EPHESOFT

Ephesoft Cloud HyperExtender Security

Leveraging the cloud to harness high performance and scalability

Table of Contents

Introduction

Ephesoft is committed to protecting and respecting your data. The Ephesoft Cloud HyperExtender and our cloud microservices are purposefully designed and built to honor this commitment.

The Ephesoft Cloud HyperExtender enables customers open to cloud processing who have volatile document processing needs to leverage the high-performance cloud image processing and OCR capability on demand.

At Ephesoft, we understand how critical security is when it comes to processing documents in the cloud. We have been hard at work to make sure that your data is protected as it traverses the Internet and into our cloud data centers and back down to your Ephesoft Transact server.

How It Works

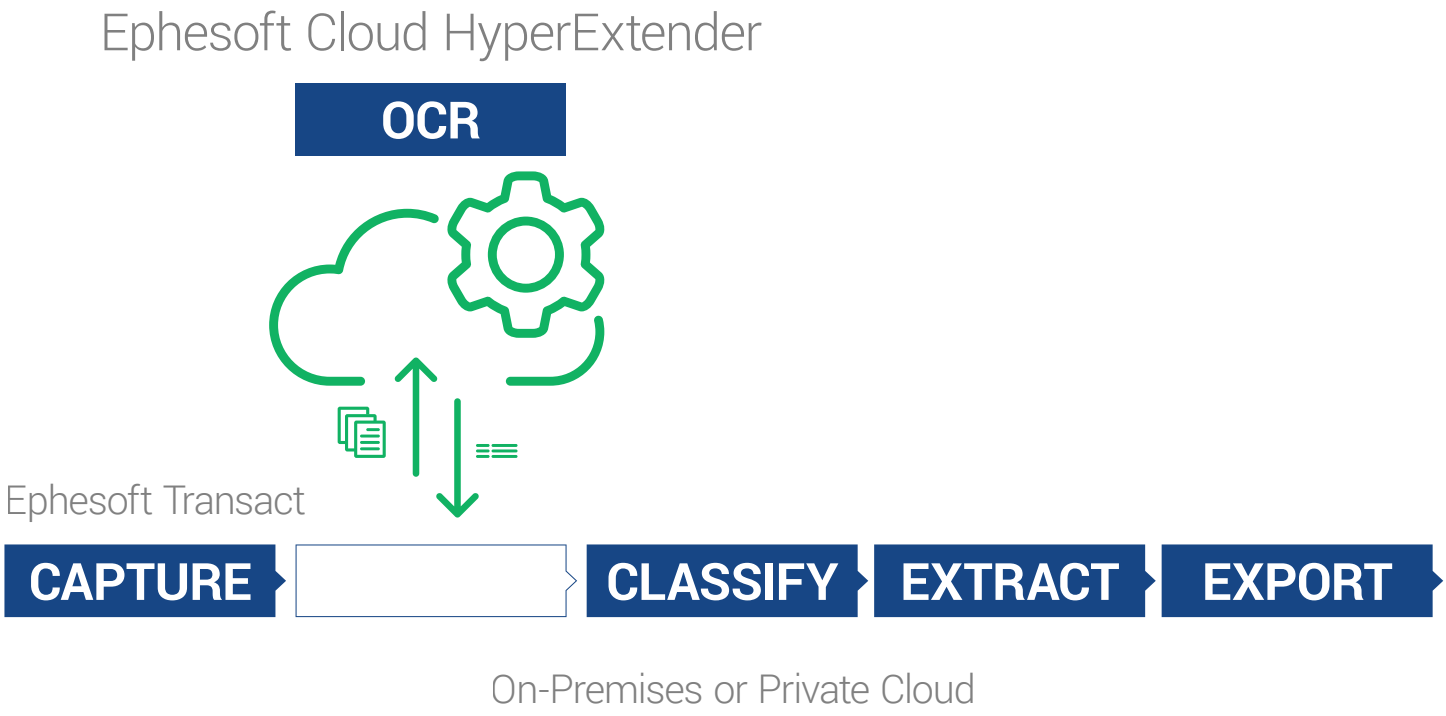
The Cloud HyperExtender seamlessly integrates into any Internet connected Ephesoft Transact installation, making the use of the cloud entirely transparent for the user.

To get started, the system administrator will complete a simple one-time registration and cloud configuration.

The batch class administrator will then reconfigure his batch class on his Transact server to turn on the Ephesoft Cloud HyperExtender, achieving unprecedented scalability on heavy resource-consuming processing like PDF to TIFF conversion and OCR.

Data Segregation

All temporary batch processing is being stored in areas which are unique for each customer in a region. Different customers will have separate storage areas ensuring that data is safe and segregated.



Encryption of Temporary Data at Rest

By default, we offer all our customers encryption of their data at rest. All objects are server-side encrypted when they are stored in your bucket with **managed keys (default)** and in a future release customers will be able to encrypt with their own keys.

Since encryption is turned on, an object will be encrypted before saving it to disk in AWS' data center and decrypted when you download the object.

Managed Keys (Default)

Our cloud vendor, AWS, encrypts each object with a unique key and additionally encrypts the key itself with a master key that rotates regularly. AWS' encryption algorithm uses one of the strongest block ciphers, AES 256, to encrypt your data.

In a coming release, we will offer customers the ability to bring their own keys so that they are in complete control of their content. Keys brought must be AES 256 keys encoded as base64. Ephesoft will never be able to see or access your key.

With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. The only thing you need to do is manage the encryption keys you provide.

When you upload an object, Amazon S3 uses the encryption key you provide to apply AES-256 encryption to your data and removes the encryption key from memory. Amazon S3 does not store the encryption key you provide. Instead, AWS stores a randomly salted HMAC value of the encryption key in order to validate future requests. The salted HMAC value cannot be used to derive the value of the encryption key or to decrypt the contents of the encrypted object. That means, if you lose the encryption key, you lose the object.

Encryption of Data in Transit

While it is important to encrypt data at rest, it is equally important to protect the privacy and integrity of the exchanged data while in transit. All the communication between the Cloud HyperExtender and the Ephesoft cloud infrastructure in AWS is through an HTTPS endpoint that is automatically encrypted using the AES-256 algorithm with Transport Layer Security (TLS). HTTPS protects against man-in-the-middle attacks, eavesdropping and tampering of communication.

TLS uses an 'asymmetric' Public Key Infrastructure system. An asymmetric system uses two 'keys' to encrypt communications, a 'public' key and a 'private' key. Anything encrypted with the public key can only be decrypted by the private key and vice-versa.

The 'private' key is kept strictly protected and is only accessible by the owner of the private key. In the case of the Ephesoft Cloud HyperExtender, the private key remains securely on AWS. Conversely, the public key is intended to be distributed to anybody and everybody that needs to be able to decrypt information that was encrypted with the private key.

Why HTTPS over HTTP?

All communications sent over regular HTTP connections are in 'plain text' and can be read by any hacker that manages to break into the connection between the REST client and the HTTP endpoint. This presents a clear vulnerability if the 'communication' is on an order form and includes sensitive information such as your credit card number or social security number. With a HTTPS connection, all communications are securely encrypted. This means that even if somebody managed to break into the connection, they would not be able to decrypt any of the data which passes between you and the website.

API Key Encryption

As part of the registration process for Ephesoft Cloud HyperExtender, an API key is provided to you. For added protection, this key is an AES 256 encrypted key.

Temporary Data Purge

Ephesoft will delete the customer's original uploaded data and processed data within 24 hours of having completed the image processing and OCR in the cloud. Deletion of data is done programmatically to ensure consistency in deletion across all data sources.

SOC (Service Organization Control) 2 Compliance

The American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC) released the revised version of the Trust Services Principles and Criteria (TSP) in 2014. Service Organization Controls (SOC) is an audit framework for non-privacy principles that include security, availability, processing integrity and confidentiality. Ephesoft has completed the SOC 2 Type 1 Audit and is currently going through the SOC 2 Type 2 Audit. We have hired an outside firm to perform the audit and will provide the report to interested parties as soon as it is available. The SOC 2 Type 2 report will confirm our compliance with the principles of security, availability, processing integrity and confidentiality.

Here is background on what SOC is directly from the AICPA website:

SOC for Service Organizations reports are designed to help service organizations that provide services to other entities, build trust and confidence in the service performed and controls related to the services through a report by an independent CPA. Each type of SOC for Service Organizations report is designed to help service organizations meet specific user needs:

SOC 2® - SOC for Service Organizations: Trust Services Criteria

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in:

- *Oversight of the organization*
- *Vendor management programs*
- *Internal corporate governance and risk management processes*
- *Regulatory oversight*

Similar to a SOC 1 report, there are two types of reports: A type 2 report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and a type 1 report on management's description of a service organization's system and the suitability of the design of controls. Use of these reports are restricted.

United States HQ
+1 (949) 335–5335
info@ephesoft.com

Ephesoft, Inc.
8707 Research Dr.
Irvine, CA 92618
United States

United Kingdom
+44 (0) 1184665000
info.eu@ephesoft.com

Australia
+61 2 9056 7490
info.au@ephesoft.com

Germany
+49 6126 5503510
info.eu@ephesoft.com

Italy
+39 (02) 8088 6345
info.it@ephesoft.com

France
+33 1 8288 4002
info.eu@ephesoft.com

Singapore
+65 3163 5499
info.asean@ephesoft.com