

securityplus

IT security news & reviews, exclusively from e92plus



Can social media be safe at work?

How to say 'yes' to Web 2.0 without compromising security & productivity

Inside this issue

The challenge of Bring Your Own Device from laptops to iPads: managing & securing devices with Absolute Software

New vendor partners & solutions - from network access control to clientless security for web browsing

Win with HOTPin 2FA from Celestix Networks

Get rewarded with our new e-centives Rewards Programme

Autumn 2011

www.securityplusonline.co.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 IT Security Distribution Partner.

So far 2011 has been very busy for us at e92plus - as well as being shortlisted again for the upcoming CRN Channel Awards, new vendors have also joined us:

- **Absolute Software's** range include the unique Computrace solution, providing complete data and asset security for mobile devices, from Windows and Macs to Androids, BlackBerrys and Windows Mobiles. Meanwhile, their Absolute Manage MDM product allows full control and administration for iOS devices such as iPads and iPhones
- **Avenda** introduced the industry's first multi-function platform for securely connecting users and their devices to wireless, wired, and VPN networks. They help deliver a scalable identity-aware network access security platform that offers role-based policy control, differentiated access, endpoint health checks, managed guest/contractor access and extensive per-user reporting
- **Quaresso** enables organisations to secure their website for every user: securing the browser and its content needs to be as flexible, seamless and easy-to-use as web applications, so Quaresso extends temporary security controls to web browser sessions anytime, anywhere, without having to deploy client software

Don't forget, SecurityPlus is unique to e92plus - and is available to our reseller partners with your own branding as part of a full marketing campaign. If you are interested in taking part, email us at securityplus@e92plus.com.

Mukesh Gupta
Managing Director of e92plus

Inside this edition

- | | | | |
|---------|---|---------|--|
| Page 3 | The latest security news
We introduce our new vendor partners, Absolute Software, Avenda Systems and Quaresso | Page 11 | Intelligent Data Tiering brings enterprise storage to everyone
Exploring Drobo's unique new feature for storage |
| Page 4 | Absolute helps Camden Borough protect its public sector computers
Helping Camden control their entire laptop estate | Page 12 | Defending the network - Application security & control
The key to an effective firewall is application control |
| Page 5 | Securing mobile devices: An exclusive Q&A with Absolute Software
How to effectively track & control mobile devices | Page 12 | e92plus Technical Support
How we can help support and grow your business with our extensive technical services |
| Page 6 | Barracuda Backup is in tune with the UK Music Academy
Delivering local storage and cloud DR for ACM | Page 13 | The future of Wi-Fi in the enterprise: Xirrus delivers capacity & performance
How to deliver the capacity your users need |
| Page 7 | HOTPin v3 delivers tokenless TwoFactor authentication for everyone
Save time and money with the new HOTPin solution | Page 14 | Need help? How to provide corporate access to smartphones & tablets
A guide to enforcing security while supporting iOS devices, Androids, tablets and more |
| Page 8 | Embrace the social web with Websense - without putting your company at risk
We explore the threats that social media presents | Page 15 | e-centives: Our exclusive new programme
Earn amazing rewards with our new scheme that's bigger and better than ever before |
| Page 10 | Security + Efficiency: Reducing IT admin with WinMagic
Introducing the exclusive new PBConnex feature | | |

The latest security news...

Introducing our new vendor partners

Laptops, Mobiles, iPads...losing track and control of all your mobile devices?

Endpoint security & management from Absolute Software

Managing and protecting your corporate IT deployment (and the sensitive data that flows through it) has never been more challenging. But all it takes is a single incident – a stolen computer or a compromised password – to transform the day-to-day into a disaster. Organisations that choose to do nothing must own the result including significant regulatory penalties and the crushing public relations fallout that can occur.

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.



Absolute
Software

Advanced Network Access Security for Bring Your Own Device (BYOD) schemes

Next generation User & Device Policy Management from Avenda

It wasn't long ago that users were assigned a computer by organisations and that was all that IT departments had to worry about. With the popularity of smartphones and tablets everything has changed - a user can connect to the network from multiple locations, using two to three different devices. The expectation is that each device should work, regardless of a user's role (employees, guests, contractors, etc.) or location or even who owns the device. In the past, NAC was all about the notion of security posture, but now organisations are highly concerned by the identity of the user coming in, and whether it is a known or unknown device.



AVENDA
SYSTEMS

Avenda Systems offers a next generation platform that includes policy management, AAA services, guest access, NAC, device registration, and reporting in one simple to deploy solution for any multi-vendor wireless, wired, and VPN network. This enables policies that can take user roles and device information to enforce network privileges. For example, a guest is allowed to use any device, but may only receive internet access, or an executive may be allowed to use an iPad, but it is not given access to VLANs containing confidential data.

Providing users with enhanced security for web information

Quaresso delivers dynamic browser security to prevent data loss

Companies are deploying cloud services in an effort to contain costs and provide anytime, anywhere access to information. However, IT departments struggle to secure unmanaged devices while Web 2.0 and social media applications are producing financially motivated, targeted threats that are moving quickly to exploit any security gaps they can find and data compliance regulations are increasing in severity.

Current web security has a fundamental flaw as it assumes a security conscientious end user operating a non-malware compromised endpoint in a world with tens of thousands of monthly scams and an estimated 12% to 25% infection rate of computers. Yet highly sensitive information (from customer data to IP) can be easily leaked while malware can compromise web sessions to steal information or credentials.



QUARESSO

Quaresso is a leading provider of on demand web information security solutions that enable web sites and applications to control and protect users' web sessions from theft or data leakage. Our flagship product, Protect On Q, gives enterprises the ability to extend security controls temporarily to web sessions, providing information security and data leakage protection wherever your users are.

Absolute helps Camden Borough protect its public sector computers

The London Borough of Camden serves around 230,000 people living in an area covering inner London, north of the West End and the City of London. Mindful of how some public sector organisations have been criticised for the failure to track computers, especially mobile devices, Camden has implemented a high level of security for its laptops.

The key challenges

- Need to ensure that information is secured against unauthorised access
- Delivering efficiencies by improving asset utilisation
- Streamline mass deployment for IT managers across large estates

Camden chose Computrace®, from Absolute® Software

According to Ian Lawrence, Technical Services Manager at the London Borough of Camden, "Computrace was the only solution that met our standard for achieving the final part of our mobile security strategy. We needed a persistent technology where there was no possibility of the client being tampered with. Now with Computrace, even if someone steals a laptop and makes an attempt to remove the agent, the technology simply rebuilds itself."

One of the challenges Camden faced was not having an accurate record of the number of laptops in the organisation. Lawrence is just completing an audit of laptops and he estimates the Borough has around 2,000, some as old as five years. Computrace tracking information has shown that the Borough's laptops are being used not just in and around London, but as far as Belgium, South Africa, the US and even Korea.

Camden uses Computrace for a variety of functions. These include **remote data delete, which is the ability to wipe the hard disk of a laptop that has been lost or stolen** as soon as the laptop connects to the internet - and theft recovery where a stolen laptop can be tracked and recovered.

Another function is geofencing where geographical boundaries are set for laptops - like those designated as presentation kit in a specific building or room, so that there is an automatic alert if the device goes outside the boundary.



As soon as Computrace was deployed, a feature Camden found very impressive was the speed of roll out. With the Computrace agent already embedded in the laptop BIOS, software activation is managed remotely via the Absolute Customer Centre portal and happens automatically when a laptop connects to the internet. Lawrence says, "When it comes to things like software deployment, there's an 80/20 rule - 80 is pretty quick, but the 20 can take forever. However, with Computrace we were seeing up to 300 Computrace activations coming in every week and in eight weeks we had gone from nothing to 900 laptops with Computrace on them."

Delivering results

"Computrace is a significant benefit to Camden because of the peace of mind it gives us, but perhaps the critical point is public perception," says Lawrence. "If one of our laptops is lost or stolen, we can say it was password protected, it was encrypted and - because of Computrace - we can remove the data, and even have the means to recover it. Being able to demonstrate you have in place the level of protection that Computrace offers, is key for a public sector organisation like the London Borough of Camden."

Another significant benefit of using Computrace has been to give a much more accurate picture of how laptops are used enabling the Borough to drive greater value out of its computer resources. Over a seven-day period, Computrace showed that around 35% of

the Borough's laptops were not being used very effectively. Lawrence can now pinpoint the laptops that are not being used, find out why and, if appropriate, give them to someone who needs a laptop. This has significantly increased the productivity the Borough can get out of its laptop hardware and avoids the need to buy new equipment, when existing equipment is underused.

"Computrace has given us a much better real-time insight into how staff use our laptops. Across the Borough we've got pools of laptops and we found that, perhaps an older laptop wouldn't get used so much, wouldn't be updated and would end up hidden at the back of a cupboard. Also, staff who have a desktop at work might take a pool laptop to work from home, and because there were no means of tracking it, it could stay there and only get used occasionally," says Lawrence.

Using Computrace, Camden can now implement a policy that if a laptop does not connect to the internet for 90 days, it sends an automatic alert and Lawrence can then use the Absolute Customer Centre to investigate why it has not called in and where the laptop is located.

Computrace is also being linked into the leaver process, so that when an employee leaves the Borough there is an alert associated with a laptop they might be using and Lawrence's team can ensure it is returned. The next stage for Camden will be to send messages or alerts to individuals or groups of laptops asking users to bring in a laptop for maintenance or sending out a general security message

- providing complete laptop security.

What results were delivered?

- Automated and reliable installation of Computrace
- Immediately identified that 30% of mobile assets were underused
- Capability added to wipe data from stolen systems

Securing your mobile devices: An exclusive Q&A with Absolute Software

We spoke to Dave Everitt, General Manager EMEA at Absolute Software, about what he sees as the major challenge for organisations in securing confidential data.

The business world is mobile whether that is using Windows based laptops, Apple Macs, iPhones, iPads, BlackBerry's or Android devices. The struggle to track, manage and protect a growing number of mobile devices on and off the corporate network, whilst maintaining data security, is a major challenge.

Although IT departments issue mobile devices with security measures in place, knowing if these are still in place once the device leaves the IT department is difficult. The Ponemon¹ Institute reported that the human factor is the major challenge with up to 50% of end users disengaging security solutions, 65% writing their password on paper (which is often included in the laptop bag) and 86% reporting they had a laptop lost or stolen. Companies need to protect their devices and the data they hold to ensure they aren't faced with potential fines of up to £500,000 from the Information Commissioner's Office (ICO).

As companies are becoming more mobile, what advice would you give to those organisations that don't have an accurate picture of their IT estate and the risks they face?

Every year regulations are tightened, penalties are increased and public trust is impacted when sensitive data is compromised. With the average cost of a data breach in the UK costing £1.9m² IT departments need to become more proactive in their approach to IT security to stay out of the headlines.

I would advise a layered approach to security which would enable companies to protect important data, utilise asset tracking solutions to determine hardware and software status, and provide the ability to take action when a risk has been identified. Adopting such a security policy is a requirement to ISO/IEC 27001 accreditation, a standard that demands a coherent and comprehensive suite of information security controls.

What is the best way for IT to gain control in this increasingly mobile environment?

IT will always be accountable for data security and ensuring optimum performance of devices, data integrity, availability and compliance. A regular ITAM solution may be able to manage patches and prevent unapproved applications being installed, but these devices, by their very nature, are rarely on the corporate network so out of reach of IT. With fewer resources to manage a complex environment and serious breaches caused by unmanaged endpoints, a fundamental component of gaining control is knowing where your devices are.

How does Computrace by Absolute Software deliver ROI to the user?

Absolute[®] Software is the leader in firmware embedded endpoint security and management. Our solutions provide IT organisations with comprehensive visibility and control over all of their devices. We deliver cross platform endpoint security and lifecycle management solutions that reduce costs, prove regulatory compliance, combat theft, and optimise productivity.

Through our partnership with leading computer manufacturers, the Computrace[®] persistence module is in the hardware, embedded into the BIOS or firmware at the factory. Once a software Agent is installed and activated, our customers enjoy a level of persistence that is virtually tamper-proof, the hardware agent repairs the software agent if missing! The delivery of a hosted service requires no additional infrastructure and the console can provide automated alerts and reports.

Computrace provides customers with an interactive environment where they can remotely manage their assets based on the daily information received from each device. In addition, if the device goes missing the hosted server can be instructed to take action such as freezing the device with a custom message or deleting files, folders and hard drives.

The user can also choose to accept a forensic tool that allows Absolute Software's theft recovery personnel to



work with local Law Enforcement to actively monitor, gather data and recover the device through forensics and legal processes.

What is your top tip for IT Security professionals?

Quite simple, it's to include Computrace with every build in their mobile IT estate, helping them to:

- Regain control of their multi-device environment
- Reduce costs through improved efficiencies
- Mitigate risk across their organisations
- Deter & respond to devices at risk

Whether the device is on or off their network, the IT Security professional can stay in contact with their IT estate providing them with the ability to take action when needed. The unique tamper-resistant technology helps to ensure that the solution remains on the device when its needed most. Absolute Software is the best way to track, manage, and protect your digital world.

1. 2010 Human Factor in Laptop Encryption UK Study
2. Ponemon Institute: Data Loss Report March 2010

Barracuda Backup is in tune with the UK Music Academy

Barracuda will provide storage and backup support for disaster recovery capabilities in support of critical media and audio content for the Academy of Contemporary Music, based in Surrey. The Academy of Contemporary Music (ACM) has selected the Barracuda Backup Service to house and store its media, audio and video content, as well as provide disaster recovery functionality for all critical data.

ACM, located in Guildford, Surrey, has been a world leader in music education for more than 15 years, providing students with a range of courses in instruments from guitar to keyboards, music production, tour production and the music business. With more than 1,200 full time students in the UK alone, plus schools in South Africa, Europe and USA, the school produces large volumes of music and video files all of which need to be stored.

Prior to the Barracuda Backup Service, all data was stored via tape drives, which were attached to individual servers. This process presented challenges to ACM as it did not have adequate staff resources or IT capabilities available to support the volumes of data being produced within the school.

"The music industry has changed so much since we first opened ACM," said Simon Mallindine, IT manager at ACM. "The volumes of data being produced daily were incredible and as we grew in size so did the volume of data. We simply didn't have the infrastructure in place to cope. We compared the cost of using tape versus purchasing the Barracuda Backup Service and found that over a three-year period the Barracuda Backup Service is one-third the price of backing up data to tape."

With so many students attending the UK school, access to data on a 24x7 basis is critical so, with this in mind, information is regularly updated and added to the servers. In the event of failure or loss of data, the school needed total reassurance that not only could information be retrieved, it could be done so in a timely manner with minimal impact to the students.

view the demo at
www.securityplusonline.co.uk/Barracuda



Why is effective off-site backup so essential?

- 43% of business who close after disasters never reopen
- Compliance requirements require off-site backup

"Within ACM we create massive amounts of data on a daily basis," said Mallindine. "The type of data we produce are the student's thoughts and inspirations, this is not always easy to recreate if lost. Therefore we need total confidence in not only our IT infrastructure but also the technical support we receive—through Barracuda Networks, we have this."

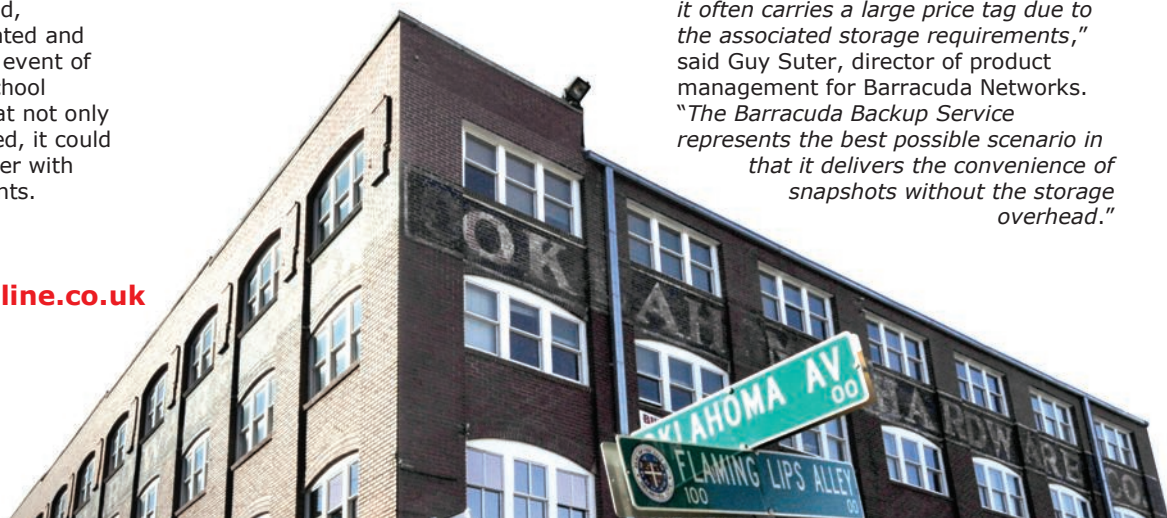
"The technical support we continue to receive has hugely exceeded our expectations," continued Mallindine. "In the event of technical issues arising we have been able to speak to a Barracuda Networks engineer directly who has been able to dial into our system, with minimal impact to our IT infrastructure and fix any problems within a 72-hour period, and all that's needed is one phone call. Support like this is truly amazing and gives us such confidence from an IT perspective."

In addition ACM, has conducted disaster recovery tests, whereby all critical data was wiped from the database and restored all within a nine-hour period. For Mallindine, this was critical to the success of the project.

"If we lose data at 6pm. we can have all our critical data back and be fully operational, even with the images for our servers, before the doors open for teaching the following morning," said Mallindine. "We can't emphasise how impressed we've been and we plan to roll out Barracuda Networks technology in each of our franchises over the next few years and we'll manage this centrally. We won't need to get on a plane or have local IT support in place, we can essentially use Barracuda Networks' local IT engineer to deliver an excellent product to our franchisees, as well as excellent service and support, that's the sort of company we like to work with."

With the Barracuda Backup Service, ACM can safely maintain backed up data using efficient replication techniques designed to conserve bandwidth and minimise the cost of disaster recovery.

"While traditional disk-to-data snapshot technology eliminates the complexity of restoring full and incremental backups, it often carries a large price tag due to the associated storage requirements," said Guy Suter, director of product management for Barracuda Networks. "The Barracuda Backup Service represents the best possible scenario in that it delivers the convenience of snapshots without the storage overhead."



HOTPin v3 delivers tokenless TwoFactor authentication for everyone

Security breaches and criminal activity no longer target just larger corporations. Organisations of all types and sizes are at risk from the increasing range of threats brought about by the proliferation of consumer technology in the workplace and the availability of tools on the internet.

Ensuring security is often perceived as complex and costly. In a recent survey nearly half of small and medium business owner's cited complexity as a primary reason for not implementing sufficient levels of protection.

Why TwoFactor Authentication?

- 64% of people will exchange passwords for chocolate
- 29% of staff know their colleagues passwords

Further- more it is an alarming fact that in the same survey 45% of those polled also stated that their company was too small to be a

target for hackers or data/identity thieves. Of equal concern should be the fact that corporate devices are still the most vulnerable endpoints from which attacks may be launched.

With the increasing impact of regulatory compliance for data handling the cost of remediation is no longer about fines alone but rising operational costs and potential negative impact to reputation.

Deploying TwoFactor Authentication to enforce security for users

Celestix Networks recognises the need for security at organisations of all sizes and have developed a portfolio of complimentary solutions that meet the needs of most modern businesses.

By deploying TwoFactor authentication, organisations are no longer vulnerable to the weakest link in the network security: the user. By removing insecure static passwords, access to the network (in particular through remote methods or on lost/stolen devices) is controlled and

secured, and able to be fully managed by the IT department. HOTPin v3 from Celestix Networks is a TwoFactor authentication solution that enables organisations to deploy tokenless authentication but without the complexity and costs associated with physical token solutions.

HOTPin uses soft tokens on smart devices, the SMS network, email, and clients for Windows and USB sticks in order to generate One Time Passwords (OTPs). This gives organisations the ability to select the most suitable means of pin generation based on their user base.

HOTPin consists of an authentication server that comes with RADIUS embedded as standard, simplifying the initial deployment and allowing HOTPin to be used with any leading remote access technology such as Celestix WSA appliances and Juniper SA series.

Provisioning of the service to users is straightforward. With a range of provisioning options including the iPhone appstore, Android marketplace or through the inbuilt provisioning website within HOTPin, initial administration to networked or remote users is easy.

HOTPin licensing is simple to manage with a single user license covering either the use of OTP through soft token, SMS, or USB/PC client.

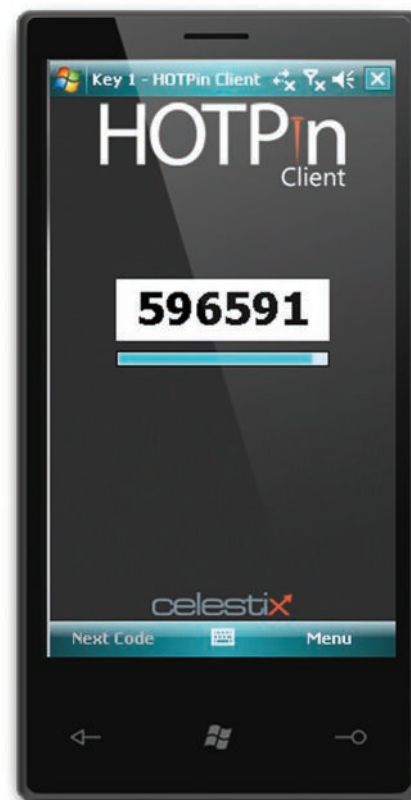
Why tokenless authentication?

User satisfaction and productivity will increase as they are no longer dependent on a distinct physical token that may expire, fail, or be lost, leaving the user with no means of access.

Statistically users will realise the loss of a phone within 15 minutes, compared to over a day before a physical token is missed. This means HOTPin users should be returned to service faster than those requiring a

Why tokenless Authentication?

- Quick and easy deployment
- Lower upfront costs & TCO
- Simple message customisation



physical token replacement. With the flexible deployment options for HOTPin a PC/Mac client could be used as a backup whilst a replacement handset is sent to the user.

Capital expenditure will be reduced because the laptop or smart device has already been accounted for. HOTPin offers flexible yearly licensing models to meet changing business needs. There is no physical token to procure, replace and renew resulting in a powerful reduction in the total cost of ownership.

Celestix Networks promotes green computing and the agenda to reduce carbon footprints and we see HOTPin helping organisations to meet corporate objectives for efficient computing.

HOTPin delivers an excellent combination of features, benefits and value to businesses of all sizes. Our solution ensures that companies can take the appropriate measures to secure their valuable assets without breaking the bank or compromising on quality.



How to embrace the social web without putting your company at risk



The inexorable rise in social media and Web 2.0 presents a new and dynamic threat to organisations. But can IT say 'yes' without comprising security, data and productivity? We spoke to Websense to find out.

What are the advantages of Social Networking, especially from the enterprise point of view?

When many people hear the term Web 2.0 they think it's only about social networking, sharing personal updates on Twitter, or watching funny videos on YouTube. The reality is that many businesses have already discovered valuable uses for Web 2.0. Businesses that are still trying to block employee access to Web 2.0 sites are missing opportunities. However, they need to have the right security policies and technologies in place in order to allow safe use of Web 2.0 while helping to drive collaboration and information exchange among employees. It can streamline communication and processes, allow businesses to interact directly with customers and key stakeholders, and can even be used for new ways to generate revenue.

The use of Web 2.0, like social networking and Twitter, is ubiquitous among consumers but more and more businesses are now taking advantage of Web 2.0 sites in new ways to interact with their customers and partners. In fact, a survey conducted by Websense reveals that the 1,300 IT managers from large companies around the world found that 95% of businesses already allow

access to some types of Web 2.0 in the workplace and 30% report feeling pressure from C-level executives to allow more access to Web 2.0 sites. Despite these risks, IT professionals can no longer simply block access to Web 2.0 since 62% of IT managers feel that Web 2.0 is necessary to their business.

How can companies leverage Web 2.0 networking tools?

Ways that businesses benefit from Web 2.0 include:

1. Improve collaboration and information exchange among employees
2. Streamline communication and processes
3. Gain market insights by having a window into customers
4. Interact directly with customers and key stakeholders
5. Find new ways to reach consumers to sell products and services

Can Web 2.0 help businesses?

Yes, it helps - and there are some great examples of how businesses and government organisations have successfully used Web 2.0. These show the benefits of Web 2.0 and prove that businesses can no longer simply say "No" to Web 2.0:

Dell says Twitter has produced \$1 million in revenue over the past year and a half through sale alerts. People who sign up to follow Dell on Twitter receive messages when discounted products are available the company's Home Outlet Store. They can click over to purchase the product or forward the information to others.

Kimberly-Clark Corp. has an online community for users and potential users of its Scott personal care products. Kimberly-Clark

now links data compiled on its community site with customer profile information, helping it identify its most loyal customers and market products to specific segments (such as parents whose children are ready to move from Huggies nappies to Pull-Ups).

What kind of security measures should be adopted to securely use social networking sites for business?

IT managers need to be able to say 'Yes' and embrace Web 2.0. However, they need the right policies and security solutions in order to ensure they organisation and its data it secure - for example, real-time analysis and categorisation of specific web content. This means that social media can be allowed, but just the malicious or inappropriate content is blocked, not the entire page or site. They need the ability to detect dynamic threats "on the fly" because Web 2.0 sites change constantly and can be compromised at any moment. Finally, they also need data loss prevention technology to prevent their intellectual property and confidential data from being accidentally or intentionally shared on a Web 2.0 site or used in ways that it should not.

IT managers can learn more about the state of Web 2.0 security and whether their current security stature is really enough by reading the IDC white paper on best practices for Web 2.0 in the workplace and by attending the webinar. Visit www.websense.com/Web2.0atWork for these tools.

They should also begin educating their employees about Web 2.0 usage policies and the risks that can come from rogue use without IT's knowledge or support. The right security solutions can allow IT to enable employee use of Web 2.0

"80% of websites with malicious code were legitimate sites that have been compromised"
Websense Threat Report





without worry. The Websense Web Security Gateway provides real-time analysis and categorisation of specific Web content on a page allows businesses to block just the inappropriate or malicious content, not the entire page or Web site. Only Websense, with the ThreatSeeker Network and the technology acquired from Defensio provides a Web 2.0 early threat outbreak detection and protection system by analysing content posted to Web 2.0, social networking and blogger networks as it's posted that gives Websense customers protection from risks before they propagate.

What are the disadvantages?

The growing use of wikis, blogs, and other Web 2.0 tools that allow user-generated content in business has created ample opportunity for cybercriminals. Hackers are increasingly targeting legitimate Web sites with 71% of sites with malicious code being existing legitimate entities.

Some IT professionals appear over confident in their security—a dangerous security gap exists when it comes to Web 2.0 threats. They need to understand the unique risks and how to protect their networks and essential information.

Businesses must balance the benefits of Web 2.0 with the potential information security risks. Because sites like wikis, blogs, and social networking sites allow user-generated content, anybody can easily embed data-stealing spyware or post spam comments and links to malicious sites or non-work content.

companies stop that while not putting a ban on social networking sites as such?

Social media can have potentially negative aspects for enterprises. A survey conducted by The Social Development Foundation of the Associated Chambers of Commerce and Industry reports that employees in the workplace spent on average an hour a day on sites like Orkut, Facebook, Myspace and LinkedIn, leading to a loss in productivity of nearly 12.5%.

Productivity is only one issue affecting a company and yet this is often being allowed to overshadow other concerns such as security. Companies need to stay competitive, attract the best employees and use the right tools for the job. With the right security and policy settings you can not only keep your company and its essential information safe, but you can empower your employees to use Web 2.0 tools at the right times and for the right purposes. For example, the marketing department may need to use Facebook or Twitter to promote the company and so have full access, while another department could be granted access to Facebook for personal use during the lunch hour. This can all be managed easily with real-time security and a realistic internet access policy. The result is that employees are happy and productive, they can all do their jobs and more importantly the company is safe.

What are some of the challenges faced by companies that allow access to social networking?

Though many organizations already allow access to some types of Web 2.0, a dangerous security gap exists. In the recent Websense Web2.0@work survey, the majority of respondents reported feeling confident in their organisation's Web security, though they admit to not having the necessary security solutions to protect from all threat vectors. Additionally, a surprising number of respondents appear to be confused on what exactly constitutes Web 2.0 – and what they don't know could put their organisations at risk. The survey also revealed the following:

“Data loss via the Web is 4 times more likely than over email”

Open Security Foundation
Data Loss Database

- 80% of respondents reported feeling confident in their organisation's Web security, despite the fact that the numbers show they are ill-equipped to protect from Web 2.0 security threats:
- 68% do not have real-time analysis of Web content
- 59% cannot prevent URL re-directs
- 53% do not have security solutions that stop spyware from sending information to bots
- 52% do not have solutions to detect embedded malicious code on trusted Web sites
- 45% do not have data loss prevention technology to prevent company confidential information from being uploaded to sites like blogs and wikis or leaked through spyware and phishing attacks

There is even confusion among IT professionals about what constitutes Web 2.0, with only 50% correctly identified wikis, video uploading sites like YouTube and hosted software/cloud computing sites like GoogleDocs to be Web 2.0.

Meanwhile, 47% of respondents report that users in their organisation try to bypass their Web security policies.

Websense have made available a template that allows you to create your own Acceptable Use Policy that includes employee use of the social web. To download a copy, and for further information on securing the social web in the work place, go to <http://ow.ly/5VbnE>.

“When it comes to the social Web, business has no choice in the matter - it's a must in today's competitive economy”

There is a perception that employees spend most of their time socialising rather than focusing on work. How can

Security + Efficiency: Reducing IT admin with WinMagic

As regulatory requirements continue to burden IT organisations, IT managers struggle to contain costs and complexity while protecting users and maintaining compliance. WinMagic's new PBConnex dramatically improves control, security, and visibility while reducing the complexity of encryption for end users.

WinMagic's revolutionary PBConnex utilises network based resources to authenticate users, enforce access controls, and manage end point devices before the operating system even loads. This unique and ground-breaking approach to Full Disk Encryption (FDE) management results in significant cost savings by streamlining both IT management and end user functionality.

Previously IT Managers and Administrators were faced with two problematic options when using pre-boot authentication for encrypted PCs:

- Enable pre-boot authentication for all devices thereby creating complexity in user provisioning, password management, policy changes and software updates
- Bypass pre-boot authentication altogether with "autoboot"; creating possible exposures to privacy issues and data breaches

PBConnex enables users to get the convenience of autoboot with the security of pre-boot authentication. WinMagic is the first FDE vendor to integrate secure network support into the pre-boot environment.

PBConnex authenticates users against Active Directory (AD) and authorises them against the SecureDoc Enterprise Server (SES) via the network before the encrypted data is read off of the drive. This means that the Active Directory (AD) administrator can control user

access to encrypted machines anywhere at any time, removing redundant and inefficient network management steps and increasing end user productivity. This delivers a minimum of 15% reduction in FDE total cost of ownership.

Ease of Provisioning

Temporary, remote and multi-workstation users can quickly and efficiently be granted or denied access by adjusting the group membership in AD. Therefore users can be supported on shared devices automatically, or granted access to specific machines without duplicating work in the SES.

Remote Management

Administrators can remotely manage encrypted laptops with real time user revocation. This also provides the capability to execute pre-boot authentication for remote computers, thus enabling secure unattended software updates overnight.

Improved Control and Password Resets

Encrypted laptops can now be supported as easily as unencrypted laptops when PBConnex is in use. PBConnex eliminates expensive and time-consuming calls to FDE administrators to re-establish password credentials. By synchronising encryption passwords with AD, a user or administrator can immediately update their password and login to a specified device. By working directly with AD, lengthy and costly delays are eliminated for password lockouts, resets and more.

Enhanced Security

With autoboot, protection is reduced to what is provided by basic Windows security, where the data encryption key

has already been exposed in the computer's memory. PBConnex avoids these issues by authenticating the computer to AD before the OS is booted and before the encryption key is vulnerable.

Policy Protection

PBConnex enables a defined group of staff to be enabled for secure access to workstations, laptops and mobile machines from a powered-off state – while ensuring users who do not belong to the defined group cannot access these devices.

If devices are taken off the network while the data is at rest, with PBConnex authentication they can't be accessed at all – ensuring total protection of any information and denying access to Windows or down-stream server applications.

Staff can have secure shared workstation access via groups in AD with single sign-on using the Windows password thus ensuring full confidence that no one else can access their Windows session and ensuring confidentiality remains intact.

In short PBConnex addresses the long-standing issue of network administrators not being able to access and administer encrypted endpoint devices in a simple and efficient fashion. PBConnex decreases the total cost of managing encrypted devices enhances overall security and provides a user experience where the protection of FDE is truly transparent. What could be better than that?

find out more at
www.securityplusonline.co.uk/WinMagic

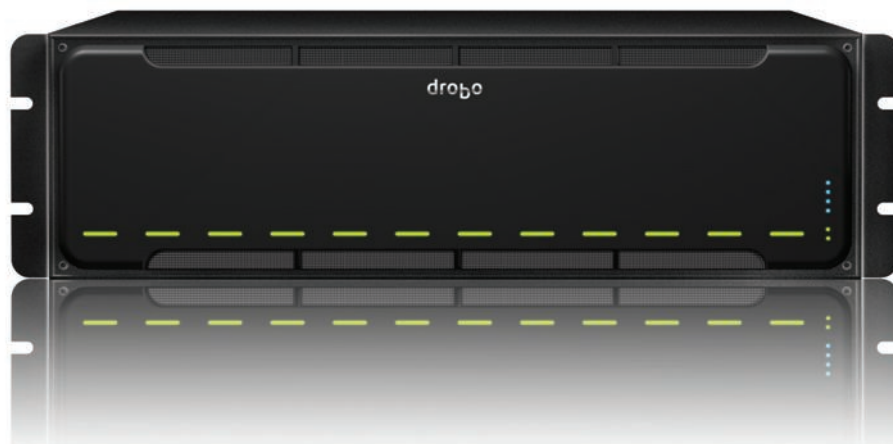


Intelligent Data Tiering from Drobo brings enterprise storage to everyone

Designed for applications like VMware, Microsoft Exchange, and backup for small and medium businesses, the Drobo B1200i offers a fundamental IT breakthrough with the new Drobo Automated Data-Aware Tiering technology. This innovation enables Drobo to automatically optimize performance over a mix of SAS and SSD drives within a single chassis. Performance levels adapt to workloads in real time (no knobs, no tuning, no waiting), making it truly application-driven, not admin-driven!

The Drobo B1200i includes:

- 12-bay SAN (iSCSI-attached) capabilities, with dual redundant power and other hardware redundancy
- Patented BeyondRAID technology for the world's most automated data protection
- Drobo's thin provisioning and thin reclamation capabilities to optimise your capacity and expandability needs



How do small and medium business IT administrators effectively use solid state drives (SSDs) to accelerate their applications? They can't. Either the array is too expensive (more than £20,000) or, even if the SMB-focused arrays allow SSDs to be used, they must be in their own pool and separate from the rest of the data. Data must then be manually sent to the fast volume (SSD) or to the normal volume. How is the IT admin supposed to figure out what data is transactional in nature, that is, what data should be sent to the fast volume? And often data has mixed characteristics, making this operation even more confusing and complicated. To get the most out of expensive SSDs, the solution must be intelligent and fully automatic—the data just needs to go to the right place automatically.

A Drobo is a single pool of drives by design. The user does not need to think about pooling drives or creating RAID groups. Also, drives of different sizes and types can be used in a Drobo. These advanced technologies make Drobos ideal for allowing SSDs and hard disk drives (HDDs) to work together optimally in the same chassis – automatically!

Being Data Aware

As data enters the Drobo, even while it's still in flight, it's already being

examined without performance being impacted. An additional check has been added to see whether or not the data is transactional in nature. If it is transactional, then the data is written to the faster tier of SSDs.

Leading enterprise storage arrays that offer tiering capabilities can cost more than £20,000, but even then, they are not always aware of what type of data is being stored.

Drobo's tiering functionality allows you to store any type of data on the Drobo and the data that can be optimised by SSDs is automatically optimised in flight. This means that any data—mixed data types **from 10 or more VMs in a vSphere cluster, Exchange databases/datastores, backup data, or files on a file server**—automatically goes to the right place.

With Drobo automated tiering, optimisation of data doesn't stop when the data reaches a transactional or bulk storage tier. As the stored data is being read off the Drobo, the data is patterned. If data on the bulk tier is frequently

read and begins to look more like transactional data, it will be migrated to the transactional tier. If data on the transactional tier becomes "cold" with very few or no read requests, it will be migrated to the bulk tier. These migrations occur in the background when the storage is not under high load and do not require any administrative interaction.

Tiering Without SSDs

Even when a Drobo doesn't contain SSDs, Drobo still puts its automatic tiering feature to work. Without SSDs, the advantage of tiering is to eliminate the write penalty when parity data is created.

Even when all HDDs in the Drobo are the same, Drobo lays out zones differently on the transactional tier than it does on the bulk tier.

For example, mirror zones are more optimized for writes and stripes are more optimised for capacity. Leveraging BeyondRAID technology, zones are automatically created and altered on the fly to optimise the Drobo for the type of data you store on it.

"As well as applications, Drobo is ideal for building a server virtualisation cluster and has been certified for VMware vSphere and Citrix Xen Server environments"

Defending the network with Cyberoam - Application security & control



With the advent of the cloud and hosted applications, tradition in network security doesn't hold up well. Applications residing "inside" the network would be "outside" on the cloud, competing for the first time with external applications for bandwidth.

This has meant that the challenge of managing cloud application access and control becomes far more complex. Yet organisations need to move out of their traditional siloed thinking that fit the era of perimetered networks. Firewalls need to open themselves to solve emerging requirements by going beyond straight forward rules to provide granular controls that apply QoS by applications and users.

The Cloud Age Challenge of Applications

At this point, organisations woke up to the fact that access to applications must be controlled not just for vulnerabilities but also for the terabytes of bandwidth they consumed and subsequent productivity loss. It's a variety of personal, professional, collaborative and entertainment applications that are causing traffic and security challenges: SaaS applications like Salesforce, collaboration tools like Microsoft Sharepoint and Google Docs plus media like Facebook, Twitter and YouTube.

Firewalls Aren't Just About Security

Traditional firewalls paid attention to the source and destination address, the ports and protocols. It didn't matter which packet was entering or leaving the network if it met the set parameters, or if the destination or source was accepted. However, the rise of port blurring added to the complexity of application control. Of critical importance is the fact that firewalls could no longer expect applications to follow a standard port-protocol combination, and greater intelligence was needed to analyse the traffic and not just the port or IP address.

Hence, managing the 4 elements of who (user), which (application), when (time) and what (bandwidth) become necessary to enhance productivity and control costs at the same time.

For example, Salesforce or Microsoft Sharepoint would always require priority in access, iTunes a decision of limited or no availability, and the user is key on granting access to IM or LinkedIn.

Cyberoam UTM appliances have built-in identity based security, allowing the organisation to define the minimum bandwidth needed for the application and apply the firewall rule accordingly, setting the highest priority to these bandwidth critical applications - and even adapt them with even greater control, such as the time of day.

Complete control is provided meaning any application (from iPlayer to GoToMyPC) can be intelligently and dynamically handled, understanding the mix of business and personal use as well as understanding the individuals role and pre-defined allocation or policy.

It means that organisations can now effectively and automatically control traffic in and out of their network without effecting business critical processes - and without compromising security.

e92plus Technical Support

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?" The e92plus pre-sales team is customer and solution focused, and able 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

Don't forget, we offer **Inclusive Installation with every order or evaluation** - that one day of on-site consultancy with an e92plus Engineer worth £975. We also provide a free Security Healthcheck with every renewal you order through e92plus, to ensure that your customer's solution is fully working and optimised for their environment.

Don't forget, for our Reseller Partners we offer **unlimited, free technical support** - ensuring you have the knowledge and support you need to sell and support your products.

find out more at www.securityplusonline.co.uk/e92plus



The future of Wi-Fi in the enterprise: Xirrus delivers capacity & performance

Within the next 5 years, wireless networking will become the primary network connection within the enterprise, driven by an ever-increasing number of wireless computing devices and mobile applications. Consumer adoption of Wi-Fi enabled smartphones, tablets, netbooks, and notebooks is forcing IT to look beyond just security and manageability of their WLANs and think seriously about the scalability, density planning, and overall user performance of their wireless services. But how can an organization implement and scale a wireless network that will deliver the same quality of service as the predictable wired network?

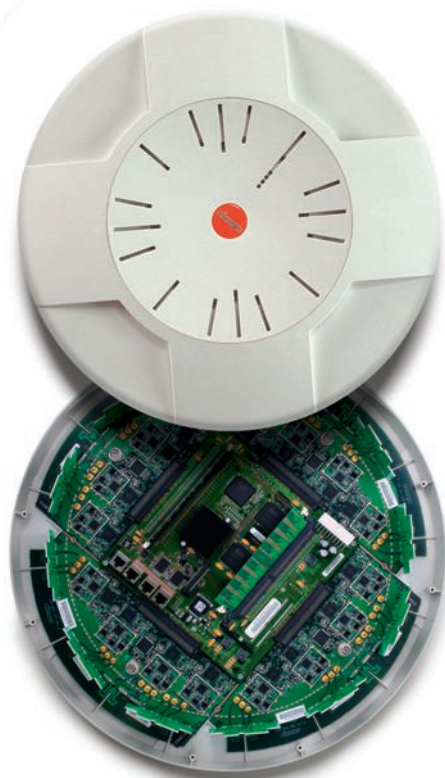
We all know that today's workforce is connected 24/7 and that technology is a critical component to how people communicate and transact on a daily basis. Businesses need to remain connected to their customers, servicing them when and where customers want. Schools need to obtain and share information with students across campuses worldwide, enabling real-time collaboration. Hospitals need to access patient records at a moment's notice, delivering better and more accurate care. Shipping ports need to track and secure containers of goods coming on and off ships, improving efficiencies and security.

The way in which we work has changed and this shift to mobility is driving a new standard for enterprise networking – one that is convenient and flexible for employees, guests, students, patients, and clients. Within the next 24 months, 60-80% of enterprise employees will rely upon wireless connectivity for their business-critical applications. Further, these people will have not one wireless device, but two or three – many are already carrying an Android, iPad, and notebook computer. Whether they are connecting to local data centers or cloud-based services, the vast majority of these devices are shipping without Ethernet ports, making wireless the de facto connection.

As this consumerisation of IT rolls forward, the demand for 24/7 mobile connectivity must be seriously thought-out, planned, and delivered. For example, many organisations were caught flat-footed with the abrupt adoption of the iPad this past year – working hard to catch up and provide a positive and secure environment in which these devices can operate has taxed many IT departments. IT needs to

remain agile and stay ahead of the mobile workers – to continue to plan and drive the change within their networks.

The manner in which WLAN networks have traditionally been deployed is flawed. The days of hot spots or overlay networks using two-radio home access points is over. These two-radio access points should be used in the home where they support a handful of people and devices, not in an enterprise supporting hundreds or thousands of users.



The days of only deploying WLAN strictly for coverage, security, and manageability has now been resolved with existing 802.11 standards. For example, with the existing 802.11 security standards, all the main WLAN vendors have a solution that resolves those concerns. Even the US Marines have deployed a WLAN for mission-critical top-secret network connections. Certainly, those standards should remain part of the planning criteria. However, the key is that IT must now focus on performance – the ability to deliver high-speed network access to thousands of users wirelessly – to support more users, deliver more bandwidth, provide a positive experience

for everyone, and keep costs under control.

The need for greater control over your Wi-Fi network has also increased. With a proliferation of wireless networks, as well as the ability for users to create their own instant 'hotspots', requires IT to be able to retain full control on who can access the network, with what device and to be quick to recognise and eliminate potential threats.

The answer to density and performance is simple – add more radios to the air – just like you add more switch ports for wired users. The cellular phone industry learned this years ago when they moved away from installing omni-directional radios to installing an array of directional radios. We need to think and plan for WLAN capacity like we do the wired network – calculate how many client devices you'll need to support and deploy the appropriate number of radios.

Some critics site that by putting more radios in the air, one creates a huge collision domain because Wi-Fi is a shared medium. Another problem that was resolved by the cellular industry – by integrating radios with directional RF patterns in a circular pattern, they were able to deploy more radios to support more clients and deliver more bandwidth.

Giving users the freedom to connect when, where, and how they want doesn't need to be difficult, time consuming or costly. Microsoft Events actually is saving money deploying Wi-Fi at their events, as is the Port of Houston and Carnegie Mellon University. Delegates expect high quality Wi-Fi - that's why Microsoft needed to be able to deliver outstanding performance as well as capacity for 3,000 people in a single room and reducing the number of Wi-Fi devices by nearly 90%.

The only Wi-Fi vendor able to deliver this performance, capacity and success is Xirrus, through their unique Wi-Fi Arrays.

WLAN is not only secure and manageable, but if done correctly will increase the mobility, productivity, and overall quality of service for the user. Stop deploying and reconfiguring costly-wired networks – deploy a secure, scalable, and cost-effective wireless network.

Need help? How to provide corporate access for smartphones & tablets

More of us have smartphones than ever before – and we want easy access to corporate email. The key challenges are around security and deployment. How can you provide access without compromising the network, while still making the experience for the users a productive one? We explain how.

Mobile email and ActiveSync

With the increased popularity of smartphones - especially the Apple iPhone, and increasingly Google Android devices - in both personal and corporate environments, it was inevitable that there would be an increase in the requests for access to corporate email on these devices. Rather than having to access corporate mail services through a secure remote access portal which is especially inconvenient on a mobile device, the sophistication of smartphones and multiple mailboxes makes access simple and convenient for the users. Microsoft use a protocol called Exchange ActiveSync (EAS), which allows mobile devices to synchronise data with Microsoft Exchange email servers. This is sometimes referred to as "push email", as the Microsoft Exchange server will relay the emails to the mobile devices, providing instant email on the go.

The Advantages of Mobile Email

There are many advantages to this solution, as it gives users access to their emails almost immediately. There is often an increase in productivity as emails can be dealt with almost immediately. It also saves the need to either log into the corporate VPN or Outlook Web Access site via a laptop or computer.

The device options include almost all smartphones and tablets, such as iOS for iPhones and iPads, Google Android, WebOS and Microsoft Windows Phone.

Microsoft Server Integrity

With this level of convenience, the security concerns should be highlighted as well. The mobile devices need to be able to communicate with the Microsoft Exchange Server, in order to be able to synchronise emails. The concern is that a direct communication tunnel can be opened up from the internet straight in to the corporate Microsoft Exchange Server.



Data Protection and Data Loss

Compliance requirements are more prevalent in our working lives, but we should be aware that the Data Protection Act and the Information Commissioner's Office state that personal information should be encrypted. By not implementing effective measures organisations could be subject to a £500,000 fine, on top of the significant impact of negative publicity. Plus, there is the very real possibility of any lost data being maliciously, being sold online or falling into the hands of a competitor.

Securing Microsoft Exchange

The best practise is not to have an internal server within the network available from the internet. With webservers it is common practise to use DMZs and by using firewall segregation, allow internet traffic into the DMZ, but not into the internal network. By placing a layer of protection in front of the Microsoft Exchange Server, it would prevent direct access from the internet.

The Celestix WSA Appliance, powered by Microsoft Unified Access Gateway, is such a device which will "reverse proxy" the communication from the internet to the Microsoft Exchange Server. This appliance will take the communication from the internet and request user authentication information. If the credentials pass the authentication check, the appliance will make the request to the Microsoft Exchange Server, and pass this information back to the mobile device. The Celestix WSA appliance will effectively break the direct commutation from the mobile device, and pass the information as requested. This process prevents the mobile device from directly communicating the Exchange Server.

The Celestix WSA appliance uses an SSL certificate to secure the communication from the mobile device on the internet, allowing the user credentials and password to be transmitted through a secure tunnel. The Celestix WSA appliance will enforce the authentication process, so this

process cannot be bypassed and can be used in conjunction with maximum login attempts and block access accordingly.

Although it is possible to force encryption on the storage cards of the mobile devices, this does not necessarily encrypt the emails.

The storage on the Apple iPhones use AES 256-bit hardware encryption, protecting the email data while the device is at rest. This should be coupled with a password on the device, or this feature will be redundant.

Microsoft Exchange Server Configuration

There are a number of features that can be enable when using Exchange ActiveSync (EAS), including:

- **Remote wipe**, to provide complete security and peace of mind for lost or stolen devices
- **Passwords integrity** (such as length, mixing characters, etc.) to match network policy
- **Maximum failed password attempts** before local wipe to prevent brute force access in the event of loss
- **Inactivity time out lock** to help prevent unauthorised access
- **Password expiration**, to force regular password changes and complement policy across all devices
- **Allow/prevent camera or web browsing** to reduce inappropriate use of the device

Secure Mobile Email

With a combination of the appropriate Microsoft Exchange Server configuration, appropriate mobile device hardware, and a Celestix WSA appliance, any organisation will be able to securely deliver emails to encrypted devices with strong security.

The leading rewards programme just got even better!

e-centives is the fantastic Rewards Portal from e92plus - and is now bigger and better than ever before!

Our exclusive rewards programme has been running for 2 years now, and has proved to be tremendously successful with thousands of points awarded to our partners to spend on fantastic gifts. However, we wanted to make it even better.

So you can now earn e-centive points with every single order placed with e92plus!

It doesn't stop there - we still have our vendor schemes where you can accelerate your rewards with additional incentives, making e-centives even more exciting.

Your key questions



How can you earn points?

Do I need to sign up again?

No, if you already have an e-centives account it will transfer to the new programme.

If you aren't signed up with e-centives, simply go to www.e-centives.co.uk and register.

How do I claim my points?

When you place an order with e92plus, you will automatically receive an email asking you to confirm your e-centive points allocation.

For all additional incentive points - such as the examples above - you need to ensure you send a copy of the order or qualifying activity (such as lead registration confirmation) to e-centives@e92plus.com

How do I spend my points?

Simply log on to www.e-centives.co.uk, check your points balance and start spending! As soon as the points are allocated to your account, you have instant access to thousands of fantastic gifts. Choose your item, confirm your details and enjoy!

It all starts on 19th September!



Get rewarded with every order!

You receive e-centives points with every order placed with e92plus - covering new business, renewals and even professional services.

Points are allocated automatically, so look out for the confirmation email when you place the order.

Accelerate your points with vendor incentive schemes

There are frequent vendor incentive schemes that offer great opportunities for you to accelerate your e-centive points total.

Exclusively available with e92plus for our launch, vendor schemes include:

Earn with Websense when you sell a V5K appliance with both Websense Web Security and Email Security Gateway - just available!

Get rewarded with Drobo when you sell the fantastic new B1200i SMB appliance

Receive points with Avira Anti-Virus or Hosted Email order over £250

Enjoy a bonus with Barracuda when you order enterprise class appliances

e92plus

Absolute[®]
Software

 **AVENDA**
SYSTEMS

 **AVIRA**

 **BARRACUDA**
NETWORKS

celestix

drobo

 **Cyberoam**[®]
Unified Threat Management

 **LG**

 **Lumension**[™]
IT Secured. Success Optimized.

NComputing[™]

VASCO
THE AUTHENTICATION COMPANY

 **QUARESSO**[™]

websense[®]



WINMAGIC[®]
DATA SECURITY

XIRRUS[®]

Web
www.e92plus.com

Tel
020 8274 7000

Fax
020 8274 7002

Argent House
Hook Rise South
Surbiton
Surrey
KT6 7LD