

JUNE UNIT REPORTS 2022



HEALTH
SCIENCES
CHIEF INFORMATION
OFFICE

APPLICATIONS - RAY AVILA

SYSTEMS - PHIL MARQUEZ

SECURITY - MIKE MEYER

TECHNOLOGY SUPPORT - RICK ADCOCK

FOR MORE DETAILS:

Marcia Sletten, msletten@salud.unm.edu

APPLICATIONS TEAM

ACCOMPLISHMENTS

- Deployed Recist Application
- Closed out SharePoint 2010 servers for July Decommission
- Updated Faculty and Student databases for new curriculum year
- Imported new MD Students into Academic DB

IN-PROGRESS

- Zoom Security Enhancement
- M365 Intune Implementation

METRICS

M365 Teams Usage

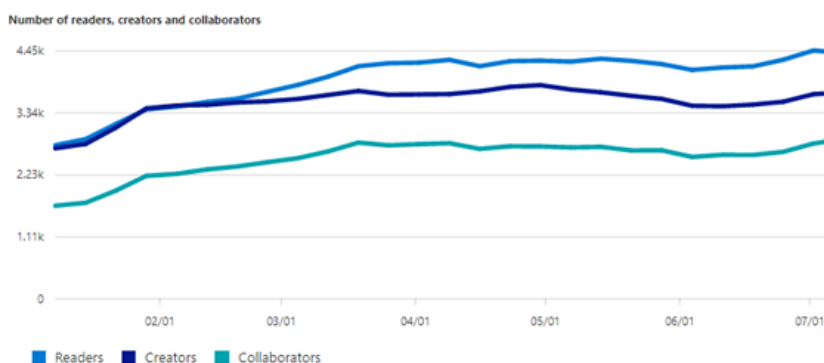
Changes in content collaboration in the last 90 days

13% ▲

[How is this number calculated?](#)

Content collaboration is defined as one person creating and sharing an Office file, and then at least one other person reading it.

Number of readers, creators, and collaborators over time



METRICS (CONTINUED)

M365 Teams Usage

Changes in after-hours collaboration in the last 90 days

12% ▼

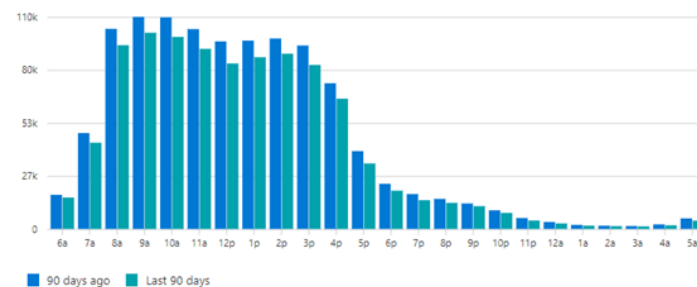
How is this number calculated? ⓘ

This represents time employees spend in meetings, emails, or chats outside the work hours defined in their Outlook calendar settings.

Viva Insights allows you to compare trends in collaboration after hours over time.

Collaboration hours by time of day

Total employee collaboration hours per week



Changes in meeting length and attendees in the last 90 days

4% ▼

How is this number calculated? ⓘ

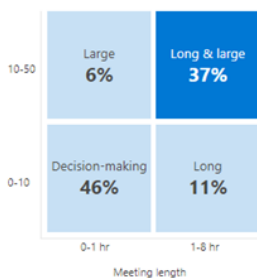
Meetings are considered long when they last more than an hour, and large when more than eight people attend.

Viva Insights allows you to compare trends in meeting effectiveness.

Meeting length and number of attendees

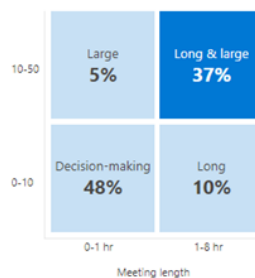
90 days ago

Number of attendees

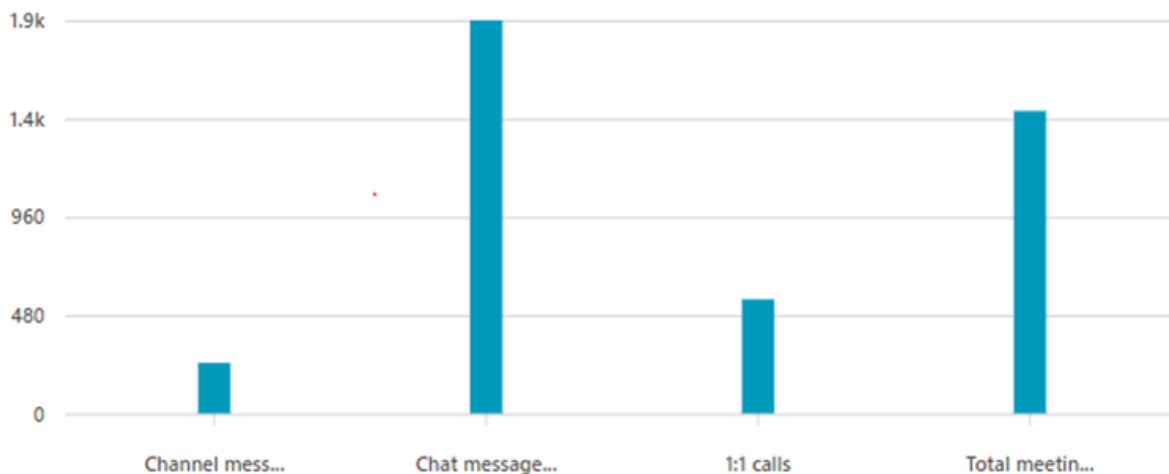


Last 90 days

Number of attendees



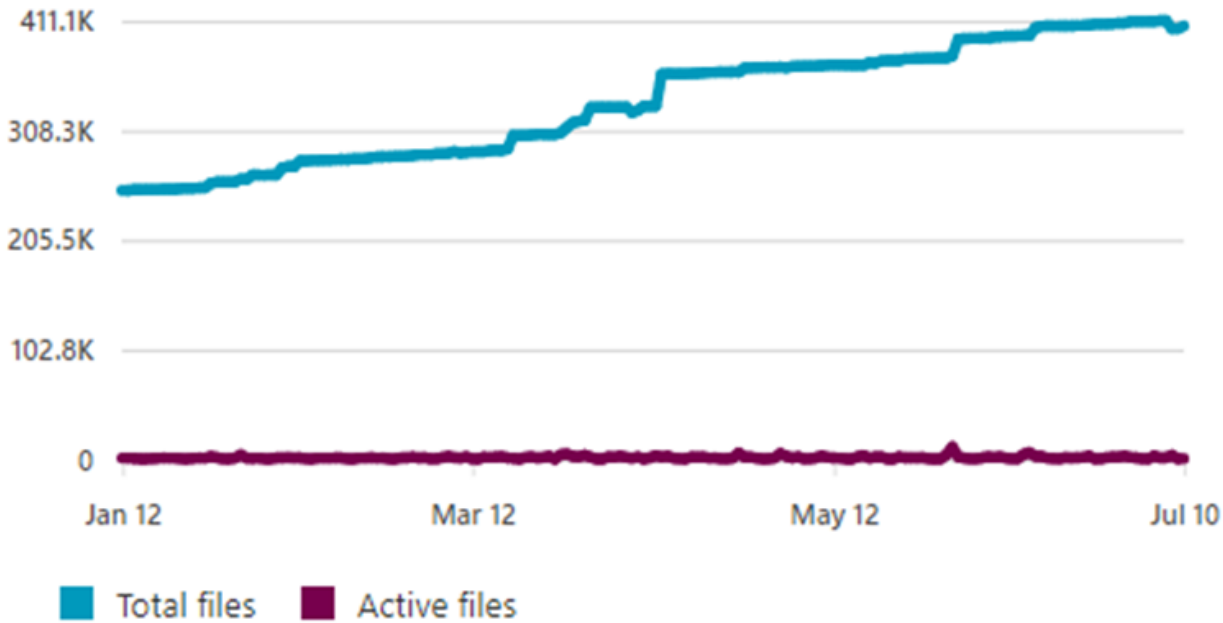
Number of total users by activity type over the selected time period



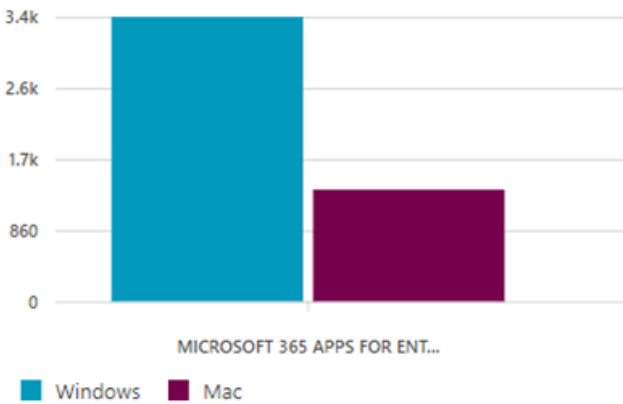
METRICS (CONTINUED)

- M365 Usage

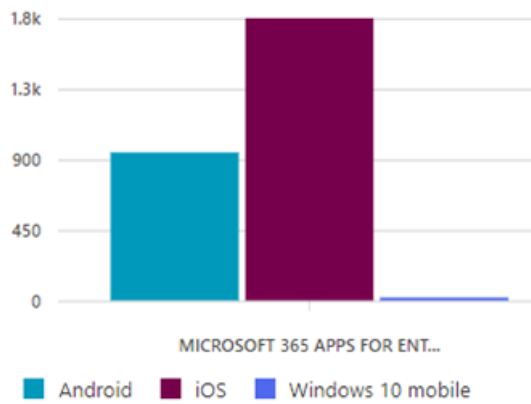
Number of total and active files



Office activations for desktop clients/apps across platforms



Office activations for mobile apps across platforms



RECOGNITION

Eliot Knight for having completed a great deal of work toward rebuilding Learning Central courses over the past 2 months.

SYSTEMS TEAM

ACCOMPLISHMENTS

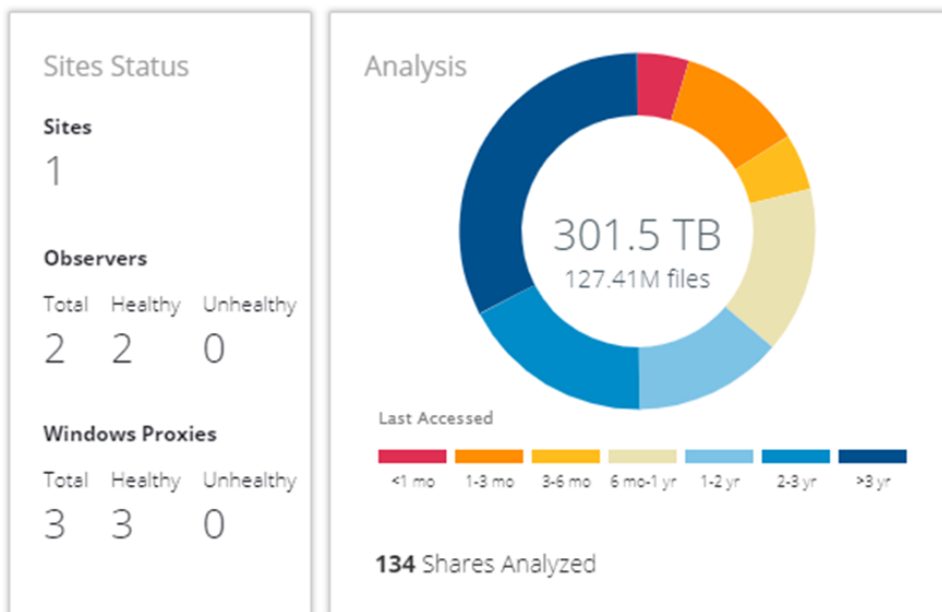
- No new major projects in June
- On Site Network Attached Storage replacement (Pure Storage)
 - COMPLETED migrations of network folders from NetApp and Dell NAS (H:\Home, O:\ and N:\) to new Pure Storage appliance
- Completed June monthly HSC Systems maintenance window on May 21 (7-9am)
 - HSC-PrintServer OS upgrade/reboot
 - \Homes shared folder cutovers
 - No issues!
- FILLED new position for Cloud Administrator in Systems team
 - Congratulations to Judson Carter who will take on this new role
 - Posted backfill position for Systems/Network Analyst 3
- Metallic cloud backup
 - Completed configuration of CDD data backup licenses in Metallic

IN-PROGRESS

- Metallic cloud backup
 - Still working to add licensing to provide Metallic backup for remaining unprotected data. All data on NetApp filers was retained with shadow copies, versioning, and replication. This will extend cloud backup and ransomware protection to include that data as well.
 - Pending resolution of move of data to cold storage solution (in progress)
- Planning for July Monthly maintenance period - 7/16/22 from 7-9am
 - Updates to PasswordState application
 - Hyper-V migrations to Nutanix

METRICS

- System availability:
 - No systems downtime
- This month's updates from Komprise Data Analysis tools showing graphs and metrics across all data stores
 - Aging reports showing data volumes by Last Accessed Dates
 - Ongoing Migrations
 - Space consumed by Top Shares

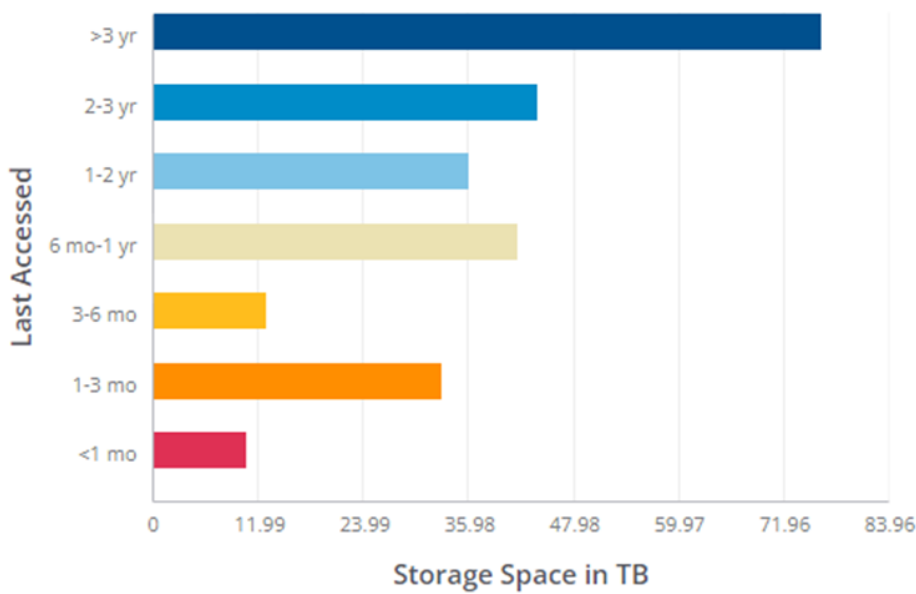


Migrations

	Active	Paused	Actionable errors	Ready for cutover	Ready for final	Completed
	2	0	1	0	0	117
Site	Active	Paused	Actionable errors	Ready for cutover	Ready for final	Completed
UNMHSC	2	0	1	0	0	117

METRICS (CONTINUED)

Data Heatmap by Time of Last Access



Size

254.2 TB

Files

91.16M

[View files found](#)

RECOGNITION

Geoff Johnson, Rick Adcock and Ray Avila for supporting the hiring process for the Cloud Administrator position. I know it's an added burden so thank you all!

INFORMATION SECURITY OFFICE

ACCOMPLISHMENTS

ACCOMPLISHMENT	IMPACT
Executed statement of work with contractor (Optiv) to conduct an executive incident response exercise (ransomware) in early November. Held first planning meeting with Optiv.	Will provide executives insight into the dilemmas of ransomware attacks, particularly the “pay or not pay” paradox.
Eight staff from Cyber Security, Network Security and ISO attended two-day Tenable operator course.	Develop proficiency in our primary tool for identifying and remediating security vulnerabilities.
Network Security and ISO ran two phishing “challenges” in July.	Reducing successful phishing attempts reduces our risk exposure to ransomware attacks.
Wave 1 IT inventory complete.	Statutory requirement.
Participated in various planning meetings for CLA audit to begin in Aug.	CLA audit will encompass the entire network this year, not only clinical functions.

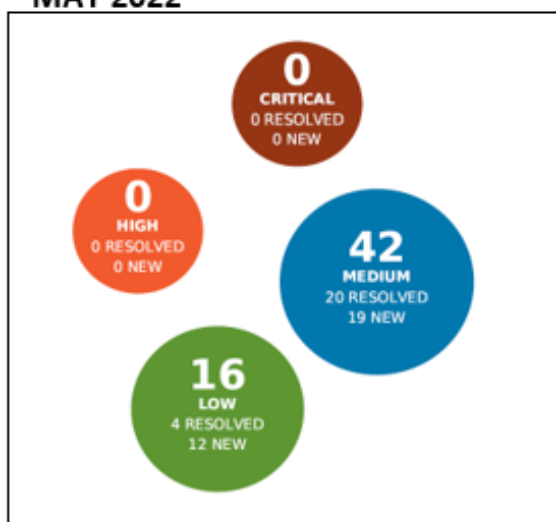
IN-PROGRESS

ACTIVITY	OBJECTIVE(S)
Implement Innovation Center Cyber Security using the U.S. government Cybersecurity Maturity Model Certification (CMMC) standards.	Conduct and document security reviews and establish security controls that are consistent and acceptable for the processing of ePHI in a cloud environment.
Improve Cyber Security Incident Response	Bring clarity to our incident response policy and plans. Provide “ransomware playbook” to speed response in the next incident. Conduct a major incident response in November 2022.
Improve Interior Security Controls	Implement additional security measures to limit lateral movement on our network if another attack penetrates our perimeter defenses.
Phishing Training	Conduct effective training in recognizing phishing attacks. Our target “click rate” is 5%. Current rate is around 30%.
Vulnerability Management	The goal of this effort for 2022 is to identify and begin to reduce our critical vulnerabilities. We have completed the first phase of this effort by successfully deploying a new product (Tenable.IO) to scan the entire network. Now the work is remediating the vulnerabilities found.
Protected DNS (pDNS) Collaboration with Main Campus	pDNS relies on threat intelligence to filter suspicious Internet addresses and is one of the major defenses against phishing, therefore ransomware. Collaboration with Main Campus will reduce overall cost for the service.

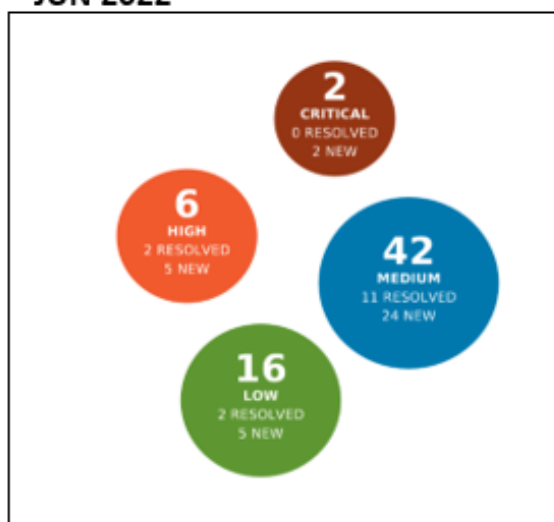
METRICS

Change requests	10
Certificate requests	1
Software and Cloud service security reviews	25
DUA/SFTP Data Transfer Support Requests	19
Other Support Request	38
Perimeter Vulnerabilities	Critical - 2 (+2) High - 6 (+6) Medium - 42 (no change) Low - 16 (no-change)
Critical Vulnerabilities on servers	June - 2,314
Malicious email blocked by email firewall	15,155,881
Outbound email blocks for PHI content	144

**Perimeter Vulnerabilities
MAY 2022**



**Perimeter Vulnerabilities
JUN 2022**



METRICS (CONTINUED)

Proofpoint Messages Processed and Rejected June 2022

Type	Messages	Percent
Blocked:PDR	10546189	61.52%
Accepted	3483163	20.31%
Blocked:Email Firewall	2609040	15.22%
Blocked:Spam	258123	1.5%
Blocked:Others	244537	1.42%
Blocked:Anti-Virus	271	0%
Blocked:Regulatory Compliance	144	0%
Blocked:Zero-Hour	94	0%
Total	17141561	100%

Notes:

PDR = Proofpoint Dynamic Reputation service

“Regulatory Compliance” = Outbound email containing ePHI not properly encrypted

Carbon Black EDR Threats Denied June 2022

— Sensor Action (4)	
Deny	466
Terminate	28
Allow	0
Allow and log	0

TECHNOLOGY SUPPORT

ACCOMPLISHMENTS

- Added the Department of Pathology to Microsoft Intune for workstation management
 - Enabled the ability to use passphrases instead of passwords on accounts
 - Hired a Technical Analyst 2 for the Classroom Technology Unit
-

IN-PROGRESS

- Remediation of unencrypted workstations
- Testing softphones for off-site access to the Automated Call Distribution system
- Creating a Microsoft Intune policy for the Mac operating system
- Creating a Cherwell workflow to correctly process requests to unblock MFA lockouts
- Working with UNMH on the deployment of Dragon Medical One

METRICS

January 1 – June 30 incidents and service request

	Service Requests	Incidents	Total
HSC IT Service Desk	1,218	352	<u>1,570</u>
Tier 2 Teams	1,120	179	1,299

HSC IT Service Desk Call Activity January 1 – June 30

Total Calls	8,193
Calls Answered	7,780
Calls Abandoned	413
Abandoned Rate	5.04%
Average Speed to Answer	<u>1:03</u>

RECOGNITION

Aaron Douglas for leading the Microsoft Intune technical implementation and taking the lead on the workstation management and enrollment features.