

Analytics Microsoft 365

Microsoft 365

Vinicius Mozart – MVP Datacenter and Cloud Management



Prevenção



Prevent



Detect



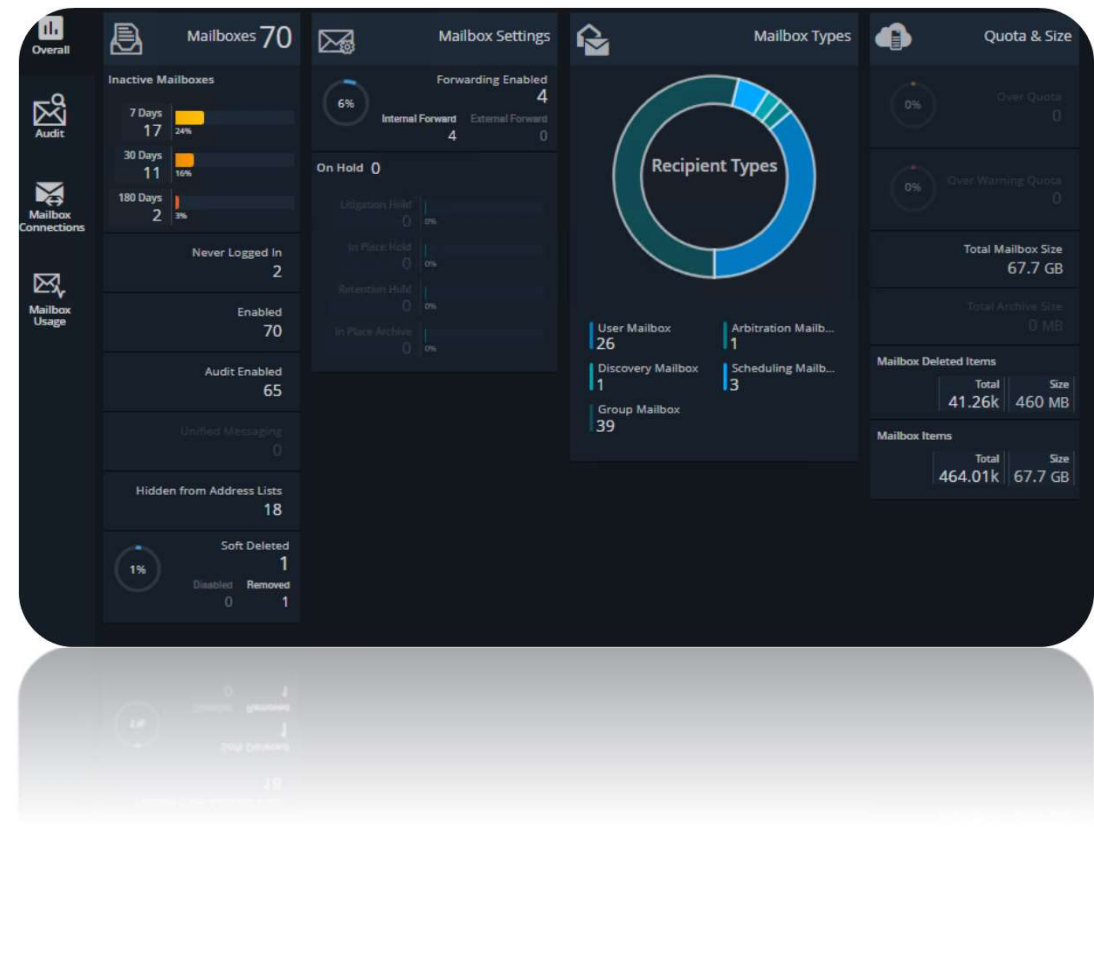
Investigate



Respond

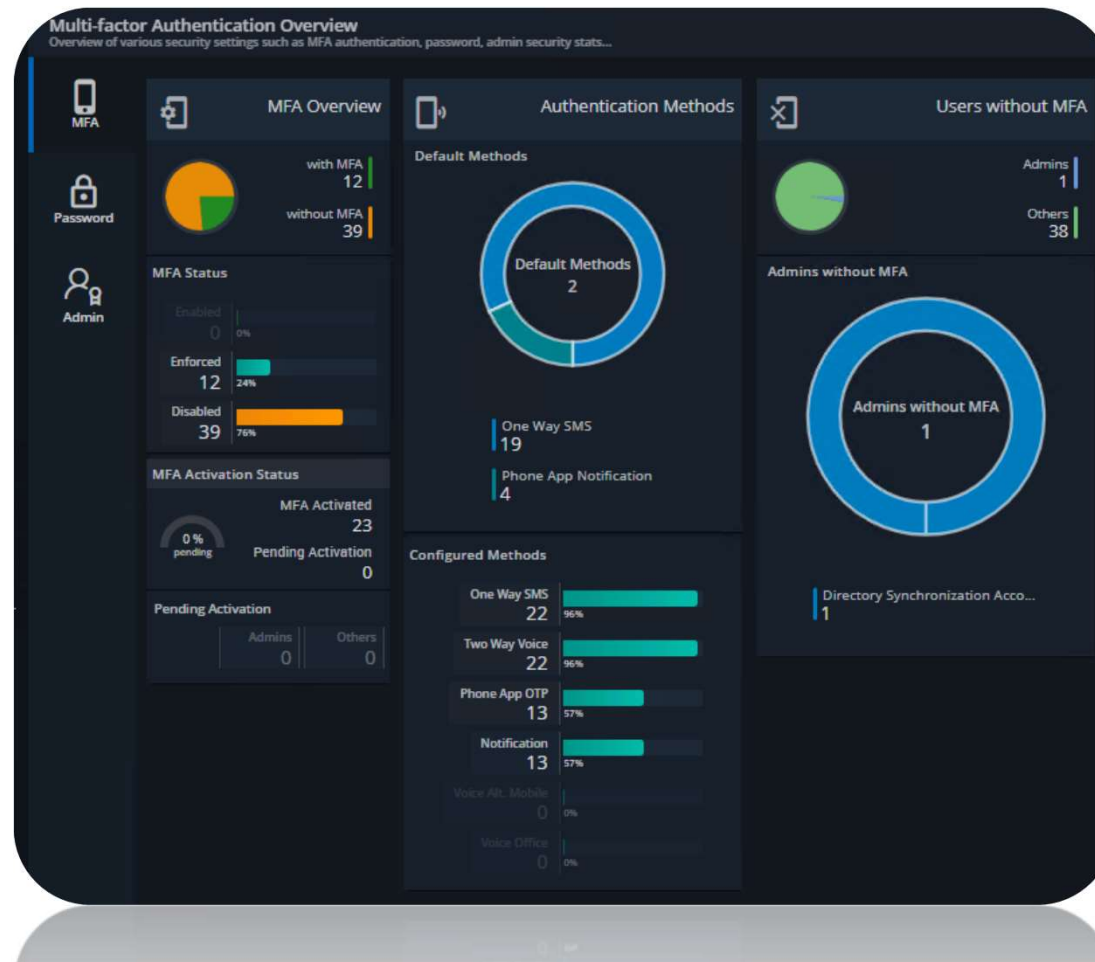
Usabilidade de ferramentas do Microsoft 365

Relatórios em tempo real sobre uso para análise e prevenção

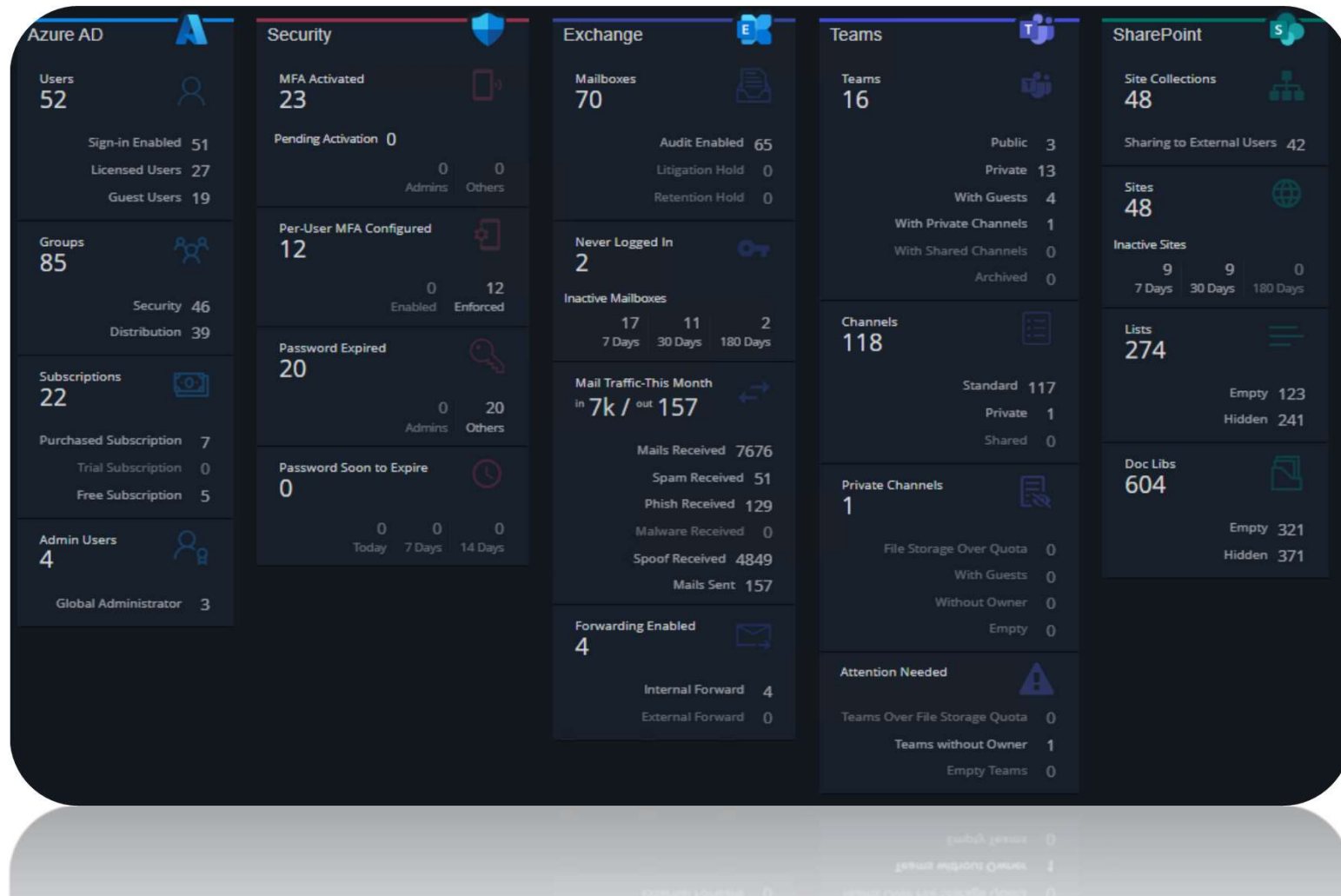


Visão geral de segurança do Microsoft 365

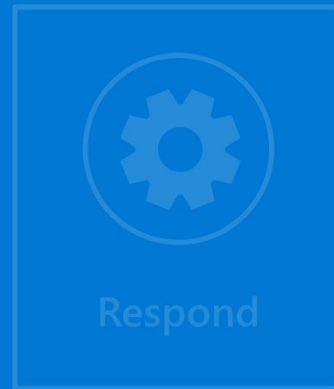
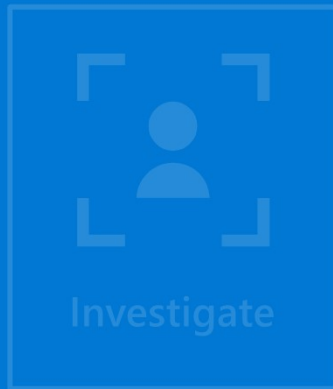
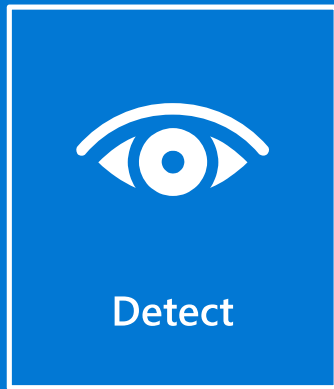
Prevenção em tempo real para configurações de segurança do Microsoft 365



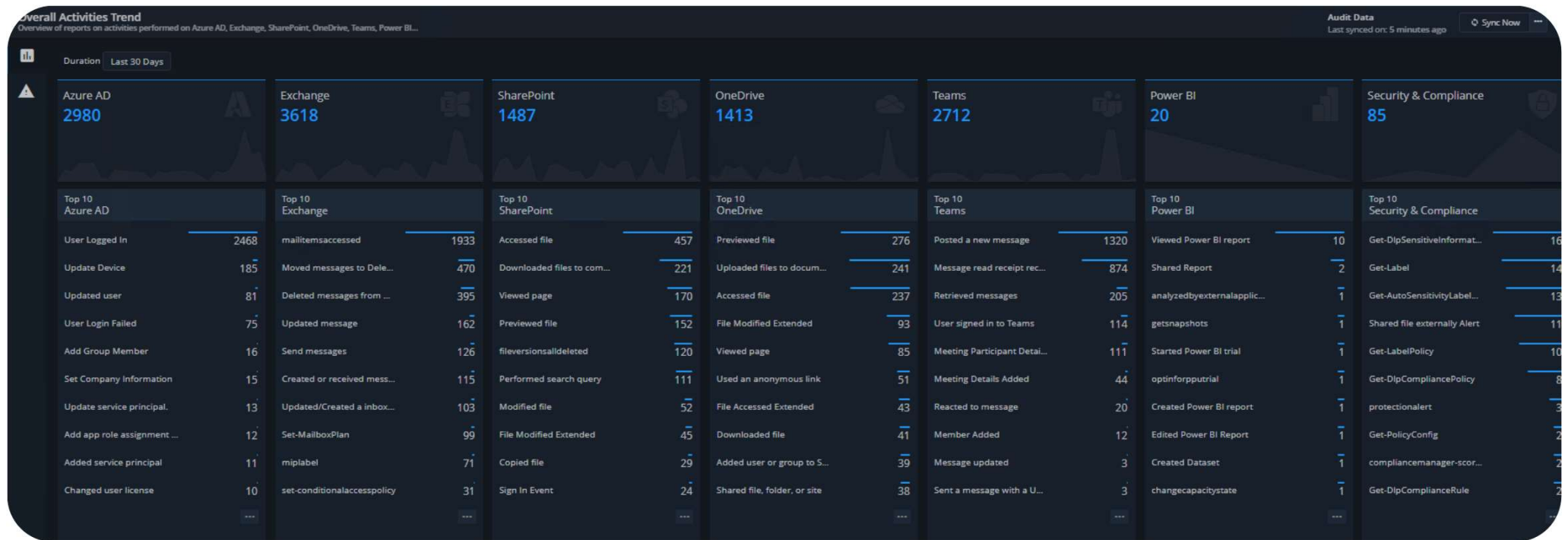
Dashboards separados por categoria



Detecção

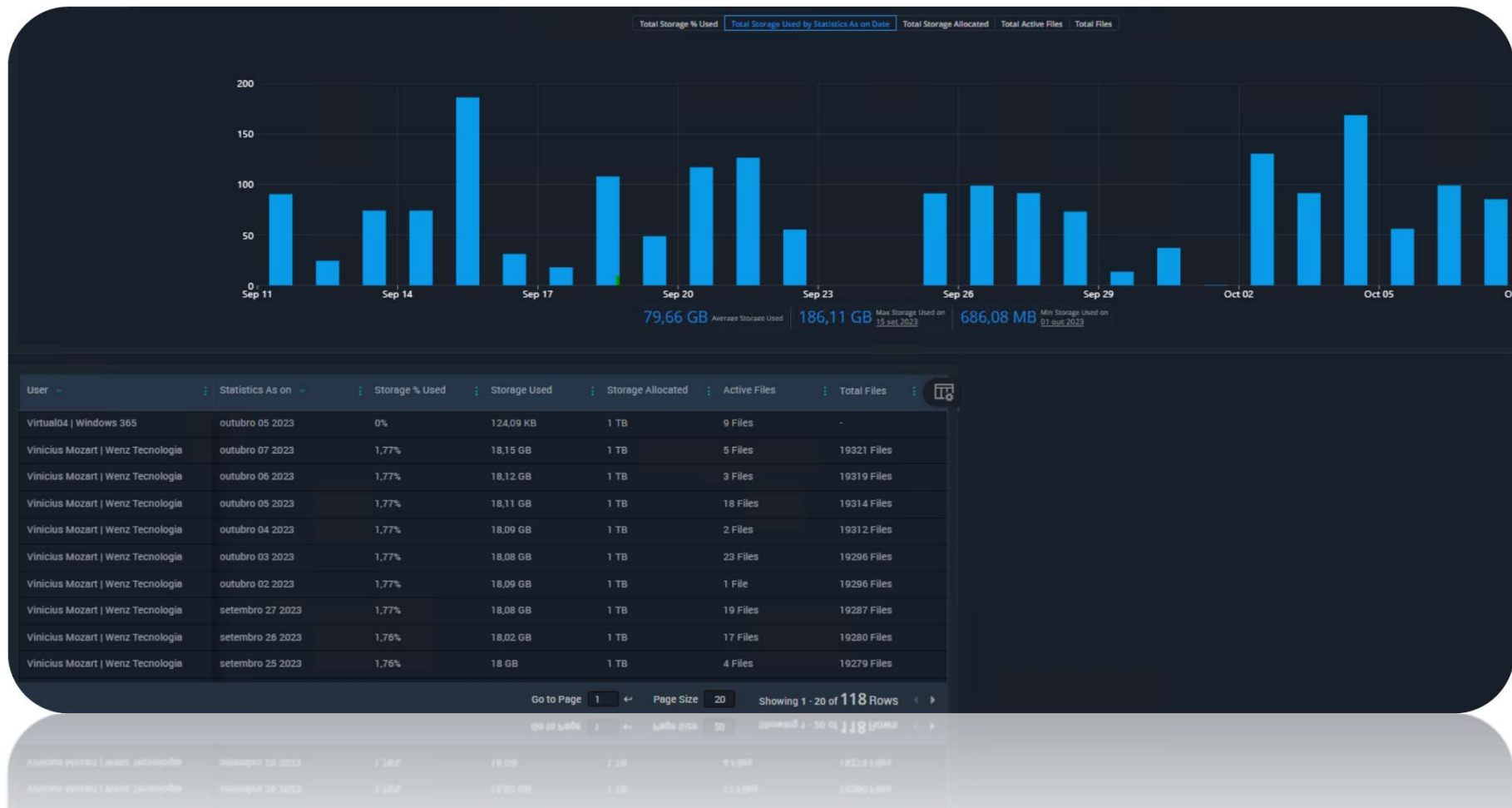


Detecção e atividades por categoria

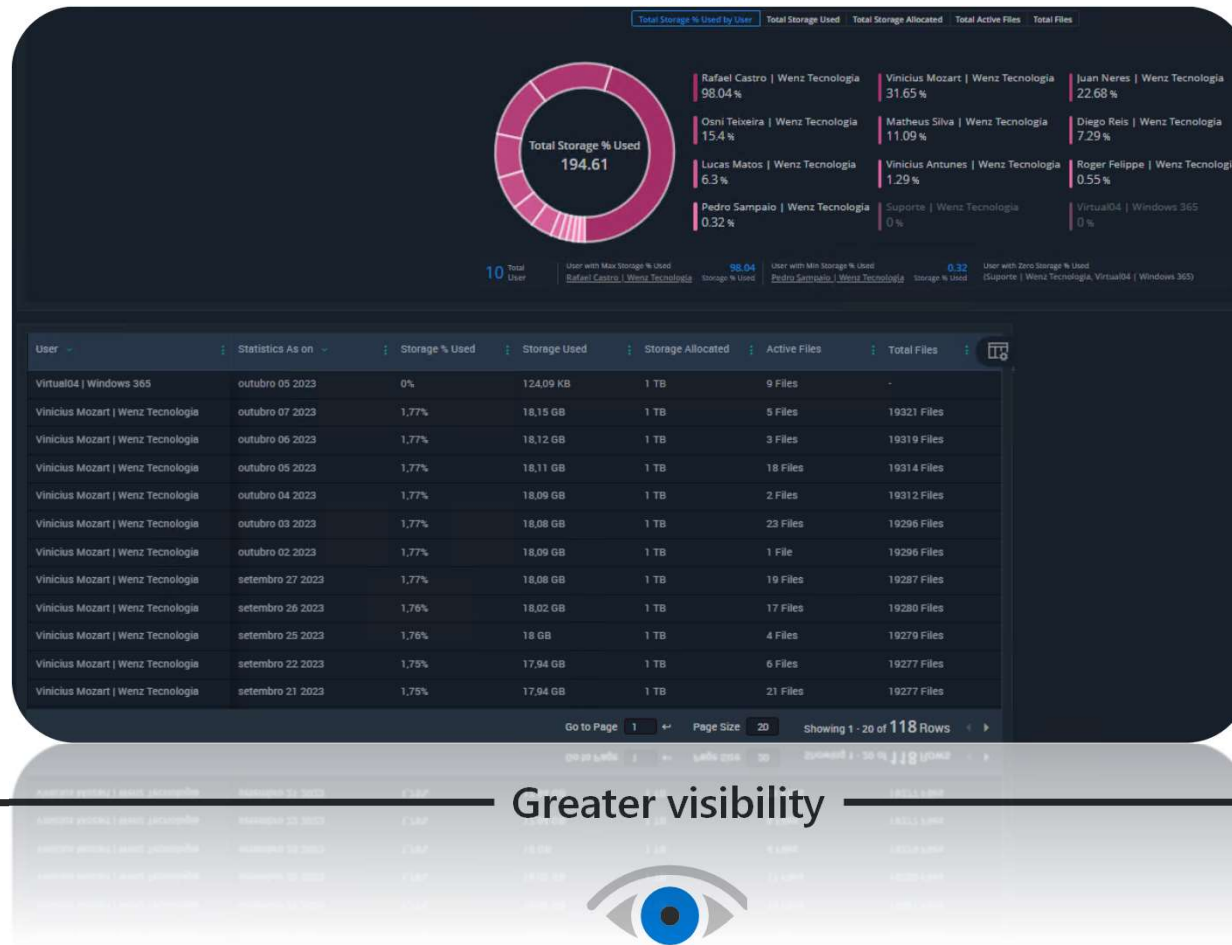


Detecção de uso

Mostrará o uso de ferramentas com relatórios individuais



Detecção de uso do storage separado por usuário



Greater visibility



Investigação



Prevent



Detect

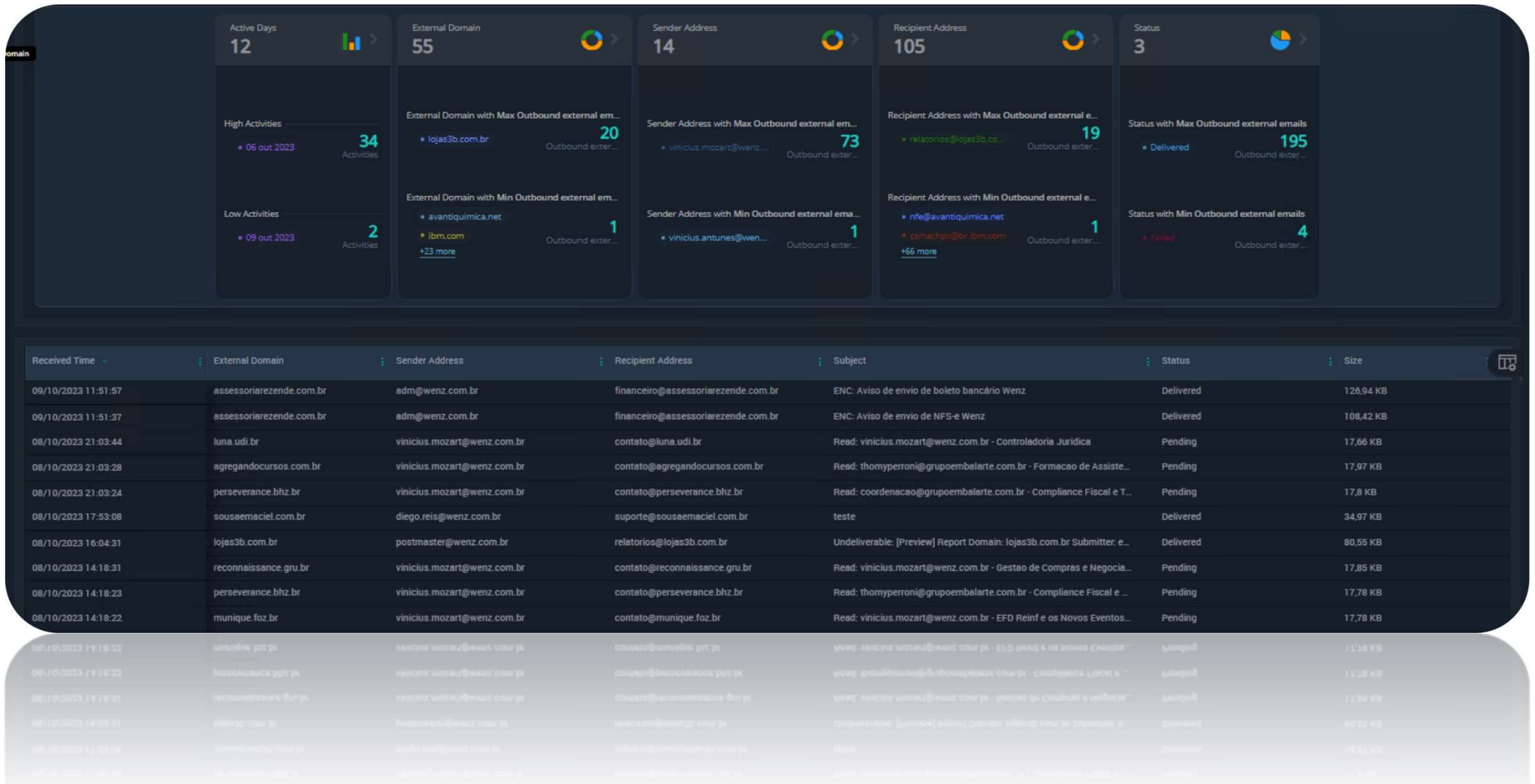


Investigate

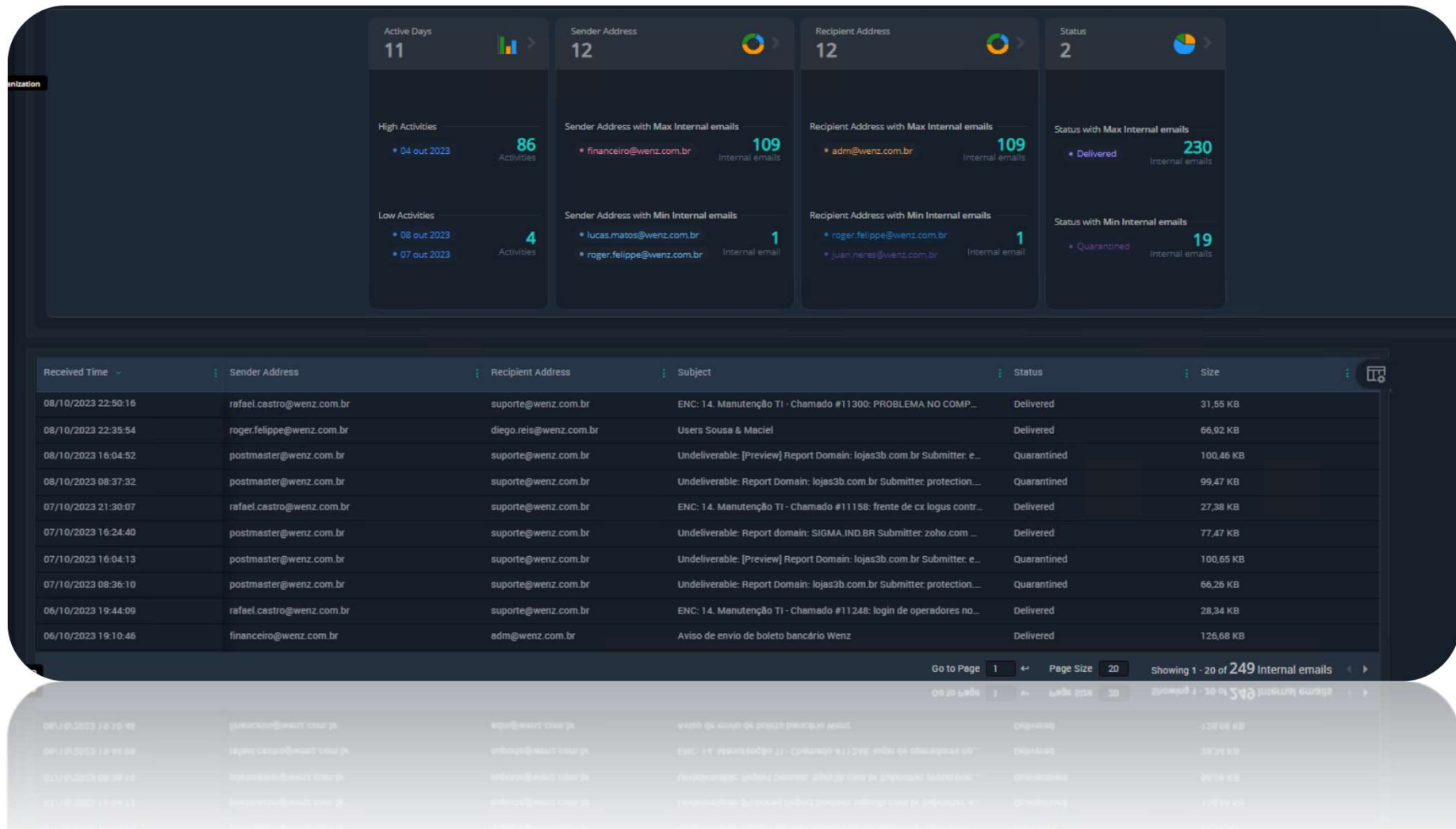


Respond

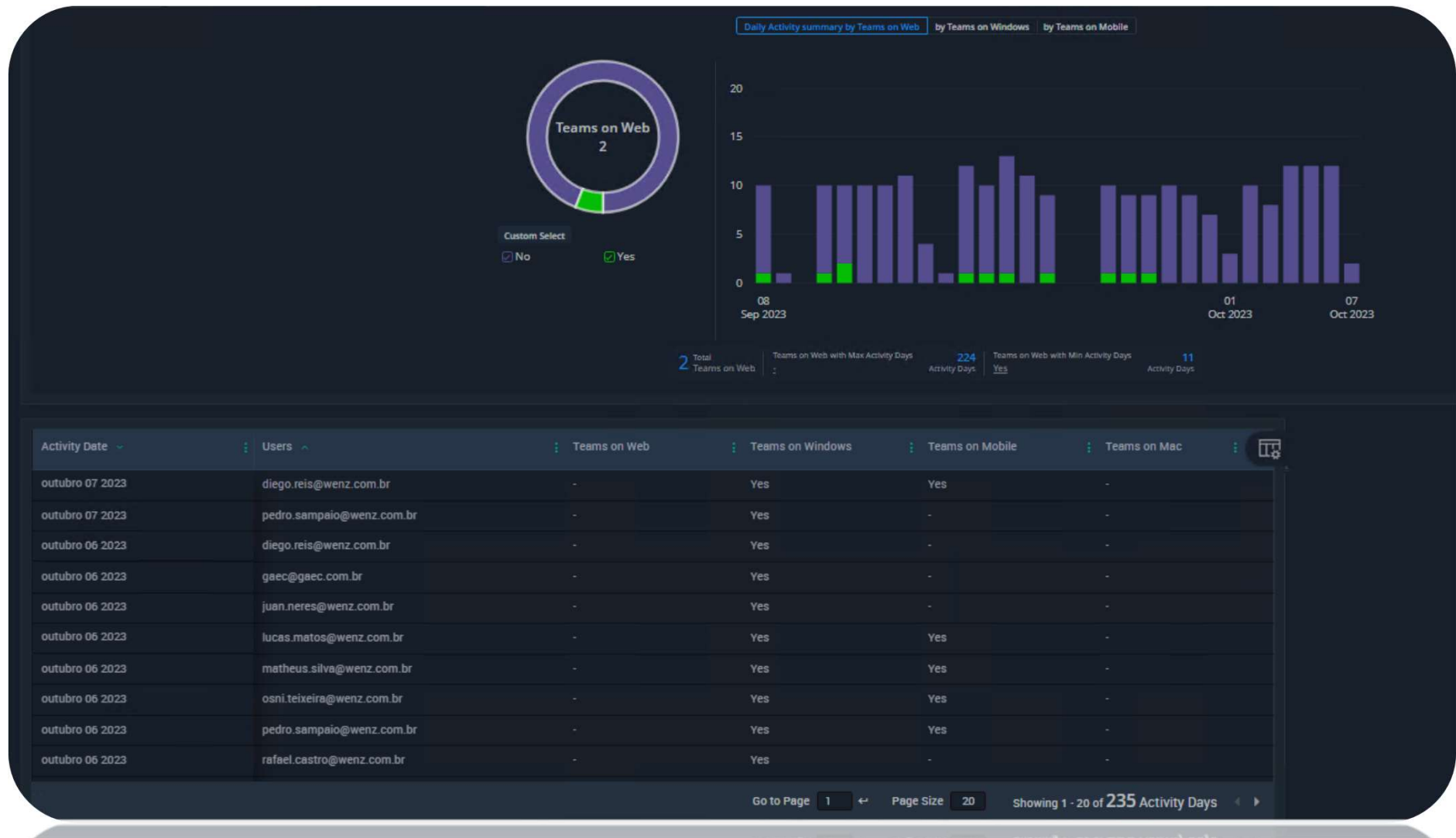
Investigação de e-mails enviados e recebidos (Externamente)



Investigação de troca de e-mails (Internos)



Investigação de usuários para formas de uso



Investigação de atividades de arquivos acessados

The screenshot displays the Microsoft Entra Audit Data interface, specifically the 'Activities Trend' section. The main view is 'Activities by All Users' for the 'Last 7 Days' period. A list of users is shown on the left, with 'vinicius.mozart@wenz.com.br' selected. The central panel shows a profile for 'Vinicius Mozart | Wenz Tecnologia' with an overall summary of 849 activities, all successful. Below this, there are charts for 'File and Folder Activities' (271 Success, 0 Failure) and 'Synchronization Activities' (36 Success, 0 Failure). The right panel shows 'Succeeded File and Folder Activities' for a specific event on Oct 07, 2023, at 07:24 PM, where a file was accessed at a SharePoint URL.

Activities By Users

User	Activities	Failure Rate
rafael.castro@wenz.com.br	1k	0% failure
VI vinicius.mozart@wenz.com.br	849	0% failure
SU suporte@wenz.com.br	598	0% failure
osni.teixeira@wenz.com.br	537	0% failure
matheus.silva@wenz.com.br	161	0% failure
diego.reis@wenz.com.br	158	0% failure
pedro.sampaio@wenz.com.br	122	0% failure
roger.felippe@wenz.com.br	112	0% failure
vinicius.antunes@wenz.com.br	99	0% failure
GA gaec@gaec.com.br	74	0% failure
VI virtual04@wenz.com.br	70	11% failure
lucas.matos@wenz.com.br	62	0% failure
juan.neres@wenz.com.br	40	0% failure
arfm	27	0% failure

Overall Summary

Category	Count
Azure AD	108
Exchange	366
SharePoint	29
OneDrive	307
Teams	39
Stream	0
Power BI	0
Security & Compliance	0

File and Folder Activities

Category	Success	Failure
File and Folder Activities	271	0

Synchronization Activities

Category	Success	Failure
Synchronization Activities	36	0

Succeeded File and Folder Activities

07 Oct 2023 07:24 PM | vinicius.mozart@wenz.com.br | File Accessed

Target(User/Group/File/Site/Mailbox...): https://wenzcombr-my.sharepoint.com/personal/vinicius_mozart_wenz_com/Documents/Wenz/Cursos/Azure Site Recovery/ASR-Modulo05/ASR-Modulo05/skins/remix/techsmith-smart-player.min.css

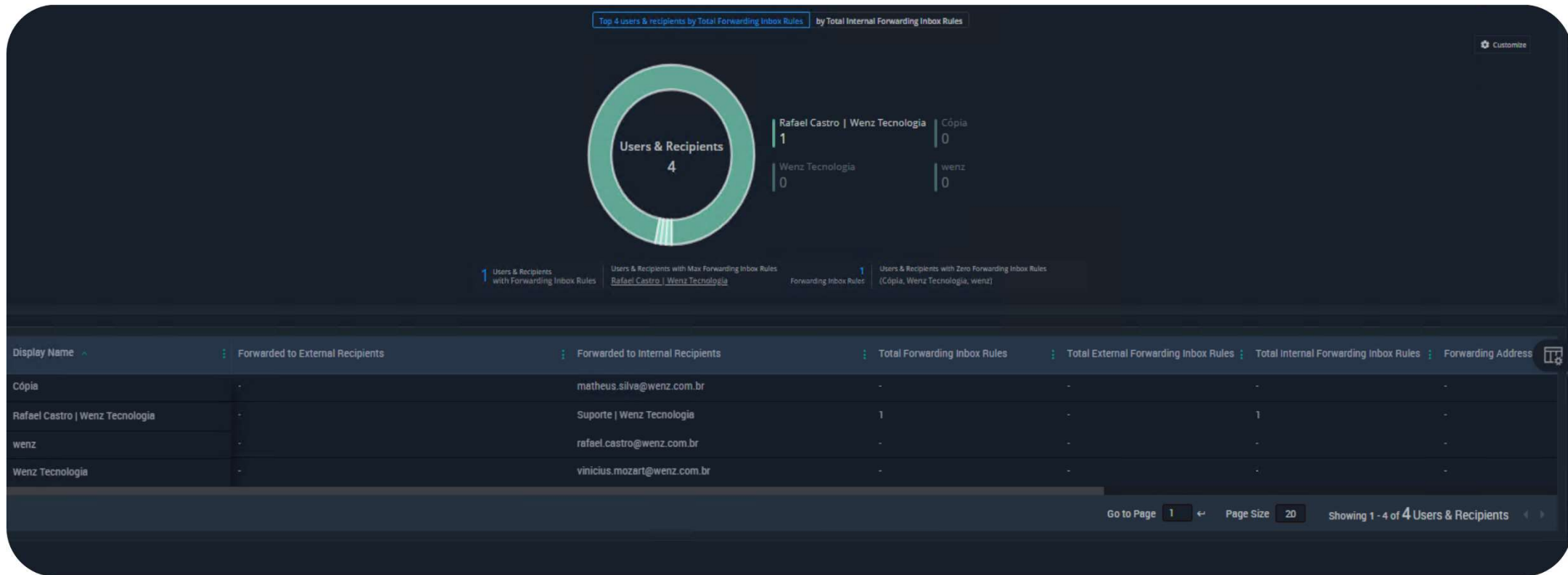
Spotlight Info

Event Time	: 07/10/2023 22:24:41
Target(User/Group/File/Site/Mailbox...)	: https://wenzcombr-my.sharepoint.com/personal/vinicius_mozart_wenz_com/Documents/Wenz/Cursos/Azure Site Recovery/ASR-Modulo05/ASR-Modulo05/skins/remix/techsmith-smart-player.min.css
User	: vinicius.mozart@wenz.com.br
Operation	: Accessed file
Workload	: One Drive

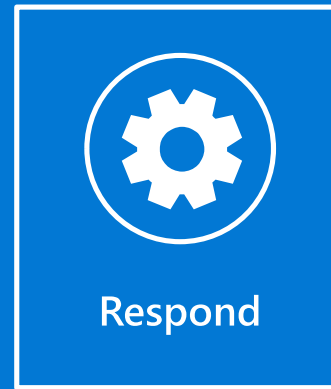
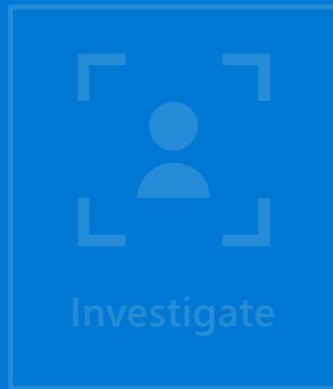
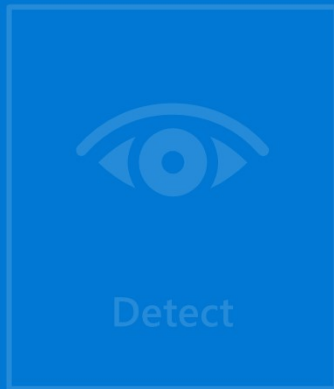
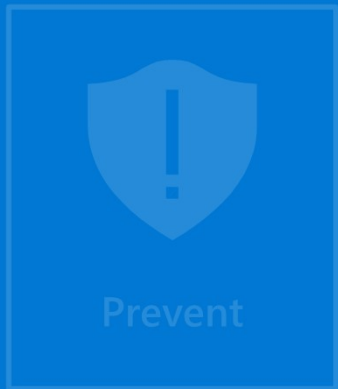
Other Info

Application Display Name	: -
Application Id	: -
Correlation Id	: afe6e1a0-80c4-4000-3a71-475d171c1377
Custom Unique ID	: No
Destination File Extension	: -
Destination File Name	: -
Destination Relative URL	: -
Detected Virus Info	: -
Do Not Distribute Event	: Yes
Event ID	: 90197f97-62b6-40cb-e967-08dbc7843331
Event Source	: SharePoint
File Sync Bytes Committed	: -
Implicit Share	: -
Is System Event	: No
Item Type	: File
List ID	: 66da6218-c0d5-43fa-86fa-f1fcbd283f5f
List Item Unique ID	: 9a218da9-2e40-41b1-b4ac-a234b4cc3397
Machine Domain Info	: -
Machine ID	: -
Operation Name	: File Accessed

Investigação de redirecionamentos de mailboxes



Respostas a incidentes



Templates para criação de alertas automáticos

56 Templates Available

Search Alert Policies

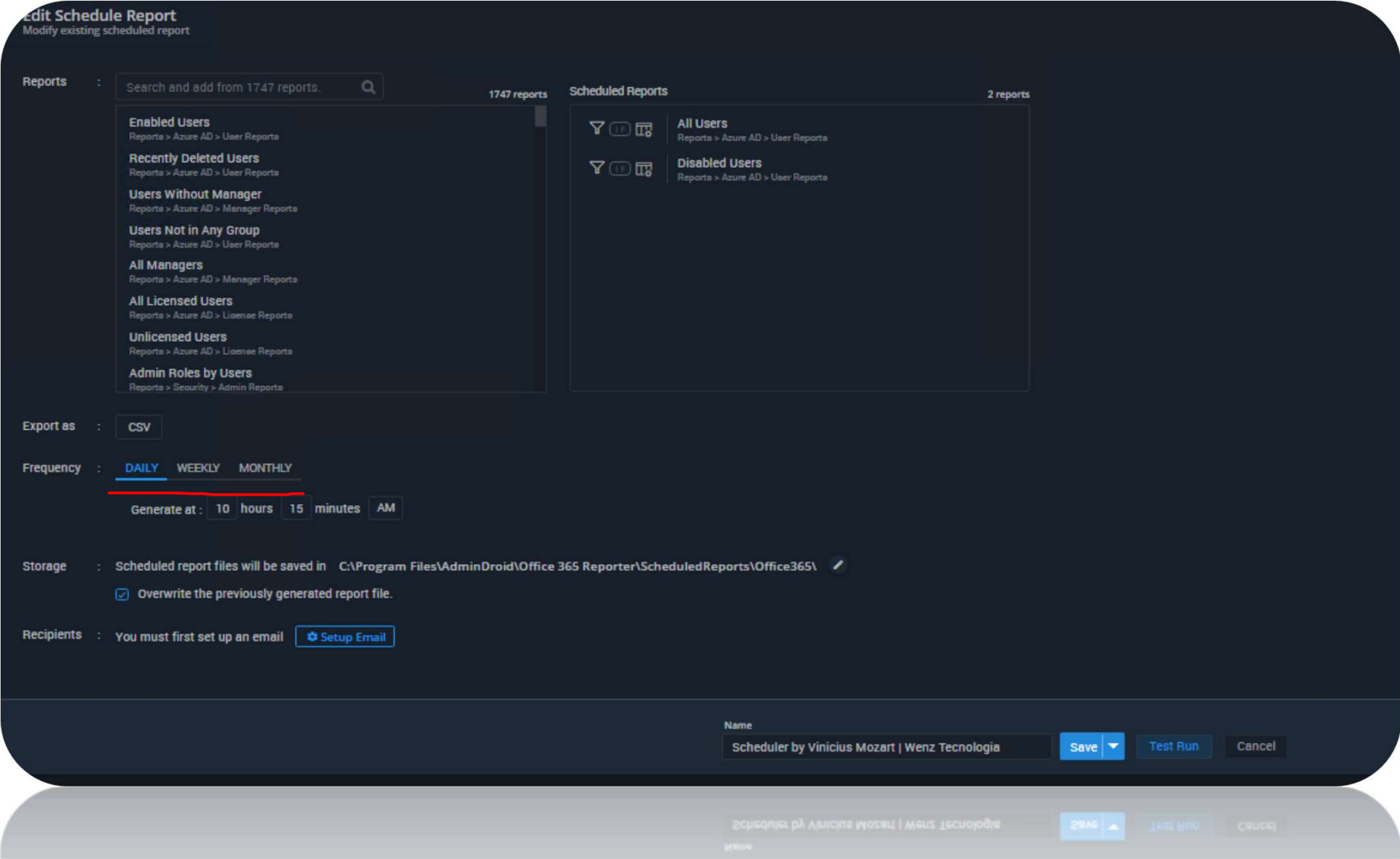
Severity

Labels

Request Template

Template Name	Description	Category	Possibility for	Action
Elevation of Global admin privilege	Creates an alert when a user is added to the global admin role in the organization.	Permission	0 alerts recently	Preview & Deploy
Elevation of Exchange admin privilege	Creates alerts if a user gets added to the Exchange admin role in the organization.	Permission	1 alerts recently	Preview & Deploy
Unusual volume of file deletion	Creates an alert with a list of users who recently deleted an unusual number of files in SharePoint or OneDrive in the organization.	Information governance	0 alerts recently	Preview & Deploy
Unusual volume of sign ins blocked by Access Policy	Creates an alert if an unusual number of sign-ins blocked due to access policy by comparing the same day in the previous week's blocked sign-ins.	Risky sign-ins	0 alerts recently	Preview & Deploy
Creation of external forwarded rule	Creates alerts when a new external forwarded email rule is created in Outlook by the users.	Threat Management	0 alerts recently	Preview & Deploy
User license changes	Creates alerts if any of the Office 365 licenses have been assigned/revoked for a user in the organization.	Configuration changes	12 alerts recently	Preview & Deploy
Anonymous link creations	Creates an alert with a list of new anonymous link created by users in the organization.	External sharing	19 alerts recently	Preview & Deploy
Teams private channel creations	Creates alerts whenever a private channel is created in Teams.	Information governance	0 alerts recently	Preview & Deploy
eDiscovery search created	Creates alerts when a user created an eDiscovery search or content search in the organization.	Information governance	4 alerts recently	Preview & Deploy
eDiscovery search exported or previewed	Creates alerts when a user previewed or exported any of the eDiscovery or content search results.	Information governance	0 alerts recently	Preview & Deploy
Unusual volume of external file sharing	Creates an alert with a list of users who recently shared an unusual number of files with any external users.	External sharing	0 alerts recently	Preview & Deploy
Malware campaign detected after delivery	Creates an alert with a list of new malware mails delivered to the users.	Threat Management	0 alerts recently	Preview & Deploy
Advanced Threat Protection configuration changes	Creates an alert if any of the Advanced Threat Protection configurations have been changed in the organization.	Configuration changes	3 alerts recently	Preview & Deploy
High level risky sign ins	Creates alerts if a high-level risky sign-in is detected for a user in the organization.	Risky sign-ins	0 alerts recently	Preview & Deploy

Agendamento de alertas



Envio de alertas via e-mail pré-definido

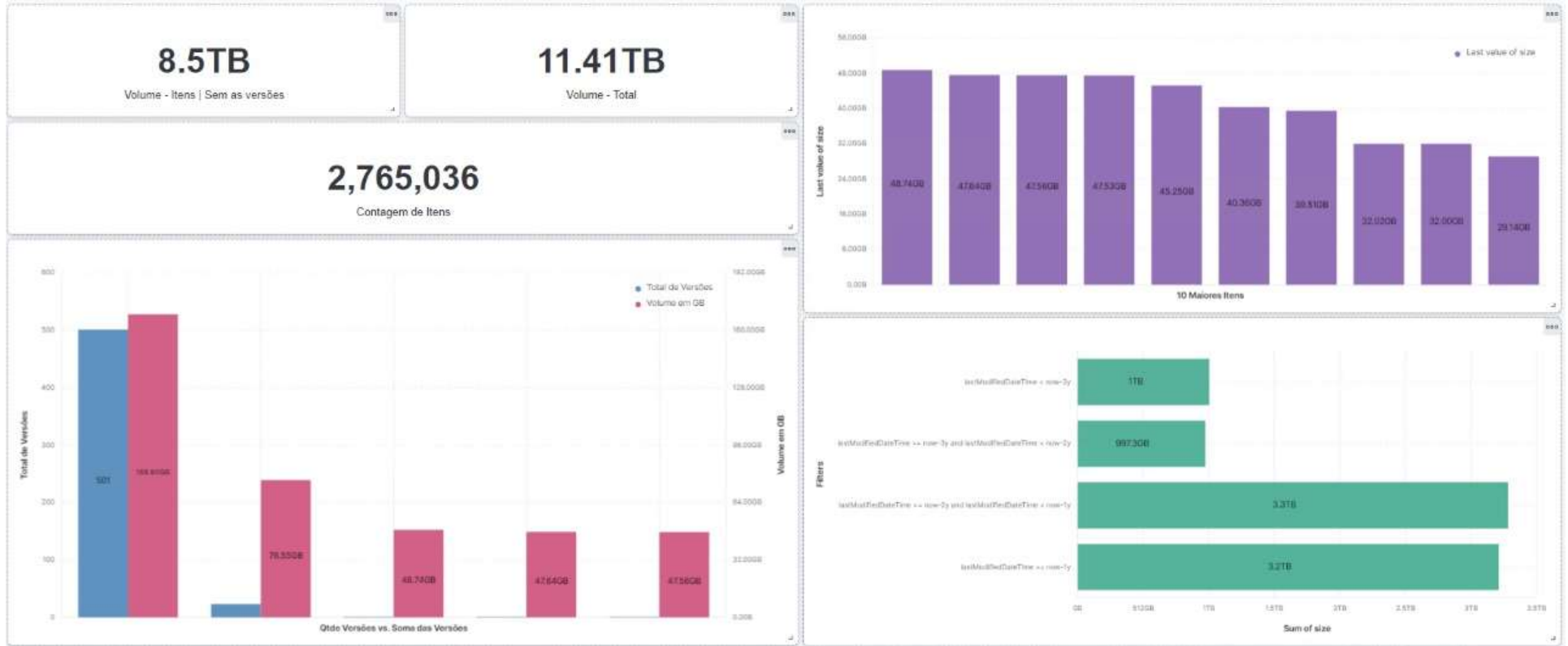
The screenshot displays the 'Edit Alert Policy' interface. On the left sidebar, navigation options include Dashboard, Alerts, Policies, Policy Templates, and Alert Reports. The main configuration area is titled 'Edit Alert Policy' and includes the following settings:

- Select Activity:** Users Added to Global Administrator Role (Audit > Security > Users Added as Admins)
- Filter:** Add Filter
- Alert Settings:** New Events (selected), Threshold, Compare
 - Create a single alert by grouping all the new Admin additions
 - Create separate alert for each new Admin additions
- Email Notification:** Send Email Notification (checked)
 - Recipients:** vinicius.mozart@wenz.com.br
 - Use a comma (,) to separate email addresses.
 - Configure sender mail to enable notification
 - Daily Notification Limit:** 24

On the right, the 'Alert Preview Console' is active, showing a table with columns: Status, Alert ID, Alert Message, and Generated Time. The table is currently empty, with a message: 'You do not have any alerts yet.'

SP Data Analytics

Dashboards em tempo real



Thank you.

