

BASTION REASONING ENVIRONMENT (BRE)

The local reasoning layer between users, AI models, and tools

The Bastion Reasoning Environment (BRE) was developed after observing teams struggle to use AI without stepping outside their organization's risk posture. On both sensitive and standard networks, the pattern was the same: AI tools wanted data sent to someone else's cloud, under someone else's controls, with someone else's promises.

BRE flips that model. It lets organizations apply AI to real workloads while they keep ownership of their data, their infrastructure, and their risk decisions. The principle is simple: AI runs inside your environment, with your tools and your identity systems, and remains accountable to you—not to a vendor's black box.

(540) 642-2798 

dkehr@dmggp.com 



Point of Contact: Mr. Daniel E. Kehr, President of DMG Group LLC

Bastion Reasoning Environment (BRE)



How BRE works

- **Deployed in your environment:** Runs on infrastructure you control (on-prem or private cloud). Data does not have to leave your network for BRE to work.
- **Policy first:** Every request runs through a policy engine that enforces your rules on secrets, regulated content, and tool access before anything is executed.
- **Tool-aware:** BRE connects to tools such as document search (RAG), HTTP-based data sources, and internal utilities under explicit policy, so AI can act but not improvise its own plumbing.
- **Fully logged:** Every action, decision, and tool call is logged with enough detail to reconstruct “who asked for what, which tools were used, and what came back.” That supports audits, investigations, and continuous improvement.

The standard toolset shipped with BRE focuses on the problems most organizations face first:

- Summarizing and querying internal documents without handing them to a third party.
- Safely calling approved external APIs and data sources under policy.
- Providing a single, consistent control point for how AI interacts with critical files, systems, and workflows.



Benefits to your Organization

- **Data sovereignty:** AI operates on your systems and stores results in your repositories. You decide what can leave the network.
- **Risk-aligned adoption:** Security and compliance teams get explicit controls and logs, instead of ad-hoc tools and shadow AI usage.
- **Vendor flexibility:** BRE is designed to work with your choice of models, RAG backends, and tools over time instead of locking you into a single provider.
- **Clear ownership:** BRE is built and owned under DMG Group LLC, so customers know exactly where the IP lives and who is accountable for roadmap, support, and security posture.



Extensibility and Ecosystem

BRE includes a clean API for third-party and internal developers to build new tools that plug into the same policy and logging framework. Any tool integrated into BRE must meet defined security and behavior standards before it is enabled in production.

That gives organizations two clear paths: they can start with the standard tools BRE ships with, and they can grow an ecosystem of BRE-compatible tools that respect the same security, audit, and control expectations from day one.

Scan the QR code for more information about DMG Group LLC.

