

Working smarter – not harder

keylogix

Key risk points

Heavy users of email and web

High risk [long-established online presence]

24/7 global business operations

Regular infections due to delays in "signature" updates

NOD32 Solution

Accurate proactive virus detection reduces risk during early hours of a new virus

Lightweight footprint

Minimal PC and network load

“NOD32 has extremely fast scanning ability, is lightweight in terms of system overhead and is heavyweight in terms of protection.”

– Antony Ranger
Keylogix Systems
Software Architect [NZ]

Keylogix provides Microsoft Office users with a suite of innovative desktop productivity tools to help increase the speed, efficiency and accuracy of document creation. Their catch-phrase is "Working smarter - not harder".

▶ The challenge

From its base in New Zealand, Keylogix sells and supports its software and services globally through its website www.keylogix.com.

As an established global business with a long 'online' history, Keylogix is very exposed to internet-borne threats every day. The company has a large population of PCs and servers (many of which are in 'unattended' test and deployment environments) including many laptops that are regularly taken off-site.

Previously Keylogix had armed itself as best it could with two virus-checkers. "However we were finding the existing software ineffectual at managing the new threats being encountered on a daily basis," says Keylogix Systems Software Architect, Antony Ranger.

The company decided it needed to review its security software, looking for a leading-edge solution, with proactive technology to stop new, fast-spreading virus and Trojan threats. After a comprehensive search and evaluation Keylogix chose NOD32 Antivirus.

▶ The solution

Keylogix Systems Software Architect, Antony Ranger says that "NOD32 has extremely fast scanning ability, is lightweight in terms of system overhead and is heavyweight in terms of protection." NOD32 has world leading 'heuristic' technology with a verifiable 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.

"Since implementing NOD32 we have seen a number of Trojans caught that would have previously wreaked havoc on our IT systems decreasing productivity and sometimes forcing rebuilds of workstations," adds Ranger. "Alongside our Windows XP SP2 deployment both implementations have certainly hardened the security both in the workplace and for roaming laptops."