Feature Sheet

NetSupport DNA

Supporting Security

We work with thousands of schools across the world, gaining their feedback to ensure our solutions are relevant, effective, and support security. From keeping the network secure to helping ensure data is safeguarded, NetSupport DNA adds an extra layer of protection.

Explore and discover

NetSupport DNA's Explorer mode provides a real-time overview of all PCs on the network, highlighting which PCs have active notifications and allowing operators to identify and resolve issues quickly. Meanwhile, the Discovery mode will automatically identify any new devices that are added and remotely deploy Agents to those devices, ensuring any new PCs never go undetected.

Monitor more than just devices

The SNMP module allows key data from network devices (e.g., 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 school firewall exceeds a certain percentage for a pre-defined period – which might suggest a Denial of Service attack.

Control the use of removable devices

Provided as standard, NetSupport DNA's endpoint security component can control the use of removable USB devices on all PCs across the school to prevent sensitive data loss or virus infection from portable media. Individual memory sticks can be assigned to dedicated users, or their use restricted to specific individuals or team members for the current day, a week, or indefinitely – making certain that data is locked down should memory sticks happen to get lost. Schools can also control the use of CD and DVD drives, e.g. blocking altogether, limiting them to read-only access, or preventing any direct execution of files.

Store your data securely

NetSupport DNA's dedicated data protection tools help schools to identify whether the software they have installed is compliant, where any sensitive information is stored, prevent data breaches and support individuals' rights by easily identifying and instantly archiving or removing all data history related to the person in question.

Internet and application usage

Students and staff on school PCs can be restricted to using only specific and approved websites or applications, thereby preventing access to insecure or inappropriate sites/applications that may risk malware or virus transmission. These controls can also prevent new software being installed or run on any PC or sensitive data being accessed or removed.

Getting consent from everyone

NetSupport DNA supports the delivery and tracking of Acceptable Use Policies across the school and prevents access to school devices until users have accepted and agreed to abide by its policies.

Seeing the relevant data for your school

User views can be set to ensure that, in Districts with multiple sites, data from one school is not visible to another. At a higher management level, the data across all the separate sites can be seen and analyzed as a consolidated report.

Be alerted to changes

NetSupport DNA also contains 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, a new application is installed, or the size of a known file changes – and much more.

Secure data - even on the go

NetSupport DNA's online safety cloud view (V4.7 and above) is a fully secure, Azure-hosted console that stores local data generated at a school, e.g. triggered eSafety keywords, screen capture, risk index alerts, reported concerns by a child or teacher, and the trending topics word cloud. The data remains fully secure, since only designated School Counselors can view it. In addition, all the monitoring and assessment of these alerts is done locally by the school; no third-party services are needed.

Screen recording

There is a rolling 60-seconds capture of screen activity held in the system memory on each student's PC in an encrypted format. Only if a critical eSafety keyword is triggered, will the screen capture be converted into a viewable file - otherwise, it's automatically deleted every 60 seconds.

Webcam use: your choice

Schools can turn on NetSupport DNA's webcam capture feature (on school network devices) to capture an image of the user in school who has triggered a critical eSafety keyword (e.g. suicide), if they wish.