GUIDEPOINT
SECURITY

ACME, Inc.

AZURE HEALTH CHECK

August 19, 2022

Version 1.0

CONFIDENTIAL

GuidePoint Security, LLC ▪ 2201 Cooperative Way ▪ Suite 225 ▪ Herndon, VA 20171

Table of Contents

Project Contacts and Document History

[CLIENT LONG NAME] Contact
Steven Jones
CISO
alt@none.com

GuidePoint Security Contacts	
Primary	**Secondary**
Adam Plead	Jonathan Villa
Account Executive	Practice Director, Cloud Security
123.456.7890	414.573.3579
alt@guidepointsecurity.com	jonathan.villa@guidepointsecurity.com

Report Version History			
Version	**Date**	**Author**	**Comments**
0.1	05/01/2022	Virgil Mado	Initial Draft
0.2	05/12/2022	Ari Pasqualiano	QA 1
0.3	05/15/2022	Virgil Mado	QA 2
1.0	05/21/2022	Ari Pasqualiano	Draft to client

Disclaimer

This document contains and constitutes the proprietary and confidential information of GuidePoint Security, LLC, (“GuidePoint”). It is provided ACME (“ACME, Inc.”) subject to and in accordance with the terms of any agreement between GuidePoint and ACME regarding treatment of confidential information and/or licensing of proprietary information. This document also contains information that is the highly sensitive confidential information of ACME and should be treated by representatives of ACME accordingly. The recipient, without the express permission of GuidePoint and ACME, may not distribute this document.

The contents of this document do not constitute legal advice. GuidePoint’s offers of services or deliverables that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such.

Executive Summary

PROJECT DEFINITION AND SCOPE OVERVIEW

ACME (“ACME, Inc”) 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 ACME’s environment in accordance with pre-defined best practices within the industry while also providing recommendations and action items to ACME for remediation where necessary. The scope of this assessment included the ACME’s Azure environment hosted in Microsoft’s Cloud. The point in time assessment was conducted between June 1st, 2022, and June 24th, 2022. 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.

FINDINGS AND RECOMMENDATIONS

During the review of ACME's current Azure Environment, GuidePoint assessed a total of 235 controls which span 23 Cloud Security Domains. Of these controls GuidePoint has identified 135 controls that could be seen as a security or best practice gap(s) and 100 controls which either meet or exceed security or best practice standards.

Some of the controls that meet or exceed security or best practice standards are as follows:

- AAD-07 Ensure that password hash sync is enabled
- AAD-19 Ensure modern authentication for SharePoint applications is required
- GOV-09 Define subscription hierarchy based on business needs
- ISAL-01 Identify a Resource Naming Convention

The following section provides an overview of the Domains and controls that where accessed and highlights the deficient areas and the areas that meet or exceed cloud security standards.

Cloud Security Domains Status

Domain	# of Controls	Pass	Fail	Overall Secure
Azure Active Directory	26	5	21	19%
Governance	6	4	2	67%
Identity and Access Management	25	11	14	44%
Encryption & Key Management	7	3	4	43%
Data Protection & Information Lifecycle	9	4	5	44%
Logging and Monitoring	22	3	19	14%
Incident Response	4	0	4	0%
Inventory Security & Asset Lifecycle	5	4	1	80%
Storage Accounts	12	0	12	0%
Virtual Machines	7	4	3	57%
WorkLoad and Application Security	3	1	2	33%
Networking	23	12	11	52%

Database Services	20	13	7	65%
Azure Policy Definitions	14	0	14	0%
Release & Deployment Management	3	1	2	33%
Supply Chain Management, Transparency, Accountability	2	1	1	50%
Threat & Vulnerability Management	4	4	0	100%
Discovery & Cloud Forensic Analysis	1	0	1	0%
Configuration & Change Management	3	2	1	67%
Business Continuity Management & Operational Resilience	7	4	3	57%
Microsoft Defender for Cloud	14	4	10	29%
AppService	11	5	6	45%
Other Security Considerations	7	5	2	71%
GuidePoint Assessment Total Overall Score	235	90	145	42%

Control Severity Rating

GuidePoint assigns ratings based on the likelihood of attack, the potential impact of a successful attack, and the ease of which an attack can be executed:

- GuidePoint assigns a high-risk classification to controls that have a high likelihood of facilitating some level of data loss or identity compromise to the Azure environment.
- GuidePoint assigns a moderate-risk classification to controls that have a low probability of data compromise but may carry a reasonable chance for an attacker to intercept sensitive information.
- GuidePoint assigns the low-risk classification to controls for which ACME may have a compensating control to prevent successful exploitation. These findings usually provide unnecessary information to attackers, and generally carry very little risk of enterprise compromise or disruption of availability due to the significant difficulty of the attack or the extraordinary circumstances that must be present for success.

In addition, some controls within the Cloud Security Architecture Framework do not expose a significant security risk and are deemed a “best practice” control. These policies and configurations should be seen as recommendations for ACME to implement if leadership deems them useful for their business purpose in the cloud.

Findings Summary

ID	Severity	Finding Title	Deficient Subscriptions
AAD-01	High	Ensure multifactor authentication is enabled for all users in administrative roles.	Sample-Sub
GOV-01	High	Cloud Spend Threshold Alarm	Sample-Sub
VM-02	High	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	Sample-Sub
ENC-01	Moderate	Use of Customer Managed Encryption Keys	Sample-Sub

Analysis of Findings

Environment Summary

ACME currently has an Azure AD Premium P1 license, and there is a total of 1 Subscriptions within the scope of this assessment.

- Sample-Sub

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 ACME's Azure Environment. GuidePoint grouped the findings within two categories: Priority Findings and Next Steps.

Priority Findings

- **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.

  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. ACME currently has 10 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 ACME review and decommission any Guest User accounts that are no longer needed. ACME currently has 200 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 ACME's security and operations teams.

- **Label sensitive 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 -** ACME currently has a tagging system in place, but it does not address the handling of resources that contain or handle sensitive data. GuidePoint recommends developing a more in-depth tagging system to address sensitive data.

    Example - Tag: DataType

    Values: Public, Corporate (private), Confidential, Highly Confidential
- **Implement Activity Log Alerts**
  Monitoring the activity within your Azure environment is a critical aspect of cloud security. By putting in place specific alerts, ACME receives notifications of any anomalies within their tenant.
  - **Recommended action -** Put in place recommended Activity Log Alerts as highlighted in this assessment.

Note: The controls in this report are mapped to, but limited to, the following organizations best practice standards Microsoft, Center for Internet Security (CIS), Cloud Security Alliance (CSA), and GuidePoint Security. Control IDs may not appear in sequential order as they are chosen specifically for each assessment based on services used in the environment and security goals.

AZURE ACTIVE DIRECTORY

AAD-01	Ensure multifactor authentication is enabled for all users in administrative roles.
Description	Enable multifactor authentication for all users who are members of administrative roles in the Microsoft 365 tenant. These include roles such as: Global Administrator Billing Administrator Exchange Administrator SharePoint Administrator Password Administrator Skype for Business Administrator Service Support Administrator User Administrator Dynamics 365 Service Administrator Power BI Administrator
Threats	• Account Breach • Elevation of Privilege • Data Exfiltration • Data Leak
Risk	Compromising any Microsoft 365 Global Administrator account will leave the organization completely vulnerable to the loss of their environment and data.
References	• CIS MICROSOFT365 1.1.1 • CIS Controls 6.5 • CSA CCM IAM-14
Criticality	**HIGH**
FINDING AND RECOMMENDATIONS	
Finding	FAIL
ACME does not have MFA turned on via the single user pane in Azure AD, via a Conditional Access policy, and is not using a third-party solution (DUO, Okta, etc.) to leverage MFA on Administrative level accounts	
Recommendations	Enable MFA via a Conditional Access policy on all administrative level accounts within the organization. This can be accomplished by creating and deploying a Conditional Access policy and assigning it to a user group that contains all the users who are assigned any administrative roles.

GOVERNANCE

GOV-01	Cloud Spend Threshold Alarm
Description	Create a billing alarm to alert the organization when cloud spend has reached an estimated threshold. This can be done using Cost Management + Billing within Azure or a third-party solution.
Threats	• Account Breach • Malicious Intruder • Data Spillage • Data Exfiltration
Risk	Unauthorized access resulting in higher-than-expected billing for allocated resources. Setting a billing alarm can provide another detecting mechanism to identify malicious activity within your Azure tenant.
References	• GuidePoint Recommendation
Criticality	**HIGH**
FINDING AND RECOMMENDATIONS	
Finding	**FAIL**
ACME does not have any cost alerts or budgets in place.	
Recommendations	Ensure that billing alarms are created to create a baseline for the estimated spend for workloads and overall azure tenant. This baseline can be used to identify spikes in resources created, which can indicate unauthorized spend/compromise etc.

ENCRYPTION & KEY MANAGEMENT

ENC-01	Use of Customer Managed Encryption Keys
Description	Using CMKs or import private keys into KeyVault improves the security of KeyVault by giving the organization additional security controls to govern the usage of and ownership of the key. If a cloud customer is relying on a third-party KMS platform, CMKs should be used to encrypt sensitive and/or log data stored in Azure
Threats	• Data Exfiltration • Data Breach • Data Leak
Risk	As it relates to sensitive data ensure that your organization has access to the keys that are used to encyrpt data. Doing so removes the risk to data if associated with the compromise of Microsoft managed keys.
References	• GuidePoint Recommendation • CSA CCM CEK-03 • CSA CCM CEK-04

Criticality	**MODERATE**
FINDING AND RECOMMENDATIONS	
Finding	FAIL
ACME currently does not leverage Customer Managed Keys within their Azure environment.	
Recommendations	Leverage Customer Managed Keys when encrypting sensitive data versus Microsoft Managed Keys.

STORAGE ACCOUNTS

ST-01	**Ensure that 'Secure transfer required' is set to 'Enabled'**
Description	Enable data encryption in transit.
Threats	• Malicious Intruder • Data Spillage • Data Exfiltration
Risk	Ensure to maintain the integrity of data as it is in transit.
References	• CIS Azure 3.1 • CIS Controls 13.10
Criticality	**MODERATE**
FINDING AND RECOMMENDATIONS	
Finding	PASS
ACME has secure transfer enabled on all storage accounts.	
Recommendations	No further recommendations.

VIRTUAL MACHINES

VM-02	**Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)**
Description	Ensure that OS disks (boot volumes) and data disks (non-boot volumes) are encrypted with CMK (Customer Managed Keys). Customer Managed keys can be either ADE or Server Side Encryption (SSE)
Threats	• Data Loss • Data Exfiltration
Risk	Microsoft Managed keys are subject to become compromised at any point in time, if this occurs the data that you encrypted with using the compromised keys are at risk.

References	• CIS Azure 7.2 • CIS Controls 3.11 • CSA CCM CEK-03
Criticality	**HIGH**
FINDING AND RECOMMENDATIONS	
Finding	FAIL
ACME currently does not leverage Customer Managed Keys within their Azure environment.	
Recommendations	Leverage Customer Managed Keys when encrypting sensitive data versus Microsoft Managed Keys.