nCrypted Cloud emerges from stealth mode with free data encryption offering

Analyst: Agatha Poon

12 Mar, 2013

Having emerged from stealth mode in early February, cloud storage security startup nCrypted Cloud is aimed at addressing pertinent concerns over data security and privacy in third-party cloud storage environments. Building on its patent-pending technology, the company provides what it refers to as a 'virtual security layer' on top of cloud storage platforms while enabling users to encrypt/decrypt data with a few mouse clicks. At present, it provides individuals and corporate customers using Dropbox with a free download of a basic version. The goal is to extend platform support to include other cloud storage providers such as SkyDrive and Google Drive following the commercial availability of the two paid versions, Consumer Pro and Enterprise, which are expected to be available at the beginning of May.

Technology and product

Data encryption is done through 'personal key' generation. When a user encrypts the data, it will generate personal key on a per-file basis. The personal key is generated based on the email address provided by the user in registering for an encrypted Cloud account and the password used for the nCrypted Cloud account identity and stored within the nCrypted Cloud software installed on the user's PC.

The company says it also generates a PKI key pair in which the public key is used to encrypt the key for the file with a personal recovery key. If the private key ever changes (due to a change in email address/password), users are still able to access their information with their personal recovery key. For the Enterprise version, multiple identities can be added. A recovery key is also created for enterprise users. If the user is no longer with the company and his or her access right to corporate data is revoked, the user can still access his or her own data.

The key pair is stored within nCrypted Cloud's database and is protected with the user's personal key. Thus, the nCrypted Cloud server does not know or have access to it because it distributes the key pair to multiple devices. Given that the data is encrypted locally, the startup says the Key Store will be invalidated if a third-party user tries to log onto the PC by altering the original user's credential.

At present, any sharing is based on first sharing in Dropbox for data delivery. The company says it is working on adding a Trusted Share option where users can simply share a file with a third party through a one-time usage URL. Upon the commercial availability of its paid versions (Consumer Pro and Enterprise), nCrypted Cloud will extend support for SkyDrive and Google Drive users. Advanced features such as a user-set timer for simple URL sharing and folder sharing between different storage providers will be available in future iterations as well.

In addition to a Consumer Basic version, which is now available for free download, nCrypted Cloud will make available two paid versions – Consumer Pro and Enterprise with audit details and centralized control of corporate data, respectively. While both paid versions are now in beta, the Enterprise version is available for up to six business organizations. As the commercial versions – expected to be available in early May – come online, pricing will be on a per-user/month basis. And the Free Consumer version will always be available as a way to drive collaboration.

Target segment

Targeting consumers and enterprises, nCrypted Cloud focuses on simplicity without compromising control. Users can select from multiple policies by right clicking on any files or top-level folders. For the secure sharing feature, however, the self-service feature is applicable only when users select folders, not individual files. Both consumers and enterprise users are able to access files/folders from mobile devices running on iOS and Android mobile platforms.

The company is working with four enterprise customers, which have already tested the consumer product, to test out the enterprise functionality later this month. Beta companies come from multiple vertical segments, including a top 10 ranked university in London (14,000 students and faculty), a Fortune 500 insurance and health care provider (40,000 employees), a federal law enforcement organization (50,000 staff), and a global science and manufacturer (58,000 employees).

Business model

The company claims to have several hundred free downloads since February and is working closely with its four beta customers to put the Enterprise version through its paces. It has been leveraging all social media outlets to engage potential customers and is identifying beta customers for the Enterprise edition through targeted media. NCrypted Cloud is looking to develop strategic partnerships with cloud storage providers as part of the go-to-market strategy, but it's still early days.

Founded in July 2012 by the former president and founder of Verdasys, Nicholas Stamos (CEO), and former distinguished software engineer of Verdasys, Igor Odnovorov (CTO), nCrypted Cloud's vision is to facilitate collaboration among consumers and enterprise users through information sharing. It raised an angel round of funding in late 2012 of more than $2.25m that will be used to bring the commercial editions to market. The company has a team of 16 employees, including a dozen full-time employees. It is potentially looking to raise further funding from strategic investors, possibly in the second half of this year.

Competition

The idea of building a security layer on top of cloud storage services is not foreign to industry players and nCrypted Cloud is not the only game in town. Companies like Sookasa and Secomba (BoxCryptor) have similar offerings, although technology implementation is quite different. Sookasa seems to focus its efforts on exploiting opportunities in the enterprise market. In the case of BoxCryptor, users must create and keep their own passwords and data will be lost if users fail to retrieve their own passwords. NCrypted Cloud is likely to be compared with Vivo, created and owned by PKWARE, in the data encryption arena. Cloudfogger also provides a freemium model to boost uptake. BoxProtect, in its current version, provides data encryption only for Dropbox users running on Mac OS X or using an iPhone or iPod Touch and is looking to extend support for additional cloud storage providers.

On the service provider side, cloud storage providers such as Amazon, Mozy, Nirvanix and Rackspace have invested considerably in hardening their offerings. Amazon, for example, claims to have each object encrypted with a unique key using the server side encryption feature. Nirvanix secures data transfers by providing AES 256-bit encryption and SSL options. That being said, users are less likely to get the level of self-service capability to define and implement security policies.

The 451 Take

Despite the growing availability of competitive offerings, nCrypted Cloud has done a good job in striking a balance between security and control. With a simple to use interface, users, for the first time, are able to define their own privacy settings and make security policies. This is likely to become the norm in the era of self-service. While Dropbox has a good representation in the cloud storage market, the ability to maintaining vendor neutrality is as important as delivering its performance claims moving forward.