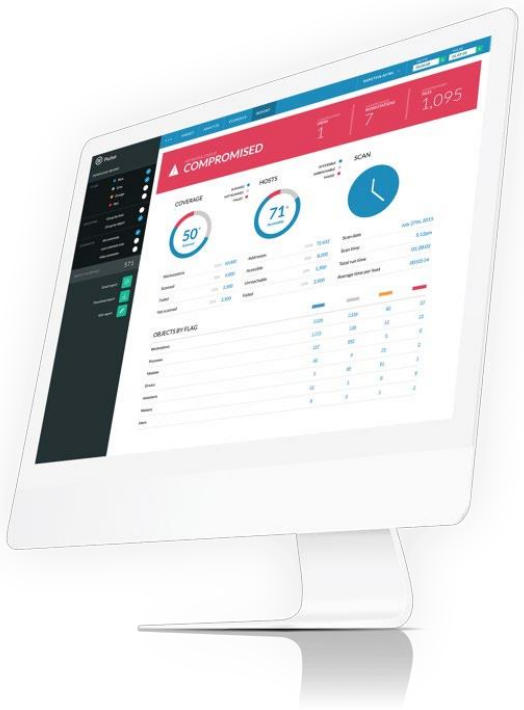
Infocyte Cloud™

MS365 Assessment

COMPANY NAME



Copyright and Acknowledgements

Copyright, Acknowledgments, and Proprietary Statement

This document contains confidential and proprietary information and is the property of Infocyte, Inc. ("Infocyte"). This document was prepared for the requesting party for the sole purpose of reviewing the threats and vulnerabilities found in their environment. It is submitted to you in confidence, on the condition that you and your representatives have, by receiving it, agreed not to reproduce or copy it, in whole or in part, or to furnish such information to others, or to make any other use of it except for the evaluation purposes stated above. The previous statement shall not apply to the extent that such statement violates any federal or state laws requiring such information to be made available to the public.

Infocyte and Infocyte HUNT are registered trademarks of Infocyte, Inc. All other trademarks, service marks, registered trademarks, and registered service marks are the property of their respective owners. Complying with all applicable copyright laws in the US and other countries is the responsibility of the user.

Infocyte Assessment Services Report

An Infocyte Assessment was conducted in the month of January 2021 for the ACME Industries IT Staff. This assessment checks the current Microsoft 365 settings for compliance against the CIS best practices as published at: as well as Microsoft's best practices published at:

Scope

Account and Authentication Critical Controls Tested

- Enable Azure AD Identity Protection sign-in risk policies
- Enable Azure AD Identity Protection user risk policies
- Enable Conditional Access policies to block legacy authentication
- Ensure modern authentication for Exchange Online is enabled
- Ensure modern authentication for SharePoint applications is required
- Ensure multifactor authentication is enabled for all users in administrative roles
- Ensure multifactor authentication is enabled for all users in all roles
- Ensure that between two and four global admins are designated
- Ensure that MS 365 Passwords Are Not Set to Expire
- Ensure that password hash sync is enabled for resiliency and leaked credential detection

Data Management Critical Controls Tested

- Ensure DLP policies are enabled
- Ensure DLP policies are enabled for Microsoft Teams
- Ensure the customer lockbox feature is enabled
- Ensure that external users cannot share files, folders, and sites they do not own

Email and Exchange Online Security Controls Tested

- Ensure basic authentication for Exchange Online is disabled
- Ensure DMARC Records for all Exchange Online domains are published
- Ensure mail transport rules do not whitelist specific domains
- Ensure notifications for internal users sending malware is Enabled
- Ensure that an anti-phishing policy has been created
- Ensure that DKIM is enabled for all Exchange Online Domains
- Ensure that SPF records are published for all Exchange Domains
- Ensure the Advanced Threat Protection Safe Attachments policy is enabled
- Ensure the Advanced Threat Protection Safe Links policy is enabled
- Ensure the Client Rules Forwarding Block is enabled

Application Permissions Tested

Ensure O365 ATP SafeLinks for Office Applications is Enabled.
Ensure Office 365 SharePoint infected files are disallowed for download

Storage

Block OneDrive for Business sync from unmanaged devices
Ensure document sharing is being controlled by domains with whitelist or blacklist
Ensure expiration time for external sharing links is set
Ensure external storage providers available in Outlook on the Web are restricted

Secondary Account and Authentication Controls Tested

Ensure self-service password reset is enabled

Secondary Email and Exchange Controls Tested

Ensure Exchange Online Spam Policies are set correctly
Ensure mail transport rules do not forward email to external domains
Ensure MailTips are enabled for end users
Ensure that Facebook contact synchronization is disabled.
Ensure that LinkedIn contact synchronization is disabled
Ensure the Common Attachment Types Filter is enabled

Application Permissions

Ensure calendar details sharing with external users is disabled
Ensure Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams is Enabled
Ensure users installing Outlook add-ins is not allowed

Auditing

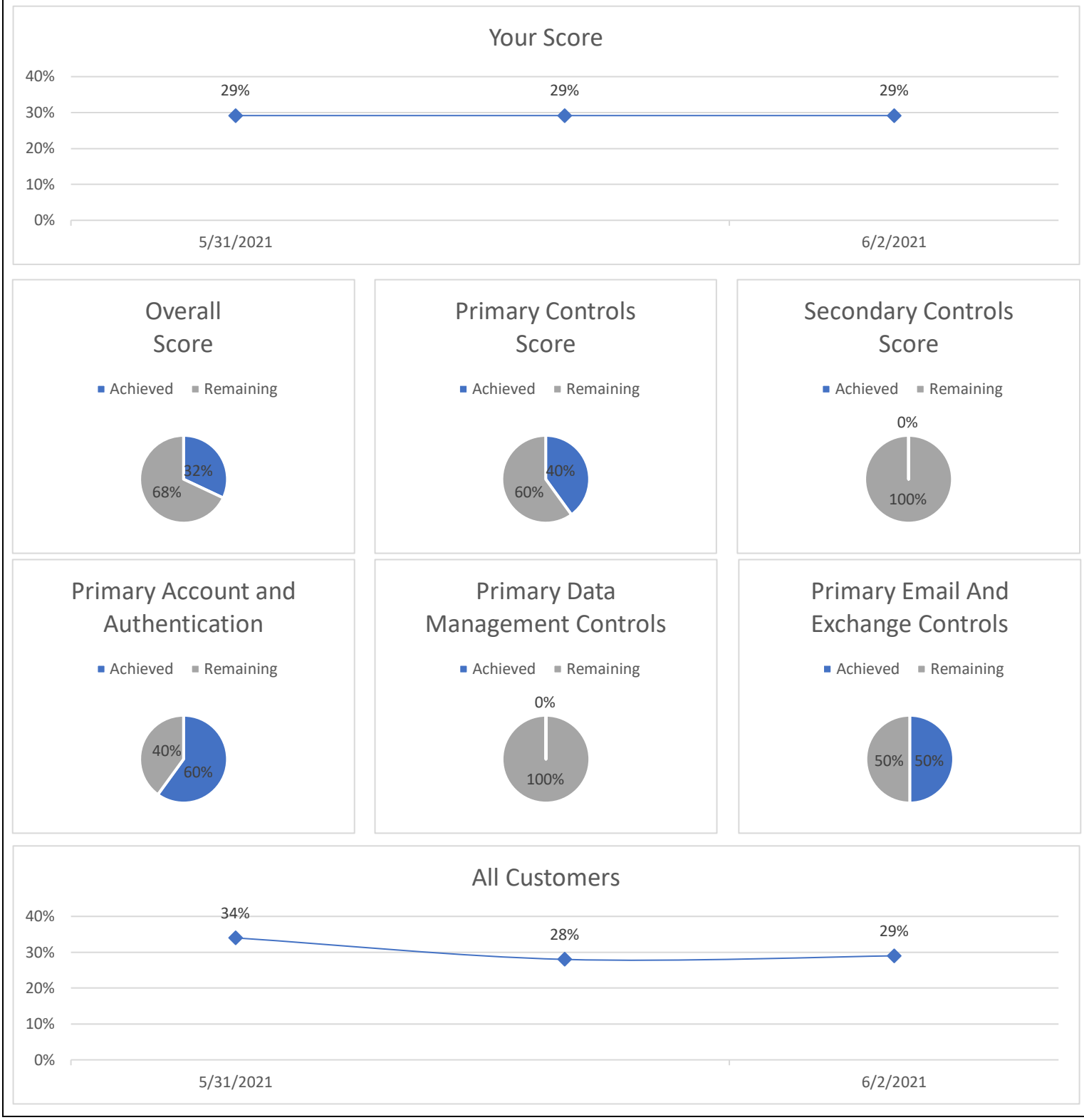
Ensure mailbox auditing for all users is Enabled
Ensure Microsoft 365 audit log search is Enabled

Domain Sampled: AcmeLLC.Com
Date(s) Sampled: 6/2/2021

Results

Controls	Weight	Score
Critical	**300**	**90**
Account / Authentication	**100**	**30**
Enable Azure AD Identity Protection sign-in risk policies	10	0
Enable Azure AD Identity Protection user risk policies	10	0
Enable Conditional Access policies to block legacy authentication	10	0
Ensure modern authentication for Exchange Online is enabled	10	10
Ensure modern authentication for SharePoint applications is required	10	0
Ensure multifactor authentication is enabled for all users in administrative roles	10	0
Ensure multifactor authentication is enabled for all users in all roles	10	0
Ensure that between two and four global admins are designated	10	10
Ensure that MS 365 Passwords Are Not Set to Expire	10	10
Ensure that password hash sync is enabled for resiliency and leaked credential detection	10	0
Data Management	**40**	**0**
Ensure DLP policies are enabled	10	0
Ensure DLP policies are enabled for Microsoft Teams	10	0
Ensure that external users cannot share files, folders, and sites they do not own	10	0
Ensure the customer lockbox feature is enabled	10	0
Email Security / Exchange Online	**100**	**50**
Ensure basic authentication for Exchange Online is disabled	10	0
Ensure DMARC Records for all Exchange Online domains are published	10	0
Ensure mail transport rules do not whitelist specific domains	10	10
Ensure notifications for internal users sending malware is Enabled	10	0
Ensure that an anti-phishing policy has been created	10	10
Ensure that DKIM is enabled for all Exchange Online Domains	10	10
Ensure that SPF records are published for all Exchange Domains	10	10
Ensure the Advanced Threat Protection Safe Attachments policy is enabled	10	0
Ensure the Advanced Threat Protection Safe Links policy is enabled	10	0
Ensure the Client Rules Forwarding Block is enabled	10	10
Application Permissions	**20**	**0**
Ensure O365 ATP SafeLinks for Office Applications is Enabled.	10	0
Ensure Office 365 SharePoint infected files are disallowed for download	10	0
Storage	**40**	**10**
Block OneDrive for Business sync from unmanaged devices	10	0
Ensure document sharing is being controlled by domains with whitelist or blacklist	10	10

Ensure expiration time for external sharing links is set	10	0
Ensure external storage providers available in Outlook on the Web are restricted	10	0
Secondary	**60**	**15**
Account / Authentication	**5**	**5**
Ensure self-service password reset is enabled	5	5
Email Security / Exchange Online	**30**	**0**
Ensure Exchange Online Spam Policies are set correctly	5	0
Ensure mail transport rules do not forward email to external domains	5	0
Ensure MailTips are enabled for end users	5	0
Ensure that Facebook contact synchronization is disabled.	5	0
Ensure that LinkedIn contact synchronization is disabled	5	0
Ensure the Common Attachment Types Filter is enabled	5	0
Application Permissions	**15**	**0**
Ensure calendar details sharing with external users is disabled	5	0
Ensure Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams is Enabled	5	0
Ensure users installing Outlook add-ins is not allowed	5	0
Auditing	**10**	**10**
Ensure mailbox auditing for all users is Enabled	5	5
Ensure Microsoft 365 audit log search is Enabled	5	5
Grand Total	**360**	**105**


Your Score
40%
30%
20%
10%
0%
29%
29%
29%
5/31/2021
6/2/2021
Overall Score
Achieved
Remaining
32%
68%
Primary Controls Score
Achieved
Remaining
40%
60%
Secondary Controls Score
Achieved
Remaining
0%
100%
Primary Account and Authentication
Achieved
Remaining
40%
60%
Primary Data Management Controls
Achieved
Remaining
0%
100%
Primary Email And Exchange Controls
Achieved
Remaining
50%
50%
All Customers
40%
30%
20%
10%
0%
34%
28%
29%
5/31/2021
6/2/2021

Remediation and Corrections

Missed Control (1)

Ensure multifactor authentication is enabled for all users in administrative roles

Result:

You have 3 out of 5 users administrative roles registered and not protected with MFA.

Why: Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Remediation Steps

1. Log in to <Link> as a Global Administrator.
2. Go to Admin centers and click on Azure Active Directory.
3. Select Enterprise applications then, under Security, select Conditional Access.
4. Click New policy
5. Go to Assignments > Users and groups > Include > Select users and groups > check Directory roles.
6. At a minimum, select the following roles: Billing admin, Conditional Access admin, Exchange admin, Global admin, Helpdesk admin, Security admin, SharePoint admin, and User admin.
7. Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and don't exclude any apps).
8. Under Access controls > Grant > select Grant access > check Require multifactor authentication (and nothing else).
9. Leave all other conditions blank.
10. Make sure the policy is enabled.
11. Create……

Missed Control (2)

Result:

Why:

Remediation Steps

Missed Control (3)

Result:

Why:

Remediation Steps

Missed Control (4)

Result:

Why:

Remediation Steps

Missed Control (5)

Result:

Why:

Remediation Steps

Conclusion

<<Conclusion Information specific to the findings>>