Realtime
publishers

Endpoint Data Encryption That Actually Works

The Essentials Series

Why Businesses Need Endpoint Encryption

Don Jones

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Introduction to Realtime Publishers i
Why Businesses Need Endpoint Encryption 1
Protecting Data—Wherever It Sits 1
Local, and Removable Data 1
No "Islands of Compliance" 2
Compliance with Internal and External Requirements 2
Internal Requirements Growing to Embrace External 2
Compatibility with Existing Processes and Systems 2
Operating Systems 3
Management Processes 3
Support Techniques and Technologies 3
Transparency for End Users 4
Automatic 4
Simple Prompts 4
Centrally Managed 4
Trackable and Reportable 4
The Problems with Endpoint Encryption 5

Copyright Statement

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Why Businesses Need Endpoint Encryption

Does your business use endpoint encryption to protect data? If not, why not? Does your business know what endpoint encryption actually is, what it offers, and why you might want to use it? Do you know the potential disadvantages, and are you aware of subtle technology differences that can make a tremendous positive impact on your business?

Protecting Data—Wherever It Sits

Your business stores *lots* of data. Much of it is likely kept on a variety of servers—databases, collaboration software, email servers, file servers, and the like. That data is relatively easy to protect: Servers offer plenty of options for encryption and so forth. Unfortunately, some of your data—potentially even *much* of it—isn't just sitting on those servers. Copies exist everywhere, primarily on *endpoints*—the places where the data is often *used.* That means client desktop computers, laptops, and more—and many companies offer no protection for data on those devices.

Local, and Removable Data

When data is copied down to a laptop computer, how protected is it? What if it's copied to a USB flash drive, or to an external USB hard drive? The best-protected server storage can't protect data when it's in transit on a flash drive, when it's on a laptop, or when it's on removable drives.

Even desktop computers aren't risk free. True, they're not often removed from the office—but it's a lot easier to break into an office and steal a few desktop hard drives than it is to break into a data center, and many desktop hard drives are a treasure trove of data. Anyone who wants to get their hands on your company's sensitive data just has to snatch a desktop's hard drive, make off with a laptop, or even just pocket a USB drive or two. Picking up a USB key that an employee accidentally leaves lying around on a desktop—or on a table at lunch, or in an airport, or anywhere else—is easy. Endpoint encryption is about protecting data *wherever* it sits: on client computers, on removable storage, as it moves from place to place via external storage, and more.

No "Islands of Compliance"

Many companies dealing with external compliance requirements—such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and so forth—do so by creating "islands" of compliance. That is, they designate specific servers and network subnets to contain all data affected by their specific requirements, and they keep all of that data within the "island." The theory is that the island means you only protect the data that *needs* protecting; the problem with the theory is that it's practically impossible to actually keep data within the island. Data is just too easy to move, and your users *have* to work with it, so data winds up in places you didn't anticipate, and didn't think to protect. Before you know it, you're out of compliance, dealing with annoyed auditors, and potentially facing fines and embarrassment.

Endpoint encryption helps to solve this problem by eliminating the need for these islands. Instead, it focuses on protecting the data that needs to be protected *wherever* that data actually sits. Ideally, endpoint encryption can do so transparently and automatically.

Compliance with Internal and External Requirements

A growing amount of data is now subject to a variety of laws and industry regulations: patient records, customer information, payment data, employee personal information, and more. Companies have increasingly focused on meeting these requirements.

Internal Requirements Growing to Embrace External

At the same time, however, companies also have their *own* requirements for data protection: industrial espionage, competitive advantages, protection of intellectual property, and more. More and more companies are incorporating external compliance requirements into their internal policies, creating a single "master policy" for data protection, and defining a single set of rules about how covered data must be treated.

Without endpoint encryption, however, you'll have a difficult time truly meeting all of those rules for protecting your data. And with the *wrong* endpoint encryption, you may find yourself spending a great deal more time and money to protect your data and keep your users productive. In fact, ensuring that your protective measures will actually work with your existing systems is one of the biggest challenges facing most endpoint encryption solutions.

Compatibility with Existing Processes and Systems

One way to protect your data is to simply put it in a place where nobody can reach it. That would be pointless, though, because data is only useful when it's *used.* That means your protection schemes have to interact with your users and your other in-place systems. In fact, those "other in-place systems" can be one of the most challenging pieces of the endpoint encryption puzzle.

Operating Systems

If you simply encrypt entire client computer hard drives, will your client operating system (OS) continue to function? Can the OS actually operate when its own files are encrypted? What about application files? Is it better to just encrypt data files? Is that sufficient protection for your data? What built-in OS components will fail or be compromised if you go with full-drive encryption? And if you do, will you be able to protect data that *leaves* the hard drive, such as data moved to external removable storage?

In fact, one of the biggest problems encountered by most companies who begin experimenting with endpoint encryption is significant negative impact to client OSs—up to and including making the computer almost unusable. That's certainly not something you want to experience in your own endpoint encryption efforts.

Management Processes

How will you manage computers once endpoint encryption is deployed? Will you still be able to copy files to a computer through logon scripts, if you're currently doing so? How will patches and updates be handled when the computer's hard drive is encrypted? All of that *should* be automatic and transparent—but it isn't always so. You'll need to take steps to ensure that whatever encryption system you choose will work properly with these existing, critical management processes.

Some encryption systems, as you'll see in the next article in this series, can disable automated patch-management systems from working properly. That's certainly an unexpected and unwelcome scenario. Although many such solutions provide workarounds for that problem, the workaround itself can significantly reduce your security level, making the entire encryption solution one giant compromise.

Support Techniques and Technologies

How will you support computers once endpoint encryption is in place? Will you be able to back them up and recover them? Migrate users' preferences and data to a new computer when the time comes? Will remote management tools continue to operate, or will you have to invest in all-new techniques and tools—or will you simply have to get by without the functionality your IT team has become accustomed to? Ideally, all of your current techniques should continue working—but you'll have to pay very close attention to the encryption technology you select.

How will you even *deploy* endpoint encryption? Will users have to upgrade to new computers? Encryption—especially whole-drive encryption—can add significant overhead to a computer; will that overhead push your older computers over the brink into uselessness? These are all important questions to consider and answer as you explore endpoint encryption.

Transparency for End Users

Let's say you come up with the perfect endpoint encryption technology that accommodates your existing processes and technologies, runs smoothly on most of your client hardware, and protects the data you need. How will your users go about using it? Retraining can be expensive, time-consuming, and ongoing—which is one reason many companies first experiment with seemingly-transparent full-disk encryption. What exactly do you need an endpoint encryption solution to do in order to be effective *and* properly used?

Automatic

First and foremost, endpoint encryption must be *automatic.* Ideally, you centrally designate the data you want protected, and it just happens, in the background, without your users thinking about it. The fewer decisions users have to make, the fewer *wrong* decisions they'll make, and the more protected your data will be.

Simple Prompts

When users do need to make a decision, it needs to be presented to them in simple terms: "You seem to be copying sensitive data to a removable USB flash drive. That data should be encrypted. Would you like to do so?" That lets you give your users options, but also helps to guide them to the decision that's most often the right one.

Ideally, as much of your endpoint encryption as possible should be done without user input, but in some cases, minimal user input may be required. Users may have to identify data that *shouldn't* be encrypted by the system, for example—such as when they have to exchange that data with an external third party, and the transmission solution is already providing mutually-compatible encryption. By keeping prompts short, simple, and clear, users gain the ability to operate the system more effectively, reducing your support costs and increasing the opportunities for the encryption system to do its job properly.

Centrally Managed

Perhaps most importantly, your endpoint encryption needs to be *managed.* Encryption key escrow should be maintained in a central, secure database so that no corporate data is at risk of being permanently lost. The choices given to users, and what data is automatically protected, should be configured in a central, policy-based system that users can't override without permission.

Trackable and Reportable

In the world of compliance—and increasingly even in companies' own internal security rules—*evidence* is king. That means you not only must have an endpoint encryption system in place but also be able to demonstrate that it's being properly used. That requires central tracking of who encrypted what and when—along with central reports to summarize that information for auditors.

The Problems with Endpoint Encryption

In the next article in this series, we'll look at ways in which endpoint encryption can fail to deliver, and the subtle techniques and technologies you'll need to consider as you move forward with protecting your company's critical data.