

# The total MSP

---

*Why providers of IT services should embrace end point management*

**December 2010**

The management of IT assets now comprises two distinct areas; data centres and end points. Comprehensive management and protection of information can only be achieved when both are under control. Managed service providers (MSPs) have typically focussed on just data centres. It's time to change their thinking.

Introducing end point management services into an MSP's portfolio opens up three new opportunities. First it enables them to offer existing customers a more comprehensive service; second, it allows them to challenge competitors who are incumbent elsewhere but only offer data centre management; and third, such services can be used to open up the lucrative mid-market, which MSPs have found hard to penetrate in the past.

The variety and number of end points that provide users access to IT services is growing fast. MSPs that fail to put in place the tools and services to help customers and prospects address end point management will lose out to competitors that do. For MSPs, ensuring user satisfaction is a big part of achieving overall customer satisfaction.

Bob Tarzey  
Quocirca Ltd  
Tel : +44 7900 275517  
Email: [bob.tarzey@quocirca.com](mailto:bob.tarzey@quocirca.com)

Clive Longbottom  
Quocirca Ltd  
Tel: +44 118 9483360  
Email: [clive.longbottom@quocirca.com](mailto:clive.longbottom@quocirca.com)



*An independent report by Quocirca Ltd.*

[www.quocirca.com](http://www.quocirca.com)

Commissioned by Kaseya

quocirca

# The total MSP

---

## *Why providers of IT services should embrace end point management*

*Effective end point management is one of the most pressing problems faced by both enterprise and mid-market businesses. Providers of IT services need to have the capability to address this fast-growing opportunity.*

- **There are now two distinct IT management disciplines**  
The storage and use of information, and therefore the need to manage it, is moving away from traditional business premises in two directions; to centralised data centres and to a chaotic array of end-user devices. This means there are now two distinct areas of IT management, over which must be layered comprehensive information management and protection.
- **Both data centre and end point management must be in place to ensure business continuity**  
Discussions around business continuity often focus on making sure centralised applications are up and running and that data centre assets are all fully redundant. However, as this report shows, the most common reason that a user cannot do their job is due to a lack of IT access because of a problem with access to the application from an end point.
- **Access to IT is required by a wide range of users with many different device types**  
End point management is not just about Windows PCs and executive smartphones. It is also about point-of-sale devices, ATMs, ticket readers, video displays and so on that customers are increasingly reliant on to interact with the businesses whose services they use.
- **To manage end points you need to know they exist**  
The first stage in getting end point management under control is to discover what exists. Once an end point is known, verified and accepted, the “handshake” it makes with the corporate network can be via the installation of a lightweight management agent. Such an agent can also add, in a complimentary manner, to overall IT security.
- **Automated management of end points**  
The presence of a management agent provides a way in for the complete control of a given device. With the right tools in place, management tasks can be automated across groups of devices. Grouping allows MSPs to achieve economies of scale across multiple customers.
- **The benefits of good end point management are wide reaching**  
It is not just about business continuity. Having the right tools in place helps ensure that information is used securely and compliantly across the whole IT estate, that end point software is licenced legally and cost effectively and that power management is efficient, saving on energy costs and providing a feed for sustainability reporting.
- **Scalability allows MSPs to open up new markets**  
In the past, many MSPs have only focussed on providing services to manage the core assets of enterprises. The introduction of end point management services allows them to offer a more comprehensive service to existing customers, challenge competitors incumbent elsewhere with data centre asset management and to target the lucrative mid-market.

### Conclusions

Good end point management is now a fundamental requirement of ensuring IT availability, data security and business continuity. Businesses of all sizes need help to achieve this. MSPs with the right tools and services in place will be well positioned to strengthen existing customer relationships and grow market share.

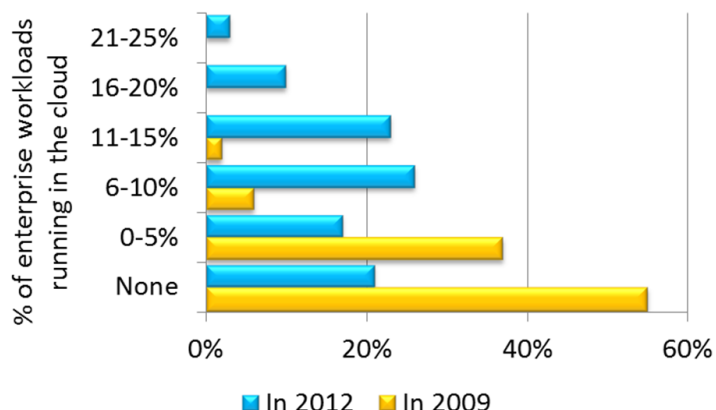
## 1. Introduction: end point management – challenge and opportunity

Data is migrating away from the office-based servers, storage systems and PCs that used to be the mainstay of much of corporate IT in two directions. The centralised storage and processing of data is moving to data centres, sometimes owned by the enterprise but increasingly owned and managed by third parties. The usage of data is moving to plethora of evermore powerful and mobile end points.

For those tasked with the management and availability of IT, the move into large data centres should make these tasks easier, whilst the increasing numbers of end points presents potential chaos and turns them back into a challenge. This means IT asset management itself has turned into two separate disciplines; data centre asset management and end point management. Only when both are under control can comprehensive data security and management be put in place.

For help with IT management most large enterprises turn to managed service providers (MSPs), at least in part, but this branching of IT has meant the dominance of MSPs is being challenged. The migration towards the use of third party data centres is often happening by stealth through the take up of cloud-based hosted services (Figure 1). When this happens at the application level (software as a service/SaaS) there is little left for the MSP to do. Even with lower level hosted services (infrastructure as a service/IaaS and platform as a service/PaaS), traditional MSP roles such as break-fix contracts for hardware are lost, even if some software infrastructure or application management remains.

**Figure 1: Growth in use of cloud – source Nov 2009, Goldman Sachs IT Spending Survey<sup>1</sup>**



Furthermore, the governance of how data is managed and used is one of the most important tasks IT managers are charged with. The movement of data into data centres, often owned by third parties, is one worry, but the ability to store huge amounts of data on end points now means that they are one of the biggest headaches for IT managers when it comes to the secure and compliant use of data, and good end point management is key to achieving this.

This paper aims to explain how MSPs can rise to this challenge by introducing new services based around end point management. As the market for the management of central IT resources is being challenged by the providers of hosted services, the growth in the number and diversity of end points has been so fast that many MSPs have yet to develop the services their traditional customers and prospects now need in this area. They need to do so, and fast, or they will leave open the opportunity for new market entrants, who do have end-point management services, to encroach on their territory.

*“By introducing end point management services, MSPs can open up new opportunities”*

In fact, by introducing end point management services, MSPs can open up new opportunities; such services developed for their enterprise customers can easily be scaled down for the mid-market. Here the diversity and number of organisations that are now as reliant on IT, as enterprises are, is huge. MSPs have largely ignored the mid-market in the past because its usage of IT was different; central IT resources were on too small a scale to

be attractive or already outsourced through the use of hosted services, but when it comes to end point management the needs of the mid-market are the same as enterprises, it is just the scale and complexity of operation is different.

## 2. What is an MSP?

The term service provider is widely used in the IT industry. Used alone, many take the term to mean a telephony service provider on the communications side of the market. This paper also talks about providers of managed hosting services; they too are a type of service provider. Many smaller companies consider their chosen value added reseller (VAR) as their main provider of IT services, although often this is just a reactive *break-fix* type of service rather than proactive support of all IT assets.

The term MSP generally has a specific meaning when used in an IT context and the definition offered by Wikipedia serves well; “*a managed services provider (MSP), is typically an information technology (IT) services provider, who manages and assumes responsibility for providing a defined set of services to their clients either proactively, or as they (not the client), determine that the services are needed*”.

Quocirca would add to this that MSPs should provide their customers with a service level agreement (SLA) that covers all aspects of IT under management. This paper also contends that a *total MSP* should offer such service for the management of, and access to, information across all a customer’s IT assets, including those in the data centre and end points. Only through doing so can an MSP ensure user satisfaction, which is a big part of achieving customer satisfaction.

So, when using the term MSP in this paper Quocirca is only referring to those that offer comprehensive IT management services or can reasonably aspire to do so.

## 3. IT and business continuity

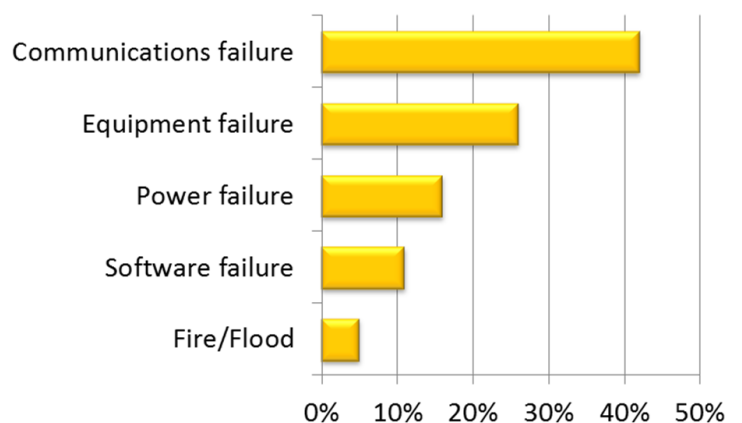
One of the most critical aspects of business continuity is the availability of IT. Sure, flood, fire or plague may mean the wholesale relocation of staff to temporary premises that specialist disaster recovery providers keep on stand-by. However, emergency premises are of little use for the day-to-day running of most businesses if IT is unavailable. Although it should be pointed out that any business should consider the extreme case of long term power failure, a well provisioned data centre can be kept going for some time; end-points and networks are more problematic.

The need to ensure IT availability has driven take-up of the use of hosted services for two reasons. First, it ensures that IT assets are not in the same buildings as human assets so both are not hit by the same disaster at the same time. Second, the providers of hosted services offer service level agreements around availability, redundancy and so on that internal IT teams struggle to match, especially in the mid-market.

Even for those businesses that maintain the majority of data centre assets in house, the necessity of ensuring the high availability of central IT resources is understood and has been a focus of much effort over the last decade or so. Any business that lives in constant fear that its business critical applications will fail has been negligent compared to others.

However, all this is to no avail if the user cannot access the application from whatever device they happen to have or that device is not configured as it should be to enable the user to do their job.

**Figure 2: Reasons for central application failure – source Plan B Disaster Recovery<sup>2</sup>**

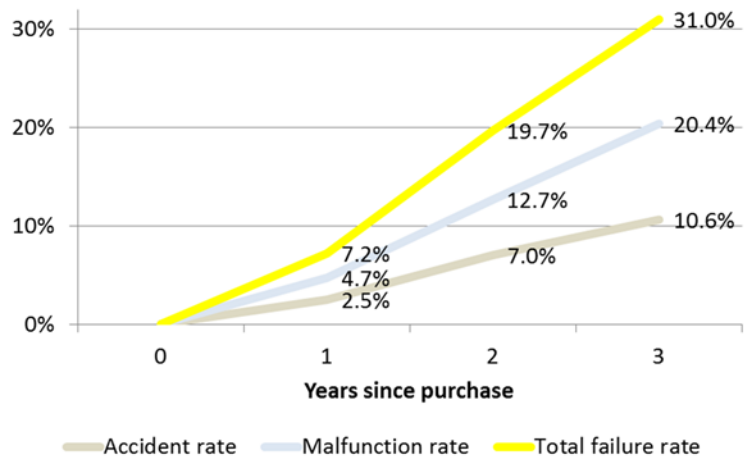


The failure of end points is much more common than that of centralised applications. Plan B, the disaster recovery provider, says the average failure rate for centralised applications amongst its customers is 1.2 per year. However, over 40% of these are down to a communications failure of some sort (Figure 2), rather than the actual data centre infrastructure.

Figures from SquareTrade (Figure 3), show that the failure rate for certain end user devices can be over 30%. That can mean tens, hundreds or thousands of individual IT outages a year depending on the size of an organisation. The overwhelming majority of productivity lost through IT failure is down to the end points being unable to access the applications that the user needs to perform their task, not the failure of the applications themselves. Some of that may be due to the occasional communications problems at the data centre end but more often than not it will be a problem with the end point itself, the end point network connection or the user of the end point.

The term “user” should be taken very broadly. As Quocirca has said in the past; *We are all IT users now*<sup>4</sup>. For many businesses, users are not just employees sitting in call centres tapping away at customer relationship management (CRM) systems or road warriors with smartphones; users are also passengers viewing video displays at stations, bank customers using ATMs and shoppers at the checkout. All users have one thing in common, to access the application they need a functional and reliable end point.

**Figure 3: Three year laptop failure rate, source SquareTrade Laptop and Netbook Reliability Report Nov 2009<sup>3</sup>**



#### 4. End points for all

The growth in the number and type of end points has created a new challenge for IT management and also created the need for a whole new aspect of managed service provision. Of course, end points have been part of the IT landscape since computers became essential to businesses, first as terminals accessing mainframes and mid-range computers and then as PCs in the client-server world.

Even though PCs complicated IT management, until about a decade ago it was still fairly uniform: a Windows PC, usually in a fixed desktop location, with a just handful of mobile users being given laptops. There are a number of trends, both in the IT industry itself and in working practices, which have led to the end point management challenge that exists today:

- Mobile workers, enabled by mobile PC and smartphones, can be, and are increasingly expected to be, online
- Home working is becoming more accepted, enabled either by the provision of mobile PCs or through the safe enablement of an employee’s home PC
- Consumerisation: the desire for users to want to use their own devices rather than those prescribed by their employer
- Integration and automation of business processes that link in customers and partners via remote end points
- The huge increase in the storage capacity of end user devices and the potential ability to copy huge amounts of sensitive data on to them
- The increase in availability of high capacity expendable storage devices such as USB thumb drives

The problem with this is that it means that the variety of end point assets that need managing is ever growing. These are not only the devices used by users but also those that enable and secure the network that provides access from those devices to central IT resources. These include:

Employee access devices	Customer access devices	Other devices
<ul style="list-style-type: none"> <li>• Desktop PCs</li> <li>• Mobile PCs</li> <li>• Thin client devices</li> <li>• Smartphones</li> <li>• POS devices</li> <li>• Public devices such as PCs in airport lounges and internet cafes</li> <li>• Shop floor devices; hardened PDAs, controller screens etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Video displays</li> <li>• Ticket machines</li> <li>• ATMs</li> <li>• RFID readers</li> <li>• PCs</li> <li>• Smartphones</li> </ul>	<ul style="list-style-type: none"> <li>• Printers and copiers; most have hard disk storage and memory these days</li> <li>• Network routers; often these have local caches to improve local performance</li> <li>• Branch office servers</li> <li>• Appliances; e.g. network security devices</li> </ul>

All these devices need managing, not just to ensure continual access to IT for all users, but also because each and every one of them is a potential security threat, either because they can be used to store sensitive data or they provide access to private networks and servers.

They all have software installed on them that needs to be kept secure and up to date. Furthermore, as the number of end points continues to increase it becomes more and more of a challenge to ensure that software licencing is compliant with vendor requirements and the purchase and use of licences is cost effective. Even in the mid-market, a long term Microsoft stronghold, the number of software vendors that need to be dealt with is increasing fast; Microsoft Windows may still dominate on PCs but with smartphones it is a different story.

Add all the different end point asset types together and take in to account the various software environments and there is potentially a lot of variety to manage. Where does an organisation, needing to get its end point management under control, start?

### 5. End point discovery and understanding

The first step towards getting the situation under control is to know what needs managing. Most end points are of little use and a limited security concern if they are not at some point attached to the corporate network. To do so they need an IP address: active IP addresses on a given network can be scanned for and a picture built of the number of devices attached to a network at any given time. Devices that are permanently attached to the network will generally be assigned a permanent IP address and they become a recognised pair. This includes desktop PCs, routers, printers and so on, although it must be recognised that even these devices do get moved on occasions.

Portable devices are generally assigned IP addresses automatically, depending on where they are getting access from. So an employee working in a hot-desking environment will attach to the network via a nearby wireless router and be assigned a spare IP address by the router or other DHCP server. The IP address will be one assigned to and understood by the business in question. However, when an employee requests access via a wireless router in their local Starbucks, the IP address will probably be new and unknown.

Whilst it is possible to get intelligence on IP addresses from specialist geolocation providers, there will likely be occasions when the provenance of an IP address pertaining to a given device requesting access is uncertain. IP addresses are essential for access and useful for discovery, but for the on-going management of end points it is necessary to be able to instantly recognise a given device as *one of ours*.

It is possible to recognise devices by looking for certain hardware characteristics such as MAC addresses (which are not suitable for use in isolation as they can be spoofed). However, it makes sense to have a universal way of instantly recognising any device. The best way to do this is to install a common software agent on all devices. This not only provides a handshake for network access control but also provides the way in to the device required for management.

So, discover devices via their IP addresses and verify them as known corporate assets or accepted end user access devices and install an agent. Henceforth a device can be instantly recognised wherever it pops up. Any agent installed on an end point for management purposes needs to be lightweight and minimally intrusive. It must also be impossible for a third party of some sort to spoof the agent, in other words, a unique agent *footprint* needs to be created that can only be recognised and used by a given management tool and will uniquely identify the device in question.

From a security perspective, this just means the device is known. Questions may need asking in certain circumstances. If a branch server previously located in Kettering is suddenly requesting access via an IP address in Kiev it has probably been stolen. However, if a notebook PC assigned to the channel manager for Eastern Europe is requesting access via the same IP address all is probably OK. Of course recognising the device is an addition to, and not a replacement for, the normal security process; user verification still needs to happen.

## 6. Management and automation

Enhanced security is a side benefit of getting end points under control. The main driver for doing so is better management. In a 2008 report, *Average Inc*<sup>5</sup>, Quocirca used existing research to attempt to define what the average company looked like in terms of its use of IT.

Average Inc has 1,500 employees, putting it on the boundary of the upper mid-market enterprise type company. 65% of employees are IT users with 20% having laptops and 10% using smartphones (the latter number has almost certainly increased since the report was written). It has 9 branch offices, some with local servers, and some without; all need local networking equipment. It has a jumble of printers and copiers with little standardisation. The point is that these days almost any organisation is likely to have more, often substantially more, end points than employees.

Once the portfolio of assets owned by a given organisation is understood and a management agent is installed on each, the process of automating management of end points can begin. To achieve this, it is necessary to create a number of overlapping groups of assets. Some of these are obvious, such as Epson printers, PCs running Windows XP or users of SAP. Other groupings that are less obvious can be just as useful, for example recognising high priority users though grouping by service level.

For an MSP, economies of scale can be achieved through grouping assets together across multiple organisations. A small mid-market company may have only one Xerox copier, but there may be 20 spread across a number of customers that an MSP can group together for management purposes.

*“For an MSP,  
economies of scale  
can be achieved  
through grouping  
assets together  
across multiple*

There should be no security issues with cross-organisational grouping. From a management point of view, applying a critical patch to tens of thousands of PCs running Windows 7 across many organisations is quite feasible with the right tools and is no different to Microsoft’s own Windows update service used by millions of consumers and small businesses. A security issue would only arise if one customer were able to see details of another customer’s assets, so it is essential that any management tool used for managing multiple customers is able to keep such data separate whilst providing an open interface for each customer to access their own data for reporting purposes.

In fact, providing access to anonymised data about end points across many organisations is of value to both the MSP and its customers. As well as providing insights for the MSP to plan ahead, it can enable the MSP's customers to benchmark themselves against others – without the full details of the “others” being visible. Questions such as the following can be addressed;

- *What is the ratio of desktop to laptop computers?*
- *What percentages of PCs are now running Windows 7?*
- *What is the most commonly use branch network router?*
- *How do we compare in wireless-WAN data usage against others?*

These sorts of tools provide the scope and flexibility required for end point management and need to be usable by an MSP alongside their traditional systems management tools that are more focussed on data centre assets.

There are a number of other benefits that MSPs can provide for customers with good end point management tools in place:

- Deliver a consistent and automated approach to undertaking routine maintenance to ensure end point devices stay available.
- Provide proactive management to increase reliability using a systematic approach that ensures visibility of all actions taken can be provided to customers.
- Automate the provisioning and setup of new end point devices to corporate standards.
- Management by exception: the ability to proactively recognise a problem has arisen or will arise soon and fix the issue via an automated process or trigger a process to replace the end point.
- The ability to disable or wipe data from lost or stolen devices to ensure data does not fall into the hands of third parties.
- The ability to police the way data is used and managed on devices; for example ensuring encryption is in place on hard drives.
- Ensuring controls are in place about the way devices can be used; for example limiting the use of USB devices or enforcing acceptable use of applications or network connections.
- Power management: remote access to end points means their power management settings can be changed and devices can be switched on and off at will and en mass. For example, all printers powered down overnight and powered up again before staff arrive in the morning can save money and provides a feed for sustainability reporting.
- Software licence management: having an exact understanding of the number of licences in use for a given product allows for better negotiations with vendors and allows the elimination of unused software licences. Conversely it also helps ensure that there is no unlicensed software in place.
- A consumer's own device can be brought under management if it is deemed necessary to install certain corporate software assets on it, for example VPN drivers and desk top virtualisation software.

## 7. The MSP opportunity

So how do MSPs that have previously focussed on the management of centralised IT assets branch out into end point management? And if they do, what opportunities does it open up? There are three key types of individual within an MSP that need be considered.

1. Technologists tasked with providing services: typically they will be used to managing smaller numbers of centralised assets. Whilst the move to high density rack and blade computing in data centres will have given them a taste of the problem of carrying out repetitive management tasks across multiple asset types, the scale of the problem they will encounter with end point management, especially when it comes to variety, is an order of magnitude worse. They need tools that allow them to pro-actively carry out a task multiple times across similar end points, taking into account that not all of them will always be available when a given task is initiated.

2. Sales and marketing staff that are tasked with finding new opportunities: they need new services to sell to existing customers and ones that will allow them to open up new accounts and break into new markets. Having an end point management service will certainly allow them to approach existing customers with an offer to upgrade to a more comprehensive service. It also enables them to break into their competitors' accounts where currently only data centre asset management is being provided. Because end point management services can be scaled down, they will also be able to target the lucrative mid-market, which is served well by managed hosting companies for elements of central IT infrastructure provision and management, but usually with nothing in place for end point management and comprehensive data management and protection.
3. Senior managers: many senior MSP managers will be concerned about how they expand their business or even maintain revenues at current levels. They should be providing the investment needed that will provide their sales and marketing teams with new services to go out and sell and their technology delivery teams with superior technology that will help ensure the success of these new services.

*There is a bright future out there for MSPs, providing they are ready to adapt.*

There is a bright future out there for MSPs, providing they are ready to adapt.

## 8. Conclusions and Recommendations

The world is not about to start using less IT, but the task of managing it is changing. Ensuring availability of both the assets that enable central applications and the end points that provide access to them is essential for business continuity. It is also essential to be able to address both data centre and end point asset management together to ensure comprehensive data security. Any MSP that is only offering central IT management services is living in the past and will lose out in the long term. End point management is an essential part of overall IT management that MSPs should embrace to ensure the on-going success of their own business and that of their customers.

## 9. References

1. Goldman Sachs Global Investment Research; A paradigm shift for IT: The Cloud – November 2009
2. Plan B Disaster Recovery – via email
3. Square Trade – 1 in 3 Laptops fail over 3 years – <http://www.squaretrade.com/pages/laptop-reliability-1109/>
4. Quocirca – We are all IT users now – <http://www.quocirca.com/reports/57/we-are-all-it-users-now>
5. Quocirca – Average Inc – <http://www.quocirca.com/reports/139/average-inc>

## About Kaseya

It may seem a bit odd, almost contradictory, for Kaseya to feature an About Us section when everything we do is really about you, not us in the least. Granted, without our IT automation software, your success might not be quite so certain or come so easily, but Kaseya can only take part of the credit.

By being a visionary and leveraging the prodigious power of our software, it's really you who's the hero. We simply provide a revolutionary means to the end. Using Kaseya software to automatically monitor, manage and maintain IT infrastructures anywhere in the world, IT managers and service providers have never looked so smart. What's even more impressive is that you can perform all of these tasks — and so many more — remotely and securely, from one computer through the Internet.

Wow, is right. Kaseya software liberates you to become more productive, less burdened, and immensely more profitable. Kaseya is all about helping you, which pleases us tremendously.



#### REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

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 this report.

## 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 advise 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>