

# Impero Patch

An optional add-on module available with Impero Education Pro, Impero Patch provides the ultimate protection for third party cross-platform software, including Microsoft applications. The ability to schedule automatic patching of outdated or vulnerable software products prevents the risk of security breaches and potential downtime, which proves essential for durable endpoint security.

## the features

### automated patching



Schedule patching for specific devices using a variety of criteria, including time and date, using active directory, or by manual group creation. Wake-on-LAN scheduled patching can be set to power on devices, apply patches and then shutdown machines once complete.



### intuitive dashboard interface

Provides a centralised overview of the network's current patching state, with access to key information such as the most popular missing patches grouped by severity.

### wake-on-LAN



Wake-on-LAN scheduled patching can be set to power on devices, apply patches and then shutdown machines once complete.



### easy-to-create policies

Create customised policies for automated patching to ensure systems are kept updated and protected, while saving time for IT teams.

### update scheduling



Configure installation schedules to determine which products will be patched by the system and when updates will be applied.



### detailed reporting

Generate reports prior, during and after the patching process and by date, time, machine, details or log type, to reveal events or errors and to prove endpoint security.

## the benefits

### minimise risk



Reduce exposure to vulnerabilities through the Wake-on-LAN service, which can be used to automatically power-on devices, apply patches, and shutdown once patching is complete.



### reduce downtime

Maximise endpoint security to reduce the potential of disruptive downtime by scheduling automated patching overnight or during non-peak times and by ensuring network devices are kept protected and up-to-date.

### save time



Automated scanning and scheduling of missing patches, and the ability to easily create policies, removes the hassle of manual processes and reduces admin workload.



### ensure accuracy

Automatically scan the network for outdated or vulnerable software to avoid the risk of overlooking update notifications or patching incorrect versions.

### improve efficiency



Scheduling automatic updates to keep systems updated improves working processes and helps to streamline networks.



### strengthen endpoint security

Keep systems updated, free from vulnerabilities and prevent the risk of viruses.