# cmd+Reporter

**cmdReporter** works like a security motion detector for anything running on, communicating with, or authenticating into a macOS computer.

cmdReporter then takes that data, formats it, & logs in JSON – so security tools like Splunk can easily collect it.

- **Why is cmdReporter different?**

  Our founder wrote the security guidance for macOS for the US government and has spent the last decade studying macOS security.

- **No kernel extension necessary**

  cmdReporter runs without kernel-level security or stability concerns. cmdReporter can be deployed as one version for all macOS computers in your environment.

- **Never calls home**

  No log data is ever sent to cmdSecurity or external servers. Your data stays with you.

- **Privacy with security**

  The default log level focuses on maintaining user privacy while still collecting all necessary security data. Higher collection levels can collect all computer and user activity.

- **JSON output**

  This will get the right data, to the right people, in the right format, faster. Nearly all security tools will natively ingest JSON without special data manipulation.

- **Light footprint**

  99% of your users will never notice cmdReporter running. Peak CPU usage of 8% and an average of 10mb of log data a day for macOS endpoints.

- **Government compliance**

  Log collection levels are mapped to NIST's published risk management framework (SP 800-37) and collect the recommended level of information.

- **Continuously streaming data**

  cmdReporter was designed to collect and process data from your endpoints in real-time, so security teams know immediately if there are ever any issues.