Quarterly Microsoft 365 Security Summary Report

Contoso Corp

Date: Sunday, January 28, 2024

Reporting Period: October 1, 2023 - December 31, 2023

TyrellTech

Prepared by Tyrell Technologies

Report Summary

To safeguard and ensure the continuity of your business it is essential to protect your applications and data. At Tyrell Technology Support Services, we believe a strong partnership with each customer is at the core of maintaining IT security. The strength of this partnership is reflected in this report, demonstrating key protections in place to defend against threats and vigilance to continually monitor and remediate issues that threaten your business.

This report is both an analysis of our current IT security posture, an accounting of activities our firm has taken to keep you safe and recommended proactive measures to stay one step ahead of cyber threats. We look forward to walking through this report and charting a path forward together.

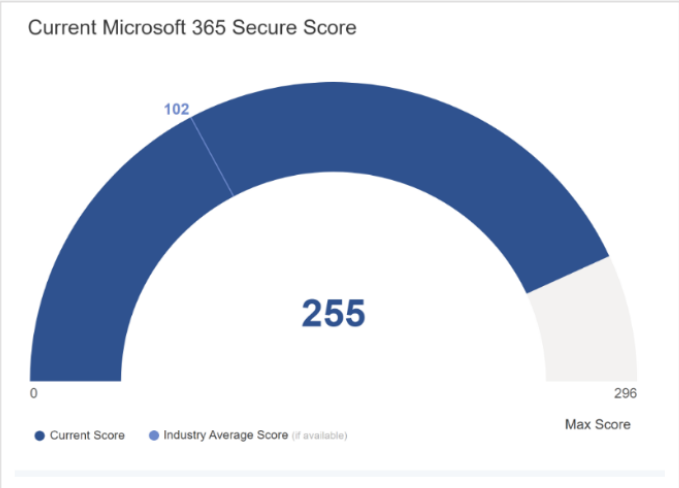
Table of Contents

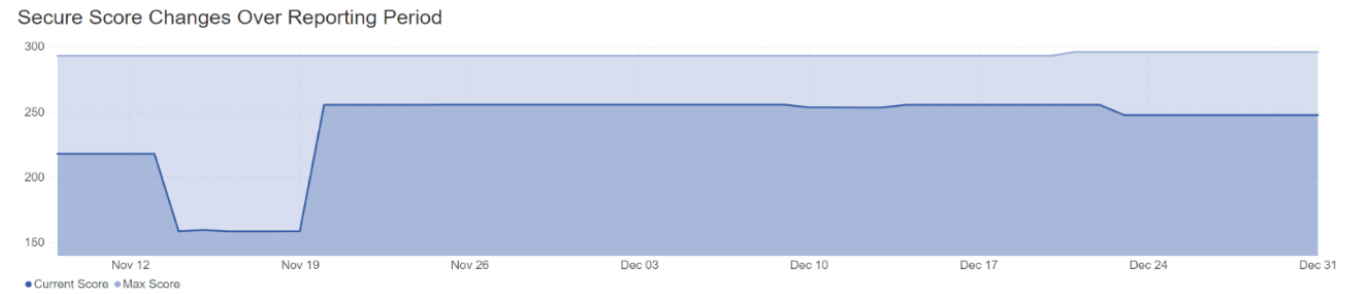
***Note**: Due to Microsoft's archiving policies or the date of initial reporting data activation, historical data represented in this report may not extend all the way back to the beginning of the reporting period. This will be remedied over time as data continues to be collected.*

Security & Compliance Summary

Microsoft Secure Score is an overall representation of your organization's security posture

Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024





Secure Score Change	Emails Received Activity	Emails Quarantined
+29.77 (between the reporting period start/end date)	156	0

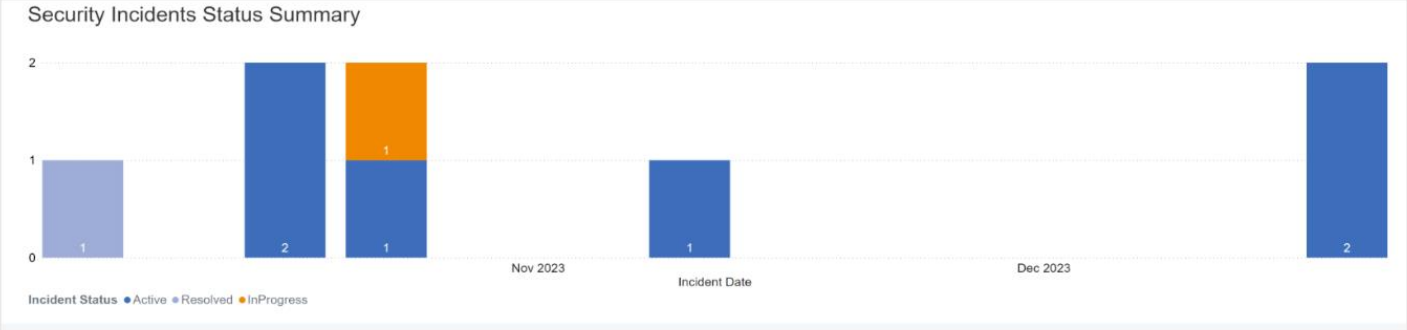
Malware Emails Blocked	Spam Emails Blocked	Phish Emails Blocked
0	0	0

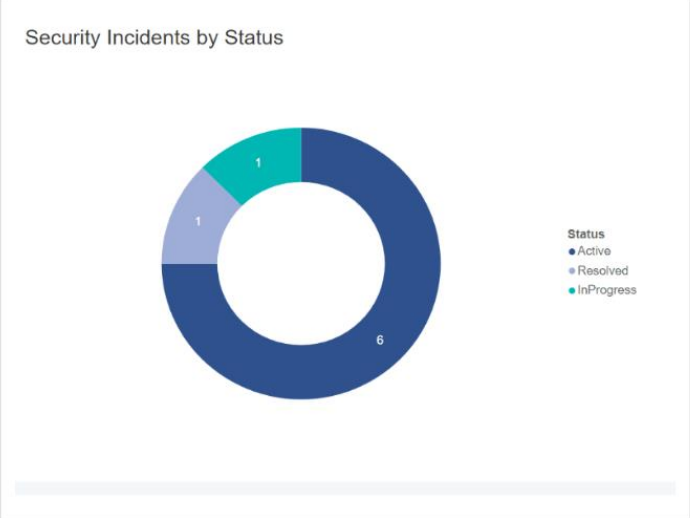
Security Support Activity Summary

Summary of monitoring and M365 incident/alert remediations

Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024

Active Monitoring	Frequency	Description
Daily Security Incidents Report	Daily	Monitoring report for M365 security incidents. Report is reviewed daily by the IT security team.
Daily Security Incidents Report	Daily	Monitoring report for M365 security incidents. Report is reviewed daily by the IT security team.





Most Common Security Incident Types

Incident Type	Count
Collection incident involving one user reported by multiple sources	4
Activity from infrequent country involving one user	1
High volume of email search activities by a privileged app	1
Rare apps with high permissions	1
Risky OAuth apps	1

Active Security Alerts

Severity ● high ● medium ● low ● informational

	2023-08	2023-09	2023-10	2023-11	2023-12	2024-01	
high			3		1	1	**5**
medium	1	1	2	1			**5**
low		2			1		**3**
informational	1	1	4				**6**

Resolved Security Alerts

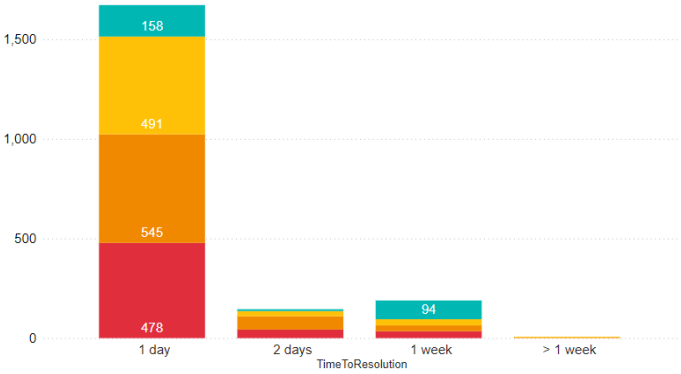
Severity ● high ● medium ● informational

	2023-10	2023-11	
high	1	2	**3**
medium	2	1	**3**
informational		2	**2**

Most Common Security Alerts

Alert Title	# Alerts
Unfamiliar sign-in properties	321
Anonymous IP address	161
Anomalous Token	40
Atypical travel	29
Password Spray	18
Activity from a password-spray associated IP address	10
Suspicious behavior: Impossible travel activity	1
Suspicious behavior: Multiple failed login attempts	1
Suspicious inbox forwarding rule	1

Security Alerts Time-to-Resolution



Severity ● high ● medium ● low ● informational

Security News

News curated from your industry to help stay on top of current developments in IT security

[Russian hackers believed to be behind cyber attack on Victoria's County Court](#) January 1, 2024

Russian hackers are believed to have stolen financial information and employee data from Victoria's County Court in a cyber attack discovered in the lead-up to the Christmas break.

Australian Broadcasting Corporation on MSN.com

[Sandworm hacker group behind cyber attack on Kyivstar – Security Service of Ukraine](#) January 4, 2024

The hacker group Sandworm, which is a regular unit of Russian military intelligence, was behind the cyber attack on the Ukrainian mobile operator Kyivstar at the end of December 2023. The attack was aimed at leaving people without communication for as long as possible, but the SBU helped Kyivstar restore its systems within days and repel new cyber attacks. The attack had a significant impact on civilians but did not have a serious effect on military communications.

en.interfax.com.ua

[HP Enterprise blames hacking on same Russian group behind Microsoft breach](#) January 25, 2024

Hewlett Packard Enterprise Co. has reported that a suspected nation-state actor, believed to be the same Russian group behind the Microsoft breach, gained unauthorized access to its email system and exfiltrated data from a small percentage of its mailboxes starting in May 2023.

MyBroadband

[Exclusive-Russian hackers were inside Ukraine telecoms giant for months - cyber spy chief](#) January 4, 2024

Russian hackers breached the system of Ukrainian telecoms giant Kyivstar for months, according to Ukraine's cyber spy chief. The attack should serve as a warning to the West about the dangers of cyberattacks.

Haaretz.com on MSN.com

[5 major threats to US national security in 2024](#) January 3, 2024

The article discusses the top five threats to US national security in 2024, including ongoing conflicts in Ukraine and Israel, growing unrest in the Middle East and Indo-Pacific, and the upcoming presidential election that may stir domestic strife.

The Hill on MSN.com

Articles powered by Bing News

Secure Score History

Changes to your Microsoft Secure Score and Max Score during the reporting period

Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024

Secure Score Change History

Summary of Secure Score Changes

Period Start Date	Period End Date	Starting Score	Ending Score	Change Amount	Starting Max Score	Ending Max Score	Change Amount	Starting % of Max	Ending % of Max	Change Amount
Oct 1, 2023	Dec 31, 2023	217.82	247.59	+29.77	293.0	296.0	+3.0	74.34%	83.65%	+9.3%

Recommendation Influencing the Score	Score Change	Max Score Change	Resulting Points	Number of Changes	Previous Status	New Status
Set action to take on high confidence spam detection	+5.0	-	5/5	1	To address	Completed
Set action to take on phishing detection	+5.0	-	5/5	1	To address	Completed
Enable impersonated domain protection	+3.2	-	8/8	4	To address	Completed
Enable impersonated user protection	+3.2	-	8/8	4	To address	Completed
Ensure that intelligence for impersonation protection is enabled	+3.2	-	8/8	4	To address	Completed
Move messages that are detected as impersonated users by mailbox intelligence	+3.2	-	8/8	4	To address	Completed
Set the phishing email level threshold at 2 or higher	+3.2	-	8/8	4	To address	Completed
Quarantine messages that are detected from impersonated domains	+2.4	-	6/6	5	To address	Completed
Quarantine messages that are detected from impersonated users	+2.4	-	6/6	4	To address	Completed
Enable the domain impersonation safety tip	+1.2	-	3/3	4	To address	Completed
Enable the user impersonation safety tip	+1.2	-	3/3	4	To address	Completed
Enable the user impersonation unusual characters safety tip□	+1.2	-	3/3	4	To address	Completed
Ensure that an anti-phishing policy has been created	+1.2	-	3/3	4	To address	Completed
Restrict anonymous users from joining meetings	+1.0	-	1/1	1	To address	Completed
Block users who reached the message limit	+0.4	-	1/1	5	To address	Completed

Additional recommendations can improve your Secure Score. Contact us to discuss your options.

Secure Score Recommendations

Improve your Microsoft 365 Secure Score with these recommended actions

Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024

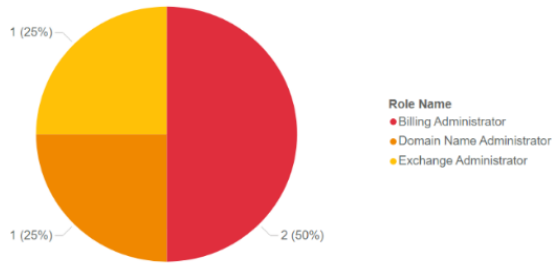
Points Available	Recommendation Action	Protects Against
10	Ensure multifactor authentication is enabled for all users in administrative roles	Password Cracking; Account Breach; Elevation of Privilege
9	Ensure multifactor authentication is enabled for all users	Password Cracking; Account Breach
8	Set the phishing email level threshold at 2 or higher	
8	Enable Conditional Access policies to block legacy authentication	Password Cracking; Account Breach
8	Enable impersonated domain protection	
8	Move messages that are detected as impersonated users by mailbox intelligence	
8	Ensure that intelligence for impersonation protection is enabled	
8	Enable impersonated user protection	
7	Enable Azure AD Identity Protection user risk policies	Password Cracking; Account Breach
7	Enable Azure AD Identity Protection sign-in risk policies	Password Cracking; Account Breach
6	Quarantine messages that are detected from impersonated users	
6	Quarantine messages that are detected from impersonated domains	
5	Set action to take on high confidence spam detection	
5	Ensure additional storage providers are restricted in Outlook on the web	Data Exfiltration; Account breach
5	Set action to take on phishing detection	
5	Ensure all forms of mail forwarding are blocked and/or disabled	Data Exfiltration; Account breach
5	Start your Defender for Identity deployment, installing Sensors on Domain Controllers and other eligible servers.	
5	Ensure 'External sharing' of calendars is not available	
5	Ensure the Common Attachment Types Filter is enabled	
4	Ensure user consent to apps accessing company data on their behalf is not allowed	Data Exfiltration; Data Spillage

Secure Score recommendations are powered by Microsoft 365. Descriptions often include technical details meant for IT security professionals. Our team stands ready to talk through each recommendation and the implications to your overall security posture.

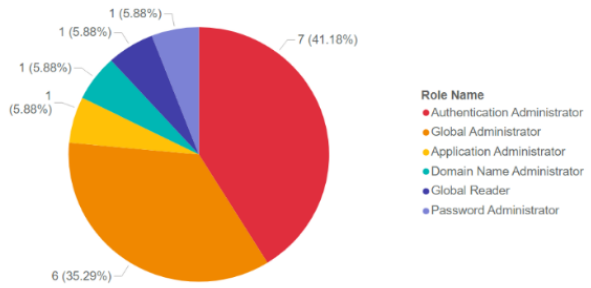
Identity and Access Security Summary

Review individuals with administrative and privileged access rights

Microsoft User Counts by Non-Privileged Admin Role



Microsoft User Counts by Privileged Admin Role



Administrators

Roles that provide permissions to manage Microsoft Entra resources, such as users, licenses, domains, etc.

Administrator Role	Privileged	User
Application Administrator	Privileged	Bianca Pisani
Authentication Administrator	Privileged	Adele Vance
Authentication Administrator	Privileged	Gerhart Moller
Authentication Administrator	Privileged	Grady Archie
Authentication Administrator	Privileged	Irvin Sayers
Authentication Administrator	Privileged	MOD Administrator
Authentication Administrator	Privileged	Patti Fernandez
Authentication Administrator	Privileged	Pradeep Gupta
Billing Administrator	-	Adele Vance
Billing Administrator	-	MOD Administrator
Domain Name Administrator	Privileged	MOD Administrator
Exchange Administrator	-	Adele Vance
Global Administrator	Privileged	Allan Deyoung
Global Administrator	Privileged	Isaiah Langer
Global Administrator	Privileged	Lidia Holloway
Global Administrator	Privileged	Microsoft Service Account
Global Administrator	Privileged	MOD Administrator
Global Administrator	Privileged	Nestor Wilke
Global Reader	Privileged	Adele Vance
Password Administrator	Privileged	Alex Wilber

Account Administration Activity

User accounts added, suspended, or deleted during the reporting period

New Accounts	Blocked Accounts	Deleted Accounts
(none)	Christie Cline	(none)
	Debra Berger	

Access Policies

Sets of guidelines that specify how access is managed and who may access key resources and information

Access Policy Name	Active State	Creation Date	Users Assigned	Users Excluded
Security Defaults	Off	-	39	0
Require multifactor authentication for guest access	On	Jan 9, 2024	0	0
Require multifactor authentication for admins	On	Nov 17, 2023	15	0
Block legacy authentication	On	Nov 5, 2023	39	0
MFA Policy 1	On	Apr 26, 2023	1	0
MFA Policy 2	On	Apr 26, 2023	8	13
Block access from specific location	Report-only	Jan 9, 2024	39	1
Require multifactor authentication for all users	Off	Nov 5, 2023	39	0
Require multifactor authentication for risky sign-ins	Off	Nov 5, 2023	39	0
Test policy	Off	Aug 1, 2023	13	0
Require password change for high-risk users	Off	Jul 14, 2023	39	1
Test App Control Policy	Off	Jun 25, 2023	39	13
Exchange Online Requires Compliant Device	Off	Apr 16, 2023	8	0
Office 365 App Control	Off	Apr 16, 2023	39	0

Sign-in Activity Summary

Risk State ● none

Risky Users

Users whose accounts are currently or were considered at risk of compromise. Risky users are investigated and remediated to prevent unauthorized access to resources

Risky Users/Alerts	Risk Level	Risk Detected	Current State
Alex Wilber — Admin confirmed user compromised	High	Nov 14, 2023, 9:07:54 AM	Confirmed compromised
MOD Administrator — Unfamiliar sign-in properties	Low	Dec 10, 2023, 8:40:47 AM	At risk
Christie Cline	Low	May 24, 2023, 10:39:32 AM	At risk

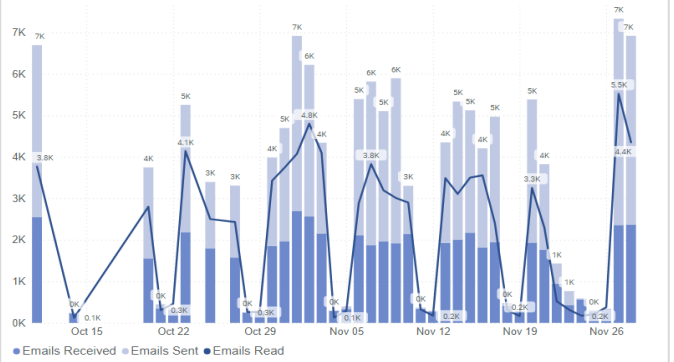
**Maximum of 50 risky users displayed. Risky User alerts are generated only for Microsoft Entra (formerly Azure Active Directory) premium licenses. Contact us to review the entire list and discuss licensing and remediation measures.*

Microsoft Email Security

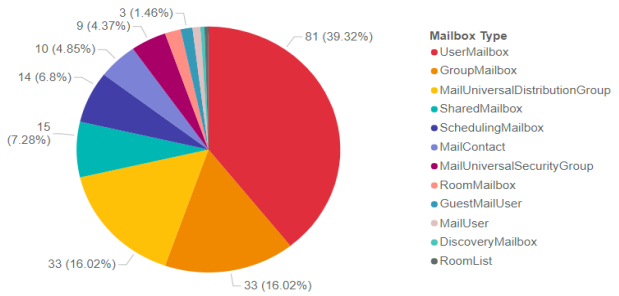
Exchange email messages and threats summary

Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024

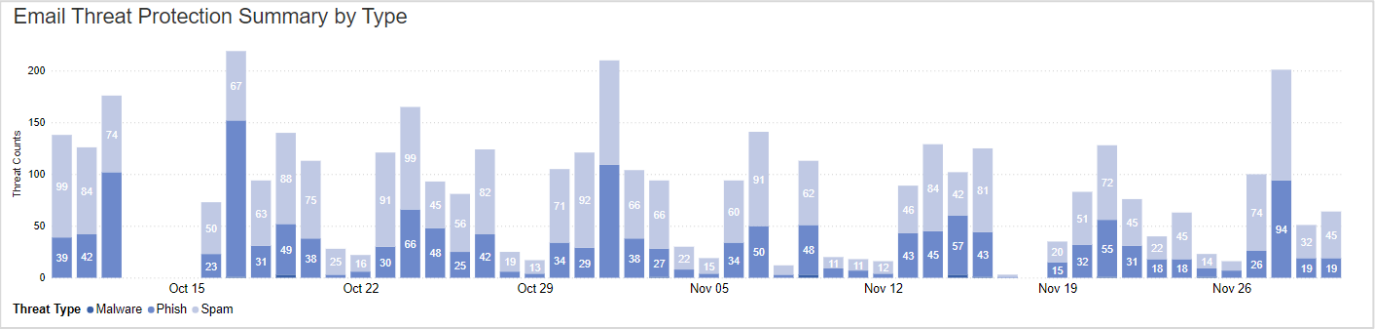
Email Activity Summary



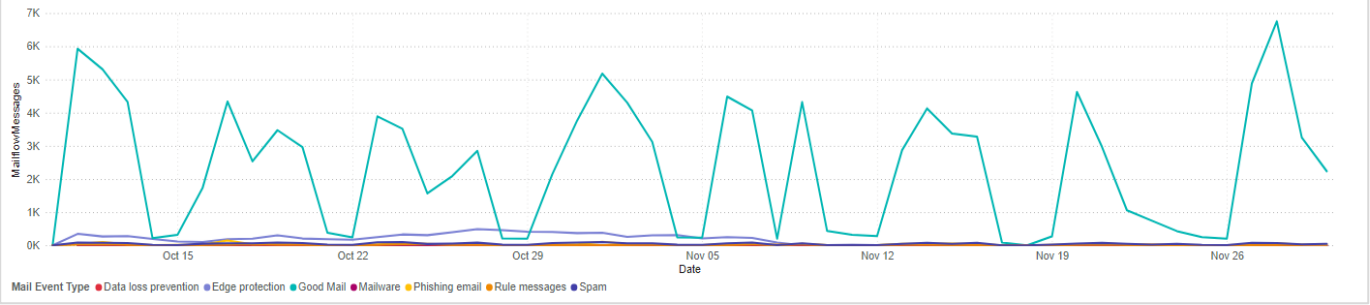
Mailbox Recipients Managed by Type



Email Threat Protection Summary by Type



Exchange Mail Flow Summary



Auto-Forwarding Email Rules for Admin Accounts

A common sign of a security breach is the existence of email forwarding rules assigned to admin accounts. We continually monitor internal and external forwarding rules for this reason.

Account Type	Forwarding Type	Rule Count
Administrator	External	1
Administrator	Internal	3

Top Email Received Counts by Recipient

Recipient Address	Messages Count
Stevens@MSDx327149.OnMicrosoft.com	7805
IrvinS@MSDx327149.OnMicrosoft.com	7690
LeeG@MSDx327149.OnMicrosoft.com	7673
JoniS@MSDx327149.OnMicrosoft.com	7419
Adams@MSDx327149.OnMicrosoft.com	7263
IsaiahL@MSDx327149.OnMicrosoft.com	7192
LidiaH@MSDx327149.OnMicrosoft.com	6869
Rainier@MSDx327149.OnMicrosoft.com	6282
GerhartM@MSDx327149.OnMicrosoft.com	6266
PattiF@MSDx327149.OnMicrosoft.com	5869
MeganB@MSDx327149.OnMicrosoft.com	5687
LynneR@MSDx327149.OnMicrosoft.com	5474
DebraB@MSDx327149.OnMicrosoft.com	5218
CameronW@MSDx327149.OnMicrosoft.com	4723
ms-serviceaccount@MSDx327149.OnMicrosoft.com	4642
AutomateB@MSDx327149.OnMicrosoft.com	4431
admin@MSDx327149.onmicrosoft.com	4416
AlexW@MSDx327149.OnMicrosoft.com	3923
BrianJ@MSDx327149.OnMicrosoft.com	3807
MiriamG@MSDx327149.OnMicrosoft.com	3790
GradyA@MSDx327149.OnMicrosoft.com	3711
PradeepG@MSDx327149.OnMicrosoft.com	3607
Crystal@MSDx327149.OnMicrosoft.com	3486
NestorW@MSDx327149.OnMicrosoft.com	3432
Total	**130675**

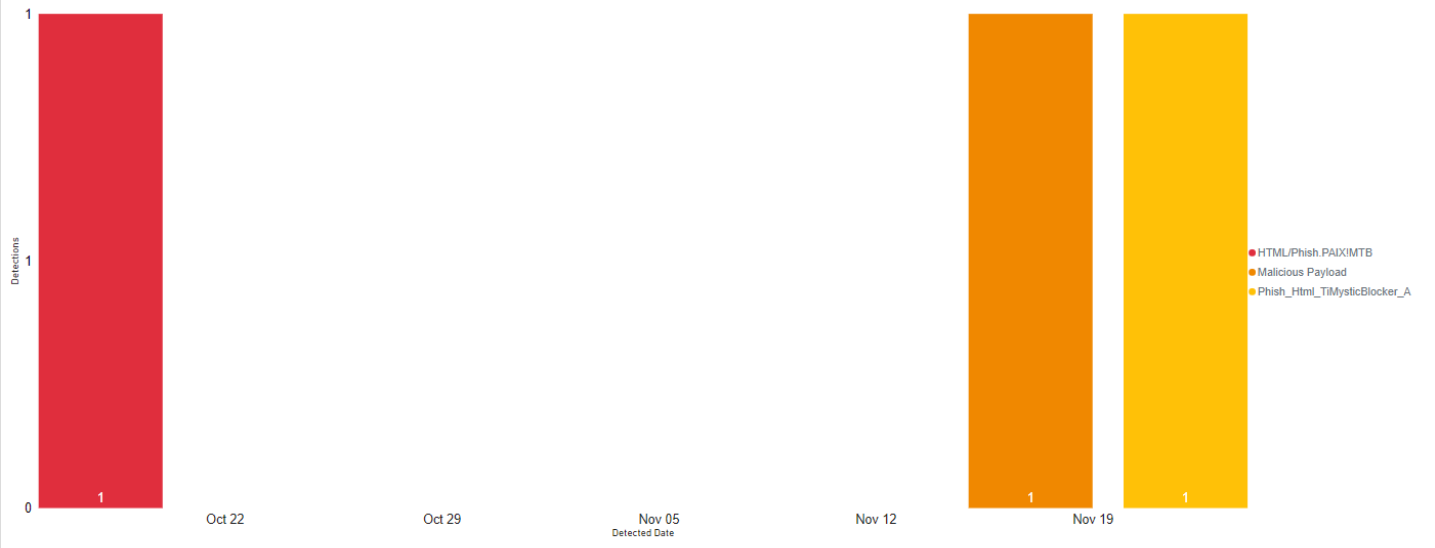
Top Spam Email Counts Received by Recipient

Recipient Address	Messages Count
LeeG@MSDx327149.OnMicrosoft.com	486
PattiF@MSDx327149.OnMicrosoft.com	473
admin@MSDx327149.onmicrosoft.com	443
Crystal@MSDx327149.OnMicrosoft.com	431
MeganB@MSDx327149.OnMicrosoft.com	420
IsaiahL@MSDx327149.OnMicrosoft.com	405
PradeepG@MSDx327149.OnMicrosoft.com	395
Adams@MSDx327149.OnMicrosoft.com	385
MiriamG@MSDx327149.OnMicrosoft.com	345
BrianJ@MSDx327149.OnMicrosoft.com	329
ms-serviceaccount@MSDx327149.OnMicrosoft.com	288
LidiaH@MSDx327149.OnMicrosoft.com	239
GradyA@MSDx327149.OnMicrosoft.com	211
LynneR@MSDx327149.OnMicrosoft.com	208
CameronW@MSDx327149.OnMicrosoft.com	204
DebraB@MSDx327149.OnMicrosoft.com	203
JoniS@MSDx327149.OnMicrosoft.com	198
Rainier@MSDx327149.OnMicrosoft.com	194
NestorW@MSDx327149.OnMicrosoft.com	160
AutomateB@MSDx327149.OnMicrosoft.com	152
Stevens@MSDx327149.OnMicrosoft.com	142
IrvinS@MSDx327149.OnMicrosoft.com	95
AlexW@MSDx327149.OnMicrosoft.com	81
GerhartM@MSDx327149.OnMicrosoft.com	63
Total	**6550**

Top Malware Email Received Counts by Recipient

Recipient Address	Messages Count
GerhartM@MSDx327149.OnMicrosoft.com	1
ms-serviceaccount@MSDx327149.OnMicrosoft.com	1
admin@MSDx327149.onmicrosoft.com	1
Total	**3**

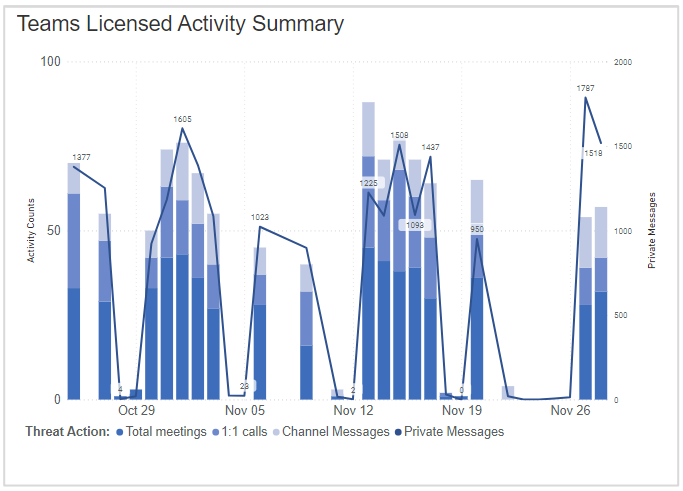
Top Malware Detections Received via Email

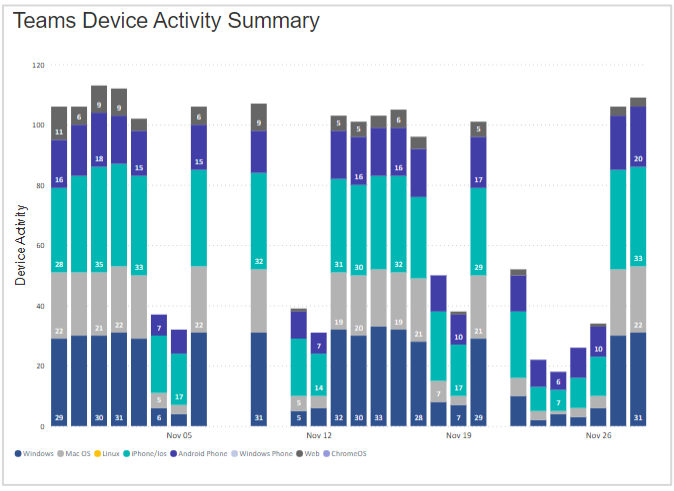


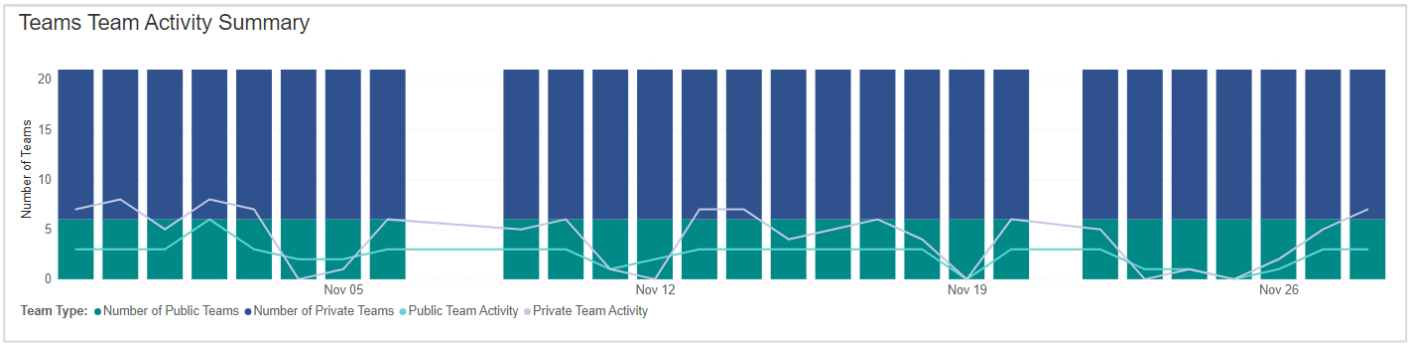
Microsoft Teams Security

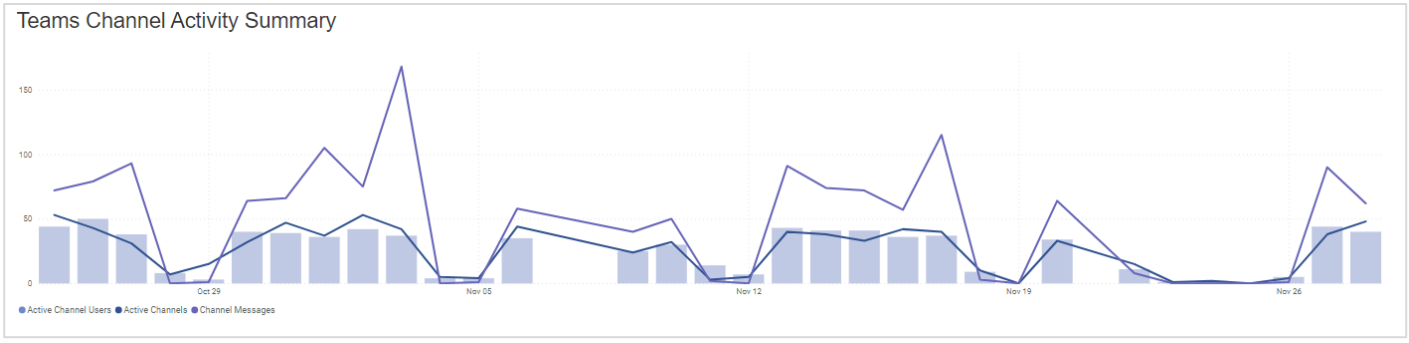
Microsoft Teams activity and security summary, including links and attachments

Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024









Microsoft Teams External and Guest Access Settings

Especially if team creation and administration is allowed by non-admin users, it's important to keep an eye on external and guest access settings.

Domain	Allowed	Blocked	Communication Allowed with Non-Organization Teams Users	Communication Allowed with External Teams Users	Communication Allowed with Skype Users	Guest Access Allowed

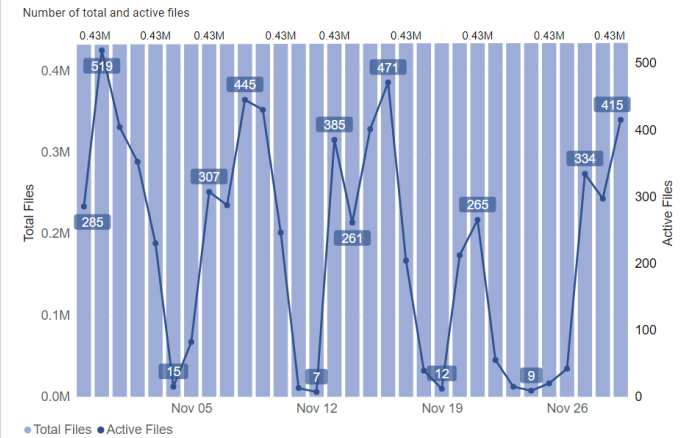
Microsoft File Security

Microsoft file storage and protection summary

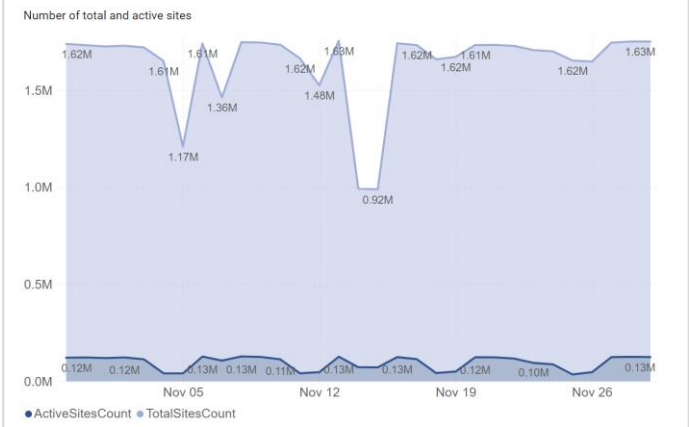
Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024

Storage

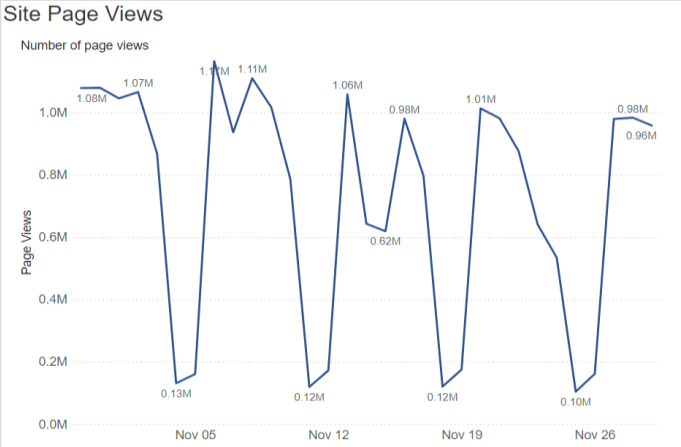
Files



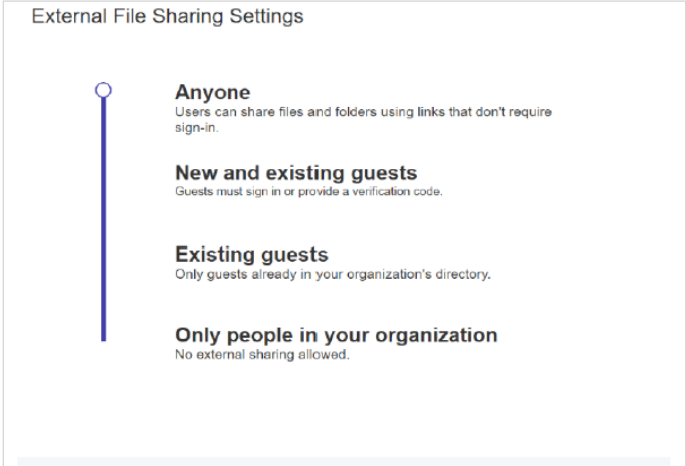
Sites



Site Page Views



External File Sharing Settings

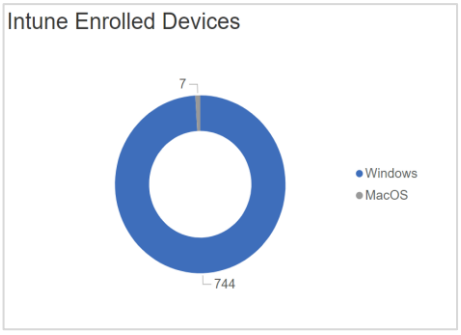


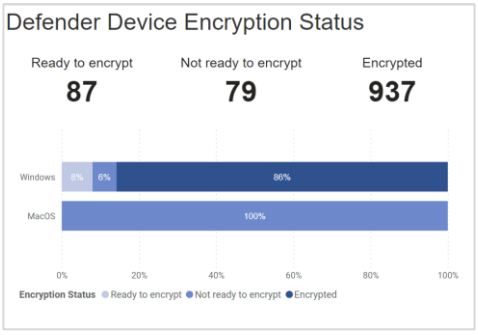
Endpoint Management Security

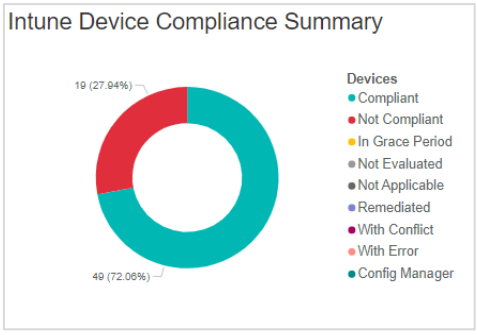
Microsoft Intune and device security summary

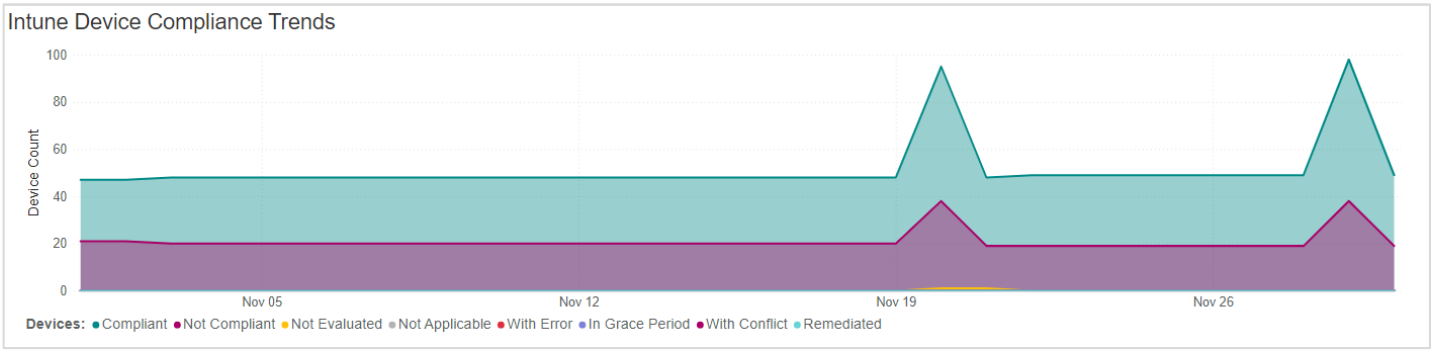
Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024

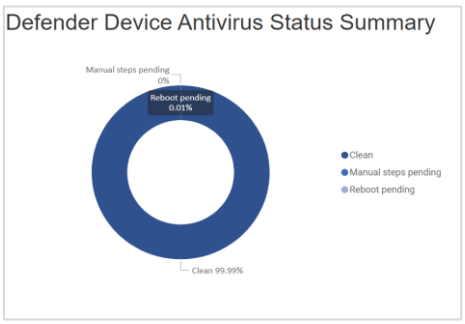
Intune Enrolled Devices	Windows	MacOS	Android	IOS	Windows Mobile	Others
1103	523	7	0	542	0	29

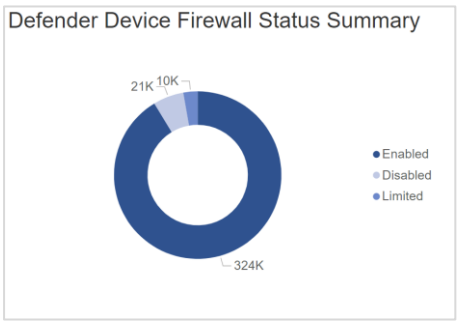


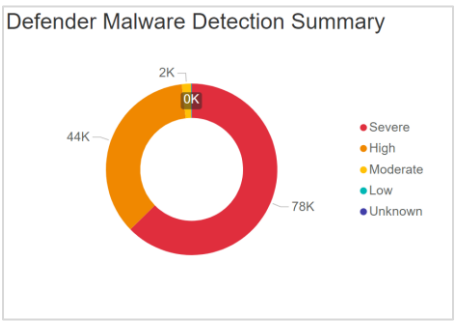












Microsoft 365 Software Licensing

All Microsoft software license SKU and usage summary

Contoso Corp | Reporting Period: October1, 2023 through December 31, 2024

Current M365 Licenses

M365 Product	Subscription Type	Status	Next Lifecycle Date	Qty Licensed	Assigned	Available
Enterprise Mobility + Security E5	Trial	Enabled	Will be expired on May 16, 2024	20	20	0
Microsoft 365 E5	Trial	Enabled	Will be expired on Mar 13, 2024	20	20	0
Microsoft 365 E5 Compliance	Trial	Enabled	Will be expired on May 16, 2024	20	20	0
Microsoft Power Automate Free	Free	Enabled	Never expires	10000	1	9999
Microsoft Power Automate Free	Free	Enabled	Never expires	10000	1	9999
Microsoft Power Automate Free	Free	Enabled	Never expires	10000	0	10000
Microsoft Power Automate Free	Free	Enabled	Never expires	10000	0	10000
Office 365 E3	Trial	Enabled	Will be expired on May 16, 2024	2	1	1
Office 365 E5	Trial	Enabled	Will be expired on May 16, 2024	20	20	0
Privacy Management - risk	Trial	LockedOut	Subscription is locked. Please contact Microsoft	0	0	0
Privacy Management - subject rights request (50)	Trial	LockedOut	Subscription is locked. Please contact Microsoft	0	0	0
Rights Management Service Basic Content Protection	Free	Enabled	Never expires	1	0	1
Windows 10/11 Enterprise E3	Trial	Enabled	Will be expired on May 16, 2024	20	2	18

License Usage in Your Market Segment

Licenses used by companies in your industry with higher Secure Scores than yours

M365 Product	Market Segment % Usage
Microsoft 365 Business Standard	50%
Microsoft Power Automate Free	46%
Exchange Online (Plan 1)	38%
Microsoft 365 Business Basic	38%
Enterprise Mobility + Security E5	31%
Microsoft 365 Business Premium	25%
Windows Store for Business	25%
Office 365 E5	20%
Microsoft 365 E5 Compliance	20%
Microsoft 365 Apps for Business	13%
Microsoft Defender for Office 365 (Plan 1)	13%
Microsoft Teams Exploratory	13%
Power BI (free)	13%
Exchange Online (Plan 2)	8%
Office 365 E3	8%
Windows 10/11 Enterprise E3	7%

Appendix – Secure Score History Detail

Detailed changes to your Microsoft 365 Secure Score over the reporting period

Secure Score Change History

Summary of Secure Score Changes

Recommendation Influencing the Score	Score Change	Max Score Change	Resulting Points	Number of Changes	Previous Status	New Status
Set action to take on high confidence spam detection	+5.0	-	5/5	1	To address	Completed
Set action to take on phishing detection	+5.0	-	5/5	1	To address	Completed
Enable impersonated domain protection	+3.2	-	8/8	4	To address	Completed
Enable impersonated user protection	+3.2	-	8/8	4	To address	Completed
Ensure that intelligence for impersonation protection is enabled	+3.2	-	8/8	4	To address	Completed
Move messages that are detected as impersonated users by mailbox intelligence	+3.2	-	8/8	4	To address	Completed
Set the phishing email level threshold at 2 or higher	+3.2	-	8/8	4	To address	Completed
Quarantine messages that are detected from impersonated domains	+2.4	-	6/6	5	To address	Completed
Quarantine messages that are detected from impersonated users	+2.4	-	6/6	4	To address	Completed
Enable the domain impersonation safety tip	+1.2	-	3/3	4	To address	Completed
Enable the user impersonation safety tip	+1.2	-	3/3	4	To address	Completed
Enable the user impersonation unusual characters safety tip□	+1.2	-	3/3	4	To address	Completed
Ensure that an anti-phishing policy has been created	+1.2	-	3/3	4	To address	Completed
Restrict anonymous users from joining meetings	+1.0	-	1/1	1	To address	Completed
Block users who reached the message limit	+0.4	-	1/1	5	To address	Completed
Set automatic email forwarding rules to be system controlled	+0.4	-	1/1	4	To address	Completed
Ensure 'Self service password reset enabled' is set to 'All'	+0.13	-	0.35/1	4	To address	To address
Enable Conditional Access policies to block legacy authentication	-7.76	-	0.24/8	1	Completed	To address

Appendix – Microsoft 365 Security Glossary

M365 security terms key to understanding the data in this report

This glossary is designed to help you understand key security terms and features within Microsoft 365. It is a mix of standard IT security terms, some that are specific to the Microsoft ecosystem, and the names and descriptions of security-related products designed to keep your accounts and data safe.

Anti-Phishing – Anti-phishing refers to a set of security measures aimed at detecting and preventing phishing attacks. In M365, anti-phishing features help identify fraudulent emails or websites designed to steal sensitive information, such as usernames and passwords.

Advanced Threat Analytics (ATA) – Advanced Threat Analytics is a technology that detects and analyzes suspicious activities and threats within your network, helping to protect against advanced attacks.

Advanced Threat Protection (ATP) – Advanced Threat Protection offers additional layers of security against sophisticated threats. It includes features like ATP for email and ATP for SharePoint to detect and mitigate advanced threats.

Anti-Malware – Anti-malware in M365 refers to the protection against malicious software or malware. It includes tools and mechanisms to detect and remove viruses, ransomware, and other types of harmful software from your M365 environment.

Azure Active Directory (Azure AD) – Azure Active Directory is Microsoft's cloud-based identity and access management service. It provides authentication and authorization services for M365, ensuring secure access to resources and applications.

Azure Information Protection (AIP) – Azure Information Protection is a Microsoft technology that helps classify and protect documents and emails based on their sensitivity. It ensures that sensitive information is encrypted and restricted to authorized users.

Conditional Access Policy – Conditional Access Policies in M365 allow you to set specific conditions that must be met before granting access to resources. These policies provide granular control over who can access what, where, and when, based on factors like location, device, and user behavior.

Data Encryption – Data encryption in M365 involves encoding data to make it unreadable without the appropriate decryption key. It ensures that even if data is intercepted, it remains secure and confidential.

Data Governance – Data Governance encompasses a set of policies and technologies, including Microsoft 365 Compliance Center, that help organizations manage data access, retention, and compliance with regulatory requirements.

Data Loss Prevention (DLP) – Data Loss Prevention helps prevent sensitive data from being shared or leaked outside your organization. It allows you to create policies that automatically detect and protect sensitive information, such as credit card numbers or confidential documents.

Endpoint Security – Endpoint security focuses on protecting individual devices (endpoints) within your organization, such as computers and mobile devices. M365 offers solutions like Microsoft Defender for Endpoint to secure these endpoints.

Identity and Access Management (IAM) – IAM solutions within Azure AD, such as Azure Active Directory Identity Protection, are essential for managing user identities and access to M365 resources securely.

Identity Protection – Identity Protection focuses on securing user identities within M365. It includes features like risk-based authentication, password protection, and identity threat detection to safeguard against unauthorized access.

Incident Response Plan – An Incident Response Plan outlines the procedures to follow when a security incident occurs. It includes steps for identifying, containing, mitigating, and recovering from security breaches within your M365 environment.

Information Protection – Information Protection is a set of tools and features that allow you to classify, label, and protect sensitive data across M365 services. It helps control who can access and share sensitive information.

Insider Threat – An insider threat is a security risk that originates from within your organization. M365 includes features to detect and mitigate insider threats, such as unauthorized data access by employees.

Microsoft Cloud App Security (MCAS) – Microsoft Cloud App Security is a comprehensive security solution that provides visibility, control, and threat protection for cloud applications and services, including those used within M365.

Microsoft Sentinel – Microsoft Sentinel, part of Azure Sentinel, is a cloud-native SIEM and SOAR (Security Orchestration, Automation, and Response) solution that collects and analyzes security data from M365 and other sources for threat detection and response.

Microsoft Threat Protection (MTP) – Microsoft Threat Protection is a comprehensive security platform that combines various Microsoft security technologies, such as Defender ATP, Office 365 ATP, and Azure ATP, to provide end-to-end threat protection.

Multi-Factor Authentication (MFA) – MFA adds an extra layer of security by requiring users to provide two or more forms of verification before accessing M365 services. This typically includes something the user knows (password) and something they have (e.g., a mobile app or a hardware token).

Safe Attachments – Safe Attachments provides protection by scanning email attachments for malware and other threats before they are delivered to your inbox. This feature ensures that malicious attachments are detected and quarantined.

Safe Links – Safe Links is a feature that safeguards against malicious URLs in emails and documents. It scans links in real-time and warns users or blocks access to harmful websites, helping to prevent users from clicking on potentially dangerous links.

Secure Score – Microsoft Secure Score is a tool that assesses your organization's security posture within M365. It provides recommendations and a numerical score, helping you improve your overall security by addressing vulnerabilities and implementing best practices.

Security Baseline – A security baseline is a set of security settings recommended by Microsoft as a starting point for securing M365. It ensures that your environment has a minimum level of security configured.

Security Compliance – Security compliance in M365 refers to adhering to security standards and regulations relevant to your industry. Tools like Microsoft Compliance Manager help you assess and maintain compliance within your organization.

Security Defaults – Security Defaults are pre-configured security settings recommended by Microsoft to enhance the overall security of your M365 environment. These settings include features like multi-factor authentication (MFA) and block legacy authentication methods.

Security Information and Event Management (SIEM) – SIEM solutions like Microsoft Sentinel collect and analyze security-related data from various sources within M365 to provide a centralized view of security events and incidents. It helps detect and respond to security threats in real-time.

Threat Intelligence – Threat Intelligence in M365 involves monitoring and analyzing data to identify and respond to cybersecurity threats. It provides real-time information about emerging threats and vulnerabilities, enabling proactive security measures.

Unified Endpoint Management (UEM) – UEM solutions like Microsoft Intune offer centralized management and security for all types of devices, including PCs, mobile devices, and IoT devices, ensuring they are compliant and secure.

Zero Trust Security Model – The Zero Trust security model assumes that no one, whether inside or outside the organization, can be trusted by default. It enforces strict identity verification and access controls, even for trusted users.

Zero-Day Vulnerability – A zero-day vulnerability is a security flaw in software that is unknown to the software vendor and, therefore, unpatched. Microsoft regularly releases patches and updates through technologies like Windows Update to address such vulnerabilities.

Appendix – Understanding your Secure Score

Details on how to interpret, utilize and manage your security using Microsoft Secure Score

---

What is Microsoft Secure Score and Why Does It Matter?

Microsoft Secure Score is a tool that helps you measure and improve your security posture across Microsoft 365 products and services. It is a numerical score based on how well you have implemented security best practices and recommendations in your organization. The higher your score, the more secure your environment is.

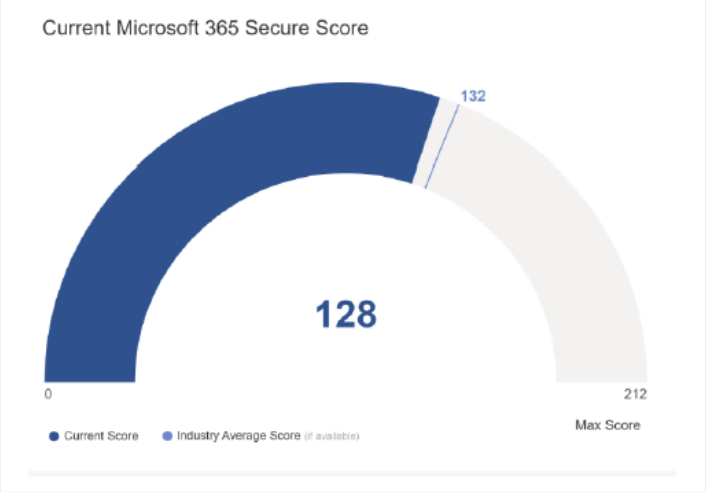
The score also represents a simplified framework for meeting or exceeding global IT security standards set forth by standards bodies like the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO 27001/27002), SOC 2, Essential 8, and others. In many ways, Microsoft Secure Score is a hybrid of each of these standards as they apply to the M365 ecosystem.

Secure Score itself is not a static number, but a dynamic one that changes as your security settings and actions change. It also reflects the evolving threat landscape and the latest security guidance from Microsoft. You can use Secure Score to track your progress over time and compare your score with other organizations in your industry or region.

Secure Score is not a definitive measure of your security, but a helpful indicator that can help you identify and prioritize security improvements. It can also help you communicate your security status and goals to your stakeholders, such as your employees, customers, and partners.

How to Interpret your Secure Score

Secure Scores are presented as a combination of the current score, the maximum possible score, and the percentage of the maximum score you have achieved. It can also be shown over time, indicating how it has changed over time and how you compare with the average score of your industry.



Your current score is calculated based on the security controls we have enabled and the security actions we have taken in your Microsoft 365 environment. Each control and action has a different weight and impact on your score, depending on its importance and effectiveness. For example, enabling multi-factor authentication for all users has a higher impact than enabling it for only some users.

Your maximum score is the highest score you can achieve if you implement all the security recommendations that apply to your organization. The maximum score varies depending on the Microsoft 365 products and services you have and the licenses you have purchased. For example, if you have Microsoft Defender for Endpoint, you can get a higher maximum score than if you don't.

Your percentage score is the ratio of your current score to your maximum score. It shows you how much of your security potential has been realized. A higher percentage score means you have implemented more security best practices and

About This Report

A partnership for protecting your cloud applications and data

As a key stakeholder in your business, you know how vital it is to safeguard your cloud applications and data from cyber threats. You also know how challenging it can be to keep up with the evolving security landscape and the best practices for securing your cloud environment. That's why you have partnered with AAA Architects to help you with your IT security needs.

We are committed to providing you with the highest level of IT security services and support. We work with you to understand your business goals, your cloud infrastructure, and your security requirements. We design, implement, and monitor security controls that are tailored to your specific needs and aligned with industry standards and regulations. We also provide you with periodic IT security review reports, like this one, that give you an overview of your current security posture, identify any gaps or issues, and recommend actions for improvement.

But IT security is not a one-time project or a static state. It is an ongoing process that requires constant vigilance, adaptation, and collaboration. Cyber threats are constantly changing and becoming more sophisticated. Security controls need to be regularly updated and tested to ensure they are effective and efficient. And your business needs and goals may also change over time, requiring adjustments to your security strategy and policies.

That's why we see our relationship with you as a partnership, not just a service. We are here to help you not only with the technical aspects of IT security, but also with the strategic and organizational ones. We want to help you strike the right balance between security and productivity, between compliance and innovation, between risk and opportunity. We want to help you create a security culture that empowers your employees, customers, and partners to work securely and confidently in the cloud.

To achieve this, we need your active involvement and feedback. We need you to share with us your business vision, your challenges, and your expectations. We need you to review our reports, follow our recommendations, and help us implement our action plans. We need you to communicate with us regularly, ask questions, and raise concerns. And we need you to support us in educating and training your staff on security best practices and policies.

Together, we can make your cloud applications and data more secure, resilient, and valuable. We appreciate your trust and your partnership.

Prepared for

Contoso Corp on Sunday, January 28, 2024