FlashStart®
INTERNET **PROTECTION**

Integrates with
the FlashStart family

ClientShield
EndPoint Protection

New for
Home & Smart
Workers

FlashStart **ClientShield**

About

FlashStart ClientShield is an end-point protection application designed for Homeworkers. ClientShield is a downloadable application that enforces FlashStart's content filtering and malware filters on an end-point device connected on a public network (mobile or fixed) outside the perimeter of an office, school etc.
FlashStart ClientShield is part of the FlashStart Cloud family and is administered under the same FlashStart Cloud dashboard.

Compatibility

ClientShield is compatible with all major OS release with immediate release on Windows ™, Android ™, iOS ™, MacOS ™ and Chromebook ™. ClientShield enforces secure DNS tunnelling to the FlashStart Cloud and is compatible with NAT environments. It is also especially suitable for slow internet connections as no data traffic is tunnelled, only DNs is tunnelled.

Privacy

FlashStart ClientShield, and all the FlashStart family, conforms to the EU GDPR privacy directives and many other regulatory requirements associated with indecency laws and child-protection. On request FlashStart will support requirements to implement local Government-approved blacklists and other statutory needs.

About FlashStart **Technology**

The Cloud

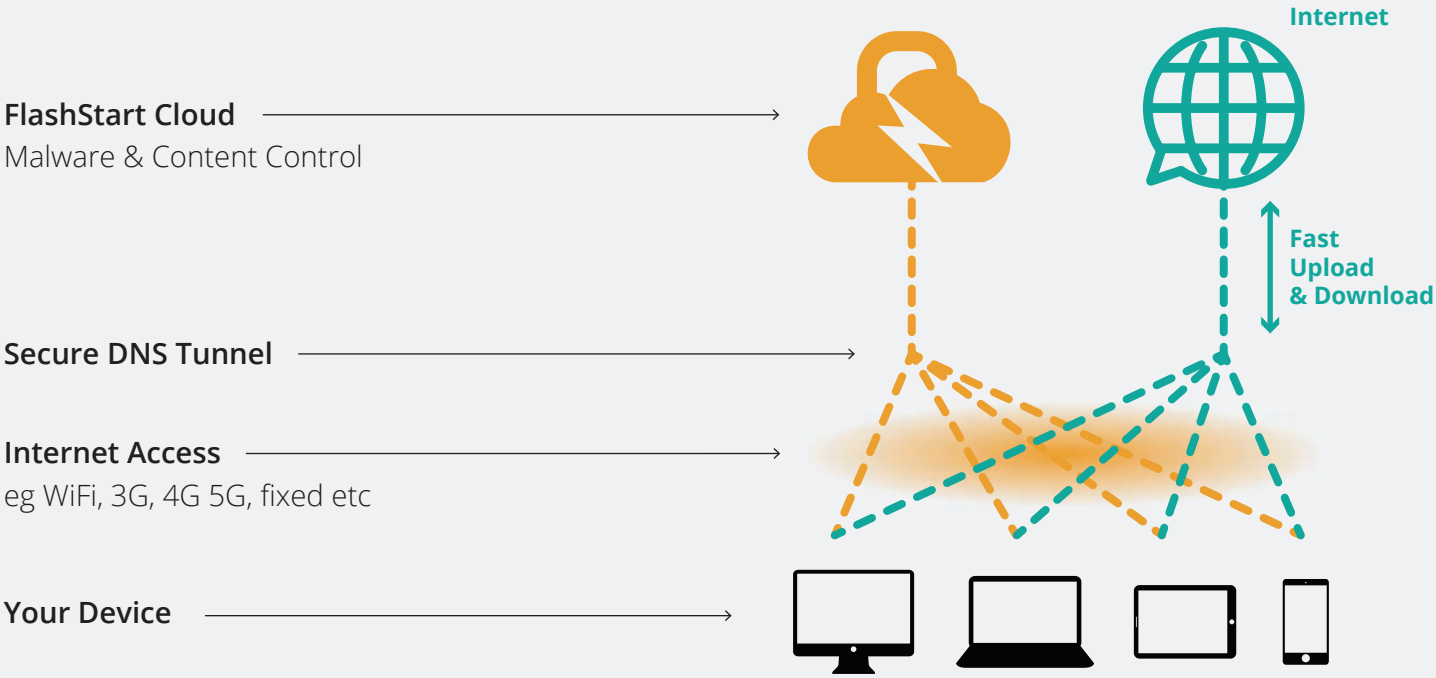
The FlashStart Cloud runs on geographically diverse server farms, providing high service availability and low latency.
Filtering is implemented using DNS technology which has an unperceivable impact on the internet performance of end users.

FlashStart only needs to inspect the very small DNS packets which precede the user-requested data transfer process.
There is no subsequent delay to data downloads.
FlashStart automatically identifies content categories and malware infected web sites being accessed by users and blocks access according to defined filtering rules. Rules can be created to monitor or block activity, and an activity log is kept for 6 months.
Filtering rules can be set by time of day and day of the week and can be varied for different user communities.

FlashStart malware detection capabilities automatically block attempts to access known malware sites, ransomware sites or sites in any country deemed to be associated with a specific threat.
Unintended blocking can be resolved efficiently to support a 'frustration-free' user experience

How does **FlashStart ClientShield** work?

A small FlashStart application is installed the remote device implementing a secure DNS tunnel that protect users from visiting Malware sites and also enforcing content control policies. ClientShield is resistant to be disabled or removed.



Key features of FlashStart ClientShield are provided in the table below.

Feature	Description
Device Compatability	Windows / Android / Chromebook / iOS / Mac OS
Locked Application	Downloaded application is tamper resistant
Network Compatibility	Optimised for low bandwidths as well as 3G, 4G, 5G, WiFi, fixed line etc
DNS Packet Latency	Typically < 35ms
Device Memory Required	< 1Mb
MDM Compatability	Widely compatible - please enquire
App Control	Yes. Control of App's via DNS Resolution
Private IP address	Support for private IP address installations (NAT & CGNAT)
Routers Pass-Through	No router configuration
Content Filter Control	85 content categories
Unified Management	Integrates with the same policies as all FlashStart Services
Whitelist & Blacklist	Yes
Safe Search	Yes. Google, BING, Duck Duck Go, YouTube
Threat Control	Ransomware, Virus, Trojans, Botnets & others
Geo blocking	Exclude high risk countries or build walled garden of safe countries to surf
Illegal Control	Illegal sexual activities, drugs, software piracy, copyright infringements (music, video etc)
Scheduling	Scheduling of access policy can be varied automatically by time of day, day of the week for each content cat.
GDPR Compliant	Service is fully GDPR compliant

Simple, fast and secure.

www.flashstart.com