



SecureWave SecureEXE/SecureNT 2.7

by David Cartwright, Techworld, March 11, 2004

Removable drives – and USB flash drives in particular – are an obvious security risk, as are unauthorised executables. We review sibling products that let you control access to both.

Pros: Simple to administer; protects against user-originated security issues that traditional firewalls can't cope with; scans don't unduly slow down the target computers.

Cons: File scans can take ages, although this is largely down to how much junk you have on your client PCs.

Buying advice: When purchasing security products, you'll generally find that adopting a small number of complementary products will provide the best protection. So by combining the products reviewed here with a traditional firewall, and perhaps a separate anti-virus system, you're maximising your chances of keeping unwanted material out of your network.

SecureEXE and SecureNT are sibling products that allow the system manager to protect the corporate network against unwanted intrusion. Although most of us have some kind of firewall device at the edge of the network, these two products provide protection at the computer level, instead; SecureEXE prevents unauthorised executable programs from running and SecureNT prevents users from attaching unauthorised devices.

Although separate products you'd probably buy both together and in fact they're managed from a single console application, which is a nice touch. Each product has a separate client component that you install on all your workstations. You put the administration application on the machine from which you want to manage the world. The server end of the system needs a "proper" database in which to store its data but if your organisation isn't large enough to need a full-blown SQL Server installation (or you don't want to spend the money on one) it's happy to use the no-cost alternative, MSDE.

SecureEXE works by allowing workstations to run only the executables that have been "authorised" by the administrator. This authorisation is based on the user ID you're logged in under and the administrator sets up the various execution roles by defining "groups" of related executables (you'd have one group for each application) and then defining whether each person could, or couldn't, run that set of programs. To set up the program groups you first run a scan on each client computer from the admin console (so it can identify the executables whose access is to be controlled) and then make your various program groups from the results.

Coarse control

SecureNT's purpose is to restrict the use of removable media to only those items the administrator deems appropriate. This includes obvious things like CDs and floppies but extends to cover any type of removable media – USB-connected disks, for instance, or PDAs connected via a serial port. Some devices, such as the floppy drive, are controlled at a very coarse-grained level (you can either deny access completely, permit it completely, or permit it read-only if in addition to wanting to keep dodgy programs out, you're also worried about your company's private data going walkabout).

Where a device allows media to be uniquely identifiable, though, you can choose to permit only specific removable media items to be inserted (since it's possible to uniquely identify a CD, for instance, you could permit someone to use, say, their AutoRoute CD but no others).

The management application follows the normal approach of having the various "main menu" options in a pane down the left-hand side, a much larger "item detail" pane on the right, and a status-cum-audit-log pane at the bottom. You switch between SecureNT and SecureEXE features simply by clicking a little tab on the left-hand side of the screen and when it comes to configuring options the dialogs are generally simple and clear.

The flow of the screens is good. The admin application allows you to come at data and permissions from any angle – you can sort item details by whatever column you wish, for instance, and when applying permissions to (say) individual CDs you can come at it from a user view (select a user and specify what CDs they're allowed to use) or a media view (select a CD and specify who can use it).

SecureEXE and SecureNT take a refreshing approach to system protection and make a useful addition to traditional network security software.

Reprinted from Techworld – <http://www.techworld.com>