THE WALL STREET JOURNAL.
U.S. EDITION ▾ Thursday, December 12, 2013 As of 9:06 AM PST

Tech Customers More Attentive to Security in the Wake of NSA Leaks

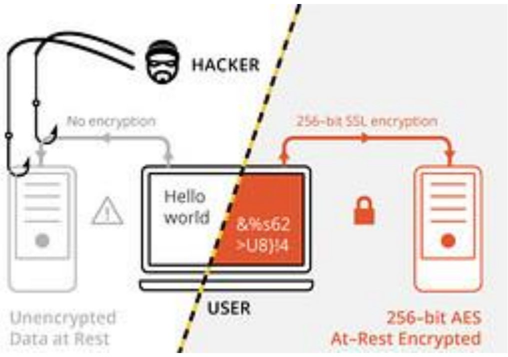
By DEBORAH GAGE

On-going revelations of NSA spying and data monitoring have made corporate customers nervous about doing business with American tech companies, and tech companies have been trying to ease their fears by bolstering the security of their products.

Indeed, security has become a selling point for companies that can demonstrate how much they care about customers' data, although how data is protected and how much it's protected are still not standard.

"Enterprises try to disregard security whenever they possibly can unless they have compliance mandates because it can reduce their agility," said Gartner Research Director Lawrence Pingree. "Even though [security] makes people paranoid and causes consternation, at the end of the day, it's all about money."

Convo Inc. Chief Executive Faizan Buzdar, whose company's online collaboration software is used by customers with very sensitive information, now encrypts data both in transit—as it travels between a server and a user's machine—and at rest, when it's sitting on the server.



Securing data in transit and at rest Convo

Encrypting data in transit is common, but encrypting data at rest is more complicated, and Mr. Buzdar says that Convo, which is a cloud company, goes beyond other vendors in its category by encrypting all data on the server at all times so that a hacker would find only gibberish.

"I think it will become a normal [practice]. It's a privacy issue and I want to see every company that has communications doing that…Given all this debate, there isn't really enough focus on what we should do," he said.

Convo's competitors, which include Jive Software Inc. and Microsoft Corp.'s Yammer, are not standing still.

Jive, whose software can reside in the cloud or on internal servers, protects data in transit and at rest and has recently contracted with a third party to keep customers' encryption keys so customers will be notified if their data is subpoenaed.

Not all customers want that service because it can make handling any data problems more challenging, according to Jive Senior Vice President of Engineering Brian Roddy, but "there's a trade-off between convenience and security. We want to give them choice," he said.

Meanwhile, Microsoft Corp., which owns Yammer, said last week that it would expand encryption and legal protections across its services and would also allow government customers to review its source code for back doors that could admit snoopers.

"Yammer data in transit between customers and data centers is always forced to use transport encryption," a spokeswoman said. "A number of security controls are in place while Yammer data resides in the data center, including the encryption of any data that is backed up."

But Mr. Buzdar, who says Convo has won deals from Jive and Yammer, says tech companies in general should do more to protect customers' data and that customers should be able to tell simply by looking what those protections are.

Like the little padlock that appears in a browser when a customer is conducting a secure transaction with a bank (showing that the data is protected in transit), data protections "should be self-evident to the user," Mr. Buzdar said.

Write to Deborah Gage at deborah.gage@wsj.com. Follow her on Twitter at @deborahgage