BIZCOMMUNITY

Gateway encryption provides an answer to cloud security concerns

By Tony Willis

30 Jul 2013

Cloud computing has moved well beyond buzzword status to become a bona fide business-enabling technology area that can be used enterprise-wide, by sales, marketing, procurement and line of business, and for multiple purposes - including collaboration.

However, despite cloud computing's evolving maturity its adoption continues to face a number of challenges due to public, hybrid and community-based cloud solutions being based on an internet-based accessibility and delivery backbone - and enterprise data being stored externally.

On the flip side, cloud is often deployed (unchecked) in silos where business units, and even individuals, are using public cloud services without considering that this might leave the business vulnerable.

The argument is often that we cannot wait weeks and months for a corporate solution when we can start using a public cloud offering within hours.

Human nature

The challenge, therefore, is for IT departments and/or their outsourced providers to deal with a very real factor: human nature. And rather than resisting it, why not simply provide a set of security precautions that enable the business rather than constraining it?

The same solution can enable on a broader level those companies that remain reluctant to move over to the cloud as they have inherent concerns about security, privacy and compliance with industry-based regulations.

The industry has been working very hard at offering viable security solutions and cloud encryption gateways undoubtedly fall into this category. These gateways enable companies to encrypt sensitive information as it moves beyond the enterprise boundary into the public cloud and then decrypts it again when it is accessed again internally by users.

Should data ever be compromised (copied, stolen or accessed) while under the supervision and custody of a public cloud provider, the data is in encrypted format and will be of no value to any person illegally trying to make use of it, as they can see only an encrypted depiction/version of this sensitive data.

Furthermore, cloud encryption gateways maintain the cloud application user experience - with near zero latency - and without needing to make any changes to the cloud application itself.

A cloud encryption gateway is deployed at the enterprise perimeter and, essentially, acts as a reverse proxy server that monitors all incoming and outgoing traffic between enterprise users and their cloud applications.

The encryption gateway examines all outgoing cloud requests, in near real-time to encrypt or "tokenise" the data, and then modifies the request to the cloud application.

Similarly, encrypted or "tokenised" data returning from the cloud application is converted, again in real time, into clear text (i.e., text that can be read) prior to being displayed to the end-user.

Cloud encryption gateways are becoming more prevalent, which is why it important to choose the right one. Here are a number of important features to consider:

- An enterprise-class solution that offers support for all cloud environments: it must be deployable on-premise and support connectivity to public, hybrid, community and even private clouds;
- Offer support across most (if not all) public software as a service cloud applications (e.g. Salesforce, Force.com, Chatter, AWS S3, Google Gmail, and Microsoft Office 365) while enforcing unified data protection policies across these applications and over any communication protocol (HTTP, SMTP, SOAP, REST etc.);
- Strong encryption and tokenisation capabilities utilising industry standards, such as AES-256 strong encryption;
- Allow for cloud application capabilities, such as indexing, sorting and reporting to be maintained;
- Support mobile devices regardless of form factor: laptops, tablets, and smart phones; and
- Support latest technologies such as HTML5 applications.

Cloud encryption gateways undoubtedly form part of a feasible security solution for cloud computing and should be considered as part of any enterprise cloud strategy, as well as with any cloud migration or deployment to an external cloud environment.

ABOUT THE AUTHOR

Tony Willis is director of enterprise architecture, global ICT architecture of T-Systems International