



Security Whitepaper

Measure Killer v2.9.5 · Brunner BI GmbH · Zug, Switzerland

This document outlines the security details and data handling practices of Measure Killer. It is intended for IT and security professionals conducting vendor reviews.

Summary of requirements

All outbound connections made by Measure Killer. Connections marked **Optional** can be ignored if they are blocked or fail.

Required connections

DOMAIN	PURPOSE	PORT	PROTOCOL
api.powerbi.com	All Power BI related API calls	443	HTTPS
api.fabric.microsoft.com	All Fabric related API calls	443	HTTPS
measurekillerlicense-hrbvcncabnddab7.switzerlandnorth-01.azurewebsites.net	License verification	443	HTTPS

Optional connections

DOMAIN	PURPOSE	PORT	PROTOCOL
*.servicebus.windows.net	License verification (legacy method)	443, 5671	TLS-encrypted AMQP
www.measurekiller.com	License verification — blacklisted licenses	443	HTTPS
raw.githubusercontent.com	Fallback — blacklisted licenses	443	HTTPS
postman-echo.com	License verification — current date/time	443	HTTPS
time.windows.com	1st fallback — date/time	UDP 123	NTP
pool.ntp.org	2nd fallback — date/time	UDP 123	NTP
microsoft.com	3rd fallback — date/time	443	HTTPS
cloudflare.com	4th fallback — date/time	443	HTTPS
ifconfig.me	License verification — public IP address	443	HTTPS
measurekiller.com/downloads	Version update check	443	HTTPS
brunner.bi	Start-up message	443	HTTPS

Data handling and privacy

Metadata-only interaction

Measure Killer only interacts with **metadata** from Power BI Desktop or the Power BI Service. At no point does Measure Killer read, store, or process actual data contained within Power BI reports or models.

Metadata includes: names of artifacts (reports, semantic models, workspaces, users), DAX and M expressions, names of measures/tables/columns/calculation groups/field parameters, uncompressed size of columns, and all definitions (report pages, visuals, visual titles, visual size).

Local processing

All processing and analysis of metadata is performed locally on the user's machine. There is no hosted database — everything is done on the user's machine and not transmitted anywhere besides XMLA or REST API calls with Microsoft directly.

XMLA endpoint connection

To retrieve metadata from semantic models in the Power BI Service, XMLA endpoints are used. Authentication happens via the user's Microsoft account (ADOMD client).

Online / offline modes

Offline modes (Single model and report, Shared model on local machine): Connect to the local Analysis Services instance. Only internet interaction is license verification at launch.

Online modes (Modes 3, 4, 5): Triggered with an active internet connection and valid license. External connections are REST API calls and XMLA connections to Microsoft only.

License verification

In v2.9.3 a new license verification method was introduced. Key facts:

Single endpoint: Hosted in Azure Switzerland North (`measurekillerlicense-...switzerlandnorth-01.azurewebsites.net`)

Method: POST request over HTTPS (port 443)

What's transmitted: local machine username, license key, installed Measure Killer version, public IP address (optional — reports "unknown" if blocked)

What's never transmitted: No Power BI metadata, report content, or user data

Encryption: All data sent exclusively over HTTPS/TLS

Legacy method: Azure Event Hubs (*.servicebus.windows.net) — can be used exclusively by disabling "Use new license verification API" in settings

Date and time verification

Measure Killer obtains the current UTC time from trusted sources for license validation, with a fallback chain:

Primary: postman-echo.com via HTTPS (443)

1st fallback: time.windows.com via NTP (UDP 123)

2nd fallback: pool.ntp.org via NTP (UDP 123)

3rd fallback: microsoft.com via HTTPS (443)

4th fallback: cloudflare.com via HTTPS (443)

If NTP access (UDP 123) is restricted, Measure Killer automatically falls back to HTTPS-based time sources.

Blacklist verification

Cryptographically signed blacklist data is verified from:

Primary: www.measurekiller.com over HTTPS (443)

Fallback: raw.githubusercontent.com over HTTPS (443)

Public IP lookup (optional)

ifconfig.me over HTTPS (443). If blocked, Measure Killer proceeds but reports the IP as "unknown".

API endpoints and security measures

All requests use **HTTPS** — data in transit is encrypted.

Access tokens are securely passed in request headers; responses are parsed as JSON for internal processing.

NTP servers are used for UTC time; if UDP 123 is restricted, Measure Killer falls back to HTTPS-based time sources.

Authentication uses **OAuth 2** via browser interaction. No passwords are handled by Measure Killer.

Once metadata has been acquired, all subsequent analyses are carried out **locally**.

REST API calls

All calls are made to Microsoft's Power BI Service and Fabric APIs in compliance with security protocols.

API	METHOD	ENDPOINT
Get Datasets In Group	GET	<code>api.powerbi.com/.../datasets</code>
Get Refresh History	GET	<code>api.powerbi.com/.../refreshes</code>
Execute Queries In Group	GET	<code>api.powerbi.com/.../executeQueries</code>
Get Reports In Group	GET	<code>api.powerbi.com/.../reports</code>
Get Datasources	GET	<code>api.powerbi.com/.../datasources</code>
Export Report In Group	GET	<code>api.powerbi.com/.../Export</code>
Get Group Users	GET	<code>api.powerbi.com/.../users</code>
Get Groups	GET	<code>api.powerbi.com/.../groups</code>
Get Capacities (Admin)	GET	<code>api.powerbi.com/.../admin/capacities</code>
Workspace Scan Status	GET	<code>api.powerbi.com/.../admin/workspaces/scanstatus</code>
Workspace Scan Result	GET	<code>api.powerbi.com/.../admin/workspaces/scanresult</code>
Post WorkspaceInfo	POST	<code>api.powerbi.com/.../admin/workspaces/getinfo</code>
Get Activity Events	POST	<code>api.powerbi.com/.../admin/activityevents</code>
Get Groups (Admin)	GET	<code>api.powerbi.com/.../admin/groups</code>
Add/Delete User (Admin)	POST/DEL	<code>api.powerbi.com/.../admin/groups/.../users</code>
Get User Artifact Access	GET	<code>api.powerbi.com/.../admin/users/.../artifactAccess</code>
Get Report Subscriptions	GET	<code>api.powerbi.com/.../admin/reports/.../subscriptions</code>
Get Item Definition	POST	<code>api.fabric.microsoft.com/.../getDefinition</code>
Get Operation State	GET	<code>api.fabric.microsoft.com/.../operations</code>
List Domains / Workspaces	GET	<code>api.fabric.microsoft.com/.../admin/domains</code>

Security testing approach

Software composition analysis: All open-source dependencies are checked for known vulnerabilities using pip-audit and OSS Index before each release.

Static code analysis: Automated analysis with Bandit (Python security analyzer) and PyLint (code quality). Each flagged item is reviewed for real vulnerabilities vs. false positives.

Automated testing: pytest for unit and integration tests — validation/parsing logic for .pbix and .rdl files, authentication flows, error handling, fail-safe behavior, and regression testing.

Rapid response: If a vulnerability is discovered, the team applies a prompt fix and releases an updated version. Bug-fix and patch versions are released on a monthly basis.

Known CVEs — Python 3.11.8

CVE	SEVERITY	ISSUE	MEASURE KILLER STATUS
CVE-2024-8088	High	zipfile.Path infinite loop	Low risk — only triggered if user uploads a malicious .xlsx file
CVE-2017-20052	Medium	DLL hijacking in pgAdmin4	Not applicable — applies to Python 2.7.13 and pgAdmin4
CVE-2024-7592	Low	http.cookies ReDoS	Not applicable — http.cookies module not used
CVE-2024-6232	Medium	tarfile ReDoS	Not applicable — TarFile not used
CVE-2015-5652	High	DLL hijacking on Windows	Mitigated — PyInstaller bundles python311.dll; .exe is code-signed; admin installer uses Program Files
CVE-2025-0938	Medium	urllib.parse accepts invalid hostnames	Mitigated — only hardcoded Power BI / Fabric API URLs are parsed
CVE-2024-6923	Medium	email header injection	Not applicable — email module not used
CVE-2024-3219	Medium	socket.socketpair() race condition	Not applicable — socket.socketpair() not used

Known CVEs — bundled libraries

LIBRARY	STATUS IN MEASURE KILLER
V8	Bundled with Qt WebEngine but no external web content or scripts are loaded. Only renders internal HTML charts.
LLVM	Pulled in by PyInstaller at build time only. Not used at runtime. No external code compilation.
libxml2 / Expat	Only parses .rdl files from Power BI Report Builder or the Export Report API — trusted, structured sources.
libvpx / libaom	Part of Qt multimedia. Measure Killer does not process or render video files.
Qt 6.7.2	UI framework. No unknown URLs or scripts loaded. WebEngine used only for internal charts.
Skia 118	Image rendering via Qt. Only predefined icons and local resources — no untrusted images.
SQLite3 3.42.0	Stores activity logs (report views, Excel activities). No external .sqlite files are opened.