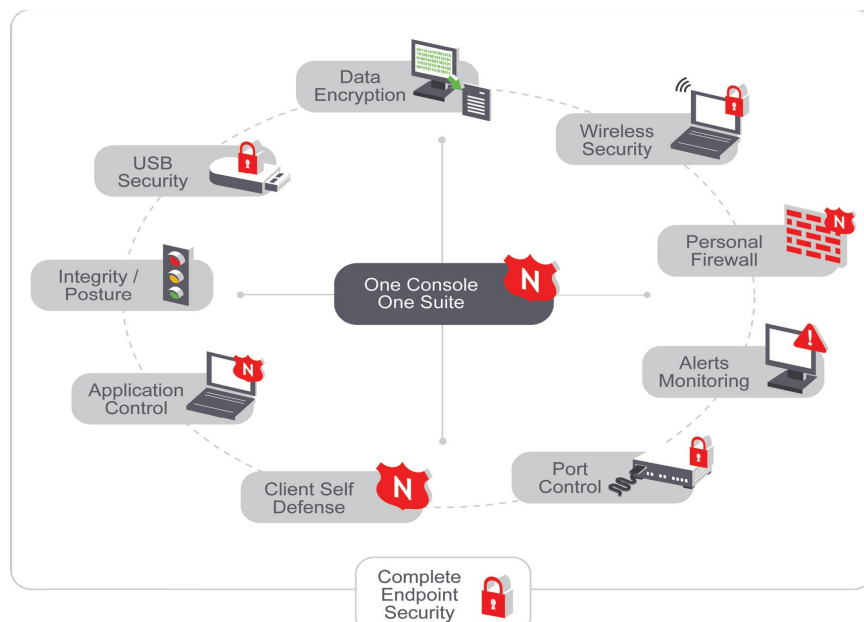


ZENworks Endpoint Security Management for the NHS

Novell **ZENworks Configuration Management (ZCM) Standard** is available free of charge to NHS Trusts under the Connecting for Health (CfH) Enterprise Wide Agreement with Novell. As part of this agreement CfH have purchased perpetual licenses for all NHS Trusts as well as upgrade protection, meaning that NHS Trusts are entitled to upgrade to future releases of ZCM Standard.

As an enhancement to the features that ZENworks Configuration Management Standard Delivers, NHS Trusts can purchase ZENworks Endpoint Security at a massive NHS discount of 74%. Endpoint Security will enable NHS Trusts to control the security of their infrastructure in ways that were not possible in the past with one centrally manageable product that integrates seamlessly with ZCM



Key Features & Benefits

Personal Firewall

Protect Trust users with transparent solutions. The world's strongest, yet easiest to use, firewall to protect against hackers, malware, protocol attacks, and more, keeping security invisible to the end-user and requiring no interaction on their part.

Wireless Security

Keep users from using bogus wireless. Centrally control when, how, and where users are allowed to connect. Doesn't just detect intrusions, it totally prevents them 24x7 in all locations. Wi-Fi connectivity can be limited to authorised and known access points, specified encryption strength, and can be disabled completely if necessary based on location. Easily control keys, MESH and WiMAX environments, enforces VPN usage if required by policy, and much more.

Encryption Solution

Stolen laptops don't have to spell disaster. Secures patient data stored on your trusts PCs, Laptops and on removable media, encrypting files so

they can only be read by authorised users. Protects sensitive information on lost or stolen mobile computers. Keys are managed transparently throughout the Trust, requiring no end-user involvement other than getting their work done in the usual way.

USB Security

Don't let your patient data walk out the door on a USB drive. Prevents intentional or inadvertent transmission of data to removable storage devices. Storage devices including USB drives, iPods, cameras, printers, CD and DVD drives can be placed in read-only mode or fully disabled, while the endpoint hard drive and all network drives remain accessible and operational. White lists of specifically approved USB drives can be employed, and in combination with data encryption ... you just couldn't be more secure from both internal and external data loss; both deliberate or inadvertent.

Application Control

Keep everyone compliant with the Trust application policies. Ensures only approved applications are run on the Trusts IT assets -- create white/black lists, or enforce applications to run (i.e., VPN) prior to network connection.

Posture and Integrity

Ensures 24x7, connected or not, that your employees are actually using their AV, Anti-spyware, or other applications running according to your Trusts policies. Insure that OS security patches, AV data files and other critical posture elements are in place and up to date. Enables you to warn, shut down and point to remediation services, or execute a custom script based on whatever triggers you choose.

Client Self Defence

Secure your security client. Protects the endpoint by ensuring that the security client cannot be altered, hacked, or uninstalled. Even with administrative rights on a machine, the user cannot disable the policy enforcement.

Device Control

Prevent rogue access. Managed at the lowest level for optimal security and performance, safely controlling connectivity via LAN, modem, Bluetooth™, Infrared, 1394 (Firewire™), and serial and parallel ports.

Alerts / Monitoring / Reporting

Keep a careful eye on everything. Provides a scalable and simple method for creating, distributing, enforcing, and monitoring security policies on endpoint devices, without forcing users to make security decisions or adjust settings. Novell offers robust and tunable reporting to assist in regulatory compliance reporting.

Common Criteria EAL 4+ Certified

The Common Criteria (CC), is an internationally recognized ISO standard (ISO/IEC 15408) used by the United States Federal government and other government organisations to assess security and assurance of technology products. Level 4+ is only achieved by a handful of companies.

For further information, or to request a demonstration of Novell Endpoint Security please contact you Novell NHS Account Manager.

For more information please contact

North:

Mark Shaw-mashaw@novell.com

South

David Penny-dpenny@novell.com

General Enquiries

Email: nhs@novell.com

Training

QA-IQ NHS Training Schedule is available at:
<http://www.qa-iq.com/learning/nhs/novell/>

ZCM is free to download from the NHS Software Portal, please contact your Novell Account Manager for access details.