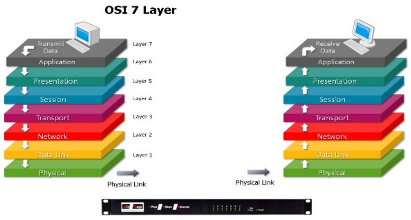
Air Gap
Network Security Solutions

Air gaps – what are they and why are they used?

Air gaps are physical breaks within a computer network. These physical breaks act at the wiring layer in a computer network, effectively between Ethernet cables, to the lay person.

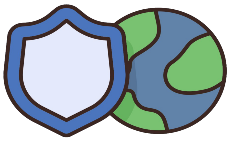


In a network which has no air gaps viruses and other malware such as worm and trojans are free to travel from device to device unimpeded. Air gaps are impenetrable breaks in the network which stop viruses and malware at the air gap.

Also air gaps disconnect devices from a network preventing the data on the device from being accessed by an unauthorised person such as a hacker.

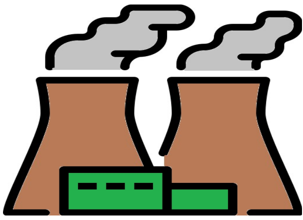
In summary – air gaps stop networks from being taken over by hackers and data being stolen.

Air gaps are a much more effective method of protecting a network than any known software method and is recommended by NCSC* for backup processes.



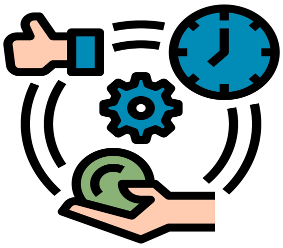
Air gaps present a hard break in a network which software by it's very nature can't. Software often has bugs in it which limits it's effectiveness and provide routes for hackers to access networks. Not only this but software can give a false sense of security as a result. This is the reason software is constantly updated to fix the issues within it.

New software features provide new opportunities for bugs to creep into software which then require constant updates to close loopholes. In addition software solutions are often convoluted and difficult to understand. A myriad of user options are given which are often interdependent with little documentation of the effect and no guarantee of operation. A wholly undesirable situation.



Air Gaps are ideal for protecting Critical National Infrastructure (CNI) and other high value assets.

Air gaps remove devices from a network when not required rendering them immune from hacking protecting the data on them from viruses and malware as well as data theft - all in one unit.



Air gaps are simple to use, simple to understand and simple to implement, meaning effective and understandable security that everyone can understand.

* NCSC – National Cyber Security Centre, a division of GCHQ