



Company

Babbage Consultants Limited

Sector

Professional services – architects and consulting engineers

IS manager

Alan Courtenay

IS topography

80 Workstations; Windows Server 2000 & 2003; practice management system OfficeCentral

Security issues and needs

Incumbent system had several shortcomings: generated false alarms; viruses not identified or cleaned; difficult to administer

Key requirements: proactive zero-hour protection against blended threats (reduced reliance on signature updates); lightweight footprint with no degradation of systems performance; automatic updates; simple centralized administration; ongoing technology development

Solution

ESET NOD32 user since 2005

Location

Auckland, New Zealand Project offices New Zealand-wide

Website

www.babbage.co.nz

Strangling threats has never been easier

There are enough headaches with managing IT without having to worry about whether or not your antivirus (AV) system is up to doing the job. When Babbage Consultants' previous AV vendor recommended ESET NOD32 to clean up after its own shortcomings, Babbage IS manager Alan Courtenay couldn't go back.

Time is money

Babbage Consultants is a leading design practice, with a diverse client base in many sectors across New Zealand, Australia, South East Asia and the Pacific Islands. As a professional services business, lost consulting time is unrecoverable.

With IT now inextricably linked to staff productivity, the last thing the business needs is interrupted access to systems, particularly email and internet connectivity, says Babbage IS manager Alan Courtenay. "This is the first area we need to protect. It only takes a small thing to make everybody stop, and we can't recover lost time."

Management headaches

Babbage's AV system did some things well, but came up short in other areas. Though proficient at scanning, it required a lot of extra management and became increasingly difficult to administer as complex internet and email threats evolved.

The main drawbacks included false alarms and inadequate cleansing, which were disconcerting, says Courtenay. "There were a lot of false alarms that you had to work out for yourself. If a virus was detected the system didn't tell you what it was, because it didn't care, nor was it adequately cleaned. For example, some remnants of viruses were left in scanned documents, which were picked up by the systems deployed by our clients. It wasn't good."

[Continued...]



In an interesting twist of fate and the eventual downfall of Babbage's previous AV supplier, Courtenay was referred by the AV distributor to ESET NOD32, which they had identified as offering good cleaning technology. The unlikely introduction saw Babbage trial a version of NOD32. The company has never looked back.

"It was their big mistake," says Courtenay. "It was the first time I had heard of NOD32. But once you see what it can do you can't go back."

Getting the NOD

ESET NOD32 has impressed Courtenay at a number of levels, no more so than the hoary chestnut of systems performance. Because antivirus software constantly runs in memory, a large footprint will hamper systems performance. However, the last thing users need is degraded performance for the sake of adequate protection. With a typical installation size of just 8MB and file updates a meagre 50k, NOD32 combines an exceptionally small footprint with superior scan speed and proven detection capability. This was important for Babbage, as its design applications already commanded significant computer processing power and network resources.

During evaluation, Courtenay felt some pressure to partner 'better known' AV systems vendors, including Symantec, but was spooked by systems performance issues. "I looked at them. I'd used them in the past, but the thing that worried me was the way they could knock a system around – like stop it dead in a lot of cases, particularly with email. I found that it slowed performance quite dramatically. A lot of people pushed us this way, but Symantec was just too heavy on the system. Once we trialled NOD32 we saw that it did so many things so smartly. And it was so obvious when we started using it."

Courtenay considered "zero-hour" protection capability as another key success factor. And this is where NOD32 leads the field, with world-leading '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. "It accurately identifies likely threats, which may not yet exist in signature files," says Courtenay. "You might scan drives to see if infected files exist,

[Continued...]

**Once you see what ESET
NOD32 can do you can't go
back.**

**– Alan Courtenay, Babbage IS
Manager**



but NOD32's ThreatSense scanning stops things from infecting your system in the first place." Detected likely threats are automatically sent to ESET for analysis, with new virus signatures incorporated into subsequent updates.

Doing the business

When AV software and threat protection systems are doing their jobs, the IT manager shouldn't necessarily know about it, because issues are dealt with in the background. So the IT manager isn't distracted by impacts, simply because security breaches don't happen. And this is the big difference ESET NOD32 is making to Babbage IT. "Compared to what we had before, managing IT threats used to cost me quite a bit of time. Now there's no cost because everything is automated and works very well," says Courtenay.

However, more than simply averting the impacts of potential threats, with ESET NOD32 Courtenay gets clever tools to administer tasks that in the past were not so simple. A central mirror server automates aspects of administration: installation automatically replicates a pre-configured setup on all clients, and administers NOD32 updates. And a console enables Courtenay to see what's going on, for things like client updates and viruses detected. "In the past, if a virus was detected, I'd have to be involved, ask the right questions, get a cleaner, apply security patches, update machines, and check others. With NOD32 you don't have to do that. You can self-select how threats are dealt with so that you don't even have to know about them, if that's what you've specified. The system gives me a lot of control."

Courtenay is also impressed with ESET's introduction of broader threat protection, such as spyware blocking. "What it says is that these guys keep on developing. The amount of work going on is evident in how NOD32 is kept up-to-date. It's not the case with other vendors. There are lots of smart people out there inventing new ways to penetrate systems. NOD32 seems to be keeping up with that."

These guys keep on developing. The amount of work going on is evident in how NOD32 is kept up-to-date. It's not the case with other vendors. There are lots of smart people out there inventing new ways to penetrate systems. NOD32 seems to be keeping up with that.

– Alan Courtenay, Babbage IS Manager

