Title: Cloud Guard Assessment – Zero Trust Lens

In today's dynamic digital landscape, the imperative to perform cloud security assessments arises from the pressing need to bolster defences against evolving cyber threats. The increasing adoption of zero-trust frameworks underscores the criticality of re-evaluating traditional security models, necessitating a comprehensive understanding of potential vulnerabilities within cloud environments. Furthermore, organizations grapple with the challenge of seamlessly integrating and leveraging existing security solutions to fortify their cloud infrastructure. As technology evolves, the imperative to conduct thorough cloud security assessments becomes paramount in safeguarding sensitive data and ensuring a resilient defence against a spectrum of cyber risks.

Persistent System recognizes the challenges faced by businesses in safeguarding their assets across diverse cloud platforms, often leading to fragmented security measures, compliance gaps, and increased vulnerability. The need of the hour is a comprehensive **Multi-Cloud Security Assessment** solution that not only identifies risks but also leverages existing security solutions to fortify cloud environments.

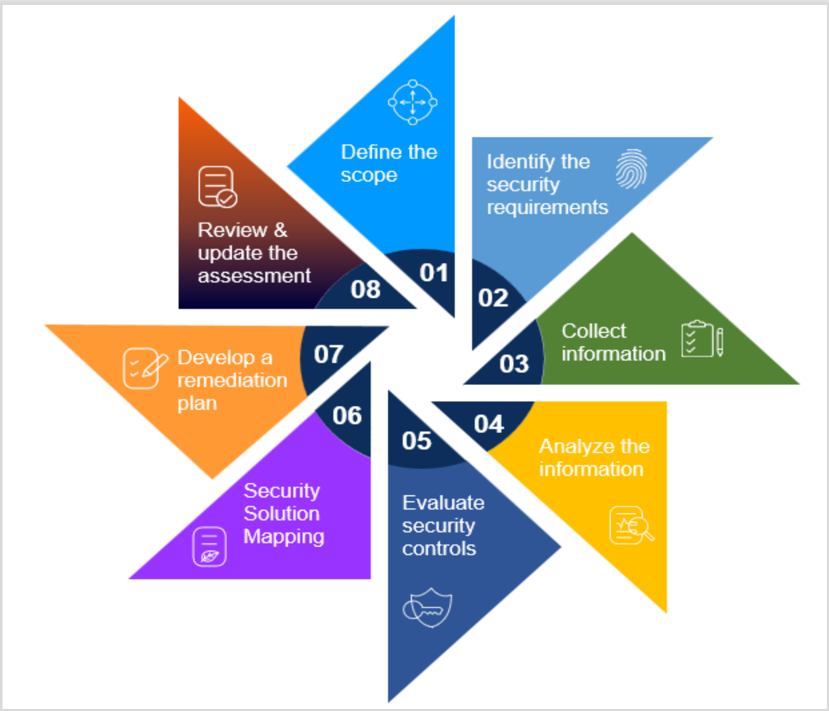
Persistent System's Cloud Security Assessment provides a comprehensive evaluation of your organization's multi-cloud environment, identifying potential security risks and vulnerabilities and recommending effective mitigation strategies. Our team of experienced cloud security experts will assess the following:

- **Multi-cloud Complexity:**
  Factor in the number of cloud providers involved. Assessing security across multiple cloud platforms and considering the interoperability challenges between different cloud environments.
- **Zero Trust Architecture:**
  Evaluate the complexity of implementing and assessing zero trust principles in the cloud environment. Determine the extent of zero trust architecture implementation, such as micro-segmentation, continuous monitoring, and identity-centric security.
- **Scope of Assessment:**
  Clearly define the scope of the assessment, specifying the assets, services, and configurations to be included across all cloud providers.
  Include the assessment of identity and access management, network security, data protection, and compliance with zero trust principles.
- **Assessment Depth:**
  Consider the depth of the assessment, including a detailed examination of security controls, policies, and configurations.
  Assess the depth of Security architecture, vulnerability scanning, and configuration reviews.
- **Expertise and Tools:**
  Ensure that the assessment team possesses expertise in multi-cloud environments and zero-trust architectures.
  Identify and budget for any specialized tools or technologies needed for assessing multi-cloud and zero-trust security.
- **Documentation and Reporting:**
  Plan for detailed documentation of findings related to multi-cloud and zero trust security.
  Include the preparation of comprehensive reports with actionable recommendations.
- **Collaboration and Communication:**

Account for time spent on collaboration with stakeholders from different cloud environments. Plan for communication efforts to ensure all relevant parties are informed and aligned.

- **Continuous Monitoring:**
  If ongoing monitoring is part of the assessment (as is often the case with zero trust), incorporate costs for continuous monitoring tools and services.
- **Regulatory Compliance:**
  If there are specific regulatory requirements for multi-cloud and zero trust, factor in additional efforts to ensure compliance.
- **Training and Awareness:**
  Consider any necessary training or awareness programs for staff involved in maintaining multi-cloud and zero-trust security.
- **Leverage Existing Security Solutions:**
  Seamlessly integrate with and leverage existing security solutions deployed by the customer, ensuring a unified security posture.
- **Customization and Flexibility:**
  Be prepared to customize the assessment based on the unique requirements and priorities of the organization.

Assessment Methodology Representation


01
Define the scope
02
Identify the security requirements
03
Collect information
04
Analyze the information
05
Evaluate security controls
06
Security Solution Mapping
07
Develop a remediation plan
08
Review & update the assessment

Unique Differentiators:

- **Unified Zero Trust Framework:**

Provide a unified Zero Trust framework that spans across public cloud providers. Ensure a consistent security posture, regardless of the complexity of the multi-cloud environment.

- **Comprehensive approach:**

We assess all aspects of cloud security, from asset discovery and vulnerability scanning to threat analysis and zero trust adoption.

- **Security solution mapping**

Post assessment and gap analysis we will perform the security solution mapping based on existing or current security solutions and required security solutions with the appropriate priorities with respect to Zero Trust Framework adoption.

- **Multi-cloud expertise:**

Our team has extensive experience in assessing and securing cloud environments across all major cloud providers.

- **Actionable recommendations:**

We provide clear and actionable recommendations to help you remediate identified risks and improve your overall cloud security posture.

Deliverables:

- **Comprehensive Assessment Report:**

Detailed findings: Identifies vulnerabilities, misconfigurations, compliance gaps, and potential risks.
Risk prioritization: Ranks risks based on severity and likelihood of exploitation.
Remediation recommendations: Provides clear, actionable steps to address identified issues.

Microsoft security solutions:

Microsoft Defender for Cloud: Centralized security management for multi-cloud and hybrid environments.
Azure Security Centre: Comprehensive security posture management for Azure workloads.
Azure Sentinel: Cloud-native SIEM for threat detection and response.

- **Executive Summary:**

Concise overview: Summarizes key findings and recommendations for senior management.
Business impact: Highlights potential business risks and implications.
Compliance alignment: Outlines compliance status with relevant regulations (e.g., GDPR, HIPAA).

- **Remediation Plan:**

Prioritized action items: Specific steps to address security issues, sequenced for the most effective risk reduction.
Resource allocation: Identifies resources needed for remediation, including personnel, tools, and time.

- **Ongoing Security Monitoring and Recommendations:**

Continuous assessment: Outlines strategies for continuous monitoring and assessment of cloud security posture.
Security best practices: Provides guidance on best practices for cloud security configuration and management.

Microsoft security solutions:
Azure Security Canter recommendations: Continuously evaluates security posture and provides actionable recommendations.
Microsoft Defender for Cloud Alerts: Real-time alerts for potential threats and anomalies.

- **Solution Mapping to Adopt Zero Trust Framework:**

Leverage existing security solutions to optimize costs while introducing a novel cost-effective solution to enhance overall security posture.

Remember: These deliverables can vary depending on the scope and depth of the assessment, as well as specific organizational requirements.

Pricing and Availability

Basic Cloud Security Assessment:
Scope: Public Cloud Environment
Duration and Frequency - Approx. 4 weeks || One time
Depth: Cloud environment Security configuration review, Security architecture Review
Complexity: Single-region setup.
Compliance: No specific compliance.
Reporting: **Standard report** with Solution mapping and heat-map analysis.
Estimate: $30K+

Comprehensive Cloud Security Assessment:
Scope: Multi-cloud environment
Duration and Frequency - Approx. 8 weeks || One time
Depth: Detailed Architecture review, Cloud Native and 3rd Party security solution configuration review, process review, penetration testing of max.10 IPs.
Complexity: Hybrid architecture.
Compliance: industry-specific requirements like CSA, and Solution mapping based on Zero trust framework.
Reporting: Customized and detailed reports.
Estimate: $75K-90K+

Note- The above cost does not include any travel and taxes. The actual cost can vary based on requirements and defined scope.

Contact Information:

For inquiries and consultations, please
contact Samir_paul@persistent.com or kumar_sambhav@persistent.com. We look forward to assisting you in fortifying your multi-cloud security and Zero Trust initiatives.