Various security methods have been employed in an attempt to inhibit illegal copying of software. Such attempts have included software security, such as password protection and requiring original diskettes to initiate startup, for example, and hardware security, such as a dongle, for example, inter alia. Further, hardware-based copy protection techniques, as well as those which involve modification or customization of executable programs, prevent software vendors from exploiting the non-traditional distribution networks that are becoming a mainstay of software distribution in the software marketplace. Therefore, these protection methods have generally proved inadequate for large-scale commercial distribution of software. Thus, most large software companies have relied on shrink-wrap licenses and legal remedies to enforce their copyrights which have proved moderately effective.

Another challenge to the software industry is regulating the installation of software. Since individual users perform most installations of software, the vendor has no control over the software installation. A user can currently purchase software that will not run on the user's computer. The user may not know the limitations of the user's computer hardware or may not understand the software's hardware requirements. If a user purchases software and the user's computer hardware is inadequate to run the software, then various problems are going to occur in the installation and execution of the software on the user's hardware. The user will have to spend much time and effort attempting to resolve the problem, often including multiple calls to the vendor's technical support lines at a cost to both the vendor and potentially the user.

Additionally, companies having large networked facilities can internally have thousands of networked computers accessible by numerous content servers on a single network. Each of the content servers can be running any of various operating systems as can the computers with which the servers are communicating. From an information management standpoint, maintaining such a computer base can be very difficult given that each user may have to install their own software or, in the case of networked software, each server has an individual copy of networked software for a subset of the users.