as much as possible. Here end-point management tools can make a big difference, especially for office-based devices. Think of the difference it would make to a power bill if all the desktop PCs, monitors and printers in a call centre were turned off overnight. End-point management tools can automate this, shutting down devices that are not in use after a certain time and waking them up again in the morning before users arrive. Even on mobile devices, power management settings can be optimised to ensure they run efficiently. This improves user access as batteries stay charged for longer and it can also lengthen device life, reducing replacement costs.

"It is in the interests of the IT department to reduce power usage as much as possible"

Most of these management tasks need to be carried out on a regular basis across tens, hundreds or thousands of end-points (tens of thousands for MSPs). This is only possible if the tasks themselves can be automated and set to run against given group end-points. There must be flexibility in how tasks are grouped, based not only on the devices, but also the users. i.e. an urgent fix to Windows needs to be applied across all PCs running the version of Windows concerned but Apple Mac users can be ignored; a new policy for web access for remote users needs to be distributed, regardless of device types but maybe not to senior managers, who are exempt.

The ability to group assets themselves, associate them with users and group by usage is essential for a successful end-point management strategy. Being able to do this enables cost of IT delivery to be quantified and the value delivered to lines-of-business to be demonstrated. Only then can an IT department prove it is a profit centre.

Demonstrating the value of IT services

There are many aspects that need to be taken into account when adding up the cost of providing IT services. As discussed above, not least of these is power consumption. Add to this the cost of hardware and software assets depreciating over time, the cost of providing network access, the cost of data centre space, the cost of the IT staff and so on and you build up a picture of the overall cost of IT provision. Lines of business can then receive reports regarding their usage of IT and informed when this is wasteful. Cross charging is also a possibility, but then the pressure is really on IT departments. The availability of on-demand IT services makes it easy for line-of-business to take allocated budgets and spend it elsewhere.

How usage is measured varies depending on the service IT is providing. Equipping ten salespeople with notebook PCs or a call centre with fifty thin clients are discrete costs that can quite easily be added up but both the salespeople and the call centre staff may use the same shared applications, for example a customer relationship



management (CRM) system. Here the overall cost of providing that application needs to be understood and then the cost allocated on a pro-rata basis across the different lines of businesses that make use of it. It should also be incumbent on the IT department to let business managers know when they are being wasteful with IT resources. Such reporting can only be achieved if management tools can report on the use of IT by groups of users.

For the IT department to focus on its profitability it also needs an insight into how different groups of assets are performing. For example, is there a cost justification for replacing older servers that are using too much energy in return for limited processing power – would new servers do better and pay for themselves in the long term? If the IT department introduces a video conferencing service, who has been using it and what productivity gains have been achieved and have employee time/travel costs have been saved? This is not just the IT department showing that it is getting a return on investment for its own services, but also that it is making an overall contribution the businesses efficiency and environmental friendliness.

“For the IT department to focus on profits it also needs an insight into how different groups of assets are performing”



A total value proposition for end-point management

Deploying end-point management tools has a cost. This cost needs to be outweighed by the benefits to the IT departments in helping it achieve the goal of being a demonstrable profit centre. Quocirca uses a total value proposition model⁸ to quantify how the cost of a given IT investment is offset by reducing costs elsewhere, creating incremental value and reducing risk.

Considerations for building a total value proposition for an investment in end-point management tools

Cost of deployment of end-point management

- The cost of investing in end-point management tools and the infrastructure to run them (using tools provided as an on-demand service is becoming an option that some might like to consider)
- Cost of consultancy for deployment and use, training etc.

Costs saved or avoided by deployment of end-point management

- Increased end user productivity through increasing mean time between failure of end points
- Avoiding fines for regulatory breach through ensuring policies for data and end-point usage are in force (e.g. PCI DSS compliance)
- Identifying and curtailing the wasteful use of IT resources
- Ensuring employee productivity, especially that of staff working remotely, through ensuring better availability of user end-points

Value created through deployment of end-point management

- Enabling consumerisation, mobility, flexible working. These are all benefits many business will recognise but can only confidently achieve if they have the visibility into users and their end-points
- Freeing up expensive human resources in IT for more complex tasks and to focus on incremental value by automating the mundane day-to-day IT management tasks
- Being able to readily scale services and ensure that IT is not a brake on business growth through the inability to manage increasing volumes of end-points

Risk reduction through deployment of end-point management

- Making sure devices are, and remain, secure
- Ensuring data is not stored on/copied to insecure devices
- Ensuring, and being able to readily prove, compliance

Conclusions

In the 21st century IT is as critical to most businesses as other utilities but, unlike other utilities, the imaginative use of IT can drive new value into existing business processes and help create new ones. However, IT departments will only ever help to achieve this if they have effective management tools at their disposal and to automate the mundane tasks freeing up IT staff to focus on value added services.

Furthermore, businesses will only bear the on-going cost of IT if the value being provided is demonstrable. So the management tools put in place must provide that insight at a granular level, so that lines of business can see the IT services they are consuming and understand their value. When this has been achieved, the IT department can consider itself a true profit centre.



References

- 1 – Gartner – Gartner press release, June 23rd 2008, <http://www.gartner.com/it/page.jsp?id=703807>
- 2 – Data Centre Knowledge – May 2009 <http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the-most-web-servers/>
- 3 – Wikipedia http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use
- 4 – The Economist – Dec 29th 2010 print edition and online http://www.economist.com/node/17797794?story_id=17797794
- 5 – Figures published by SNS Europe, Volume 10 Issue 4, Summer 2010 – Interview with Head of IT at the European Bioinformatics Institute
- 6 – Quocirca, You sent what!, April 2010 – <http://www.quocirca.com/reports/475/you-sent-what>
- 7 – CBS News investigation, April 2010 <http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml>
- 8 – Quocirca's Total Value Proposition - <http://www.quocirca.com/services/tvp>



About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower everyone from individual consumers to large corporations and IT service providers to proactively manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform. Kaseya solutions are trusted by IT service providers and a wide variety of industries including: banking, consumer packaged goods, education, financial services, government, healthcare, military, real estate, retail and transportation. The company is privately held and based in Lausanne, Switzerland with 33 offices in 20 countries. To learn more, please visit <http://www.kaseya.co.uk>



REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations with regard to end-point management.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca would like to thank Kaseya for its sponsorship of the report and Metia for commissioning it.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium-sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at <http://www.quocirca.com>