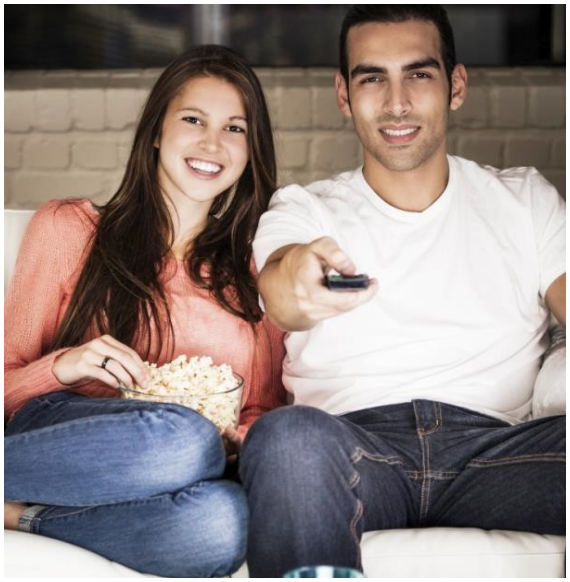
Enghouse Networks

espialtv

EspialTV Services Security and Infrastructure Guide

Version 1.2

May 2021



Contents

Overview

Enghouse provides a software as a service (SaaS) solution for video services providers under the brand name EspialTV. The scope of the solution offered is shown at a high level in the figure below.

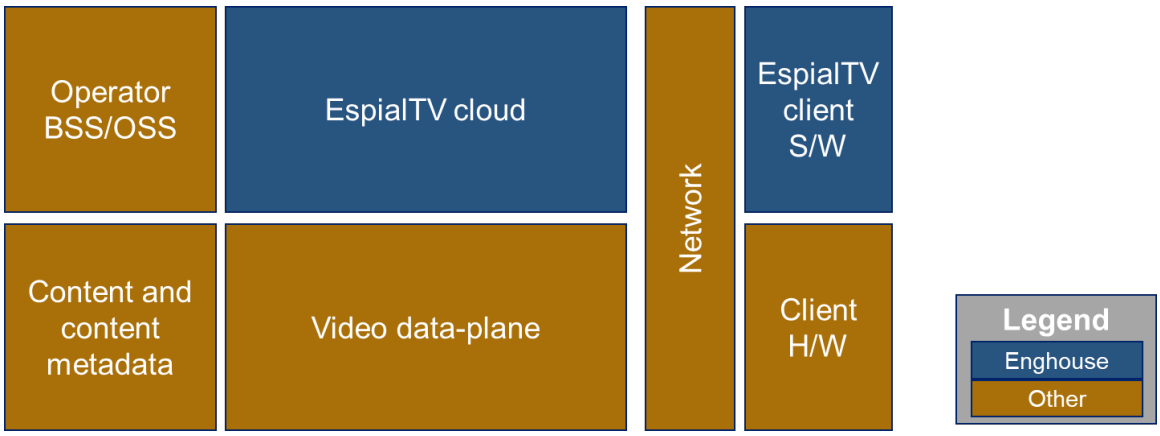


Figure 1 - High level view of EspialTV solution scope

Technical and organizational security and privacy measures are implemented for the EspialTV solution as per Enghouse policy and according to the architecture, intended use, and the type of service provided. The Software as a Service (SaaS) solution provides client software applications running on set-top-boxes (STBs) or other devices and a cloud-based solution for managing deployment, administration, operation, maintenance, and security of the solution. Operators using Enghouse's SaaS product continue to manage their end-user accounts, appropriate use of the Enghouse SaaS EspialTV product, and the data processed per the terms of the EspialTV Software Master Subscription Agreement.

Data Security and Privacy Measures

The data security and privacy measures are designed to protect and defend Enghouse's EspialTV service against risks related to the usage of the data, the software application, and the data itself. This document describes the overarching Enghouse policies and practices that are incorporated into the EspialTV Service.

Governance

Enghouse's IT security policies are established and managed by the Enghouse IT organization. Compliance with IT policies is mandatory and audited.

Security Policies

Enghouse security policies are regularly reviewed and refined as required to keep up with the changing world we live in and to defend against modern threats; they are in line with broadly accepted international standards. Upon determination that a security incident has occurred, Enghouse will promptly notify affected clients as appropriate.

Access, Intervention, Transfer and Separation Control

EspialTV's architecture for the cloud services maintains logical separation of client data. Access to client data is restricted to only those authorized personnel as per job duties. This access is controlled under IT policy and is monitored. Privileged access authorization is individual, role-based, and subject to regular review. Access to any client data is restricted to the level required for the delivery of services and support to the operator (i.e., least required privilege).

In addition to our own data center, Enghouse uses AWS as our primary service provider utilizing dual production instances, with active and standby locations. Enghouse employs AWS VPCs and network security groups to enforce access rules.

Upon termination of service, all confidential data will be deleted per the EspialTV Software Master Subscription Agreement in accordance with Enghouse's Data Privacy Policy.

Service Integrity and Availability Controls

Enghouse Engages security partners to perform penetration testing. Modifications to application software are governed by Enghouse's change management policies. Changes to network devices and firewall rules are also governed by change management policies and are separately reviewed by IT staff prior to implementation.

EspialTV products use secure protocols and strong authentication (TLS and X.509 certificates) to communicate over the Internet. Software payloads are also encrypted and signed to prevent tampering. Data center resources are monitored 24x7 by Enghouse to ensure service availability, and system architecture is subject to independent review for security issues.

Business continuity and disaster recovery plans are in place, maintained, verified, and tested. Recovery point and time objectives are established in accordance with architecture and intended use as provided in the Master Software Subscription Agreement. Backup data is encrypted.

Enghouse subscribes to a service that sends daily reports on security vulnerabilities found in the open source libraries and commercial products used in Enghouse client software and data centers. Each reported issue is analyzed for possible impact, and actions such as upgrades and patches are scheduled according to the severity of the issue. Enghouse's infrastructure is subject to disaster recovery and redundancy. Business continuity plans are regularly revalidated.

Activity Logging and Input Control

Changes made to cloud services are recorded and managed under change management policy. All administrative access to the cloud service is logged and monitored.

Physical Security and Entry Control

Access to production AWS consoles is limited to authorized operations personnel only, and the use of 2-factor authentication is mandatory.

Your Responsibilities

It is your responsibility to ensure that the set of security measures described herein meet your business needs.