Microsoft 365 Quarterly Security Summary Report

Prepared for Salty Soul Foundation

Date: Friday, November 14, 2025

Reporting period: July 1, 2025 through September 30, 2025

Report Summary

To safeguard and ensure the continuity of your business it is essential to protect your applications and data. At Tyrell Technologies, 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.

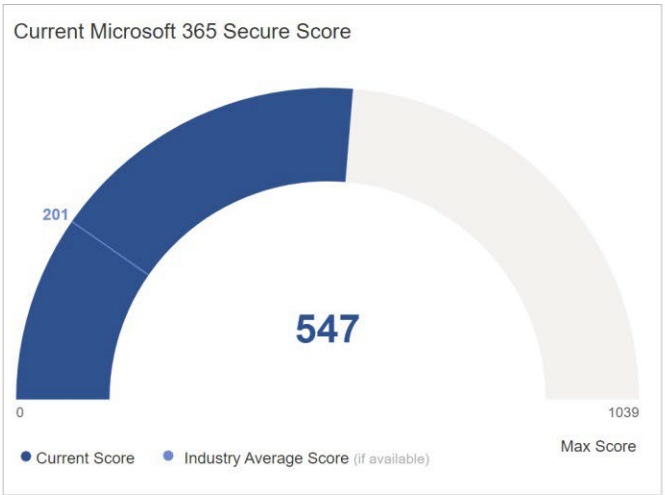
Table of Contents

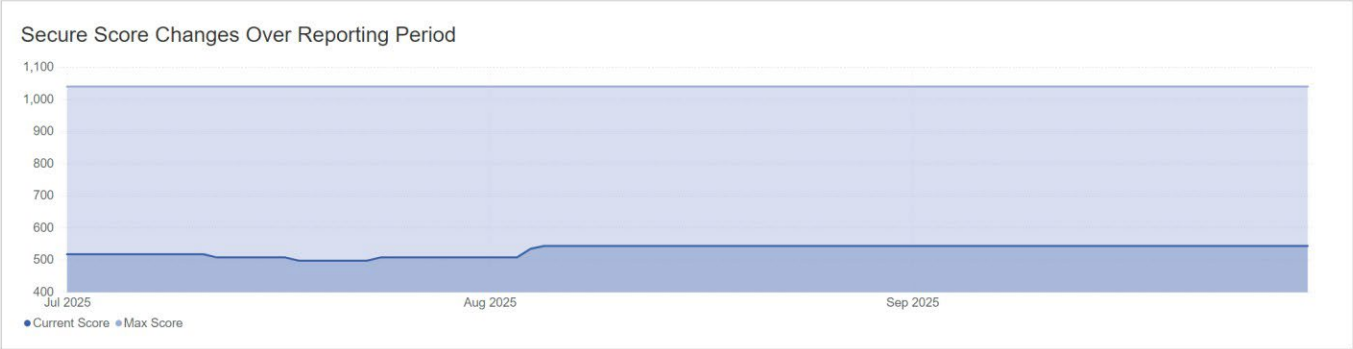
***Note**: Due to Microsoft's archiving policies or the date of initial reporting data activation, historical data represented in this report may not extend all the way back to the beginning of the reporting period. This will be remedied over time as data continues to be collected.*

Security Summary

Microsoft Secure Score is an overall representation of your Microsoft 365 security posture

Salty Soul Foundation | Reporting period: July 1, 2025 through September 30, 2025





Net Secure Score Change	Emails Received Activity	Emails Quarantined
+25.84 (between the reporting period start/end date)	**5348**	**225**

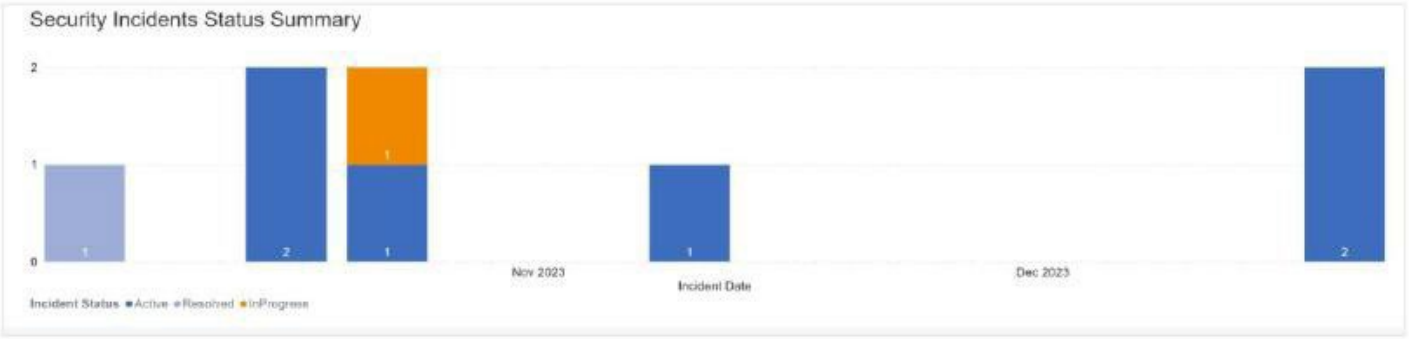
Malware Emails Blocked	Spam Emails Blocked	Phish Emails Blocked
0	**860**	**258**

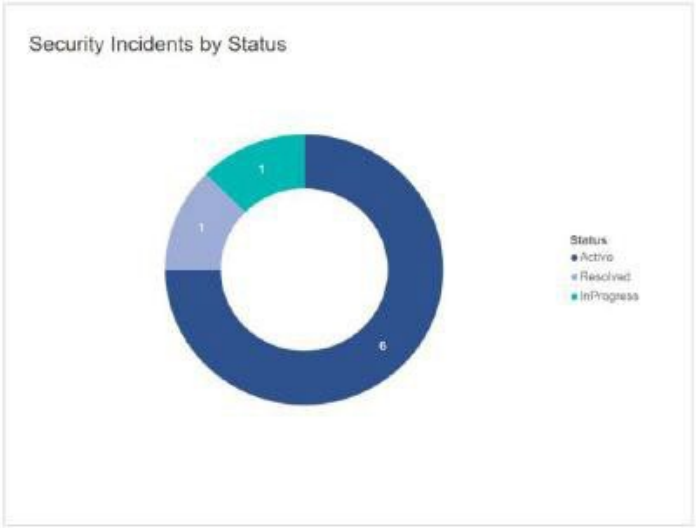
Security Support Activity Summary

Summary of monitoring and M365 incident/alert remediations

Salty Soul Foundation | Reporting period: July 1, 2025 through September 30, 2025

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 for your industry to help stay on top of current developments in IT security

From Human to Cyborg: Cybersecurity Visionary Len Noe Unveils Explosive Documentary 'I Am Machine' at Hacker Halted

Len Noe, a prominent ethical hacker, premiered his documentary 'I Am Machine' at the Hacker Halted 2025 conference, which focuses on the intersection of human identity and machine augmentation within the context of cybersecurity and ethics. The conference, themed 'Order from Chaos,' aims to address the complexities of modern cyber threats and emphasizes the need for resilience and clarity in cybersecurity practices. Noe's documentary and keynote address challenge traditional views on security and technology, highlighting the evolving relationship between humans and machines.

The Manila Times

ODNI reforms to disband cyber threat intel unit

ODNI is disbanding the Cyber Threat Intelligence Integration Center (CTIIC) as part of broader reforms aimed at reducing inefficiencies and saving costs. The decision, driven by Director Tulsi Gabbard, is based on the belief that the CTIIC is redundant due to existing capabilities within the National Intelligence Council and other Executive Branch entities. Critics argue that this move undermines U.S. cyber capabilities and the ability to respond to real-time threats, while supporters claim it streamlines operations and refocuses the agency on its core mission.

Federal News Network

Angered consumers sue after cyberattack at NY Business Council

Numerous lawsuits have emerged following a cyberattack on the New York Business Council, indicating significant consumer anger and concern over the incident. The lawsuits suggest a pattern in the claims, highlighting the impact of the breach on affected consumers and the potential consequences for the organization involved.

Times Union on MSN.com

Noem fires two dozen FEMA employees over alleged cybersecurity gaps

Homeland Security Secretary Kristi Noem has dismissed two dozen FEMA IT employees, including senior leaders, due to their alleged failure to adhere to security protocols, which has raised concerns about the protection of sensitive data.

CNN on MSN.com

Russia is quietly churning out fake content posing as US news

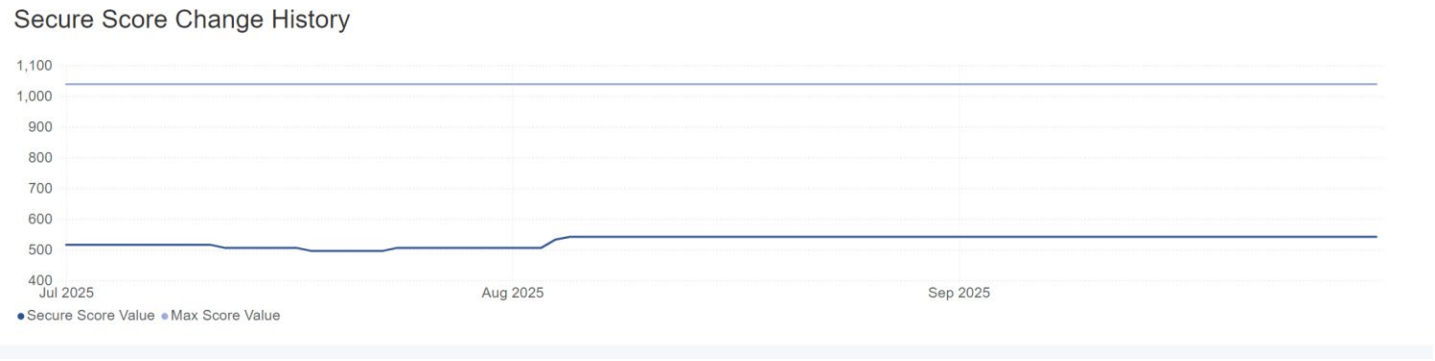
A pro-Russian propaganda group is exploiting significant news events to disseminate disinformation by impersonating reputable US news outlets. This tactic highlights the ongoing threat of misinformation campaigns and the challenges they pose to public trust in media.

POLITICO on MSN.com

Secure Score History

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

Salty Soul Foundation | Reporting period: July 1, 2025 through September 30, 2025



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
Jul 1, 2025	Sep 30, 2025	516.66	542.5	+25.84	1039.0	1039.0	-	49.73%	52.21%	+2.49%

Recommendation Influencing the Score	Score Change	Max Score Change	Resulting Points	Number of Changes	Previous Status	New Status
Turn on real-time protection	+5.0	-	10/10	1	To address	Completed
Block JavaScript or VBScript from launching downloaded executable content	+4.5	-	9/9	1	To address	Completed
Block Office applications from creating executable content	+4.5	-	9/9	1	To address	Completed
Block all Office applications from creating child processes	+4.5	-	9/9	1	To address	Completed
Block executable content from email client and webmail	+4.5	-	9/9	1	To address	Completed
Encrypt all BitLocker-supported drives	+4.5	-	9/9	1	To address	Completed
Turn on PUA protection in block mode	+4.5	-	9/9	1	To address	Completed
Change service executable path to a common protected location	+2.67	-	8/8	1	To address	Completed
Disable the built-in Guest account	+2.67	-	8/8	1	To address	Completed
Enable Microsoft Defender Antivirus real-time behavior monitoring	+2.5	-	5/5	1	To address	Completed
Enable 'Network Protection'	+1.33	-	4/8	1	To address	To address
Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile	+0.33	-	1/2	1	To address	To address
Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile	+0.33	-	1/2	1	To address	To address
Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile	+0.33	-	1/2	1	To address	To address

Recommendation Influencing the Score	Score Change	Max Score Change	Resulting Points	Number of Changes	Previous Status	New Status
Disable 'Autoplay' for all drives	-1.33	-	4/8	1	To address	To address
Disable SMBv1 client driver	-1.33	-	4/8	1	To address	To address
Disable the built-in Administrator account	-1.33	-	4/8	1	To address	To address
Fix unquoted service path for Windows services	-1.33	-	4/8	1	To address	To address
Secure Microsoft Defender Firewall domain profile	-1.5	-	4.5/9	1	To address	To address
Secure Microsoft Defender Firewall public profile	-1.5	-	4.5/9	1	To address	To address
Secure Microsoft Defender firewall private profile	-1.5	-	4.5/9	1	To address	To address
Enable Automatic Updates	-2.5	-	0/5	1	To address	To address
Enable EDR in block mode	-4.0	-	0/8	1	To address	To address

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

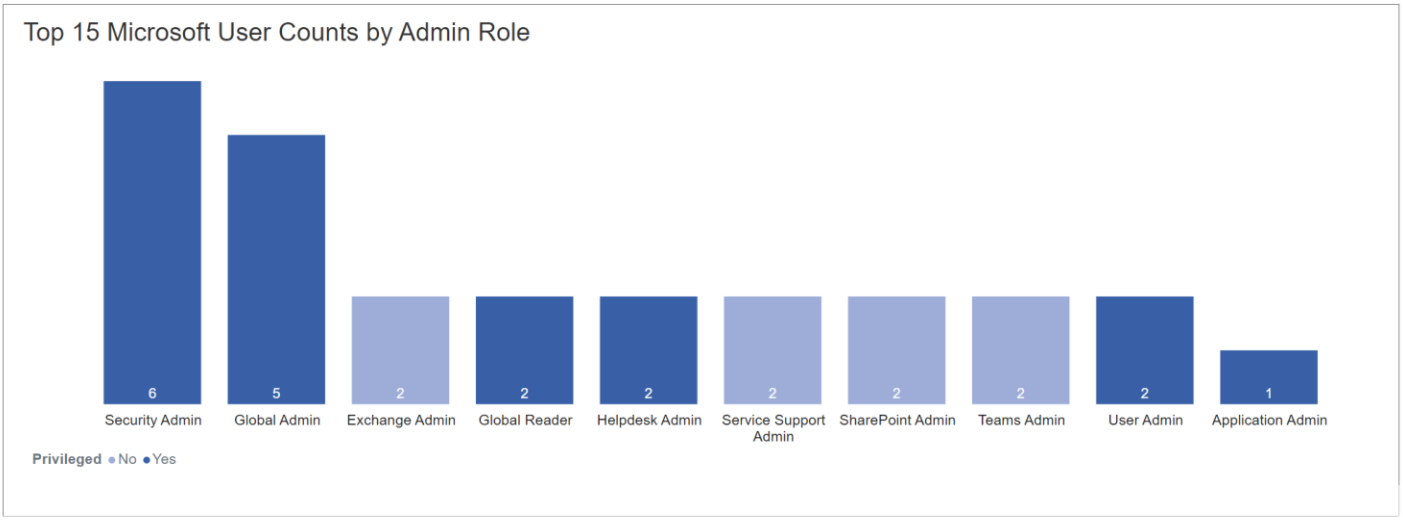
Salty Soul Foundation | Reporting period: July 1, 2025 through September 30, 2025

Points Available	Recommendation Action	Protects Against
9	Use advanced protection against ransomware	
9	Block abuse of exploited vulnerable signed drivers	
9	Block persistence through WMI event subscription	
9	Block executable files from running unless they meet a prevalence, age, or trusted list criterion	
9	Block Adobe Reader from creating child processes	
9	Block credential stealing from the Windows local security authority subsystem (lsass.exe)	
9	Block execution of potentially obfuscated scripts	
9	Block untrusted and unsigned processes that run from USB	
9	Block process creations originating from PSExec and WMI commands	
9	Block Win32 API calls from Office macros	
9	Enable Microsoft Defender Antivirus email scanning	
9	Block Office applications from injecting code into other processes	
9	Block Office communication application from creating child processes	
8	Disable 'Allow Basic authentication' for WinRM Service	
8	Enable 'Local Security Authority (LSA) protection'	
8	Disable 'Allow Basic authentication' for WinRM Client	
8	Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM & NTLM'	
8	Ensure that intelligence for impersonation protection is enabled	
8	Enable impersonated user protection	
8	Set the phishing email level threshold at 2 or higher	
	Showing 20 of 96 recommended actions. Completing all others will allow you to get 319.5 additional points.	

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.

Administrative Roles Summary

Review individuals with admin access rights and other user accounts administered during the reporting period



Administrators

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

Administrator Role	Privileged	User
Application Administrator	Privileged	Alex Chacko
Cloud Application Administrator	Privileged	Alex Chacko
Exchange Administrator	-	John Helms
Exchange Administrator	-	John Helms - Salty Soul
Global Administrator	Privileged	Alex Chacko
Global Reader	Privileged	John Helms
Global Reader	Privileged	John Helms - Salty Soul
Helpdesk Administrator	Privileged	John Helms
Helpdesk Administrator	Privileged	John Helms - Salty Soul
Security Administrator	Privileged	Alex Chacko
Security Administrator	Privileged	Jimmy B
Security Administrator	Privileged	John Helms
Security Administrator	Privileged	John Helms - SSF
Security Administrator	Privileged	Nishant
Security Administrator	Privileged	Sachin T
Service Support Administrator	-	John Helms
User Administrator	Privileged	John Helms - Salty Soul

Account Administration Activity

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

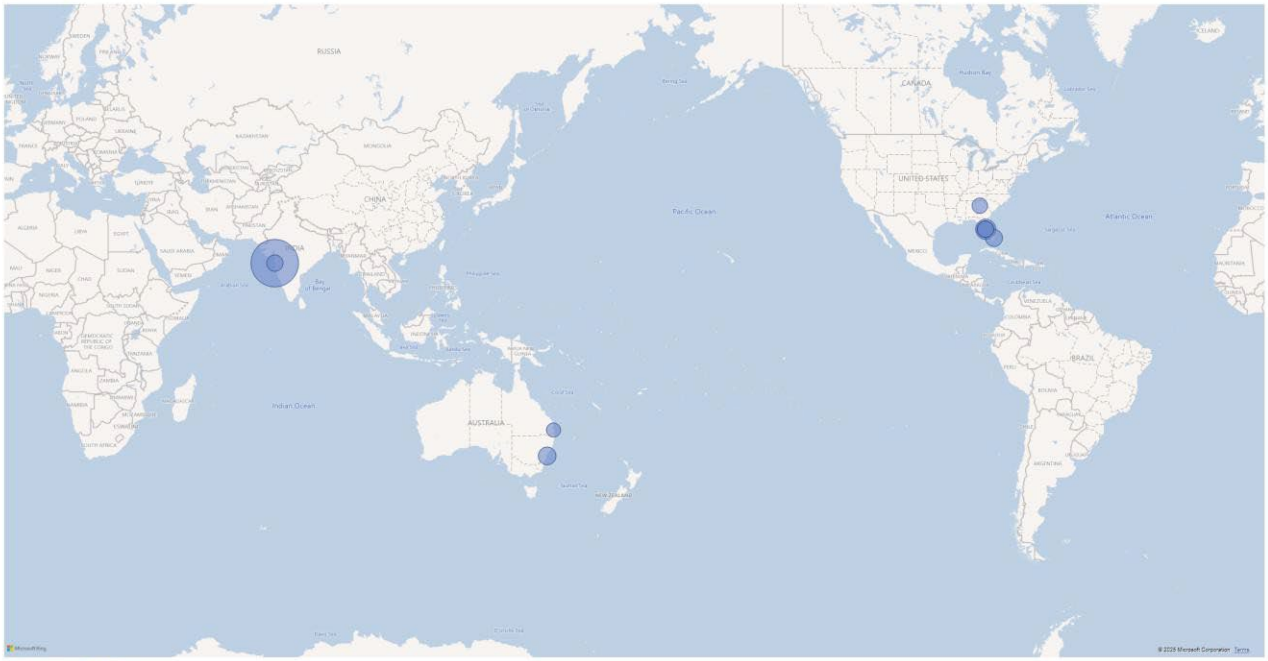
New Accounts	Blocked Accounts	Deleted Accounts
Shashi	(none)	(none)

System Access Security Summary

Review successful and risky sign-in activity and access policies

Sign-In Activity

Successful Logins



Risk State none

Failed Logins

Risk State none

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	On	-	17	0

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

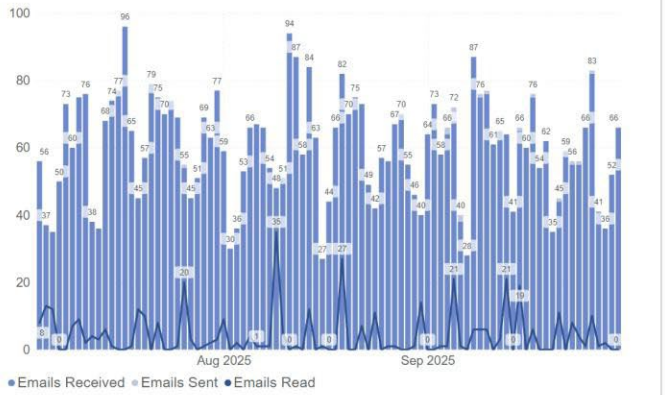
**Maximum of 50 risky users displayed. Risky User alerts are generated only for Microsoft Entra Id premium licenses. Contact us to review the entire list and discuss licensing and remediation measures.*

Microsoft Email Security

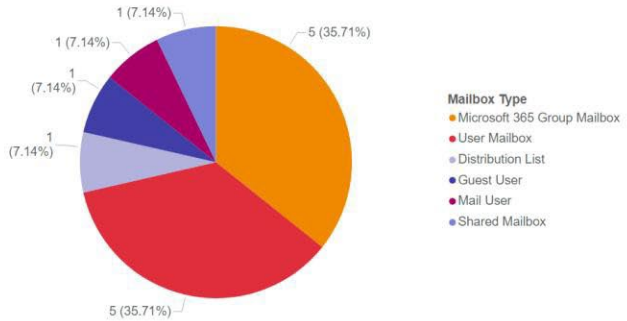
Exchange email messages and threats summary

Salty Soul Foundation | Reporting period: July 1, 2025 through September 30, 2025

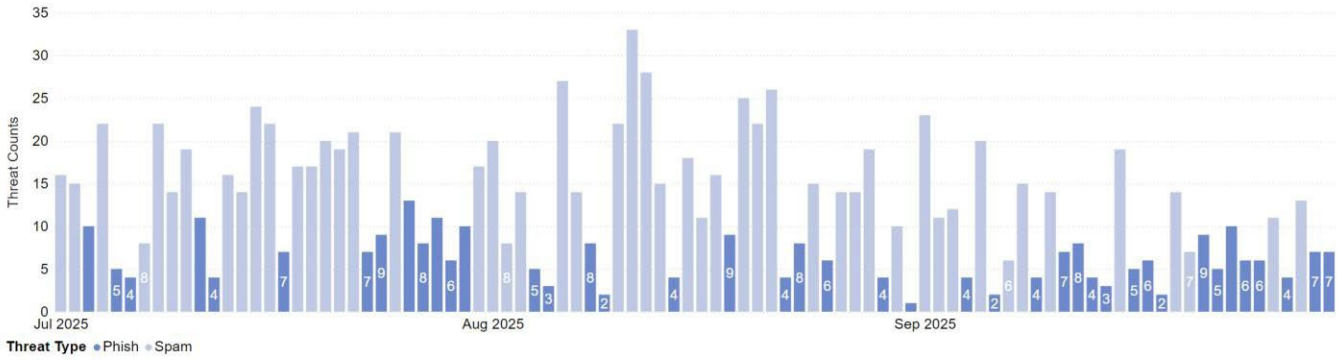
Email Activity Summary



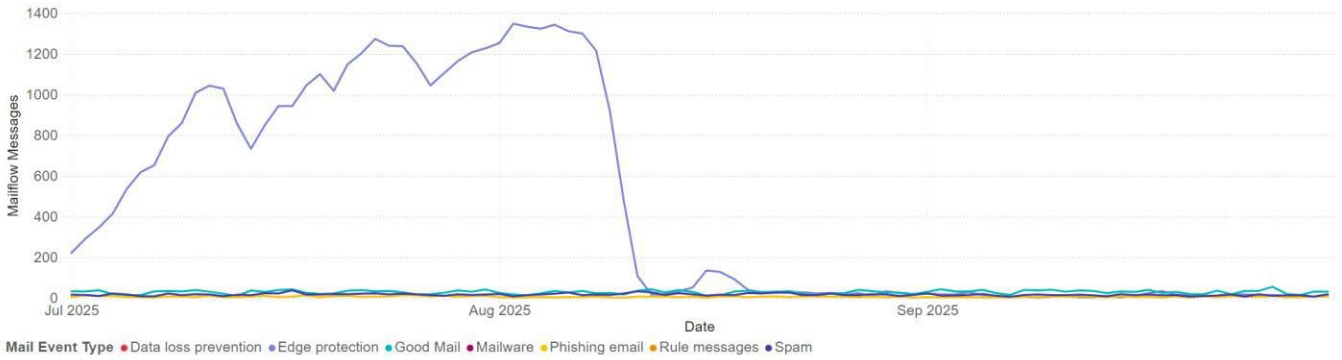
Mailbox Recipients Managed by Type



Email Threat Protection Summary by Type



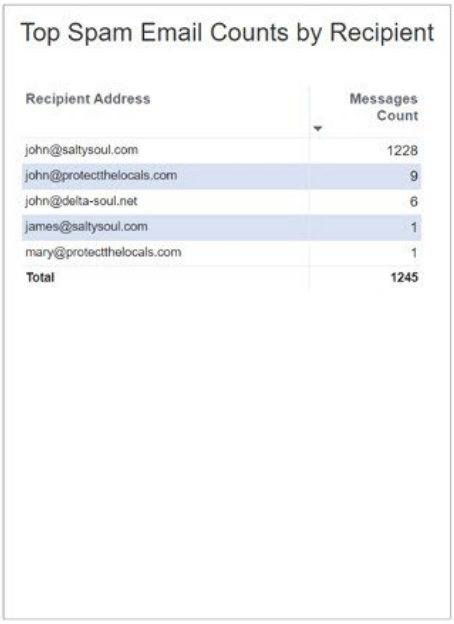
Exchange Mail Flow Summary

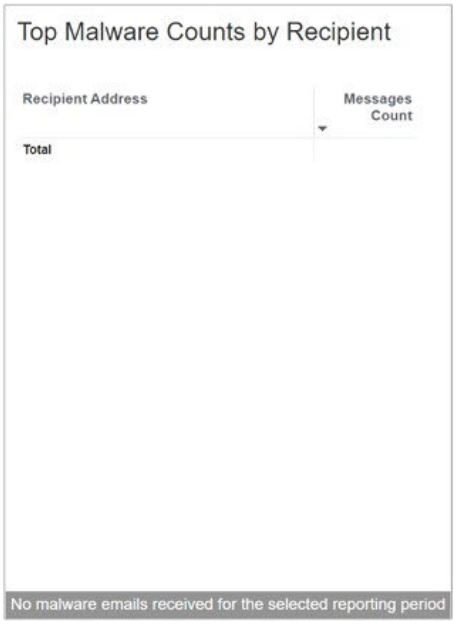


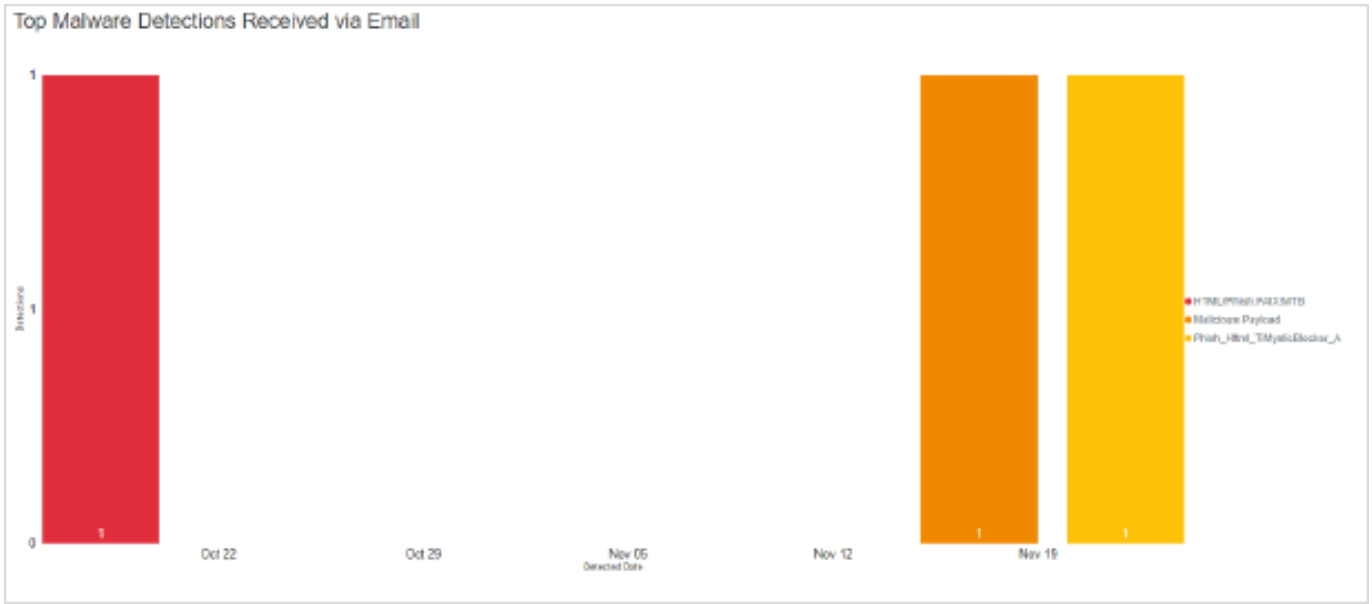
Auto-Forwarding Email Rules for Admin Accounts

A common sign of a security breach is the existence of email forwarding rules. This is especially true for those that target external recipients. We continually monitor internal and external forwarding rules for this reason.

Account Type	Forwarding Type	Rule Count
External	Administrator	1
Internal	Administrator	0

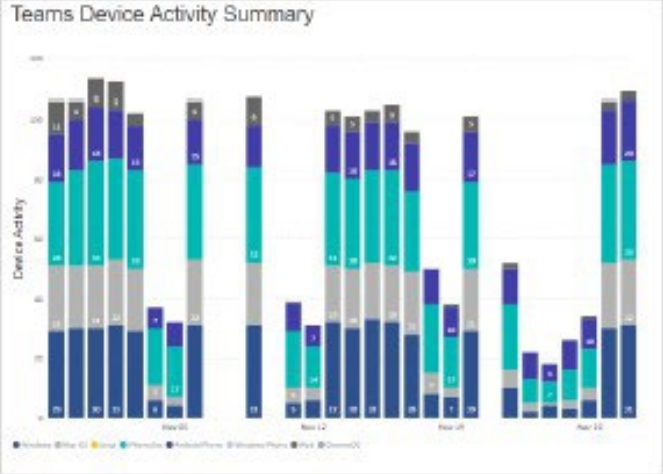


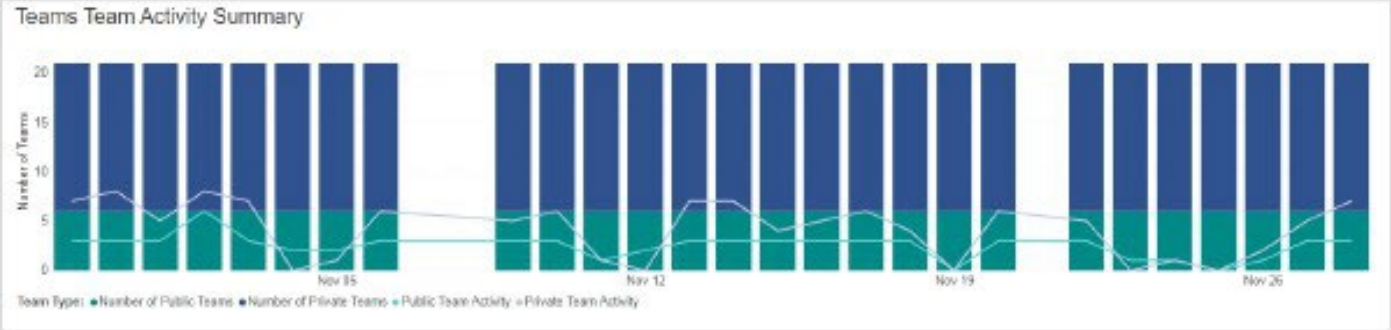




Microsoft Teams Security

Microsoft Teams activity and security summary, including links and attachments





Microsoft Teams External and Guest Access Settings

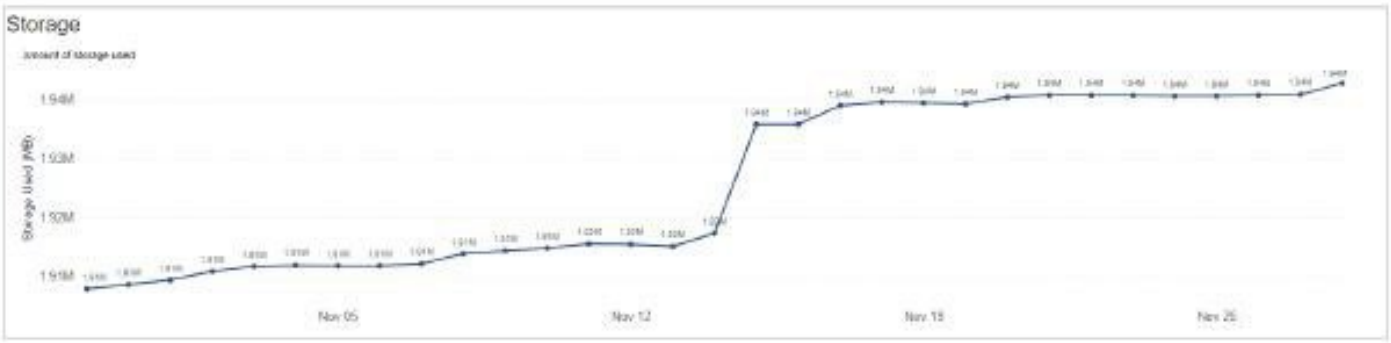
Especially if team creation and administration is allowed by non-admin users, it's important to keep an eye on external and guest access settings.

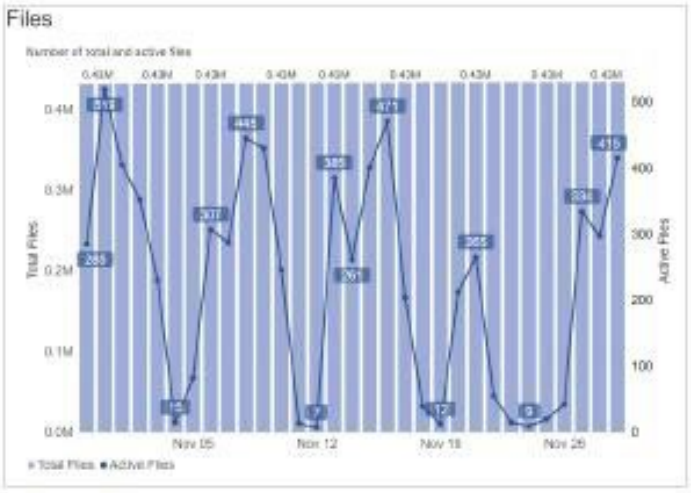
Domain	Allowed	Blocked	Communication Allowed with Non-Organization Teams Users	Communication Allowed with External Teams Users	Communication Allowed with Skype Users	Guest Access Allowed
Allow all external domains	All	None	Yes	Yes	No	Yes

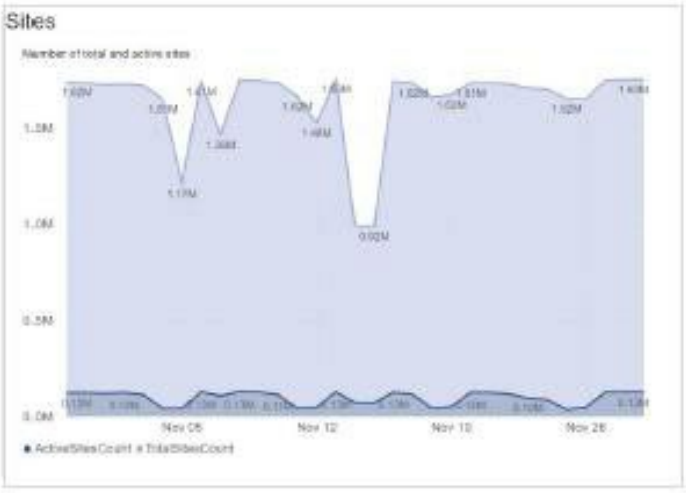
Microsoft File Security

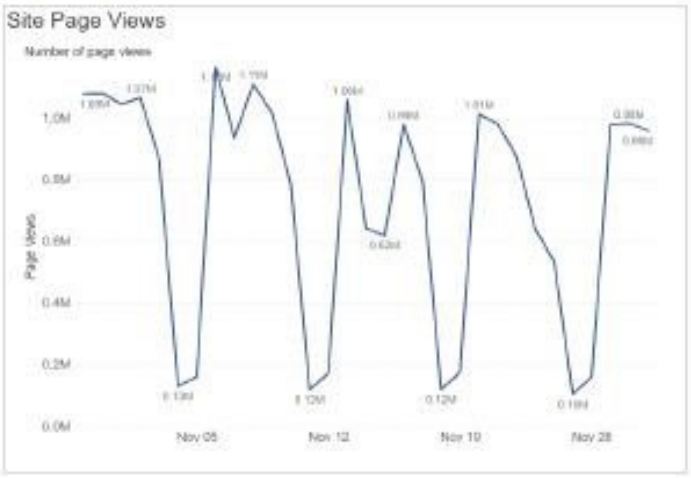
Microsoft file storage and protection summary

Salty Soul Foundation | Reporting period: July 1, 2025 through September 30, 2025





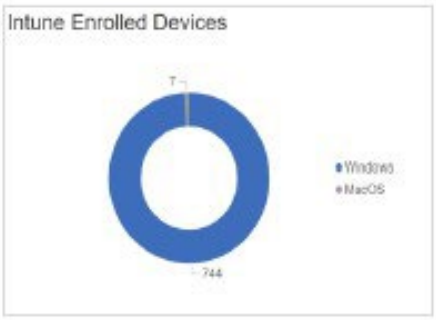


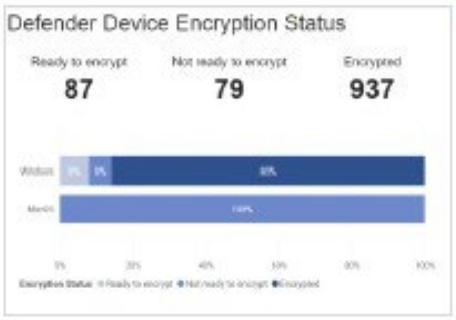


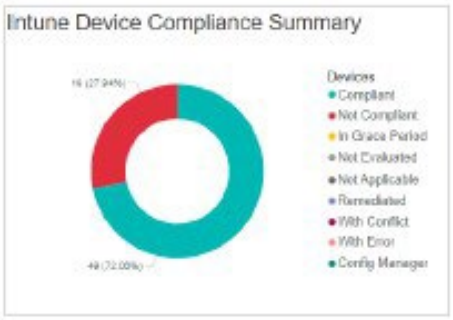
Endpoint Management Security

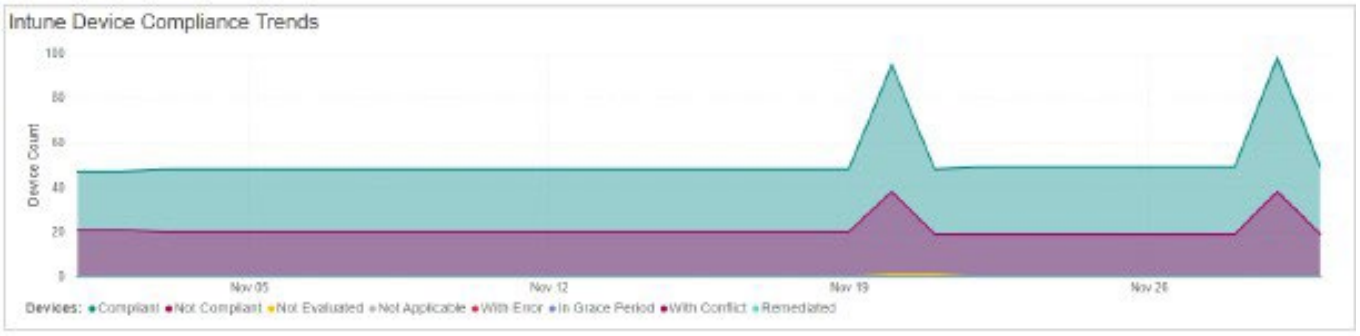
Microsoft Intune and device security summary

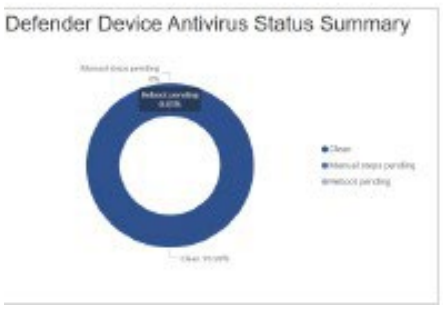
Intune Enrolled Devices	Windows	MacOS	Android	IOS	Windows Mobile	Others
1103	523	7	0	542	0	29

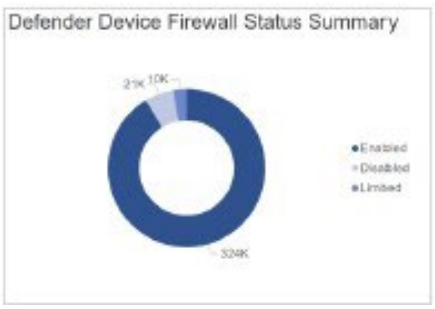


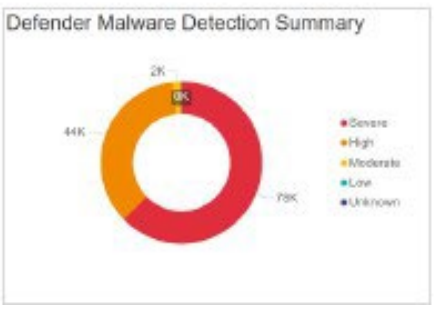












Microsoft 365 Software Licensing

All Microsoft software license SKU and usage summary

Current M365 Licenses

M365 Product	Subscription Type	Status	Next Lifecycle Date	Qty Licensed	Assigned	Available
Microsoft 365 Business Premium	Purchased	Enabled	Will be renewed (or expired) on Apr 15, 2026	5	5	0
Microsoft Copilot Studio Viral Trial	Free	Enabled	Never expires	10000	1	9999
Microsoft Fabric (Free)	Purchased	Enabled	Will be renewed (or expired) on Nov 22, 2025	1	1	0
Microsoft Power Automate Free	Free	Enabled	Never expires	10000	2	9998
microsoft_cloud_for_nonprofit_addon_basic	Purchased	Enabled	Will be renewed (or expired) on Jul 10, 2026	1	0	1
Nonprofit Portal	Trial	Enabled	Will be renewed (or expired) on Apr 13, 2032	25	7	18
Power Pages vTrial for Makers	Free	Enabled	Never expires	10000	1	9999
Power Virtual Agents Viral Trial	Free	Enabled	Never expires	10000	1	9999
Windows Store for Business	Free	Enabled	Never expires	1000000	0	1000000

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 Premium	81%
Windows Store for Business	59%
Microsoft 365 Business Basic	52%
Nonprofit Portal	30%
Rights Management Service Basic Content Protection	26%
Microsoft 365 Business Standard	26%
Exchange Online (Plan 1)	26%
Office 365 E1	22%
Microsoft Teams Phone Resource Account	19%
Microsoft Stream	19%
Microsoft Teams Phone Standard	19%
Microsoft Copilot for Microsoft 365	15%
Teams Premium (for Departments)	15%

Secure Score History Detail

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

Salty Soul Foundation | Reporting period: July 1, 2025 through September 30, 2025

Secure Score	Max Score	Score Change	% of Max	Max Change	Change Date	Change Description	Recommendation Influencing the Score
542.5	1053.0	-	51.52%	-	Sep 30, 2025	Current Secure Score	Current Secure Score
542.5	1053.0	+3.33	51.52%	-	Aug 5, 2025	Recommendation has been completed; Recommendation score points increased	Fix Microsoft Defender for Endpoint impaired communications
539.17	1053.0	-1.33	51.2%	-	Aug 5, 2025	Recommendation score points decreased	Fix unquoted service path for Windows services
540.5	1053.0	+3.33	51.33%	-	Aug 5, 2025	Recommendation has been completed; Recommendation score points increased	Turn on Microsoft Defender for Endpoint sensor
537.17	1053.0	+3.33	51.01%	-	Aug 5, 2025	Recommendation has been completed; Recommendation score points increased	Fix Microsoft Defender for Endpoint sensor data collection
533.84	1053.0	+4.5	50.7%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Block executable content from email client and webmail
529.34	1053.0	+4.5	50.27%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Block Office applications from creating executable content
522.17	1053.0	+1.33	49.59%	-	Aug 4, 2025	Recommendation score points increased	Enable 'Network Protection'
520.84	1053.0	-4.0	49.46%	-	Aug 4, 2025	Recommendation score points decreased	Enable EDR in block mode
524.51	1053.0	-1.33	49.81%	-	Aug 4, 2025	Recommendation score points decreased	Disable 'Autoplay' for all drives
525.84	1053.0	+2.5	49.94%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Enable Microsoft Defender Antivirus real-time behavior monitoring
523.34	1053.0	-1.5	49.7%	-	Aug 4, 2025	Recommendation score points decreased	Secure Microsoft Defender firewall private profile
524.84	1053.0	+5.0	49.84%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Turn on real-time protection
519.84	1053.0	+2.67	49.37%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Change service executable path to a common protected location
517.17	1053.0	+0.33	49.11%	-	Aug 4, 2025	Recommendation score points increased	Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile
516.84	1053.0	+4.5	49.08%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Encrypt all BitLocker-supported drives
512.34	1053.0	-1.5	48.66%	-	Aug 4, 2025	Recommendation score points decreased	Secure Microsoft Defender Firewall domain profile
513.84	1053.0	+4.5	48.8%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Block JavaScript or VBScript from launching downloaded executable content
509.34	1053.0	-1.33	48.37%	-	Aug 4, 2025	Recommendation score points decreased	Disable SMBv1 client driver
510.67	1053.0	-2.5	48.5%	-	Aug 4, 2025	Recommendation score points decreased	Enable Automatic Updates
513.17	1053.0	+4.5	48.73%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Turn on PUA protection in block mode

Secure Score	Max Score	Score Change	% of Max	Max Change	Change Date	Change Description	Recommendation Influencing the Score
508.67	1053.0	-1.5	48.31%	-	Aug 4, 2025	Recommendation score points decreased	Secure Microsoft Defender Firewall public profile
510.17	1053.0	-1.33	48.45%	-	Aug 4, 2025	Recommendation score points decreased	Disable the built-in Administrator account
511.5	1053.0	+4.5	48.58%	-	Aug 4, 2025	Recommendation has been completed; Recommendation score points increased	Block all Office applications from creating child processes
507.0	1053.0	+0.33	48.15%	-	Aug 4, 2025	Recommendation score points increased	Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile
506.67	1053.0	+3.34	48.12%	-	Jul 24, 2025	Recommendation score points increased	Fix Microsoft Defender for Endpoint impaired communications
503.33	1053.0	+3.34	47.8%	-	Jul 24, 2025	Recommendation score points increased	Turn on Microsoft Defender for Endpoint sensor
499.99	1053.0	+3.34	47.48%	-	Jul 24, 2025	Recommendation score points increased	Fix Microsoft Defender for Endpoint sensor data collection
496.65	1053.0	-3.34	47.17%	-	Jul 18, 2025	Recommendation score points decreased	Fix Microsoft Defender for Endpoint impaired communications
499.99	1053.0	-3.34	47.48%	-	Jul 18, 2025	Recommendation score points decreased	Turn on Microsoft Defender for Endpoint sensor
503.33	1053.0	-3.34	47.8%	-	Jul 18, 2025	Recommendation score points decreased	Fix Microsoft Defender for Endpoint sensor data collection
506.67	1053.0	-3.33	48.12%	-	Jul 12, 2025	Recommendation score points decreased	Fix Microsoft Defender for Endpoint impaired communications
510.0	1053.0	-3.33	48.43%	-	Jul 12, 2025	Recommendation score points decreased	Turn on Microsoft Defender for Endpoint sensor
513.33	1053.0	-3.33	48.75%	-	Jul 12, 2025	Recommendation score points decreased	Fix Microsoft Defender for Endpoint sensor data collection
516.66	1053.0	-	49.07%	-	Jul 1, 2025	Initial Secure Score	Initial Secure Score

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

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.

Microsoft Entra ID – Entra ID 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 Purview, 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 M365, such as Entra ID 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.

Cloud App Security (CAS/CASB) – Cloud App Security and Cloud Access Security Broker are terms representing comprehensive security solutions that provide visibility, control, and threat protection for cloud applications and services, including those used within M365. Defender for Cloud Apps and Cloud App Discovery are solutions designed to help manage cloud app security.

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.

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.

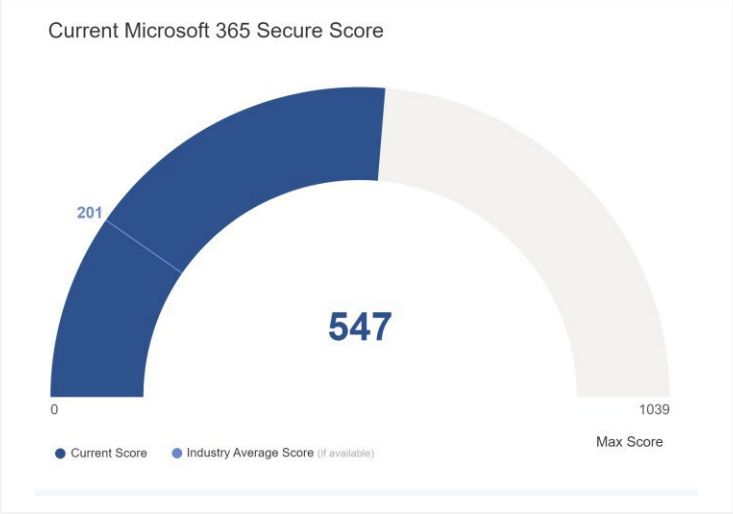
The score also represents a simplified framework for meeting or exceeding global IT security standards set forth by standards bodies like the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO 27001/27002), 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

recommendations. However, there is no universal threshold or benchmark for what constitutes a good or bad percentage score. It depends on your specific security needs and risk appetite, as well as the external factors that affect your security, such as your industry, your geography, and the regulatory requirements you have to comply with.

Improving Your Secure Score and Your Security

This report offers a summary list of high-value security recommendations that can help improve your score and your security. We can also provide a more detailed set of recommendations categorized by the Microsoft 365 products and services they apply to, such as Exchange Online, SharePoint Online, or Microsoft Entra ID. We can also show them ranked by their impact on your score and their level of implementation difficulty. We can also review recommendations by their status, such as planned, ignored, or resolved.

Some of the recommendations are easy to implement, such as turning on audit logging or reviewing sign-in reports. Our security policies dictate that most of these are implemented by default, when the impact on your use of IT systems is negligible. Others may require more planning and testing, such as enabling encryption or configuring conditional access policies. Some of the recommendations may not be applicable or feasible for your organization, such as disabling legacy authentication or blocking external sharing. We are happy to discuss the implications of any of Microsoft's recommendations you are interested in to improve your score.

Naturally, as recommendations are implemented, your score will increase and your security will improve. However, you should not focus only on your score, but also on the security outcomes and benefits you achieve. For example, you may not see a significant increase in your score by enabling multi-factor authentication for all users, but you will significantly reduce the risk of account compromise and data breach. We can help you weigh the tradeoffs.

How we Evaluate Your Secure Score for Your Company's Needs

Secure Score is a useful tool, but it is not a one-size-fits-all solution. You may have different security needs and challenges than other organizations.

One way to define your Secure Score goal is to build your own security baseline. This is the minimum level of security you want to achieve and maintain for your organization. You can use the industry and regional averages as a reference, but you should also consider your own risk profile and security requirements. For example, if you are in a highly regulated or competitive industry, such as healthcare or finance, you may want to have a higher security baseline than the average. If you are in a low-risk or niche industry, such as education or arts, you may be comfortable with a lower security baseline than the average.

When setting a baseline goal, it is important to consider what circumstances might seriously impact business continuity, the loss of competitive intellectual property, or customer confidence in your brand. For example, if you want to protect your data from unauthorized access or leakage, you may want to focus on the recommendations that involve encryption, access control, and data loss prevention. If you want to prevent or detect malicious attacks, you may want to focus on the recommendations that involve threat protection, identity protection, and security monitoring. That said, there are some security elements that are essential to every business.

Some of the security recommendations considered essential are:

- Enable multi-factor authentication for all users and admins
- Turn on audit logging and review audit reports regularly
- Enable Microsoft Defender for Office 365 and Microsoft Defender for Endpoint
- Configure security defaults or conditional access policies
- Enable encryption for email and files
- Review and update your security settings and policies regularly

We can help you evaluate the pros and cons of each recommendation and decide whether it is worth implementing for your business. Microsoft Secure Score and the related security recommendations offer a valuable method of evaluating your security posture, setting a baseline goal, and continuously monitoring adherence to this goal over time.

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 Tyrell Technologies 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

Salty Soul Foundation on Friday, November 14, 2025