Flash&Start®

INTERNET **PROTECTION**

Cyber security:
connections
from **Remote**

flashstart.com

Our **solution** for **work from home**

Info

FlashStart's DNS monitoring enables the same cloud-based protection settings adopted for the corporate network, even on remote devices that are connected anywhere.

Endpoint protection benefits the off-site worker and remote-connecting devices, but, more importantly, it benefits the company, as more and more hacker attacks originate from smart working.

Total protection

Full compatibility enables remote work protection by installing FlashStart's Client Shield application in remote devices. By following set policies that can be changed in seconds from the corporate office, 85 categories of system filtering allow blocks to be generated to dangerous sites but also inappropriate content.

Protection everywhere

It cannot be disabled by the worker on company-provided devices and is automatically activated anywhere, even by changing connectivity or WiFi.

Perché scegliere FlashStart?

Remote protection
Security for the worker and for companies increasingly exposed remotely. Protection from attacks aimed at damage, fraud, theft of sensitive, banking and technology data.

Work efficiency
Targeted control of inappropriate content during working hours, and online sources of distraction. Immediate changes from the office, at no additional cost.

Protection everywhere
Protection of the user wherever he/she connects: from home, hotel, bar, to a public WiFi... Automatic activation at every change of connectivity (4G, 5G, WiFi...).

Maximum compatibility
Full compatibility with laptops, smartphones, desktops and any connecting device. No accessories to match and undetectable battery consumption.

Extremely high speed
Using a secure and encrypted VPN tunnel to filter DNS requests, with no slowdown in browsing, very fast thanks to Global Anycast Network.

Privacy compliance
Detailed, privacy-compliant traffic reports by category and macro category, with the ability to schedule email delivery.

Functions / Technical features

Malware Protection
Navigation security from malware,
ransomware, botnet, phishing...

IP protection from blacklists
Upkeep of public IPs out of global blacklists.

DNS Intelligence on contents
Parental control and personalized web filtering
for households, schools, organizations
and companies.

Detailed analytics
Analytic reports in real time, by visited category
and macro category, and scheduled via email.

Blacklists based on A-I
Over 90 categories continuously
updated through Artificial Intelligence.

Maximum compatibility
Possibility to connect it to every Router,
WiFi HotSpot, Firewall and Gateway. Support for
static IP, dynamic IP (IPU4, IPU6) and DNS protocol.

Local Cache DNS
Optional DNS Proxy that can be added to the
ISP net to further reduce the resolution latency.

Research engine filtering
Block of explicit contents (violence,
porn...) that can be activated for searches
on Google, Bing, YouTube and DuckDuckGo.

Geoblocking
Block of navigation towards countries
at risk of hacker attacks and cyber threats.

Maximum global experience
Appreciated for more than 10 years by Internet
Service Provider in150 countries.