EXTENDED DETECTION & RESPONSE

Cloud Security

HOW CAN TELEFÓNICA TECH HELP?

Migrate to the cloud confidently with a security solution designed to protect your company's assets and applications throughout their lifecycle

The digital transformation of businesses is closely linked to the adoption of the public cloud,
which introduces a new paradigm of shared responsibility with providers (CSPs) and new security challenges.

According to Gartner, 95% of security issues in the cloud are customer generated.
The radical change in the provision of services based on programmatic interfaces, the lack of visibility of workloads uploaded to the cloud or the Agile methodologies and DevOps practices associated with the cloud, where security often takes a back seat, make it quite easy to expose the cloud infrastructure for security issues such as configuration errors.

Telefónica Tech's Cloud Security is a security solution designed to identify, assess, and manage all cloud challenges and threats in a comprehensive way. Companies need to protect workloads throughout their entire lifecycle, from the coding and CI/CD phases to the execution phase, when they are deployed in the cloud. The concept of "shift-left security" emerges, allowing organizations to build applications securely without losing agility.

WHO IS THIS SERVICE FOR?

Organizations in public cloud (AWS, Azure, GCP, OCI, Alicloud) or hybrid cloud, concerned about lack of visibility, control, and governance in cloud and DevOps processes.

Customers who want a recurring service that implements a continuous assessment of security in the cloud.

Organizations that have a relevant volume of public and/or private cloud assets in their IaaS and PaaS modalities.

OUR VALUE PROPOSITION

Our service

Telefónica Tech's Managed Cloud Security service aims to return control of public and hybrid cloud security to CISOs and security managers through capabilities that protect assets and applications throughout their lifecycle.

The service is based on cloud-native security technologies such as CNAPP (Cloud Native Application Protection Platform). Beyond the technology, the service offers a set of processes and deliverables that will allow our customers to have a high-level view of cloud security based on KPIs and see its evolution based on continuous improvement.

What does it allow you to do?

This service will allow you to have the following capabilities:

› **Posture Governance capability:** for visibility and governance of assets deployed in the cloud. This capability provides a continuous security assessment according to a policy framework adapted to the customer's context.

› **Monitoring capability:** runtime protection of workloads running applications. Detection of suspicious activity such as Malware & cryptomining or communication with disreputable IPs. A 24/7 triage and alert handling.

› **Shift-left capability:** workload bastioning, vulnerability scanning, and best practices on compute workloads deployed in the cloud.

› **Workload Super-Vision capability:** this capability moves security controls to the left: to the development and CI/CD phases. It includes scanning of container logs, code repositories or CI, among other functionalities.

Benefits

Dynamics of deliverables

Our service regularly delivers reports with breaches and vulnerabilities of the cloud infrastructure and applications throughout their lifecycle. These reports are followed by an action plan to solve the most relevant breaches. Additionally, high-level indicators are included that will allow to see the state of security, its evolution and help determine the action plan, in order to continuously improve security and promote a cultural change in the company.

24/7 Monitoring

24/7 monitoring is included for security alerts that require proactive treatment. Alerts will be triaged, discarding false positives, and including recommendations for remediation, in case the threat is confirmed.

The service is more than a security tool.

Forget about managing complex cloud security platforms. The service offers a high-level view based on KPIs that allows you to monitor cloud security and see the evolution based on continuous improvement.

Telefónica Tech's differential value

Our team is responsible for the delivery and configuration of the CNAPP platform used by the service, providing close guidance and support throughout the deployment and operation process.

Our Cloud Security team is focused on cloud security and integrated into the iSOC.

Cloud Security is a customized service that adapts to the customer's context, both in terms of controls and policies configuration and remediation actions.

EQUIPMENT, TEAMS, AND ACHIEVEMENTS

Our teams

› **+1.800** SecOps employees

› **+1.500** security certifications.

› **+30** Cloud MSS analysts.

Achievements

› A broad spectrum of references makes us **one of the leading MSSPs in the cloud.**

› Our main customers include several **Ibex 35 companies.**

› **Cloud MSSP Partner certified** by the main cloud security manufacturers.

BUSINESS MODEL

It is a service that offers an annual subscription which includes everything necessary to secure both the public and private cloud and DevOps processes.

The price is based on the number of workloads or assets protected. The service has three different modalities that include the different capabilities of the service:

› **Governance** modality: includes the Posture Governance capability.

› **Defense** modality: includes Monitoring, Workload Super-Vision, and Shift-left Security capabilities.

› **Advanced** modality: combines the capabilities of Cloud MSS Governance and Cloud MSS Defense.

RELATED PARTNERS

paloalto
NETWORKS

RELATED SERVICES

SIEM Management

24/7 monitoring and correlation of security events with alerts and incident management, providing a solid foundation in security threat detection.

Contact us to start the digital transformation of your organization.