LEONARDO CYBER & SECURITY SOLUTIONS

SECURE PUBLIC CLOUD

LEONARDO'S SOLUTIONS FOR THE SOVEREIGN AND SECURE CLOUD

Technical paper

June 2024

the

INDEX

Leonardo's Secure Public Cloud solution is an innovative and cutting-edge platform that allows the services of the main public clouds to be used in a secure and sovereign way, ensuring the control and protection of organizations' sensitive data. With Leonardo's Secure Public Cloud solution, organizations can take advantage of the benefits of cloud computing, such as scalability, flexibility and efficiency, while addressing aspects such as security and regulatory compliance in an integrated way. The data remains under national jurisdiction at all times protected from access by third parties, such as foreign governments or companies.

The Secure Public Cloud solution offers a wide range of cloud services, such as compute, storage, networking, analytics, artificial intelligence and machine learning, integrated with Leonardo's cybersecurity solutions that enable the monitoring and prevention of cyber threats, the management of user identities and authorizations, encryption and secure data storage. In addition, Leonardo's Secure Public Cloud solution allows you to manage heterogeneous cloud environments, both public and private, in a simple and unified way, through a dedicated web portal that allows the selection of the cloud services that best suit your needs, the configuration and monitoring of cloud resources, and the migration of data and applications between different cloud environments.

Leonardo's Secure Public Cloud solution is the ideal answer for organizations that want to adopt cloud computing in a secure and sovereign way, safeguarding their strategic data and complying with current regulations.

SECURE PUBLIC CLOUD

The main functional features of Leonardo's Secure Public Cloud solution are:

- **Key management**: to manage encryption keys outside the Cloud Service Provider's control perimeter;
- **Governance Model**: to ensure security by policy/design by creating a segregated and self-consistent standard environment for each customer;
- **Confidential Computing**: to make it impossible for cloud provider operators to access the data in use, guaranteeing data sovereignty;
- **Hub & Spoke Solution**: to ensure that all network traffic can be controlled and monitored;
- **Back-up**: Ensure sovereignty over stored data by managing backups in the private cloud.

KEY MANAGEMENT

Cloud Key Management is a crucial component for ensuring the security of cryptographic data within cloud solutions. It allows you to manage the life cycle of

encryption keys (generation through certified cryptographic devices, backups, direct installation on cloud key vaults, access monitoring, periodic rotation and revocation) autonomously, securely and outside the availability of the Cloud Service Provider. Through the use of reliable third parties certified FIPS140-level 2, a high level of autonomy in the management of cryptographic keys is guaranteed, following both the Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) models. These templates allow you to maintain full control over cryptographic keys, allowing for flexible and customized deployment. The key management solution makes it possible to replicate cryptographic data in two high-reliability data centers located in two distinct regions throughout the country, ensuring maximum availability and redundancy.

The solution allows organizations to maintain complete and transparent control over their cryptographic keys, ensuring a higher level of security and compliance.

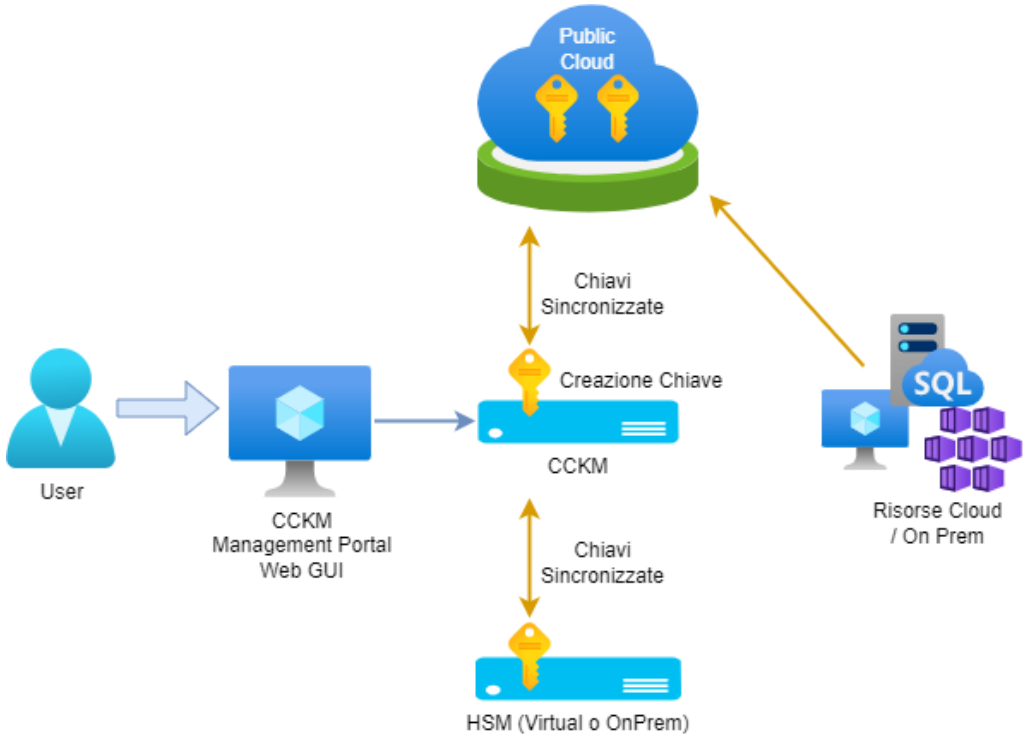

Figure 1 - Key Management Reference Architecture

GOVERNANCE MODEL

The governance model provides a structured and highly secure approach to managing customer environments within the Secure Public Cloud. For each client, a segregated

and self-consistent standard environment is created, allowing for effective and personalized management.

By using privilege delegation services such as Policy Manager and Privileged Identity Management, you can manage the customer's environment's specific monitoring and security services to the manager's environment, providing complete visibility, large-scale automated intervention, and enforcement of defined policies.

Administrative privileges, disabled by default, are assigned to operators only after a rigorous authorization process: this approach guarantees a high level of security and mutual control between customer and provider.

Features of the management model include:

- uniform and standardised management of client tenants;
- the creation, deployment and automatic updating of predefined sets of security rules in line with international best practices;
- the definition of standard roles for each function;
- the availability of secure templates integrated with security tools;
- unified identity management;
- Security event management.

Thanks to this integrated and comprehensive approach, it is possible to create a secure cloud environment that meets the specific needs of our customers.

CONFIDENTIAL COMPUTING

Confidential Computing is a fundamental pillar for strengthening data confidentiality and security; in the proposed solution it is applied at the level of virtual machines (VMs), Kubernetes clusters (K8S) or Hardware Security modules (HSMs for the protection of cryptographic keys) and implemented using hardware-based trusted execution environments. Technologies such as AMD SEV or Intel Software Guard Extension (SGX) enable you to create secure enclaves within which applications can perform operations on sensitive data in a secure, isolated environment. The use of confidential computing minimizes so-called Trusted Compute Bases (TCBs) on the hardware, software, and operational planes, thus ensuring greater security and reducing potential vulnerabilities. The adoption of enforcement techniques based on technological components such as hardened operating systems rather than on organizational processes, also ensures robust protection of sensitive data. The solution adopted, through remote attestation services, offers transparency on residual risks and mitigations that can be implemented, allowing customers to make informed decisions about the security of their data. For example, the use of Trusted Platform Module (TPM) technology allows you to verify that the software used by a specific system is in a *trusted* state before performing operations that impact sensitive data and information.

The attack patterns that can impact cloud-based applications can vary and use different techniques to target infrastructure or data: consequently, the approach

adopted for Confidential Computing addresses different areas of vulnerability such as hypervisor and container breakout, firmware compromise or other insider threats, which require specific defense strategies.

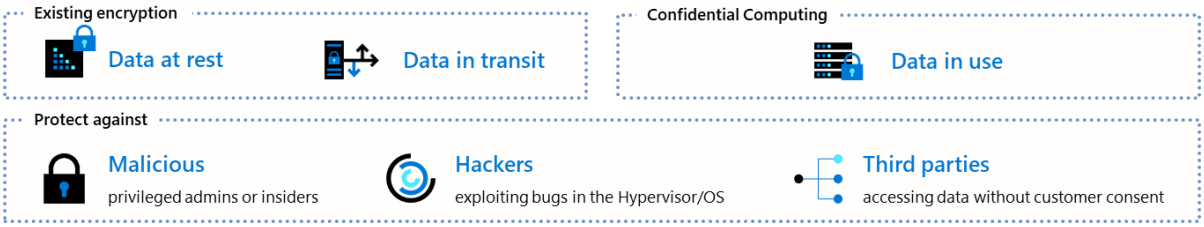

Figure 2 – Confidential computing solution

HUB & SPOKE SOLUTION

To ensure a secure and controlled environment in the Secure Public Cloud, a Hub & Spoke model has been developed that allows the implemented framework to exercise traffic control and management of DMZs within the cloud environment. The customer has the option to create "spoke" virtual networks within the segments, where specific policies are activated that govern the connection with the Virtual Network Hub. This approach allows you to centralize control and prevent the creation of resources that are not centrally controlled, such as public IP addresses, thus helping to maintain a secure cloud environment that complies with the security needs of your organizations.

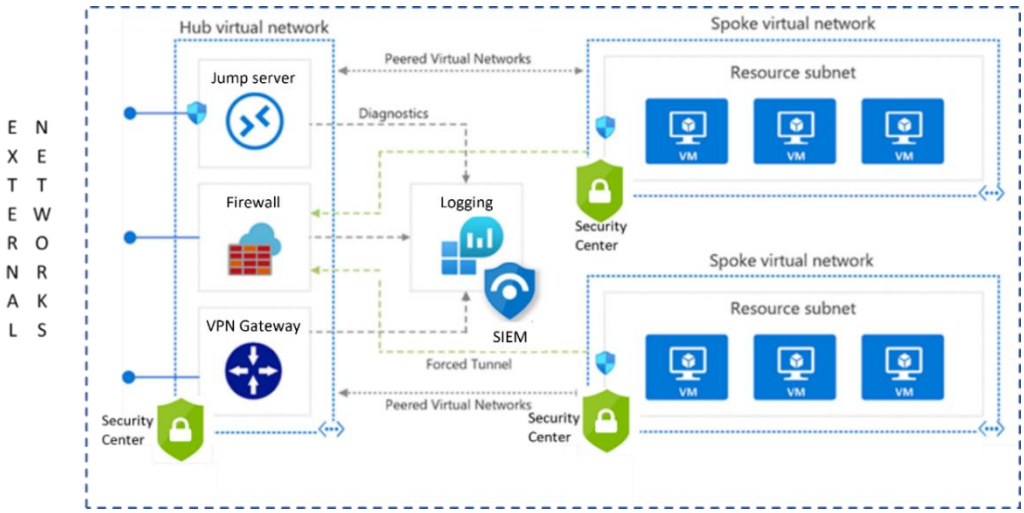

Figure 3 – Hub & Spoke Solution

BACK-UP SOVEREIGNTY

In the context of the Secure Public Cloud, ensuring data sovereignty is paramount. To this end, an independent copy of the data is available, outside the services provided by the Cloud Service Provider (CSP), through the implementation of an additional layer of storage on Leonardo's or the customer's private datacenters. This service, integrated with the resources in the Public Cloud, is made possible through Backup-as-a-Service

and ensures that the storage containing the protected data is under the control of Leonardo personnel or the customer.

The service involves the use of snapshot or stream-based backup techniques, ensuring the recovery and recovery of the virtual machines involved. Encryption of data at rest and in transit is applied to provide an additional layer of security, even for virtual machines that already implement disk encryption mechanisms. This approach ensures that customer data is protected at every stage, enabling reliable recovery when needed, and providing greater peace of mind and control for Secure Public Cloud users.

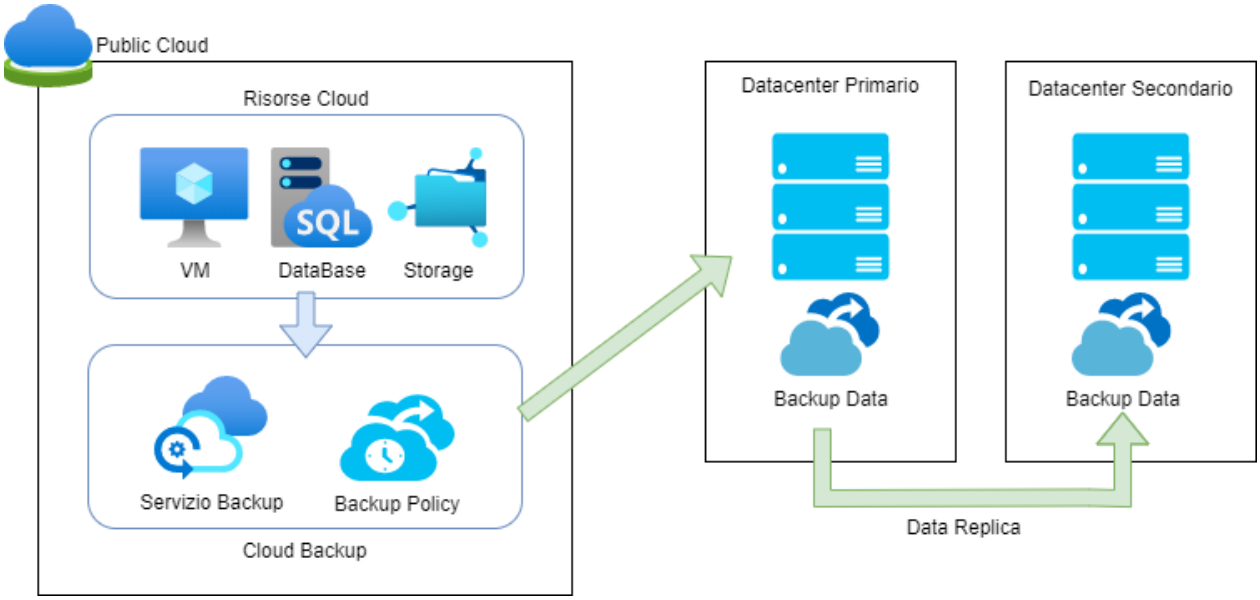

Figure 4 – Reference architecture backup

REFERENCE ARCHITECTURE

The reference architecture of the proposition is shown in Figure 5 where a Secure Public Cloud environment – in this case Microsoft Azure – is represented connected to an on-premises environment via Azure Express Route that offers a fast, secure and dedicated connection.

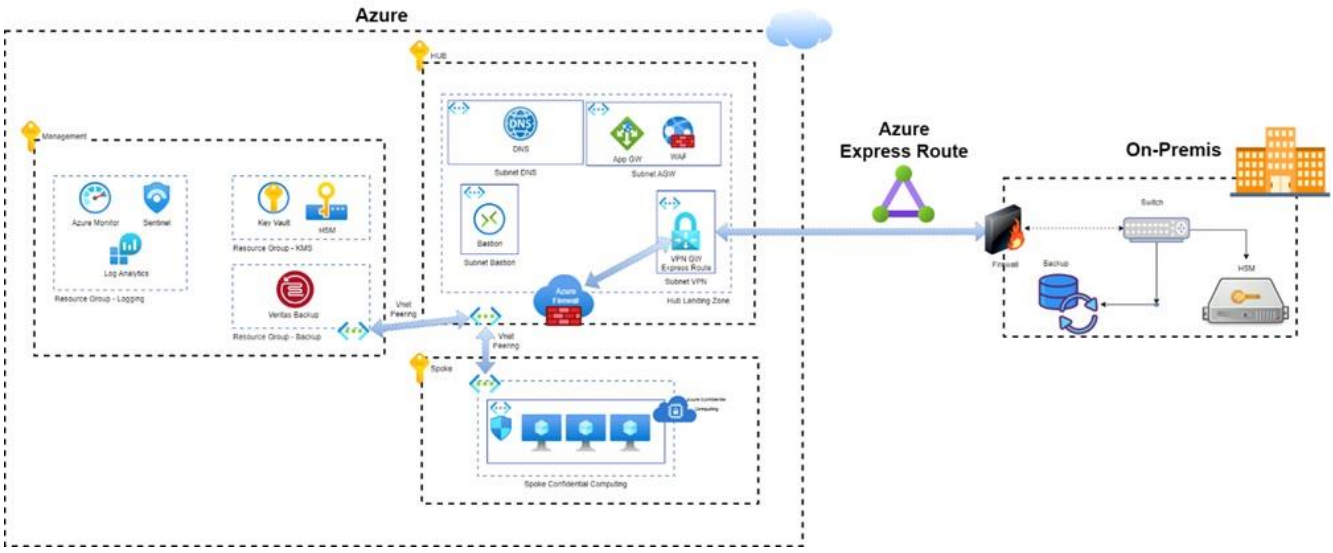

Figure 5 - Hybrid Azure environment

The Secure Public Cloud environment is structured through a Hub&Spoke model, consisting of several subscriptions. One of the spokes hosts IaaS services, i.e. virtual machines (but can also include PaaS, CaaS, and SaaS services).

The "Hub" is dedicated to connectivity modules, with WAF/Application Gateway services acting as an entry point for public connections from the outside, such as access to an application exposed to the Internet through the Web Firewall. In addition, the "Hub" is equipped with the Bastion service, which is used for private and secure management of virtual machines.

The "Management" spoke hosts central services such as backup, monitoring, log collection and SIEM, for monitoring events, such as accesses or any critical events, and creating alerts.

Spokes communicate with each other via Virtual Networks, with the ability to restrict traffic by using network security groups to create separate, protected islands.

Spoke management and permissions are managed through the use of security groups and role-based access. Resources such as IaaS, PaaS, etc. can be logically divided into resource groups for more efficient and secure management.

The on-premise environment and the cloud environment are integrated through dedicated connectivity, allowing two-way communication of resources between the two environments. The connection of the two environments also allows cloud resources to be backed up to the on-premises environment in order to comply with data sovereignty requirements. Cloud resources can securely access and use the keys managed by the on-premise HSM, bringing a higher level of security to the solution, since the keys to decrypt data on the cloud are not stored within the cloud provider.

SECURE CLOUD MANAGEMENT PLATFORM

The Secure Cloud Management Platform (CMP), implemented with a Secure by Design approach, provides tools and capabilities to securely manage resources within the Secure Public Cloud environment. The platform also allows the management of a hybrid environment where private components (on premises) and components hosted on public clouds coexist. The platform provides tools that implement resource provisioning, operations automation, performance and security monitoring, or access management. The CMP allows the use of Confidential Computing resources to ensure the protection of sensitive or critical data and information during their processing.

The Secure Cloud Management Platform consists of integrated modules, such as:

- **Inventory & Classification**: allows the discovery of resources present on public and on-premise clouds that make up the overall architecture. Within the Secure Cloud Management Platform inventory, a catalog that contains resources enables integrated asset management. In addition, the Inventory & Classification module allows the classification of each service according to its technical characteristics. An appropriate dashboard allows for an aggregated view of the information being managed.
- **Monitoring & Analytics**: collects performance and capacity metrics from the services detected by the Inventory and Classification module. Through graphs that allow you to analyze the trend of the collected and stored data, it is possible to have evidence of situations in which it is necessary to optimize the use of resources.
- **Security & Compliance**: Allows you to verify the compliance of resources with defined policies. The Secure Cloud Management Platform also integrates encryption services (Key Management System) that allow you to implement encryption mechanisms external to the public Cloud provider (Bring Your Own Key or Hold Your Own Key).
- **Cost Management**: supports the management of costs related to Cloud Service Providers and the examination of metrics related to the costs of services detected by the inventory and classification module. The module allows the visualization of the expense graphs for each asset of the CMP in order to analyze the historical trend. The what-if analysis makes it possible to evaluate the trend of expenditure by simulating the inclusion of new resources provided by Cloud Service Providers within the infrastructure or the modification of the characteristics of the services already present to minimize costs.
- **Provisioning**: allows the management of the "provisioning" of the resources provided in the catalog on the various Cloud services of the managed architecture. The module supports custom catalog mapping to service catalogs on both public and private clouds.
- **Orchestration**: supports the construction, in an autonomous and standardized way, of a catalog of even complex Blueprints by inserting and managing virtual machines, storage, Kubernetes clusters, network components and other elements that integrate infrastructure resources.

LEONARDO CYBER & SECURITY SOLUTIONS

LEONARDO

leonardo.com