GUIDEPOINT
SECURITY

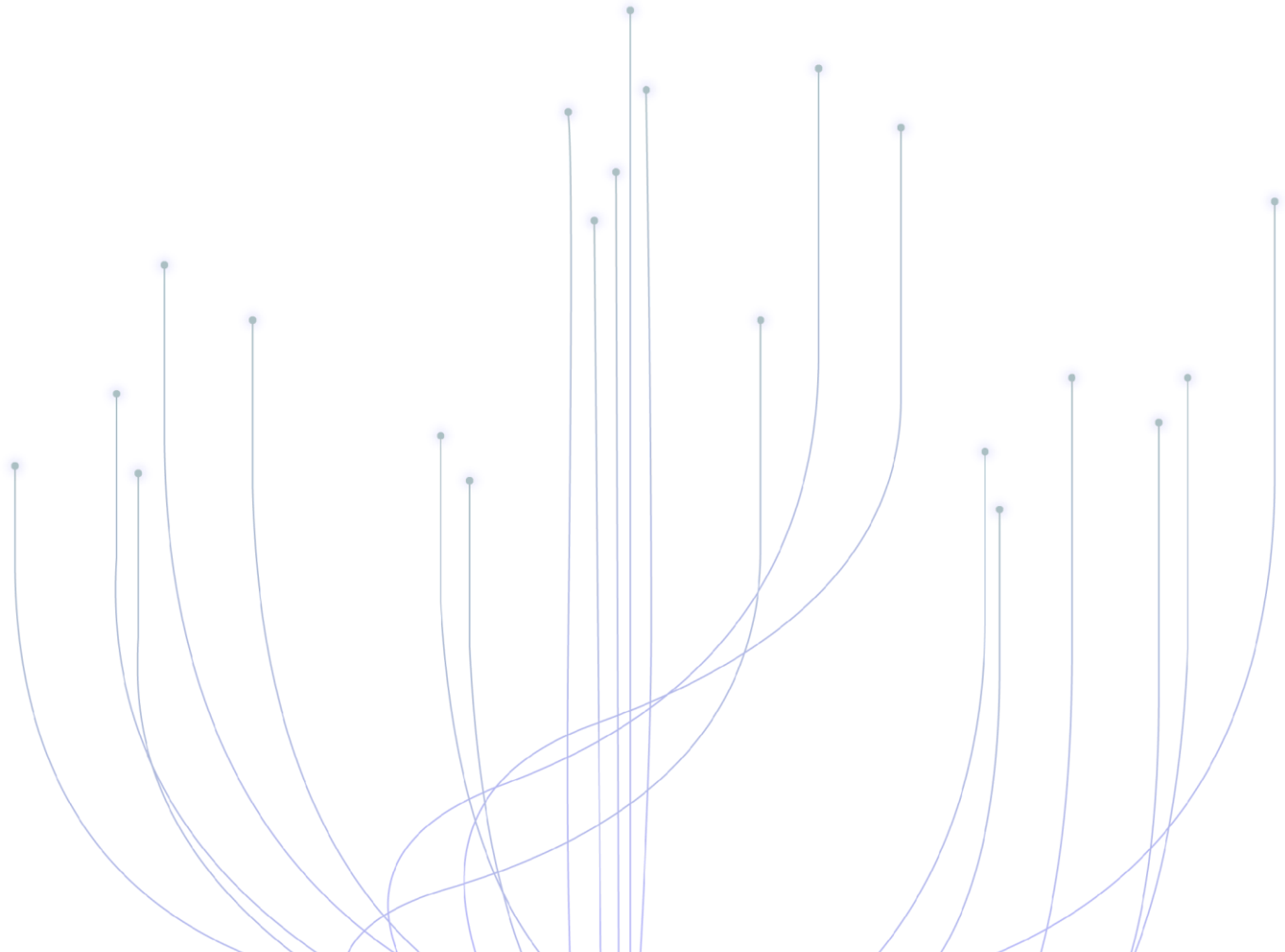
ACME, Inc

Microsoft 365 Health Check

July, 2024

Version 1.0

Table of Contents



Project Contacts and Document History

ACME, Inc. Contact
Steven Jones
CISO
alt@none.com

GuidePoint Security Contacts	
Primary	**Secondary**
John Doe	Jonathan Villa
Account Executive	Practice Director, Cloud Security
123.456.7890	414.573.3579
boris.kusmanoff@guidepointsecurity.com	jonathan.villa@guidepointsecurity.com

Report Version History			
Version	**Date**	**Author**	**Comments**
0.1	06/01/2024	Virgil Mado	Initial Draft
0.2	06/12/2024	Ari Pasqualiano	QA 1
0.3	06/15/2024	Virgil Mado	QA 2
1.0	06/21/2024	Ari Pasqualiano	Draft to client

Disclaimer

This document contains and constitutes the proprietary and information of GuidePoint Security, LLC, ("GuidePoint"). It is provided Acme, Inc ("Acme, Inc") subject to and in accordance with the terms of any agreement between GuidePoint and Acme, Inc regarding treatment of information and/or licensing of proprietary information. This document also contains information that is the specific to Acme, Inc and should be treated by representatives of Acme, Inc accordingly. The recipient, without the express permission of GuidePoint and Acme, Inc, 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, Inc ("Acme, Inc") engaged GuidePoint Security, LLC ("GuidePoint") to review the Microsoft 365 environment and identify configuration components that require improvement or do not meet security best

practices. This Microsoft 365 Security Assessment evaluates Acme, Inc environment in accordance with pre-defined best practices within the industry while also providing recommendations and action items to Acme, Inc for remediation where necessary. The scope of this assessment included the Acme, Inc Microsoft 365 environment hosted in Microsoft's Cloud. The point in time assessment was conducted between June 1st, 2024 and June 12th, 2024.

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

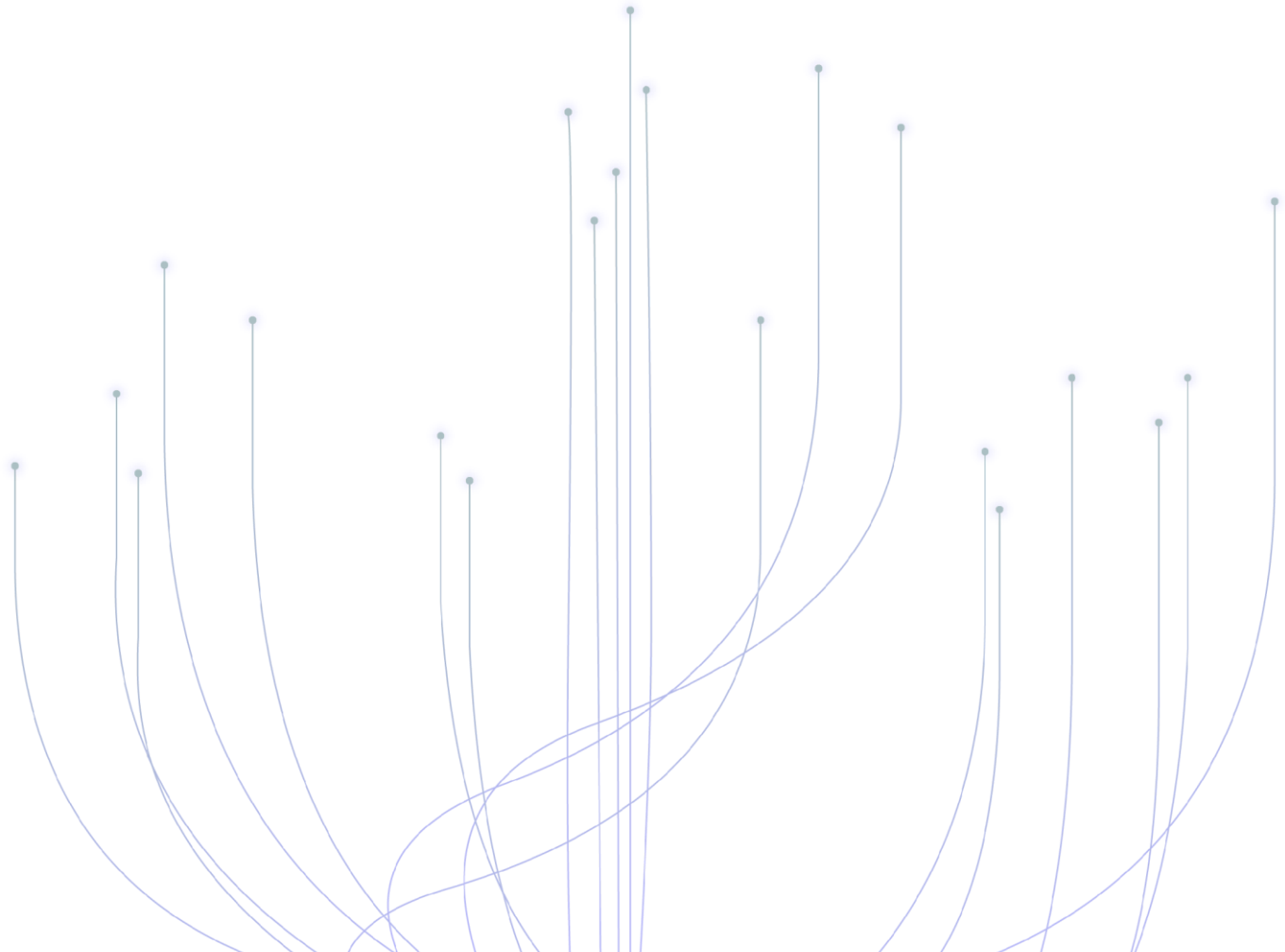
Findings are technical configurations identified within the customer's in-scope cloud environment. The findings are discovered in real time using programmatic means to the public cloud provider's API on behalf of the cloud customer. GuidePoint uses a custom process to read configuration metadata, process 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, M365 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 M365 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	
Implementation Guidelines	Implementation guidelines provided by the Cloud Security Alliance's Cloud Control Matrix (CSA CCM)	
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.



GUIDEPOINT SECURITY

Findings Summary

Finding Severity Summary - Acme, Inc LLC				
	Critical	**High**	**Moderate**	**Low**
Missing	**0**	**6**	**4**	**0**
Needs Improvement	**0**	**6**	**4**	**0**
In Place	**0**	**2**	**3**	**0**

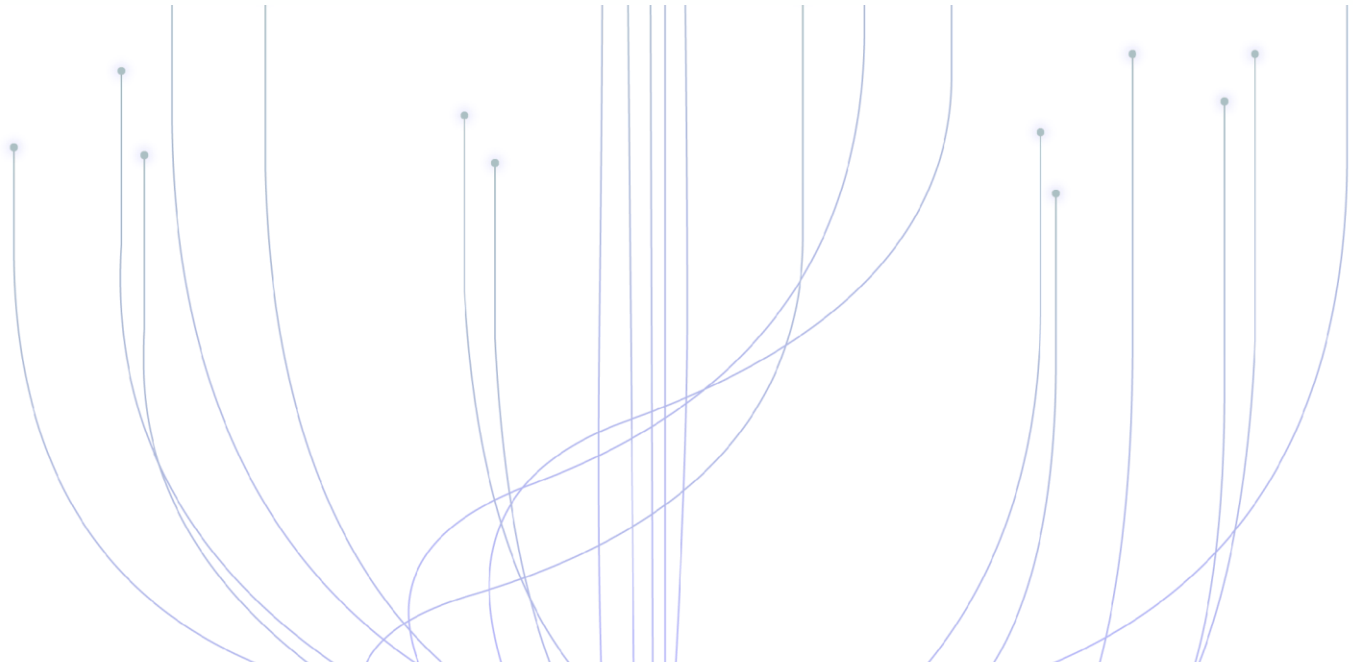
CONTROL GAPS

MISSING

Control ID	Severity	Title
CCC-01	High	Change Management Policy and Procedures
DSP-01	High	Security and Privacy Policy and Procedures
SEF-03	Moderate	Incident Response Plans
UEM-06	Moderate	Automatic Lock Screen

NEEDS IMPROVEMENT

Control ID	Severity	Title
DSP-17	High	Data Protection
HRS-11	High	Security Awareness Training
DSP-07	Moderate	Data Protection by Design and Default
IAM-01	Moderate	Identity and Access Management Policy and Procedures



Analysis of Findings

ENVIRONMENT SUMMARY

Acme, Inc currently has multiple M365 licenses in place, the predominant being Microsoft 365 F3, and utilizing Microsoft Entra ID P2 for their Entra ID license. GuidePoint has identified that this tenant currently has a total of 2,815 user accounts in place, of which 277 are guest users.

Using best practices documented by Microsoft and operational experience obtained by GuidePoint's Cloud Security Architects the following roadmap was developed to help strengthen the security posture of Acme, Inc Microsoft 365 Environment. GuidePoint grouped the findings within two categories: Quick Hits and Next Steps.

QUICK HITS

- **Ensure expiration time for external sharing links is set**

  Ensuring that expiration times for external sharing links are set is crucial for enhancing security and reducing the risk of data exposure in your organization. External sharing links allow external parties (e.g., customers, partners, vendors) to access files and resources within your organization's environment, such as documents stored in SharePoint, OneDrive, or Teams. However, without setting an expiration time, these links could remain accessible indefinitely, potentially exposing your organization to various risks.
  - **Recommended actions -** GuidePoint recommends enabling expiration for external link sharing within SharePoint.

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, Inc security and operations teams.

- **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, Inc currently has 35 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 the role's permissions.
  - **Recommended actions -** GuidePoint recommends evaluating the need of these users to have 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.

Findings

Change Control and Configuration Management

CCC-01 Change Management Policy and Procedures	
Criticality	High
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 ly or externally (i.e., outsourced). Review and update the policies and procedures at least annually.
Implementation Guidelines	A documented and approved change management policy (and associated process documentation) should: a. Ensure that changes are tested, documented, risk assessed, and authorized in a consistent and timely manner. All changes (e.g., major, minor, and emergency and the qualifying criteria) in organization assets, applications, system software, and informational technology (IT) infrastructure (e.g., hardware, operating systems, communications equipment, and software) and associated configurations should be under the scope of the change management policy. b. Be communicated and made accessible to all employees and interested parties involved within the change management process (e.g., service/application owners, project leaders, IT, operating systems staff, contractors, etc.). c. Include the management of emergency changes.
Status	**MISSING**
GuidePoint Analysis	Users are currently allowed to communicate with Teams users whose accounts are not managed by an organization. GuidePoint recommends disabling this setting and blocking all external domains from Teams and Skype, along with creating a list of allowed domains.

Evidence		
MISSING	**M365-DM-003**	Ensure external domains are not allowed in Skype or Teams

Cryptography, Encryption & Key Management

CEK-03 Data Encryption	
Criticality	High
Control Specification	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.

Implementation Guidelines	Data protection/data encryption is the process of changing plaintext into ciphertext using a cryptographic algorithm and key. a. Organizations should be able to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). b. Data at rest involves databases, end-user workstations, and file servers. c. Data in transit involves system interfaces, public networks, and electronic messaging. d. Cryptography provides data protection: ity, integrity, availability, and source authentication. e. Cryptographic key management system security policies rules need to protect the ity, integrity, availability, and source authentication of all keys, algorithms, and metadata. f. Key management technology and processes should be NIST FIPS validated and/or National Security Agency (NSA)-approved by other relevant international standardization bodies. g. Approved algorithms and key sizes should reside in the CKMS. h. Quantum-resistant encryption is developing quickly, and it is recommended that this technology is closely monitored so the organization is not exposed.
Status	**IN PLACE**
GuidePoint Analysis	No further recommendations

Evidence		
IN PLACE	**M365-SCB-16**	Enforce Data Encryption in Transit

Data Security and Privacy Lifecycle Management

DSP-01 Security and Privacy Policy and Procedures	
Criticality	High
Control Specification	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.

Implementation Guidelines	Policies and procedures should include provisions for the following: a. Data classifications with clear definitions and examples. b. Acceptable use, handling, and storage of data by classifications. c. How long the classified data should be retained. d. How/when the classified data should be destroyed. e. Responsibilities of data stewards. Maintain a data inventory and document data flow diagrams and associated technical measures. Document data protection controls and third-party data sharing practices. This documentation and associated risks should be shared with customers and data owners as needed. Examples include but are not limited to: • Access controls and data loss prevention (DLP) solutions with data tagging capabilities. • Define testing intervals based on data classification types or levels. • Executive leadership should approve policies (cf. GRC-01). • Note: Data life cycles include all stages (processing, storage, and transmission).
Status	**MISSING**
GuidePoint Analysis	At the time of the assessment there were no Data Retention policies in place. Customer lockbox is currently not enabled. There are currently no labels or label policies are in place.

Evidence		
MISSING	**M365-DM-008**	Create Data Retention Policies based on labels to protect and delete data
MISSING	**M365-DM-001**	Ensure the customer lockbox feature is enabled
MISSING	**M365-DM-002**	Ensure SharePoint Online Information Protection policies are set up and Ensure SharePoint Online Information Protection policies are set up and used

GUIDEPOINT

SECURITY