LEONARDO CYBER & SECURITY SOLUTIONS

SECURE CLOUD MANAGEMENT PLATFORM

LEONARDO

Most organisations are undergoing the digital transformation of their processes and operations. The vast amount of data generated by services, sensors, connected devices and applications constitutes a valuable source of information that can be leveraged by companies thanks to the adoption of new disruptive technologies, such as Big Data or Artificial Intelligence. Data-driven innovative solutions are enabling public administrations to provide value added services for citizens and businesses, and to effectively support public safety and security in the country. At the same time, new applications are allowing private organisations to accelerate innovation, identify new business opportunities through data analysis, optimise production processes and improve the quality of their products and services.

The Cloud is one of the key enablers of this digital transformation. Thanks to its flexibility and scalability, it allows the implementation of services that guarantee business continuity, performance and efficiency. In recent years, the implementation of the Cloud-First strategy has resulted in an increasing use of this technology by public administrations and large companies through the adoption of public Cloud solutions. However, many organisations have not yet completely abandoned their private on-premise data centres, and services and applications migration to the Cloud is still in progress.

As a consequence, they have architectures in which new services on the Cloud coexist with solutions and applications on legacy technologies. Moreover, to avoid the technological lock-in the diversification of Cloud services, using different providers or solutions is one of the most common practice today. This approach allows the same organization to adopt architectures composed by multiple Cloud solutions, both on-premise and private, and by edge devices, in a continuum of hybrid models allowing to manage in an optimal way the requirements and criticalities of the different data and services.

The complexity of managing these heterogeneous environments arises mainly from the distribution of services across different technologies that must cooperate as if they were a single entity, ensuring performance and service quality. At the same time, the presence of multiple cooperating environments increases the cyber risk enlarging attack surface, and makes the adoption a strong cybersecurity posture extremely important for the company. Furthermore, the organisation's policies, best practices and regulations must be managed in an integrated way across the entire architecture.

SECURE CLOUD MANAGEMENT PLATFORM

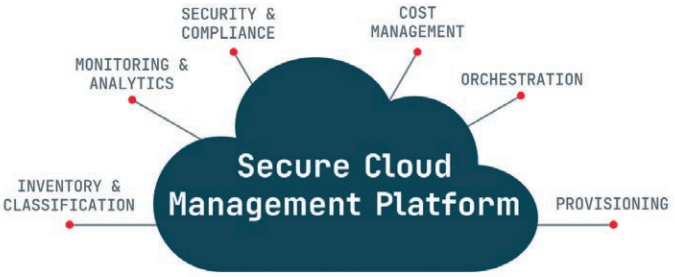
Leonardo has developed the **Secure Cloud Management Platform** to meet the increasing need to manage, orchestrate, protect and govern hybrid, multi-cloud and edge computing environments. The Secure Cloud Management Platform, implemented with a Secure by Design approach, plays an essential role in managing complex hybrid and multi-Cloud environments, where services provided by diverse Cloud Service Providers, and services deployed on Cloud, on premise, and in edge infrastructures, must coexist and cooperate. This integrated approach allows an overall visibility on the resources, simplifies their management and facilitates their optimisation within the infrastructure, thus enabling constant control over performance, quality of service provided and security. The Secure Cloud Management Platform also enables the use of *Confidential Computing* resources to ensure the protection of sensitive and critical data during the processing activities.

CONFIDENTIAL COMPUTING

Confidential Computing allows data and information to be processed within protected areas of memory and processor (enclaves) ensuring that data can only be accessed and viewed using code that is authorised for that specific purpose. In this way, the operating system, the hypervisor and untrusted code are not allowed to access the data, thus guaranteeing their protection.

SECURE CLOUD MANAGEMENT PLATFORM MODULES

The Secure Cloud Management Platform consists of several integrated modules that address all the aspects related to the management of hybrid or multi-cloud environments.



- **INVENTORY & CLASSIFICATION:** to identify and classify the resources available on the public and on premise clouds of the overall architecture. The resources are listed in a catalogue, inside the inventory of the Secure Cloud Management Platform, which enables their integrated management. Services classification according to their technical characteristics is also possible. This module allows to manage all the resources in a uniform way, regardless of the allocation of workloads, which may be on different Cloud Service Providers or on the organisation's on-premise private Cloud.

- **MONITORING & ANALYTICS:** to collect and visualize performance and *"capacity"* metrics relative to the resources detected by the INVENTORY & CLASSIFICATION module. Through graphs that allow the analysis of trends of the collected and historical parameters, it is possible to understand if and when it is necessary to optimise the use of resources. In addition, this module supports the decision-making process by providing a what-if analysis tool, which allows the simulation of possible scenarios to assess the impact of any changes in the capacity of the infrastructure, or the migration of workloads from one environment to another.

- **SECURITY & COMPLIANCE:** to centrally verify the compliance with regulations, standards, and best practices. The Secure Cloud Management Platform also integrates encryption services (Key Management System) that enable the implementation of encryption mechanisms external to the public Cloud provider (Bring Your Own Key or Hold Your Own Key).

- **COST MANAGEMENT:** to manage the costs related to Cloud Service Providers and analyse the cost related metrics for services detected by the INVENTORY & CLASSIFICATION module. The module allows the visualisation of current and past expenditures data, both aggregated and per asset. The what-if analysis makes it possible to evaluate expenditure trends by simulating the introduction of new resources provided by Cloud Service Providers, or the modification of the characteristics of services already available in order to optimize costs.

- **ORCHESTRATION:** to support the autonomous and standardised creation of a catalogue of complex Blueprints. It is possible to include Virtual machines, storage, Kubernetes clusters, network components and other elements that integrate infrastructure resources.

- **PROVISIONING:** to manage the *"provisioning"* of the resources included in the catalogue on the different Cloud services of the managed architecture. The module supports the mapping of the customised catalogue to service catalogues on both public and private Clouds. The customised catalogue, which is fully managed by the customer, allows resources to be selected and provisioned on the different environments constituting the hybrid Cloud or multi-Cloud architecture.

The complete visibility of all information related to the services managed through the Secure Cloud Management Platform is provided through dashboards displaying aggregate metrics, data related to individual assets, reports for the analysis of information, and indicators related to the services.

CLOUD MATURITY MODEL

The Cloud Maturity Model is a tool supporting a consolidated process that addresses evaluation and feasibility activities related to the Cloud migration for an organisation. Using this iterative model, Leonardo supports its Customers in the evaluation of their state of Cloud migration through the analysis of the infrastructure, the identification of specific performance, efficiency and security objectives, the definition of the expected and desired state of adoption, the analysis of current gaps and the identification and planning of the interventions to be implemented. The monitoring of Cloud migration activities is enabled by dashboards showing the progress of objective indicators for measuring and evaluating the achieved progress. Following the implementation of the identified interventions, the process is iterated to evaluate their effectiveness in order to identify further actions that can be implemented to guarantee that the Cloud migration process is in line with the organisation's objectives.

BENEFITS

- Integrated management of resources independently of Cloud Service Provider
- Integration with the major Cloud Service Providers and Cloud technology providers
- Availability of dashboards and reports showing aggregate metrics and individual assets data
- Possibility to simulate scenarios through what-if analysis to perform cost optimization
- Continuous monitoring of infrastructure performance and capacity
- Analysis and monitoring of costs related to aggregated services or individual asset
- Support for autonomous and standardised deployment of Blueprint catalogue
- Homogeneous control of infrastructure security posture
- Integration *of Bring your own key, Hold your own key and Confidential Computing* mechanisms
- Support in evaluating the best migration strategy to the Cloud

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

This publication is issued to provide outline information only and is supplied without liability for errors or omissions. No part of it may be reproduced or used unless authorised in writing. We reserve the right to modify or revise all or part of this document without notice.

2022 © Leonardo S.p.a.

MM09141 09-22