

Company

AUT

Sector

Tertiary education

Technology services manager

Russell Barron

IS topography

5,000 desktops; Novell, Windows and Linux platforms; Novell Groupwise email

Security issues and needs

Risk points: Email; web services; remote devices (600 laptops) connecting to unsecured sources; unauthorised software introduced by users

Compelling event: Incumbent system price hike

Key requirements: Robust AV solution; lightweight footprint with no degradation of systems performance; automatic updates; simple centralised administration; proactive zero-hour protection against blended threats (reduced reliance on signature updates); easy enterprise de-installation capability

Solution

ESET NOD32 user since 2005

Location

Auckland, New Zealand

Website

www.aut.ac.nz

Float like a butterfly, sting like a bee

The trouble with the so-called heavyweights of antivirus software is that they're quite literally too big for their boots. Their super-sized footprints place such an overhead on IT systems that users frequently experience degraded performance. But more enlightened IT managers are picking up on a rising star that is out-pointing the big boys with a lightweight footprint and the punch of a super heavyweight contender.

▶ With size comes risk

As New Zealand's fourth largest university, AUT administers 25,000 students and is spread over three Auckland campuses. AUT's technical services team manages a heterogenous IT environment, including desktop and user support, training, web services, email, file storage, print, applications deployment and management. With 5,000 desktops and 600 plus laptops, there is plenty of scope for the introduction of IT security threats. The challenge for AUT was robust protection that didn't break the bank or impede systems performance.

▶ The downside of super-size

AUT's previous AV system was working well enough. However, the institution faced a license price hike if it were to renew its contract. So it took the opportunity to evaluate other enterprise grade offerings. While it's hard to look past the established market leaders, experience had taught Technology Services manager Russell Barron to be wary of an automatic selection. "The Nortons and McAfees of this world seem to have various issues either to do with price per unit, deployment, or the normal overhead these sorts of products create on network resources. We've always tried to focus on an AV product that does its job very well, instead of being bundled as part of a larger suite that does a whole lot of things that we are not necessarily interested in. We wanted a very focused solution."



[Continued...]

“One of the features that attracted us to ESET NOD32 was the very small and quick updates. NOD32 is very good, particularly for remote users, in a low bandwidth environment.”

– Russell Barron,
Technology Services Manager
AUT

▶ The power of an experienced community

The tipping point came when Barron considered the accumulated recommendations he gathered from his IT staff, many of whom were using ESET NOD32 on their home computers. “With the upcoming renewal, a number of my staff approached me and explained that they’d been using NOD32 at home, and from what they had seen it looked like a good product. It had good features, good feedback from the user community, and good reports on its effectiveness. It seemed to fit well inside a large organisation.”

▶ Small but perfectly formed

NOD32 combines an exceptionally small footprint with superior scan speed and proven detection capability. At its heart is “zero-hour” ‘heuristic’ technology, called ThreatSense. The technology has a documented track record of pre-detecting a very high percentage of new threats during the critical time period between the emergence of a new threat and the release of a traditional virus signature update.

A key success factor for AUT was NOD32’s suitability for low bandwidth environments, due largely to a remarkably small installation size of just 8MB and file updates of 50k. With a significant number of remote users, many of whom were using dialup internet connections to access AUT’s systems, it was important that antivirus updates were manageable in a small bandwidth environment. Super-sized file updates would have proved a significant sticking point, says Barron. “The issue with large file sizes is that high bandwidth overhead encourages users to start avoiding updates. They tend to say, ‘No, I won’t’ and before you know it they are way out of date. One of the features that attracted us to NOD32 was the very small updates.”

Deployment was another consideration. Barron’s view was that high systems overhead was a reliable indicator of problematic deployment, to which product suites added further complication. “Not all AV systems are simple to deploy. High overhead systems sometimes cause other applications on the PC to stop working,” says Barron. “Another sticking point is the component parts of a suite, which sometimes don’t work well individually.”

“ Anything that encourages the user community to keep their machines updated is a huge boon for IT. ”

– Russell Barron,
Technology Services Manager
AUT

NOD32 scores top marks

Using application deployment tool Novell ZENworks, it took AUT just four days to complete the first wave of installations to 3,500 workstations. Currently, 4,250 AUT desktops are protected by NOD32. But without a centralised approach to deployment and ongoing management the price of protection can come at a huge cost for large organisations like AUT. IT can't afford to engage in user education that requires some sort of individual user activity to complete systems installation. So deployment had to be completely invisible to end users. What's more, organisations need also to consider de-installation, says Barron. "If it can't be done in an enterprise fashion and requires manual de-installation from individual PCs you have a major potential problem."

With ESET NOD32 Barron gets 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 setup on all clients, and administers NOD32 updates. A console provides AUT IT Services centralised visibility of enterprise-wide client updates and viruses detected.

The nature of AV protection means that putting a figure on return on investment is extremely difficult, because you can't calculate savings on security breaches that haven't occurred. But it goes without saying that any threat that successfully disrupts the systems supporting the delivery of information and teaching to 25,000 students would be very costly. However, Barron sees tremendous advantages, and indirect savings, for the institution's IT in NOD32's inherent strengths in keeping a large and disparate community protected. "Anything that encourages the user community to keep their machines updated is a huge boon for IT," says Barron. "Administration workload is certainly less. We used to have issues around the scripting required for transparent and seamless deployment of program upgrades. Some required a de-installation first. But NOD32's updates and upgrades are simpler, with a smaller workload."

