Realtime publishers

Endpoint Data Encryption That Actually Works

The Essentials Series

Making Endpoint Encryption Work in the Real World

sponsored by

CREDANT®

We Protect What Matters

Don Jones

Copyright Statement

Making Endpoint Encryption Work in the Real World

If traditional endpoint encryption—full-disk encryption and simple file-and-folder encryption—don't do a great job of solving today's business needs, then what would? What kind of endpoint encryption *would* solve more of the critical data protection needs for today's businesses?

The Key: Policy-Based Encryption

The answer is *policy-based encryption.* Essentially, this is taking the best of full-disk encryption—not having to make users decide what to encrypt but rather having it happen automatically—and combining it with the benefits of file-and-folder encryption—lower-overhead, fewer conflicts, and better compatibility.

Essentially, your company defines centrally-controlled policies about what kind of data gets encrypted. Endpoint-level agents store these policies and implement them automatically, transparently, in real-time. Because the policy agent runs on client computers, the policy agent can apply file-level encryption to *any* file, no matter whether it's on a client computer's hard drive or stored on an external, removable storage device. The real flexibility of this approach lies in the different *types* of policies you could create.

By User

Do you have specific users in your company—perhaps the CEO, the corporate attorney, or a valued researcher—who produce data that must *always* be protected? Then simply direct your policy-based encryption system to always encrypt data created by that user. Now, wherever that user saves data, the data will be protected. That might be on the user's client computer, but it also might be on someone else's computer that the user has logged into, a USB drive they're carrying home for the weekend, or a removable hard disk that's used to archive important information.

By Group

Managing encryption on a per-user basis can quickly become overwhelming in large organizations, so being able to manage based on user groups—such as roles within the organization—is also a must-have feature. Perhaps you need to encrypt everything from the company's legal department, or everything from the research department. By simply placing users into groups that reflect the type of work they do within your organization, you're automatically ensuring that the right data is protected. If someone changes job roles, just update their group membership, and the right encryption rules automatically apply.

By Data Type

Not every piece of data generated by any one user needs to be encrypted, and so you should also be able to specify what *kinds* of data get encrypted: target Word or Excel files, or perhaps Access databases, or even data files created by a line-of-business application. This can be *especially* useful for the temporary files created by many applications because those might otherwise be ignored—yet might linger on disk and turn out to be a security problem at some point.

Combo Policies

Of course, the *best* and most flexible systems will let you combine these criteria. For example, "Encrypt all Excel documents generated by anyone in the Finance group, or that is saved by the CEO or CFO." These multi-criteria policies let you be extremely granular, centrally declaring what kind of data you want protected.

In fact, fine-grained encryption policies are what *really* help cut down on excess processing overhead. There's probably no need to encrypt that video from a recent conference that your CEO downloaded from the Internet, so simply encrypting "everything from the CEO" isn't much better than full-disk encryption. But by further narrowing your policies to types of data and other criteria, you're starting to really identify what's important to you and to make sure it's always protected.

"Get Everything" Encryption

The idea behind a policy-based encryption solution is that it watches *who* is creating and using data, and sees *what* kind of data they're working with—it doesn't need to be "location sensitive."

Local Storage

Local storage is obviously encrypted by the agent. This helps protect data if a laptop or desktop computer hard drive is stolen. However, because *only necessary files* are encrypted, the rest of the operating system (OS) can continue to function normally. Continue to back up and restore files normally—they'll be encrypted in the backups, too. Keep patching your OS and applications just as you always have: There's no barrier to waking a computer from sleep or shutdown, and the OS and application files aren't encrypted.

Best of all, if *someone else* uses the computer, the data *remains protected*—unlike in full-disk encryption schemes, where once you have access to the disk, you have access to everything on it. Multiple users can share a computer, and the policy-based encryption agent can ensure that each user's files remain private to them.

Removable Storage

Removable storage can also be protected in this fashion. There's no need for special encryption-enabled devices (which often lack central manageability); the policy-based encryption agent simply makes sure that the desired files are encrypted as they're written to the storage device. Unplug it, let users take it with them, and the data will still be accessible *to that user alone* when the user plugs it into another computer.

What About Network Storage?

You can't ignore network storage, of course, but it's not considered an *endpoint* because it's not where data is actually *used.* Typically, server OSs can offer their own robust tools for encrypting and protecting users' data—and, for servers, full-disk encryption solutions can make a lot of sense, with fewer of the drawbacks that crop up when full-disk encryption is deployed to client computers.

Transparent and Effortless

The idea behind these policy-based encryption solutions is that they take decisions out of your users' hands. You're not going with the all-or-nothing approach, but you're also not requiring your users to be sensitive to data protection requirements. You're making the encryption decision yourself, at the central policy level. You get the transparency of the full-disk approach (actually, better transparency), with the granularity of the file-and-folder approach.

Automatic Encryption

Policy-based encryption can be completely automatic. Because you're not using full-disk encryption, which often requires a pre-boot authorization (PBA) to unlock the drive for the OS, you're not requiring users to remember additional passwords. Policy-based encryption is more transparent but can still be trusted to grab all the data you've centrally defined as needing protection.

Best of all, users can't *override* that central encryption policy, as they can with simpler, "voluntary" file-and-folder encryption schemes. You're assured of the right data being protected all of the time, without having to train your users.

Deployment of such a system is also easy: The agent can simply begin scanning for matching data and start encrypting it on the spot. You don't need to take the entire computer offline (as is needed with full-disk encryption) in order to begin protecting all of the data that you actually care about. Change your mind about what data needs encryption? Simply update your central policy, and the agents on your endpoints will update their behavior automatically.

Simple User Prompts

With a well-designed policy, users shouldn't be prompted to make encryption decisions very often—but some solutions may allow you to specify "optional" or "recommended" encryption, and the endpoint-based agent should provide simple, clear, and understandable prompts to help users make the right decisions. As you evaluate endpoint encryption systems, be sure to specifically evaluate their "user experience" so that you can select a solution that requires the least end-user training and will generate the least end-user support overhead.

Central Key Escrow and Recovery, Central Reporting

Another aspect of central manageability is the ability to recover lost encryption keys, decrypt data from employees who have left the company, and to centrally report on the usage of the encryption system.

Key Escrow and Recovery

Key escrow is usually implemented as a secured database where copies of user encryption and decryption keys are maintained. Escrow enables a trusted administrator—or, more commonly, multiple individuals—to retrieve keys for other users for the purpose of decrypting those users' data. Primarily used as a "backup" to an employee leaving the company, key escrow and recovery is a crucial feature in any encryption system.

Reporting and Tracking

Another crucial feature is the ability to report on who is using encryption, and for what—and to report on who has modified any of the central encryption policies being implemented by your endpoint agents. Reporting and tracking can be a decisive feature for companies dealing with regulatory compliance issues: With the right reports, you can *prove* to your auditors what you're encrypting, *demonstrating* your compliance with regulations and making shorter work of otherwise time-consuming audits.

Conclusion

Although many companies have tried and turned away from endpoint encryption over the years, more and more are opting to try again these days. Some companies opt for full-disk encryption primarily so that they "don't have to worry about it," choosing to deal with the compromises, conflicts, and workarounds required to continue to manage their endpoints once the encryption solution is in place. With policy-based encryption, however, *you don't need to compromise.* You can decide what needs to be encrypted, and it'll just happen—even across removable storage devices.

It's possible that full-disk encryption may have a place within some portions of your company—for certain users, perhaps. Certainly, inexpensive options (such as BitLocker, which is built-in to some editions of Windows, or new hard drives with built-in encryption) seem cheap and easy. Be careful, however, to ensure that *all* of your needs are met—particularly consider interoperability, reporting, and centralized management—by whatever solution you choose.