F5 Friday: Big Data? Big Risk&hellip;

Lori MacVittie, 2011-16-12

#bigdata #infosec Storing sensitive data in the cloud is made more palatable by applying a little security before the data leaves the building…

When corporate hardware, usually laptops, are stolen, one of the first questions asked by information security professionals is whether or not the data on the drive was encrypted. While encryption of data is certainly not a panacea, it’s a major deterrent to those who would engage in the practice of stealing data for dollars. Many organizations are aware of this and use encryption judiciously when data is at rest in the data center storage network.

But as the Corollary to Hoff’s Law states, even “if your security practices don’t suck in the physical realm, you’ll be concerned by the inability to continue that practice when you move to Cloud.”

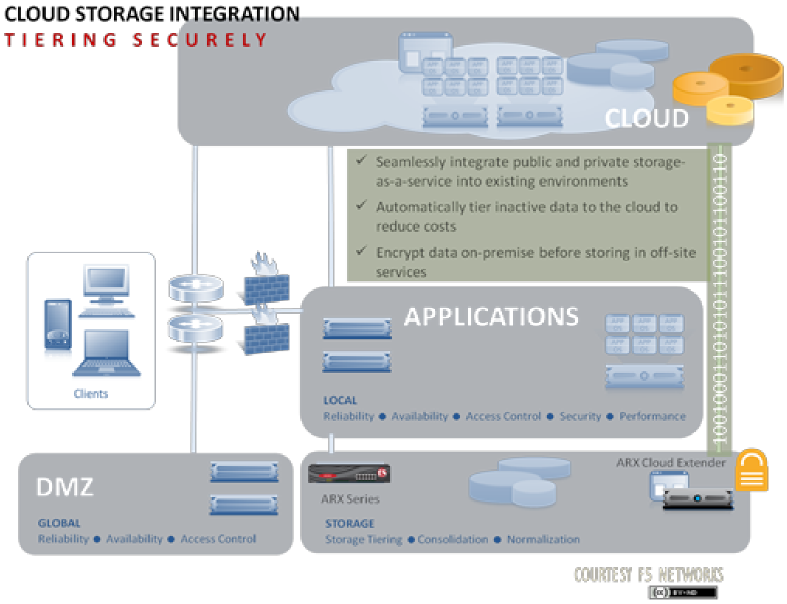
It’s not that you can’t encrypt data being moved to cloud storage services, it’s that doing so isn’t necessarily a part of the processes or APIs used to do so. This makes it much more difficult to enforce such a policy and, for some organizations, unless they are guaranteed data will be secured at rest they aren’t going to give the okay.

A recent Ponemon study speaks to just this issue:

> According to the report entitled "Data Security in the Cloud Survey of U.S. IT Operations, IT Security and Compliance Practitioners", only one third of IT security practitioners believe cloud infrastructure (IaaS) environments are as secure as on premise datacenters, while half of compliance officers think IaaS is as secure.
>
> -- Ponemon Institute Survey on Cloud Data Security Exposes Gulf between IT Security and Compliance Officers

INTEGRATION and REPLICATION

In order to make cloud a more palatable option it is necessary to ensure that data can be stored securely off-premise. A tried and true method is to encrypt the data before it leaves the building. And yet the same Ponemon study found that less than one-third of respondents’ organizations do just that.


CLOUD STORAGE INTEGRATION
TIERING SECURELY
CLOUD
✓ Seamlessly integrate public and private storage-as-a-service into existing environments
✓ Automatically tier inactive data to the cloud to reduce costs
✓ Encrypt data on-premise before storing in off-site services
Clients
APPLICATIONS
LOCAL
Reliability ● Availability ● Access Control ● Security ● Performance
DMZ
GLOBAL
Reliability ● Availability ● Access Control
ARX Series
STORAGE
Storage Tiering ● Consolidation ● Normalization
ARX Cloud Extender
COURTESY F5 NETWORKS

A possible explanation for organizations’ failure to encrypt data being transferred to the cloud is a lack of process and integration with the ways in which the data is transferred. Storing data in “the cloud” is generally accomplished via an API, and rarely do these APIs include a flag for “hey, encrypt my data.”

There are technical reasons why this is the case; encryption – at least encryption worth the effort and compute consumed – often makes use of certificates and keys. Those keys should be unique to the organization. Using a general cloud storage service encryption API would require either sharing of that key (bad idea) or the use of a common provider key (yet another bad idea), neither of which is an acceptable solution.

The answer is, of course, to encrypt the data before transfer to the cloud storage service. The cloud storage service, after all, doesn’t care what the data is – it just cares that it has to store it for you.

This brings us back to the problem of process and integration at the infrastructure layer. What organizations need to leverage cloud storage services is the means to automatically encrypt data as it's headed for the cloud. What organizations need is for that cloud storage service to be integrated with their own, data center based storage in a way that makes it possible to leverage cloud storage automatically, encrypting the data when it's bound for the cloud.

Organizations need a common, overarching storage solution that can seamlessly integrate cloud storage into operational processes and automatically provide a layer of security through encryption of the data when that data might be stored off-site, in a cloud storage service.

F5 ARX and ARX Cloud Extender (CE) is that solution. In addition to its core aggregation and intelligent tiering capabilities, adding ARX CE to the architecture will allow for the seamless extension of storage to the cloud securely.

> When ARX CE is preparing to send data to public cloud destinations, the data is encrypted using AES-256 bit encryption for each object. Further, all transfers from the ARX CE-enabled Windows file server to public cloud storage occur over SSL (HTTPS), which provides network layer encryption.
>
> -- Securing Data in the Cloud with ARX CE

The Ponemon study revealed that “less than half of IT practitioners (35%) and compliance officers (42%) believe their organizations have adequate technologies to secure their IaaS environments.” So not only do organizations believe the cloud is less secure, they also believe they don’t have the right tools to secure it and thus take advantage of it.

F5 ARX and ARX CE addresses the operational risk associated with storage in the cloud – by integrating cloud storage services into operational processes it alleviates the manual burden imposed on IT to schedule transfers and prioritize files across tiers. With the ability to automatically apply encryption to data and use a secure transport channel to cloud storage services, it adds a layer of security to data stored in the cloud that would otherwise not exist, giving IT the confidence required to take advantage of lower cost storage in the cloud and realize its benefits.

F5 ARX Cloud Extender Resources

- Securing Data in the Cloud with ARX CE (How To)
- ARX Tiered Storage: Best Practices
- Getting Up And Running With F5 ARX Virtual Edition
- F5 Storage Solutions
- F5 ARX 1500 and 2500
- F5’s New ARX Platforms Help Organizations Reap the Benefits of File Virtualization
- Network World – F5 Rolls Out New File Virtualization Appliances

- Analyzing Performance Metrics for File Virtualization
- Strategies for a Seamless and Secure Transition to Enterprise Cloud Storage
- Building a Cloud-Ready File Storage Infrastructure
- SSDs, Velocity and the Rate of Change
- F5 Friday: If Data is King then Storage Virtualization is the Castellan
- F5 Friday: F5 ARX Cloud Extender Opens Cloud Storage
- F5 Friday: ARX VE Offers New Opportunities
- Disk May Be Cheap but Storage is Not
- All F5 Friday Posts on DevCentral
- Tiering **is** Like Tables, or Storing in the Cloud Tier

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com