Solution Brief

\Orchestrating a brighter world NEC

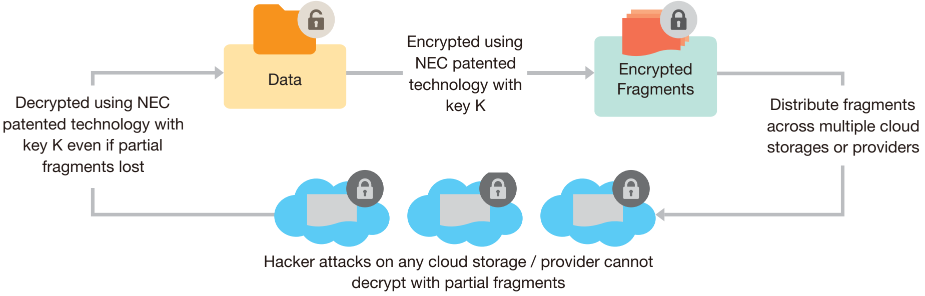
Secure Multi-Cloud Gateway

"All or nothing data encryption technology for the heterogeneous cloud domain"

Securing Multiple Clouds As You Expand

Ever expanding business needs are forcing companies to think beyond their own private clouds and tap on the public cloud for business agility. There's just one issue — securing the data passing through the various servers. In the wake of high-profile cyber attacks in recent years, IT leaders have struggled to find ways to rapidly expand IT resources to achieve business goals while protecting the data from being exposed to unauthorized users. This balancing act of maximizing access while putting up a robust defense against cyber threats has never been tougher.

Be too slow to provide adequate cloud storage and employees set up their own shadow IT resources, increasing the risk of cyber attacks to the entire enterprise. Rush to provide cloud access without enough thought and IT leaders risk the same outcome. The need for action is more urgent today as organizations grapple with changing needs in the workplace. While employees appreciate the speed and scalability of the cloud, many do not understand the risks they face when they use cloud services, especially those not authorized by their organizations.


Data
Encrypted using NEC patented technology with key K
Encrypted Fragments
Distribute fragments across multiple cloud storages or providers
Hacker attacks on any cloud storage / provider cannot decrypt with partial fragments
Decrypted using NEC patented technology with key K even if partial fragments lost

This calls for a rethinking of how data can be protected, as organizations big and small store more their information on multiple clouds. The approach may not be about creating sanitized areas for staff to work in, because these virtual spaces could end up being too costly and cumbersome to set up and use. They are not foolproof, either. In a high-dependency hospital ward, it is important for people entering and leaving to ensure they observe hygiene habits as well. Its efficacy depends not on sealing off everyone but on ensuring people followed the best practices when accessing the area. The same applies for cloud access. While being secure, a solution has to be fast and easy to use. It also has to be to cost-efficient, so it does not detract from the benefits of deploying on the cloud in the first place.

In a study of more than 2,000 office workers in the United States and the United Kingdom in 2015, 93 per cent of respondents were found to engage in "unsafe" online behavior that could jeopardize their employer's or customers' data[1].

A separate survey in the UK the same year revealed that most office workers are unclear on their company's position on cloud storage. Conducted by CensusWide, the study found that 65 per cent of the 1,000 employees surveyed don't have or don't know their company's policy on cloud storage[2].

Rethinking Cloud Security

NEC's Secure Multi-Cloud Gateway brings encryption, reliability and verification — three important factors — to the table, while enabling customers to continue using their existing hardware and software over multiple clouds. Key to this is an "all or nothing" encryption technology. Even if a cyber criminal were to break into a cloud server and steal a fragment of the data stored on it, he would not be able to decrypt the information and view part of the data.

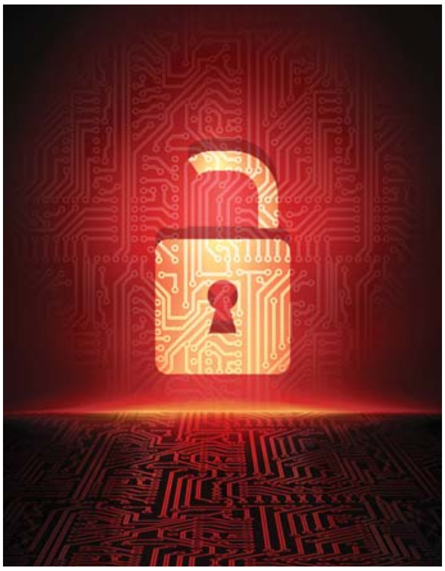
Each data segment secured with NEC's Secure Multi-Cloud Gateway is encrypted with a key, before it is distributed over multiple clouds. An authorized user not only has to have the right key to decrypt the data, but has to have all the fragments in place. This reduces the chance of a hacker accessing part of the information, for example, if he manages to break into a cloud server. The solution is also harder to crack compared to traditional encryption solutions, where a hacker can take a compromised fragment of data and decrypt it with a stolen key. What if an attacker, such as an insider, manages to steal all the data fragments as well as the key? This unlikely scenario can be made even less likely if the key was a physical token which does not store any data anywhere and cannot be digitally copied.

Using Silicon Biometrics, a unique physical key can be used to decrypt data by an authorized user. This key, unlike traditional forms that may be "listened to" or possibly cloned, cannot be duplicated because its physical attributes change when someone tries to open it up for inspection or for tampering. With such a key enrolled with the NEC's Secure Multi-Cloud Gateway, users can still easily log on to services, while having a more secure way of authenticating themselves to a cloud system. Together with the "all or nothing" encryption technology from NEC, it forms a formidable security solution for accessing data online.

Besides encryption, NEC's Secure Multi-Cloud Gateway also provides reliability and verification. With the solution, small meta data can be highly replicated in-house while large data can have lower replication on the cloud. With integrity checks built in, this brings added reliability to the data stored on multiple clouds. For verification, NEC's solution is able to detect remote failures on data availability rather than the server's availability. It retrieves proof that the data is indeed available for audit purposes. Easy to use and fast to set up, NEC's Secure Multi-Cloud Gateway does not require any modification to existing cloud configurations. The same applies to databases, file systems or apps, which remain as they are.

For large organizations such as governments and enterprises that have multiple clouds, this is an important factor. NEC's solution brings added security and reliability to a large number of users who are accessing the information from various points of the enterprise. Small and medium enterprises (SMEs) will also benefit. With a cost-effective physical key that uses Silicon Biometrics, they would not worry about paying extremely high prices to securely access their information on the cloud.

Looking further ahead, the rollout of the Internet of Things will also mean more collection and storage of data on various clouds. Encumbering this endeavor with proprietary security measures or rolling things out first without adequate measures in place would both be costly mistakes that require rectifying in the future. A setup that is agile yet secure is the smarter way for organizations to deploy sensors or smart devices, along with the associated cloud storage and processing.



Why choose NEC?

With years of experience behind us, NEC is well-placed to help protect the data stored increasingly on distributed cloud setups. We have worked with governments, city planners and other public agencies in projects as varied as identification and public transport. Our solutions include national identification, law enforcement, immigration, protection of critical installations, safeguarding of cyber infrastructure and emergency and disaster response.

Get in touch

To find out more about securing your cloud data with NEC, contact us over e-mail at safety@gsd.jp.nec.com.

WE MAKE CITIES SAFER
Using technologies to safeguard lives and property

NEC Corporation | Global Safety Division
■ 2, Fusionopolis Way, #07-01, Innovis, Singapore 138634
■ nec.com/safety ■ safety@gsd.jp.nec.com.

[1] http://www.esecurityplanet.com/network-security/93-percent-of-office-workers-engage-in-risky-behavior-online.html

[2] http://www.realwire.com/releases/Rampant-Employee-Use-of-Cloud-Storage-Services-Placing-Business-Data-at-Risk