API Fortress Releases Open Source API Debugging Microgateway - Bloodhound

Capture, Transform, Track, and Debug Live API Conversations

New York, NY — June 9, 2020 — API Fortress, the leader in data-driven and functional API testing and monitoring, announces Bloodhound, a lightweight API debugging gateway that is free to download and open source. In less than 3 minutes, developers and engineers can begin using a powerful, purpose-built tool for API transaction debugging. Watch the Bloodhound Demo video.

Bloodhound allows teams to route API calls to any logger for comprehensive analysis to uncover solutions to difficult bugs, or test an API in ways not possible before. This gives QA teams the insights to ensure that microservices and database-connected APIs behave as they should in real-world conditions.

Patrick Poulin, co-founder and CEO at API Fortress remarks: "It's never been easier to build new APIs. But the mindset of how we test and monitor them hasn't evolved. Writing a handful of functional tests using a small subset of fake data against a staging environment is not enough. With Bloodhound, you can do more. In capturing and transforming your APIs, you can reproduce real world scenarios, and find clarity while trying to debug any problem."

Before the generally available release of Bloodhound, the gateway was deployed to several API Fortress customers that are among the world's largest retail, financial services, healthcare, and telecom companies. While the platform is flexible and creating addons is simple, several out-of-the-box use cases included:

- **Transforming Databases to APIs**: Create data-driven functional tests when test data is locked in a database (PostGres, MySQL, MS SQL Server, MongoDB, Redis, and more).
- **Testing APIs Beyond a Normal Functional Test**: Extend what can be tested by transforming the API into unique scenarios such as throttling, broken or unexpected headers, invalid payloads, and status code changes, etc.
- **Detecting Signals from Noise**: Understand the interdependencies in complex API call arrays to help teams create or improve documentation for new API projects.
- **Acting as an Echo Server**: Understand what requests look like from an API server's POV to capture issues not revealed during a send or receive.
- **Internal Policy Enforcement**: Add authorization layers to unsecured APIs - popular when exposing APIs to third parties or contractors.
- **Live Contract Validation**: Compare Swagger/OpenAPI specs to live API transactions to detect potentially dangerous anomalies.

For more information about Bloodhound from API Fortress, please visit APIFortress.com.