GUIDEPOINT
SECURITY

[CLIENT LONG NAME]

Azure Health Check

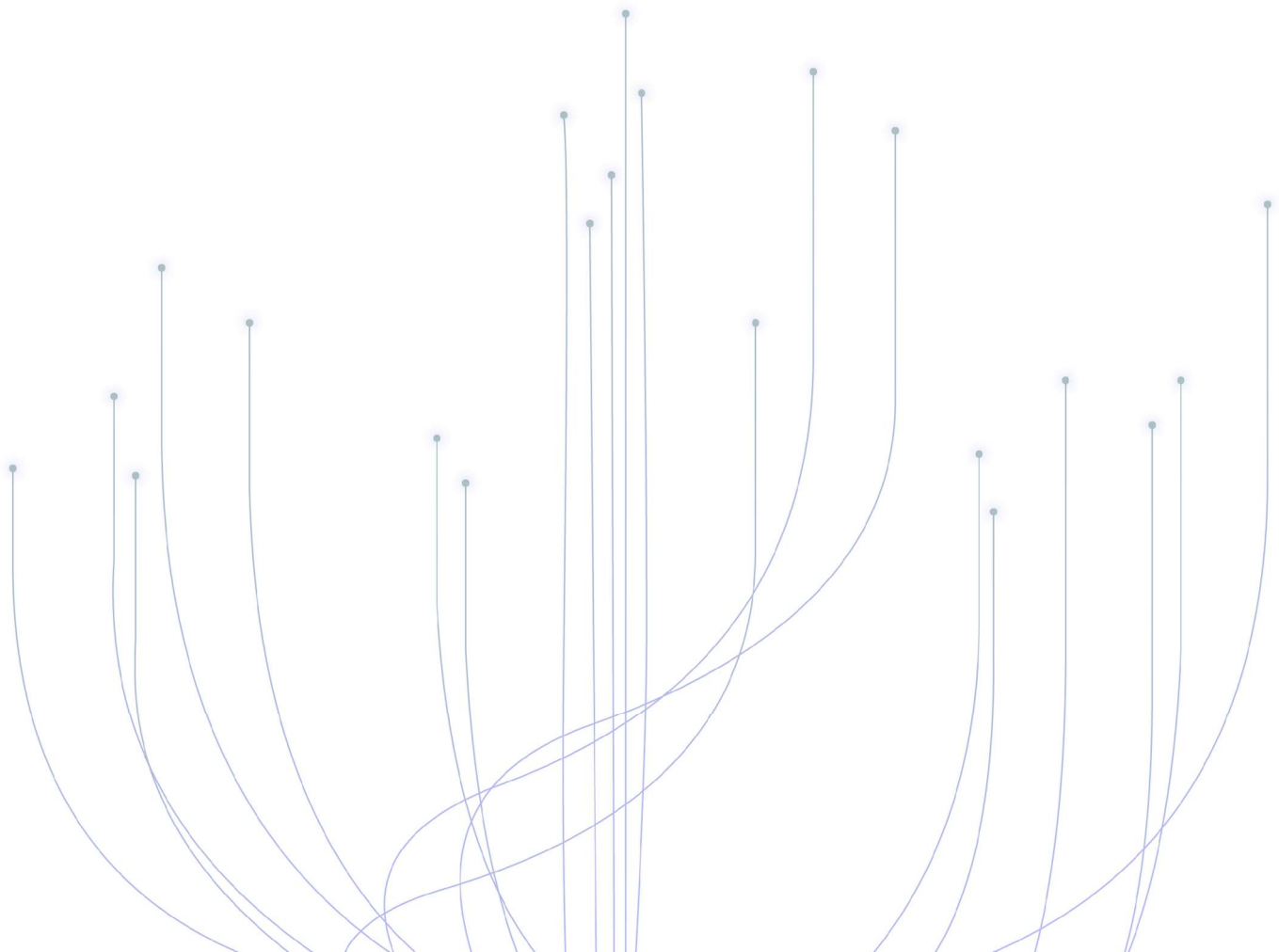
MONTH, 2026

Version 0.1

Executive Summary

PROJECT DEFINITION AND SCOPE OVERVIEW

<Client> (“<Client>”) engaged GuidePoint Security, LLC (“GuidePoint”) to review the Azure environment and identify configuration components that require improvement or do not meet security best practices. This Azure Security Assessment evaluates <Client>’s environment in accordance with pre-defined best practices within the industry while also providing recommendations and action items to <Client> for remediation where necessary. The scope of this assessment included the <Client>’s Azure environment hosted in Microsoft’s Cloud. The point in time assessment was conducted between [Date], and [Date]. GuidePoint was assigned the Global Reader role within Azure AD and the Reader role at the subscription level in order to perform a manual assessment of resource and service configurations, leveraging PowerShell when audit procedure allowed.



CONTROL AND FINDINGS CRITICALITY DEFINITIONS

In order to clearly communicate the security posture of the environment within the diverse nature of public cloud architectures, GuidePoint represents the information using two (2) categories.

CONTROLS

Information Security has well established standards; however, the known standards were written for data centers that do not have the same rate of service expansion or shared responsibilities as the public cloud provides. GuidePoint Security has aligned with the Cloud Security Alliance's Cloud Controls Matrix (CSA CCM) as the recognized industry standard for cloud assessments. The controls identified in this report are derived from the CSA CCM which can be further mapped to other industry standards if and when needed.

Severity	Defining Characteristics
Critical	When the finding needs immediate attention or awareness due to being recognized as an industry standard critical control or known vulnerability.
High	Represented as a criticality, a control is ranked as "high" when an insecure design or implementation pattern may impact the ity, integrity, or availability of the environment and or data stored therein.
Moderate	Represented as a criticality, a control is ranked as "moderate" when there are defense-in-depth options available, or security is partially inherited through the Shared Responsibility Model.
Low	Represented as a criticality, a control is ranked as "low" if the absence of the control does not create or increase risk when coupled with another vulnerability.

FINDINGS

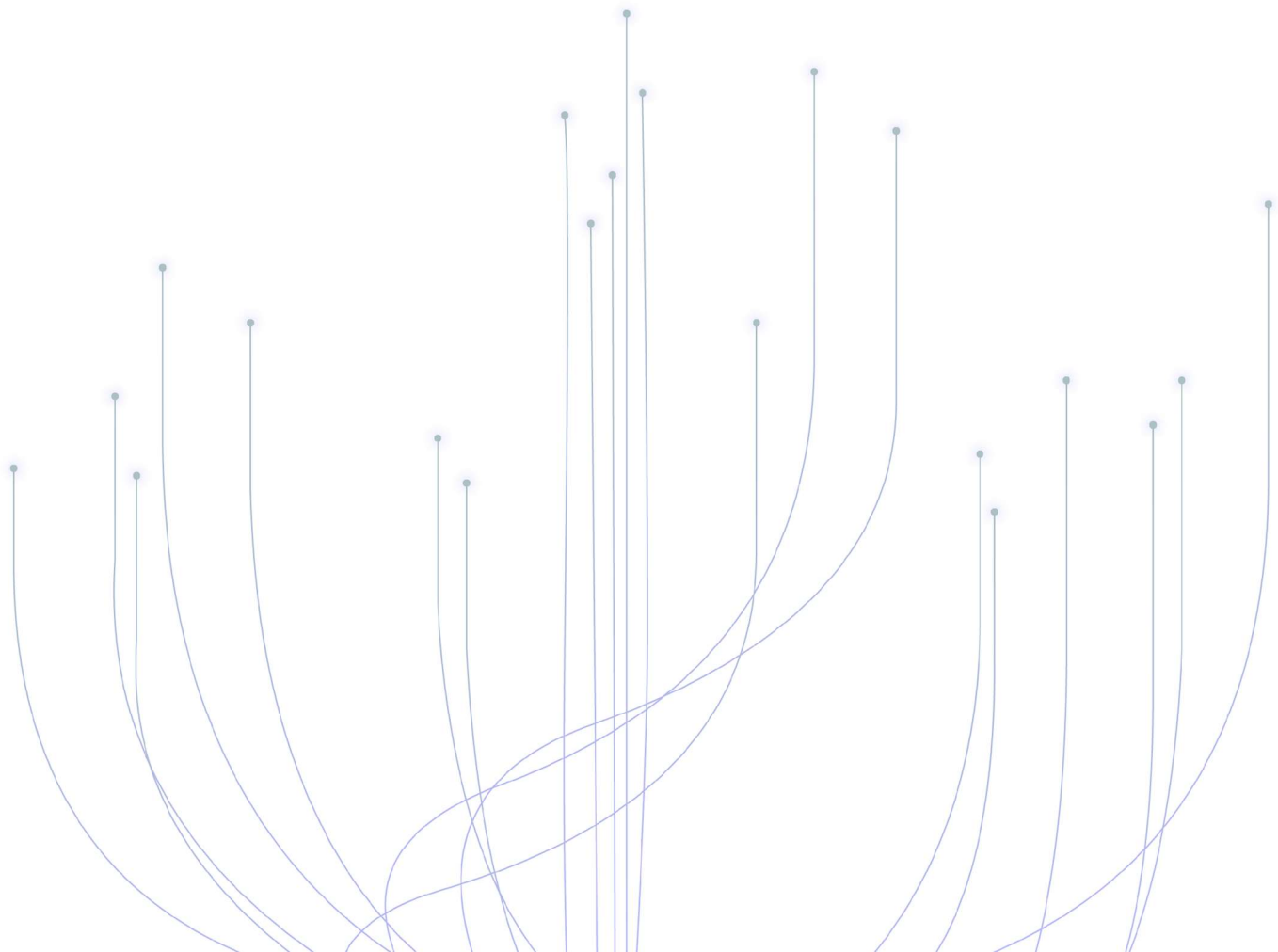
Findings are technical configurations identified within the customer's in-scope cloud environment. The findings are discovered in real time using programmatic means to the public cloud provider's API on behalf of the cloud customer. GuidePoint uses a custom process to read configuration metadata, process the metadata, and return finding status based on available security configuration options for the cloud services. GuidePoint may alter the finding status based on information obtained by the customer in order to better contextualize the finding's status.

Severity	Defining Characteristics
Missing	When the finding deviates from the CIS Benchmark, Azure Best Practices, or Cloud Security Best Practices.
Needs Improvement	When the configuration was found to be in state that did not pose an immediate risk. However, when evaluated as a whole, the configuration may need improvement to maintain a consistent security posture across the environment.
In Place	For configurations consistent with published Azure and Cloud Security Best Practices.

REPORTING FORMAT

GuidePoint Security uses the following reporting format to describe the findings identified in this assessment. The goal of the assessment is to report from a perspective of people, process, and technology. This is represented by the Control. The support evidence, identified as a Finding, is used to inform the analyst who will provide a response within the GuidePoint Analysis section.

Control ID Control Title		
Criticality	Determination of severity of the control	
Control Specification	The Cloud Security Alliance's Cloud Control Matrix (CSA CCM) description of the control	
Control Status	Determination of current security posture when all findings are considered	
GuidePoint Analysis		
GuidePoint Security's analysis of the current security posture using findings to inform the decision.		
Evidence		
Finding Status	**Finding ID**	A title representing configuration information used to inform the status of the security posture. Details can be found in the provided findings matrix.



Findings Summary

Finding Severity Summary - [CLIENT LONG NAME]				
	Critical	**High**	**Moderate**	**Low**
Missing	**0**	**0**	**0**	**0**
Needs Improvement	**0**	**0**	**0**	**0**
In Place	**0**	**0**	**0**	**0**

CONTROL GAPS

MISSING

Control ID	Severity	Title
[Control ID]	[Severity]	[Title]
[Control ID]	[Severity]	[Title]
[Control ID]	[Severity]	[Title]

NEEDS IMPROVEMENT

Control ID	Severity	Title
[Control ID]	[Severity]	[Title]
[Control ID]	[Severity]	[Title]
[Control ID]	[Severity]	[Title]

Analysis of Findings

ENVIRONMENT SUMMARY

< Tell story of Client's current Azure Environment>

<Client> currently has an Azure AD Premium P1 license, and there where a total of 5 Subscriptions within the scope of this assessment, which included.

- MCA-SSV-NPD
- MCA-SSV-PRD
- MCA-IT-HUB
- MCA-APPS-PRD
- MCA-APPS-NPD

Using best practices documented by Microsoft and operational experience obtained by GuidePoint's Cloud Security Architects the following document was developed to help strengthen the security posture of <Client>'s Azure Environment. GuidePoint grouped the findings within two categories: Priority Findings and Next Steps.

PRIORITY FINDINGS

<Touch only on the high to moderate items and highlight at least 3 to 5, no more than this.>

- **Require MFA for all users**
  Multi-factor authentication (MFA) helps protect devices and data that are accessible to their users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, can increase the level of protection if one factor is compromised. <Client> has MFA Conditional Access Policies in place, however they contain exclusions.
    - **Recommended actions -** GuidePoint recommends enforcing MFA for all users, all apps, at all times. It is recommended that a Zero Trust model be followed.

- **Limit number of Global Administrator**
  Limiting the number of global administrators in your tenant is an essential factor in protecting your cloud environment. However, not having enough can also pose an issue as only a global administrator can reset another global administrator's password. <Client> currently has <#> global administrators; since this is the highest privileged role, having this many global administrators increases your attack surface dramatically. If a global administrator is compromised, the attacker gains access to all of the role's permissions.
    - **Recommended actions -** GuidePoint recommends evaluating the need of these users having the Global Admin role assignment, as this is the highest privileged role. Microsoft recommends having no more than 2 to 4 Global Admins in place.

- **Review and decommission no longer relevant Guest user accounts**
  Guest user accounts should be reviewed on a regular basis to ensure that only relevant parties have access to your tenant. Forgotten Guest user accounts have been used in the past as attack vectors to gain access to cloud environments.
    - **Recommended action –** GuidePoint recommends that <Client> review and decommission any Guest User accounts that are no longer needed. <Client> currently has <#> Guest user accounts, all of which are still active.

NEXT STEPS

GuidePoint has identified findings that require additional planning and collaboration from other organizational teams to implement stable and secure solutions. GuidePoint recommends reviewing the "Next Steps" findings with <Client>'s security and operations teams.

<Highlight 2 to 3 that well require planning and configuration. High and Moderate items>

- **Label information based on data classification**
  By implementing a robust data classification policy an organization can determine how data is handled within their cloud environment, therefore allowing them to focus efforts on protecting mission critical information. Resources without appropriate data classification tags are vulnerable to misconfiguration, data loss, data leakage, and improper access permissions.
    - **Recommended actions -** <Client> currently has a tagging system in place, but it does not address the handling of resources that contain or handle data. GuidePoint recommends developing a more in-depth tagging system to address data.

      Example - Tag: DataType

      Values: Public, Corporate (private), , Highly

- **Implement Activity Log Alerts**
  Monitoring the activity within your Azure environment is a critical aspect of cloud security. By putting in place specific alerts, <Client> receives notifications of any anomalies within their tenant.

    - **Recommended action -** Put in place recommended Activity Log Alerts as highlighted in this assessment.

Findings

Audit & Assurance

A&A-04 Requirements Compliance	
Criticality	High
Control Specification	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.
Control Status	[UPDATE]

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence		
[INTERVIEW]	**AZ-SCB-01**	Jurisdictional and Regulatory Data Compliance

Business Continuity Management and Operational Resilience

BCR-02 Risk Assessment and Impact Analysis	
Criticality	Moderate
Control Specification	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.
Control Status	[UPDATE]

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence		
[INTERVIEW]	**AZ-SCB-07**	Impact Analysis

BCR-03 Business Continuity Strategy	
Criticality	Moderate

Control Specification	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.
Control Status	[UPDATE]

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence

MISSING	**AZ-MGF-002**	Azure Managed Grafana is Zone Redundant
[INTERVIEW]	**AZ-SCB-06**	Business Continuity Testing

BCR-08 Backup

Criticality	Moderate
Control Specification	Periodically backup data stored in the cloud. Ensure the ity, integrity and availability of the backup, and verify data restoration from backup for resiliency.
Control Status	[UPDATE]

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence

MISSING	**AZ-ST-011**	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage
NEEDS IMPROVEMENT	**AZ-KV-005**	Ensure the Key Vault is Recoverable
[INTERVIEW]	**AZ-SCB-10**	Ensure Backups and Snapshots are Copied to a Second Region
[INTERVIEW]	**AZ-SCB-05**	Business Continuity Plan

Change Control and Configuration Management

CCC-01 Change Management Policy and Procedures

Criticality	Moderate

Control Specification	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.
Control Status	**[UPDATE]**

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence

MISSING	**AZ-ST-003**	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account

CCC-02 Quality Testing	
Criticality	Moderate
Control Specification	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.
Control Status	**[UPDATE]**

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence

[INTERVIEW]	**AZ-SCB-64**	Standardize Infrastructure Deployments
[INTERVIEW]	**AZ-SCB-14**	Enforce Configuration Standards of the Cloud Infrastructure
[INTERVIEW]	**AZ-SCB-63**	Standardize Application Deployments
[INTERVIEW]	**AZ-SCB-45**	Protect Deployment Templates from Unauthorized Changes

CCC-03 Change Management Technology	
Criticality	Moderate

Control Specification	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).
Control Status	**[UPDATE]**

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence		
NEEDS IMPROVEMENT	**AZ-CNS-001**	AKS clusters installed with Azure Policy add-on
[INTERVIEW]	**AZ-SCB-15**	Electronic Discovery - Assets
[INTERVIEW]	**AZ-SCB-12**	Configuration Management
[INTERVIEW]	**AZ-SCB-13**	System Standardization and Baselines

Cryptography, Encryption & Key Management

CEK-01 Encryption and Key Management Policy and Procedures	
Criticality	Moderate
Control Specification	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.
Control Status	**[UPDATE]**

GuidePoint Analysis

[UPDATE]
GuidePoint analysis analysis analysis
GuidePoint recommendation recommendation recommendation.

Evidence		
MISSING	**AZ-ENC-002**	Private Key Management - KeyPairs
REVIEW	**AZ-POL-008**	Azure Policy: Require blob encryption for storage accounts
REVIEW	**AZ-POL-007**	Azure Policy: Enforce encryption on Data Lake Store accounts
REVIEW	**AZ-POL-006**	Azure Policy: Audit missing blob encryption for storage accounts