

Faster, Smaller, Easier.



NOD32 Case Study

Company
Christchurch Polytechnic
Institute of Technology (CPIT)

Sector
Tertiary education

Senior Security Consultant
Erica Griffith

IS topography
2,000 PCs; 150-200 Apple Macs;
assorted PDAs and wireless
handheld devices running on
Windows with a Novell backbone
and using Novell GroupWise email

- Security issues and needs**
- Risk points: Internet gateways; email; web services; remote devices (laptops, PDAs and wireless handheld devices); external hard drives; pen drives
 - Compelling event: Significant price increase following license renewal
 - Key requirements: An accurate antivirus system with a lightweight footprint to minimise impacts on PC performance. Automated rollout and administration.

Solution
ESET NOD32 user since 2008

Location
Christchurch, New Zealand

Website
www.cpit.ac.nz

Faced with escalating threats, antivirus vendors keep adding extra layers of protection to keep their customers safe. However, it comes at a cost, as increasingly heavy-duty protection saps systems performance. But what good is a flak jacket when it's made of lead? It might repel shrapnel, but it's hell for moving out of harms way.

Keeping the IT environment safe, without degrading systems performance, Christchurch Polytechnic Institute of Technology (CPIT) senior security consultant Erica Griffith chose ESET NOD32 to keep the South Island tertiary institution fully protected.

Administration headaches

Two critical factors drove CPIT to re-evaluate IT security: administration efficiency and cost. While its incumbent system offered adequate protection, managing client engine upgrades was troublesome. A Novell user, the absence of Microsoft Active Directory was a stumbling block. Making matters worse, CPIT senior security consultant Erica Griffith says various attempts to solve the problem using third-party tools failed. "After several attempts with different tools we still couldn't reliably confirm that server and virus engine definitions were up-to-date, or whether engines were running at all." CPIT eventually developed a programme that polled individual PCs to check registry settings and file definitions, coming to rely on this workaround rather than inbuilt reporting provided by the vendor. While it went some way to fixing the problem, a significant price hike tipped things over the edge. "We expected a price increase, but the scale of it forced a rethink," Griffith says.

Re-evaluation

In the market for a new antivirus system for CPIT's 2,000-plus PCs, Griffith deduced that so-called brand leadership did not necessarily correlate with performance. "Some of the lesser known brands deliver exactly the same – if not better – all around performance than so-called big brands," she says. CPIT's evaluation focused on footprint, systems resources, and cost, as well as traditional antivirus functionality. "We tested NOD32 and other products against our incumbent provider and were sold on reduced systems resource requirements, ease of use, management, rollout and configuration," Griffith says. In Griffith's mind, virus detection accuracy is reasonably even across a clutch of tier one offerings. Leading independent virus research authority Virus Bulletin Magazine [UK] has found that NOD32 is the only product that has not missed an in-the-wild virus in 46 separate tests over nine years. Griffith says NOD32 satisfied CPIT's technical and financial evaluation, but reference checks swung the final decision. "I was really surprised by the number of large organisations running NOD32. Talking to a few of them reinforced our final decision."

we protect your digital worlds



“We tested NOD32 and other products against our incumbent provider and were sold on reduced systems resource requirements, ease of use, management, rollout and configuration,”

*Erica Griffith, senior security consultant,
Christchurch Polytechnic Institute of Technology (CPIT).*

Smaller overhead, less frustration

CPIT has reduced end user frustrations and streamlined systems management. “From the outset the aim was to reduce administrative overhead and address user frustrations,” Griffith says. “NOD32 has an extremely light footprint – one of the lightest, as far as I can tell. Other systems we tested used more than 100MB of client disk space, while NOD32 uses only 40MB. The same goes for RAM requirements – one system used about 50MB of RAM idling, whereas NOD32 clocked around 3MB.” But more than just leaner system requirements, intelligent virus scanning functionality modulates CPU usage according to PC user behaviour. Griffith explains: “If a user is sitting at their machine, but not using it, virus scanning will use the entire CPU – because the system is idle. However, when the mouse is moved, CPU usage immediately dips back down to around 10 percent. The other systems we tested don’t do it efficiently.” The upshot is fewer user complaints – a sound indicator of IT effectiveness. “Most people haven’t even realised that we’ve changed antivirus providers. However, the people who used to complain about slow scanning speed and sluggish performance have definitely noticed the benefits. I haven’t had a single complaint – that’s a huge plus for us,” Griffith says.

Administration wins

Pleasing end users is one thing, but slashing administrative overhead by two fifths is quite another. Griffith says managing IT using NOD32 is a case of “set and forget”. NOD32 offers a compact suite of management and reporting tools. A central mirror server automates aspects of administration, such as installation, which automatically replicates a pre-configured set-up on all clients, and administers NOD32 updates. A console offers centralised visibility of enterprise-wide client updates and viruses detected. “We’ve retained the same level of security accuracy, while substantially reducing the time it takes to administer the system,” Griffith says. “We no longer have to run our own reporting module or spend days updating scanning engines. I simply put files in the appropriate locations and our scripted roll out tool handles the rest,” she says. As a footnote, Griffith adds that buyers of new software should always consider the ease of de-installation. “Getting our previous AV product off some machines was an absolute nightmare,” she says.

we protect your digital worlds

