securityplus

IT security news & reviews, exclusively from e92plus

CRN THE CHANNEL AWARDS 2011 FINALIST

How safe is your network?

We explore how to meet the challenges of compliance, BYOD and the latest threats to your data

DATA LOSS INCIDENT LOST MOBILE DEVICE NETWORK INTRUSIO

Inside this issue

Featured vendors:

QUARRI™ Lumension IT Secured. Success Optimized. HUAWEI AVIRA

Spring 2012

www.securityplusonline.co.uk

infosecurity® EUROPE 24-26TH April 2012 Earls Court, London, UK

Introducing SecurityPlus

The leading security magazine from e92plus

Welcome to the latest edition of SecurityPlus from e92plus:
essential industry insights and interviews from your award winning security distributor.

2012 has seen us working with new vendors, expanding our portfolio in both security and virtualisation with three new vendors:

- **Cryptocard** is an industry innovator in Two Factor Authentication, and in particular Authentication as a Service, bringing organisations cost reduction, simplicity and flexibility. Cryptocard were recently purchased by Safenet, a Gartner Leader in Data Protection, enabling them to change the way organisations deploy and manage their authentication strategies and platforms
- **Neocoretech** have developed a VDI solution that delivers outstanding efficiency and flexibility without the cost or complexity of the current alternatives. NDV differentiates itself through a simpler, more flexible approach that can deliver VDI from a deployment with 25 users on a single server to a distributed architecture serving thousands of users across multiple sites
- **Huawei** are a leading global information and communications technology (ICT) solutions provider. In partnership with e92plus, Huawei will be showcasing its strength in the field of network security and secure remote access and showing how their secure solutions help enterprises realise business by transforming complex security issues into simple and reliable solutions

This year will also see e92plus back at InfoSecurity, as we will be exhibiting in partnership with four of our vendors: Avira, Huawei, Lumension and Quarri. Please drop by to see us, and you'll find lot's of information on their exciting solutions later in this issue.

Mukesh Gupta
Managing Director of e92plus

Inside this edition

Web Browsers: the weak link in enforcing PCI Compliance

Does your company process credit card information via a browser? Data loss from theft or leaks, malware and Man-in-the-Browser attacks – all of the risks involved in delivering information through web browsers – has led to the development of a wide range of security policies to achieve PCI compliance. Even if you believe your organisation is compliant, critical security gaps remain in the current standard technologies used to meet the requirements.

Gaps in Your Encryption
PCI Requirement 3 mandates organisations must protect stored cardholder data. Encryption is the preferred and most widely used technology for this requirement. However, if you're using a web-based processing or payment application, any credit card processing conducted in the web browser leaves the data at risk. All the encrypted data is unencrypted when it's rendered in the browser on the endpoint and in use. Data can remain in the web browser cache in clear text format, where it can be easily extracted by either malware or end users. Even simple, everyday tasks such as cut, copy, paste and screen capture put sensitive data in the system-wide clipboard, which is also rendered in clear text format and easily accessible, even after the web session has ended. In addition, stored user names and passwords from browser sessions remain available in the authentication cache and vulnerable to malware.

Does Your Anti-Virus Prevent Malware Infections or Zeus Attacks?
Endpoint security and antivirus effectiveness are an on-going debate; however, the use of and regular updates of antivirus software or internet security programs to prevent malware infections are still a PCI requirement. In their 2011 Banking Security Test, MRG Effitas reported that of 27 Internet Security products tested on Windows PCs, only a handful were effective in preventing the Zeus botnet. Their report went on to conclude that users need to employ additional security measures on top of traditional anti-virus or internet security suites to counter threats posed by modern malware.

While keeping antivirus maintained and updated sounds simple, the Verizon 2011 PCI industry compliance report states that only 64% of companies they tested for PCI compliance achieved this in 2010.

Challenges to Your Web Application Security
The shift to web applications and cloud services has also created additional PCI compliance challenges. Requirement 6 states that organisations must develop and maintain secure systems and applications. Demonstrating security controls built in your own in house applications can be challenging – many are legacy systems in which comprehensive security controls likely don't exist. Many organisations are also using web-based payment applications supplied by their bank to process transactions, leaving them no control over critical security updates and patches.

The QSA view

"*Quarri Protect On Q (POQ) helps clients achieve and maintain PCI compliance by addressing a variety PCI issues, including data encryption and application security, that have historically been difficult to solve*," said Andy Dalrymple, PCI QSA, PTP Consulting. "*With its on demand deployment, POQ also acts as a compensating control for endpoints that don't have the latest security updates installed. And its data theft protections also ensure organisations can prevent replication of confidential data by careless or malicious end users*."

However, it is possible to build security into the browser session, something you do have control over. Making the browser secure from local malware threats protects data from keyloggers, screen scraping and cache raiders. Encrypting and deleting data written from the browser to the local cache, preventing the cut, copy, paste, print and screen capture features and delivering this secure web browser protection as part of the application closes many of the current security gaps in meeting PCI requirements.

Move With Us Closes Web Browser Gaps in PCI Compliance
Move With Us are one of the UK's leading residential property experts for consumers buying, selling and valuing their homes. In the Move With Us call centres, telephone operators take credit card information over the phone and enter that information into a web-based credit card application. In order to comply with PCI DSS requirements, Move With Us needed to secure that information from malware.

The Move With Us IT department deployed Quarri Protect On Q (POQ) for their credit card application, enabling them to control and protect the users' browser session content from theft or data leakage by malware. POQ provides zero-hour malware defence against keylogging, framegrabbing, cache mining and other attacks. As it's not signature-based, it offers a much higher level of compensating controls than standard antivirus software. All browser session data is encrypted and digitally shredded when the session ends.

"*We tested many security products and chose Quarri Protect On Q because it offered strong malware protection*," explained Anthony Hall, IT Manager for Move With Us. "*POQ is also the only one that is delivered on-the-fly, so we don't have to worry about the call centre staff using an unsecured desktop*."

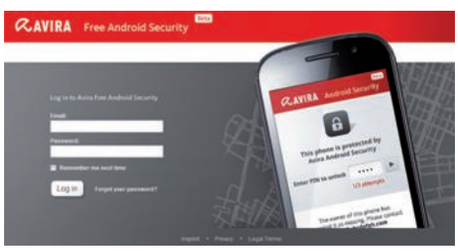
"*Quarri Protect On Q helps us achieve PCI DSS compliance*," stated Hall. "*We needed a way to secure credit card data in our call centre web payment application. POQ was quick and easy to deploy to our end users, which was very important to us. Best of all*," continued Hall, "*POQ is on demand so there's no client installation. It's deployed as part of the application browser, which makes it very simple and very effective*."

POQ's on demand deployment gives organisations the ability to extend security controls temporarily to web sessions, securing the data in the credit card web application from any endpoint. In a disaster recovery situation staff can easily work from home, with no changes to working practices or software. Everything to protect sensitive data is delivered on-the-fly when the user logs in, encrypted, then securely deleted, along with any residual data, when they log out. And, with Protect On Q's enforcement feature, all users accessing the application are using the protected browser. In addition, central log files of all user activity provide compliance with PCI DSS auditing requirements. "*We're confident our data is protected*," stated Hall. "*Our PCI QSA auditors are happy and so are we*."

It's the world's most popular mobile OS… securing devices on Android

Have you ever felt lost after leaving your smartphone at home? If so, then you already know that your Android is worth much more than the sum of its parts.

This constant companion keeps some of your most important data at your fingertips. That's why you need to be prepared in case your device ever leaves your hands. After all, your smartphone may be replaceable, but what about its contacts, messages, photos and saved passwords?



Location Tracking: Instantly pinpoint the device's location.
Search for your smartphone the smart way! Avira Free Android Security can locate your device's signal and display its location on a Google map.

Remote Lock: Hide your stuff from prying eyes.
Shield your personal information as soon as you think your device is missing. Lock your phone to secure its contents and display special instructions to anyone who finds it.

Remote Wipe: Protect your privacy, no matter what.
Phone stolen or hopelessly lost? Even in the worst case, your privacy is safe and sound. Visit the Web Console to erase all contacts, messages, apps, photos, login credentials and settings.

Remote Scream: Give yourself a holler!
Can't find your phone? Maybe it isn't far away or no one has noticed an unattended phone. Log in to your account and trigger a loud noise from the device, even if it's in silent mode.

Owner Notification: Be reachable when your phone is found.
Being a hero was never so convenient! The person who finds your locked phone can contact you at another number simply by tapping a button on the touchscreen.

Device Administration: Monitor battery life and more—for up to five devices.
Check remaining battery life as well as device specifics such as model, carrier and Android version. There's even a record of places a phone's location has been tracked, screams triggered and remote locks/unlocks.

The forgotten OS in the workplace: delivering security on Macs

With every technological advance, the Macintosh platform becomes even more versatile and enjoyable to use. It's no wonder that the popularity of the Mac continues to soar among individuals and professionals looking for crisp graphics, unrivaled usability and slick performance.

Unfortunately, the Mac is also attracting more attention from cybercriminals. Avira is committed to preserving the security of the Macintosh platform. Backed by over 25 years of proven technology, Avira Free Mac Security not only eliminates emerging Mac threats but also crushes any PC viruses that might spread by way of a Mac.

Real-Time Protection
Avira Free Mac Security is constantly on guard for viruses and other threats. Every file accessed by the user and the system is silently inspected so that no infected file sneaks in between system scans.

More Security for the Whole Network
Though Macs are less vulnerable to viruses, they share and collaborate with PCs, mobile devices and other hardware. Empowering each Mac with Avira's antivirus expertise optimizes the overall security of any network.

Three Ways to Scan
The full system scan performs a thorough check of the entire system without disrupting your normal activities. The quick scan checks typical malware hideouts in order to deliver a quick bill of health. Finally, the custom scan allows the user to check individual files and folders manually.

It's All About Convenience
Taking a page from the playbook of Apple, the technical sophistication of Avira Free Mac Security is disguised by its simplicity. Users are treated to an incredibly clean interface that delivers award-winning security in a matter of clicks.

Centrally manage the security of all Macs, PCs and servers on your network
The Avira Management Console (AMC) allows you to install, manage, monitor, configure and update all machines' security from a single Windows server or PC. The AMC is much more than a time saver: it's peace of mind. Extensive reporting and alert functions enable you to respond in a timely, effective manner to any security issues that may arise.
Any combination of Macs, PCs, Windows servers, Unix servers and Unix workstations can be managed through the AMC. To get started, simply contact us for your license key.

Ask about your free copy of Mac or Android Security from **Avira on Stand L65**

Top 10 Tips for better IT Security and Compliance

The following 10 IT security and compliance tips offer cost effective and efficient ways to improve security without unnecessarily increasing the workload on the IT department.

1. Use Anti-Virus as Part of Your Defence-In-Depth Strategy

Anti-Virus will always play a role in endpoint security, no matter how loudly some pundits proclaim its demise. Anti-Virus should be used as a part of a defence-in-depth strategy that combines layers of technologies to minimise risk and exposure.

2. Leverage Application Whitelisting to Fill the Gaps

Anti-Virus and application whitelisting are the ying and yang of endpoint security. Anti-Virus blocks threats based in a blacklist approach: if an executable is on the list, if is not allowed to run. On the other hand, whitelisting works with a trust-based approach that defines what can be trusted and prevents unwanted / untrusted executables from running on the system. Even if you don't turn on the blocking feature, whitelisting gives crucial intelligence on what applications are running on your endpoints.

3. Control Your Ports

We're not talking about Group Policies that just disable ports, nor are we talking about gluing them shut. The majority of users need to plug devices into their computers to get business done, and banning removable media in order to battle the risks associated with its use hinders daily business activities by employees.

4. Mesh Compliance with Security Practices

The most effective organisations first determine where their business risks lie, then put technology and processes in place to mitigate those risks. Then they figure out how those measures satisfy compliance obligations. When organisations get that flowchart backwards—when they act first to check the boxes to fulfill compliance duties—they tend to leave chinks in their security armour. In addition, they usually spend more money because they reinvent the wheel with duplicate practices, chasing new activities every time a new regulation comes out.

5. Be Ready To Deploy Fixes Quickly

Many organisations must walk a fine line, balancing high-priority software updates with the need to avoid major disruptions to end users. Capabilities such as wake-on-LAN and payload caching allow organisations to not only offer a pull model, but also push patches outside of normal business hours. Also, in distributed environments patch staging allows one endpoint in a segment to pull down a patch, while other endpoints wait in sequence.

6. Know That Hackers Love Third-Party Apps

These days, it isn't just heterogeneous operating systems that organisations have to worry about - there's also the frenetic application environment. According to 39% of IT professionals, the use of third-party applications is one of the top three factors causing the greatest rise in IT risks. When these applications are unpatched and insecurely configured, the attack surface greatly increases. In fact, Secunia says "An 80% reduction in risk can be achieved by either patching the 12 most critical or the 37 most prevalent programs in a sample portfolio." (*Secunia, Half Year Report, July 2011*)

7. Encryption Is Your Friend

If you look at the frequent headlines about data breaches plaguing organisations, lost laptops, media and devices still contribute to many data breaches today. In fact, last year the Privacy Rights Clearinghouse statistics showed that breaches caused by lost, stolen or displaced laptops and devices made up about 40% of all the records exposed in 2011. Encrypting data on PCs, laptops and mobile devices is a fundamental first step toward instituting improved data protection. If a lost or stolen endpoint falls into the 'wrong hands', Full Disk Encryption (FDE) will ensure that the data isn't readable, thereby drastically reducing the risk of costly breaches.

8. Establish and Enforce Secure Configurations

In the same vein as patch management, configuration management offers an efficient means to drastically improving the protection of your endpoints. Limit privileges for end users to keep system settings as closed as possible, and enforce measures such as firewall settings. This will drastically reduce the attack surface hackers have to go after on your systems.

9. Kick Spreadsheets to the Curb

While simple spreadsheets might seem like an easy and cheap way to track compliance activities at first, the reality is that they'll end up costing the business buckets of money during the audit process. The problem with spreadsheets is that they don't scale well and they're limited. As organisations grow and regulatory requirements increase, ad hoc tracking methods like spreadsheets, word documents or sticky notes on someone's cube don't give decision-makers or auditors the kind of overall risk posture visibility necessary to efficiently prove compliance.

10. Keep Executives in the Loop

Frequently these days, security and compliance is a boardroom issue. As such, it is logical that your executives would want to know what the IT department is doing to keep the business safe and the auditors at bay. Don't frustrate your executives. Instead, filter your reports to them. Speak in their language and explain to them the ROI of the security dollars they're spending.

Conclusion

Each of these tips – individually – will make a big difference in the security and compliance posture of your organisation. But together, they work even better. A layered security approach is the best bet for thwarting hackers and insiders – even if they find a chink in one layer of the armour, there's another layer able to engage the threat underneath.

What's your plan for mobile security?

It's a complex problem that requires a holistic approach

Mobility is here. Mobility is now. Mobility (along with cloud and social media) is one of the three new technologies that brings new productivity opportunities—and associated security risks. Add in the consumerisation of IT, an explosion of corporate and personal mobile devices, and you have one of the major IT security strategy challenges of 2012.

The challenge is how to enable productivity and mitigate the threats, vulnerabilities, and risks in a way that strikes the best balance and lowest total costs. How do you establish a mobile security strategy that encompasses both corporate and personal devices?

Organisations that narrowly focus on one aspect of the problem and fail to holistically address the security challenges posed by mobility, device proliferation and consumerisation run the risk of lower user satisfaction, lower productivity, higher costs and even exposure of sensitive data.

Start with your goals

Regardless of the devices involved and who owns them, what are you trying to accomplish? Is the goal to provide mobile access to useful corporate resources such as email, file services, and intranet apps? If so, having highly limited, isolated mobile devices provides little value. In order to provide secure mobile access to these valuable resources (which is the goal of most organisations), you must:

1. Protect accessed data that is now local to the client device, and
2. Protect the client device itself, which serves as a conduit to both local and remotely accessible resources.

As you clarify your objectives you reveal the security tools and technologies that you will need, for example:

- Communication over unsecure networks requires an authenticated and encrypted tunnel
- Protecting data that is both stored and in use on mobile devices requires encryption and data loss prevention (DLP)
- Device protection requires configuration management and anti -malware software

Ponemon Survey on Mobility

Most IT professionals don't know how or what data is leaving their networks through mobile devices.

75% recognize that mobile devices put their organisations at risk. Only 33% have the necessary security policy in place.

64% are concerned with employees taking photos or videos in the workplace, with fears about the loss of confidential information.

56% say that employees circumvent or disengage security features such as passwords and key locks.

50% have seen an increase in malware infections due to unsecured mobile devices

41% experienced data loss because of unsecured mobile devices, including laptops, smartphones, USB devices, and tablets.

Identify and understand the threats

It is easy to see why data loss is such a high priority for mobile security. Regulatory requirements and the low cost of mobile devices contribute to the problem. As the table opposite illustrates, most organisations should start with a focus on tools and techniques that help protect mobile data.

Countermeasures and other related control

Tier 1: Mobile Device Management (MDM)

The term mobile device management is an artifact of convenience in this context. It's the capabilities that matter most, not the specific product category they come from. Some organizations get everything they need from Exchange ActiveSync® or BlackBerry® Enterprise Server, while others require a fully blown enterprise-class MDM solution. No matter which MDM solution makes sense, most organisations will eventually find it necessary to also implement some of the supplemental security measures described below.

Robust MDM solutions should include the following:

- Application management - includes the ability to inventory a device's applications, distribute/update software, and restrict the use of individual applications. It also often includes support for a self-service portal and/or enterprise app store.
- Configuration management and resource control - this entails having control over a wide range of device-level capabilities and parameters including password requirements, camera functionality, SD card usage, and VPN, Wi-Fi, Bluetooth, and encryption settings.
- Device integrity - all of your defences are effectively undermined when a mobile device is jailbroken or rooted. Being able to detect this condition is, therefore, a critical capability
- Most organisations identify data loss as the top concern in the mobile scenario. That's why the primary emphasis should be on tools and techniques that help protect mobile data

- Device recovery and loss mitigation (including device tracking, manual/automatic lock-out, manual/automatic wiping of all or selected data, and support for device-level backup and restore
- Support and service management - Remote control is useful for technical support, while expense control is intended to moderate usage and costs (e.g. roaming)

Tier 2: Supplemental Security

MDM-oriented security capabilities are an excellent starting point for a mobile security strategy. However, as mobile access scenarios continue to expand and the development of mobile malware continues to accelerate (in other words, as vulnerabilities, threats, and risks continue to grow), the effectiveness of MDM for security drops lower and lower. IT needs to implement measures that pick up where MDM leaves off in order to bolster secure access, threat protection, and data protection.

Key topics to address include secure remote access, threat protection (what organizations need is a robust web security "cocktail" that examines content from every possible angle to detect new threats) and data protection.

Tier 3: Emerging security measures

This third tier of countermeasures is fairly new to the market, and is often classified as advanced or emerging. Early adopters of such technologies tend to have a very low tolerance for risk, extremely sensitive data, or face very strict regulatory requirements.

Characteristics of an ideal enterprise solution

No one hands in their laptop or desktop when they get a smartphone, so mobility just adds to the challenges of enterprise security. This - and budget pressures - drive the need for administrative efficiency and low cost of ownership when selecting mobile security solutions. For today's businesses, ideal solutions will be those that are enterprise-class in nature and that keep costs down by minimising the number of products and vendors.

Enterprise-class key features that should be a part of all mobile security solutions to further reduce cost and improve effectiveness include: centralised management, role-based administration, directory integration, group policies, flexible reporting, and configuration audit trails.

Meeting the organisation's needs with a smaller set of products and vendors invariably reduces cost and complexity while improving integration and effectiveness. This is why IT/security managers typically favour solution providers that offer the greatest portfolio of capabilities for the greatest number of devices they intend to support. Ideally, the advanced threat and data protection capabilities needed to support mobile devices are available as integral extensions of the solutions already being used to provide similar capabilities for the organisation's fixed users/devices.

The need to support mobile devices is here and now

The challenge is complicated by a number of factors, especially: (a) the diversity of platforms and devices and how this impacts both the need for certain controls and the available solutions, and (b) the diversity of potential ownership, reimbursement, and usage scenarios, and how to maintain a balance between user and corporate expectations.

Because of these complexities, there is no straightforward, one-size-fits-all recipe for success when it comes to solving the security-for-mobility problem. Nonetheless, organisations should:

- **Remain focused** on the most important objective – ensuring adequate protection of mobile data – while balancing this with need for a positive user experience and reasonable cost of ownership
- **Pursue a layered approach** where MDM-oriented security capabilities are supplemented by the advanced controls described herein for secure access, threat protection, and, above all else, data protection
- **Favour solutions** that deliver a high degree of administrative efficiency and low overall TCO based on their capacity for consolidation and incorporation of enterprise-class features, such as centralised management, directory integration, and robust reporting

Threat	Risk
Lost or stolen device	Unauthorised access to local or network-based data; data loss
Lost or stolen media card	Local data loss
Misuse of local comms (e.g., Bluetooth, IR)	Compromised/infected device, data loss and potentially degraded operation
Compromised apps	Data loss and potentially degraded operation
Malware	Data loss and potentially degraded operation
Web/network-based attacks	Data loss and potentially degraded operation

Howden Joinery Group secures remote access with Barracuda Networks

Large nationwide businesses are more likely to have significant numbers of senior staff who are frequently on the move. Howdens is no different, with area managers and other senior staff spending much of their time travelling between the company's hundreds of depots and to their customers in the building trade.
To maximise their productivity, Howdens' senior management need reliable remote access to their emails. Furthermore, they have to ensure that this access is fully secure, and that web applications such as email are protected from malicious attacks, and can only be accessed by legitimate users.

> "We needed a dedicated firewall that was specifically designed to protect remote access to our webmail; one that was cost-effective, easy to manage and secure"
>
> **Ru Gardner, Howdens Security Team**

Howdens had, for some time, been using a content filtering device, employed as a reverse proxy server, to protect its webmail applications from malicious external online attacks. Although this was generally effective at its primary purpose it was far from satisfactory, as Ru Gardner of Howdens' Security Team explains.

"*Our legacy system did the job of protecting our Outlook Web App from the intrusion of malware, but it caused us a major management headache*," says Gardener. "*Quite simply, it was vastly over-engineered for the job of acting as our web application firewall, and was too costly, complex and time-consuming to manage and configure, especially given the wide variety of smartphones and tablets we use*.

"*Our business relies on email, so downtime is unacceptable, as remote workers need to be in contact with suppliers and customers at all times. Our employees increasingly found themselves using a virtual private network (VPN) to access their email securely on the go, but this required staff to log in every time they wanted to check their mail, which was far from ideal. Meanwhile, maintaining the security of the webmail applications was a constant strain on IT resources and threatened to become unmanageable"*.

The solution: Web Application Firewall from Barracuda Networks

Howdens chose Barracuda Networks' Web Application Firewall (WAF) for the job of securing its webmail from external threats and ensuring that only trusted devices could access company's online email system. The company installed two Barracuda WAF 660 appliances: one installed in the primary and one in the secondary datacentre. These firewalls ensure that all incoming traffic to its webmail applications is screened for malicious attacks, such as hackers attempting to exploit vulnerabilities to steal sensitive data contained in emails.

All email traffic passing through the firewalls uses the HTTPS protocol, providing secure, encrypted communication between remote workers and their webmail servers. The appliances handle traffic from around 160 employees who use the Outlook Web App (OWA) to access emails from remote desktops, and over 130 users of Microsoft's ActiveSync protocol for handheld devices, used predominantly by senior management, area managers and IT staff.

Barracuda's appliances monitor all traffic passing between its web applications and remote devices, as well as providing reports about attackers and attack attempts. A whitelist of all staff smartphones is kept on the devices to ensure that only recognised and approved hardware may successfully connect with company webmail systems.

Assuring modern, manageable and secure mobile email

Howdens legacy content filtering system was only ever effective for logging onto Outlook Web App for webmail, and was very difficult to configure effectively for mobile devices using ActiveSync. Barracuda's firewall appliances now ensure that Howdens' management has secure, reliable access to email, wherever they are and no matter what device they use.

"*While the assurance that email will be a reliable tool has been a boon for the company's field workers, the effect on IS staff has also been significant with greatly reduced complexity in both support and maintenance processes*," says Gardner.

"*It's a relief to know that we have the technology in place to protect webmail access on all devices used across Howdens' operations," he continues. "Rather than being a source of occasional frustration for senior management, and the bane of the IT department, remote email is now a trusted and reliable function*."

The Barracuda firewall's intuitive, real-time interface enables Howdens' IT staff to manage and monitor email access across its networks; add email functionality to any new mobile device without difficulty; and ensure that they always know that legitimate devices are connecting safely with the company's webmail.

"*The installation process was smooth and quick, with our new Web Application Firewalls plugging simply into both our datacentres*," says Gardner. "*We were also appreciative that Barracuda took the time to understand our needs; recommended technology that was perfectly suited to our requirements; and provided expert, helpful and friendly support when required. The capital outlay on Barracuda's technology is quickly paying itself back through huge reductions in time IT staff spend on managing email security, as well as the increased productivity for staff working remotely. It has reduced our reliance on VPNs*."

> "It's a relief to know that we have the technology in place to protect webmail access on all devices we use."
>
> **Ru Gardner, Howdens Security Team**

HOWDENS
JOINERY CO.

Learn more about how Howdens delivered secure access with **Barracuda on Stand D10**

Web Application Firewalls & PCI Compliance

Why are threats to websites different from those directed at the network?

Compared with the network level, you don't need to be highly skilled to use the internet. This not only makes it easier to use legitimately, but also encourages the malicious misuse of web applications. In addition, the internet also offers many possibilities for concealment and making action anonymous meaning the risk for attackers remains relatively low and so does the inhibition threshold for hackers.

Many web applications that are still active today were developed at a time when awareness for application security in the internet had not yet been raised. There were hardly any threat scenarios because the attackers' focus was directed at the internal IT structure of the companies. In the first years of web usage in particular, professional software engineering was not a priority, so web applications usually went into production without clear security standards. Their security standard was based solely on how the individual developers rated this aspect and how high their respective knowledge was.

The problem with more recent web applications: Many offerings demand the integration of additional browser plug-ins and add-ons in order to facilitate the interaction in the first place or to make it dynamic. These include, for example, Ajax and JavaScript. While the browser was originally only a passive tool for viewing web sites, it has now evolved into an autonomous active element and has actually become a kind of operating system for the plug-ins and add-ons. But that makes the browser and its tools vulnerable. The attackers gain access to the browser via infected web applications and as such to further systems and to their owners' or users' sensitive data.

Some assume that an unsecured web application cannot cause any damage as long as it does not conduct any security-relevant functions or provide any sensitive data. The opposite is the case. One single unsecured web application endangers the security of further systems that follow on, such as application or database servers.

What's wrong with just using my network firewall?

Unlike traditional network firewalls or intrusion detection systems that simply pass HTTP/S traffic, Web Application Firewalls proxy all traffic and insulate Web servers from direct access by attackers.

What do Web Application Firewalls provide?

Web Application Firewalls protect web applications and services from malicious attacks, as well as increasing the application performance and scalability. Compared to traditional network firewalls, they are designed to protect against highly targeted, malicious attacks that are directed against data and network access hidden behind errors or flaws in website code.

With an explosion of web applications for many business transactions - from Corporate Email to Document Sharing / Distribution and Secure Transactions, the need to secure those applications against data or financial loss is paramount.

How do Web Application Firewalls help with PCI Compliance?

In response to the increase in identity theft and security breaches, major credit card companies collaborated to create the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. It applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers and service providers, as well as all other entities that store, process or transmit cardholder account data.

This means that any organisation that deals with credit or debit card information through their website, or where that data can be accessed through the website, is subject to a range of legislative requirements.

PCI DSS Requirements

Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Controls

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

What and who to see **at InfoSec 2012**

Absolute Software is the leading provider of firmware-embedded endpoint security and management for computers and mobile devices.

Their solutions provide organisations with comprehensive visibility and control over all of their endpoints, anywhere, anytime. With Absolute Software, organisations can optimise productivity, reduce operating costs, prove compliance, and respond to computer theft.

Stand D31

With over 250 million customers, Avira is the fastest growing Anti-Virus company in Europe. This is based on a product range that lead the market for both virus detection and performance.

InfoSec 2012 will see the UK launch of two new solutions - Avira Mac Security and Avira Android Security, providing extended coverage for more mobile devices to complement the existing workstation and server solutions.

Stand L65

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions.

The company's expansive product portfolio includes protection against email, Web, IM threats, and solutions that improve application delivery and network access, message archiving, backup and data protection.

Stand D10

Authentication Leader meets Cloud Visionary

SafeNet has acquired Cryptocard and together, we now offer the most complete solution available for strong authentication and access control.

Cryptocard's Authentication-as-a-Service capabilities will help customers around the world accelerate deployment of authentication solutions, with improved flexibility and lower cost to the business.

Stand C80

Celestix Networks is a global leader in IT security solutions for unified threat management, data-centric security, secure application access, traffic optimisation and tokenless 2FA.

Their solutions are designed for reliability, performance and ease-of-use making Celestix the preferred security partner to corporate and federal organisations worldwide.

Stand C40

Huawei is a leading global information and communications technology (ICT) solutions provider. Since assuming control of the Huawei Symantec partnership, they will be exhibiting the new range of diversified security solutions at InfoSecurity Europe 2012.

Huawei will be showcasing its strength in the field of network security and secure remote access and showing how their secure solutions help enterprises realise business by transforming complex security issues into simple and reliable solutions.

Stand L65

Registration for InfoSec 2012 is free with e92plus! Visit **www.e92plus.com/infosec** for details

Lumension Security, Inc. is a global leader in endpoint management and security, helping over 5,000 customers protect their vital information and manage critical risk across network and endpoint assets.

InfoSec 2012 will see Lumension demonstrating Intelligent Whitelisting™: the industry's first integrated, application whitelisting solution that brings together the combined strengths of patch management, application control, anti-virus, and trust-based change management into a single, integrated solution.

Stand L65

Quarri Technologies, Inc. empowers organisations to keep their sensitive data secure.

Protect on Q defends against both external and internal attacks and prevent unauthorised use and replication of confidential data by controlling both malicious and careless end-user behaviour, while allowing users to remain productive and have a seamless online experience, while also enabling organisational compliance with industry standards and government mandates.

Stand L65

Websense is a global leader in unified Web, data, and email content security, delivering the best security for modern threats at the lowest total cost of ownership.

InfoSec 2012 will include demonstrations of Websense's award winning solutions, plus the UK launch of Websense Mobile Security: their industry leading web security solution that is paired with data-aware defences and MDM features to control mobile devices for security, risk, and compliance.

Stand F10

WinMagic's full-disk encryption simplifies protecting data on desktops, laptops, and removable media. WinMagic is trusted by organisations worldwide to minimize risk, meet compliance regulations and protect valuable information against unauthorised access.

WinMagic is the first company to integrate secure network support into the pre-boot environment with PBConnex.

Stand C72

We are an award winning Valued Added Distributor, with over 20 years experience in the channel. Specialising the security, we provide extensive sales, marketing and technical services to our reseller partners, delivering solutions for organisations from SMBs to enterprise and helping to grow our partner's business

We will be exhibiting at InfoSec 2012 with 4 of our key vendor partners, providing insight on their latest technology.

Stand L65

Infosecurity Europe brings the information security community together all year round so you can stay connected to your peers and network both face-to-face and online.

Held at Earls Court in London from the 24th to 26th April 2012, it will feature hundreds of leading security vendors, distributors and resellers, and host over 10,000 visitors from the industry.

Registration is free with e92plus, saving you £25, just visit www.e92plus.com/infosec for details.

Stand L65

Delivering **complete network security** with a single appliance

Network technologies are developing fast, but as more and more enterprises conduct business, promote themselves and use cloud services, so come the threats. Once online, their networks face a variety of threats ranging from network attacks, intrusion and spam to numerous viruses, worms, Trojan horses, DoS, DDoS, IP Spoofing and port scanning. Unfortunately, most SMBs do not have significant investment available to invest in enterprise security solutions, especially with different requirements - from the firewall to remote access to outbound content filtering - often requiring dedicated solutions.

The changing nature of the workforce has also led to different demands being placed on the network. The diversified distribution of services, increasing employee numbers or remote sites has led to the central network no longer being the only perimeter, but still the central hub for corporate data and applications.

These remote staff and offices need secure access to the head office, while still managing their own networks, security policies and users. IT departments require the ability to administer the entire network and domain, including access to consolidated reporting, ideally from a centralised interface. With such a diverse network and user profile, ease of administration and enforcement of security while maximising productivity is key.

Who are Huawei?

Huawei is a leading global provider of commercial telecom networks and it is currently serving 45 of the world's top 50 telecom operators. Through continuous customer-centric innovation, Huawei responds quickly to customers' needs with a comprehensive, customised set of offerings.

In 2012, Huawei acquired the joint venture Huawei Symantec, to bring together their full portfolio of network security, storage and computing solutions.

Key facts:

- Huawei's products and solutions are deployed in over 140 countries
- Huawei supports the communication needs of one-third of the world's population
- Huawei Europe has a capable and professional team with over 3,000 employees
- 46% of Huawei's employees are engaged in R&D activities

The solution for many organisations has been to deploy a UTM appliance - a single device providing 'Unified Threat Management' and a range of supporting features. This includes the traditional network firewall with additional modular services that can be added as required.

The Eudemon series have been developed by Huawei for both SMB and enterprise users. They are all in one security products built with industry-leading software architecture, offering full UTM security capabilities of firewall, Anti-virus, anti-DDoS, IPS (Intrusion Prevention System), online behavior management, Anti-spam, URL filtering and VPN solution. They provide comprehensive high-performance security protection against all sorts of threats at the egresses of small and medium-sized enterprises, branches of large enterprises, networks for counties and cities and internet cafes etc. Easy to deploy and maintain, they not only build a highly reliable network connection to keep business continuity but also reduces administration and maintenance costs.

The Eudemon series can serve as a headquarters' networking, branch/ local office/remote site egress gateway, providing diversified VPN, firewall and UTM solutions with 3G and WiFi functions. These communications features give organisations crucial extra resilience - the ability to support multiple internet lines (such as ADSL and 3G) ensure failover in the event of a faulty connection at a significantly lower cost than conventional dedicated lines.

They also support VPN access at any time and any place for employees on business trips to improve working efficiency and lower communication costs. They are able to realise VPN interconnection between branches and headquarters, safeguarding data transmission, facilitating internal resource sharing and offering high-performance VPN hardware encryption to satisfy site-to-site VPN requirements.

A network vulnerable to threats and risks is likely to swamp business with huge disasters and information leaks, with business interrupted and even bankruptcy as a result. A reliable network is at the core of avoiding such potential safety hazards. The Eudemon UTM series are ideal security protection devices for small and medium-sized enterprise networks to ensure business consistency and productivity.

How Europe's corporations are tackling consumerisation in the enterprise

Consumerisation, the trend towards the use of employee-owned devices for work-related activities, continues its inexorable rise. In fact, over 100 new tablets were launched in 2011 and that number is expected to increase in 2012*.
http://tabtimes.com/analysis/ittech-stats-research/2011/12/16/andrew-eisner-over-100-tablets-were-introduced-2011-heres

Along with that, 2011 saw a range of high-profile smartphone launches across the iOS, Android and Windows platforms. Consumers have more gadgets and technology than ever before and are bringing these devices into the workplace, using them to conduct both personal and corporate tasks. It's a scenario that turns the traditional notion of enterprise IT on its head and raises vital issues for senior IT professionals.

There is a groundswell of fear that the risks of allowing personal devices into corporate enterprises are simply too great. Portability raises the likelihood of loss or theft, with the potential for sensitive data to be compromised. Naturally, the existence of corporate data on personal devices opens the door to misuse and insider threats: corporations must balance the need for data security with their employee privacy responsibilities.

Yet here's the conundrum: the potential benefits of consumerisation are widely acknowledged: increased employee productivity; more cost-effective corporate IT provision; and improved employee experiences. That's why many agree that the future of organisations and the ability to meet employees' needs is conditional on the integration of personal and business IT requirements.

It's an uncomfortable reality, and opinion is divided on the best course of action - 15% of organisations continue to apply an outright ban on the use of employee-owned devices for work-related activities. But many others are taking a different line, accepting consumerisation and putting strategies in place to embrace the benefits – while managing the risks.

Our research points to a tipping point in the debate having been reached. 23% of companies surveyed now offer full, regulated access to the corporate network for employee-owned devices, and a further 29% allow restricted use, with some access, such as to email and other applications, though with increased security measures.

Responsibility for the content held on employee-owned devices varies between the countries polled (UK employees bear responsibility as often as their employers; in Germany, less so). However, the reality is that corporations are likely to carry the can should a security breach occur. And the fall out can be costly on several fronts, such as increased regulatory scrutiny, punitive regulatory action, and adverse PR coverage. Perhaps surprisingly, the public sector shows a much higher rate of acceptance of the use of personal devices at work, disproving perceptions that they might be less innovative in their IT strategy.

What does the future hold?
There is clearly an acceptance by senior IT professionals of consumerisation as an ongoing scenario, and recognition that it must be proactively addressed. The challenge for these professionals is to assess their unique company reality, and how they can harness consumerisation effectively, without losing control or compromising the security of their data. The ability of organisations to stay flexible and nimble will be vital to keeping up with whatever new form factor or operating system emerges (such as the new Windows Mobile OS).

For the moment, fear continues to exist over the risks associated with the phenomenon of consumerisation. Our view is that the only way these will be allayed is for organisations to put the appropriate infrastructure in place, with properly briefed employees who have bought into the overall process for the long term. To download the free whitepaper "The Benchmark: How Europe's corporations are tackling consumerisation in the enterprise please visit www.absolute.com/consumerisation

A 10 step approach to tackling consumerisation

If consumerisation is here to stay, what can your enterprise do to ensure effective management? Here's a useful checklist for every organisation looking at their options.

1. Create a simple and clear policy around employee-owned devices.
2. Consider providing a list of supported devices so the scope of the policy is clearly defined.
3. Outline the responsibilities of the employee and the employer.
4. Outline the types of action IT may have to take if a security incident occurs.
5. Have the employee sign off on the agreement.
6. Enforce it.
7. Deploy technology that supports the mobility of consumerisation. Ensure it includes remote management and security capabilities that can touch devices on and off the network.
8. Use the data from each device to ensure it complies with corporate policies.
9. Have a method to quickly and effectively remove the device from the network if a security breach occurs or if it is in non-compliance.
10. Stay current. Keep up-to-date with new technological developments and update this checklist accordingly.

News from InfoSecurity 2012

Complexity and Total Cost of Ownership holds back 2FA

In Q1 2012 Celestix Networks commissioned its first survey into the state of the authentication market in the small and medium market sector.

The survey concluded that the SMB market has not adopted strong authentication to the same level as larger corporations. Alarmingly, 63% of the SMB market has not yet deployed a strong authentication solution and the majority of organizations polled still rely on the static password to authenticate user identity.

As for the reasons for failing to protect against unauthorised access, 47% of SMB organisations cited technical complexity as the primary obstacle to deploying authentication technology. Complexity was viewed as an issue at time of deployment but also from an ongoing management perspective. Complexity was also referenced from the user's perspective, an issue relating to the historic need to carry and use a hardware token.

When selecting a two factor authentication solution it is no surprise that ease of deployment is the number one consideration for the small and mid -size enterprise. But total cost of ownership was also ranked highly with almost a third of respondents citing cost as a primary qualification factor. Cost has traditionally gone hand in hand with two factor authentication due to the need to procure provision and renew physical tokens.

In an attempt to lower the cost of authentication, vendors are now providing a broad range of token free solutions. In an attempt to gauge the SMB opinion of whether these methods would help to lower the barriers to deployment the survey asked whether the availability of mobile device based one time password generation would be of interest. Almost half of organisations polled stated that such a solution would improve user adoption and lower costs.

Finally, Celestix was keen to know more about the state of the mobile device market within the SMB. We found that 45% of organisations had standardised on the Apple iPhone, with Android, Blackberry and Windows Mobile making up the other 55%.

The latest version of HOTPin, the Two Factor Authentication solution from Celestix, is designed to deliver highly secure yet affordable authentication to the market. You can find out more on Stand C40.

Delivering the ultimate in encryption

WinMagic Launches SecureDoc Version 5.3 Full-Disk Encryption with Wireless PBConnex at Infosecurity

SecureDoc v5.3 is the First FDE (Full Disk Encryption) solution with Wired and Wireless Pre-Boot Network Authentication, SecureDoc OSA and Removable Media Container Encryption. SecureDoc v5.3 will also introduce two other key features to simplify data encryption and management: SecureDoc OSA, which provides seamless Self Encrypting Drive (SED) integration, and Removable Media Container Encryption (RMCE), which makes it simple for users to securely transport and share data.

So what does PBConnex offer?

- **Reduced Cost of Ownership** – Users can quickly be granted or denied access to devices based on Active Directory membership easily allowing devices to be shared; password changes/resets take effect immediately in AD
- **Enhanced System Security** - Authenticates the user's access rights against SES and their credential against Active Directory before the OS boots and before the network encryption key becomes vulnerable to attacks
- **Improved User Experience** - Provides single-sign on with Windows credentials, no wait time to access data on other corporate devices which the user has been granted access to, quick and easy password reset. PBConnex is a superior network and device encryption system

"*As a company built on innovation, WinMagic is committed to the constant improvement of our products, whether through new features or basic enhancements that improve the overall user experience and IT management capabilities*," said Thi Nguyen-Huu, CEO of WinMagic Inc. "*With the addition of Wireless PBConnex, SecureDoc OSA and Removable Media Container Encryption, SecureDoc 5.3 once again raises the encryption bar in terms of increasing productivity, reducing IT management and providing a seamless user experience. We are excited to be able to demonstrate these latest innovations at InfoSec*."

Tablets and smartphones: Challenge or opportunity?

Tablets & smartphones are coming - is your network ready?

The proliferation of smartphones and tablets in the consumer space is quickly working its way into enterprise networks. Users are falling in love with their mobile devices and are pushing to bring the convenience and productivity these devices provide into the work place. Laptop shipments have surpassed desktop shipments, smartphone shipments have surpassed laptop shipments, and the number of tablet shipments is expected to grow 1,100% over the next three years. In short, users want mobile devices.

Most significantly, they want their own - and they want corporate network access. 75% of enterprises already have a "bring your own device" policy in place (many include tablets) according to Aberdeen Group, and Gartner predicted that "by 2014 90% of organisations will support corporate applications on personal devices."

Tablet and smartphone challenges for IT

The influx of new devices creates three challenges for network administrators:

1. Maintaining high performance

Most wireless networks were designed as an overlay network to the wired infrastructure and were not designed to support large numbers of users (i.e., high user density). Wi-Fi is a shared medium, so the more devices on the network, the higher performing the network needs to be. This means networks need to be upgraded to ensure sufficient bandwidth and handle the traffic .

2. Creating secure environments

With mobile devices, two main aspects of security need to be addressed. The first goal is to ensure that only the people and devices that need to be on the network are allowed on the network — user authorisation and authentication. The second goal is to be sure that devices getting on the network comply with corporate policies — network access control.

3. Providing appropriate access

Just because a user/device can have access to a network doesn't mean that that user/device should have access to all of the elements of the network. Proper classification and segmentation of the network must be implemented.

Wireless networks designed for BYOD

To handle more end-user devices properly, and to support bring BYOD policies on a wireless network securely, four key steps must be followed. Those steps include:

Design for growth.

As more devices use the corporate wireless network, the network needs to be able to handle the increased utilisation of network resources. This can be accomplished by providing more bandwidth and/or by limiting the bandwidth utilised by each device. It is ideal to provide more bandwidth for end users, but if that is not an option, it may be desirable to restrict user bandwidth to prevent some devices from monopolising the network.

Design for security.

As different types of devices access the network, it must be ensured that the devices and the network are secure. First, network access should be restricted by using proper network authentication and authorisation (802.1x). Second, the network traffic should be encrypted using the latest network security (such as WPA and AES). Finally, client devices should be checked to confirm they are running the latest antivirus software and patches (through Network Access Control).

Identify devices & enforce policies.

Just because a user has the credentials to access the network, that does not mean that user should get access to all of the corporate resources. For instance, a corporate employee on his company-provided laptop may get access all of the corporate resources. However that same employee, using his own iPad, may only be provided access to corporate email and the web. A guest may only need access to the Internet. Xirrus Arrays allow different user groups to be created with each group being mapped to specific VLANs, access control list, and QoS parameters. By assigning devices and users to a specific group IT administrators can easily control who has access to which information from what devices. Xirrus' Device Fingerprinting identifies the devices operating systems such as iOS®, Microsoft® Windows®, BlackBerry®, or Android™ and can then classify the device type such as tablet, laptop, or smartphone. Once the device has been identified, a policy can be applied to control a device's reach and behavior. The device ID, along with the user ID, can be used together to map that instance to a specific user group.

Monitor continuously.

As more devices are brought onto the network, the network should be constantly monitored to verify that all resources are being efficiently utilised. Network traffic should also be analysed to be sure there are no issues or network bottlenecks. As monitoring continues, changes should be made and future growth planned for. As new devices are introduced to the network and new security threats are identified, the cycle should be constantly tweaked to maintain a secure, high-performing mobile network.

Tablets & smartphones: good for business & IT

More and more users are expecting to be able to use their mobile devices at work. Business is working wireless into operations objectives to help increase productivity. IT administrators must be able to support this influx of devices or run the risk of alienating employees and stymieing that productivity. Tablets and smartphones can present a challenge for network administrators, but the opportunities available as they are embraced are significant.

Bringing the power of the cloud to Two Factor Authentication

Identity theft is a big worry for all organisations and individuals and with uptake of tablets and smartphones exploding and data traffic growing at an exponential rate, is now the right time to adopt affordable, automated, cloud-based two-factor authentication?

The increased agility that mobile computing and the cloud bring are commercially wonderful, but they make authentication of users harder. That's a serious problem, because fraud and identity theft are major threats to every organisation and individual now. It is getting to the stage where two-factor authentication is an essential rather than a 'nice-to-have'.

It has fallen into the latter category for many CIOs in the past because it was perceived as being too difficult and expensive. That's simply not the case today. Two-factor authentication is easy, can be delivered as SaaS, and it's totally automated and affordable. If you have not looked at it again recently, maybe it's time you did?

You don't need to be a visionary to see why it's needed. When all digital information was stored in one place, within the data centre, it was relatively straightforward. You simply put a ring of steel around that resource, deployed a VPN and ensured that no-one who was not properly authorised could get in. However, the widespread adoption of SaaS and cloud applications, such as Salesforce, mySAP, Google Docs and Microsoft Office 365 and others, means that, all of a sudden, your intellectual property is in many different places.

Users are accessing data from many different locations – and on a wider assortment of devices which they are demanding the right to use to access corporate data. Apple iPhones and iPads, Android smartphones and tablet PCs – more users logging into the data centre from public places – from airport lounges, in coffee bars and on trains. It is getting much harder to protect digital identities.

Most CIOs will know all too well that passwords just aren't good enough as a form of protection. You can have the very best antivirus software, firewalls and intrusion prevention and detection systems in place, but they are not going to be effective if someone knows how to get into the system – and all they usually need is a current valid user ID and password; that information is, unfortunately, very easy to obtain.

Even if you enforce fairly strict polices and make users change them on a regular basis, passwords provide only a temporary form of resistance against any hacker with the right tools. So why do so many organisations continue to rely on them? Well, they may not feel they have any real choice. They may have looked at two-factor authentication – which provides one-time-use, never-to-be-repeated password access for users – but dismissed on cost or complexity grounds.

But all that's changed. Authentication is now simple, easy to implement and manage (it can be entirely automated in fact), and very cost-effective – typically, it will cost no more than the price of a cup of coffee, per user, per month. It is delivered as a SaaS application so there is no need for expensive and difficult up-front capital investment. One-time-use passwords can be delivered to laptops or tablets or to smartphones, so there is no need to purchase hard tokens or card readers and the service is fully automated to there is no need to tie up valuable IT resources on back-room management of processes.

For a demonstration on how you can use Cryptocard's unique cloud platform to deploy 1,000s of users in 30 minutes, visit the Cryptocard Stand C80.

The unified approach to network security: the end of the multiple solutions era

It's 1pm in the afternoon and you receive a call from your office that the network is down. It needs fixing, but at this precise moment, you visualize an array of appliances, neatly labelled Firewall, Gateway Antivirus, Anti-spam & Anti-Spyware, Intrusion Detection and Prevention, Content Filtering and VPN, all sitting in a row with cables worming in and out of them. Lost in this maze of networking, you look through various reports to figure out what has "actually happened".

Multiple solutions are typically developed and managed by different vendors, which can pose a challenge when it comes to interoperability. The security infrastructure. The solution comes from UTM appliances, delivering comprehensive security in a single product. They leverage a host of tightly integrated security solutions that work in tandem systematically to provide comprehensive network security, with a single centralised platform that allows administrators to monitor and manage their network security effectively.

However, most UTM appliances currently on the market focus only on IP address-based reporting and controls so we know where network activity is occurring, but we're still not sure who the actual user is. As internal and external threats continue to evolve, it's even more important to know who is accessing files and receiving malicious spam who is posing a threat to your network security?

Identity-based UTM solutions address this market challenge, providing the interoperability and operational flexibility that all organisations demand.

Talk to e92plus about how Cyberoam can help provide an effective solution, delivering advanced network security for organisations from SMBs to enterprise.

Flexible, dynamic… but does VDI deliver a secure desktop?

Is VDI the future, or is it here now?

HP recently spread doubt on the future of the PC in their organisation, and IBM gave it the last rites. Server virtualisation is now a mainstream technology, even for SMBs, and the time for desktop virtualisation is here.

This is mainly dictated by purely rational factors: economic, organisational ...and since 2005, the number of virtualised desktops has doubled every year. To date, it is estimated that the market for virtualised desktops is expected to exceed $4 billion. This figure represents the middle range, not taking into account the renewal of projects in many sectors as (or when) investment flows back in the public sector.

Of course, PCs aren't just under threat from thin clients deploying VDI. The explosion of tablets has drawn market share from traditional PCs, and analyst firm Gartner estimates that the worldwide PC market shrunk by 1.1% in Q1 of 2011. Most significantly, that was against a predication of growth. Ironically, one of the few vendors to enjoy an upward spike was the one who made the most disruptive product: Apple. And they aren't a mainstream business solution.

All this has mean that the drivers for VDI have helped grow the market, and solutions have become simpler and easier to embrace. The move from large deployments to branches and SMBs has changed the workplace for many, and VDI has become seen as the most secure solution for the latest trend of BYOD.

Securing the desktop

One of the central benefits of VDI is the ability to deliver a fully secure desktop, centrally controlled and managed. But what is achievable?

It's an issue that includes several parameters, making the task complex by definition:

- Test and deploy security patches (OS and applications)
- Protection at different levels by layers dedicated: web filtering, Anti-Virus, USB port control …
- Data backup

VDI allows you to define models that contain both an operating system and one or more applications. The system duplicates the model to dynamically create virtual PCs as needed. Developments (updates and patches) to applications or operating system are only applied to the models. The concept of complex, manual deployments no longer exists since the operation is performed transparently to create a virtual PC. If a model has evolved, all virtual PCs to it will automatically be updated - guaranteeing a consistent level of safety.

VDI also allows you to define non-persistent virtual PCs that meet their original state at each restart. It therefore becomes possible to offer consistent, fresh desktop to all users - which by definition has the effect of ensuring endpoint security and applications, since all the unwanted application installations or other viruses are gone.

This technology is here now, and VDI is no longer the reserve of enterprise, and dependent on expensive infrastructure. Speak to e92plus about Neocoretech, and how it can deliver secure, flexible and cost effective desktops.

Independent technical advice

It's easy to ask someone "**what product do you want**?", but it takes **good technical and business understanding** to ask "**what do you want to achieve**?"

At e92plus we have over 20 years experience delivering expert technical advice and consultancy on the latest security technologies. Our pre-sales team is customer and solution focused, and able to bridge the gap between the business requirements and the technical solutions by focusing on the requirements of the customer and finding the right solution, what vendor or product is required.

Our pre-sales consultants will be able to help you in the following areas:

- **Recommend products**, services and solutions to meet business requirements - from initial enquiry to evaluation to technical proposals
- Hold **technical webinars**, including product demonstrations
- **On-site visits**, including site surveys and pre-sales consultancy
- Assist with **free evaluations and proof-of-concepts**, including installation
- **Provide guidance on the latest technologies** - from choosing between cloud, appliance or software solutions, to understanding how to secure mobile devices and manage your confidential data

Visit us on Stand L65 to learn more about how we can help support your business.

Delivering more for less
Bringing VDI to the mainstream

As small businesses assess the fall out of the Eurozone crisis and ponder on the long term viability of the UK economy, many businesses are starting a new financial year and developing a business plan to support growth in difficult times. For some, investing in technology will be a key growth strategy for 2012, and for others it will just be a case of doing more for less. Either way, before these technology decisions are made a business has to be sure that each purchase will deliver a return on their investment.

So what should you be looking for? There are significant advances in technology today that allow an organisation to save both money and energy, whilst delivering a first class experience for the user. Many businesses are extending high speed internet access, considering investing in a more mobile workforce or looking at driving down the cost of PC acquisition. However, acquisition is just one piece of the puzzle as ongoing management and support is fast becoming more of a financial challenge for businesses. There are proven alternatives emerging to the traditional 'PC per desktop' model though, such as desktop virtualisation.

The concept behind virtual desktops is simple: today's PCs are so powerful that most people only use a small fraction of their power. Desktop virtualisation enables a single server to power up to 100 users – with each user getting their own computing session. The low entry and on-going costs of this approach to desktop computing access is turning the old economics of PC purchasing and maintenance on its head.

The most attractive benefits of desktop virtualisation come from its low cost of entry, dramatically reduced lifecycle and maintenance costs, and vastly reduced energy consumption when compared to traditional PCs. Most companies save around 75% on upfront acquisition costs alone. It also immediately lowers capex as well as offering longer term opex reductions.
On-going support costs such as installation, maintenance and replacement are also lowered by on average 75% compared to traditional PC environments. Installation time is dramatically reduced because there are far fewer PCs to image and install. A small business with 11 seats can be set up in as little as two hours because only one host is needed. A 30-seat office can be set up in a day because only three servers are needed. IT staff appreciate the quick installation, simple operation, and data security.

Because access devices only draw between one to five watts of electricity compared to a typical PC, which draws 110 watts (or more), companies can save up to 90% on electricity costs. As well as important sustainability issues, a 30-seat office, for example, would save £445 per year in electricity cost – an 89% reduction compared to an all-PC lab.

So, for businesses facing tough challenges trying to keep a competitive edge and continue their own growth, there is no doubt technology can help deliver 'more for less'. In re-writing the rules of PC economics, desktop virtualisation is certainly one solution worth looking into.

Key tips for SMB –
How to get more 'IT' for less:

1. **Don't be afraid to consider new alternatives to the old way of doing things**. Whether it is online tools, alternative applications, or desktop virtualisation to affordably extend computer access, there are innovative, low cost technology alternatives for just about any IT 'problem'.
2. **Extend high speed Internet Access**. It's key that staff have access to the most current online information and tools.
3. **Consider the emerging access devices**. They will be more affordable and easier to maintain making it possible to provide more staff with access to computers.
4. **Consider the cost of a technology** over its entire lifetime, not just the initial acquisition cost. Maintenance, energy consumption, ewaste, and useful life should all be considered when comparing technology alternatives.
5. **Promote online collaboration tools**. These are often free and easy to use.
6. **Take the time to promote online security practices**. This applies for both personal information and network security so that staff know how to use the Internet and online tools wisely.

The leading provider of multi-seat computing and VDI is NComputing, whose solutions range from a simple 5-seat deployment to hundreds of users. For more information on NComputing, and how their products can help deliver cost effective, simple environmentally friendly computing, contact e92plus or visit www.ncomputing.com.

Security solutions

2 Factor Authentication

Anti-Phishing

Anti-Spam

Anti-Spyware

Anti-Virus

Backup & Disaster Recovery

Browser Security

Business Continuity

Cloud / SaaS Security

Content Filtering

Content Security

Continuous Data Protection

Data Loss Prevention

Desktop Virtualisation / VDI

Email Archiving

Email Content Filtering

Endpoint Lockdown & Protection

Encryption for Hard Disks & Removable Media

Firewalls

Identity & Information Rights Management

IM & P2P Control

Internet Link Balancing

Intrusion Prevention & Detection

ISP Load Balancing

Mobile, Tablet & iOS Security & Management

MultiLink VPN

Network Access Control

Patch / Vulnerability Management

Quality of Service (QoS)

Server Load Balancing

SSL-VPN / Remote Access

Unified Threat Management (UTM)

URL/Web Content Filtering Appliance

URL/Web Content Filtering Software

Wireless LAN

Cloud / SaaS security is one of the biggest trends in IT—but is it right for your organisation?

Ask about the options available, from 2FA authentication to web and email security to business continuity.

With data no longer residing purely on the network, providing encryption for mobile devices is not just an option.

Encryption provides security for your data when at rest, and we can help provide solutions that cover Windows, Mac and Linux as well as the latest HD technology.

When the CEO demands you provide network access for his tablet, an effective BYOD policy is no longer a nice to have—it's essential.

Talk to us about solutions that can help secure and manage your mobile device estate, provide users with secure desktops and prevent data escaping.

With tightening budgets but ever increasing threats, how can you protect your network without breaking the budget?

UTM solutions offer comprehensive features in a single appliance, with one interface and reporting engine to help you protect your network, users and data.


e92plus
Your IT Security Distribution Partner
Absolute Software
CRYPTOCARD
experts in authentication
AVIRA
BARRACUDA
NETWORKS
celestix
neocoretech
soft as hardware
Cyberoam
Unified Threat Management
HUAWEI
Lumension
IT Secured. Success Optimized.
NComputing
VASCO
THE AUTHENTICATION COMPANY
QUARRI
websense
WINMAGIC
DATA SECURITY
XIRRUS
Online
www.e92plus.com
Telephone
020 8274 7000
Twitter
@e92plus
Argent Court
Hook Rise South
Surbiton
Surrey
KT6 7NL