impero
education pro

patch management feature*

Keeping software updated is vital for the security of a network, particularly when education establishments are required to cater for a plethora of users. Impero Education Pro's intelligent patch management feature provides the ultimate protection for third party cross-platform software, preventing the risk of security breaches and potential downtime. Scheduled automatic patching of all outdated or vulnerable software products is simple, secure and time-saving, essential for durable endpoint security.

*Patch management is an optional add-on feature available in Impero Education Pro.

the benefits

⚠ minimise risk

Impero Education Pro's patch management feature prevents network security threats generated by users. The Wake-on-LAN service can be set to power-on computers, apply patches, and then power-off the computers, providing essential protection for the network and minimising exposure to vulnerabilities.

⚠ reduce downtime

Maximising endpoint security reduces the potential of downtime since network machines will be kept protected and up-to-date.

🔒 secure network

Detailed reports offer an instant view of patching across a network for simple analysis and tracking. Ensure maximum security via configuration of patch management, achieved by creating customised profiles for automated patching. If required, run manual scans at the click of a button.

🕐 ensure accuracy and save time

Automated patching eliminates the risk of overlooking update notifications or accidentally patching incorrect versions. The ability to automatically scan a network for outdated or vulnerable software removes the hassle of manual processes and reduces admin workload though automated policies.

the features

features

> create profiles for automated patching

> add PCs to specific profiles

> select software products for authorised patching

> active directory and manual group creation

> compatible with Microsoft and non-Microsoft applications

> wake-on-LAN scheduled patching

> schedule by time and date

> shutdown on patch completion

> install results over 24 hour period

> generate reports by date/time/machine/details/log type

> export reports to CSV file

> report on events throughout the patching process

> report on errors throughout the patching process

> report on deployment throughout the patching process

benefits for network managers

> saves time through automated patching and easy-to-create policies

> removes the risk of overlooking update notifications or accidentally patching the wrong version (when manually patching)

> provides a centralised overview of the network's current patching state

> keeps systems updated

> prevents vulnerabilities and security threats

> reveals most popular missing patches grouped by severity

> reduces the chance of downtime by maximising endpoint security

> scheduled automated patching overnight or during non-peak times

benefits for teachers/ senior leadership teams

> ensures software is up-to-date so resources are functional for teaching, learning and working

> reduces disruptive downtime

> removes the risk of exposing vulnerabilities to the network

> ensures a safe online learning environment

benefits for the site

> ensures durable endpoint security

> reduces downtime to ensure that equipment is functioning correctly across the school for staff and students alike