System4u MDR Service

Sample Security Assessment Report

Time: Last 30 days

Page: 1.1 Organization Score

License: Business Premium

1 Summary - 1.1 Organization Score (2024-03-27)

Organization Score

27 %

Risk Score: 55 / 75

Risk Scores

Module	Indicator	Value	Score
Cloud Identity (7)			
	1 Sign-in Failure Ratio (%)	7.73 %	1
	2 Untrusted Network Access Ratio (%)	100 %	3
	3 Conditional Access Bypass (%)	100 %	9
	4 Legacy Authentication (%)	0 %	0
	5 Single Factor Authentication (%)	100 %	9
	6 Single Factor Authentication - Admins (%)	100 %	9
	7 Global Roles Overassignment (%)	11.76 %	9
Endpoint (4)			
	1 Unmanaged Device Access (%)	100 %	9
	2 Non-compliant Device Access (%)	0 %	0
	3 Unencrypted devices (%)	40 %	3
	4 Last Contact Risk > 30 days (%)	80 %	3

Time
Last 30 days

Page
1.2 Recommendations

License
Business Premium

1 Summary - 1.2 Recommendations (2024-03-27)

Recommendations

Module ↑↓	Recommendation ↑
Cloud Identity (4)	
	Re-design your Conditional access policies as soon as possible.
	Please enable multi-factor authentication to enhance security.
	Please enable multi-factor authentication for all admin accounts to enhance security!
	Please reduce the number of global roles assigned to a single administrator account.
Endpoint (3)	
	Make sure your devices are properly managed or access is coming from a trusted network!
	Please ensure your devices are encrypted.
	Please ensure your devices connect to your MDM regularly. Otherwise, it is not possible to eval

Time: Last 30 days

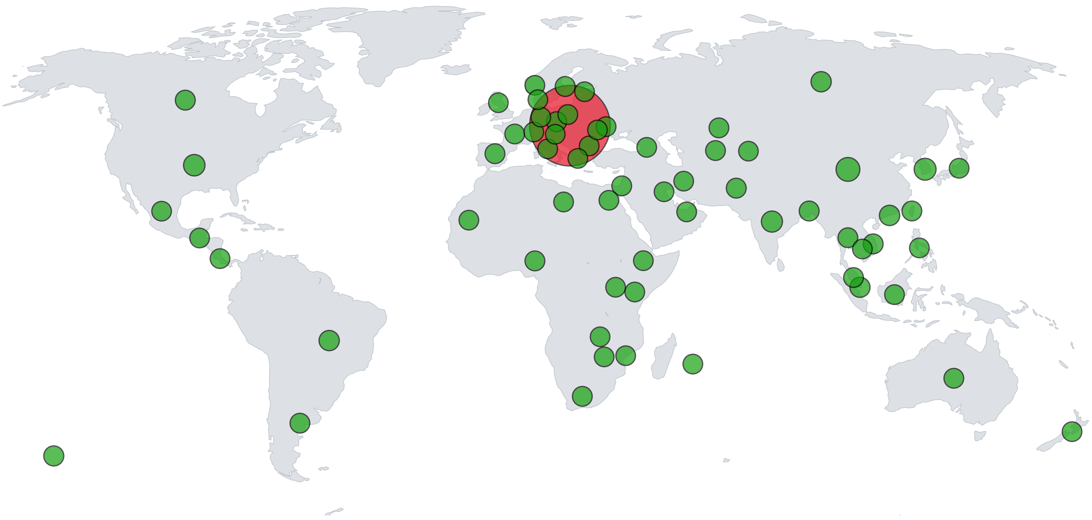
Page: 2.1 Detected Networks

License: Business Premium

2 Cloud Identity - 2.1 Detected Networks (2024-03-27)

Detected Networks

Locations Map



1/2

Slovakia	Other	China	South Korea	United States	India	Hong Kong
6.97K	316	233	123	97	81	39

Countries
64

Cities
325

Networks
531

In a hybrid work environment, where employees work from different locations and devices, it is important to monitor sign-in logs to ensure the security of your organization's data and resources. A high number of source networks in sign-in logs can indicate that users are signing in from multiple locations or devices, which can be a sign of a security risk or ongoing attack.

Time

Last 30 days

Page

2.2 Sign-ins

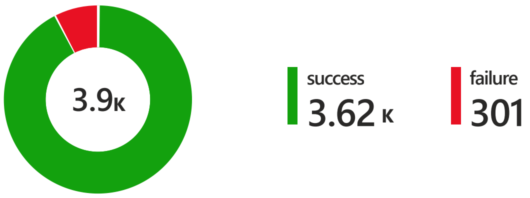
License

Business Premium

2 Cloud Identity - 2.2 Sign-ins (2024-03-27)

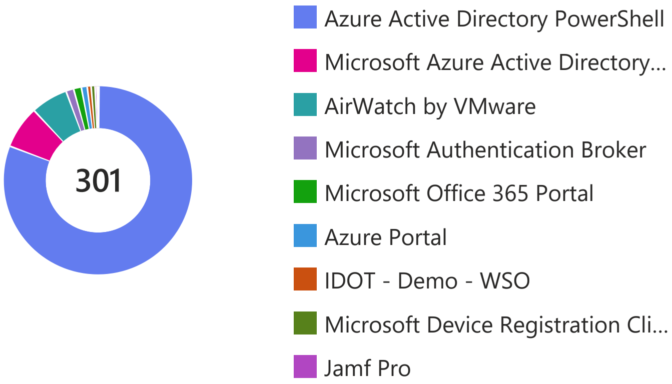
Sign-ins

Sign-in Attempts by Result Type



A high amount of sign-in failures can indicate a potential security risk for your organization. It could be a sign of a brute-force attack, where an attacker is trying to guess the password of a user account by trying many different combinations. It could also be a sign of a denial-of-service attack, where an attacker is trying to overwhelm your system with a large number of sign-in attempts.

Top 10 Apps with Authentication Failures



Risky Countries

Location ↑↓	SignIns↑↓	Success↑↓	Failure↑↓	FailureRate ↑↓
CZ	170	139	31	18.24%
IE	3507	3480	27	0.77%

Sign-ins from locations where unsuccessful and some successful attempts were detected.

Time
Last 30 days

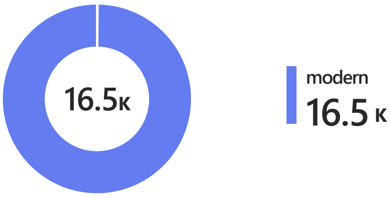
Page
2.3 Authentication

License
Business Premium

2 Cloud Identity - 2.3 Authentication (2024-03-27)

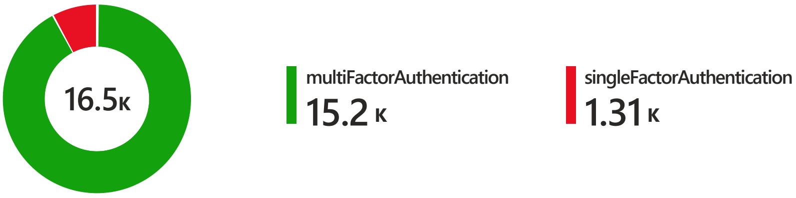
Authentication

Successful Sign-ins by Auth Type

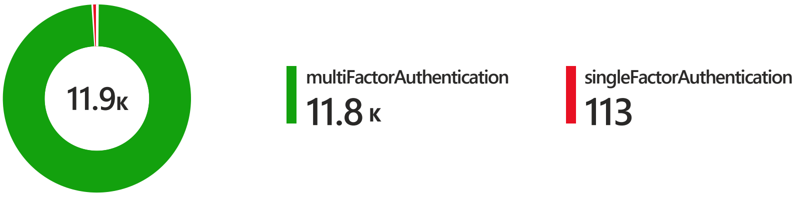


Legacy authentication protocols often do not support modern security features like multi-factor authentication (MFA), which can leave systems vulnerable to brute force attacks, credential stuffing, and other common attack vectors.

Successful Sign-ins by Factor Usage

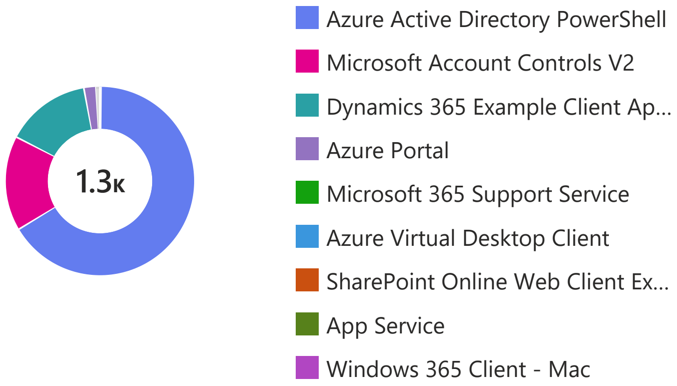


Successful Sign-ins by Factor Usage - Privileged Accounts



Low usage of multi-factor authentication (MFA) in sign-in logs can indicate a potential security risk for your organization. MFA adds an additional layer of security to the sign-in process by requiring users to provide two or more forms of verification to prove their identity. This makes it more difficult for attackers to gain access to your organization's data and resources using stolen or compromised credentials. If MFA is not widely used within your organization, it can increase the risk of unauthorized access and potentially lead to data breaches or other security incidents.

Top 10 Apps with Single Factor Authentication



Time: Last 30 days

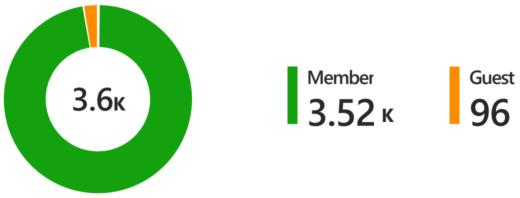
Page: 2.4 User Types

License: Business Premium

2 Cloud Identity - 2.4 User Types (2024-03-27)

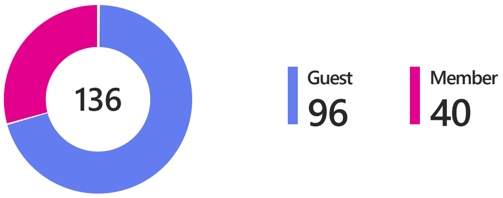
User Types

Successful Sign-ins by User Type



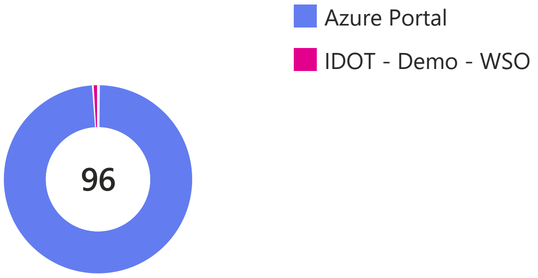
In Entra ID, there are two types of user accounts: members and guests. Members are typically users within your organization, while guests are external users who have been invited to access resources within your organization. The main difference between members and guest accounts is the level of access they have to your organization's resources. Members have broad access to resources within your organization, while guests have limited access to resources that have been specifically shared with them.

Single Factor Authentication by User Type



Whether a user is a member or a guest, not using multi-factor authentication (MFA) can increase the risk of unauthorized access to your organization's data and resources.

Top 10 Apps with Guest Access



Time: Last 30 days

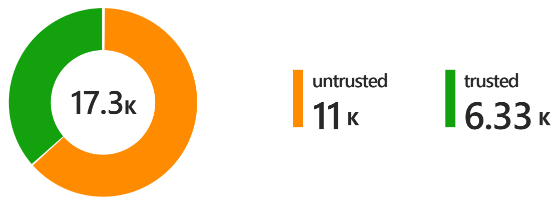
Page: 2.5 Network Trust

License: Business Premium

2 Cloud Identity - 2.5 Network Trust (2024-03-27)

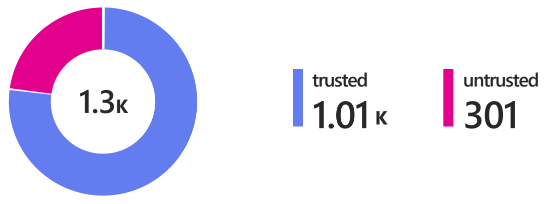
Network Trust

Successful Sign-ins by Network Trust



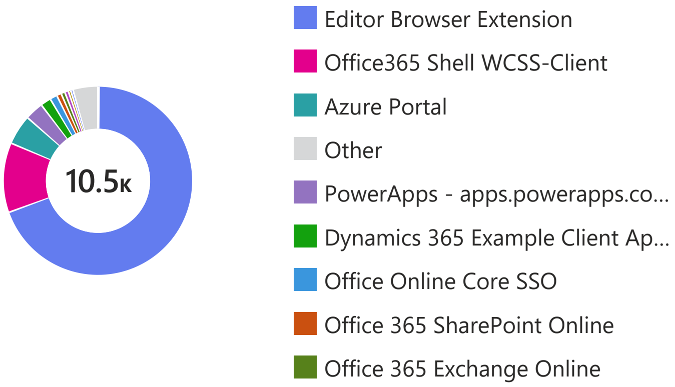
Trusted locations are ranges of IP addresses that an organization considers secure. Untrusted locations are locations that the organization does not consider secure, such as public Wi-Fi networks or locations outside the organization's control. Conditional access policies can be used to enforce different levels of security for access from trusted and untrusted locations. For example, the policy may require multi-factor authentication (MFA) for access from untrusted locations, but not for access from trusted locations.

Single Factor Authentication by Network Trust



If a user accesses resources from an untrusted location and multi-factor authentication (MFA) is not used, it can increase the risk of unauthorized access to your organization's data and resources. Without MFA, it can be easier for attackers to gain access to your organization's data using stolen or compromised credentials, potentially leading to data breaches or other security incidents. It is important to have Conditional Access policies in place, such as enforcing MFA for access from untrusted locations, to ensure the security of your organization's data and resources.

Top 10 Apps Accessed from Untrusted Locations



Time
Last 30 days

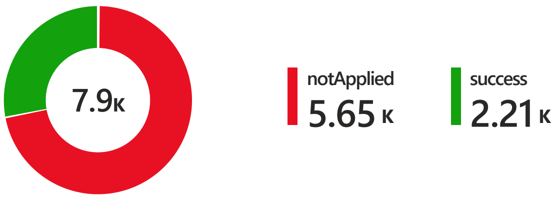
Page
2.6 Conditional Access

License
Business Premium

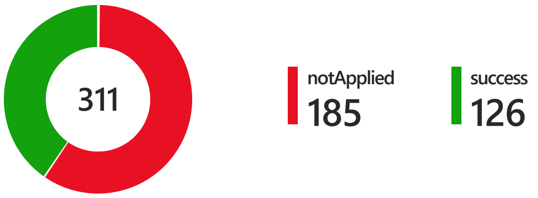
2 Cloud Identity - 2.6 Conditional Access (2024-03-27)

Conditional Access

Successful Sign-ins by Conditional Access Status

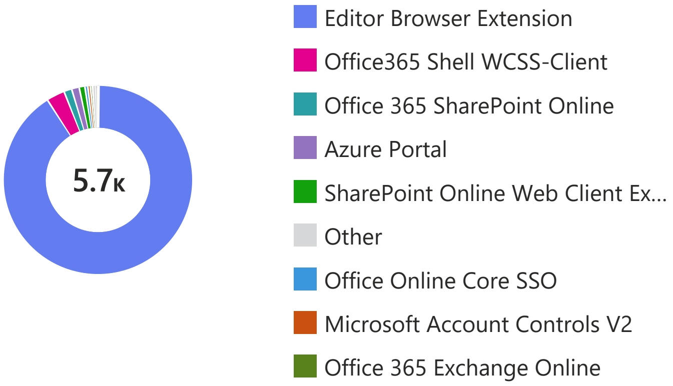


Successful Sign-ins by Conditional Access Status - Privileged Accounts



If a Conditional Access policy is not applied for access, it can increase the risk of unauthorized access to your organization's data and resources. Conditional Access policies help to ensure that only authorized users, devices, and apps are able to access your organization's data. Without these policies in place, it can be easier for attackers to gain access to your organization's data, potentially leading to data breaches or other security incidents. It is important to have Conditional Access policies in place and to regularly review and update them to ensure the security of your organization's data and resources.

Top 10 Apps Accessed Outside Conditional Access



Time
Last 30 days

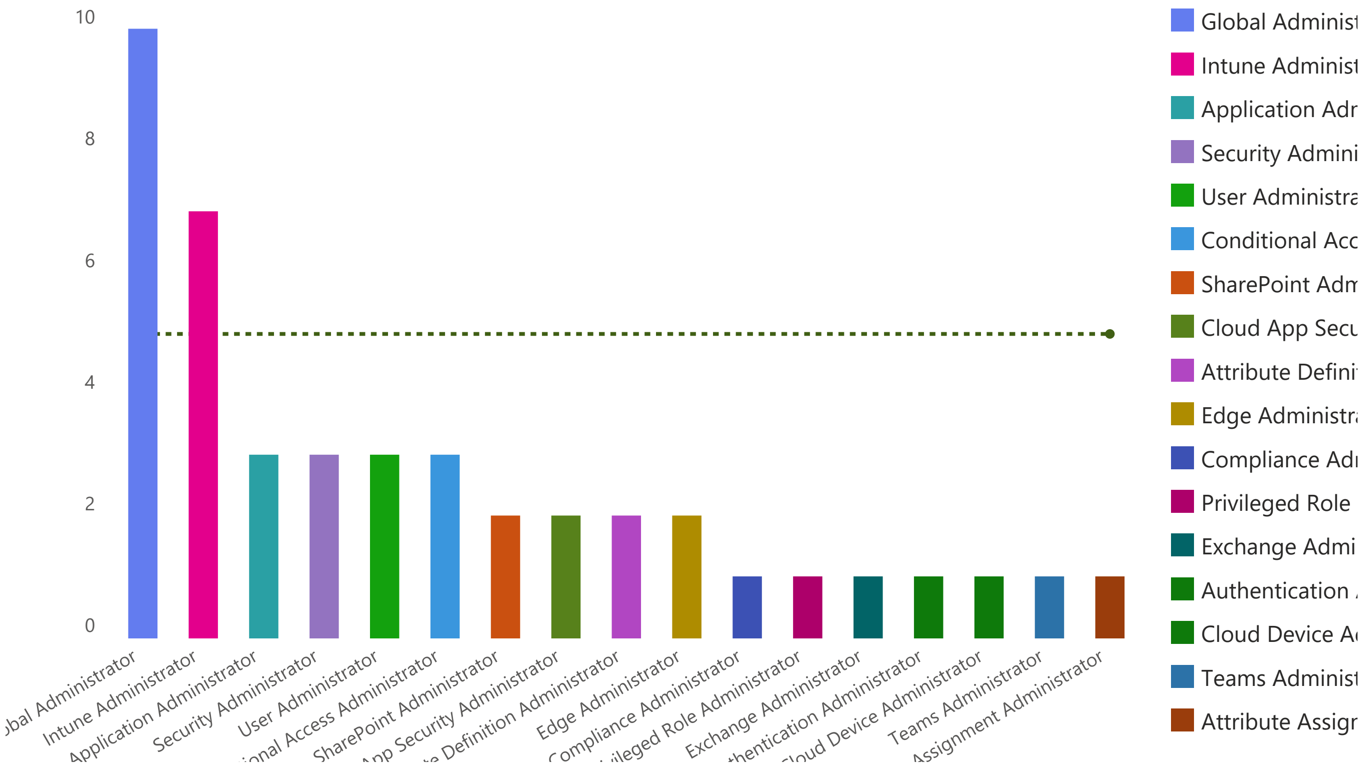
Page
2.7 Global Roles

License
Business Premium

2 Cloud Identity - 2.7 Global Roles (2024-03-27)

Global Roles

Global Admin Role Assignments by Role



It is important to have a sufficient number of global administrators to manage the organization's Microsoft 365 environment effectively, but it is also important to limit the number of global administrators to reduce the risk of security breaches.

Time

Last 30 days

Page

3.1 Device Access

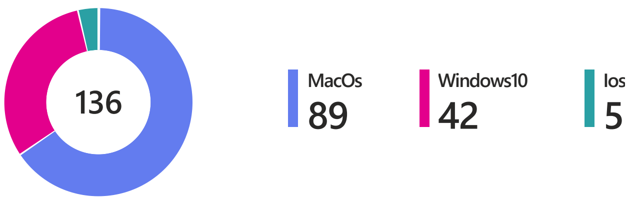
License

Business Premium

3 Endpoint - 3.1 Device Access (2024-03-27)

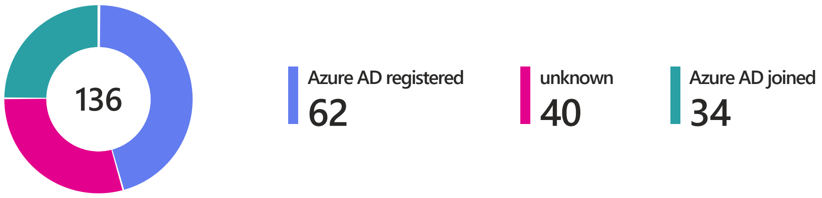
Device Access

Sign-ins by Device OS



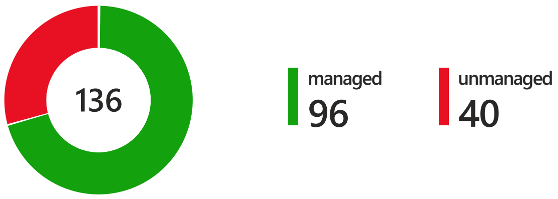
Device platforms detected in Sign-in logs refer to the operating systems of the devices that are used to sign in to Microsoft 365 or other services. This information can be useful for monitoring and analyzing sign-in activity, identifying trends, and detecting potential security issues. For example, if an organization primarily uses Windows devices, but the sign-in logs show a high number of sign-ins from Android devices, this could indicate a potential security issue that needs to be investigated.

Sign-ins by Device Trust Type

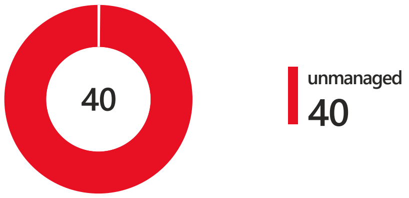


Azure AD registered, Azure AD joined, and Hybrid Azure AD joined are three different types of device registration in Entra ID (Azure AD). Each type of device registration provides different levels of access and management capabilities. It is important to choose the appropriate type of device registration based on the organization's needs and requirements. Unknown device type refers to a device that is not recognized by Azure AD

Sign-ins by Device Management Status

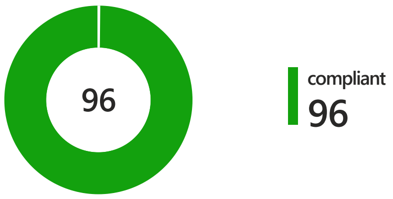


Sign-ins from Untrusted Networks by Device Management Status (w/o Guests)



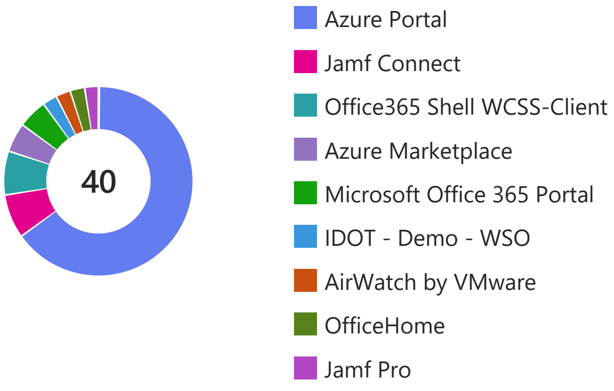
Managed devices are devices that are enrolled in a mobile device management (MDM) solution and are managed by an organization's IT department. This allows the IT department to configure, secure, and monitor the devices according to the organization's policies. On the other hand, unmanaged devices are devices that are not enrolled in an MDM solution and are not managed by the organization's IT department. These devices do not have the same level of security and control as managed devices and may not comply with the organization's security policies. Unmanaged devices can pose a security risk if they are used to access sensitive corporate data.

Sign-ins from Managed Devices by Device Compliance



Non-compliant devices are managed devices that do not meet the security and compliance policies set by an organization. These devices can pose a security threat to the organization's network and resources. For example, compromised devices such as jailbroken iOS or rooted Android devices can strip away integral security settings and may introduce malware into the network.

Top 10 Applications Accessed from Unmanaged Devices



Time
Last 30 days

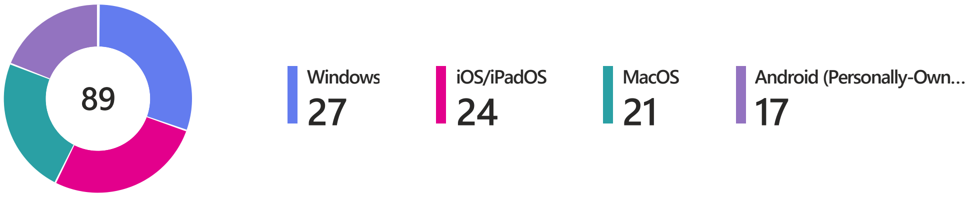
Page
3.2 Device Management

License
Business Premium

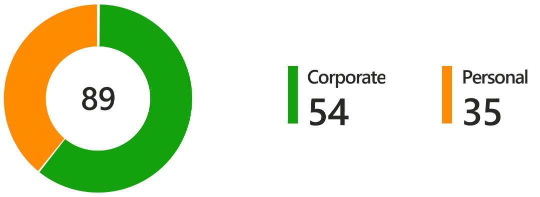
3 Endpoint - 3.2 Device Management (2024-03-27)

Microsoft Intune

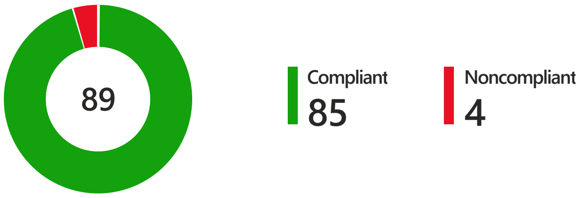
Devices by OS



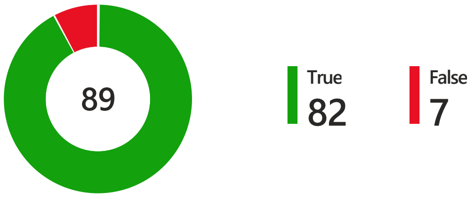
Devices by Ownership



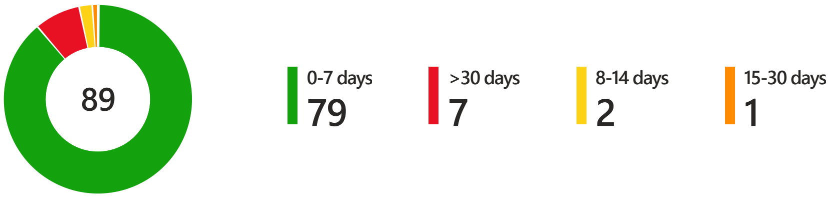
Devices by Compliance



Devices by Encryption Status



Devices by Last Contact



Time: Last 30 days

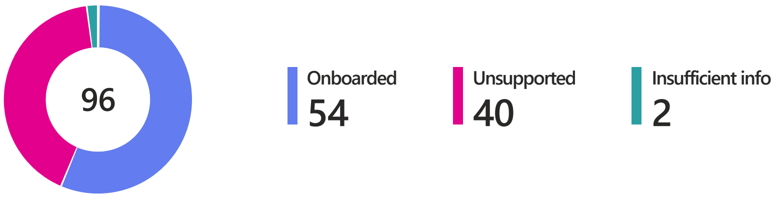
Page: 3.3 Device Protection

License: Business Premium

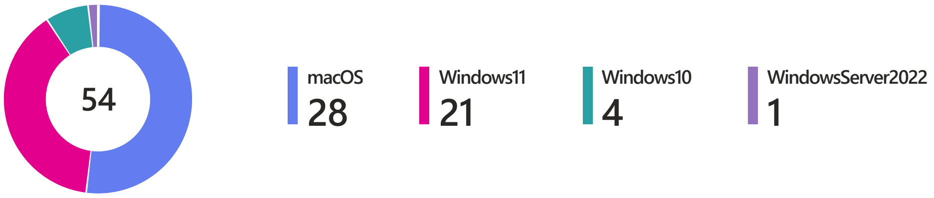
3 Endpoint - 3.3 Device Protection (2024-03-27)

Microsoft Defender for Endpoint

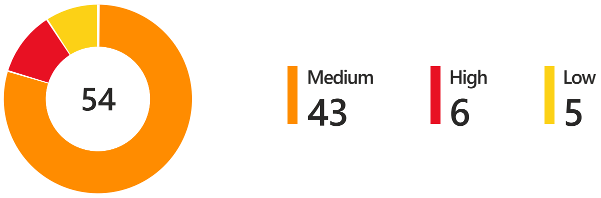
Detected Devices by Onboarding Status



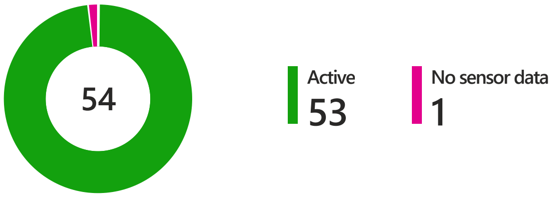
Onboarded Devices by OS



Onboarded Devices by Risk



Onboarded Devices by Sensor Health State


Active 53
No sensor data 1