NSA vs. Encryption

Article written by Datto developer Dan Fuhry first appeared on MSPmentor.com in November 2013.

> **"We will stand in our firm commitment to protect you and your customers."**

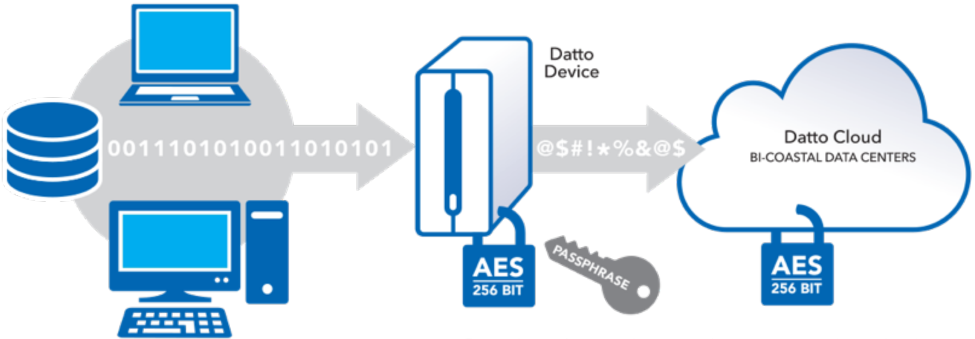
If you've been watching the news lately, there is no doubt you have heard about the National Security Agency's (NSA) surveillance scandal. Recent months have seen a revelation of programs that capture domestic and international traffic indiscriminately. Encrypted data gets saved for a certain number of years, in case they ever decide to decrypt it.

If this alarms you, that's good. You should be alarmed. I was too, on a very personal level, and have actively been working on changing some long-established habits in order to protect the information that is private and personal to me.

For MSPs not in the United States you should be even more alarmed. It's not even your own government that has the encrypted data, and since you don't have constitutional protection in the U.S., there is nothing legally standing in the NSA's way to prevent them from using their dark magical cryptographic powers to obtain your confidential business or personal data.

This is a frightening proposition indeed, which is why I want to talk about the position Datto has taken regarding the recent revelations.

Before we go any further, allow me to briefly describe my role here. I'm a developer with Datto, and I designed the encryption feature for Datto SIRIS. I picked the ciphers, hash algorithm parameters, and random number generator algorithm, had them peer-reviewed, and then wrote the code. I've been an applied cryptography and authentication enthusiast since high school. When I was a little kid, I printed numbered passes for people to present as they entered my room. Security is my life and breath.



Datto's end-to-end encryption prevents data viewing, tampering or theft during the entire continuity process

In cryptography, the terms "enemy" and "attacker" are thrown around a lot, and while it might seem a little politically incorrect, I view the enemy as anyone who might view or tamper with your customers' data without the permission of that customer. That includes unauthorized users within your customer's company and external attackers. It includes the government, and technical support and operations personnel at Datto. It includes you and me. If your customers want nobody to view their data, then I consider it my personal mission and goal to make it impossible for anybody to view their data without the key.

My design for Datto's encryption system provides unique encryption keys per agent, so there is no single key that can decrypt every dataset we have. The key used to encrypt your actual data is the master key, and that master key is only ever stored in an encrypted fashion. It's completely random – not derived from a passphrase – and no human ever sees it. When you enter your passphrase, your Datto device does some number crunching on that passphrase and some additional data to get a user key. That user key is used to decrypt an encrypted copy of the master key. This gives you the ability to change your passphrase without having to re-encrypt the entire dataset, and have multiple valid passwords per agent.

The important thing to realize here is how vital your passphrase is to decrypting your data. Without it, the number crunching required to find your data is impossibly immense, even for the NSA. Datto doesn't keep your passphrase anywhere. Therefore, no court can compel us to hand over your unencrypted data, because we don't have it and can't get it.

"The important thing to realize here is how vital your passphrase is to decrypting your data."

In the face of current events, we at Datto know that our customers may view the government as an enemy in the cryptographic sense, and we respect that. We are absolutely aware that our Partners, especially those who are international, want to keep their customers' data out of the hands of the U.S. government. I'm writing this to personally guarantee to you that anything you consider a threat, we do too, and we have designed our products accordingly. We will stand firm in our commitment to protect you and your customers.

Starting November 11, every Datto SIRIS will come with end-to-end, agent-level encryption as a standard feature. This is part of Datto's commitment to our Partners to create "regulatory safe" solutions and products. Get more information on Datto's information security controls in our new whitepaper, "5 Cornerstones of HIPAA Compliance" or reach out to partners@dattobackup.com.