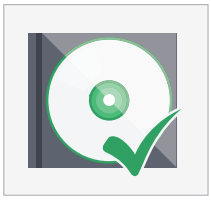
Increase security with NetSupport DNA

NetSupport DNA is an IT Asset Management suite – with a twist. As well as the standard inventory, software licensing and software distribution features you would expect, in addition to innovative print and energy monitoring features, NetSupport DNA also includes a range of tools designed to work as part of an organisation's broader desktop and network security planning.

So how does NetSupport DNA help increase desktop security? Here are eight ways:

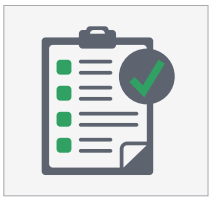
Endpoint security

NetSupport DNA includes a flexible endpoint security feature that allows the use of memory sticks to be controlled, with access for each memory stick restricted to a specific user or department. Use of any memory stick can also be tracked and reported, and DNA endpoint security can help prevent both data loss and infection from portable media.



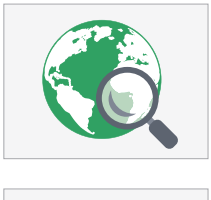
USB/DVD control

NetSupport DNA also offers controls for user access to USB storage devices and CD/DVD drives, either preventing use altogether, limiting them to read-only or allowing use but preventing execution of any files directly from them. The feature ensures a company can control and, in conjunction with the Internet and App modules, prevent new software being installed or run on any PC.



Application whitelisting

NetSupport DNA also provides the ability to monitor and report on all application use and, within that, create whitelists of approved applications that can be assigned to users and departments. Application use can then be limited to only approved company applications – and unknown applications can be prevented from being used and causing any subsequent security issues.

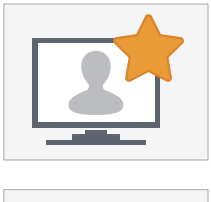


Internet security

Much like application control, NetSupport DNA includes the use of approved and restricted URL lists, as well as monitoring and recording all internet activity. Access on company PCs can be limited to only specific and approved websites, thereby preventing access to insecure sites that may risk malware or virus transmission.

Proactive scanning and alerts

NetSupport DNA features a powerful alerting suite with many alerts designed to help maintain security. Alerts can be triggered instantly: for example, if a key service such as anti-virus is stopped, or a new application is installed, or the size of a known file changes – and much more. Alerts are designed to operate in combination to highlight potential security risks and prevent systems from becoming compromised.

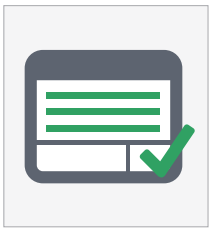


Automatic discovery

NetSupport DNA will monitor the enterprise and automatically identify any new devices that are added, ensuring any new PCs never go undetected. Once identified, NetSupport DNA can be remotely deployed onto those devices to ensure security policies and usage controls are enforced.

SNMP monitoring

The SNMP module in NetSupport DNA allows key data from network devices such as network switches and firewalls to be discovered and then monitored. Alerts can be trigged for dozens of scenarios, such as alerting if the inbound traffic on the company firewall exceeds a certain percentage for a pre-defined period of time, which might suggest a Denial of Service attack.



Acceptable Use Policies

Acceptable Use Policies form an integral part of the key information security policies used by most organisations. It is common practice for new staff to sign an AUP before using company resources for the first time, or to confirm they have read any changes to such a policy whenever it is updated. NetSupport DNA supports the delivery and tracking of AUPs across the enterprise and prevents access to the desktop until users have accepted and agreed to abide by the organisation's policies.

To find out more visit: www.netsupportdna.com