



Complete Firewall Protection

There has been a significant rise in cyber threats in recent years and new ways of compromising IT environments and stealing data are being developed daily. We're constantly researching and testing the leading defence methods and always recommend a multi-layered approach to provide multiple barriers of defence against these cyber threats.

Protecting your organisation and data from the threat of hackers, malware and viruses is a serious business. With so much critical data being held not only on your servers, in the cloud, on laptops, desktops and hand-held devices, your business needs an integrated security solution. We have implemented a wide range of security solutions for our clients and as such, have a wealth of expertise and experience of all the major security tools and technologies.

Complete Firewall Protection is a solution providing a business grade level of protection for your organisation giving you peace of mind that you have the highest levels of security in place. At the heart of this service is a Firewall device and software will be installed on all of your PCs, Laptops and Servers to monitor suspicious behaviour.

The firewall and security services will be monitored 24/7 365 by Sharp European Technology Support Centre (ETSC) as part of the Complete Firewall Protection service. Any suspicious behaviour will be flagged to the team, and remedial action will be taken, often before you even know about it. Updates will be carried out as and when there are new releases and you will be provided with regular reports.

SHARP
Be Original.

Key Features



Intrusion Prevention

Software that proactively monitors a network and takes preventative measures against suspicious activity.



Intrusion Detection

Software that monitors a network and alerts the user if suspicious activity is found.



Web Filtering

Software designed to restrict what websites a user can visit on their computer.



Content Filter

Software that restricts or controls the content that a user is capable to access.



Malware Filtering

Software that helps protect a user from malicious software.



Data Loss Prevention

Software that detects potential data breaches and prevents them by monitoring, detecting and blocking sensitive data while in use.



Reputation Enabled Defence

Reviews the destination of outbound connections and identifies its threat level based on intelligence feeds. Using the returned threat score, known threats are blocked and safe destinations are allowed.



Gateway AntiVirus

Allows applications to check files for viruses by providing a Simple Object Access Protocol (SOAP) based virus scanning web service.