Viruses, worms, trojans, riskware, and spyware are seen today as the biggest IT security threat to organizations around the world. Hackers also actively look for unprotected systems that contain important data or machines that could be used for other purposes, such as distributing illegal material or creating attacks against other systems.

F-Secure Linux Security protects Linux machines and network storages effectively against malware, spyware, riskware, and attacks from the network.
Linux security can be easily deployed and managed in mixed environments where an unprotected Linux machine is a potential vector for an attack or malicious content that would make a corporation vulnerable. Linux security offers:

**Comprehensive Protection against malware**
Stops all types of malware, including Linux and Windows viruses.

**Firewall management**
Provides robust monitoring and filtering of Internet traffic, preventing unauthorized access.

**Real-time, on-the-fly anti-virus scanning**
Prevents distributing harmful content across machines.

**Host Intrusion Detection and Prevention**
Keeps hackers and crackers from opening backdoors, installing rootkits, changing critical files, or saving unwanted files on corporate server and desktops.

**Multiple anti-malware engines**
Superior detection with highly advanced anti-malware engines, ensuring the best possible protection against current and future malware.

**Centralized management, reporting, and alerting**
Provides easy configuration, reporting and alerting to administrators of any security incidents or virus activity.

**Extensive Linux distributions support**
Supports a wide range of Linux distributions and versions.