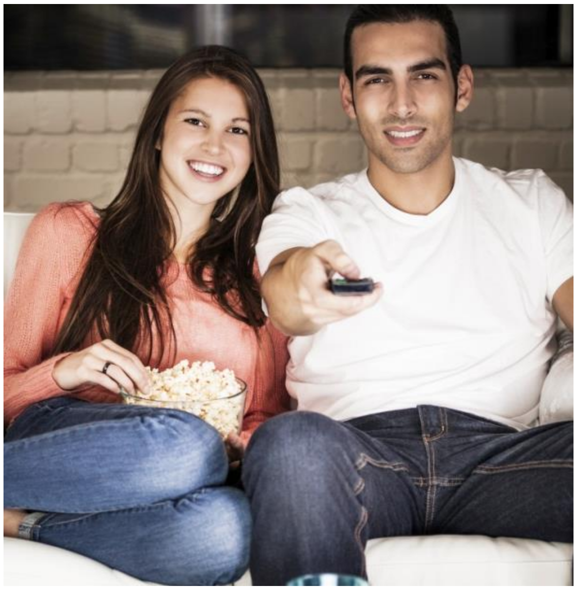
Elevate Services Security and Infrastructure Guide

Version 1.0

November, 2017



Introduction

Overview

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

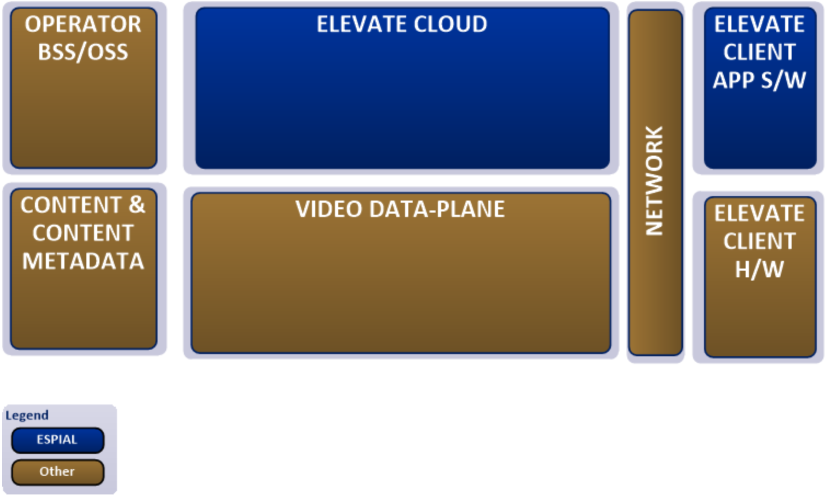


Figure 1 - High level view of Elevate solution scope

Technical and organizational security and privacy measures are implemented for the Elevate solution as per Espial 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 Espial's SaaS product continue to manage their end user accounts, appropriate use of the Espial SaaS Elevate product, and the data processed per the terms of the Elevate Software Master Subscription Agreement.

Data Security and Privacy Measures

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

Governance

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

Security Policies

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

Access, Intervention, Transfer and Separation Control

Elevate'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 if controlled under IT policy and monitored. Privileged access authorization in 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 (ie least required privilege).

Transfer of data within Espial occurs behind firewalls.

Upon termination of service, all confidential data will be deleted per the Elevate Software master subscription agreement in accordance with Espial's Data privacy policy.

Service Integrity and Availability Controls

Penetration testing and vulnerability scanning is conducted regularly. Modification to application software are governed by Espial'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.

Elevate 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 Espial to ensure service availability.

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

Espial subscribes to a service that sends daily reports on security vulnerabilities found in the open source libraries and commercial products used in Espial 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. Espial'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

Under IT Physical security policy, only authorized physical access to the data center is possible. Access is via card readers and under surveillance camera monitoring. Access is only allowed by authorized personnel. Terminated employees are removed from the access list and must surrender their access badges. Access badge distribution is logged.

Your responsibilities

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