

Contacts:

Quocirca Ltd
Tel +44 118 948 3360
inquiries@quocirca.com

Content Security Securing Internet Communications

Executive Summary

Purchases of information security protection have traditionally been seen as tactical, against such historical threats as Viruses, Worms and Trojans, and more recently Spyware and Spam – categories of software that can be grouped together under the heading of malicious content. As these threats evolve however, tactical procurements are failing to give companies the comprehensive protection they need, and in the meantime the threats are evolving to take into account the widening range of Internet-based communications mechanisms.

This report summarises the business impacts of breaches in security caused by malicious content, for example in terms of data confidentiality and loss of service, and considers how today's threats differ from their historical counterparts. This is largely due to a blurring of the edges – each potential security exploit may be due to a combination of techniques, exploiting system vulnerabilities, network holes and even human nature.

Just as there is no clear definition of the “problem”, so the “solution” can be difficult to define. This paper explains why the only suitable security protection against Internet-based threats is one which provides a comprehensive coverage of known issues, and which is flexible enough to meet current and future needs. By understanding both the risks and the impacts, we can define what we need to see in any integrated solution.

As well as implementing technological solutions, there is plenty a company can do to minimise the risks of its IT systems being compromised. Technology can only be a part of the answer. This report considers what steps organisations can take to minimise Internet-based security risks. All organisations are different but some example guidelines are given here, not least to demonstrate that technology is only one piece of the puzzle.

REPORT NOTE:

This report has been written independently by Quocirca Ltd to address certain issues found in today's organisations. 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.



*An independent report by
Quocirca Ltd.*
www.quocirca.com
Commissioned by
Aladdin Knowledge Systems



1 Contents

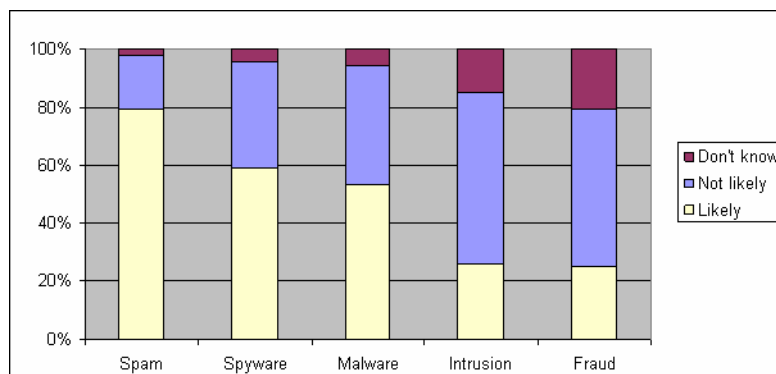
| | | |
|-----|--|----|
| 1 | Contents..... | 2 |
| 2 | Introduction | 3 |
| 3 | A Brief History of Malicious Content | 4 |
| 3.1 | Viruses..... | 4 |
| 3.2 | Worms | 5 |
| 3.3 | Trojans..... | 5 |
| 3.4 | Adware and Spyware | 5 |
| 4 | Internet Threats – the Next Generation | 6 |
| 5 | New Threats, New Protection | 7 |
| 5.1 | Covering the Threat..... | 8 |
| 5.2 | Delivering the Service..... | 8 |
| 5.3 | Assuring Operational Aspects | 9 |
| 6 | Assuring Business Protection | 9 |
| 7 | Conclusion | 10 |
| | About Aladdin Knowledge Systems Ltd..... | 11 |
| | About Quocirca | 12 |

2 Introduction

“No, Mr Sullivan, we can’t stop it! There’s never been a worm with that tough a head or that long a tail! It’s building itself, don’t you understand? Already it’s passed a billion bits and it’s still growing. It’s the exact inverse of a phage – whatever takes it in, it adds to itself instead of wiping ... Yes, sir! I’m quite aware that a worm of that type is theoretically impossible! But the fact stands, he’s done it, and now it’s so goddamn comprehensive that it can’t be killed. Not short of demolishing the net!”

(John Brunner, “Shockwave Rider”, 1975)

Thirty years on from John Brunner’s ground-breaking novel, the security of today’s computer systems is as big an issue as it ever was. According to a Quocirca research study conducted at the start of 2005, 20% of the 3,000 respondents had seen some kind of system failure caused by Spyware or other malicious software (Malware), and over half expected to be subjected to an attack in the future (see chart). Gone are the days when virus attacks used to happen to somebody else, and when Internet worms were the stuff of hearsay and anecdote. Every day it seems, new forms of attack are developed that traditional models of protection cannot properly deal with.



For not-for-profit agencies just as much as commercial businesses, while these threats can impact in a number of ways, all lead ultimately to a financial cost:

- Availability and access.** An IT system, a computer desktop or a Web site can be rendered unavailable. Each case is frustrating for the user, and may result in a direct financial impact if a sales transaction cannot be completed, for example. In each case, access can either be directly prevented or a system slowed to the point that it is no longer usable.
- Efficiency and productivity.** Even if an IT system is still accessible, it may be running at a sub-optimal level. Wait times and failed responses can slow a user’s activities, rendering a staff member less efficient or making a customer wait unnecessarily. Within the machine, transaction times can be slowed – and as we’ve already noted, transaction times often mean money.
- Data confidentiality.** The information an organisation wants to keep private can go beyond salaries and credit card numbers; there are documented cases of attempts to access hospital records of celebrities with an aim to sell the information to the press. Some email viruses work by sending a random local file to a randomly selected set of addresses from a local address book: it is too easy to imagine how some confidential data might be circulated in this way.

- **Data integrity.** If data can be viewed in transit, it could also be changed. This could be damaging to a business in a number of ways, for example, a contractual document could be modified or 'lost', or a bank account balance could be changed. If a document is sent without the sender's knowledge, it can be difficult to prove that it was the result of a virus rather than a user: the technical term is "non-repudiation" but it boils down to being able to verify the sender's identity.

Even if malicious content has no immediately damaging effect, it still has the potential to do so. Such content can be seen as a back door into the corporate network, and just because it has not been accessed yet that does not mean that it will not be in the future. So, what kinds of malicious content are there? Let's take a look.

Did you know?

An official survey conducted in 2003 by the UK's Department of Trade and Industry showed that 68% of large businesses had suffered from a virus attack, even though 99% had some form of virus protection in place.

3 A Brief History of Malicious Content

*The fatal day, th' appointed hour, is come,
When wrathful Jove's irrevocable doom
Transfers the Trojan state to Grecian hands.
The fire consumes the town, the foe commands;
And armed hosts, an unexpected force,
Break from the bowels of the fatal horse.*

(The Aeneid Book II, Virgil)

The Trojan Horse is as old as Socrates, if not older. Just as we can learn from wisdom of the Greek philosophers, there is value from understanding the traditional types of malicious content.

3.1 Viruses

According to the original definition in the Internet report RFC 1135, "A virus is a piece of code that inserts itself into a host, including operating systems, to propagate. It cannot run independently. It requires that its host program be run to activate it." The mechanism for getting an "infected" program from one computer to another was often the human being who would (inadvertently) transfer the program using a floppy disk.

Gotta start somewhere

The first documented computer virus was known as "Elk Cloner" and was written by Rich Skrenta, when he was in ninth grade, that's 13 years old. It ran on Apple II computers, and displayed a poem.

The virus has evolved considerably since those lowly days. With the arrival of email, writers found that the viruses did not have to hide themselves inside legitimate executables – a viral program could be given some innocuous name, purporting for example to be a screen saver or game, and generally the foolishness of the user could be relied upon to open it (this still remains true, as illustrated by last year's Kournikova virus). As such, viruses have grown just as fast as the proliferation of email, if not faster as the opportunity to read and exploit a user's email address book has been exploited.

3.2 Worms

Worms have one of the longest histories of all malicious content: they were wreaking their damage on UNIX networks before networked Windows was even a twinkle in Bill Gates' eye. The worm released on 2 November 1988, which exploited holes in the Sendmail, Finger and Rsh programs, remains one of the largest proportionate security breaches the Internet has ever suffered; fortunately, the Net was not in such wide use back then.

A worm could be described as a network-savvy virus, and indeed most of today's "viruses" are in fact worms. Its purpose is to discover and exploit weaknesses in a network, primarily so that it can propagate itself. Usually this involves discovering poorly configured and secured computers, firewalls and routers: given the Internet, this can be quite a few! A worm may include some viral content (known as its "payload") but this is not always the case. The more "successful" worms of recent times have often achieved this success by looking for security holes in the Microsoft Windows environment, but history suggests non-Microsoft environments are equally at risk.

It's a Blast

By April 2004 the Blaster worm was estimated to have hit over 8 million computers worldwide. It has been noted as a contributory factor in the August 2003 power outage that hit the North East of the USA and Canada, called "the largest power outage in history". A Minnesota teenager who modified the original MSBlast code and unleashed the result is now serving an 18 month prison sentence.

3.3 Trojans

Trojan programs run in the background of the computer, usually without a user's knowledge. Historically, they became prevalent in the mid 1980's, shared through bulletin board systems by masquerading as popular software (such as PC-Write, a word processor). When run, Trojans could be quite damaging – deleting files for example, or scrambling their contents. More recent Trojans have been used to enable a local computer to be controlled from a remote location – for example the NetBus and BackOrifice Trojans.

Unlike network-borne viruses and worms, Trojans in their traditional sense were relatively uncommon (though of course, they could be delivered as a payload in the same way as an email or worm-borne virus). Trojans, and indeed viruses and worms, remain a threat, but their Adware and Spyware offspring are becoming more of a challenge.

3.4 Adware and Spyware

Adware is software incorporating some kind of advertising mechanism. At its most innocuous it just displays adverts, as illustrated by the free version of the commercial Web browser Opera. Adware may incorporate a number of other features, for example feedback mechanisms to help the advertiser. The advertising element of the software may run as a separate program from the main software functionality, and while most Adware is essentially harmless, it still has the power to impact productivity. Multiple Adware programs can reduce the number of processor cycles available for desktop applications – the user will have no indication of why their computer is grinding to a halt.

Beware of software bearing gifts...

Spyware and Adware packages are often included in the installation routines of less reputable shareware and downloadable programs, including some P2P software packages and even programs claiming to be spyware removal tools!

Check deep within the Terms of Acceptance, and you might find you're agreeing to a Trojan program. Certain packages, such as Grokster, will install such things even if you explicitly say you don't want to!

Adware usually will tell you it is being installed, and it is usually possible to uninstall it. There is no clear line between what is "innocuous" and what is "intrusive" however. When the software starts becoming too intrusive, it is probably better to classify it as Spyware. It is understandable that the two are often confused, particularly as Spyware often deliberately states that it is Adware.

The first use of the term “Spyware” was back in the mid-Nineties, but it wasn’t until the end of 1999 that it was defined as we understand it today – software which monitors how a computer is used, and sends its reports to another computer via the Internet. There exist Spyware programs that log credit card numbers, or username and password entries (PWSteal is one). Spyware generally tries to hide its presence, and uses a variety of techniques (for example, running as multiple processes that can restart each other) to prevent its removal.

Pre-emptive Strike

In January 2004, the computer company Dell started issuing all new computers with anti-Spyware software, when it found that 20% of all of its helpdesk calls related to Spyware.

Spyware is also the name for software that hides out on a desktop computer as a kind of “sleeper agent”, ready to undertake malicious activity without the user’s knowledge. A pre-broadband example was fake dialler software, which would call a premium rate phone line rather than the user’s standard ISP connection. More recent examples are Spyware acting as a conduit for Spam or Internet porn (For example, Migmaf); more alarmingly, it has been used as the starting point for Distributed Denial of Service (DDOS) attacks, where multiple infected computers are used to launch an attack on a specific Web site. By using a computer as a base for onward attacks, the originator becomes very difficult to trace. According to the BBC News such “sleepers” have been traded in chat rooms for money.

4 Internet Threats – the Next Generation

“I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We’ve created life in our own image.”

(Stephen Hawking)

Just as the categories of malicious content have grown and evolved, so have their methods of transmission. While email is a popular transport for malicious content, many exploits are reliant on some form of malicious Web content – that is, content that looks like normal Web content, but in some way links to, or causes a vulnerability to be exploited. With today’s email clients supporting HyperText Markup Language (HTML) of course, the threats are equally applicable for email clients as they are for Web browsers. Any one of the following techniques may be used to circumvent security measures, and there are others:

- **Web scripting.** The scripting capabilities of HTML-based files can be used for good or ill. HTML can embed files in a number of formats, for example Javascript; it can also be used to run programs written in other languages, such as ActiveX controls or Java applets.
- **Redirecting pages.** One, ostensibly harmless Web page can be linked to another which contains malicious content. In itself this might not be a problem, but a user may be prompted as to whether to run the scripts, and may see nothing wrong on the surface. Worse still, some HTML code can force a download to take place or a script to be run automatically. All it can take is for the user to open the page or pass a cursor across a link.
- **Malformed files.** A number of weaknesses in software programs (including Web Browsers) are caused by program failure if the program itself is faced by corrupted data files. Specially constructed data files can cause errors, which may result in a security breach. A recent example was the JPEG exploit, a particular issue as JPEG graphics files are not generally picked up by virus checking software.

- **Bad cookies.** Cookies contain data about Web pages a user has visited, and are highly useful for retaining settings about frequently visited Web sites. They have other uses, for example they can be a basis of tracking which Web sites a user has visited for good or ill.
- **Fraudulent content (Phishing).** What may appear to be a perfectly valid Web site could, in fact, be a mock-up, designed to capture username and password information.

Security attacks will often choose the weakest route. While the above may be the most common approaches at the moment, as one set of holes are closed, attention will inevitably turn to others. Given the malformed file risk for example, any program that accesses the Internet, running on any operating system, is potentially at risk. This includes the more esoteric communications tools that have been developed to use the Internet, not least:

Messaging tools. The first instant messaging tool to achieve widespread adoption was ICQ (“I seek you”), launched in November 1996 to a small group of users. Six months later the number had grown to 850,000 registered users of the program and a new category of Internet software was born. Online providers such as Yahoo! and MSN followed suit with their own messaging clients, and ICQ was bought by America Online (AOL) in 1998. Today, all such tools offer a number of functions, not least the ability to transfer files between users. Such functions can be exploited as a conduit for malicious content. There are other, similar tools which also offer file transfer features – Internet Relay Chat (IRC) and other clients offering multi-user chat for example, as well as voice messaging tools such as Skype which are rapidly gaining in popularity.

Peer to Peer (P2P) file sharing applications. Perhaps the first P2P file sharing network can be considered to be the USENET, started by two research students to exchange files. Now owned by Google and although it is mostly used for transferring messages, it remains one of the biggest information sharing sources on the Net. More recently and accelerated with the arrival of broadband Internet connectivity to the home, P2P file sharing tools such as Kazaa, eDonkey and BitTorrent have grown in popularity for the (often-illegal) transfer of music and video content. Not only can malicious content be transmitted in this way, but also the tools themselves are notorious for incorporating Adware and Spyware packages in their installation routines.

Such tools as these are not always being properly controlled by corporate IT departments. Indeed, some messaging tools and P2P programs deliberately try to overcome security restrictions (by piggybacking on HTTP for example), potentially opening back doors into what might be considered a secure environment. Things are not stopping with these tools: only recently for example, Google’s Blogger service was found to be used as a conduit for spyware. Unfortunately, as the available mechanisms become increasingly diverse then so do the threats, and the protections need to evolve to keep up. Traditional antivirus solutions offer little protection against Spyware, for example. What are current solutions missing, and what should solutions for the wider threats of malicious content incorporate?

5 New Threats, New Protection

“There are no such things as incurables, there are only things for which man has not found a cure.”

Bernard M. Baruch (1870-1965), “Adviser to US Presidents”

It is not in dispute that protections against malicious content such as intrusion detection, antivirus and anti-spam software serve a useful purpose. However, as we have discussed, the problem is far broader (and indeed, harder to pin down) than point solutions can deal with. While it is clear (from the DTI statistics, for example) that such tools are not adequate, it is less clear what can be done about the new threat. There are a number of reasons why existing solutions are failing to meet these challenges:

- they do not cover the whole range of threats
- they do not adequately meet service requirements
- they do not consider management and operational aspects

We can use these reasons as a starting point to characterise what any replacement solution *should* contain.

5.1 Covering the Threat

Sooner or later, a paper such as this needs to advocate a holistic approach – and with reason. As we have seen there is no single threat, rather there are a number of issues that can be exploited in combination. Inevitably then, any solution needs to adopt the same approach. We can consider the holistic approach in terms of ensuring it is inline, comprehensive and integrated.

- **Inline** – security needs to exist like a filter rather than as an external diagnostic tool, which requires things to go wrong before it puts them right. Any inline facility should conduct real-time inspection of data as it crosses the network, without compromising performance. There is a need to protect a number of different traffic types, notably mail and Web traffic, but also newer types such as P2P.
- **Comprehensive** – a comprehensive solution is one which offers protection mechanisms against all known issues. Where possible, it should also protect as best as possible against issues it does not know, by using heuristic techniques to detect potential breaches of security.
- **Integrated** – if individual solutions are failing, then the answer is to consider an integrated solution. Not only will any gaps in coverage be filled, but also an integrated solution is simpler to manage, and offers a clearer view on what is secured. Individual security capabilities need to work together to support the whole.

The JPEG exploit mentioned above is a prime example of how poorly integrated, inflexible protection mechanisms can allow security breaches to slip between the cracks. Malicious content can arrive in so many ways, it is not enough to focus on one type of file format, or to protect any one program.

5.2 Delivering the Service

Whatever security features and functions are provided, they need to help, rather than hinder the organisation. Here are some of the qualities you should expect from a security solution:

- **Performance** – the solution should not cause a bottleneck to the organisation. In particular, any inline solution (see above) should have a minimal impact on data latency, that is, the time data takes to cross the network.
- **Scalability** – we need to be sure that the performance can be maintained as the network load changes. This is about right-scaling: there is no more point having a vastly over-specified system, than having an under-specified one.
- **Extensibility** – any solution needs to be flexible enough to deal with future requirements. The security solution should act as a framework, enabling new features to be plugged in as necessary. Clearly this impacts the company providing the solution – will it be around in five years time?

At the same time as assuring protection, it is highly important that existing IT systems and networks continue to work effectively. Security products should therefore ensure they impose only a minimal impact on the operational environment.

5.3 Assuring Operational Aspects

Finally, we need to take the operational and management aspects of the solution into account. The best kind of security is the kind you can't see and that you don't need to spend every working moment dealing with (who has that kind of time, after all?). It therefore needs to be:

- **Automated** – it should be possible to automate common management tasks, e.g. antivirus signature updates. Where corporate security policy exists, it should also be possible to use this as input, for example to define acceptable file types and patterns of behaviour.
- **Adaptive** – the solution should be able to reconfigure itself in order to deliver the most effective service. For example, new virus signatures should be downloaded on an appropriate basis – such as outside office hours.
- **Usable** – any facilities need to be as simple as they are effective, and should incorporate appropriate visual tools. Any management interfaces must, of course, also be secure!

One of the most important things any security solution can do is provide an audit trail. This becomes of primary importance after a breach, to enable the cause to be determined and evidence to be collated.

6 Assuring Business Protection

"The deviation of man from the state in which he was originally placed by nature seems to have proved to him a prolific source of diseases"

Edward Jenner (1749-1823), who discovered a vaccination for smallpox

Security issues cannot be solved by technology alone. As well as implementing technical security measures, a business can do many things to further reduce its own security risks and strengthen its protection. Here, we give a number of guidelines to help organisations further protect their interests against the risks of malicious content.

- **Start and End with Security Policy**

A starting point for any security implementation is to define a security policy that is aligned with business needs. For this reason, a business needs to understand how it undertakes its activities, and the real security threats it faces. A corporate IT security policy should be written in such a way that existing and new threats can be taken into account. Note however that the presence of a policy does not automatically mean an organisation is protected – the policy needs to be implemented correctly, and kept up to date.

- **Adopt a Holistic Approach to Risk Management**

Good security is not about risk avoidance, which would be too expensive (and ultimately impossible to achieve), but risk management. A holistic view of all the risks a company faces, gives a far better perspective on what are the biggest risks to the corporate IT environment, and therefore what should be treated first. There is no point, for example, implementing many layers of electronic security measures, if the lock on the machine room door is broken!

- **Cure is as Important as Prevention**

Business continuity (or disaster recovery) planning incorporates defining the procedures and steps that should take place following a major failure of IT, for the recovery of

systems and data. You cannot protect against everything, and the best security is no substitute for ensuring you have such measures in place. At the very least you should have maximum confidence in your data backup and recovery capabilities.

- **Practice What is Preached**

It is not enough to *want* security – you have to *do* security. This means, that working practices should build in security considerations. These may range from formal practices (such as, the HR department informing the IT department when a person leaves the company), to informal considerations (not leaving passwords on a Post-it on the side of the screen, for example). Users often have to be protected from themselves: as the adage goes, never put down to malice what you can put down to stupidity.

- **Implement security management procedures**

Good security management stems from a good security manager. It is important to assign security responsibility to an appropriately placed individual, and then to ensure the person has everything necessary to carry out the role. Procedures should include an appropriate level of review and audit, involving third parties where necessary – nothing helps improve security practice as much as regular review.

7 Conclusion

It used to be said that a chain is as strong as its weakest link, but in these, hyper-networked days, the chain analogy is less and less applicable. Instead we can consider an analogy of water seeping through rock – water will find whatever porosity it can to reach the lowest possible level. It is worth having as broad a definition of the threats as possible, as like water, they find their way through. Traditional mechanisms are like a system of dykes – adequately protecting against the threats they were designed for, but not flexible enough to offer protection against new threat types.

Whether we like it or not, and despite the downturn, we are in the middle of the information revolution. Change is the only constant, with new capabilities causing new threats. Not least for example, Web services and Service Oriented Architectures will transform how we think about applications; meanwhile, wireless networking is driving new ways of accessing corporate data. New device types are appearing, with MP3 players merging with cell phones and RFID chips moving from pilots to full deployment.

Each development in communications can offer a number of welcome benefits, but these can offer small comfort from a security perspective. To attempt to deal with any issues individually is doomed to failure – we face a diverse, multi-channel future with all the positives and negatives that implies. If a business is serious about ensuring its security, it needs to deal with it in a comprehensive fashion. While there is no guarantee of 100% protection, there can be no excuse for failing to do so, and the price of failure may prove very expensive indeed.

About Aladdin Knowledge Systems Ltd

Aladdin is a global provider of software digital rights management (DRM) and enterprise security. Aladdin products include: the HASP® family of hardware and software-based products that flexibly protect, license and distribute software and intellectual property; the USB-based eToken™ device for strong user authentication and e-commerce security; and the eSafe® line of integrated content security solutions that protect networks against known and unknown malicious code, spam, non-productive and inappropriate content. eSafe addresses all layers of content security, and delivers superior protection that is easy to deploy and manage. Visit the Aladdin Web site at <http://www.Aladdin.com>.



About Quocirca

Quocirca is a company that carries out world-wide perceptual research and analysis covering the business impact of information technology and communications (ITC). Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry in the following key areas:

- Business Process Evolution and Enablement
- Enterprise Applications and Integration
- Communications, Collaboration and Mobility
- Infrastructure and IT Systems Management
- Utility Computing and Delivery of IT as a Service
- IT Delivery Channels and Practices
- IT Investment Activity, Behaviour and Planning
- Public sector technology adoption and issues

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of a company'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 the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly polling users, purchasers and resellers of ITC products and services on the issues of the day. 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, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain.

Quocirca's independent culture and the real-world experience of Quocirca's analysts, however, ensure that our research and analysis is always objective, accurate, actionable and challenging.

Quocirca reports are freely available to everyone and may be requested via www.quocirca.com.

Contact:

Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom
Tel +44 1753 754 838