

Mobile Security / Endpoint Control

After another Government departments revealed the number of mobile devices they'd left scattered around the pubs and train seats of the country, the Foreign Office has just coughed up the statistics on how many of its gadgets went missing last year.

Since August 2010 Foreign Office bods lost 28 computers and 37 mobiles phones including standard issue BlackBerrys. Admittedly 12 of the computers and 22 of the mobs were lost overseas, so it is possible that the civil servants mislaid their gadgets while riding camels, ducking under enemy fire or escaping similar sticky spots in the line of duty.

Top Ten Recommendations for Secure, High Performing Endpoint Control:

1. Better performance that's virtually unbeatable

Scan speeds can be improved with a solution that automatically whitelists common Windows OS files. If they don't change, don't scan them, resulting in even better network performance. You also need performance from your VMs, but you shouldn't have to sacrifice protection from the latest threats.

2. Host intrusion prevention so reliable it's on by default

You need advanced Host Intrusion Prevention (HIPS) to stop today's fast moving threats. Your Intrusion Prevention should be so easy to use and reliable so that it's active and automatically cleaning up by default, so threats will be gone before you even knew they were there.

3. Fewer clicks to get more done

Your management console should be easy to use. With a great solution it's easier to find computers, manage alerts, set policies and clean up threats.

4. Web scanning that works in any browser

Web protection that works however users browse, wherever they are. Today, the web is the #1 source of malware. Web Filtering should provide the same security on or off the network and should also help reduce your hardware costs by as much as 50%. An advanced web malware scanning solution uses script emulation, behavioural analysis and all kinds of other clever stuff to block malicious websites before they get to the browser. And live URL filtering means your users are instantly protected from sites known to be bad.

5. Managing access to the riskier bits of the web

The web is a fantastic tool, but you might want to make sure your users aren't browsing to sites they shouldn't be. This needs to be granular so that your users are enabled rather than restricted in their work requirements.

6. Everything your web gateway does, at the endpoint

Know the threat, know what you need to patch. 90% of vulnerabilities can be patched. Yet, many computers are at risk because patching is hard. You have to be confident that you're secure because you need to be identifying, prioritising and scanning constantly for critical threat-related patches.

7. Know the patches you're missing and get smart about patching

One simple scan finds out which computers are missing patches from Adobe, Apple, Citrix, Microsoft, Skype and more.

Patches should always be rated - critical, high, medium and low. You should be told which threats a patch prevents so you can easily identify the most important ones.

8. Easily deploy full disk encryption

Encryption at endpoint is by far the best way to make sure that data stored on desktops and laptops is kept secure. With encryption you can easily encrypt workstations and see their status.

9. Simple management

Encryption should be integrated into other security solution with no separate deployment or console required. Easily install full disk encryption to your computers with just a few clicks. Then check status, policy, and user activity simply in your centralised console.

10. Easy password recovery

We know users forget their passwords. So you need to ensure you can get them back with an easy to use challenge/response wizard.

CONNECT



Welcome to the Winter edition of the nonstop/IT newsletter

Twas the night before Christmas, when all through the house, not a creature was stirring, not even a mouse... Well, that's all very good for Father Christmas but for I.T. teams there are always creatures stirring in the darkness. The fortunate position for I.T. today is that with the right solutions and system management capabilities, you can sleep your Christmas excesses off with a little more confidence that nothing is indeed stirring.

You may have seen the news for Bristol that a groundbreaking partnership between the Bristol City Council and the University of Bristol is going to provide a huge expansion on the city's free access to Wi-Fi internet. This is fantastic news for the city. This will of course enable more smart phone and laptop users to gain connectivity to your business systems. Is this a worry? How are we going to manage this explosion in the growth of "bring your own device"? How can we manage miscellaneous devices wanting to connect to our critical data? Inside we briefly explore how your I.T. departments can manage these endpoint devices centrally and efficiently.

Also in this edition of the nonstop/IT newsletter we are delighted to be announcing that nonstop/IT are the sole reseller for the UK launch of the in-house e-mail archiving solution from ArcMail. We have received great feedback from our trial users; in particular around the ease of installation, scalability and levels of functionality.

www.nonstopIT.com

In this issue...

- UK Launch of ArcMail
- Mobile Usage Statistics Update
- Securing Endpoints
- ArcMail Case Study



We would like to take this opportunity to wish you all a very merry Christmas and a safe and happy new year.

For those of you working on managing systems on Christmas Day, we hope you have a day without major incident and still have time with family and loved ones.

"Happy Christmas to all, and to all a good-night!"

Telephone 0117 370 2200

Contact Us...

T 0117 370 2200
F 08452 605 805
E sales@nonstopIT.com
Bristol Head Office
163 Whiteladies Road, Bristol, BS8 2RN

Your key contacts...

Andrew Wright, Sales Director
awright@nonstopIT.com

Andy Hanson, Technical Director
ahanson@nonstopIT.com



www.nonstopIT.com