Microsoft Dynamics 365

Power Platform Governance Blueprint Series Ep. 3

Securing the tenant

Use tenant-wide settings to secure the Power Platform in your tenant and protect data from top internal and external threats.

7 key steps

1. Limit email exfiltration with Exchange export rules
2. Change tenant setting to limit the ability to share apps with everyone
3. Limit gateway installers
4. Configure tenant isolation
5. Configure endpoint filtering
6. Configure connector action controls
7. Use tenant-wide analytics to monitor assets and users

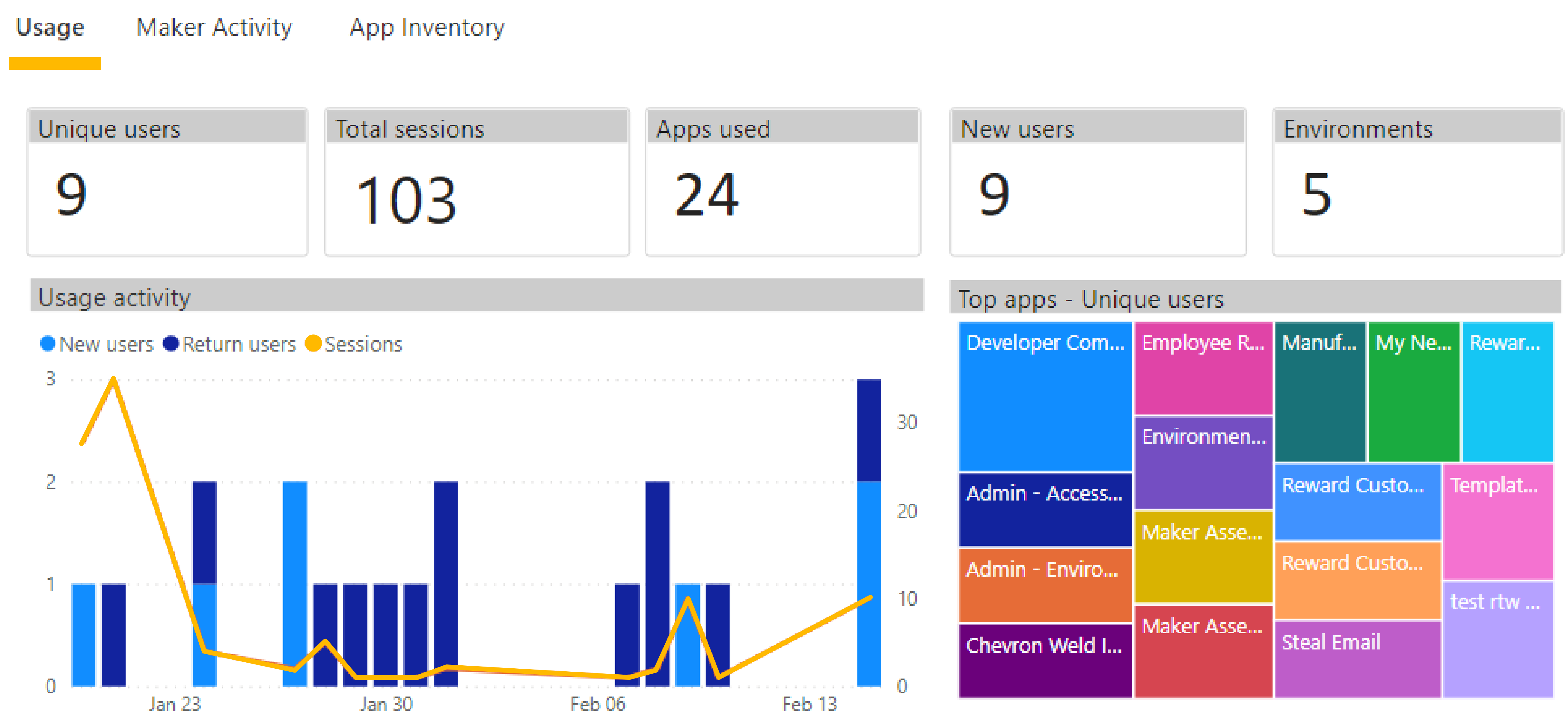
Understand key terms

On-premises data gateway:
the bridge providing quick and secure data transfer between on-premises data and Power BI, Microsoft Flow, Logic Apps and PowerApps.

Tenant isolation:
a way to block external threats from establishing connections into your tenant and your tenant from establishing external connections that put data at risk.

Connectors for sensitive data:
connectors in a particular group that can't share data with other groups.

Monitor analytics: usage, maker activity, app inventory



Usage | Maker Activity | App Inventory

Unique users: 9

Total sessions: 103

Apps used: 24

New users: 9

Environments: 5

Keep learning

Watch the entire Microsoft Teams Power Platform Governance Blueprint Series.