# SECURITY+

# MIND THE GAP

## WALKING THE LINE BETWEEN MODERN THREATS AND USER PRODUCTIVITY

SPRING 2013 / IN THIS ISSUE

DEFENDING AGAINST MODERN THREATS

SECURING THE CLOUD

THE NETWORK GOES WIRELESS

THE REALITY OF DATA SECURITY

e92plus

securityplusonline.co.uk

# SECURITY+

## The leading industry magazine from e92plus

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

It's been an interesting start to 2013; with the challenges in the economy, the continuing growth in threats and the changing IT landscape. At e92plus, we are building on 2012's record-breaking year and this magazine features some very exciting content from our vendor partners who we have started working with.

In particular, this includes the leading Wi-Fi security vendor AirTight Networks, privilege management leader Viewfinity, insights on visual privacy from the world leading 3M and a Q&A from the fastest growing backup vendor in the USA, Unitrends.

We also highlight some of the key vendors to visit at InfoSecurity in 2013, and we'll be there in partnership with them. If you want to arrange any demonstrations, meeting or evaluations, we'd be delighted to hear from you.

Finally, we always appreciate feedback on SecurityPlus magazine – so feel free to drop us a line at **securityplus@e92plus.com**. We look forward to hearing from you.

**Mukesh Gupta**
Managing Director of e92plus

# INSIDE THIS EDITION

# CAN YOU SEE THE RISK? LOST PRODUCTIVITY FROM VISUAL PRIVACY CONCERNS COSTS $1M PER YEAR

Diversified technology company 3M today announced the results of a new Visual Privacy Productivity Study, conducted by The Ponemon Institute. Key findings revealed that companies can lose more than data as remote working increases, with 50% of employees answering that they are less productive when their visual privacy is at risk in public places.

The study showed that employees are forced to either trade-off working and risking private data being overlooked by nosy neighbours, or stop working altogether. Based on these findings, lost productivity due to employee visual privacy concerns is potentially costing an organisation with more than 7,500 people over $1 million per year.

*"While many companies realise that snooping and visual privacy presents a potential data security issue, there has been little research regarding how the lack of visual privacy impacts a business' bottom line,"* says Mr. Ponemon. "*As workers become more mobile and continue to work in settings where there is the potential for visual privacy concerns, companies need to find solutions to address productivity as it relates to computer visual privacy in addition to dealing with the fundamental security issues of mobile devices.*" When asked how their organisation handles the protection of sensitive information in a public place, 47% did not think any importance was placed on this and that no adequate policies were in place.

In addition, more than half stated that their visual privacy had been violated whilst travelling or in other public places such as cafes, airports and hotels, and two out of three admitted to exposing sensitive data on mobile devices. The study concludes by stating that equipping mobile workers with privacy filters on their devices makes them twice as productive when on-screen data is protected. With the average privacy filter costing from £30, this can quickly be recovered by the increase in productivity and the potential cost of compromised data. Companies with mobile workers should have clear and defined policies, educating staff on data security and equipping them with the appropriate tools.

1. Employees are 50% less productive when their visual privacy is at risk and lost productivity costs an organisation around £350 per person per year
2. Visual privacy impacts on transparency as users that value privacy are less likely to enter data on an unprotected screen.
3. Women value privacy more (61%) than men (50%), and women's productivity is more positively impacted than men's when the screen is protected with a filter.
4. Older employees value privacy more, with 61% of over 35's compared to 51% of under 35's placing importance on privacy.

"*Productivity loss is a major discovery in this survey and will hopefully encourage companies across all sectors to consider employee working practices and behaviours,*" said Rob Green, Marketing Executive at 3M's Speciality Display & Projection Division. "*Our range of privacy filters and screen protectors provide essential security of on-screen data for a wide range of mobile devices including laptops, smartphones and tablets. The new Detachable Privacy Filter concept provides the user with the flexibility to instantly transform their tablet display from an open to closed setting by simply attaching the filter for instant visual privacy. The filter can be re-attached and detached as many times as the user wishes, without causing any marks or damage to the screen or device.*"

**The study showed that employees are forced to either trade-off working and risking private data being overlooked by nosy neighbours, or stop working altogether...**

**96%** of data breaches that occurred in 2010 were avoidable.

**$3M** is the average cost to business per incident of physical data theft.

**67%** of working professionals surveyed in the US had worked with some type of sensitive data outside the office

**80%** Chance that you've already become a victim of others reading over your shoulder

Visitors to the 3M stand (E92) at Infosecurity Europe will see some creative examples of the lengths people go to in order to hide their sensitive data in public spaces, and include devices for Apple iPhone, iPad and laptop product ranges.

# BYOD: TRANSFORMING THE WIRELESS NETWORK

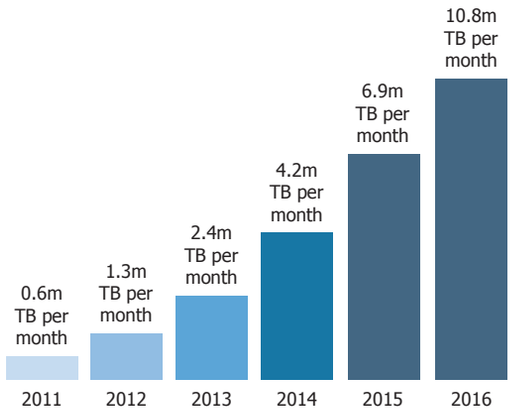
The proliferation of tablets, smartphones, and other smart devices has increased dramatically in the past several years, and use of these 'consumer class' products on enterprise networks is nearly ubiquitous. A recent study showed 90% of organisations polled allow some level of personally owned technology to be used — a phenomenon commonly referred to as BYOD (Bring Your Own Device). Many organizations are even contributing to this evolution by partially funding the purchase of employee-owned devices that are used as a business tool.

Until recently, the enterprise has been hesitant to embrace the tablet, having seen several false starts of similar products in the past. However with tighter corporate budgets and CFOs looking to leverage the cost benefits of personally owned devices, times have changed. Only a short time ago, standard corporate issue was a laptop and a business-focused smartphone such as a Blackberry. Today, it is a laptop, full-featured smartphone, and a tablet that are coming to work — in some cases this has tripled the number of wireless devices accessing the wireless network.

This growth in use of smart devices has resulted in a dramatic shift of traffic to and emphasis on wireless networks since these devices do not have wired Ethernet ports. This shift is challenging IT staffs to engineer wireless networks that can support the demands of this new paradigm today and that are able to adapt to increased and changing requirements tomorrow. No longer does IT have the luxury of predictability in controlling the type and quantity of devices on their networks – they just need to support this new mobile revolution. As a result wireless vendors are being challenged to deliver wireless solutions designed for tomorrow, not yesterday.

**Basic Design Considerations**

In granting personal mobile devices access to the enterprise network, there are some basic design considerations which fit into two categories: Capacity and Security. Together these address the challenges of supporting the sheer number of devices accessing the network and segmenting the different classes of users once they are on.




**Capacity**

Capacity deals with not just the number of devices, but also understanding variable device capabilities and following best practices when designing the network. Some key best practices include:

**Maximizing the Use of 5GHz**

There is up to seven times as much bandwidth available in the 5GHz vs. 2.4GHz unlicensed spectrums used by Wi-Fi, as well as much less non-Wi-Fi interference in 5GHz. As a result, optimizing use of 5GHz is a fundamental requirement for achieving optimal Wi-Fi performance. As many Wi-Fi APs (radios) as possible should be set to operate in 5GHz. Typically some radios will need to be set to 2.4GHz to support certain clients (smartphones and legacy clients). Both spectrums must be supported in most wireless networks, but it is key that all new wireless infrastructure is designed with a 5GHz focus. The latest generation of wireless access devices provide multi-state radios supporting both bands, allowing IT managers to switch bands as more and more devices support the higher performing 5GHz band.

**Design for Appropriate Signal Strength**

The Wi-Fi signal level design criteria typically used for laptops (nominally -70dBm RSSI) is not sufficient for tablets and smartphones, especially when they will be deployed in dense numbers. Since these devices transmit at lower signal levels and have inferior antennas compared to laptops, networks must be designed with stronger signal to ensure maximum data rates. Wi-Fi networks for tablet and smartphone support should be designed with a minimum -65dBm signal strength in BOTH the 5GHz and 2.4GHz bands in all locations.

**Provide Sufficient Radio Bandwidth**

Because of lower transmit power and limited 802.11n data rate support, tablets and smartphones will typically achieve much lower traffic throughput performance compared with laptops. More Wi-Fi radios are therefore required to support these devices in a wireless environment compared to a similar number of laptops, as multiple devices will share the same radio. A general rule of thumb is to design the wireless network with enough radios to handle the expected number of devices at a ratio of 15 per 5GHz radio and 8 per 2.4GHz radio for a typical office or classroom levels of required experience. Higher numbers of devices per radio are appropriate in deployments without high performance requirements, which lower limits will need to be employed for higher capacity needs.

**Provide Scalability/Upgradability**
As more devices use the corporate wireless network, the network needs to be able to handle the increased utilization of network resources. This can be accomplished by deploying upgradable wireless solutions that do not require 'forklift' upgrades when additional capacity and bandwidth is needed. New generation of wireless products are engineered to provide modularity that allow the addition and/or replacements of radios without having to replace the whole infrastructure. These platforms operate similarly to a traditional wired network chassis allowing the addition of more radios and the ability to upgrade radios from one technology to another, e.g. 300Mbps 802.11n to 450Mbps 802.11n to (future) 1.3Gbps 802.11ac without the concern of oversubscribing a centralized controller. Today's wireless solutions must be designed to last as long as wired infrastructure (5-7yrs) and this requires a scalable/upgradable design.

**Security**
Security considerations around access control and data management are crucial to plan. While control of the device itself may have been relinquished, IT must focus on the control of the network and data infrastructure in support of these devices. Knowing not only who is on the network but visibility into what device they are using, what application they are using, and where they are located can feed into deciding which access policies to enforce for that user's session.

The deployment diagram and control chart below shows all the components for an end-to-end mobility solution and how policies can define access. The following example set of use cases depicts how different user and devices may be controlled on a network.

User/device management tools allow administrators to create policies to balance security and access in a BYOD environment, achieving greater productivity without increasing risk on the network. In the above case, corporate users with a corporate device can receive unrestricted access, yet that same user with a personal device may have restricted rights. Some devices (games) may be totally blocked from the network. The capability exists today to define users and device types – it is just a matter of defining and implementing a corporate policies.

| User | Client Device | Access Policy |
|---|---|---|
| Employee | Corporate Device | Full Access |
| Employee | Approved BYOD Device | Limited Access |
| Contractor | Approved BYOD Device | Limited Access |
| Guest | Approved BYOD Device | Internet Only |
| Employee | Personal Device | Blocked |
| Unknown | Unknown | Blocked |

**About Xirrus**
Organizations depend on high-bandwidth voice, video, and data going to and from mobile devices. Business is done in the cloud. Today, you need high performance wireless. Xirrus delivers it. Our wireless solutions provide wired-like capacity and reliability, superior security, and perform under the most demanding conditions – all in a modular, upgradable platform designed to meet tomorrow's changing requirements.

## THE ULTIMATE IN WI-FI: DELIVERING WIRELESS FOR 3 MILLION VISITORS AT THE NEC

A major challenge faced by the exhibitions industry is persuading visitors to take time out of the working day to visit events. To continue attracting a high volume of visitors, the NEC needed to enable people on site to stay connected to their social and business circles through a fast and reliable Wi-Fi network.

Kathryn James, MD at the NEC, said: "*NEC visitors want to stay connected with their social and business lives at all times, and our customers told us that Wi-Fi was a priority if we wanted to make the NEC an even better place to visit.*"

The NEC decided to implement Xirrus to support thousands of concurrent, heavy bandwidth users across its exhibition, conference and organiser suites. The new infrastructure optimises Wi-Fi connections for those devices operating at 2.4 GHz range as well as the increasing number of those using the 5GHz range such as the new iPhone5.

To address these issues the NEC installed 155 Xirrus Wireless Arrays to provide free and ubiquitous wireless access throughout the halls, offices, public areas, catering outlets and conference suites, providing seamless connectivity for up to 22,000 concurrent users.

"*Xirrus was the only supplier that demonstrated the ability to deliver high density Wi-Fi for the exhibition industry,*" said Murray Dickson, the NEC's Business Solutions Analyst. "*Xirrus' unique grouping of multiple APs within a single array was key along with visibility into applications on the network so we can deliver a more reliable user experience.*"

"*Having fewer physical units helped us to reduce resources spent on infrastructure installation, as well as support and maintenance. Additionally, Xirrus allows us to future proof our investment as Its arrays are designed to support the new 802.11ac standard - if we want to upgrade, we can add or swap 802.11ac modules into existing arrays,*" he added.

"*It's fair to say that we're now one of the most – if not the most – diversely connected venues in the UK*" says Andrew McManus, IT Director at the NEC. "*Our customers are now able to connect to all of their remote services as if they are at home or in their office. Our entire site is now hyper-connected inside and out".*

# THE ALL-IN-ONE BACKUP SOLUTION
## EXACTLY WHAT'S NEEDED FOR TODAY'S AGILE IT ORGANISATIONS

**A Q&A with Unitrends' Managing Director, EMEA, Kevin Moreau**

**With thousands of customers around the globe you are constantly interacting with IT staff. What do you think is IT's biggest backup challenge they are trying to address?**

Within the backup and data recovery space, there are key trends that are impacting all IT organisations globally. Mid-market organisations (sub 1,500 employees) in particular are resource-constrained and need to manage ever-increasing data growth pressures which tax IT infrastructures and require newer and agile data recovery strategies. Ask any IT Director, and they'll tell you how virtualisation and cloud computing have dramatically transformed the data center. While these technologies provide for many business advantages, they can also introduce unintended complexities – especially for data protection and recovery strategies.

A major question is how best to protect data across heterogeneous environments. IT is now tasked in trying to manage and protect data across physical, virtualised and cloud-based systems and servers. Many are struggling with this because they've adopted a multi-vendor approach to data protection – where they are employing different backup and recovery vendors for different infrastructure setups.

You can't blame them: Many traditional backup and data recovery solutions are ineffective in virtual and cloud environments, and conversely, many backup vendors today specialise only in virtual or cloud-based data protection. So, the net result is that companies are taking on a multi-vendor approach to data protection without thinking about the budgetary costs and the resource drain associated with doing so. This approach is neither economical nor practical.

The second major pain point IT is facing is how to do more with less. It's no surprise that the last few years have put IT departments in a tough spot – especially within the mid-market. They just don't have the budget or resources to deploy and manage complex data protection solutions. Unfortunately, many IT organisations think that this means they can't receive enterprise-class data protection – and so they settle on mediocre solutions.

**What is Unitrends vision for solving today's critical backup & data recovery issues?**

IT environments are complex, data is increasing, there are fewer IT resources – our goal with every one of our products is to make it easy and affordable for our customers to protect data across these heterogeneous environments. Our technology is easy to use and our pricing is simple.

While many backup and recovery vendors force companies to customize their data center makeup around their data protection solutions, we believe that companies should be able to easily adapt their data protection solutions as their data center evolves. As such, our solutions not only protect data within hybrid environments, but they also support more than 100 different versions of servers, operating systems (Windows, Hyper-V, VMware, Mac OS, Linux, AIX, Solaris), SAN, NAS, hypervisors (Hyper-V and VMware) and applications (Exchange, SQL, Oracle). In other words, we provide our customers with maximum flexibility so that IT remains responsive and agile to the changing needs of its users and to the evolving technology landscape.

Additionally, as downtime tolerance diminishes, organisations are looking for a turnkey approach to data protection, overall improved performance in terms of improved backup windows, faster restore and recovery times; and overall lower TCO (total cost of ownership). Few backup and data recovery vendors provide an all-in-one solution that enables you to protect physical and virtual infrastructures with a single pane of glass and thus reduce the management overhead of managing your complex backup environment.

**What is one of the most key but overlooked aspects when considering a backup solution?**

We've talked about the value proposition of our technology – unified data protection that is easy to use and affordable – and that is one of three critical company goals that enable us to stand out in a competitive industry. However, probably the most critical aspect does not involve the backup technology at all - it is your backup vendor's customer support.

With today's complex data centers, the unfortunate reality is that it's no longer a matter of if but when a disaster will strike. Customer support is often undervalued in the industry. Many customers put technology and price over support, and as such, some vendors create the appearance of customer service without actually delivering on it. Unitrends understands that customer support is actually a significant business differentiator, and we uphold a strong commitment to customers throughout our organisation.

We want our customers to feel confident that when the unthinkable occurs – and their data is at risk and their jobs are at stake – they have a strong customer support team in place that will guide them to a solution. This is the exact opposite of many other vendors in the industry that hold their customers' feet to the fire when they need help the most. Our commitment to customer service and support is so strong that we strive to achieve a customer satisfaction rating of 98% or above – that's unheard of in the industry today.

# WHAT ARE THE CONSEQUENCES OF DATA LOSS?

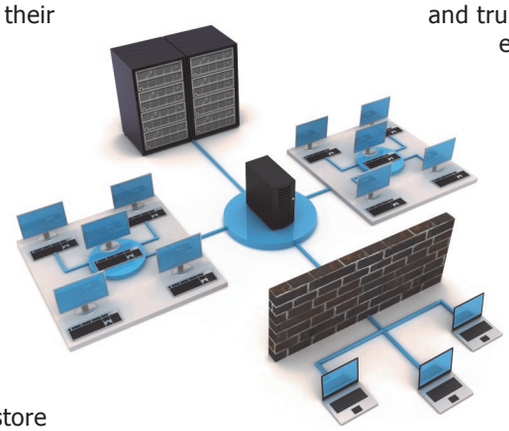
The consequences of data loss are dire; here is a sampling of just a few statistics related to the impact of data loss on business:

- **93% of companies that lost their data centre over 10 days due to disaster went bankrupt within one year.** 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately (National Archives & Records Administration)
- **94% of companies suffering from a catastrophic data loss do not survive** - 43% never reopen and 51% close within two years. (University of Texas)
- **77% of those companies who do test their tape backups found back-up failures** (Boston Computing Network, Data Loss Statistics)
- **7 out of 10 small firms that experience a major data loss go out of business within a year** (DTI/Price Waterhouse Coopers)
- **96% of all business workstations are not being backed up** (Contingency Planning and Strategic Research Corporation)
- **50% of all tape backups fail to restore** (Gartner)
- **25% of all PC users suffer from data loss each year** (Gartner)

In addition, the challenge is only growing– not just in the consumer space (with 100TB uploaded to Facebook daily, or 48 hours of video to YouTube every minute) but also in business with UK companies expecting a 42% average increase data by the end of 2014.

**How confident are most IT organisations that their backup and data recovery strategy will hold up in the event of a disaster?**

When it comes to disaster recovery planning, many businesses start out well enough: they conduct initial testing of their backup and restoration approach, relying on this plan ever after. Meanwhile, these same businesses continue to grow, and alongside that their data store grows too, leaving their original disaster recovery plan outdated and their operations at severe risk.



According to Gartner, 43% of all companies that experience a major disaster will go out of business if they cannot gain access to their data within twenty-four hours. Based on National Archives records, 93% of businesses that lost their data center for ten days went bankrupt within one year. Any unplanned interruption in your business can cause loss of customers and prospects. The strategy you choose to guard against that loss depends on these three factors:

1. **How much data you need to protect**
2. **How long you can endure downtime of operations**
3. **Your IT budget**

These factors will inform your decision to adopt a virtual, cloud, or physical disaster recovery method, or some combination of these, to support your data protection needs. Ultimately, customers want a solution that allows them to focus on their business rather than their backup.

**Are there certain industries that are more versed in best practices regarding data recovery strategies?**

We serve companies of all sizes and across all verticals both in the U.S. and internationally. They come from a range of industries – government, education, healthcare, energy, transportation, financial services, and more. Regardless of the industry, data is the lifeblood of your organisation and something that needs to be protected at all costs.

There is little difference in need from one organisation to another; the difference comes in terms of how they choose to implement their strategy. We work with companies who want an easy-to-use and affordable backup and data recovery solution that they can plug in and trust to protect rapidly expanding volumes of data across heterogeneous environments. We work with customers in terms of what their environments look like today, what their evolving virtualisation strategy is (if they have one), the amount of data they need to backup and protect, including internal SLAs they may have around RTO and RPO – essentially we do an entire tech audit. We also walk them through optimal data recovery strategies - ensuring that they have a plan, they test it, and re-test it.

Additionally, we've found that resellers are looking for better ways to address the needs of their existing customers, and also to attract new customers. They are looking for a truly adaptive and scalable solution, offering complete protection - physical, virtual, and cloud-enabled - for their customers. We offer resellers a proven back up and data recovery all-in-one solution that's appealing to their customers.

**Can you talk about the competitive landscape and why Unitrends offering will win over competing products/services?**

Let me reiterate that our business model – focused on unified and affordable data protection, coupled with unrivaled customer service and support. No other provider offers all-in-one data backup, archiving, instant recovery and disaster recovery solutions capable of addressing the needs of businesses as they move into the cloud, embrace virtualisation and maintain existing physical infrastructure.

Plus, our unparalleled ability to address businesses' data protection needs regardless of which IT assets they have in place is backed by an equally robust customer support. We offer the mid-market enterprise-class data protection at the lowest TCO in the industry. That's a winning combination that no other backup or data recovery vendor can top.

# APPLE VS. ANDROID

## WAR EXTENDS INTO ENTERPRISE APP DEVELOPMENT

**Absolute Software research shows Apple only just dominates in enterprise app development in UK and US, while Android wins in Europe.**

Independent research released by Absolute® Software shows that Apple only just wins out when it comes to enterprise app development. Although, Android trumps the technology giant in both France and Germany.

The global survey of CIOs, commissioned by Absolute Software, the industry standard for persistent endpoint security and management solutions, shows that nearly two thirds (64%) of UK companies chose Apple as their default operating system for app development. Compare this to less than half (41%) of French companies and 53% of Germany companies.

"*In order to win the app battle, Android needs to bump up their security to the standard set by Apple. As different devices make their way into the enterprise, employees expect greater access to business applications and data from the field. This presents an increasingly difficult challenge for IT who need to manage and support a deployment across a multitude of operating systems and form factors*," remarked John Sarantakes, Senior Vice President and General Manager, EMEA for Absolute Software.

The fact that Samsung Galaxy is continuing to beat the iPhone 5 in the smartphone war could be a reflection of France and Germany being more open to BYOD practice. The same research found that the UK sees the integration of business and personal data as far less important than Germany or France. Fewer than four out of ten (39%) CIOs in the UK see it as the future, compared to 59% in France and 50% in Germany.

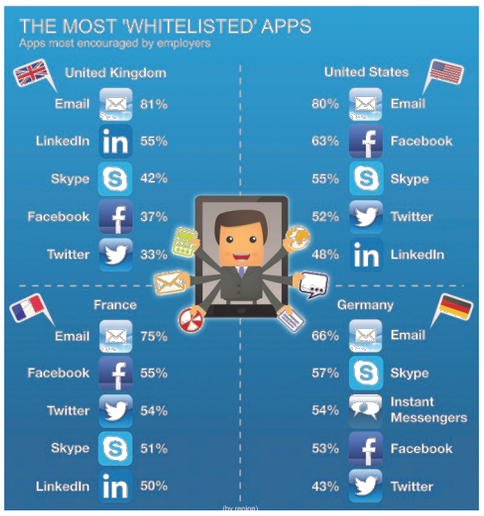
"*IT needs to recognise this shift and be prepared to address security or productivity fears that may arise, as the battle of platforms is not going to end any time soon*, " commented Mr. Sarantakes.

### In the security battle, Apple is King

For the most part, the most requested app for employees is email. However it appears that IT is most fearful of file sharing apps and, only 9% of IT decision makers would choose to build an app for email. These figures reflect the fear of Android security vs. the seemingly 'ironclad' iOS platform.

When it comes to blacklisting apps, UK organisations are the most concerned about security in relation to blacklisting, with 93% stating security concerns over productivity reasons. The keen focus on security in the UK is a possible reason for Android lagging behind in terms of enterprise app development.

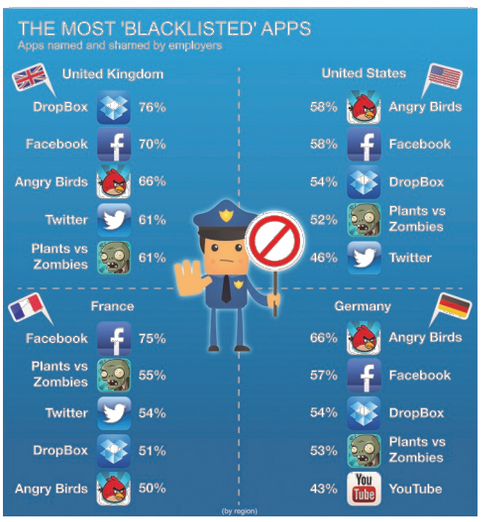
One area where organisations can retain control over data is through self published apps, rather than relying on generic third party apps. This can either be bespoke developments, or through solutions such as AbsoluteApps to distribute in-house apps, or AbsoluteSafe which allows for fully secure distribution of confidential files and data.


When it comes to influencing BYOD policies, there is a clear need to cover demands for multiple mobile OS - especially with the potential re-emergence of BlackBerry as well as strength of Microsoft Mobile, and their continued investment in both the mobile and tablet OS market.

Independent specialist technology market research company, Vanson Bourne, conducted the survey. The research surveyed 1,200 IT decision makers from a variety of vertical sectors across the UK, France, Germany and the United States.

# BYOD: BALANCING THE SECURITY TIGHTROPE


The case for BYOD and its imminent arrival, together with the advent of employee owned devices on the corporate network, doesn't need to be made. If you're reading this magazine, you know that BYOD isn't coming, it's already here.

However, there is a careful security balance to be approached, to ensure that corporate data is secured and devices managed without affecting productivity or losing the benefits that BYOD was designed to bring in the first place.

With any BYOD strategy, a negative assumption needs to be made: data and devices are at risk. That's true on corporate devices as well as employee ones. Here are some easy stats:

- 88% of IT administrators, if laid off tomorrow, would take valuable and sensitive company information with them
- Over 600,000 laptops are lost or stolen each year from U.S. airports
- 60% of data breaches occur from behind the network firewall

So, accidentally or by design, employees will always be the weakest link in computer security strategies that rely on their diligence to provide consistent protection. With mobile devices – especially their own – that risk only increases.

So the first step is to define the list of form factors and operating systems you will support, and to ensure network accessibility – and we cover the necessity of wireless elsewhere in this issue. Next you need to define policy, which is crucial and defines the balance that IT must maintain between respecting the privacy of the employee while securing the corporate network and any data contained on the device.

Now that you have all of the internal requirements identified and in order, you need to select the appropriate software application that will allow you to properly manage and secure corporate and employee-owned mobile devices. Plus, these questions are those often applied to LAN workstations or servers, and are often taken for granted or handled manually. But BYOD and consumerisation is changing these rules, and organisations are looking for solutions that manage devices across the entire network.

**Platform flexibility**

- Does your proposed solution work and integrate with your existing network environment, and can it provide a single console for manage both mobile and desktop/ LAN devices?

**Administration and Configuration**

- Does it allow for role-based administration, allowing you to enable staff to perform their duties and increase IT staff productivity?

**Mobile Apps Management**

- Can you distribute both in-house and third party apps, and support self-service apps to help users find and deploy approve apps themselves?

**Security**

- Can you apply complex policies, applying to all devices by defining permissions by role or department? Does it all provide data & device security, remediation and data recovery, plus enterprise security controls?

Of course, BYOD applies not just to mobile devices, but also to laptops. One opportunity that introducing BYOD brings is highlighting the requirement to proactively manage the laptop & mobile devise estate, and introducing the chance to regain control of devices, secure data and reduce loss.

Absolute Manage delivers cross-platform asset management, and for Lincoln Public Schools - who manage over 17,000 laptops & PCs - the benefits were clear:

"*The automated asset management tools have reduced the time-consuming need for onsite support. Technicians now have a routine, methodological way to automatically push new software and updates, and to manage patches and imaging. There is a lot less running around. It's easy to generate detailed inventory reports – Absolute Manage helps us be good corporate citizens without killing ourselves in the process".*
Kirk Langer (Director of Technology, )
Lincoln Public Schools

This solution supports over 35,000 students across 61 schools, requiring only 4 IT support staff to manage their entire deployment. It has also freed up frontline staff: "*We now save about 250 plus hours of instructional time annually so, instead of gathering information on computers, teachers can better prepare for lessons*".

Absolute Manage is a lifecycle management and mobile device solution that allows IT administrators to manage PC, Mac®, iOS, Android, and Windows® Phone devices from a single console. Customers can remotely engage with their deployment and perform standard maintenance routines as well as take strategic and responsive measures based upon the requirements of each device.

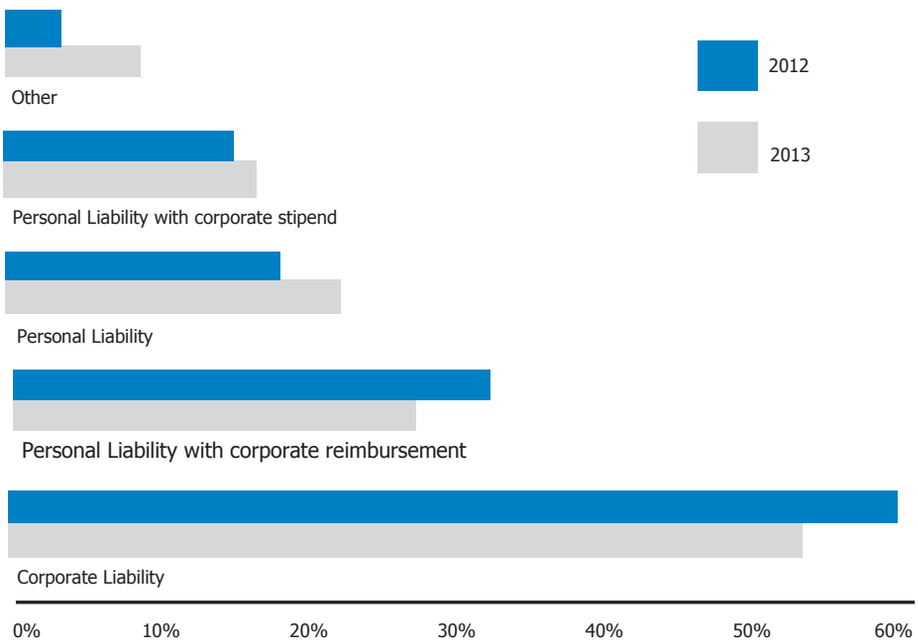
# GLOBAL DATA PROTECTION MATURITY IN 2013

The job of protecting sensitive information has become more difficult in the last couple years. One factor is the booming use of mobile devices, which is putting considerable pressure on traditional network perimeter defenses. This growth also means that priceless corporate data is now as likely to be outside of the corporate firewall as within its protective reach. In addition, the adversaries intent in gaining illicit access to confidential data are growing in number and sophistication. In order to counter these trends, organisations need to develop and maintain the appropriate data protection best practices that keep them compliant and secure.

In the 2013 results, just 6% of respondent organisations categorised as having Optimal data protection maturity, with 26% classified as Operational, 41% labelled Standardising, and 27% in the Ad Hoc group. Clearly, we have a lot of work to do.

**Changing IT Network Landscape**
Obviously, bring your own device (BYOD) has significantly impacted IT security. Last year, the estimated use of personally-owned devices in the organisation at 0 – 20% was 46% and those who put it at 20 – 100% was 45%. This year, we see the gap reversing and widening somewhat,

**How are personal mobile devices, such as phones and tablets, financially and administratively managed within your organisation?**




In late-2012, Lumension conducted the 2nd annual worldwide survey of organisational attitudes, policies and programs designed to protect sensitive information – be it so-called "toxic" customer data (PII) or valuable organizational intellectual property (IP). Approximately 300 respondents from around the globe completed the survey, which examined the challenges faced by organisations trying to protect data under their care today.

with more organizations in the 20 – 100% (46%) than in the 0 – 20% range (42%). Additionally, about 30% or organizations reported to have minimal or no security polices which address their data protection concerns.

When asked "how are personal mobile devices, such as phones or tablets, financially and administratively managed with your organisation," respondents in 2012 said these devices were classified as "corporate liability" or, an extension of the corporate network, with a personal-use policy strictly defined. In 2013 though, this dropped to 52% with the biggest increase seen in the "personal liability" without reimbursement or stipend. This gives a good indication of just how far organisations have come in embracing BYOD. However, again highlighting the need for organisations to pay closer attention to the changing IT environment, there is a dark side to this "Personal Liability" device statistic – it suggests minimal or no access policy, which puts data privacy initiatives at risk.

In order to better understand the data protection guidelines within organisations today, we asked about the restrictions included in employee agreements. An overwhelming majority of the respondents indicated that corporate confidentiality (81%) clauses were included, followed by customer confidentiality rules (63%) and mobile device policies (59%).

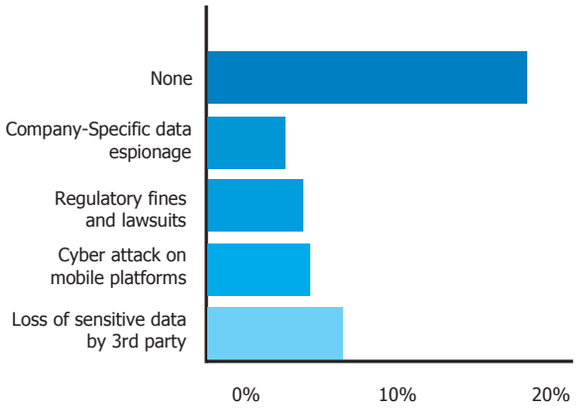
In fact, much like last year, just under 50% of organisations have set out an explicit statement of what rights the company retains to data on personal devices. Taken as a whole, this suggests that employment agreements may not have kept pace with the changes in the IT environment – potentially putting confidential or sensitive data at risk. The average reported security spend ratio (relative to overall IT budget) dropped from 6.1% in 2011 to 5.6% in 2012.

**Increasing Threat Landscape**
Also examined in the 2013 Data Protection Maturity report was perception around the increasing threat landscape. Accordingly, respondents identified their greatest issues as network intrusion by a virus or malware (58%), theft of IT assets such as laptops (43%) and the accidental loss of data by employees (42%). It is interesting to note that the "none" category dropped by almost 5% from 2012. However, the largest changes from 2012 were seen in following categories:

1. **Virus or malware network intrusion…10% increase**
2. **Targeted cyber attacks…7.5% increase**
3. **Theft of IT assets (such as laptops)…6% increase**

However, almost every category increased in some amount (with only "cyber attack on mobile platforms" decreasing), and demonstrate the multitude of threat vectors and the increasing magnitude and sophistication of attacks. This has led to an increasing feeling of endpoint insecurity among IT professionals year on year, which has risen from 59% to 67% since 2009. The overwhelming perception that no data protection regulations pertain suggests a fundamental disconnect between the regulatory landscape and our respondents understanding of it.

**Have you experienced any of the following incidents in the past year?**




**Uncertain Regulatory Landscape**

Data privacy and data breach notification rules have been on the books for some time now, and the regulatory environment is ever-changing as government and industry grapple with these issues.

Indeed, respondents were uncertain or unaware about what statutory and industry regulations apply to their organisations. On average, just over 25% of respondents claimed to be compliant to any of the regulations, with planned compliance at just about half that - meaning around 60% of respondents did not think any of these regulations were applicable.

Digging deeper, we find that just over 25% of respondents state their organisation is not compliant with any data protection regulations, while about half suggest none of them are actually applicable. However, as we noted in last year's study, almost all jurisdictions have some sort of data privacy law that applies, not only to confidential customer data but employee data as well – so these results are hard to understand.

True, the regulatory landscape is changing rapidly. In 2012 we saw changes to many industry regulations (such as the recently updated PCI DSS), and most jurisdictions have some sort of data protection law which applies to employee personal information. In addition, we're starting to see governments becoming concerned about cyber-espionage, at least when it comes to so-called critical infrastructure. The biggest threat issues seen in 2012 were: network intrusion by a virus or malware (58%), theft of IT assets such as laptops (43%) and the accidental loss of data by employees (42%).

That notwithstanding, the overwhelming perception that none of the data privacy regulations pertain (both individually and in aggregate) suggests a fundamental disconnect between the regulatory landscape and our respondents understanding of it. Organisations hoping to meet their data protection obligations need to understand all the regulations which apply.

**Data Privacy Best Practices**

As the old bromide goes, the only thing that is constant is change. IT departments are in the midst of some significant changes, driven by both organizational and end user needs. Increasing use of personal devices to access organisational data and increasingly sophisticated attacks from motivated adversaries are just two of these that impact the protection of sensitive organisational and customer data. In the last year, 58% of our respondents indicated that their organisation had been infiltrated by a virus or malware, while another 42% had employees accidentally lose data. The growth in BYOD and the gradual erosion of the traditional network boundary serves to remind us that a best-in-class approach to data protection should not only focus on comprehensive administrative policies and pragmatic technical controls, but must also find its origin in the core of the organization. Indeed, organisations must engage on multiple fronts to provide superior data privacy:

**Visibility:** understand, through surveys and technical measures, how consumer devices are being utilized within the organization. This is needed as a baseline to understand basic risk and behavior and to recruit executive buy-in for future measures.

**Cultural indoctrination:** make data protection core to the mission of the organization with executive backing. Data protection awareness and understanding should be as "everyday" as locking the front door.

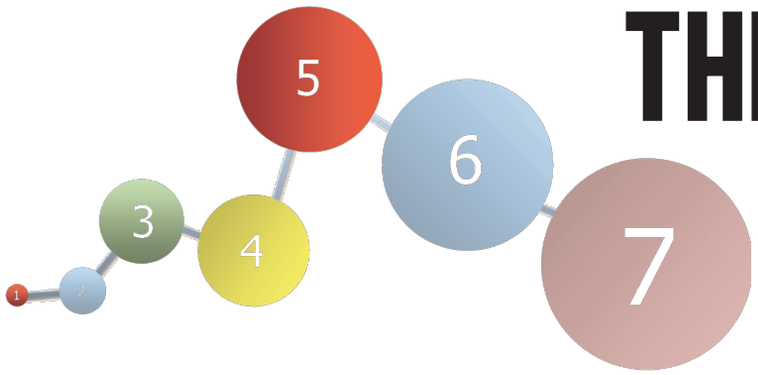
**Policy:** develop official policies with legal and liable guidelines for both organization and employees. A comprehensive data protection policy should be put in place to cover all devices no matter whether they are owned by the company or staff. IT policies should be regularly reviewed and updated to fortify against ever evolving exploit techniques.

**Training:** educate end users and staff regularly to ensure awareness of these policies and the importance of data protection. The approach of simply ensuring that staff, upon commencement of employment, sign-up to a policy which might have remained unchanged for several years, is no longer adequate.

**Technical control:** do not forget low hanging fruit. Enforcement starts at a simple level – ensure that anti-malware software is up-to-date and promptly deploy security patches. Investigate encryption technologies fundamental to providing protection for your data. Small and mid-market companies may find it easier to implement solutions such as device control to eliminate additional risk without requiring the effort and overhead of a full DLP solution. As financial constraints allow, implement increasingly sophisticated technical controls which concentrate on reinforcing the business' mission and have strategic commitment from above.

View the full survey and whitepaper at **www.lumension.com/data-protection-maturity**

Paul Zimski is an IT security industry expert and oversees marketing and solution strategy at Lumension, and regular speaker at major security events such as RSA and HIMSS.




# THE 7 STAGES OF ADVANCED THREATS

Security used to be easy: patch your software and update your AV (Anti-Virus), and you'll have an effective defence. Websense Security Labs have proved the ineffectiveness of this old strategy. They analysed a four month period with six vulnerabilities and found that if an organisation deployed the patches immediately, they were still open to vulnerabilities 88% of the time. Exploit kits focus on these windows of opportunity and while updating software patches and AV signatures is a good security practice and is still advised it is not a front line defence for today's advanced threats. If you want to develop and manage an effective defence, you need to understand how advanced threats work. Here we describe a seven-stage model that will help you evaluate your current and planned defences.

## Stage 1: Reconnaissance

Hackers access credentials and research social media profiles to gain intelligence about people they're targeting. Their goal is to build highly personalised "lures" that are likely to be opened and acted upon.

## Stage 2: Lures

There are two types of lures: web lures and email lures. Web lures prey on human curiosity. They are a common tactic of search engine optimisation (SEO) poisoning, where hackers lure recipients who are searching for breaking news, celebrity gossip and other popular topics. Web lures are increasingly sent in broad, untargeted attacks via social media, where they are spread among friends in private social networks.

Email lures rely less on news, events and social media. Instead, they typically contain a notification a user might expect to receive: order notifications, ticket confirmations, delivery notices, test emails and tax return information are the top five examples. Such seemingly typical content allows email lures to bypass spam filters. Email lures are usually sent in highly targeted, low-volume attacks to specific individuals using intelligence gleaned from social media.

Because a good email defence starts with a great web defence, are you confident your current defences can analyse social media to identify lures and protect users? Do your web and email security solutions share and correlate threat intelligence? Do they recognise that 92% of spam contains a potentially unsafe URL?

## Stage 3: Redirects

Users are usually directed to a survey, a rogue AV offer or a fake web page where an exploit kit is waiting. Traditional redirects include SQL and iFrame injections that take users blindly down a path to services, content and offers they often do not desire. "Malvertising" (malware advertising) is a tactic to redirect unknowing users from within popular websites. Newer redirect tactics include postings made to social networking websites, fake plug-ins, fake certificates and heavily obfuscated JavaScript. Redirects are often dynamic and change quickly — are your defences fast enough to assess these web links in real time?


## Stage 4: Exploit Kits

In the past, hackers used lures to redirect users down a path that would enable malware to be installed onto their systems. It was a method that, though damaging at first, could be quickly detected by threat lab intelligence and thereafter prevented. Today, exploit kits such as Blackhole are used to deliver a malware dropper file, and this dropper file is sent only after a vulnerability is detected in a targeted system. If no vulnerability is detected, the user is redirected to a safe web page and the exploit kit remains hidden.

An understanding of exploit kits is important for analysing advanced threats and developing real-time defences. For example, Blackhole uses criminal encryption, which means that AV engines and generic deobfuscation tools will have difficulty detecting it. Is AV your only defence at the web gateway? If so, it's highly likely that exploit kits can penetrate and infect your systems through vulnerable applications.

## Stage 5: Dropper Files

This stage is where most organisations focus their forward-facing defences, which analyse every file entering their networks for malware. Unfortunately, what worked in the past might now provide a false sense of security. The problem is that few AV engines can detect today's dropper files that use dynamic packers for which no known signatures and patterns are available. One of the most popular dropper files is Rogue AV, which contains a fake offer to scan and clean your system. Traditionally focused on Windows systems, new versions such as Mac Defender or Protector are now targeting Apple computers. What do you have other than AV to protect against advanced threats and data theft?

Note: The next two stages indicate two inescapable conclusions: **No defence is 100% effective, and containment is the new defence for data loss prevention (DLP).**

## Stage 6: Call Home

A typical advanced attack "calls home" to download malware and tools while sending back valuable information. The problem is that most defences are only forward-facing — they do not analyse

the outbound call-home communications sent from within an infected system. These call-home communications commonly use dynamic DNS to avoid detection.

Fortunately, there are emerging technologies to defend against this stage of advanced attacks. For example, infected systems and bots attempting to call home can be blocked from using dynamic DNS, while users can opt to continue on to trusted sites. Destination awareness in the context of DLP is also a potential defence, as is geo-location awareness. (In the latter case, however, because most malware communications, hosting and phishing originate in the US, most policies will not block these domains.)

Do you have defences that analyse outbound traffic for call-home communications, or perform contextual analysis of data, user, destination and other variables to prevent confidential information from being sent to personal web mail, social media or personal cloud accounts??

### Stage 7: Data Theft

Data, in the end, is what attackers are after - and that's what attackers get when they are able to bypass the insufficient security defences at the previous six stages. Yet even at this 7th stage there are defences emerging to keep confidential data safe.

Can your defences detect password files leaving your network or the use of criminal encryption on outbound files? Can they catch confidential data being exported in low volumes per request to avoid detection? Do they provide forensic reporting that shows what data was blocked from leaking?

Independent lab results confirm that in real-world network conditions, Websense TRITON stops more threats than competing security solutions. Get the proof with our report and find out why conventional defences don't measure up! **www.websense.com/proveit**

**How did we reach these conclusions?**

The primary source of data for this report was the Websense ThreatSeeker® Intelligence Cloud, composed of "big data" clusters used by Websense Security Labs to collect and manage up to 5 billion inputs each day from 900 million global endpoints. The world's largest threat intelligence network, the ThreatSeeker Intelligence Cloud provides visibility into real-time threat activity, including threats occurring within encrypted social media systems and other secured networks. Data retrieved was analysed in real-time by Websense ACE (Advanced Classification Engine) with over 10,000 analytics.

# 2013 THREAT REPORT

Last year put 'trust' to the test. Can mobile devices be trusted on the network? Can users trust IT to protect them from the latest exploit? Can IT trust users to access social media safely? Can businesses trust their current defences to protect against emerging threats? The evidence collected by Websense® Security Labs™ researchers suggests that for many organizations the answer to these questions is no. Explosive growth in several key indicators of global online criminal activity points to a crisis of trust, as we question the viability of "standard" security practices that have served us well over the past decade.

## Malware Behaviour

Cybercriminals adapted their methods to confuse and circumvent specific countermeasures. Fifty percent of web-connected malware became significantly bolder, downloading additional malicious executables within the first 60 seconds of infection. The remainder of web-connected malware proceeded more cautiously, postponing further Internet activity by minutes, hours or weeks, often as a deliberate ruse to bypass defences that rely on short-term sandboxing analytics.

## Social Media Threats

Shortened web links— used across all social media platforms—hid malicious content 32 percent of the time. Social media attacks also took advantage of the confusion of new features and changing services.

## Mobile Threats

A study of last year's malicious apps revealed how they abuse permissions. Especially popular was the use of SMS communications, something very few legitimate apps do. Risks also increased as users continued to change the way they used mobile devices.

## Email Threats

Only 1 in 5 emails sent was legitimate, as spam increased to 76 percent of email traffic. Phishing threats delivered via email also increased.

## Web Threats

The web became significantly more malicious in 2012, both as an attack vector and as the primary support element of other attack trajectories (e.g., social, mobile, email). Websense recorded a nearly 6-fold increase in malicious sites overall. Moreover, 85 percent of these sites were found on legitimate web hosts that had been compromised.

## Data Theft/Loss

Key changes in data theft targets and methods took place last year. Reports of intellectual property (IP) theft increased, and theft of credit card numbers and other Personally Identifiable Information (PII) continued to grow. Hacking, mal-ware and other cyberthreats continued to be a common method of attack.

# TOP PITFALLS TO AVOID WHEN REACHING FOR THE CLOUD

**The imperative of High Reliability, Redundancy and QoS for Stable Cloud Computing**

Cloud computing is one of the most captivating technologies in today's IT world. Cloud computing, with the revolutionary promise of computing as a utility, has the potential to transform how IT services are delivered and managed. The demand for cloud computing solutions is expected to grow exponentially. As a substitute of investing millions of dollars in continuous installation and maintenance, IT managers can rent/ hire required resources from service providers, which are set as a cloud. This approach has led to a paradigm shift in enterprises that hunt for cost-effective solutions to achieve high application performance without a negative impact on IT budget and infrastructure.

## What's the impact of the cloud?

- **On-demand Self Service –** Businesses can automatically extend and grow their service, without complex or expensive investment.
- **Instant, Anywhere Access –** With a central point of access over the internet, organisations can access critical applications, resources or services from any location, making it simple to have a single accessible infrastructure for head office, branch office or remote workers.
- **Rapid Elasticity -** Capabilities can be rapidly and elastically provisioned to quickly scale out and rapidly released to quickly scale in. This can also be done automatically.

## Cloud Deployment Models

It's not just a simple choice when deciding to move to cloud services – there are wide range of different models for deployment.

**Private Cloud -** The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on premise or off premise.

**Community Cloud -** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations).

**Public Cloud -** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services.

**Hybrid Cloud -** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that are bound together which enables data and application portability.

## Top Pitfalls to Avoid

The buzz around cloud computing resonates through every segment of the IT and networking industries. Cloud computing will have a profound impact on corporate networks, particularly wide area network (WAN) performance. Cloud data centres are "far away" from the users. Therefore, all employees will be "remote" from their data. As a result, there are potential pitfalls that can interfere with or negate the benefits of cloud computing.

## Solving the Cloud Challenge

One must consider the importance of WAN connectivity and uptime regardless of the WAN infrastructure a client uses for Cloud Computing (private lines, public, or a hybrid). Companies can ask simple questions like, "what would happen if computing comes to a complete halt due to a failure in the WAN?" to evaluate their need. The best strategy is to combine multiple lines of different carriers so that automatic failover takes place immediately.

There are a number of essential elements to consider, however, when implementing such a strategy.

**Problem 2: Inadequate bandwidth and latency -** A company's bandwidth capacity can impact the end users Cloud Computing experience, especially if critical business applications are in the cloud such as CRM. As Tom Nolle, President of CIMI Corp, a consultant to service providers, said: "You can't write an SLA for the Internet."

**Solution 2: Create a bigger pipe and deploy Quality of Service (QoS)** – companies can use a router clustering device to create a bigger pipe to the internet. Along with the auto line failover they require for high availability to their mission critical Cloud Apps, they can aggregate two or more lines through a router clustering device for the combined speed of the connections. As well as the failover benefits, the monthly reoccurring price of leasing the lines may cost less than leasing one big line.

## Single Site Redundancy and Reliability for WAN Computing End Users

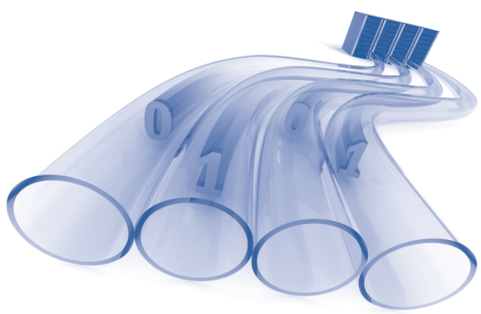
The greatest challenge for enterprises or end-users that deploy cloud computing from an infrastructure point of view will be making sure that they always have access to the remote data centres which contain these services. While many larger offices would likely use MPLS or other private line technology to access these data centres, that still leaves open the potential for an outage on that private link. Smaller offices may only use Internet-based connectivity to access these data centres, and again will require the ability to failover in the event that their primary Internet connection fails. In both these scenarios, some type of inexpensive

**Problem 1: WAN connectivity, reliability, redundancy, availability issues.** The benefits and cost savings enjoyed through cloud computing are dashed if their data connections fails. Private and public WANs share potential points of failures, such as an ISP physical line failure. A loss in connectivity leads to a total disconnect to all of the cloud resources, from CRM to VOIP. This can stop an entire business running, and have catastrophic impact.

**Solution 1: Router Clustering -** Companies using cloud computing Services can bypass connectivity issues by using a router-clustering device at each location. Router clustering devices aggregate any type of data connections, such as T1, DS3, DSL, cable, wireless, MPLS, etc., and provide intelligent and automatic failover when services or components fail. A router clustering device can aggregate lines of same or different types from different providers, which increases reliability substantially. This gives the power back to the end user, and gives the end user real peace of mind that its network is up and running despite failures. Router clustering devices will failover all WAN data traffic, including VoIP calls and Thin Client Sessions seamlessly.

data lines (e.g. internet broadband based), will be required to ensure uptime for offices utilising cloud computing to cut costs and improve productivity.

FatPipe products provide the perfect solution to the requirement for WAN redundancy for these cloud computing customers or service providers. With the ability to provide automated failover along with several load balancing algorithms, FatPipe ensures that businesses deploying Cloud computing solutions remain up and running even in the event of a link failure. FatPipe provide the highest level of VPN security, fault tolerance, and speed for mission critical VPNs meaning corporations can deploy VPNs anywhere in the world and still get the highest quality of service using local providers by aggregating any combination of DS3, T1, E3, E1, DSL, wireless, and cable lines. With increased bandwidth, bidirectional load balancing, and line failover utilizing the multiple connections, the solution provides redundancy and VPN load balancing benefits without BGP or any special equipment or software, as well as providing up to 9x the WAN security compared to using IPSec.



## WAN Acceleration and improving the user experience

When preparing for cloud computing implementation, IT managers have the choice of adopting public, private, or hybrid clouds. These differ in the aspects of security and control over data that determines the usefulness of the cloud services. Generally, private clouds deliver a reliable security level for a company's sensitive data, and control over mission critical applications. However, the crucial factor that many companies fail to look is uptime having a huge impact on disaster recovery and business continuity. Private lines are more expensive than public lines, and can prevent a company from getting the line speed to support cloud computing.

When companies expand, IT administrators are challenged to control issues of high latency and excess bandwidth usage. Mission critical applications require higher priority because they require adequate bandwidth and rapid transfer rates. On adopting optimisation, companies using cloud services discover a major reduction in their capital investment with an increase in overall business productivity. Whether the company using cloud computing services has one or multiple locations, FatPipe can provide the redundancy and high-availability required for cloud computing implementation. Companies can also benefit from implementing QoS to best utilise the current lines they use.

FatPipe's WAN Acceleration technology offers the highest performance level of WAN acceleration and optimisation available using patented and patent pending technology. With FatPipe WAN Acceleration, organisations can significantly boost WAN performance through acceleration of applications, and better utilisation of the current WAN infrastructure. Bundled with cloud computing solutions, FatPipe's WAN Acceleration can ultimately result in saving you thousands of pounds a year on additional hardware, software and bandwidth costs. With Fatpipe, organisations can benefit from:

- **High Performance -** Achieve faster results with WAN acceleration over multiple data lines for even faster speeds
- **De-duplication** - Between 4 to 18 times average data reduction - e.g. 400mbps of LAN traffic becomes 40mbps on the WAN
- **Works with Single and Multiple Lines** - Support either single lines, or combine multiple connections for the ultimate reliable, redundant, efficient, optimised and secure WAN
- **Site Load Balancing**—Provide resiliency and continuity for cloud computing across multiple sites

Cloud computing is an evolving paradigm within the IT industry and one that will only gain momentum as more and more enterprises realise the significant cost savings and capital expenditure savings which can be enjoyed. End-users must have reliability, security, redundancy, availability and scalability built-in to their WAN infrastructure to ensure that they can take advantage of the cost savings created by Cloud computing solutions. FatPipe's technology and products bridge this gap and empowers Cloud solution providers and their customers to confidently address WAN challenges.

**Problem 3: Slow speeds and latency between remote offices and HQ:** A company may MPLS for core HQ connectivity, but remote offices may struggle to use an inefficient VPN over slower lines.

**Solution 3: WAN Optimisation** between remote offices and HQ can optimise traffic between the remote or branch sites and the head office, to other cloud services and even optimise specific traffic flow.

# EMERGING TRENDS INCREASE THE NEED FOR MULTI-LAYERED ENDPOINT SECURITY

**By Leonid Shtilman, CEO, Viewfinity**

Most well-known breaches have been executed by intruders targeting a particular organisation or entity with a specific intent. The attacker's software is compiled and packaged during the final moments just before the attack, thus often rendering them unknown and unidentifiable to conventional perimeter security protection mechanisms. Some attacks were done by foreign entities, some possibly even by foreign governments, and were politically motivated. These political attacks are very well organised by a group of people united by a common agenda. However the data breach evolution is not so much cyber warfare any longer, rather it's more along the level of cyber civil warfare launched by hacktivists. What we're seeing evolve are attacks that are now full-out, well planned cyber robbery and cyber civil warfare.

Increasingly, today's enterprises are recognizing that it is necessary to implement a very layered and granular approach to endpoint security in order to succeed.

The increasing incidence of Advanced Persistent Threats (APT) makes it clear that organisations should move to a locked down environment to ensure their users can't install rogue software on the network (whether purposely or by mistake). For example, the recent issue of government keyloggers being secretly installed and invoked on endpoints could be thwarted by privilege management software restraints. A highly-regarded opinion among IT professionals is that controlling rights on personal computers and servers is a crucial part of any security solution. Adhering to the principle of least privileges is in the best interest of all companies, whether commercial sector, healthcare, within government agencies, etc.

There have been a lot of stories about the potential for attacks on critical physical infrastructure, and now unfortunately the stage has been set for a real attack. Local critical infrastructure attacks will likely happen – someone will shut down an area of a country, the electric or power grid for example. Looking ahead, there is a real call to action for more security around those communications networks.

Security is a moving target because it's twofold: companies should not only invest in new security software, but they should change the way employees work. Most companies think that if they implement traditional technologies (antivirus, firewall) and use sophisticated passwords, it will be enough. Our ever-changing environment requires several layers of protection. Only IT personnel should have administrative passwords, and they should be kept in a vault and handled only through identity management techniques.

Companies are most ill prepared to handle privileged accounts, which are the basis, or entry point if you will, for all attacks. Perpetrators take over these accounts, or gain access through these accounts, to further penetrate your environment and take over servers and other IT infrastructure sources.

**The ideal solution is to set up a risk-based application control framework that doesn't necessarily block all unknown applications but instead establishes default behavior for managing applications not yet classified by your organisation.**

A good many years ago, progressive thinkers in security put forward whitelisting technology as the perfect enhancement and compliment to antivirus' blacklisting strategy as a way to counter the fast-moving, polymorphic malware that was just then starting to bombard signature-based blocking mechanisms. The constant stream of zero-day attacks and malware variations has made it necessary to utilise many layers of protection to effectively combat the infiltrations. In today's highly vulnerable online corporate environments, careful control of applications and user-privilege levels are the very foundation of IT security. Most IT professionals agree that controlling which applications are allowed to run in your environment and reinforcing that

protective layer by allowing standard administrative rights only are the best practices for reducing security risks.

The ideal solution is to set up a risk-based application control framework that doesn't necessarily block all unknown applications but instead establishes default behavior for managing applications not yet classified by your organisation. These are applications that are not yet part of the white or black lists and are allowed to run on the computer but in a restricted "greylist mode" with limited privilege rights and access to resources. Through automation, greylisted applications are processed and either whitelisted or blocked. If whitelisted, the application continues to run in standard user mode only and administrative privileges are managed with software.

This combination adds a fortified level of application security currently unheard of with the typical whitelisting strategies seen today.

Viewfinity's customers are very successfully securing their endpoints through efficient and simple management of administrative rights and they have asked us to extend our privilege management capabilities to include full application control and whitelisting. Application whitelisting, managing trusted sources, forensic analysis and monitoring, and utilisation of reputation databases are natural extensions to our current solution. There is great danger if administrative rights are allowed in a whitelisting model: users that retain administrative rights may attempt to bypass or uninstall application control agents, and attackers may target the whitelisting mechanism to get bad code recognised as legitimate.

Not only are there security benefits, but there are also significant cost reductions when exerting more restrictions on end-user desktops with application control. Most projects will see a reduction in help desk calls and the need to reimage endpoints as benefits of application control software. We took our customer's advice, and the advice of prominent analysts who follow this market, to create a winning combination to ensure a "Least Risk Environment." We're pleased to be the first and only vendor to offer an automated method for handling unknown applications, the greylist capabilities, so that users may continue to work without interruption.

Taking a layered approach to security is critical - current events show this is a problem that isn't going away. This trend will continue to dominate the security landscape with increasingly elegant solutions emerging to create customised and meaningful privilege management regimes. As more organisations move away from Microsoft Windows XP and embrace Windows 7 or 8, the challenge of reducing the cost and complexity of managing endpoints will only increase.

# DO UNNECESSARY AND UNCONTROLLED ADMIN RIGHTS RISK CORPORATE SECURITY?

A recent survey of more than 600 IT security professionals found that the majority of respondents – 68% - do not know who in their organisations has local administrator rights.

Following the 68% who did not know who had local administrator rights, 20% of those said that between 15-30% of their user base still had administrator rights on their Windows-based endpoints.

**So why do users still have local admin rights?** The survey showed that:

1. 35% claim they need admin rights to do their job
2. 30% said it's because local admin rights have not been removed
3. 19% said local admin rights are tempo-rarily reinstated due to user need (i.e., "privilege creep")
4. 16% did not know - they were unaware that they had admin rights

"Admin rights" can be used by malware to install malicious software on local computers through the administrator account. Further penetration into the IT environment is then accessible through this vulnerability allowing other security threats to enter a corporate network.

"*A moderately managed user loses $586 in productivity due to time spent on self-administration, fixing system problems and downtime. However, this means users have to enlist IT for application installation support, and they incur costs when they have to wait for IT to install applications for them. We estimate this cost to be $38 per transaction, based on the salaries used in the travelling notebook user TCO model (which would have a user mix similar to developers and engineers). Therefore, when you add direct and indirect costs, the total cost of a help desk call for application installation is between $58 and $73*"
Gartner: The Cost of Removing Administrative Rights for the Wrong Users. Terrence Cosgrove, 2011

*Privilege management and application control tools help achieve total cost of ownership (TCO) reasonably close to that of a locked and well-managed user, while giving users some ability to control their systems*
Gartner: The Cost of Removing Administrative Rights for the Wrong Users Terrence Cosgrove, 2011

# DEBUNKING DATA ENCRYPTION MYTHS

**Data encryption is a major headache for the user and IT**

When computer processors were less powerful, data encryption significantly slowed system performance. As a result, data encryption was established in many people's minds as a technology that caused poor performance. Fast forward a few years and encryption operations are performed silently and efficiently in the background - even in mobile devices. Today, IT professionals advocate the universal use of encryption on all computing devices within. Most agree that these solutions must be implemented in a way that can be managed and monitored consistently via central administrative management tools that deploy and maintain the encryption software transparently, with minimal impact on users. Individual solutions should be compared on a point-by-point basis to see how they measure up.

**There is no compelling reason for encrypting personal or corporate data**

Protection of assets (the primary reason for encrypting data) encompasses two major concerns that are fundamental to organisations of any size:

- Meeting regulations that apply to the protection of private individual data.
- Preventing unauthorised access to information that could impinge on intellectual property issues, offer unfair advantages in competitive relationships, reveal sensitive product roadmaps, engineering plans or unpublished financial results, or put an organisation in an uncomfortable position if exposed in the media.

Data encryption backed by a solution that ensures organisation-wide compliance would serve these goals very effectively.

**OS-Based encryption protection is sufficient for enterprises**

Encryption capabilities available through operating systems (OS), like Microsoft's BitLocker, do offer some degree of protection against data breaches. However, these single-dimensional solutions lack the rigor, manageability, cross-platform support and more comprehensive encryption features that characterize serious enterprise encryption solutions.

**Comprehensive encryption solutions for enterprises are too expensive**

You can currently buy a laptop for as little as £300, but if the information on that laptop is compromised, the financial repercussions can dwarf that expense. In a study released by the Ponemon Institute, it was determined that the least significant aspect of the loss was the actual cost of replacing the laptop. The results of the financial loss assessments were astounding and included the following statistics:

- The average cost of the laptop losses of organisations surveyed was $6.4 million for each company.

**$6.4M** is the average cost of laptop loss for a company

**30%** of corporate laptops are encrypted, despite most containing confidential data

- The combined laptop loss for those organisations was $2.1 billion.
- 46% of the participants said the lost laptops contained sensitive or confidential data, but only 30% were encrypted.
- The average cost per lost laptop, considering all factors, was $25,454.
- Use of encryption can reduce the cost per lost laptop by $20,000.

Furthermore, data breaches can cause long-term, if not irreparable damage to an organisation's reputation. In one example, a data breach at an American University exposed 31,000 names, health records, financial data and social security numbers! The upshot? Not only was this breach an embarrassment to the school, but something that severely impacted the confidence in the integrity of the institution.

The challenge with data security solutions for most organisations is balancing the expense of the solution against the productivity of the users, thereby maximising the TCO of the solution.

A recent study from the Ponemon Institute looked into what an encryption solution would cost an average organisation per year. The results were shocking. What became apparent was that with features like pre-boot network authentication (WinMagic's PBConnex), data encryption solutions could help reduce TCO by not only managing encryption and security but improving the efficiency of other processes for IT Administrators such as support. Looking at typical costs associated with password resets and device staging alone, the savings were staggering.

WinMagic provides the world's most secure, manageable and easy-to–use data encryption solutions, with a focus on reducing TCO for customers as well as enterprise class security.

# INDUSTRY UPDATE

## IS THE AGE OF THE DESKTOP PC REFRESH DEAD?

New figures from Gartner, Inc. are confirming an emerging trend: PC shipments are in decline, and so is the future of the corporate PC desktop refresh cycle as tablets enter the scene in earnest.

Gartner research shows that worldwide PC shipments declined 4.9% in Q4 2012 compared to 2011. There will be some individuals who take on the new low-cost tablets as well as a traditional PC experience, but Gartner believes they will be exception and not the norm, as shared PCs will abound in the workplace.

The key word here is "shared." The necessity of having one fat-client PC desktop per employee is no longer the only solution for the enterprise. The PC environment, in turn, is quickly going virtual, as enterprise IT departments turn to desktop virtualisation as a means of forgoing the costly "new desktop system for everyone" refresh cycle.

This demonstrates the appeal of desktop virtualisation, and why shared computing has so much potential - offering a solution to both the challenge of BYOD and the fiscal cliff of the imminent desktop refresh. NComputing's portfolio of desktop virtualisation solutions, multi-OS client and the HDX Thin Client that's optimised for Citrix provides a compelling reason to move towards VDI.

## FINDING THE CODE TO SIMPLE USER PROVISIONING

A high cost element in the implementation of any new IT system is often migrating users, and 2FA (Two Factor Authentication) is no different. The key to user engagement, and lower support costs, is ease of use.

As well as reduced cost, the familiarity of using mobile devices has other benefits. Users are very sensitive to the whereabouts of their phone mobile device, meaning loss or damage is often noticed and rectified promptly, while devices are easy to back up and restore if found or replaced. In addition, more intuitive deployment and user provisioning methods can be used—such as the innovative use of QR codes, increasing security and helping reduce support calls and failed installations.

Celestix HOTPin addresses these issues head on and delivers a solution that does not compromise the core purpose of the solution, to secure the user's identity from theft.

## THE TRUE COST OF CLOUD AUTHENTICATION

What is the true cost of moving to the cloud for your authentication? It's not just about the upfront licence.

Once you get over 100 users, the cost of the management rises to around 70% of the total project cost—and that figure stays consistent as users increase. Therefore, for mid size and enterprise deployments, the ongoing costs for change resolution, housekeeping, upgrades and onboarding is significant enough to mean savings of 60% are possible with cloud authentication.

"**Gartner predicts that, by 2017, more than 50% of enterprises will choose cloud-based services as the delivery option for new or refreshed user authentication implementations, up from less than 10% today**."
-Gartner Magic Quadrant for User Authentication 2012

SafeNet Authentication as a Service is the industry's first true cloud authentication platform, offering dramatically lower TCO for authentication with the widest choice of tokens and simple migration for users of legacy solutions.

## CURB THE THREAT AND NOT THE DEVICE

In last decade we have witnessed a huge change in market and usage of mobile devices, from personal usage to BYOD and CYOD (Choose Your Own Device). What risks are presented by this change, especially in small businesses?

**Unknown applications—**Android, in particular, offers the ideal entry point for malware or malicious applications, even for those devices that have been allowed for corporate use.

**Missing Authentication**—with a range of new OS types to deal with, and devices no longer domain members, how can IT fully track user activity?

**Lack of logging and report**—with increasing complexity, roaming users and multiple network devices, the challenge is on for a single view of an entire organisation.

Cyberoam's UTM appliances provide granular, identity based security and reporting enabling SMBs to enjoy enterprise benefits, all managed from a simple management interface.

# VISUAL DATA SECURITY:

## STRENGTHENING THE WEAKEST LINK

With increased mobility and versatility of data, most organisations and individuals have taken at least some action to protect themselves through the installation of security software and hardware. According to Secure, the European Association for Visual Data Security, one core area of data security which is often overlooked is the potential for sensitive, personal information and data on-screen to be seen, captured and used by unauthorised individuals.

Security risks are present wherever data is displayed on screen – whether on Smartphones or tablets, laptops to desktop PCs; and the threats are ever-present both inside the office and out. Users face increasingly frequent and innovative data attacks, so organisations must ensure that the defences they have in place protect against all potential data breaches and not just some.

**Breaching visual data security is easy**

Visual data security breaches can happen in a number of ways. Unauthorised people can view sensitive information while it is displayed on the screen; they can readily capture images of sensitive information using high resolution digital cameras or camera-equipped Smartphones and tablets. Passwords or other sensitive information displayed on the screen could subsequently be used by an unauthorised person to access other systems. Private data could be downloaded onto a computer for further examination and quickly shared with others via the Internet, email or social media.

This is more than a purely hypothetical threat. A 2012 survey conducted by the UK Polling organisation ComRes , found that nearly three-quarters of employees surveyed, 71%, have been able to see or read what someone is working on – either in the workplace or in a public place such as on a train, in an airport or a coffee shop. Furthermore, 57% of people surveyed for the Visual Data Security Study 2010 said they had stopped working on their laptops in public through concerns over privacy. A survey of IT professionals conducted by BH Consulting for this study found that 82% of respondents had little or no confidence that users in their organisation would protect their screen from being viewed by unauthorised people.

*"You spelled 'confidential' wrong"*

**But what's the impact?** Security breaches resulting from intruders hacking into a computer network or from a computer virus infection can be easily proven through evidence gathered in log files and other mechanisms; but with visual data they are harder for organisations to identify.

**71%** of employees have read other people's work in a public place.

**So the threat is real - what's the response?** The industry is raising awareness of visual data security across Europe by working with partners in industry and government. As a first step, it recommends a thorough and systematic analysis of the sensitivity of data, it's location and method of access. This enables organisations to take action such as enhancing security of remote working and restricting access through public networks, such as roaming Wi-Fi connections.

Training is another important part of countermeasures. Users working in public places should be encouraged to be aware of their surroundings and to ensure that data on their screens cannot be overlooked. They should also be trained to turn off their computers if they feel their screen is being observed. Information on unattended screens should be protected by the use of password protected screen savers.

Best practice procedures such as the ISO 27001:2005 Information Security Standard and The Standard of Good Practice for Information Security developed by the Information Security Forum – explicitly require organisations to take steps to ensure the visual data security of their information.

**Getting physical with security**

For those users who regularly work on sensitive information in public areas, privacy filters should be deployed on the screens to reduce the risk of data being overlooked by unauthorised personnel. The diversified technology company 3M has developed a growing range of filters designed to protect not just computer displays and laptops, but also tablets and smartphones, from prying eyes.

Privacy Filters from 3M black out the screen to everyone but the user sitting directly in front of it without compromising functionality, and allowing for easy removal. However, even with privacy filters installed, attention still needs to be paid to the siting of fixed equipment and workstations. Computer screens should be positioned and angled to make it difficult for unauthorised personnel to view them, with screens near windows positioned so they cannot be viewed from outside. Staff members who work from home, remote offices or public places should be advised similarly how to position their devices.

Through analysis, technology and training, organisations can ensure that poor visual data security is no longer the Achilles heel of their security framework.

# WHO TO SEE AT INFOSEC

**Stand F35**

Absolute Software is the industry standard in firmware-embedded endpoint security and management solutions for computers, laptops, and ultra-portable devices – and the data they contain. Absolute Software, a leader in device security and management tracking for more than 18 years, has over 30,000 commercial customers worldwide.

**Stand F86**

Cyberoam is a leading global provider of network security solutions offering comprehensive security for networks of the future. Cyberoam's Identity-based UTM appliances integrate multiple security features, over a single platform. Cyberoam is accredited with prestigious global standards and certifications like CheckMark UTM Level 5 Certification, ICSA Labs etc.

**Stand E62**

Celestix is a leading provider of two-factor authentication and secure remote access solutions. Our products enable organisations to enforce strong security controls for both users and devices when requesting access to corporate resources. The company also provides solutions for Microsoft DirectAccess, simplifying remote access.

**Mayfair Room (Meetings on Application)**

Lumension Security, Inc., a global leader in endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. At InfoSec, Lumension will be hosting 1-to-1 briefings and product demonstrations for key partners.

**Stand F85**

SafeNet is a leading global provider of data protection. For over 25 years, Fortune 500 global corporations have turned to SafeNet to secure and protect their most valuable data assets and intellectual property. SafeNet's data-centric approach focuses on the protection of high value information throughout its lifecycle, from the data centre to the cloud

**Stand L71**

Viewfinity provides privilege management and application control for desktops, laptops and servers, empowering enterprises to meet compliance mandates, reduce security risks, and lower IT costs. The Viewfinity solution allows enterprises to control end user and privileged user rights for applications and systems which require elevated permissions.

**Stand H50**

Websense is a global leader in providing comprehensive security technology at the lowest total cost of ownership. Our products allow organisations to safely use social media, cloud applications and mobile devices, while protecting against targeted attacks, advanced malware and the loss and theft of confidential data.

**Stand H85**

WinMagic is trusted by organisations worldwide to minimise risk, meet compliance regulations and protect valuable information against unauthorised access. WinMagic's SecureDoc full-disk encryption suite provides protection of data-at-rest stored on desktops, laptops, and other mobile devices by encrypting all data on the disk.

# DIFFERENT SHADES OF CLOUD WI-FI: REBRANDED, ACTIVATED, MANAGED

All "Cloud" Wi-Fi is not created equal
The race is on to put cloud in Wi-Fi. Currently, the cloud managed Wi-Fi space is expanding rapidly. Naturally, Wi-Fi vendors, traditional and emerging, want to be in the cloud Wi -Fi game. Nobody wants to be without a "cloud" solution! Controller -less Wi-Fi vendors have explicitly built cloud-managed Wi-Fi from the ground up, while controller Wi-Fi incumbents have repositioned traditional offerings in the direction of cloud Wi-Fi.

**The word "Cloud" in the name doesn't tell the whole story**
When vendors associate the word cloud with their Wi-Fi solutions, they can be referring to a wide disparity of technology and capabilities. This is quite apparent in light of some recent developments.

**Is your cloud Wi-Fi genuine, or is it controller over WAN imitation?**
With rising popularity of the cloud Wi-Fi in distributed Wi-Fi deployments, there is also an attempt to pass off the legacy controller technology as the cloud Wi-Fi by deploying conventional controllers over the WAN. Realising that it is not feasible to deploy many smaller controllers in the distributed Wi-Fi deployments such as retail, remote offices, etc., the controller over WAN architecture deploys bigger controllers at the HQ and calls it a cloud Wi-Fi. However, the controller over WAN Wi-Fi does not measure up to the true cloud Wi-Fi for many reasons.

**Controllers over WAN rebranded as Cloud**
Often legacy systems merely change the product name but does changing terminology get controllers to measure up to the true cloud? Controller over WAN cloud Wi-Fi is merely the practice of deploying stack of controllers at headquarters to manage APs at the branches. However, such an architectural approach is severely limited and doesn't render all the good properties of a true cloud Wi-Fi. This was made quite evident when Cisco recently acquired a cloud Wi-Fi startup to gain entry in the cloud Wi-Fi game. There are many traditional Wi-Fi vendors who still call it a cloud Wi-Fi if you simply deploy controllers over WAN links.

**Cloud ACTIVATED Wi-Fi**
Another vendor recently announced the launch of its cloud-based Wi-Fi provisioning service. Although it includes the term "cloud", it is important to note the use of the word "provisioning"! On a closer look, this solution appears to be merely a cloud based AP inventory system which leads in with the cloud but then redirects the APs back to the onsite controllers or to the onsite AP management servers. The APs communicate with the cloud provisioning portal as the first point of contact, but then they have to connect to the onsite controllers or the onsite management servers if the centralised management benefits are to be achieved. The cloud provisioning portal just tells the APs the addresses of their onsite management servers.

## So what are the real drawbacks of imitation cloud?

**Equipment deployment and management overhead:** True cloud Wi-Fi relieves the enterprise IT from the overhead of deploying and managing excess equipment. In the controller over WAN architecture however, enterprise IT is responsible for deploying and maintaining controllers at the HQ. For high availability, it is required to deploy redundant controllers. Additionally, if the controller-based architecture is multi-layered such as controller layer, services layer and console layer, the equipment overhead occurs at multiple layers of the architecture.

**Dependency on the health of the WAN link:** To cite an example, one large vendor's deployment guidelines recommend reserving 12.8 Kbps WAN bandwidth with 300ms round trip guarantee between each remote AP and the HQ controller for CAPWAP control messaging (for data+voice, it recommends 25 Kbps with 100ms round trip guarantee). This bandwidth is presumably required to support delay sensitive and continuous "chatter" of control messaging occurring between the remote AP and the controller. The more the chatter, the higher the chances of service degradation due to problems over the WAN links. True cloud does not require any bandwidth reservation thus making it much more reliable compared to the controller over WAN.

**Lost access functionality at the edge**: Controller over WAN Wi-Fi offers degraded functionality when the WAN link is down or when the controller fails. For example, when the controller fails or when the WAN link to the controller is down, remote APs turn off important access services. For example, they turn off guest WLANs as these guest WLANs require functions such as click-through splash page, sign-on splash page and redirection; which needs controller co-ordination. On the other hand, true cloud Wi-Fi does not have such controller dependency, so access services will be up independent of what happens to the branch connectivity to the HQ.

**Security failure at the edge**: Controller over WAN Wi-Fi can drop security cover if the WAN link goes down or the controller stops running. For example, the entire security cover (which is weak to begin with anyway) evaporates if the AP loses connectivity to the controller. That includes IDS, IPS, rogue detection, and PCI. With the true cloud, APs are built as intelligent devices which maintain the security cover even when they are not talking to their cloud manager. In the true cloud architecture, security at the edge is not degraded when APs lose contact with the cloud manager.

**Complexity of configuration**: Force-fitting controllers into the cloud results in complex and error prone network configuration and management. Network admins have to work with distinct silos of configuration domains such as controller groups, mobility groups, AP groups, and WLAN IDs; and cross referencing among them. True cloud, on the other hand, offers intuitive web based console with elegant configuration and network management workflow which directly relates to the way network is organised from functionality perspective and not controller perspective. While superior user experience is difficult to describe in words, it becomes instantly apparent as soon as the controller over WAN configuration interface is viewed side by side with the true cloud Wi-Fi console.

**So what is genuine Cloud Managed Wi-Fi?**

Typically cloud-managed Wi-Fi should have the following comprehensive set of features:

- Plug-and-play deployment and configuration of APs
- Centralised network management and monitoring, and comprehensive security – entirely in the cloud!
- All the server side complexity for device, network and security management is subsumed in the (public) cloud
- End users don't have to install onsite stacks of controllers or management servers, which results in large capital and operational savings
- Admins manage the network infrastructure and security from the single pane of glass web based console
- APs are designed to be smart-edge which can operate relatively independently of the management server

There are real differences among the many Wi-Fi solutions despite having the word cloud in them. Indeed, true cloud Wi-Fi is not about throwing controller over WAN link. There is a large gap in benefits between the genuine cloud Wi-Fi and the controller over WAN imitation. Cloud Wi-Fi is a different architectural thinking which enhances the simplicity, reliability, and economics of Wi-Fi deployments.

The moral of the story is that when new technologies arrive, associated buzzwords quickly get into the product lineups. However, the underlying features may differ greatly. One has to look beyond the buzzwords to find out what the specific solution is all about and which benefits of the new technology concept it actually offers.

AirTight Wi-Fi™ - true cloud MANAGED Wi-Fi with the best wireless security built in.

## DOES GOING WIRELESS MEAN ACCESS ALL AREAS FOR NETWORK SECURITY?

Wireless LAN infrastructure attacks are today one of the most critical and immediate threats to enterprise networks. To make matters worse, the consumerisation of Wi-Fi is flooding enterprises with personal smartphones and tablets, which are tearing down the network security perimeter; organisations without an official WLAN are also at risk.

How does this happen? The vulnerabilities are normally:

- **Poor Wi-Fi configuration**: a study found 24% of enterprise APs to be open or using poor security
- **The use of SOHO tech**—the study also found 61% of APs to be basic with minimal management
- **Mobile workers are easy targets**, with poor security habits (such as using open Wi-Fi to connect to corporate systems)
- **Rogue APs**—the ability for corporate smartphones to create their own hotspots can easily lead to backdoors
- **Guest Wi-Fi access** is becoming essential for many organisations - but that means exposing the network to unlimited unknown and uncontrolled devices

The need for a dedicated secure Wi-Fi solution is clear, complementing the existing network but providing essential security that legacy vendors can't provide.

Consistently rated the industry's best wireless intrusion prevention system (WIPS), AirTight is the only vendor to receive the highest "Strong Positive" rating from Gartner two years in a row in its annual MarketScope Report on Wireless LAN IPS. AirTight is also the only vendor to be rated at the top in all Gartner MarketScopes for Wireless LAN IPS till date. Ease of use, automatic device classification and accurate threat detection, and reliable threat prevention differentiate AirTight WIPS from other competing WIDS/WIPS solutions.


Absolute Software

AVIRA

AirTight NETWORKS

Bitdefender

celestix

FAT Pipe

Cyberoam
Unified Threat Management

Lumension
IT Secured. Success Optimized.

NComputing

SafeNet

VIEWFINITY

UNITRENDS

websense

WINMAGIC
DATA SECURITY

XIRRUS

www.e92plus.com 020 8274 7000 @e92plus Argent Court, Hook Rise South, Surbiton, Surrey KT6 7NL