

SecureEXE and SecureNT

One of the biggest tasks that can face the network security administrator is the ability to control the activities of all individuals within the organisation who have access to their network. Couple that with the need to stop certain activities that generate from outside sources and the administrator's task really can become a big problem. With so many potential threats and vulnerabilities, you really do have to champion the cause and find a secure and easily managed solution.

However, potential vulnerabilities also arise from I/O devices, where no control is enforced on casual and unauthorised usage. What you need are applications that you can trust, which will take the hard work out of the equation and the guesswork out of who's doing what on your network. By initialising a method of control over your users, which stipulates who is authorised to access what, you will be able to limit the use of applications and devices which you may not want running, and which could open up holes or affect other system settings.

In this review we have taken two solutions from the same developer and looked at the potential control that they provide over users utilising everyday applications and devices. One of these solutions has passed our way before. *SecureEXE* provides you with the control over who runs what of the applications that are already available on your network. It achieves this by allowing you to authorise only the applications you want your users to execute on your network. By recording in a database only those applications that you want to allow, you can control who has access to what. By utilising this list, which may be defined by user or group permissions, every time users try to execute an application, you ensure that they can only open and use the application if they are authorised to do so.

SecureEXE achieves this because a local agent checks the user's request against the database, comparing user credentials with their permissions. However, as added protection, each executable binary file is given a SHA-1 hash signature by *SecureEXE*, which ensures if anything enters your network and is not recognised it simply will not open. *SecureEXE* does not use filenames to recognise authorised applications, as these can be easily manipulated. Using the unique file signature makes this a far more secure method of protection than some other methods of recognition such as file length and size attributes. In this way *SecureEXE* can eliminate the threats posed by such things as Trojan horses and viruses that may enter your network. However, this solution also stops activities during working hours that also threaten your network security, such as downloads, games, and other unlicensed software, to protect your network and system settings further. And you don't need updates for known viruses, because using *SecureEXE* ensures that unless already authorised, applications cannot be run; there-



by Jayne Parkhouse

Version: 2.5.2b
Supplier: SecureWave
Price: £6,750 (either product; up to 250 users/clients); £9,000 (purchased together)
Contact: +352 265 364 11
 sales@securewave.com
 www.securewave.com

FOR *SecureEXE* provides critical application security and stops unauthorised executables from being run on your systems, while allowing users the right permissions to access the applications they will need to complete their work. *SecureNT* delivers protection to intellectual property and critical business data by disabling I/O devices on users' machines unless they are specifically granted access.

AGAINST Just one tiny flaw. Having had the software delivered, installation was delayed for 1 hour and 39 minutes because of having to receive a test licence file; patience was never my strong point.

VERDICT Both products add an extra layer to network security and deliver some much needed control to both application and I/O devices that may become a vehicle for unauthorised use.

[Ed Note: the following marks reflect both *SecureEXE* and *SecureNT* as individual solutions.]

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★☆
Value for money	★★★★☆
Overall Rating	★★★★★

fore known or unknown it makes no difference, if it's not on the authorised list it's got no chance!

Installation was straightforward and was remarkably quick and easy to accomplish; with links provided for missing system requirements such as MDAC 2.6 SP1, complying with installation prerequisites was eased. Once up and running, populating your authorised application list is again easy with the concise and useful documentation supplied with the solution. Setting user permissions is similarly accomplished with ease and enables the control needed to ensure only the users you want to access certain applications can, and that applications outside your authorised list are never executed on your system.

Network protection needs to be complete, and although you can stop unauthorised applications and undesirable executables from being run with the assistance of *SecureEXE*, you are still vulnerable. How do you stop data being removed once legitimately opened? Sensitive data may be a target for certain individuals and the ease with which an employee can copy and remove critical information should send alarm bells ringing for any security-minded administrator and his or her employers. As we've already intimated earlier in this review, the second and equally helpful network control application is for I/O devices, and control is easily achieved with the aid of *SecureNT*.

SecureNT enables all means of removing data to be controlled, ensuring CD writers, floppy drives, other writeable media and any plug-and-play device that can assist in extracting information, can be disabled on every machine on the network with ease. No more PDAs connected to PCs without authorisation, and USB devices able to store data are no longer of any use. *SecureNT* even protects against plug and play devices that neither Windows 2000 or XP can manage within its group policies.

Again, as with *SecureEXE*, installation of *SecureNT* was a simple affair and it was easy to set up and use. Setting your chosen devices for authorised use is easy with the aid of the access control list (ACL). This is all achieved centrally and demands that I/O devices are assigned to the list and that the appropriate users are provided with authorisation for only those devices which you want them specifically to have access to. This ensures that only trusted users have access to certain devices, with access permissions being either scheduled or fixed; this greatly reduces the risk of losing confidential information, business-critical data and intellectual property.

The administrator is also afforded extra control across the network, stopping the introduction of unlicensed software and inappropriate games and devices, and for those who do have access rights, usage is still monitored to deter misuse and promote a more secure environment. Reports and logging are also available to the administrator, bringing tighter control to the business and ensuring usage is both appropriate and authorised.

With these two solutions available to secure your network, productivity should also be encouraged among your employees. With all the distractions otherwise available to them and the temptations of illicit software use removed, time will be spent more productively. Malicious code and hacking software will be unable to penetrate your defences; arriving maybe, but without the capacity to execute and run, they are rendered harmless to your systems. With all this extra control, reports and monitoring available, network security becomes easier to control and execute. Changes to authorised lists can be made on both solutions with ease, on the fly, freeing up the security administrator's time to solve other problems and enabling them to keep their network maintenance up to date and all systems on go.