pyxis

Cloud Security Services

SERVICE PROPOSAL

Pyxis Cloud Security Services

We analyze, design, and join your IT and Compliance teams to optimize the security of your Cloud. Currently, in Cloud environments, providers comply with various security standards that apply to their data centers, leaving the responsibility to their clients to a greater or lesser extent for the final security configurations and data protection. It is necessary to have strategies and tools to minimize the vulnerability of your information in the cloud. Secure your Cloud environment and deploy solutions reliably and easily.

The services that make up the Cloud Security Services suite are described below:

Cloud Security Approach (CSA) - 2 months Assessment

This service proposes a critical look at the infrastructure and services deployed in the Cloud, as well as a vision with the premises of Security by Default and Zero Trust for new solutions. Through the CSA, opportunities for improvement related to the client's infrastructure are identified and weighed, recommending a design that complies with good practices and updated security standards.

Cloud Security Posture (CSP) - 2 months Assessment (Powered by Guayoyo)

The service focuses on identifying vulnerabilities through Cloud infrastructure misconfigurations regardless of whether your cloud is public or private. The CSP measures compliance against CIS Benchmarks, alerts teams to problems, and recommends a Solution.

Cloud Security Deployment (CSD) - 4 months Implementation

The result of the CSA on the state of security of the infrastructure and the possible threats that may compromise it will be the input to implement cybersecurity solutions at different points and with different approaches (offensive or defensive), which allow the client to mitigate the risks for their organization.

Cloud Security Compliance (CSC) - 4 months Implementation

Today the corporate environment often requires compliance with different standards to comply with regulations on the business they develop, for example, PCI-DSS, HIPAA, and SOX. These requirements are focused on the protection of information assets, so it is necessary to add an additional specific analysis to good cloud security practices. CSC allows explicit confirmation of compliance with the norm or standard through the execution of tests on the solutions to be certified.

Cloud Security Score Improvement (CSSI) - 6 months Implementation

Strategic evolutive maintenance service on Cloud solutions. It allows incorporating new services and technologies under a controlled and stable process that improves security features. In this way, it is possible to improve the score of the Cloud environment and maintain it over time, with the support of security experts.

Microsoft Partner

Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Cloud Security Services

Powered By:

More Information:
www.pyxis.com.uy/cloud-security

View in:
Azure Marketplace

Pyxis Cloud Security Approach

It is currently important and increasingly necessary to follow and implement the good practices of security in Information Technology, particularly for cloud environments, providers comply with various security standards that apply to their data centers, although they leave the responsibility to their clients to a greater or lesser extent on the final security configurations.

Also, it is a common practice that the cloud approach of many companies follow the guidelines of the business, without considering the security from the early stages of defining architecture and infrastructure. As a more immediate consequence, a very high percentage of the incidents of security happens due to poor service configurations or with their default values.

Cloud Security Approach proposes a mandatory look at the infrastructure and services deployed in the Cloud, as well as a vision with the premises of Security by Default and Zero Trust for new solutions. Through the CSA, opportunities for improvement related to the client's infrastructure are identified and weighed, recommending a design that complies with good practices and updated security standards.

The phases that make up the CSA are described below:

1.- Current Situation Assessment

A starting point to know the reality of the client, understand the needs and challenges that the client's infrastructure currently has, as well as the new requirements and improvement options that it hopes to obtain. In this way, we work together on definitions of the new Cloud solutions that best suit the business.

2.- Safe Infraestracture Design

Cloud infrastructure development brings with it a set of practices and ways of working that are not fully comparable or equivalent to on-premise scenarios. Therefore, it is necessary to understand how the current reality of the client adapts to a Cloud environment. New forms of access will be considered, identity management, and other aspects that make up the design of information security in the Cloud.

This is the main phase of the CSA, where the design that best suits the client's needs is defined, considering and prioritizing security according to the best practices and experiences in the area.

3.- Improvement Recommendations

After achieving a design according to the client, the recommendations for improvement will be presented, emphasizing the benefits that will be obtained with the new infrastructure, the considerations that must be taken into account, and other changes that the new configuration may imply .

4.- Accompaniment in the Implementation Strategy

We trust that this phase will generate the most important added value for the client, where the guidelines suggested in the previous phases will be followed, a new stable and reliable solution will be achieved with the security guarantees that have been agreed upon.

We join the client in these first steps, advising and clearing up any doubts that may arise during the implementation stage.

Microsoft Partner

Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Cloud Security Approach

Powered By:

More Information:
www.pyxis.com.uy/cloud-security

View in:
Azure Marketplace

Cloud Security
Posture

pyxis

Pyxis Cloud Security Posture

Detect and fix security breaches in your Cloud infrastructure

The security posture of a cloud solution refers to the state and measures to protect it from cyber threats. Although cloud environments have established themselves as versatile solutions, they are difficult to protect due to their wide attack surface and range of threats.

Configuration vulnerabilities in Cloud environments are one of the most common errors that lead to data breaches and non-compliance issues.

Cloud Security Posture (CSP) focuses on identifying vulnerabilities through cloud infrastructure misconfigurations regardless of whether your cloud is public or private, measures compliance against CIS Benchmarks, warns teams of issues, and recommends a solution.

This is accomplished by examining and comparing the cloud environment against a defined set of security tests, best practices, and known risks to identify security issues for remediation.

CSP can be purchased as part of CSS or separately to kick start a technical review and security upgrade of your cloud solution.

Benefits

- Provides security visibility
- Help with regulatory compliance and good practices
- Prevents exposure to risk
- Drives remedial response

Microsoft Partner

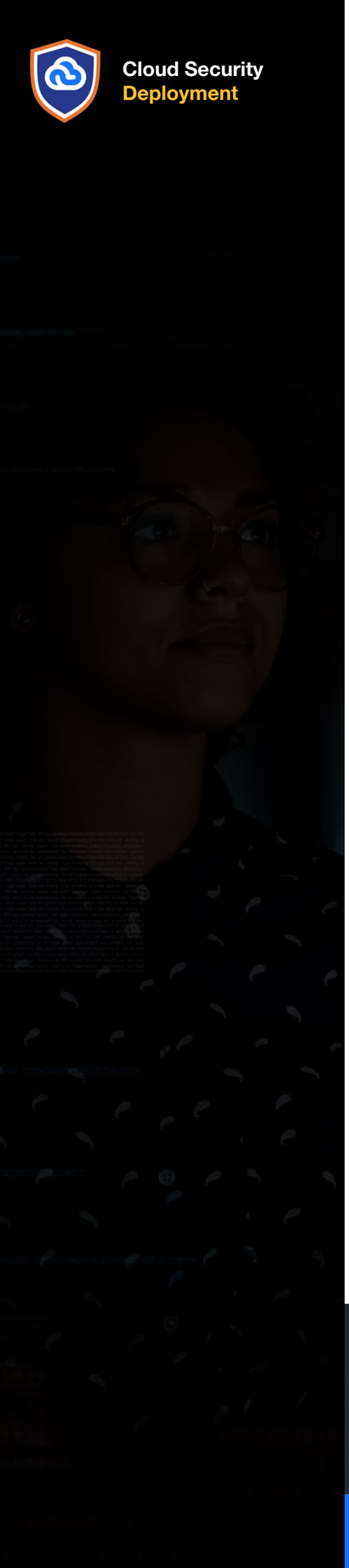
Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Powered By:

View in:
Azure Marketplace

More Information:
www.pyxis.com.uy/cloud-security

Cloud Security
Deployment



pyxis

Pyxis Cloud Security Deployment

Cloud Security Deployment (CSD) is the most convenient value proposition for cloud onboarding. CSD is the way forward to implement the security and workload architectures that emerge from the included assessment and analysis.

We consider the following phases of work in this initiative:

1.- Assessment
The Cloud Security Approach is included as an initial phase. This proposes a mandatory look at the infrastructure and services deployed in the Cloud and a vision with the premises of Security by Default and Zero Trust for new solutions.
Through the CSA, opportunities for improvement related to the client's infrastructure are identified and weighed, recommending a design that complies with good practices and updated security standards.

2.- Design
The result of the CSA on the security status of the infrastructure and the possible threats that may compromise it, will be the input to implement cybersecurity solutions at different points and with different approaches (offensive or defensive), which allow the client to mitigate the risks for their organization. In this stage, the proposed architectures are validated and the implementation design is generated, considering each environment's particularities, considering migration modalities, budget, collaborative work, and methodologies, among others

3.- Implementation
Once the design is defined in this instance, the solutions are implemented in the Cloud. This phase consists of instantiating and creating Cloud services to form the proposed security infrastructure. .

4.- Validation
After the defined infrastructure has been implemented, an instance of validation of configurations, services, accesses, processes, and communication flows is executed, ensuring the reliability and effectiveness of the final solution.

Microsoft Partner

Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Powered By:

View in:
Azure Marketplace

More Information:
www.pyxis.com.uy/cloud-security

Cloud Security
Compliance

pyxis

Pyxis Cloud Security Compliance

Today the corporate environment often requires quality depth and different standards to comply with regulations on the business they develop, for example, PCI-DSS, HIPAA, and SOX. These requirements are focused on the protection of information assets, so it is necessary to add an additional specific analysis to good cloud security practices.

The Compliance service (CSC) includes Approach (CSA) and Deployment (CSD) services and complements them from the beginning considering compliance with the standard that the client requires.

CSC allows explicit confirmation of compliance with the norm or standard through the execution of tests on the solutions to be certified.

- Cloud Security Approach
- Cloud Security Deployment

The phases of the Compliance services are described below :

Scope and Standard
The first phase that must be established is the required regulatory framework (standard to be met) and the scope that it will have in the customer's new Cloud infrastructure. Compliance is generally applied to information assets in relation to the standard that is followed, therefore in this phase the scope of compliance of the solutions to be deployed in the new infrastructure must be agreed upon with the customer.

Compliance
The second phase of this service is the empirical confirmation of compliance with the standard, in the implemented infrastructure with the operational solutions. For this, configuration check activities, accesses, and important procedures for the audit processes will be carried out.

Microsoft Partner

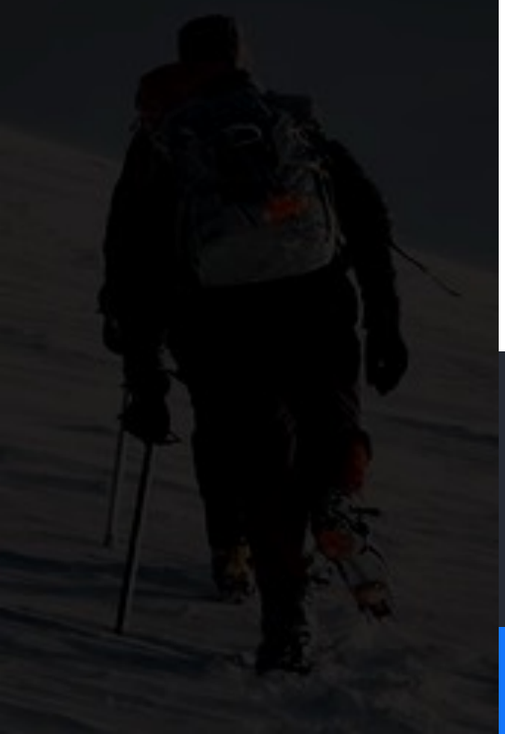
Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Powered By:

View in:
Azure Marketplace

More Information:
www.pyxis.com.uy/cloud-security

Cloud Security
Score Improvement



pyxis

Pyxis Cloud Security Score Improvement

One of the main challenges that customers face in cloud infrastructures is governance. Cloud providers are constantly updating and releasing new products. In turn, organizations take advantage of the virtues of these environments to achieve more dynamics and agility in the acquisition and deployment of new technological solutions to support the business.

This leads to a reality of permanent change, and in this scenario, having control of the assets and their status is a very complex task. To attack this problem, there are different frameworks where their score and posture are defined as a way of evaluating each Cloud environment and identifying levels of maturity in which organizations are found.

Cloud Security Score Improvement is a strategic evolutive maintenance service on Cloud solutions. It allows the incorporation of new services and technologies under a controlled and stable process that improves security features.

In this way, it is possible to improve the score of the Cloud environment and maintain it over time, with the support of security experts.

We offer the CSSI as part of the CSS, to give an holistic and complete view of the Cloud infrastructure of the organization after the assessment (CSA) and implementation (CSD).

The CSSI can be acquired independently, offering advice based on good practices, improving the organization Score in its Cloud.

Microsoft Partner

Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Powered By:

View in:
Azure Marketplace

More Information:
www.pyxis.com.uy/cloud-security