MERCURY IT

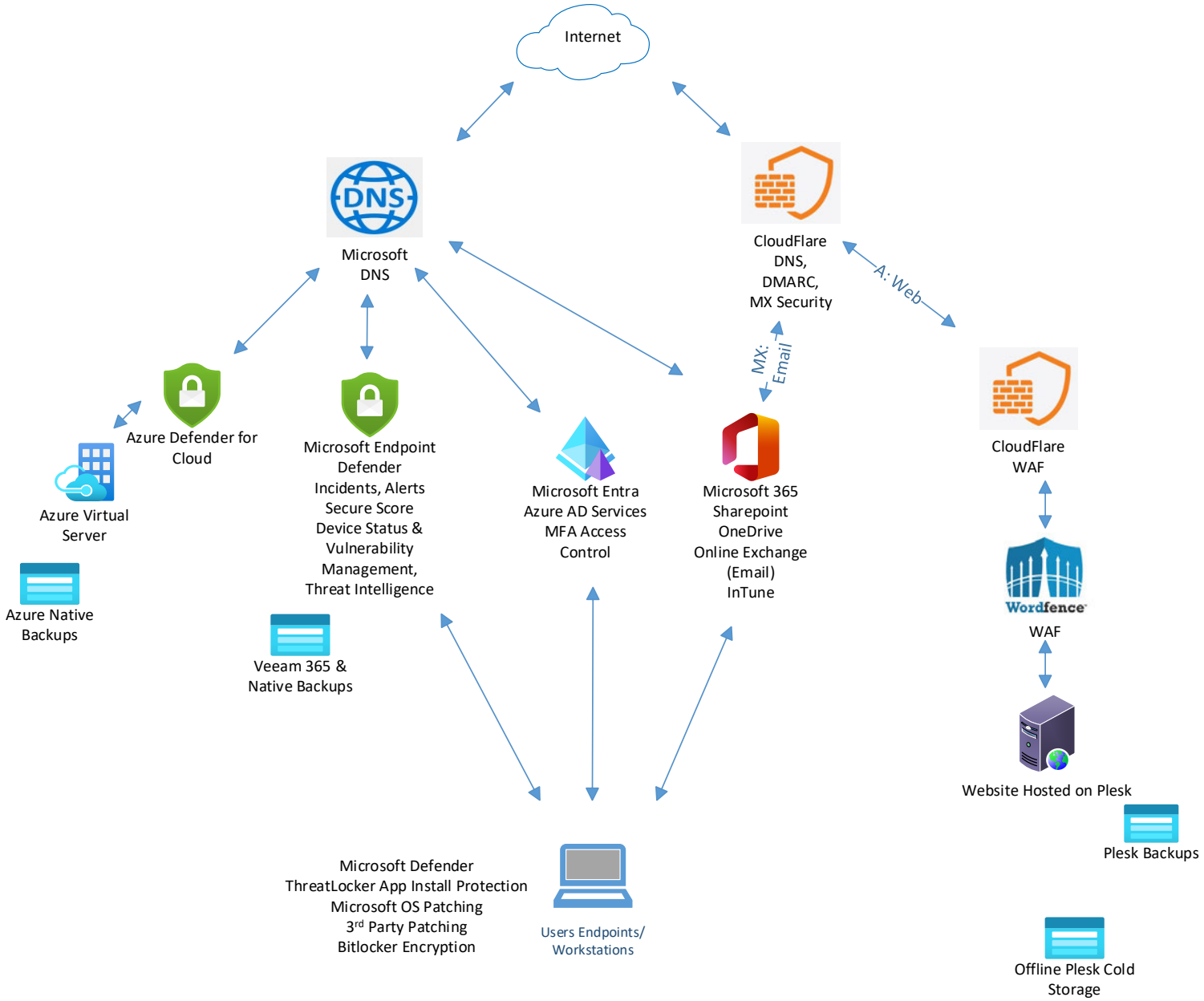
Company XYZ
Managed Security Services & SOC
Monthly Report

Executive Summary

Status	Security Layer	Action
	MFA User Access Control	11 user accounts to be setup with MFA. Conditional access policy to be setup
	User Access Microsoft Entra	No action required
	Microsoft 365 Defender Incidents	There were no high or medium severity incident that required action for the month of October
	Microsoft 365 Defender Alerts	There were no high or medium severity incident that required action for the month of October
	Microsoft 365 Secure Score	82.94%. No action required above monthly maintenance
	Microsoft 365 Device Status & Vulnerability	The exposure and device scores are expected. Will be improved with the monthly security updates
	Microsoft 365 Threat Intelligence	The threats exposed do not require action. Will be patched via normal monthly patch process
	Microsoft Azure Defender for Cloud	Medium level recommendations to be assessed and changes made where required
	Kaseya Workstation OS Windows Patching	13 devices not on Windows 11 version 23H2 need to be reviewed
	Manage Engine 3rd Party Application Patching	There are a small number of failures which no further action required
	Threatlocker Workstation Status	56 devices secured. Additional device recommendations to be reviewed and assessed by XYZ
	Email Online Exchange Reporting	There are no storage concerns or actions to take
	Email Integrity Status (MX record)	No MX DNS or DMARC record issues. The Email health check identified 3 low warnings to be actioned
	CloudFlare DNS and WAF	There are no threats detected or mitigated
	Wordfence WAF	No action required
	Sharepoint and OneDrive Storage Usage & Trends	There are no storage concerns or actions to take
	Veeam 365 Backup Status	No issues with Veeam 365 backups
	Azure Backup Status	No issues with Azure backups
	Dark Web	There are no compromises
	Quarterly MIT Red Team vs Blue Team Activities	No Red Team activities this month. Actions from previous Linux vulnerability tests are under action
	MIT SOC Vulnerability Hunting and Actions Taken	No action required

MERCURY IT

Security Architecture (Example)



User Access Control Management

The status of user accounts is:

- 84 Sign-in Enabled Accounts
- 73 Accounts with MFA
- 8 Accounts without MFA

The following accounts haven't set up an MFA method

- User.surname@xyz.org.nz
- User.surname@xyz.org.nz
- User.surname@xyz.org.nz
- User.surname@xyz.org.nz
- User.surname@xyz.org.nz

MFA is enforced to all users with a conditional access policy, theGABreakGlass@xyz.org.nz is excluded from this policy.

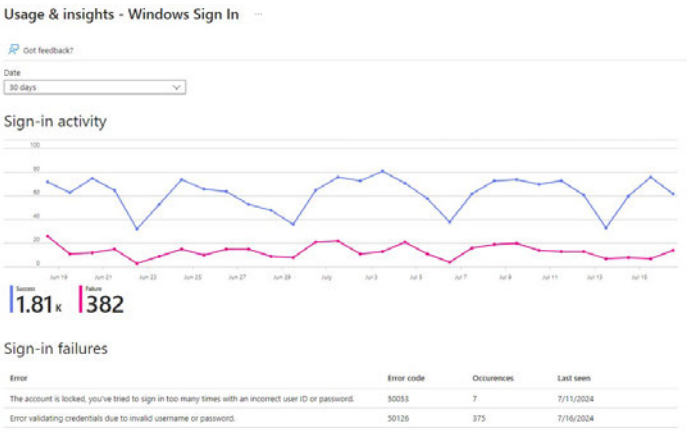
The recommended action as next step is to setup a new conditional access policy to protect account that don't have MFA setup. This would require users to re-enter MFA to be able to change or add MFA to their account. This policy would exclude the IP addresses of the company offices. New users having no MFA methods would need to setup MFA when they are in a XYZ office.

User Access Microsoft Entra Reporting

Successful/failed logins to Azure Entra are monitored with Windows Sign-in and Bing reviewed as below:

Application name	Successful sign-ins	Failed sign-ins	Success rate
Windows Sign In	1876	389	82.83%
Bing	180	198	47.62%
Microsoft Authentication Broker	183	37	83.18%
Outlook Mobile	82	18	82.00%
Microsoft Office	111	18	86.05%
Microsoft Edge Enterprise New Tab Page	20	13	60.61%
OfficeHome	358	13	96.50%
Racingintegrityboard.org.nz WordPress Internet SAML	44	12	78.57%
Microsoft Power Query for Excel	1	11	8.33%
Office 365 SharePoint Online	267	10	96.39%
Microsoft Teams	51	9	85.00%
FCM HUB	156	9	94.55%
Office 365 Exchange Online	278	8	97.20%
Microsoft 365 Support Service	30	6	83.33%
Apple Internet Accounts	29	6	82.86%
O365 Suite UX	26	5	83.87%
MM_Reactions_PME_PROD	0	4	0.00%
Gmail	6	3	66.67%

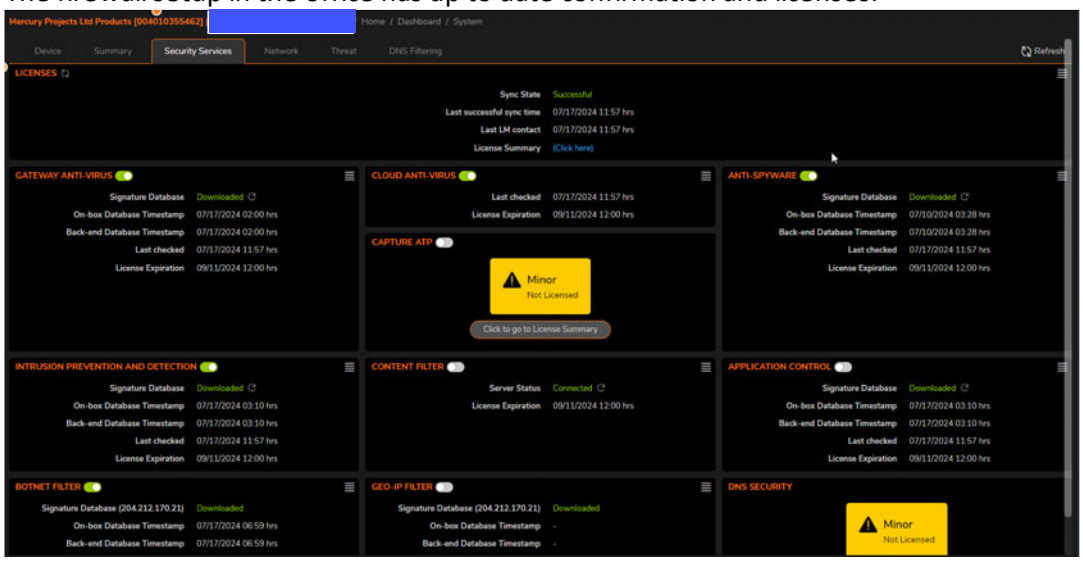
The failed logins for Windows interactive sign-in process (unlocking and signing into their computers) are expected for these errors to happen when users forget or mistype their passwords.



These sign-in failures are expected, these are cause when user sessions expire due to MFA policy which requires users to re-sign in every 30 days.

Firewall Perimeter Control

The firewall setup in the office has up to date confirmation and licenses.



There are 276 firewall rules setup with some disabled rules. Action to clean up disabled rules.

There were 4 valid admin logins for the month and no failed logins.

Microsoft 365 Defender XDR Incidents

An incident in the Microsoft Defender portal is a collection of related alerts and associated data that make up the story of an attack. If a sever or high incident NSOC will investigate, manage, implement, and document the response to it.

There were no incidents that required action.

Incident name	Tags	Severity	Investigation state	Impacted assets
Initial access incident involving one user	Credential Phish	low	2 investigation states	Accounts: [redacted] ,Mailboxes: [redacted]
Unusual ISP for an OAuth App	-	low	Unsupported alert type	Apps: Microsoft 365
Unusual ISP for an OAuth App	-	low	Unsupported alert type	Apps: Microsoft 365
Email reported by user as not junk	-	low	Queued	Accounts: [redacted] ,Mailboxes: [redacted]

Microsoft 365 Defender XDR Alerts

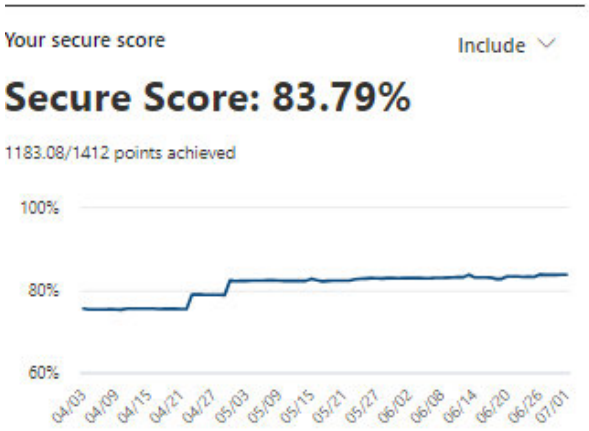
Alerts are the basis of all incidents and indicate the occurrence of malicious or suspicious events in your environment. Alerts are typically part of a broader attack and provide clues about an incident.

There were no severe or high alerts that required action.

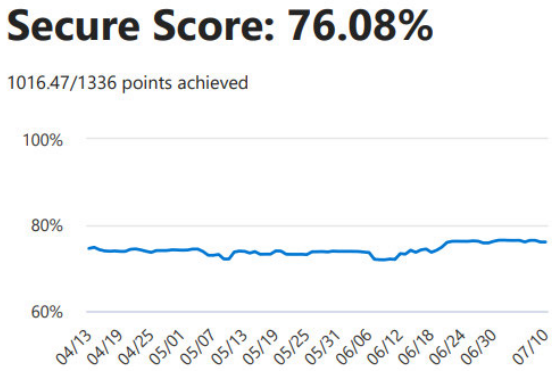
Alert name	Severity	Impacted assets	First activity
Email reported by user as malware or phish	Low		2024-06-30T01:33:00.000Z
Email reported by user as malware or phish	Low		2024-06-30T01:33:00.000Z
Email reported by user as malware or phish	Low		2024-06-30T01:33:00.000Z
Email reported by user as malware or phish	Low		2024-06-30T01:33:00.000Z
Email reported by user as malware or phish	Low		2024-06-25T03:00:00.000Z
Email reported by user as junk	Low		2024-06-25T03:00:00.000Z
Email reported by user as malware or phish	Low		2024-06-25T03:00:00.000Z
Email reported by user as malware or phish	Low		2024-06-24T09:17:00.000Z
Email reported by user as malware or phish	Low		2024-06-24T09:17:00.000Z
Email reported by user as malware or phish	Low		2024-06-24T09:17:00.000Z
Email reported by user as malware or phish	Low		2024-06-24T09:17:00.000Z
Email reported by user as malware or phish	Low		2024-06-23T04:29:00.000Z
Email reported by user as malware or phish	Low		2024-06-23T04:29:00.000Z
Email reported by user as malware or phish	Low		2024-06-23T04:29:00.000Z
Email reported by user as malware or phish	Low		2024-06-23T04:29:00.000Z
Email reported by user as malware or phish	Low		2024-06-21T21:49:00.000Z
Email reported by user as malware or phish	Low		2024-06-21T21:49:00.000Z
Email reported by user as malware or phish	Low		2024-06-21T21:49:00.000Z
Email reported by user as malware or phish	Low		2024-06-21T21:49:00.000Z

Microsoft 365 Secure Score

XYZ Secure Score



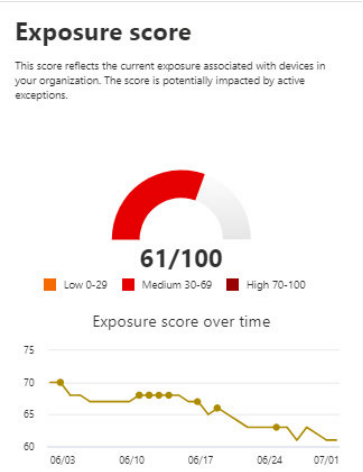
MIT Secure Score

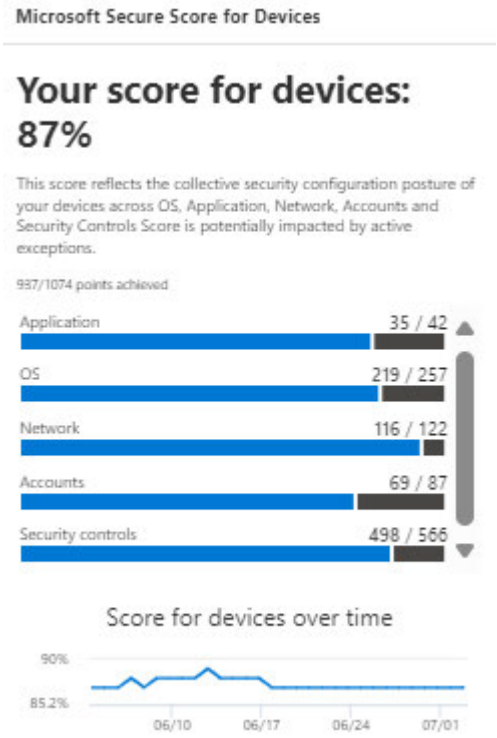


Microsoft 365 Device Status Summary & 365 Vulnerability Management

The exposure score reflects the current exposure associated with devices in your organisation. The device score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score.

The exposure and device scores are expected and will be improved with the monthly security updates via the scheduled patch process via Kaseya & Manage Engine.

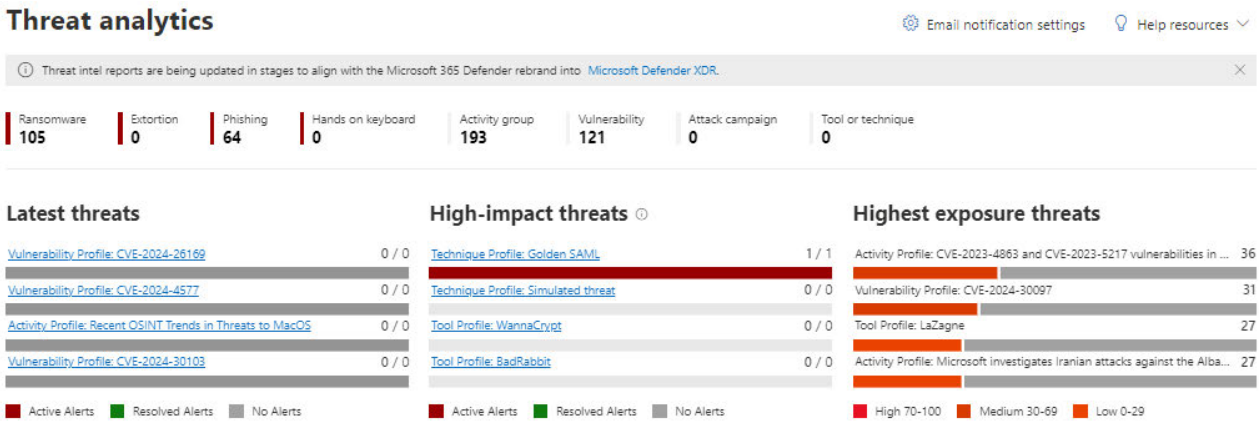

Exposure score
This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.
61/100
Low 0-29
Medium 30-69
High 70-100
Exposure score over time
75
70
65
60
06/03
06/10
06/17
06/24
07/01


Microsoft Secure Score for Devices
Your score for devices: 87%
This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.
937/1074 points achieved
Application 35 / 42
OS 219 / 257
Network 116 / 122
Accounts 69 / 87
Security controls 498 / 566
Score for devices over time
90%
85.2%
06/10
06/17
06/24
07/01

Microsoft 365 Threat Intelligence

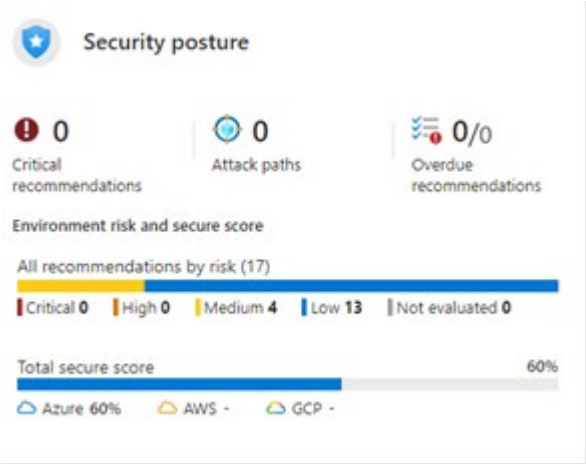
Microsoft365 Threat Intelligence is a product that provides interactive tools to analyse prevalence and severity of threats in real time.

The threats exposed do not require immediate action and will be patched via the normal monthly patch process.



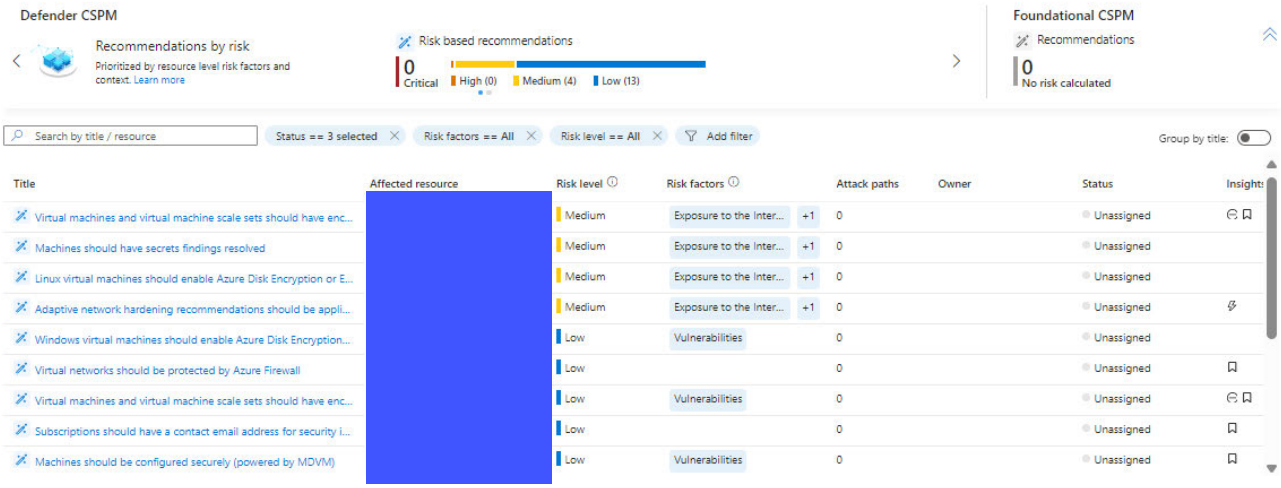
Microsoft Azure Defender for Cloud

The Azure Cloud Defender Score is for the security posture risk within the Azure infrastructure which application is hosted. The security posture is expected with no further action.



Recommendations

The 4 medium level recommendations will be actioned.



Workstation Kaseya Windows Patching

XYZ workstations Microsoft Windows patch management process is defined as:

- Core Microsoft Windows patches run first Monday every month. This excludes preview patches.
- Any machine not patched will be followed up by Mercury IT
- Driver updates are applied 2 months after they are released due to the historical issues

For Kaseya workstation Windows patching there were:
There are a total of 73 devices categorized by their respective build versions:

- Windows 11 version 23H2 Professional x64 Edition Build 22631: 56 workstations
- Windows 11 version 22H2 Professional x64 Edition Build 22621: 14 workstations
- Windows 11 version 21H2 Professional x64 Edition Build 22000: 2 workstations
- Mac OS X 14.5 BldID: 23F79: 1 device

Action required to investigate the 16 devices not on Windows 11 version 23H2 to either decommission or force the workstations to be updated 23H2.

Workstation,	Last User	OS		Last Checkin
XYZ-tab03,	User 1	11	Professional x64 Edition Build 22621	01/07/2024
XYZ-lap24,	User 2,	11	Professional x64 Edition Build 22621	11/06/2024
XYZ-lap17,	User 3,	11	Professional x64 Edition Build 22621	04/07/2024
XYZ-lap57,	User 4,	11	Professional x64 Edition Build 22621	08/05/2024
XYZ-lap76,	User 5,	11	Professional x64 Edition Build 22621	11/07/2024
XYZ-lap75,	User 6,	11	Professional x64 Edition Build 22621	08/07/2024
XYZ-LAP59,	User 7,	11	Professional x64 Edition Build 22621	11/06/2024
XYZ-tab02,	User 8,	11	Professional x64 Edition Build 22621	10/07/2024
XYZ-lap55,	User 9,	11	Professional x64 Edition Build 22621	16/03/2024
XYZ-lap74,	mitadmin,	11	Professional x64 Edition Build 22621	21/06/2024
XYZ-lap06,	User 10,	11	Professional x64 Edition Build 22621	11/06/2024
DESKTOP-jrq3pbg,	MIT_Tech,	11	Professional x64 Edition Build 22621	04/12/2023
XYZ-lap29,	User 11,	11	Professional x64 Edition Build 22000	11/07/2024
XYZ-LAP54,	User 12,	11	Professional x64 Edition Build 22000	20/05/2024

Workstation Manage Engine 3rd Party Patching

Manage Engine has been configured to patch 3rd party applications as follows:

Patch Criteria			
Criteria	Microsoft Applications	Third Party Applications	Anti Virus Applications
Updates & Severities	NA	Critical,Important,Moderate	Definition Update
Applications	NA	All	All

The following applications are scheduled to be patched by Manage Engine.

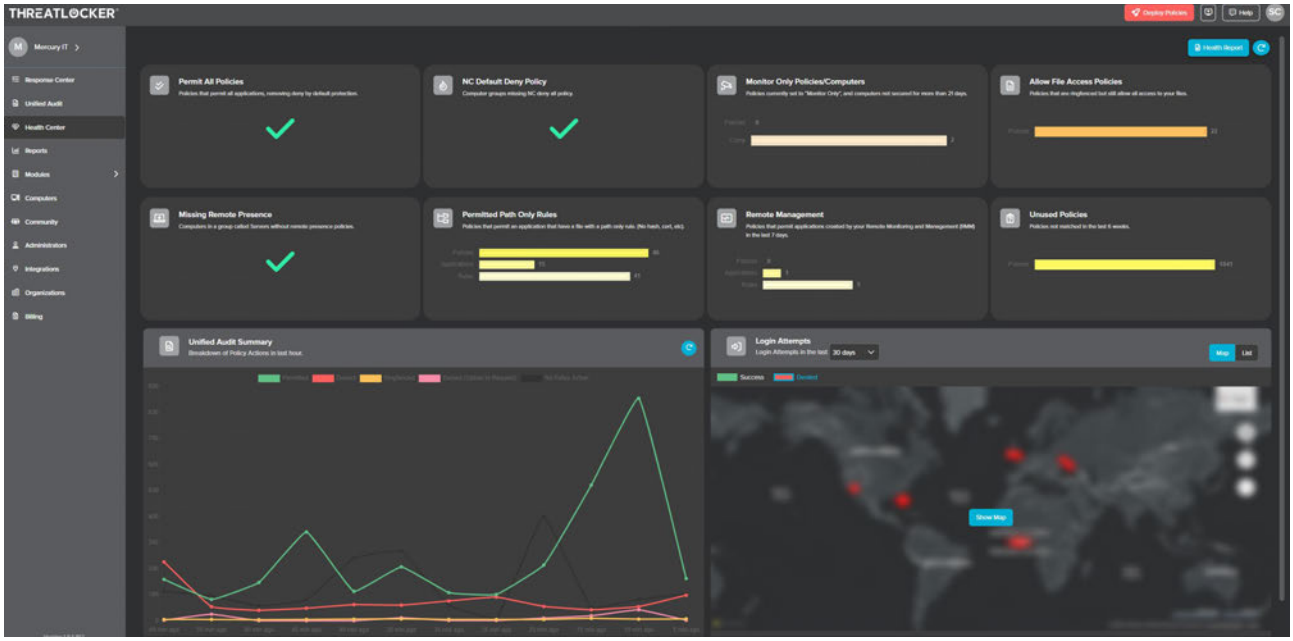
Patch ID	Bulletin ID	Patch Description	Missing Systems	Installed Systems	Failed Systems
339566	TU-117	Zoom Workplace (x64) (6.1.1.41705)	1	6	1
339524	TU-072	Adobe Acrobat Reader DC (x64) (24.002.20895)	2	16	1
339495	TU-530	Lenovo System Update (5.08.03.47)	1	2	1
339407	TU-017	Google Chrome (x64) (126.0.6478.126, 126.0.6478.127)	1	45	1
339303	TU-024	7 Zip (exe) (x64) (24.07)	1	42	0
339253	TU-017	Google Chrome (x64) (126.0.6478.114, 126.0.6478.115)	1	1	0
339135	TU-021	VLC Media Player (X64) (3.0.21)	14	7	0
339134	TU-021	VLC Media Player (3.0.21)	8	0	0
336162	TU-1438	Poly Lens (1.3.2)	3	0	3

There are 73 agents in Kaseya for XYZ but only 49 agents have been deployed with Manage Engine to date. There are 23 agents that haven't been online since June.

Workstation ThreatLocker Health Status

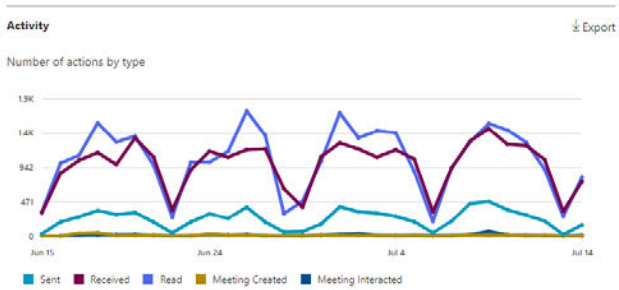
Threatlocker still needs refinement and learning as it is blocking several valid applications. The action is for Mercury IT to whitelist and continue to monitor on a regular daily/weekly basis.

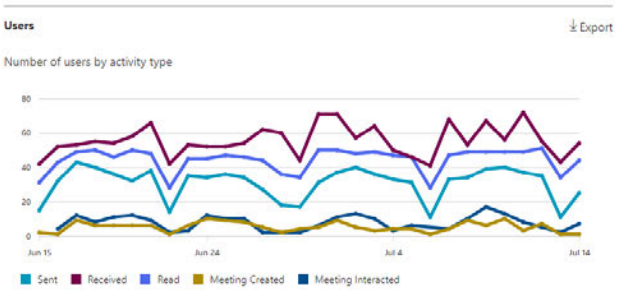
Somew examples of applications being blocked from download include:
Spotify, Chrome extensions, Brother Help application, Candy Crush, Sky, iCloud, Cooking Fever, Curl, Razer (game), iTunes.

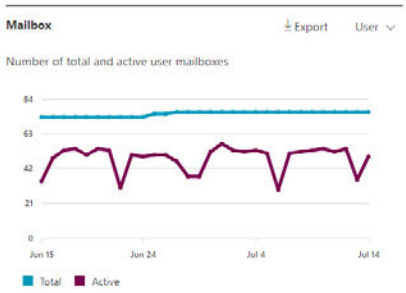


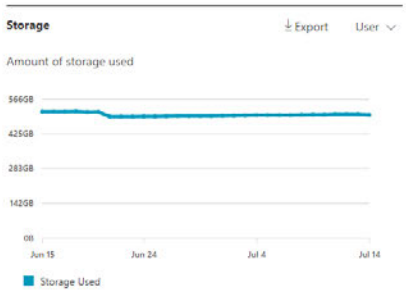
Email Online Exchange Reporting

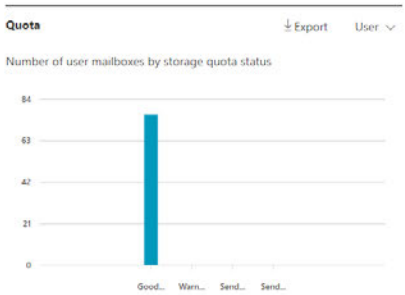
The Exchange online reporting stats are expected and do not highlight an issue or determined attack therefore no action is required.









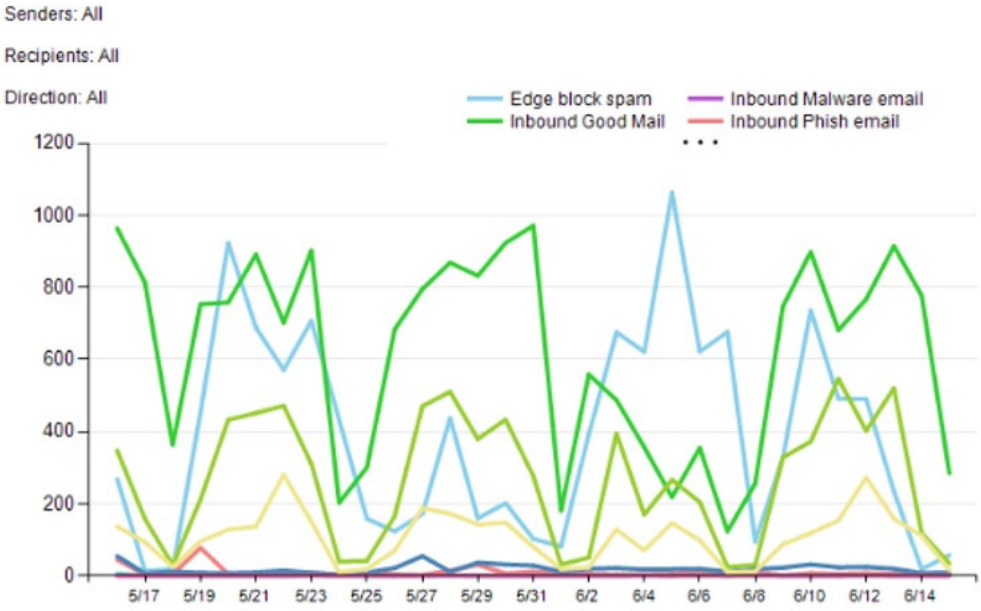


Top 10 Mailbox Size

Business Premium has up to 1.5tb archive mailbox. business standard and below have 50gb archive mailbox. Option to turn on archive mailbox + policy to move emails to the archive mailbox after 1-2 years. There are no storage concerns or actions to take.

Username	Last activity date (UTC)	Item count	Storage used (MB) ↓	Quota status
[redacted]	Sunday, July 14, 2024	135,279	46,599	Good (under limits)
	Sunday, July 14, 2024	149,251	40,716	Good (under limits)
	Saturday, July 13, 2024	71,220	30,747	Good (under limits)
	Sunday, July 14, 2024	88,921	29,092	Good (under limits)
	Sunday, July 14, 2024	65,261	27,616	Good (under limits)
	Sunday, July 14, 2024	60,711	24,634	Good (under limits)
	Sunday, July 14, 2024	74,518	22,794	Good (under limits)
	Sunday, July 14, 2024	87,530	21,688	Good (under limits)
	Monday, July 19, 2021	122,112	20,805	Good (under limits)
	Sunday, July 14, 2024	72,872	18,428	Good (under limits)

The email stats are expected and do not highlight an issue or determined attack therefore no action is required.



Edge block spam	Inbound Good Mail	Inbound Malware email	Inbound Phish email	Inbound Spam email	IntraOrg Good Mail	IntraOrg Phish email	IntraOrg Spam email	Outbound Good Mail
12002	19320	8	322	578	8209	6	1	3285

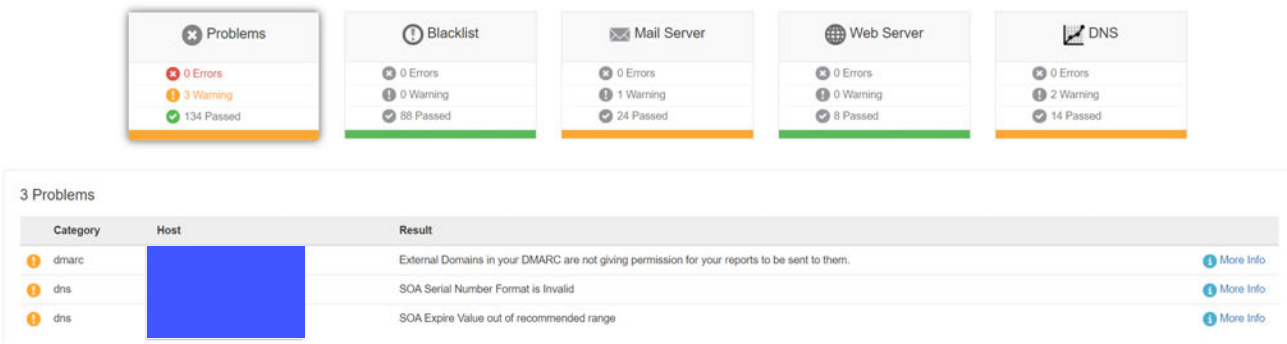
Email Integrity Status

DMARC changes were made to the Xyz.org.nz domain with the following status:

	Test	Result
!	DMARC External Validation	External Domains in your DMARC are not giving permission for your reports to be sent to them.
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

When comparing to MXTools 83 known Email blacklists there were no records of Xyz.org.nz being blacklisted.

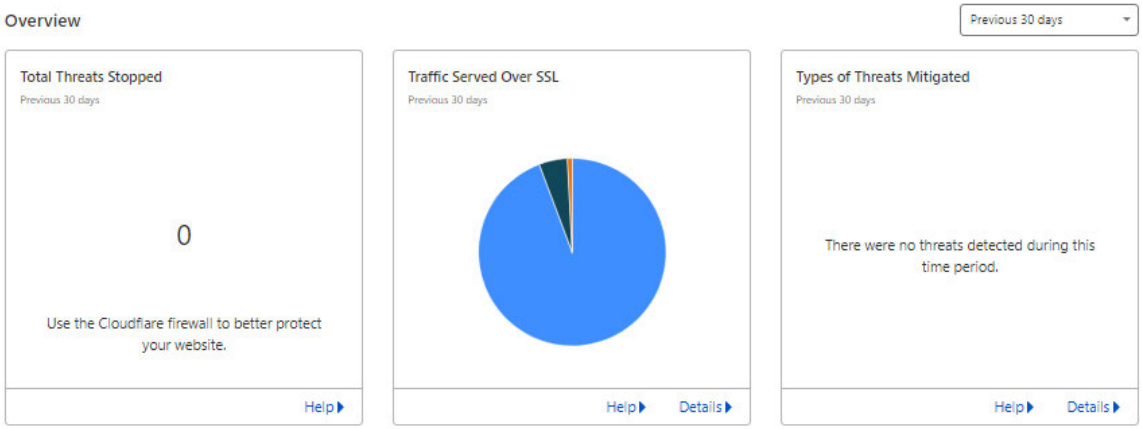
The MXTools Email health check identified 3 warnings that will be investigated as follows:



CloudFlare DNS and WAF

The xyz.org.nz website uses Cloudflare Pro, which offers several key features to enhance security and performance. Cloudflare hosts the DNS, providing fast and reliable domain resolution. It protects the site with a robust Web Application Firewall (WAF) and managed rulesets that filter out malicious traffic and prevent common web attacks. Additionally, Cloudflare's Automatic Platform Optimization (APO) significantly boosts the performance of the WordPress website by serving dynamic content from Cloudflare's edge network, reducing load times and improving user experience.

CloudFlare manages and secure the DNS and provides Web Application Firewall protection.
There were no threats detected or mitigated.

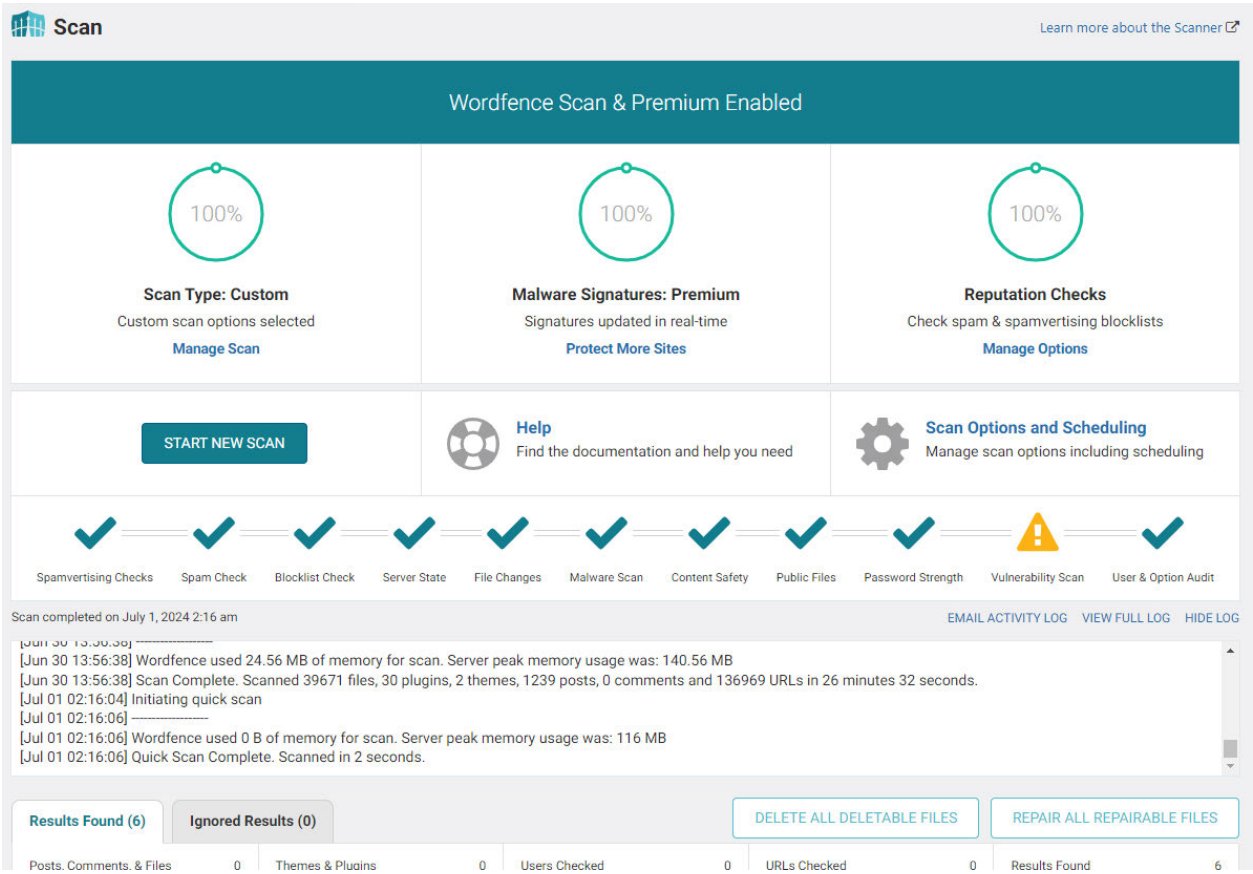


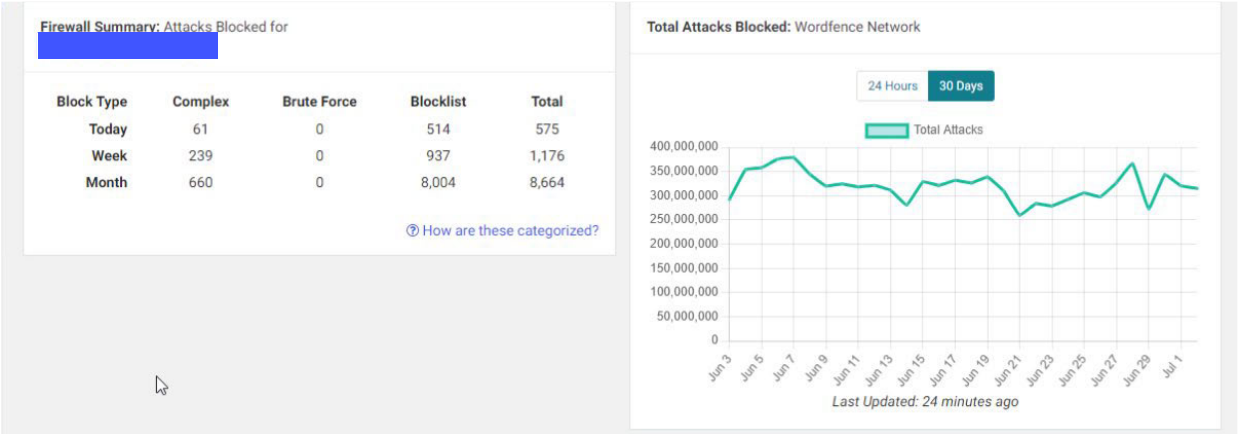
Wordfence WAF

Wordfence is an on-server WAF that provides an additional layer of security for the xyz.org.nz website. It performs comprehensive security and vulnerability scans, identifying and mitigating potential threats. Wordfence is specifically designed for WordPress, giving it an edge over generic WAF solutions by offering tailored protection and optimization for WordPress sites. It includes features like real-time threat defence, login security, and malware scanning, ensuring the website remains secure against evolving threats.

The website was patched regularly through the month. There was a vulnerability identified when the screen shot below was taken but the website was patched/updated very soon since taken.

There is still one plugin showing an issue - wpDataTables, however this is not relevant to XYZ. This has been set as ignore now so we shouldn't see the warning for it anymore.

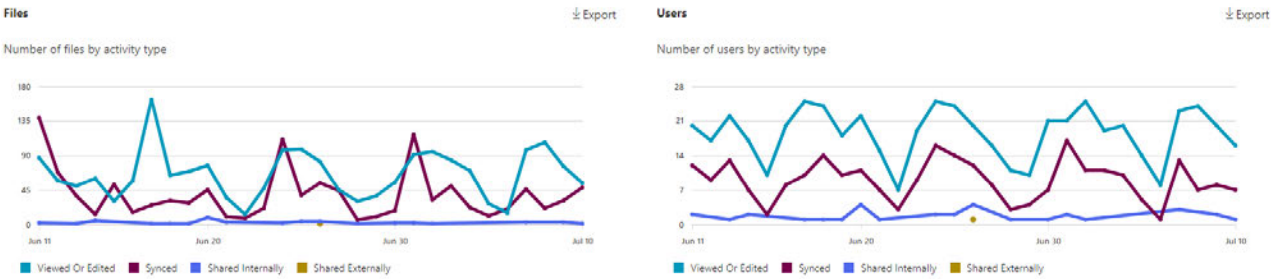




Sharepoint and OneDrive Storage Usage & Trends

Sharepoint currently has 1.30TB available of 1.87TB limit.

OneDrive Storage – Limit 1TB per user



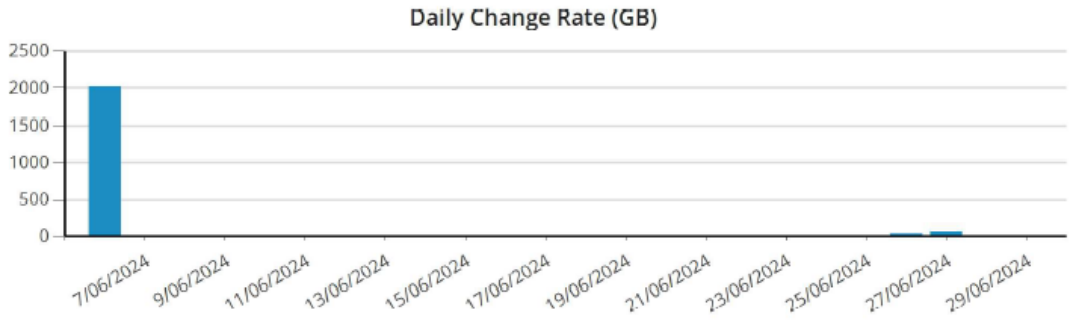
Owner principal name	Last activity date (UTC) ⓘ	Files	Active files	Storage used (MB)
	Wednesday, July 10, 2024	27,753	235	143,609
	Tuesday, July 9, 2024	3,677	32	83,474
	Wednesday, July 10, 2024	8,922	33	60,568
	Monday, July 8, 2024	17,852	128	42,759
	Tuesday, July 9, 2024	7,505	16	37,241
	Wednesday, July 10, 2024	1,081	97	32,532
	Wednesday, July 10, 2024	4,611	13	26,802
	Wednesday, July 10, 2024	10,887	67	25,945
	Wednesday, July 10, 2024	2,585	95	25,031
	Tuesday, June 25, 2024	330	3	24,843

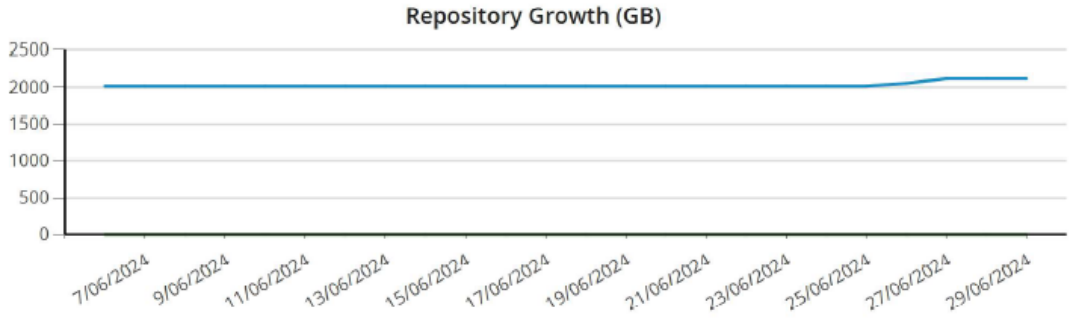
Veeam 365 Backup Status

There are 74 licenses.
There were no backup errors and all backups were processed.

[redacted]	[redacted]	Backup	Success	Transferred: 95.5 MB (181 items) at 71.2...	12/07/2024 8:00 am
		Backup	Success	Transferred: 316.0 MB (159 items) at 244....	12/07/2024 4:00 am
		Backup	Success	Transferred: 135.9 MB (178 items) at 78.2...	12/07/2024 12:00 am
		Backup	Success	Transferred: 1.0 GB (896 items) at 757.8 K...	11/07/2024 8:00 pm
		Backup	Success	Transferred: 934.9 MB (987 items) at 542....	11/07/2024 4:00 pm
		Backup	Success	Transferred: 1.4 GB (1415 items) at 856.8...	11/07/2024 12:00 pm
		Backup	Success	Transferred: 1.9 GB (553 items) at 1.3 MB...	11/07/2024 8:00 am
		Backup	Success	Transferred: 4.8 MB (30 items) at 3.7 KB/...	11/07/2024 4:00 am
		Backup	Success	Transferred: 31.6 MB (144 items) at 16.7...	11/07/2024 12:00 am
		Backup	Success	Transferred: 419.1 MB (519 items) at 271....	10/07/2024 8:00 pm
		Backup	Success	Transferred: 1.2 GB (1444 items) at 201.2...	10/07/2024 4:00 pm
		Backup	Success	Transferred: 450.8 MB (1288 items) at 29...	10/07/2024 12:00 pm
		Backup	Success	Transferred: 100.0 MB (245 items) at 84.2...	10/07/2024 8:00 am
		Backup	Success	Transferred: 40.3 MB (68 items) at 30.1 K...	10/07/2024 4:00 am
		Backup	Success	Transferred: 13.8 MB (41 items) at 6.1 KB...	10/07/2024 12:00 am
		Backup	Success	Transferred: 786.5 MB (2307 items) at 13...	9/07/2024 8:00 pm
		Backup	Success	Transferred: 46.5 GB (28288 items) at 3.0...	9/07/2024 12:00 pm

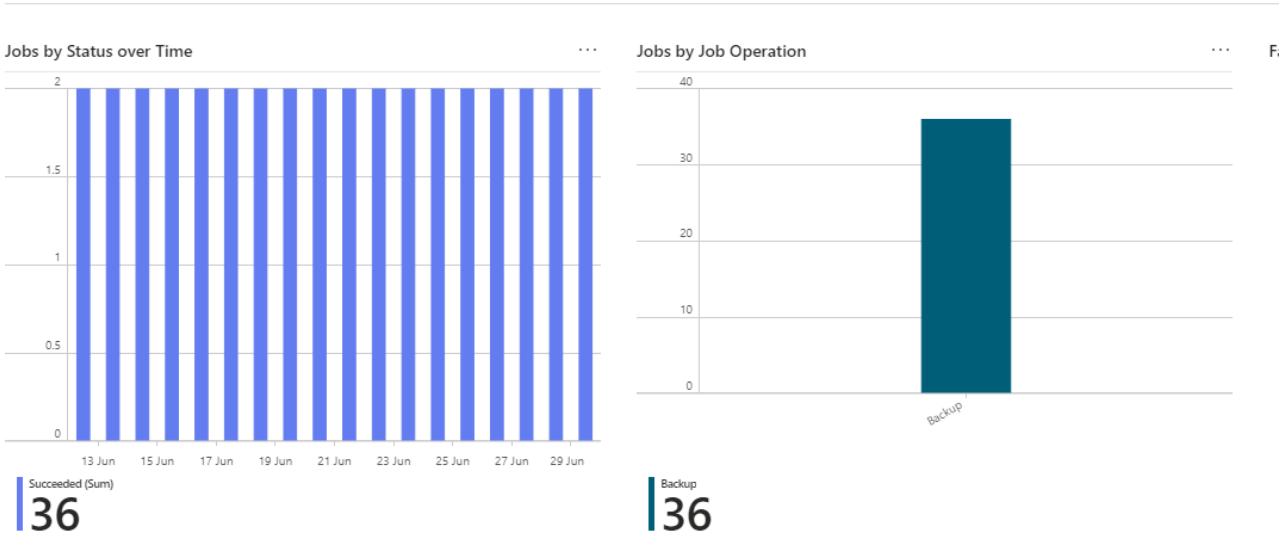
Repository: [redacted]

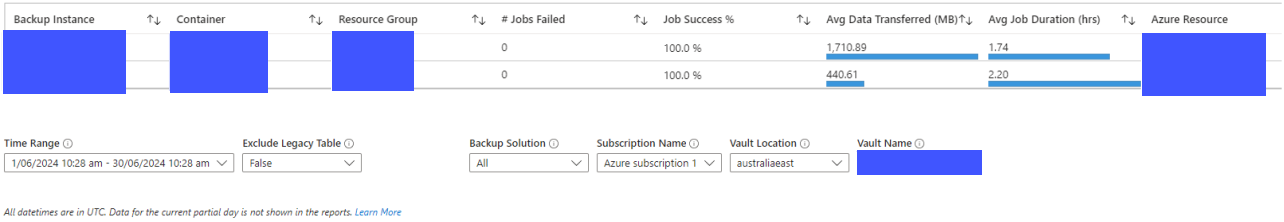


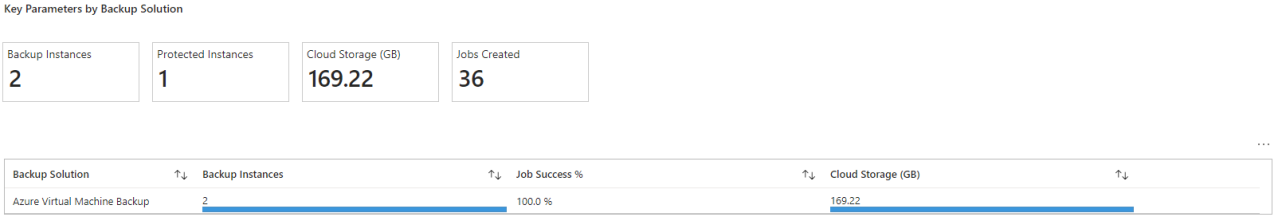


Azure Backup Status

There were no backup errors and all backups were processed.







Darkweb Reporting

Solution to detect your compromised credentials in real time on the Dark Web

- Domain Monitoring – No Compromises
- Personal Email Address Monitoring – No Compromises
- IP Address Monitoring – No Compromise

Quarterly MIT Red Team vs Blue Team Activities – 2nd Quarter Report

No Red Ream action for this period.

Actions planned for next month include data centre vulnerability scanning and Linux server vulnerability scanning.

MIT NSOC Vulnerability Hunting and Actions Taken

Generic search for vulnerabilities across all vendors and software that

- Count relevant vulnerabilities found
- Count of required actions taken

Our NSOC team hunted and identified 67 potential vulnerabilities.

- One of the Microsoft vulnerability (Phishing campaign targeting New Zealand organisations) - This was resolved by applying 365 token security protection to tenancies that had 365 E5 license. Patched Successfully.
- Other 5 Microsoft Vulnerabilities were addressed by either applying updates or patches
- One of the Veeam vulnerability has been resolved by applying the latest update to the new VSPC server.
- 3 WordPress vulnerabilities are resolved as all active woocommerce sites on our development servers are on 8.9.3
- One of the WordPress vulnerability (Hackers deploy crypto drainers on thousands of WordPress sites) - update XYZ Wordpress
- Microsoft Outlook Zero Click flaw was patched within 24 hours of being reported

See below summary of all vulnerabilities identified for June.

Vendor/Application	**Count**
Fortinet	4
HP	1
Lenovo	1
Linux	8
Microsoft Servers and Windows workstation 10 or 11 operating systems	12
QNAP	2
SonicWall Firewall	2
Synology	5
Veeam backup software	2
Wordpress	30
Grand Total	**67**

There are 24 vendors/applications that our MIT 24/7 NSOC team hunt out as follows:

Cisco Meraki, Watchdog, LastPass, Lenovo, Crowdstrike, Connectwise, Cloudflare, Macs, SonicWall, Veeam Backup, Microsoft Servers and Windows workstation 10 or 11 operating systems, Kaseya, Shadowprotect Backup, Malwarebytes, Mikrotik routers, Ubiquiti, HP, Ruckus, Linux, Wordpress, Fortinet, QNAP, Synology