Technical questions.

Q. Is DeviceLock software or hardware?
A. DeviceLock is software.

Q. What exactly does DeviceLock do?
A. DeviceLock controls user access to various types of computer devices (such as USB and FireWire ports, Bluetooth and Wi-Fi adapters, CD-ROMs, and so on). DeviceLock allows administrators to block access to devices by one user and, at the same time, allow access to these devices by another user.

NetworkLock, an extension to DeviceLock, provides control over network communications. Administrators can designate user access to the FTP, HTTP, SMTP, Telnet protocols, instant messengers (ICQ/AOL Instant Messenger, Windows Live Messenger and Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), webmail and social networking applications (Gmail, Yahoo! Mail, Hotmail; Facebook, Myspace, LinkedIn, LiveJournal, Odnoklassniki, Vkontakte, Twitter).

ContentLock, another extension to DeviceLock, extracts and filters the content of data copied to removable drives and plug-n-play storage devices, as well as that transmitted over the network. Administrators can create rules that specify which content can be copied and transmitted.

Q. *Is DeviceLock encryption software, i.e. does it encrypt the data?*
A. No. DeviceLock does not encrypt any data. It only controls user access to devices.

Q. How does DeviceLock protect data?
A. Access control for devices works in the following way: DeviceLock intercepts every request coming from the user to a device. Then, DeviceLock checks whether this user is allowed to use this device or not. If access is allowed, the request is passed on to the device. Otherwise, the user receives an “access deny” message and can’t access this device.

Access control for protocols works in the following way: Every time the user wants to access a remote network resource, DeviceLock intercepts this connection request at the kernel level of the OS and checks the user rights in the appropriate Access Control List (ACL). If the user does not have the right to access this protocol, an “access denied” error is returned.

Q. Which devices can be controlled by DeviceLock?
A. USB ports, FireWire (IEEE 1394) ports, serial (COM) ports (including internal modems), parallel (LPT) ports, infrared (IrDA) ports, Bluetooth adapters, Wi-Fi (wireless) network adapters, CD and DVD drives (including writable drives), floppy drives, tape devices, any removable storage devices (including memory sticks, flash drives, external hard disks, ZIP drives, etc.), any type of printer, including local, network and virtual printers, the Windows Clipboard, Windows Mobile, BlackBerry, iPhone, iPod Touch, iPad and Palm OS-based PDAs and smartphones.

Q. Which network protocols and applications can be controlled by DeviceLock?
A. The FTP, HTTP, SMTP, Telnet protocols, instant messengers (ICQ/AOL Instant Messenger, Windows Live Messenger and Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), webmail and social networking applications (Gmail, Yahoo! Mail, Hotmail; Facebook, Myspace, LinkedIn, LiveJournal, Odnoklassniki, Vkontakte, Twitter).

Q. Does DeviceLock work on UNIX (Linux, FreeBSD, etc.) or Mac?
Q. Does DeviceLock work on Windows 95, Windows 98 or Windows Me?
A. No. DeviceLock works only on Windows NT 4.0 SP 6, Windows 2000, Windows XP, Windows Vista, Windows 7 or Windows Server 2003/2008.

However, there is an unsupported product called DeviceLock Me that can work on Windows 95/98/Me. DeviceLock Me has limited functionality compared to DeviceLock – it can't control USB, FireWire, Bluetooth, Wi-Fi and Infrared devices.

Q. Should DeviceLock be installed on every computer in the network or only on a server?
A. DeviceLock must be installed on every computer where it's needed to control user access to devices. DeviceLock has a small agent (DeviceLock Service) that is invisible to users and works on each computer.

Q. Does DeviceLock support remote network management?
A. Yes. DeviceLock has a centralized management console. Administrators can manage DeviceLock agents on every computer in their network from this central console.

Q. Can DeviceLock be remotely deployed to network computers?
A. Yes. Administrators can deploy DeviceLock agents on every computer in the network from the central console. Also, DeviceLock agents can be deployed in an Active Directory domain using the MSI installation package and Group Policy.

Q. Do I need to manually connect to each computer in the network to change permissions there?
A. You can do it manually by connecting to each computer. Alternatively, if you have a large network, you can simultaneously set permissions to any number of computers using the Set Service Settings plug-in of DeviceLock Enterprise Manager. Moreover, in an Active Directory domain, DeviceLock's permissions can be managed via the Group Policy.

Q. Can users bypass DeviceLock's security on their local computer, i.e. disable DeviceLock?
A. No. Only users with administrative privileges are able to manage DeviceLock. If your network is configured properly and regular users don't have administrative privileges then it's impossible to disable DeviceLock.

Q. Does DeviceLock set permissions when the user logs into the system?
A. No. Permissions are applied immediately after the administrator has changed them at the management console.

Q. What would happen if two or more users are logged in at the same time on the same computer (in case of Terminal Server or XP Fast User Switching)?
A. DeviceLock controls users' requests to access devices or protocols in a real time. Each user has his/her own security context and DeviceLock knows which user is trying to access a device or protocol. Hence, it's possible to deny one user access to a device or protocol and, at the same time, allow another user access to this device or protocol, even if both users are trying to access the device or protocol simultaneously.

Q. Is it possible to set permissions to devices or protocols for user groups?
A. Yes. You can set permissions for individual users as well as for user groups.

Q. Where DeviceLock takes a list of users and user groups?
A. DeviceLock takes account lists from the Windows security subsystem. These are the standard accounts used everywhere in Windows (e.g. for system logon, file/folder permissions, etc.).

Q. Does DeviceLock work with the Active Directory?
A. Yes. DeviceLock's permissions and settings can be changed via the Group Policy and deployed in an Active Directory domain. Also, DeviceLock retrieves accounts from the Active Directory as well as from the Domain Controllers.

Q. Is it possible to protect access to devices with a password?
A. No. DeviceLock is user-level access control software. It doesn't support weak custom solutions like password protection.

Q. Is it possible to protect access to devices or protocols for a certain time period?
A. Yes. You can define the time of the day and day of the week when the device or protocol should be accessible to a user.

Q. Is it possible to block the USB port but allow USB mouse and keyboard?
A. Yes. You can completely block ports but allow certain devices, like: mouse, keyboard, printer, scanner, modem, and Bluetooth adapter.

Q. Is it possible to allow the reading of files from the device but deny writing to it?
A. Yes. For those devices that support the reading/writing of files (like floppy, CD-ROM, flash drive, memory stick, ZIP, and other removable devices) you can block the writing operation but allow the reading.