

DATA SOVEREIGNTY & RESIDENCY

Your Data Stays on Your Server

Where the information your team puts into Neuron lives, what can ever leave the server, and the controls that keep your engagement data inside your own walls.

Your Engagement Data Never Leaves Your Server

Neuron is software you run on your own server. The information your team puts into it, the scoping detail, the host and service data, the findings, the uploaded evidence, the client names, and any text the AI helps you draft, is created, stored, and processed on that server and nowhere else. It is never transmitted to PenTest.WS LLC, and it is never sent to any cloud service or other third party. This is a property of how the product is built, not a clause written into a contract.

- **Your data stays put.** Engagement content lives only in the database on your server. PenTest.WS LLC receives no copy of it at any time.
- **No cloud dependency to operate.** Neuron runs entirely on your hardware. It does not call out to any service in order to function.
- **You hold the only key.** Sensitive data is encrypted at rest with a key that lives on your server and is never shared with PenTest.WS LLC.
- **Nothing goes out silently.** Every connection the software can make to the internet is switched off until an administrator deliberately enables it.
- **Air-gap supported and verifiable.** Neuron can run with the server fully isolated from the internet, and you can confirm that yourself with your own firewall.

Everything in One Place: Your Own Database

Every artifact your team produces in Neuron is stored in the database that runs on your server: findings and their full revision history, uploaded evidence and screenshots, generated reports, your branding and logos, shared working files, and captured credentials. None of it is placed in cloud storage operated by PenTest.WS LLC or by any third party. There is no external storage bucket, no vendor file store, and no off-server cache holding your information.

Sensitive values are encrypted at rest using strong, industry-standard encryption. The key that protects them is held on your server, under your control. PenTest.WS LLC never holds that key, which means PenTest.WS LLC could not read your data even if it somehow came into possession of a copy of your database.

Put plainly: if PenTest.WS LLC were ever compelled to produce everything it holds about your engagements, it would have nothing to produce. The data was never sent, and the means to decrypt it was never shared.

Drawing the Line Precisely

Precision matters more here than reassurance. Neuron does not claim that a server connected to the internet emits no network traffic at all. It makes a stronger and more useful claim: that none of the traffic the software can produce carries the contents of your engagements. The table below draws that line exactly.

NEVER LEAVES YOUR SERVER

THE ONLY CONNECTIONS NEURON CAN MAKE, AND WHAT THEY CARRY

- Findings, methodology, and report content
- Uploaded evidence, screenshots, and attachments
- Client and engagement identifying information
- Captured credentials and sensitive notes
- Every prompt sent to the AI, and every word it generates in reply

- **License activation.** Your license serial number and a hardware fingerprint, sent once when an administrator activates online. No engagement data.
- **Update check.** The current version and platform, so the server can learn whether a newer release exists. No engagement data.
- **Software and model downloads.** An inbound transfer that pulls a file onto your server. Nothing is uploaded.
- **Public security feeds.** A request for publicly available vulnerability and technique data. Nothing about your work is included.
- **Your own integrations.** Traffic to systems you operate (email, ticketing, single sign-on). PenTest.WS LLC is never in the path.

Not one of these connections carries the contents of your engagements. And in an air-gapped deployment, the first four do not happen at all.

§ 4 · EXPLICIT CONSENT

Nothing Reaches the Internet Without an Administrator's Permission

Neuron treats reaching the internet as an exception that an administrator must authorize, never a default the software assumes. Every capability that could make an outbound connection ships switched off. Enabling one, or running it once, requires a deliberate action by an administrator, and the software first presents a confirmation that names the exact destination it is about to contact and reminds the administrator to consider high-security and air-gapped environments before proceeding.

There is no hidden background traffic. The software does not check for updates, fetch data, or contact a licensing server on its own initiative. The following are taken directly from what an administrator sees in the product before any connection is made:

BEFORE A SOFTWARE UPDATE CHECK

"This will establish a connection to the update server over the internet to check for software updates. If you are in a high-security or air-gapped environment, ensure internet connectivity is authorized before proceeding."

BEFORE ONLINE LICENSE ACTIVATION

"This will connect to the Neuron licensing server to activate your license with the current hardware fingerprint. Your serial number and fingerprint will be sent securely."

BEFORE ENABLING PUBLIC SECURITY FEEDS

"This will cause the application to periodically connect to external vulnerability databases over the internet. Ensure this is suitable for your security environment."

Because each of these capabilities is off by default and individually gated behind its own confirmation, an administrator who simply never enables them operates a server that makes no outbound connections at all. Connectivity is a decision your team makes, item by item, with full visibility into where the traffic goes.

§ 5 · ON-PREMISES AI

The AI Runs on Your Hardware, Not in the Cloud

Neuron's optional AI features run entirely on your server. When an operator asks the AI to draft a finding, rewrite a passage, or generate an executive brief, the request is handled by a model running on your own hardware, and the result is returned locally. The prompt and the generated text never leave your server.

There is no third-party AI service behind Neuron. There are no credentials for a hosted AI provider anywhere in the product, and there is no fallback that would send a request to an outside service if the local model were busy or unavailable. The entire AI cycle is local by construction.

There is no external AI service to send your data to, because the product contains no way to reach one.

The governance of the AI feature, what it is used for, how its output is reviewed, and who is accountable for it, is described in the companion Responsible AI Policy.

§ 6 · AIR-GAP

A Fully Isolated Deployment You Can Verify Yourself

Neuron supports running on a server with no connection to the internet whatsoever. This is a fully supported way to deploy the product, not a workaround. In an air-gapped deployment, the license is activated through a one-time offline exchange rather than an online call, software and model updates are applied from files an administrator brings to the server, and the public reference feeds are simply left off. With outbound traffic blocked at your firewall, Neuron continues to operate at full capability, including its AI features.

You do not have to take our word for any of this. Place the server behind a firewall that denies outbound traffic, and watch the logs. Your engagement data has nowhere to go, and the product keeps working exactly as before.

§ 7 · YOUR INTEGRATIONS

Connections Go to Systems You Own

Neuron can connect to a small number of systems that you operate: your mail server for sending email, your ticketing system if you choose to push findings to it, and your identity provider for single sign-on. In every case the connection is to infrastructure you own and configure, using credentials you supply. PenTest.WS LLC is never an intermediary, and none of this traffic is visible to PenTest.WS LLC.

These integrations are configured by your administrators and can be left unconfigured entirely. When they are in use, they move your data only between systems that already sit inside your own environment.

Neuron Does Not Phone Home

Neuron collects no usage analytics, no telemetry, no crash reports, and no samples of your content. It does not measure how you use the product and report that back to PenTest.WS LLC. This is not a setting you have to locate and switch off. The capability to collect and transmit such data is simply not built into the product.

Licensing follows the same principle. Once activated, Neuron validates its license on the server itself, with no recurring call to a licensing server and no heartbeat. A connected server and an isolated server behave identically here: neither contacts PenTest.WS LLC to keep the software running.

Who Controls What

The matrix below separates the responsibilities that fall to PenTest.WS LLC as the software vendor from those that remain with your organisation as the operator of the server. ● indicates the primary owner of the activity; ○ indicates a contributing role. The pattern is consistent: PenTest.WS LLC builds and supplies the software, and your organisation controls the server, the data, and every decision about connectivity.

ACTIVITY	PENTEST.WS LLC	YOUR ORGANISATION
Building and delivering the Neuron software	●	
Supplying AI models through the update channel	●	
Operating the server and the network boundary around it		●
Holding the database where all engagement data is stored		●
Holding the key that encrypts data at rest		●
Deciding whether the server may reach the internet at all		●
Approving each individual online action (updates, activation, feeds)		●
Reviewing AI-drafted content before it reaches a client		●
Investigating and remediating security defects in the software	●	○

The Assurance Is Structural, Not Contractual

Your engagement data lives on your server, in your database, under your key. The software makes no outbound connection unless one of your administrators turns it on, and even then it carries only license and version information, never your work. You can isolate the server completely and confirm, with your own firewall and your own logs, that nothing leaves. And whether the server is connected or fully air-gapped, Neuron works the same way. Your data stays where you put it.