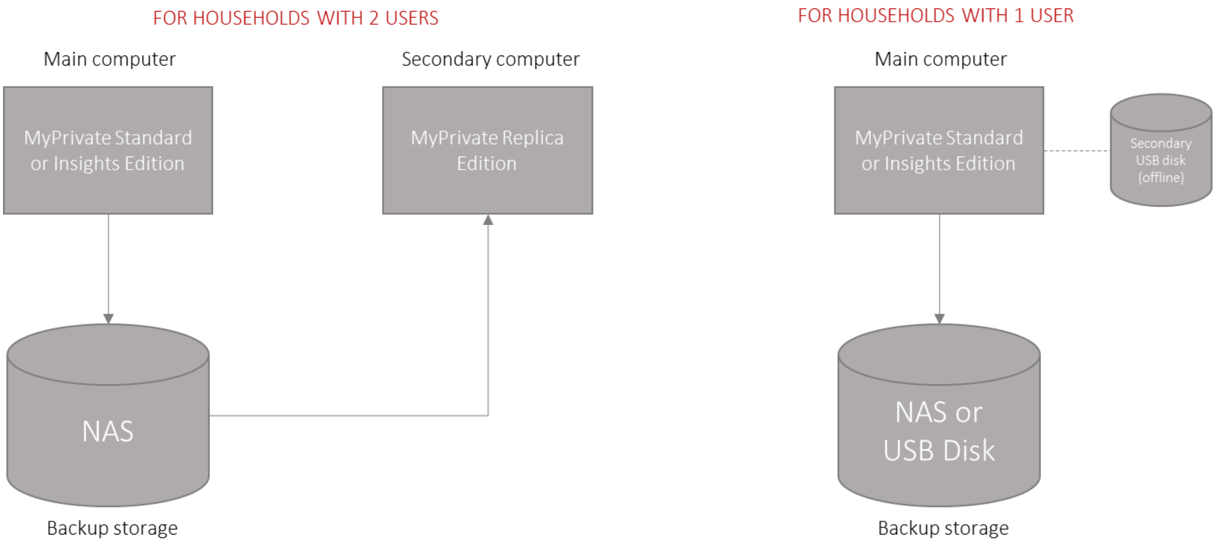
MyPrivate Security Guidelines

Users of MyPrivate will cumulate precious history over the years, and it is vital to protect the information against loss, corruption or theft.

While there are no 100% fool-proof solution, applying many good practices to make it highly unlikely that theft or major data loss will occur.

Most of the MyPrivate households have one or two users; the following minimum hardware configuration is recommended for solid protection:


FOR HOUSEHOLDS WITH 2 USERS
Main computer
MyPrivate Standard or Insights Edition
Secondary computer
MyPrivate Replica Edition
NAS
Backup storage
FOR HOUSEHOLDS WITH 1 USER
Main computer
MyPrivate Standard or Insights Edition
Secondary USB disk (offline)
NAS or USB Disk
Backup storage

Configuration recommendations

- Windows 10 Professional with automatic download and installation of updates.
- Use of the standard Windows Defender and Windows Firewall.
- Use of a VPN when connected to an outside network such as a café, hotel or airport.
- Data encryption of your drives; for the main computer, secondary computer and USB devices the native Windows Bitlocker functionality can be used while for the NAS drive the vendor must provide encryption support; in case of theft of the computer, NAS or USB Hard drive the data will not be readable.
- For households with 1 user
  - In addition to the backup on NAS or USB disk, a separate offline USB disk is required for monthly backups using the native MyPrivate backup function; in case of infection with ransomware of the main computer and/or NAS the offline storage will remain intact.

- For households with 2 users
  - No Windows file sharing between primary and secondary computer; this ensures protection in case of infection with ransomware of either computer and/or the NAS.
  - On the main computer, activation of Windows File History with daily update frequency; in addition, activation of the native MyPrivate backup with weekly frequency. Multiple recovery options remain available in case of disk or database corruption of either computer or NAS.
- The main computer, secondary computer, NAS and USB Disk should never be all left physically in the same place to protect against theft, water or fire damage.
- Configuration of the web browser with preset links to common links such as financial institutions, reducing the risk of becoming a phishing victim.
- Activation of password protected screen saver with short timeout, protecting against unauthorized access in public places.
- Careful reading of the guidelines for entering and managing codes in the MyPrivate Family module.
- No use of cloud storage functions such as OneDrive, DropBox for storage of MyPrivate data.
- USB keys should not be plugged in any computer unless known from a trusted origin; there are known instances of USB keys infected with viruses and/or ransomware.