

## Securing Cloud Computing by GED-i

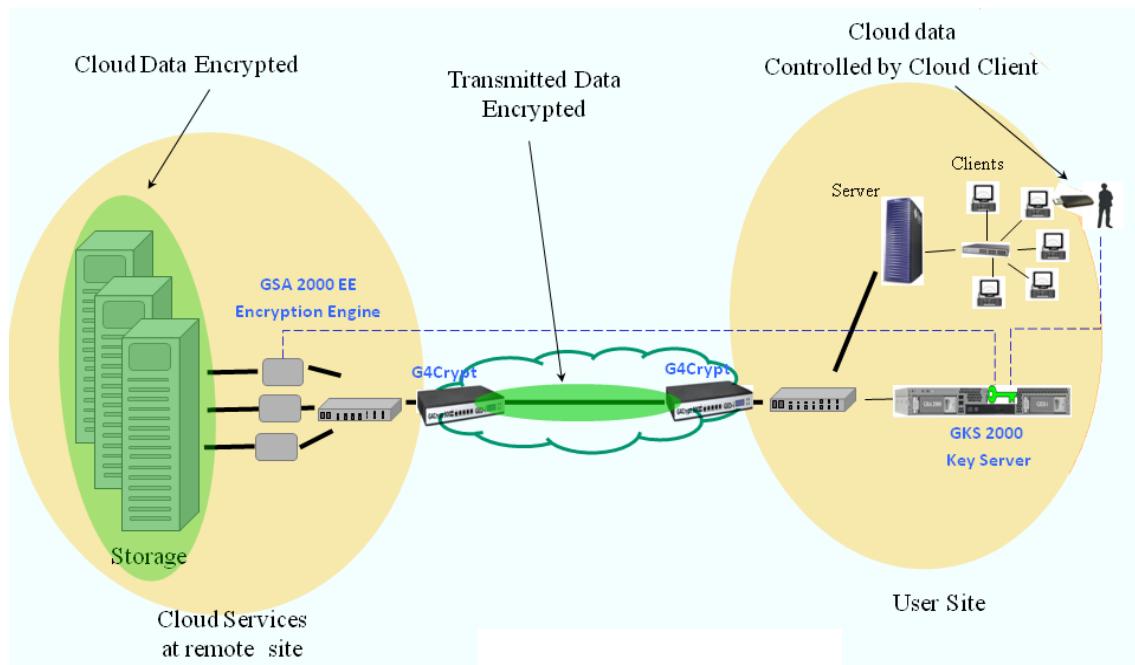
### General

Most IT professionals estimate that the **cloud computing** environment will dominate the deployment and usage of the IT and storage environment in the near future.

The usage of storage in the cloud environment presents new challenges regarding data security, since clients' data H/W platform and computing resources are remotely located and shared by several clients.

GED-i's product line presents a complete and optimal security solution for the cloud that can be controlled by the **cloud client**.

Based on the combination of GED-i's proven **Storage Encryption (GSA 2000)** product, the **Remote access and encryption control (G4EC, G4AC)** and **IP network encryption (G4Crypt)** product, GED-i offers a unique and total security solution for Cloud computing clients.



### Cloud computing security challenges

The main considerations for IT security in public and private cloud computing environment relates to higher risk to data theft, data integrity and data availability, due to the remote location of clients' data and computing environment. In addition, as storage is shared between clients, the client must rely on the cloud

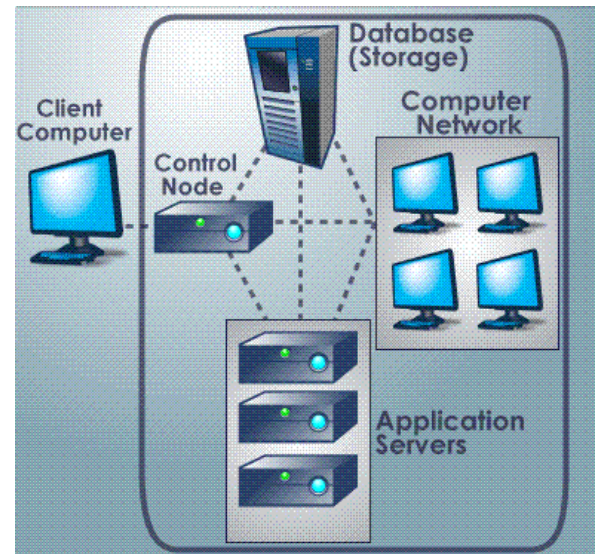
provider "sanitizing" storage that is no longer needed by the client, as this might reveal sensitive information to the next client that gets this storage allocation.

To ensure that the data is secured and available in the cloud environment, a security solution should cover all the layers composing the cloud, starting at the physical hardware layer and up to the application level within the virtual machine, **while data is in rest or in transfer**.

In Cloud computing, extra protection is needed since the hardware, i.e. servers, switches and storage are shared by several unrelated users. Consequently, risk of unauthorized access to or usages of private data and resources is significantly higher.

Since virtual machines may be moved dynamically from one hardware platform to another, security in cloud architecture is more complicated than usual computing environment. Therefore, in addition to classic protection methods and solutions, cloud deployment security requires specific solutions.

Data and software should be classified into layers. The lowest layer is the hardware bios, then the hypervisor (e.g., ESX, Hyper-v, XEN layer), next layer includes the virtual machines with associated applications, and the uppermost layers includes the data used by the applications within the virtual machines.



Since multi-users and unrelated users share the same hardware, the risk of unauthorized access to private data or resources is much higher. Therefore, suitable security architecture, control and monitoring tools should be deployed and used.

It is recommended that such tools will be used by the cloud users, while each client monitor and control only his own data.

At the same time, the cloud management tools should monitor and control the local data, s/w, hardware and the cloud users, without having an access to the cloud user data itself.

Failure to secure even one of these layers will lead to a breach and data privacy violation.

In cloud environments **most of the data resides most of the time** on the **storage**. Therefore, it is essential to protect the data, both physically and logically on the storages device itself. The protection should give an answer to data theft, data integrity and data availability as regard to storage data.

GED-i s' solutions for cloud environment presents security solutions for the data residing on, transferred to the cloud storage and used by the cloud client, while its security is **controlled by the cloud client**.

### **Cloud computing security solution by GED-i**



Based on the combination of **Storage Encryption** (GSA 2000), **Remote access and encryption control** (G4EC, G4AC) and **IP network encryption** (G4Crypt) GED-i offers a unique full security solution for **Cloud** computing clients.

GED-i solutions for cloud environment include the following:

- GSA – GED-i's Encryption solution for SAN
- G4EC – GED-i's remote Encryption Control
- G4AC – GED-i's Storage Access Control
- G4Crypt – GED-i's IP network Encryption

### 1. GSA

The GSA solution is a real time encryption system for FC\iSCSI SAN storages. The GSA solution encrypts all of the storage's data in real-time and transparently to the client/end user.

Encryption may be selected for whole storage or per specific LUN and it can be associated with every user or to specific services.

The GSA solution is based on encryption engine appliances – GSA2000 and GED-i Key Server - GKS2000. The Key server (GKS) creates millions of AES 256 encryption keys for each storage device. Keys are produced randomly by a hardware TRNG card within the GKS. The GKS can be located remotely at local site while the storage installed at remote site. Therefore, the permanent keys are located far from the encryption engines.

Within, the GSA2000 appliances the encryption keys are located in the RAM memory only (i.e., never on disk).

The GKS 2000 & GSA 2000 appliances separation enables to locate several GSA2000 units in the cloud environment while the GKS 2000 is located at the customer site.

The GSA Advantages in cloud environment:

- Independent security system
- On line encryption/decryption system at almost line speed
- Millions of AES-256 keys
- Separation of the GSA2000 appliances from their remote GKS2000 - Keys Central Manager, enabling the GKS2000 to be kept at the customer site.
- Encryption at block level for all data type
- Separation of authorization

### 2. G4EC

G4EC is unique add-on product to GSA 2000, enabling users to control storage encryption and access to the storage data.

The G4EC enables, per specific **service server** (oracle, Mail Exchange, DB, etc) to selectively control whether a specific service encrypted data will be decrypted and sent to specific service servers.

It functions as a service, bi-directional storage Firewall (FW) system. It blocks (FW mode) access to FC\iSCSI SAN storages based on a trigger. Switching-on the FW mode of operation is based on an insertion of a protected USB dongle (token) or other Administrator activator of the FW. The FW modes are predetermined, so the switching from one mode to another mode is quite fast.

The G4EC solution is based on GSA 2000 appliances installed in-line, i.e., between the switches\fabrics and the SAN storages.

The G4EC Advantages in cloud environment:

- Enables the cloud's customer to control access to its' cloud storage from Encryption and Access control aspects.
- Independent security system
- FW with triggered switching modes
- Bi-directional FW – (read/write access blocker)
- Separation of authorizations

### **3. G4AC**

The G4AC solution is a triggered, bi-directional storage Firewall (FW) system controlling access only, that is, without storage data encryption. It blocks access to a FC\iSCSI SAN storages based on a trigger. Activation of the FW mode of based on an insertion of a protected USB dongle or other Administrator activator of the FW. The FW modes are predetermined, so the switching from one mode to another mode is quite fast.

The G4AC solution is based on G4AC appliances which are installed in-line, i.e., between the switches\fabrics and the SAN storages. There is a G4ACs' central manager that manages all the G4ACs. There is separation of authorization between the one who operate the G4AC appliance and who is responsible for the central G4AC manager.

The G4AC Advantages in cloud environment:

- Enables the cloud's customer to control the access to its' cloud storage.
- Independent security system
- FW with triggered switching modes
- Bi-directional FW – (read/write access blocker)
- Separation of the G4AC appliances from their remote G4AC Central Manager. Therefore, enable to the cloud's customer to control the access to its' cloud storage.
- Separation of authorizations

#### 4. G4Crypt

The G4Crypt solution is based on dedicated encryption appliances that encrypt outgoing IP traffic using IPSec.

The IPSec encryption is based on AES-256. The Encryption Keys handling can be by Internal Certificate Authority or optionally by External Certificate Authority. GED-i's G4Crypt solution enables optional failover, automatic BYPASS and switching back when the failure is repaired. The G4Crypt appliances are remotely managed by SNMP or locally, after two factor authentication. The G4Crypt system can work in Point-to-Point mode or in Point-to-MultiPoint mode.

The G4Crypt Advantages in cloud environment:

- Enables encryption over the network between the cloud client and the cloud site.
- Enables optional bypass in case of failover.
- Enables real encryption, unlike in ordinary IPVPN which is only a Tunnel.
- Enables remote management by SNMP. As compared to ordinary VPN solutions which are supplied as extra feature to the Firewall appliances – it might be risky to enable FW to be handled remotely.
- Encryption actually starts at the client site gateway up to the cloud (and not from the closest switch-board supplied by the Internet infrastructure company).