Portable Data Protection Options

	TYPE/COST	DESCRIPTION	PROS	CONS	VENDORS
THEFT PREVENTION	**Cable lock** $25 to $70	A cable that attaches to the laptop either with adhesive or the unobtrusive micro security slot that's standard on most laptop computers. The other end of the cable is looped around a stationary object.	Inexpensive, low-tech option that's easy to use and discourages casual thieves. Both key and combination locks are available.	May encourage user to leave laptop unattended in a public place. Some cable locks are bulky.	Kensington, PC Guardian, Targus
	Laptop alarm $40 to $100	A car alarm for laptops. The device makes noise when the laptop is moved.	Attracts attention to the would-be thief. May come as part of another product, such as Caveo's motion-detection encryption PC card.	Limited options. One vendor, TrackIt, is no longer manufacturing the device. May encourage user to leave laptop unattended.	Caveo, Targus
TWO-FACTOR AUTHENTICATION	**Token or card** $20 to more than $100 for the hardware, plus administrative costs	A small device needed, in addition to a password, to access a laptop computer. It may combine with encryption to lock down the hard drive. Common devices include: a token that plugs into the USB port; a smart card that the user swipes or inserts into the machine; a proximity card that the user hangs around her neck; and a device like the RSA SecureID that generates an extra passcode for the user to enter at log-on.	When configured properly, easy for the user. It may work with the device's existing hardware, such as a USB port. Coupled with encryption, this option provides excellent security.	Expensive, especially considering the replacement and support costs when users lose the devices (and they will). The device also does little good if it is stored with the laptop. Many require an extra reader.	Authenex, Ensure Technologies, Kensington, RSA, SecuriKey
	Biometrics $40 to $200 for the reader, plus administrative costs	Authenticates the user with something he "is"—usually a fingerprint—in addition to something he "knows," a password or PIN. It may combine with encryption to lock down the hard drive.	User can't misplace the authentication device. Coupled with encryption, this option provides excellent security.	Expensive. Although some laptops, including certain models of the Sony Vaio and Lenovo's ThinkPad, have an integrated biometrics reader, more often a reader must be added on. Also, the jury is still out on the accuracy of biometrics. And some users consider biometrics an invasion of privacy.	Microsoft, Silex, Targus
ENCRYPTION	**Windows XP's built-in encryption** Included in purchase of Windows XP	Windows XP's Encrypting File System (EFS) is built into the operating system. Users can password-protect files or folders through the Properties menu (available by right-clicking on a file or folder). If a folder is encrypted, any new files saved or moved into the folder will also be encrypted.	The price is right. EFS can be paired with Microsoft's Active Directory and Group Policy, so that users will be able to encrypt an entire file system or just parts of it. Operating system log-on gives user access to encrypted files, so unencryption happens transparently when the user is logged in.	Very difficult to manage from an enterprise perspective because of the user intervention required. Also, files are generally encrypted only when they are stored on the hard drive. That means, for instance, an encrypted file sent as an attachment can be opened by the recipient without a password.	Microsoft
	File- and folder-based encryption $85 to $129 per seat. Annual or management fees may apply.	Add-on software that encrypts certain folders or certain types of files. User gets access with a password or via two-factor authentication. Some products touted as "intelligent" or policy-based, meaning that system administrators can specify, for instance, that any new Microsoft Excel file automatically be encrypted, or that shared customer lists be encrypted. File-based encryption is available for laptops, PDAs and smart phones.	Unlike Windows EFS, folder-based encryption is meant to be managed on an enterprise level. This type of encryption traditionally has better options for two-factor authentication than full-disk encryption, because authentication happens when the system is completely up and running. This option can keep an encrypted file or folder from being shared. If the user loses or forgets his credentials, he can still use the device.	Expensive. Difficult to administer, because companies have to work out detailed policies, and users have to comply with them. Separate authentication means extra work for the user. If a device containing personal information of customers is lost or stolen, the company will have to be confident that sensitive information was on an encrypted part of the hard drive to avoid disclosing the breach in states, such as California, that mention encryption in their disclosure laws.	Authenex, Beachhead Solutions, Credant, TrustDigital
	Full-disk encryption $76 to $129 per seat. Annual or management software fees may apply.	Add-on software that encrypts an entire hard drive, including applications. Once the user logs on, either with a password or two-factor authentication (described above), files are automatically encrypted and unencrypted on the fly. Can be installed on laptops, PDAs or smart phones.	Easy on the user, because authentication occurs only once, at log-on. Processors have gotten fast enough that users probably won't notice any performance degradation on newer laptops. If a fully encrypted device containing personal information is lost or stolen, the company probably will not have to disclose the breach under disclosure laws in some states, including California.	Expensive. Encrypting and unencrypting the entire drive, including large applications, may slow down older laptops. Difficult to administer, especially if the user loses or forgets his credentials. Files are encrypted only while they're on the device. Authentication options have traditionally been quite limited for full-disk encryption, compared with options for file-based encryption.	Authenex, Mobile Armor, Pointsec, Safeboot
REACTION	**Laptop tracing** $18 to $60 per year for one computer. Cheaper if purchased for multiple years.	A service that lets you track where your laptop is. The idea is that the stolen laptop secretly dials "home," and its owner can use the IP address or phone number to help law enforcement track down the unit.	Stolen laptops are rarely recovered, so if getting a laptop back is a priority, computer tracing is a good option. Some vendors work with police to recover stolen devices.	Though the idea of a tracing system for laptops has been around awhile, it's never really taken off, so its effectiveness is relatively unproven. Usually, recovering the hardware is the least of the company's concerns.	Absolute Software (which licenses the technology to CyberAngel and WinLocate), LaptopLocate
	Device reset/ remote kill Often included as a feature in other software, such as Beachhead's encryption software and Novell ZENworks' mobile device management tool	Software that resets or wipes the device if it is lost or stolen. This ranges from a utility that does a reset, to software that rewrites all data so it can't be recovered with forensics. Widely available for PDAs—BlackBerrys are commonly set so that 10 invalid password attempts trigger a reset. Less common for laptops—devices that may not be synced or fully backed up, so the consequences of wiping the data are much more extreme.	For devices like PDAs that are synced to a computer or server, there's little risk to erasing all the device's data if it's simply misplaced. The remote clear option can be deployed either automatically if the device does not "phone home" for a certain amount of time or after too many invalid password attempts, or pushed out manually when a device is reported lost or stolen. This option eases the embarrassment factor of a handheld computer gone missing.	Some remote-kill products are available only when the device is online. The information is not always overwritten, so someone could still do computer forensics on the device to access much of the data. Credant, for instance, says that its remote kill for laptops meets Department of Defense standards for ensuring that files are not recoverable, but its remote kill for smart phones and PDAs does not.	Beachhead Solutions, Credant, Intellisync, Novell, Sybase, TrustDigital