panagenda

OfficeExpert™

Digital Experience Monitoring Solution

Actionable insights for Teams call quality troubleshooting

Enterprise organizations are embracing Microsoft Teams as their communication and collaboration platform. Many are relying on Teams voice for all calls and meetings. This places a new burden on IT support groups to maintain an ***optimal digital experience for performance quality*** wherever users are working, from home, on the road, or at an office location.

OfficeExpert provides detailed performance data from all endpoint devices – Network, CPU, and Memory Usage. The information is gathered from localized agents running on computer endpoints, which provides the most accurate metrics to measure performance and identify digital experience issues. If you really want complete oversight to manage performance quality for your employees' digital experience, then OfficeExpert can help provide full visibility from a single pane-of-glass.

- **Quickly Troubleshoot Teams Call Quality Issues**
- **Spotlight ISPs with Performance Problems**
- **Identify Necessary Device Upgrades**
- **Monitor Unmanaged Networks for Remote Users**

Key Features

Real-Time Reporting Dashboards

All telemetry data for Teams calls and meetings are gathered as they happen and transmitted back to the central performance monitoring database which powers a *Digital Employee Experience dashboard.*

Proactive Digital Experience Monitoring for Remediation

Evaluate local network and device performance, plus ISP response times, to optimize employee hardware tuning and home office network optimization.

Empowers IT Support for Fast Troubleshooting

IT operations and technical support groups can quickly analyze call quality performance from actual user endpoints to perform root cause analysis and remediate issues.

Panagenda software solutions provide in-depth analytics and optimization of IT collaboration environments including Microsoft 365. With panagenda you benefit from a comprehensive set of consulting services and innovative software solutions that streamline IT operations for your collaboration platform. Our experienced solutions architects, consultants, and developers support customers in over 70 countries including 10 million user endpoints.

Security / Architecture

Permissions to Install Endpoint Agent
Common installations for the local agent application are performed from supported IT software deployment tools. The agent can be installed on any Windows or Mac Device by a standard user with no administrative rights. No special firewall or antivirus exceptions are necessary for the agent to transfer data.

User Credential Security
The local agent application does not save, transmit or utilize the user's Microsoft 365 credentials. The agent operates using a delegated permission model and never has access to the user's credential. In most enterprise scenarios the agent will silently authenticate when the user is logged in. If authentication is required, the user will authenticate directly with either Microsoft, your company's on-premises ADFS server, or your 3rd party identity provider.

File Storage on the Endpoint Device
The agent is not designed to store data locally under normal operation. However, it can store temporary files on a user's machine if connectivity to Microsoft Azure is limited. This temporary data does not contain display names, usernames, email addresses, passwords or any other sensitive information. Regardless of the anonymized nature of this data, it is encrypted at rest. All data gathered by the agent is encrypted from inception until successful transmission to the SaaS platform. This includes in-memory storage, during transmission, and while at rest.

Network Communications
By design, the local agent will operate in the same manner as a Microsoft 365 application and communicate with any of the IP ranges and hosts required by Microsoft. Microsoft publishes their up-to-date IP address list here.

In addition to the standard endpoints used with Microsoft applications and services, the local agent will also need to access the Microsoft Azure based service for OfficeExpert. This endpoint can vary based on the location of the organization's data:

Location	Host	Port
United States	us.epmapi.com	443
EMEA	eu.epmapi.com	443

Data Security in Transit
All communications with the OfficeExpert API maintain the following standards:

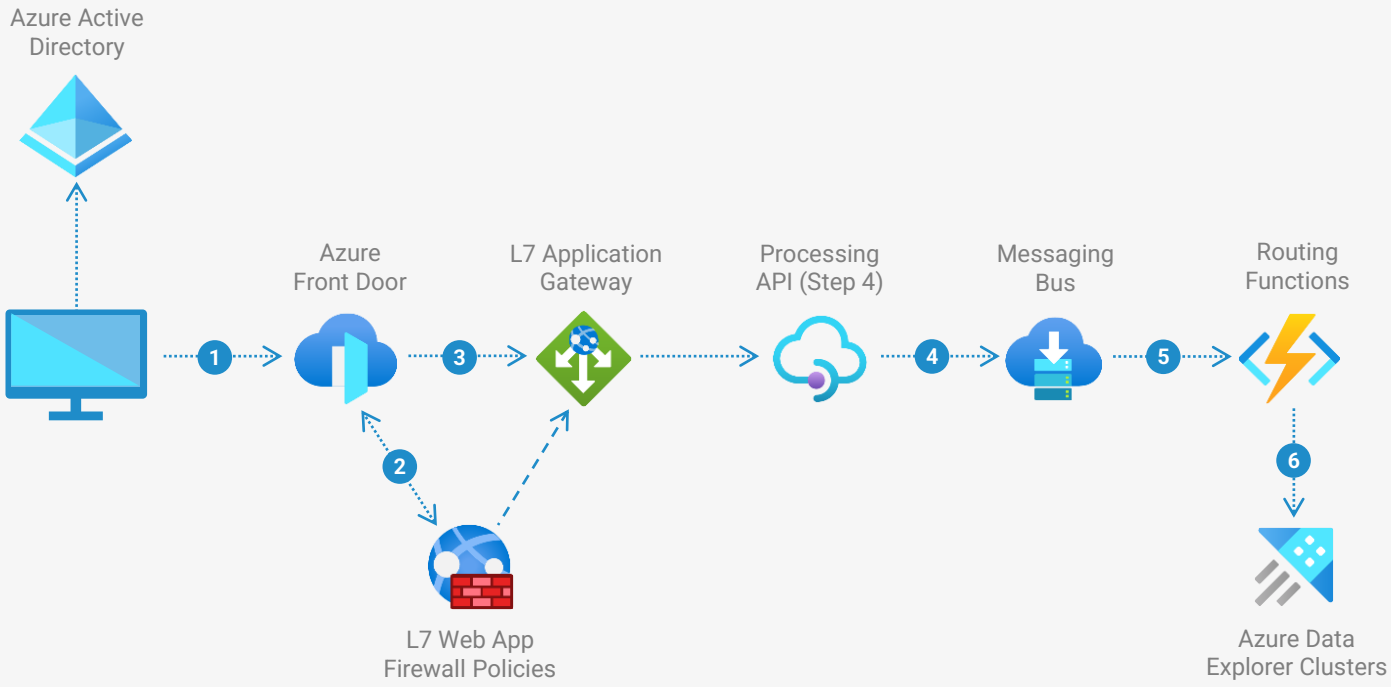
- Communications only take place over SSL/TLS secured connections.
- Communications require an authenticated connection from the agent on the client machine.
- Data transmission payloads for all communications is encrypted separately from, or in addition to, the SSL/TLS layer.

Data Privacy
Please read our Data Privacy document here: Data Privacy

Endpoint Data Gathering – How It Works

OfficeExpert™

Device-to-Azure SaaS Routing



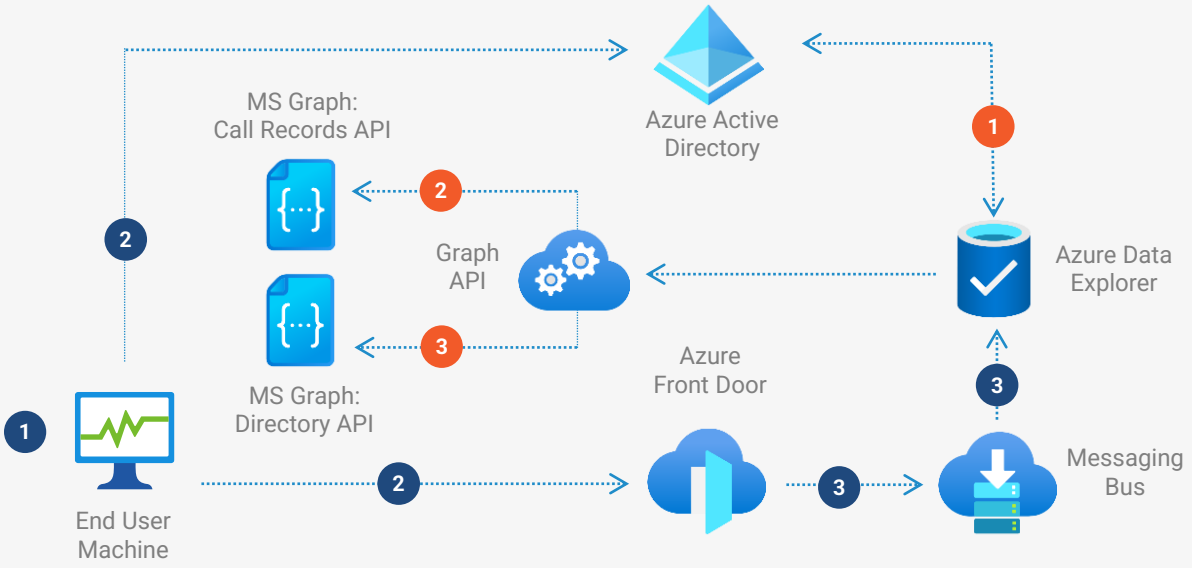
Process Steps

1. All communications from the client to the OfficeExpert EPM service are encrypted and authenticated.
2. When the agent first communicates with the MS Azure Front Door the requests are validated for the presence of a current, valid authentication token. The firewall policies active on the AFD also provide scanning against malware and checking against known BOT signatures. The payload remains encrypted at this step.
3. Traffic is passed to a layer 7 application gateway that decrypts the payload and validates the payload is free from malware, or injection attacks, and that it matches a known payload type.
4. Telemetry data is decoupled from any identifiable data and routed through a messaging bus for processing by a storage function. Although customer identifiable data is not part of a payload at this point, the messaging bus does maintain data at rest encryption.
5. Routing functions send the data to the dedicated database holding the customer's data.
6. Data in the cluster is stored in a dedicated database for each customer and data at rest is always encrypted.

Solution Architecture

OfficeExpert™

Data retrieval, transmission and storage diagram for processing steps



1. Using the registered Azure AD Application, a MS Graph Token is acquired from Azure AD using OAUTH2.
2. Using the MS Graph JWT Token, call quality data is retrieved from the Microsoft Graph Call Records API. Data is processed through multiple tiers and stored within the Azure Data Explorer using a separate database instance per customer.
3. Like point 2 above, Azure AD data is pulled from the MS Graph API and stored within the Azure Data Explorer customer database.

1. The client-side application creates data from Teams, Exchange, OneDrive, and SharePoint simulations, plus system and network information.
2. Azure issues an authentication token through the client application, and the client securely sends the data collection to Azure via the closest Azure Front door.
3. Client information is processed through multiple tiers and finally stored in Azure Data Explorer. Data from any given customer is stored in a separate database instance for security purposes.

MS Azure AD Application 1

The multi-tenant app is registered in the OfficeExpert EPM hosting tenant and is responsible for the windows agent. From the customer side, a one-time consent is required to the following delegated permissions:

- User.Read
- Mail.ReadBasic
- Teams.App.Read
- Chat.Read
- TeamsActivity.Read
- Presence.Read.All
- Sites.Read.All
- EWS.AccessAsUser.All
- Files.Read.All
- EAS.AccessAsUser.All
- ChannelMessagine.Read.All

MS Azure AD Application 2

Similar to App 1, an additional app is required to retrieve call quality data from the MS Graph API. Consent is required to the following permissions:

- User.Read (delegated)
- CallRecords.Read.All (application)
- User.Read.All (application)

MS Azure AD Application 3

A final app is used for the dashboard reporting access. No permissions are needed for this app.

info@panagenda.com | +1 617-855-5861

For more information about our unified data analytics solution for endpoint performance monitoring contact your sales representative or visit our website.
www.panagenda.com

panagenda