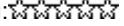


Tools: Primers

Primer: End-Point Device Security
By [David F. Carr](#)
2006-10-12

Article Views: 416
Article Rating:  / 0

End-point security protects against threats such as personal computers. A look at some strategies.

What Is It? End-point security protects against threats to the network "end points" controlled by users, mostly their personal computers. One big change to corporate security: Large amounts of data can be quickly and easily copied onto a keychain storage device, an iPod, or other inexpensive consumer devices that connect through a PC's Universal Serial Bus (USB) interface. As a result, it's now easier for sensitive corporate information to walk out the front door. Solutions include products from specialty software vendors that target portable storage device security, as well as features being added to security software suites from vendors like McAfee.

Is That Really a New Threat? You could say it's the same threat as when floppy disks ruled. Even then, it was possible for a 1.4-megabyte floppy to hold Social Security numbers and fall into the wrong hands. Today, that threat has been amplified. "You can put gigabytes of data on these things, as opposed to what you used to be able to put on a floppy," says Roy A. Balkus, CIO at Naugatuck Savings Bank in Naugatuck, Conn. He has implemented Centennial Software's DeviceWall product to control USB usage at the bank.












Who Are the Vendors? Centennial Software sells DeviceWall, which can prevent data from being copied to removable media or force it to be encrypted. SmartLine's DeviceLock has been marketed since 1996 as a tool for controlling access to floppy and CD drives, and now addresses USB ports. Device control is a feature of Verdasys's Digital Guardian and SecureWave's Sanctuary, as well as the Entercept intrusion-prevention system from McAfee. Technology buyers must decide between niche vendors focused on this specific problem and those that offer broader products that address other aspects of information security. For example, the Verdasys technology also aims to prevent proprietary data from being e-mailed out of an organization.

What Can I Do About End-Point Security?

Gartner analyst Rich Mogull outlines several strategies you can employ:

- ▶ Disable USB ports and other worrisome connection options on PCs whose users aren't allowed to remove corporate data.
- ▶ Track and monitor data being copied onto removable storage as a way of enforcing acceptable use policies for corporate data.
- ▶ Make access to USB devices and other storage mechanisms a restricted privilege controlled by an enterprise network security policy, with device access profiles for users and groups of users.
- ▶ Use software to prevent device access from a PC unless the device meets corporate standards. For example, a PC can be configured to connect only to USB storage devices that encrypt data, ensuring that the data cannot be easily removed if the device is lost or stolen.

Microsoft's network administration tools provide a basic mechanism for disabling PC devices, but specialty vendors have carved out a niche with more sophisticated solutions, according to Mogull. Verdasys's Digital Guardian, for

Rate This Article:	
Poor	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/> Best
<input type="button" value="Rate"/>	
Add This Article To:	
 Digg this	 Furl
 Del.icio.us	 Google
 Slashdot	 Simpy
 Y! My Web	 Spurl!
 E-mail	 PDF Version
 Print	

instance, can prevent users from copying data from specific file servers, he says.

Are There Any Pitfalls?

Security managers should not impose a solution that's too draconian, Mogull says. "I advise clients to take a step back and ask, 'What's the risk to us, really?'" he explains. Nonetheless, employing data-copying restrictions might make sense for companies or departments that deal with large amounts of sensitive consumer data or proprietary information that may be vulnerable to corporate espionage.

[Email Article To Friend](#) ♦ [Print Version Of Article](#) ♦ [PDF Version Of Article](#)