



**ESET SMART WHITES**  
White Papers that distil the Essence

---

## Choosing Smart Online Security for SMBs

### IT Security – A Road Too Hard?

IT Security has evolved into a convoluted specialty that sees experts arguing about esoteric topics like academics debating the finer points of the constitution. Enterprises have IT departments and Chief Security Officers to guide them through the jungle that is malware, and the maze of products and services that offer safe passage.

IT security can be a difficult burden on the shoulders of those who run SMBs or home offices. This white paper puts security issues in perspective, explains the arcane business of malware in plain words, examines the key security issues for small/home businesses and offers simple, practical answers to complex questions.

### The Internet – a Boon to Small Business, a Haven for Hackers

US Security expert Bruce Scheiner talks about the 'security theatre', where vendors make their customers feel secure 'by offering protection against threats that were not that great in the first place.' He adds that 'buyers can't tell the difference between good and bad [products]' and that many security vendors 'play on emotion and fear'.

The other side of this coin is how much trouble security experts have in deciding whether a new file or piece of code is malicious or harmless. It's hard to tell the difference between adware and spyware. Microsoft's Windows Genuine Advantage licence check has been compared to spyware<sup>1</sup>, and Sony has been accused of installing a rootkit to prevent its CDs being copied<sup>2</sup>.

The threats may be exaggerated but they are real. The painful ones are:

- **Malware Infections** – viruses, worms, trojans and spyware
- **Data Loss or Data Theft** - most of all business-critical and confidential data
- **Spam Overload**
- **Identity Theft** – more accurately: impersonation with intent to defraud

According to a recent report, businesses are more worried about spam than hackers<sup>3</sup> but malware still holds the top spot. Loss of data is serious but data can be quickly restored from backups. Malware infection is more disruptive to business because it spreads like fire and is almost impossible to contain.

### Endpoint Security – the First Line of Defence

Most attacks are aimed at the 'endpoints', the PCs and laptops that connect users to the internet. Every business has policies, safety checks and fire drills. How many have a code of conduct for the internet? How many businesses ensure that the code is known and adhered to? In security, an ounce of prevention is worth a tonne of cure.

---

1. <http://windowssecrets.com/comp/060615/>

2. [http://en.wikipedia.org/wiki/2005\\_Sony\\_BMG\\_CD\\_copy\\_protection\\_scandal](http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal)

3. <http://www.silicon.com/research/specialreports/thespamreport/0,39025001,10004641,00.htm>

## Conduct Unbecoming

Most disasters aren't caused by hackers or viruses but by ignorant users. Last year, her Majesty's Revenue & Customs in the UK [lost two disks](#) with comprehensive personal data on 25 million British citizens. Also in the UK, a low-level staffer [mailed a copy](#) of the whole national child database to the National Audit Office in London.

Train your staff on sensible, responsible use of the internet. Make sure they don't open email attachments from untrusted sources or visit dubious websites and download free screensavers or programs. Check that they use strong passwords or show them how to create them. Use the resources below or get someone in to run through the essentials.

<http://www.security.iaa.net.au/>

[http://www.dbcde.gov.au/communications\\_for\\_consumers/security/e-security](http://www.dbcde.gov.au/communications_for_consumers/security/e-security)

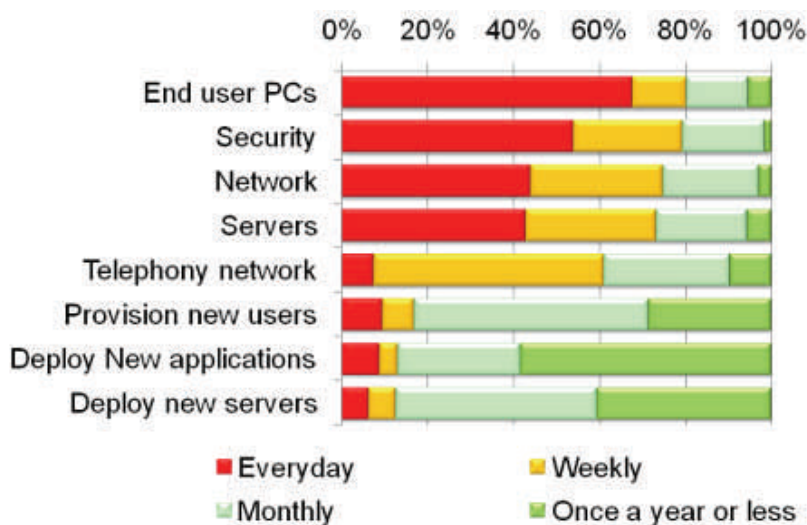
[http://www.dbcde.gov.au/data/assets/pdf\\_file/0007/18952/ISEbooklet\\_06.pdf](http://www.dbcde.gov.au/data/assets/pdf_file/0007/18952/ISEbooklet_06.pdf)

## Secure your systems

Ensure that your PCs, laptops and servers have the latest software patches applied. *Secunia* provides a free 'software inspector', a program that highlights and updates PC software<sup>4</sup>. Ensure that the web browsers on your PCs are secured with JavaScript and have phishing protection enabled<sup>5</sup>. Install a utility like McAfee's Site Advisor, which flags suspect internet sites for users right in the search engine listings<sup>6</sup>.

## Reality Check - Constant threats and Chronic Shortage of Resources

Many SMBs find it hard to feed the IT monster every day. The task is often relegated to a tech-savvy staffer or a roving IT consultant on contract. Many small businesses expect users to shoulder much of the burden. A recent survey conducted by Quocirca in the UK<sup>7</sup> concluded that 'almost 80% of SMBs think it is critical for employees to be able to backup their own devices and many expect them to be able to do day-to-day maintenance.' The graph shows the order of priorities:



4 [http://secunia.com/software\\_inspector/](http://secunia.com/software_inspector/)

5. [http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45\\_qci1241319,00.html](http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45_qci1241319,00.html)

6. <http://www.siteadvisor.com/>

7. <http://www.quocirca.com/pages/analysis/reports/view/store250/item19812/>

The survey also found that over 90% of SMBs provide their employees with laptops and more than half allow access from handheld mobile devices that can expose the company to threats picked up by mobile users in unsecured wireless hotspots. Most SMBs also offer e-business facilities to their customers and partners.

Businesses take these risks in order to remain competitive, but protecting the business is a drain on precious resources. That's the conundrum.

### The Ideal Endpoint Security Product for SMBs – a Wishlist

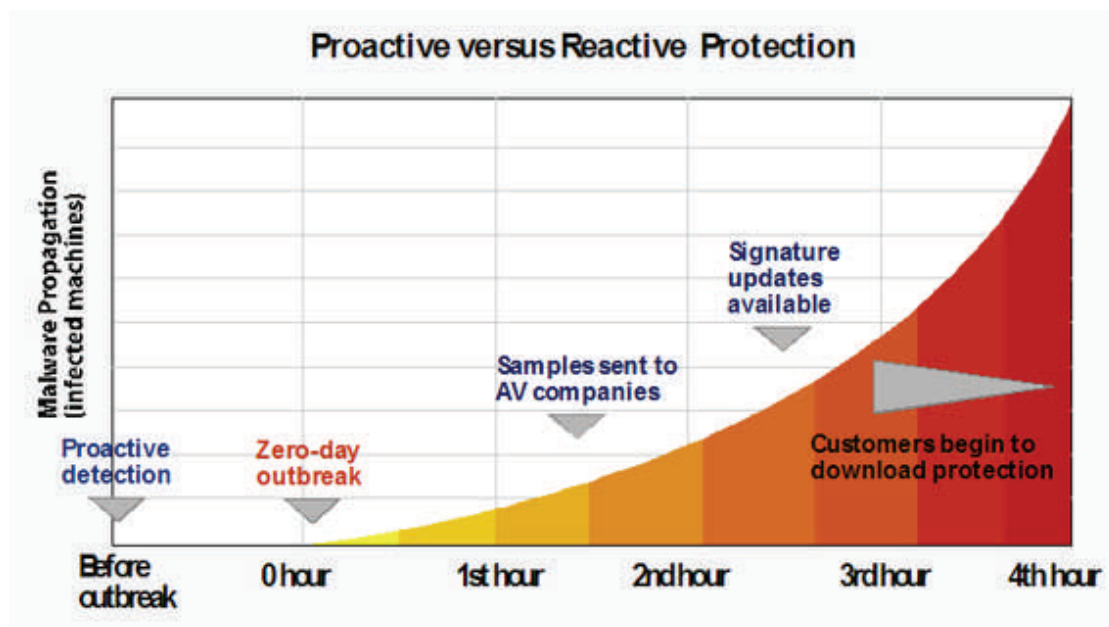
- 100% protection in real-time
- Zero maintenance – set and forget
- Zero false positives – intrudes only when strictly necessary
- Automatic, non-intrusive signature updates
- Zero performance impact on users' PCs
- Low intrusiveness for least impact on user productivity
- Easy to deploy, monitor and update from a central console

No security product provides 100% protection - that remains an elusive goal – but modern security suites like ESET's Smart Security meet the remaining essentials for SMBs, reducing the maintenance burden while raising endpoint security.

### Heuristic/Behaviour Detection is Crucial

Antivirus vendors used to rely on recognizing virus signatures – they still do but also employ heuristic techniques that identify today's 'blended' threats by their behaviour.

In a round of tests conducted by AV-Test.org in March 2008, Symantec and McAfee earned 'satisfactory' marks for 4 – 8 hour response times to respond to new malware outbreaks with signature updates. Microsoft's Forefront came in last on this score<sup>8</sup>. That's more time than a new virus needs to infect every computer on a network.



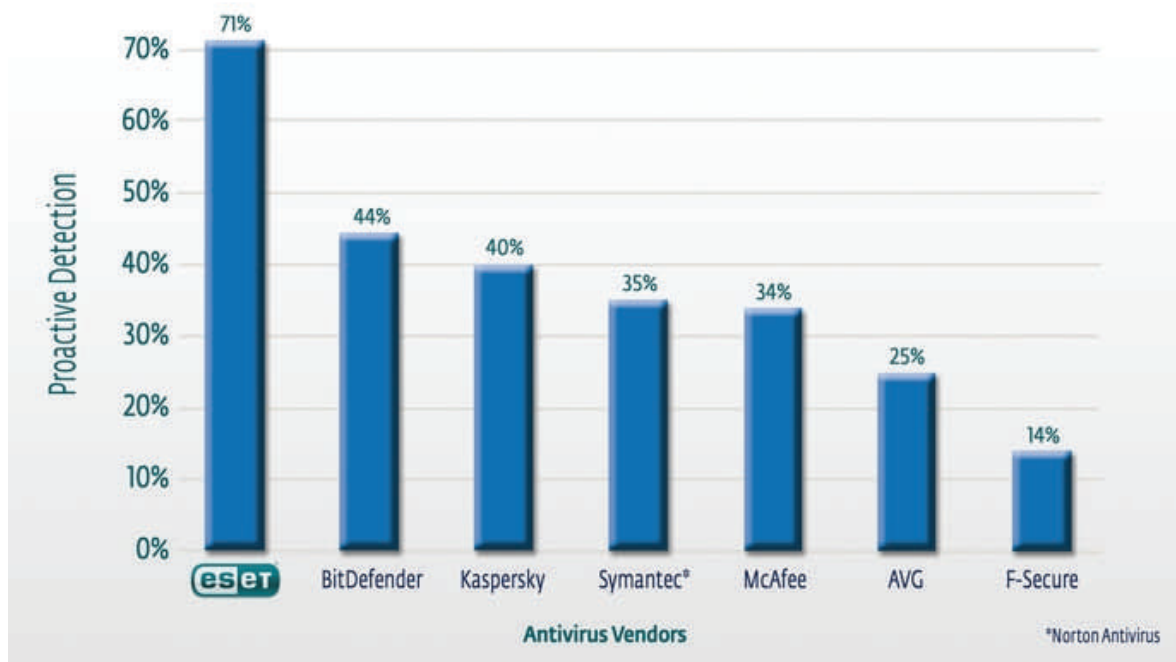
8. [http://www.darkreading.com/document.asp?doc\\_id=144046](http://www.darkreading.com/document.asp?doc_id=144046)



To test the heuristic protection offered by security vendors, test lab AV-Comparatives runs proactive/retrospective tests, which use versions of AV software that have not been updated for up to 3 months. This shows how good their heuristics are at detecting malware that has surfaced since the last signature updates.

Heuristic techniques borrow from artificial intelligence and are still evolving, so it's not surprising that heuristic techniques developed by different vendors vary in effectiveness. What is surprising is the degree of variance.

### Proactive Threat Detection by AV-Comparatives — November 2007



Its outstanding performance in these and other tests have won NOD32 the 'Best AV' award in 2006 and 2007 from AV-Comparatives. What makes ESET's Heuristic Detection so effective is its ThreatSense engine, which affords the highest available protection from zero-day threats. ESET is a pioneer in the field of heuristics - for more technical detail on this aspect of security, please check these whitepapers:

[http://www.eset.com/download/whitepapers/HeurAnalysis\(Mar2007\)Online.pdf](http://www.eset.com/download/whitepapers/HeurAnalysis(Mar2007)Online.pdf)

[http://www.eset.com/download/whitepapers/ESET\\_IDC-VendorSpotlight\\_July2007.pdf](http://www.eset.com/download/whitepapers/ESET_IDC-VendorSpotlight_July2007.pdf)