Realtime
publishers

Endpoint Data Encryption That Actually Works

The Essentials Series

Why Endpoint Encryption Can Fail to Deliver

Don Jones

Copyright Statement

Why Endpoint Encryption Can Fail to Deliver

As I mentioned in the first article in this series, many companies start exploring endpoint encryption and quickly become disappointed. The technology doesn't seem transparent enough, isn't centrally manageable, or perhaps doesn't work well with their existing systems and processes. What, exactly, goes wrong?

Traditional Solutions

First, let's look at the two most traditional forms of endpoint encryption: full-disk and file/folder.

Full-Disk Encryption

Full-disk encryption is exactly what it sounds like: You encrypt the entire disk of the client computer. Encryption keys may come from some kind of central storage, or may be delivered by a Trusted Platform Module (TPM) embedded within the computer's motherboard. Either way, that encryption key is required to decrypt the hard drive contents, and is typically needed to even start the computer each day.

Full-disk encryption is, on the surface, easy: encrypt everything, and don't worry about it. In addition to the weaknesses I'll outline below, however, full-disk encryption can be expensive, often requiring newer and more powerful computers and operating systems (OSs). In most cases, it's overkill—you're typically encrypting tons of data (and paying for that encryption in slower performance) that doesn't need to be protected.

An example of full-disk encryption is the BitLocker technology that ships with select editions of Windows Vista, Windows 7, and later OSs. Not all full-disk encryption solutions support removable storage devices.

Simple File/Folder Encryption

Simple file and folder encryption can be seen in technologies like Windows' Encrypted File System (EFS), which first shipped with Windows XP and Windows Server 2003. Essentially, users pick what files and folders they want to encrypt—and that's it.

The biggest problem with this approach is that it places the entire burden on the user. The user has to figure out what data should be encrypted, and they have to remember to *do* it. Not all file and folder solutions support removable devices, which is another weakness.

Traditional Weaknesses

These two traditional encryption approaches have some pretty significant weaknesses. This isn't necessarily "beating up" on these approaches, but if we're going to find an endpoint encryption solution that really works in the real world, we're going to have to acknowledge what *doesn't* work about these older approaches.

Too Many Point Solutions

Very few full-disk or file-and-folder approaches can protect your data *wherever* it sits. Removable USB drives—especially those ubiquitous flash drives—are probably the most commonly-missed endpoint storage.

That's not to say solution vendors haven't tried. The problem is that you wind up with a bunch of disparate, disconnected encryption solutions: *This* one for full-disk encryption of the client hard drive. *That* one to encrypt removable USB hard drives. *That* solution for USB flash drives. *Another* one for data being transmitted across the network.

Some of them might be centrally managed, and some of them might not. Experience suggests that some of them will likely conflict with each other from time to time, and supporting that many different forms of encryption can be really difficult. You'll likely be awash in different encryption keys and mechanisms and management tools—it can be a nightmare. What's needed is *one* solution that protects *everything* that you need protected—no matter where it sits.

Conflicts with OSs and Management Systems

One problem that full-disk encryption has especially encountered is conflicts with the host OS (Windows, for most businesses). Although built-in solutions like Windows' BitLocker do a good job of avoiding OS-level conflicts, many third-party solutions have encountered issues, and some vendors have had to do a significant amount of work to avoid those issues. Some companies who've explored full-disk encryption have had to back off, simply due to hardware and OS incompatibilities. Those incompatibilities can sometimes be alleviated if you have a standard client hardware platform and can find a solution that is known to work with that platform; that does, however, limit your flexibility in adopting other kinds of hardware.

Other application-level conflicts can arise, and you'll need to test very carefully for those. For example, applications like Microsoft Outlook that need to be able to create and manage offline cache files can cause compatibility problems with encryption software. You may also need to re-evaluate your client computer backup and recovery techniques and processes, as you may well have to change them or select different tools once full-disk encryption is in place. For example, suppose your users let their computers shut down every night. Your patch management system needs to be able to wake those computers and apply patches—but with full-disk encryption, that "wake" will be interrupted by the encryption solution's authentication prompt, preventing the actual OS from starting and stopping the patches from being deployed.

The bottom line is that, for some companies, full-disk encryption is simply overkill. It can impose significant performance overhead, and the main reason to use it is because you don't have a better, more granular way of managing what gets encrypted. You *should* aim for that more granular way, if possible.

One of the most-cited complaints about full-disk encryption is the way it can conflict with critical management systems and processes—including patch-management systems, disk defragmentation systems, and so forth. Some full-disk encryption vendors provide workarounds to these potential conflicts, and it's important that you consider them when selecting a solution.

Full-Disk Encryption = Full-Disk Access

Another problem with full-disk encryption is that it isn't really "user-aware." Think about it this way: A user encrypts his laptop using a full-disk encryption solution. They have to turn that laptop over to your IT staff for upgrades or repairs, and the staff needs to be able to *use* the computer—meaning they have to be able to start the OS. The encryption solution can allow that—but the IT staff will have access to *everything on the hard drive.* You can't just turn off a "part" of the full-disk encryption (that's the whole point of full-disk, after all).

Too Many Hurdles for End Users

Both full-disk and simple file-and-folder encryption are far from transparent. With the first, users have additional password prompts to start their computers (and IT must typically manage and sync additional passwords). With the second, users have to actively decide what files to encrypt. Neither solution is easy for users: They both require additional training, additional support time, and additional non-productive overhead for the entire organization.

Doesn't Protect the Data *Everywhere* It Goes

Removable storage is one of the biggest ways for your data to suddenly become unprotected. Many full-disk encryption systems simply ignore removable drives; others may offer to encrypt the contents of the *entire* removable drive, making it more difficult to use the drive to share data with other users while using it to carry protected data.

Less Compatible with Older Machines

Traditional encryption solutions are often less compatible with older machines. Older OSs and older hardware don't provide the power needed to support full-disk encryption, for example, which can add 10% or more overhead to a computer's continual processing needs. File-and-folder encryption is commonly more compatible, but again requires the most effort on the part of the user.

> **Note**
>
> Most companies' experience with simple file-and-folder encryption is that users don't employ it consistently enough to really accomplish the business' data protection goals.

Too Difficult to Deploy

Traditional encryption solutions can also be difficult to deploy. Encrypting an entire disk, for example, can take hours, so users need to make sure that process doesn't kick off until after business hours. Users accustomed to taking a laptop home with them may need to leave it in the office for an evening—and will be disappointed if everything didn't go smoothly because their computer won't be ready to use when they come to work the next day.

Deploying a file-and-folder encryption solution can be less impactful, but who decides what will be encrypted and when that will happen? It's up to your users—who may forget, may not select the right files, or may not use the solution consistently enough to meet your goals.

Making Endpoint Encryption Work in the Real World

The final article in this series will explore the techniques and technologies that can make endpoint encryption practical for a real-world company like yours. If you're putting together a "shopping list" of features and functionality that you'd like in an endpoint encryption solution, the next article will guide you through that. The focus will be on neither full-disk encryption nor on simplistic file-and-folder encryption, but rather on more granular, centrally-managed *policy-based* encryption.