



TakeWare Gatekeeper

Now you're back in control!

The not-so-quiet revolution that has brought about the '*iPod Generation*' also brings with it a new and widespread threat – including **Mass Data Theft** via a data-highway that is faster than the Internet and has been completely unprotected. This comes via iPods, smart-phones, pendrives and a plethora of other removable devices, increasingly from people **inside as well as outside**. **The biggest threat to many organisations today**, large and small, yet has been almost entirely neglected - until now! The **DTI's Information Security Breaches Survey 2006** has clearly identified this emerging threat.

Schools and colleges as well as businesses and other organisations are all increasingly at risk not just from data theft, malware and other dangerous content but also from law suits for breach of **copyright** and the **data protection act** – with directors and governors increasingly held personally liable.

Gartner Research has said: "*Organisations are increasingly putting themselves at risk by allowing the unauthorized and uncontrolled use of portable storage devices*". "*These are ideal for anyone intending to steal sensitive and valuable data. Employees may also be responsible for losing data if they inadvertently mislay these devices. The impact of this goes beyond the commercial value of the data.*"

TakeWare® Gatekeeper **intelligently enforces policies** – standalone or across your network - allowing only authorised devices and authorised use. It **actively monitors and polices** both content and the use of all types of portable device, including USB, firewire hard-drives, flashdrives, cameras, iPods etc.

Fit and Forget: TakeWare® Gatekeeper is designed to quietly get on with the job of protecting your PCs and your network – without the need for constant attention from administrators to technicians.

Features

- Intelligent automated protection
- Excludes unauthorised devices completely
- Excludes dangerous and unwanted content
- Controls access to your documents and data
- Constant, comprehensive monitoring
- Protects laptops and PCs even when disconnected
- Full audit trail
- Integrated management of content and devices
- Protects your data
- Supports full range of devices
- Central control
- Flexible reporting

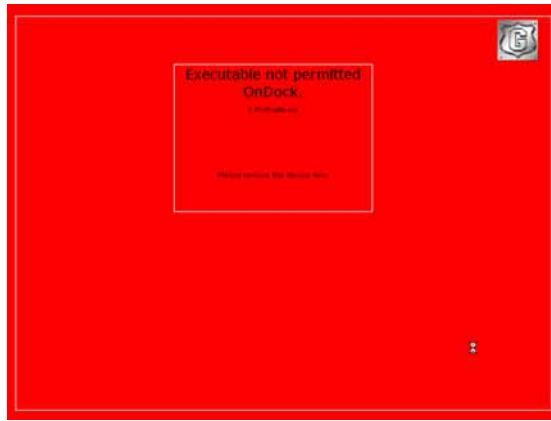
Benefits

- Fit & Forget – no need for constant attention (or dedicated technicians)
- Prevents Mass data and identity theft
- Control – better control of your information
- Security – protection from the internal treat.
- Traceability & Accountability – Full audit trail
- Productivity – better use of your technology
- Convenience – Allows controlled use of devices
- Flexibility – No need to block ports etc
- Compliance – Data protection, S&O, MiFID ...
- Fit & Forget – no need for constant attention.

TakeWare® Gatekeeper – Advanced Intelligent Protection



Unauthorised device rejected,



Authorised device rejected due to banned content

Management Console

Managers open the console by just clicking on the tray icon.



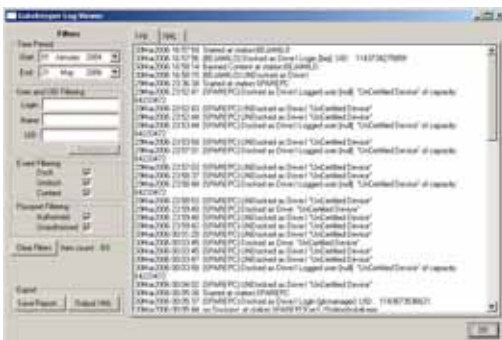
Site Settings

Site Password, Acceptable use policy and banned and executable files can be changed.



Enrol - Drive Authorisation

Authorise a device 'here and now' from the console or use 'Remote Enrol' to allow a user to enrol a new, empty, device when they login. Enrolment places a 'passport' onto the device and electronically seals it in place. The passport is electronically signed and cannot be changed by the user (any attempt to do so renders it invalid).



Flexible Reporting

Audit date can be viewed centrally with flexible reporting and export

TakeWare® Gatekeeper – Advanced Intelligent Protection