Enterprise Social Network Convo Adds At-Rest Encryption To Its Servers To Better Protect Client Data

Posted Dec 12, 2013 by Alex Wilhelm (@alex)

Convo, an enterprise social network that competes with the now Microsoft-owned Yammer, today announced that it has added at-rest encryption (ARE) to its servers in order to better protect its client information.

Recent revelations relating to the National Security Administration (NSA) have taught the technology community and world at large that data isn't safe from surveillance, and other forms of snooping. One NSA program, MUSCULAR, became infamous for tapping communication links between American companies' data centers abroad.

The Washington Post reported that the NSA has "secretly broken into the main communications links that connect Yahoo and Google data centers" abroad, and that by "tapping those links, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans."

In response, Google and others are working to encrypt the data that flows between their vast server installations. Microsoft, for example, went as far as calling the NSA and others of its ilk "advanced persistent threat[s]."

Convo's move today echoes those efforts, by expanding the amount of its data that is encrypted. At-rest encryption is just that: encrypting the data sitting on servers. This information is distinct from data that is in transit, which could be comprised in other ways. It's important to encrypt information on the go, as MUSCULAR taught us, but also encrypting data that is just sitting about internally could become the next frontier in protecting customer and user information.

This hits home, as a number of publications that I have worked at use Convo. I would frankly not like the NSA to learn the things that I've said about it. I only publish the polite versions, such as they are.

According to Convo, it is the first product of its kind to add ARE to its technology stack. I spoke to the company today and it indicated that it expects this form of protection to become as common as SSL in the coming years, though it could take longer for larger firms to follow in its footsteps. The more data that you have, the larger the challenge.

Though there are extant reports that the NSA is working to end encryption as we know it, it remains clear that we need more, and not less data protection. At-rest encryption is another brick in the wall separating our right to privacy from government intrusion. As an industry, we need to get to work on building that wall as high as we can.

Top Image Credit: Flickr