Sphere Shield

Encryption for Cloud Apps and UC services

Requirement Background

Organisations may wish to benefit from cloud infrastructure but be wary of uploading their content to servers not under their control. Risks include access by cloud service employees, legal requirements in foreign jurisdictions, giving up participation in legal subpoena processes, compliance regulations and mass data collection by foreign intelligence services (e.g. PRISM).

Highlights

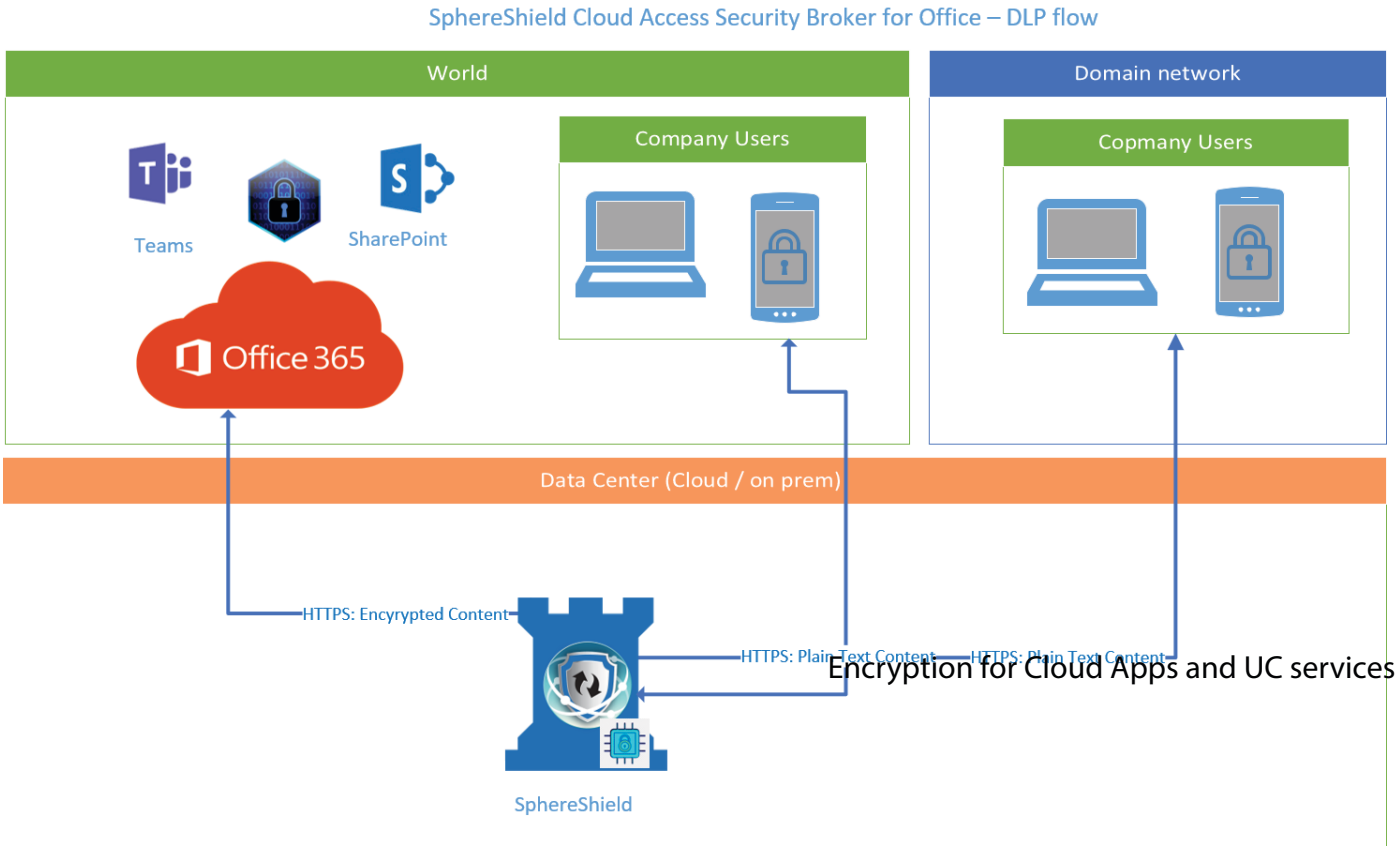
- Use Microsoft Teams, but store message content and files on prem
- Message content not stored on cloud servers
- No compliance issues storing data in foreign data centers
- Benefit from world class enterprise cloud solutions while retaining control of data
- Data encrypted before it reaches the cloud
- Use existing DLP infrastructure

Design

How

Using a Forward Proxy SphereShield can replace sensitive content on an on prem or VPS proxy server.

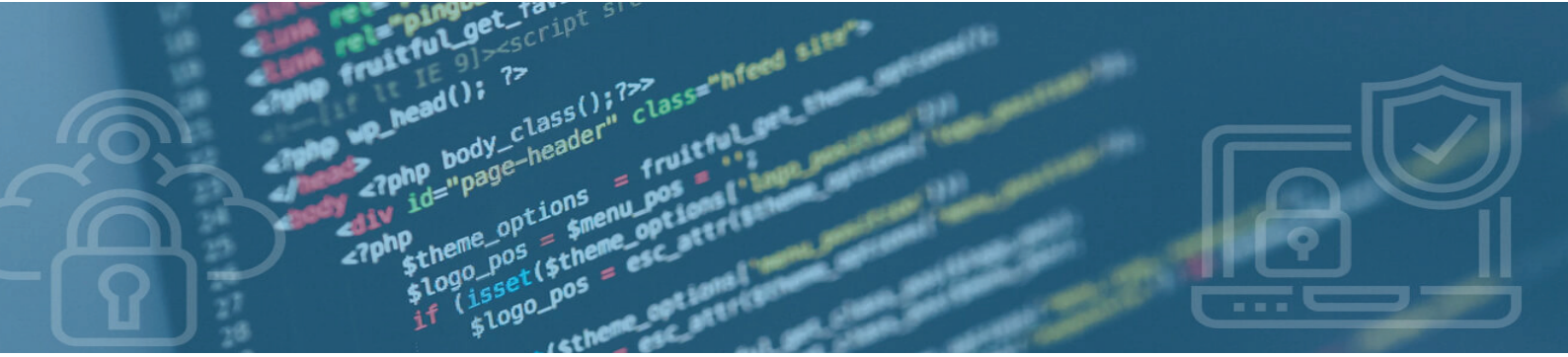
Clients would send and receive plain text content as usual, protected by SSL as before.
Clients would be configured to use SphereShield as their (forward) proxy. The proxy would inspect the traffic and replace content with encrypted content, so that the content stored on the cloud service would not be viewable.
Clients receiving content from the cloud service, sent to them by other users, would receive that content via the SphereShield proxy too, which would decrypt the content before it reaches the client.



Encryption

Content would be encrypted using an AES Symmetric key, as the SphereShield server would be responsible for both encrypting and decrypting the content. In this way the cloud service remains responsible for storing the content, but can't view it.

Protection of the single encryption key is important, as content cannot be easily re-encrypted with a new key and if the key is leaked then it impacts all stored data.



What

Content that requires encryption could include the following:

Level 1: Message text, attached files.
Level 2: User's real names, calendar content, Team, conversation and channel names
Level 3: Call and chat metadata (who spoke with who and when)

About AGAT Software

AGAT is an innovative software provider specializing in security and compliance solutions. AGAT's SphereShield product suite handles threats related to authentication and identity, as well as content inspection and data protection. Utilizing this expertise, AGAT developed SphereShield to secure unified communication (UC) and collaboration platforms such as Skype for Business, Microsoft Teams and Webex Teams.

AGAT's client base consists of government offices, banks, insurance companies and large industrial global corporations, including Fortune 500 companies.

For more information, visit http://AGATSoftware.com

For updates, follow us on LinkedIn & Twitter.

AGAT Software, Har-Hotzvim Hi-Tech Park,

Jerusalem, Israel

Tel: +972-2-5799123

Mail: info@agatsoftware.com