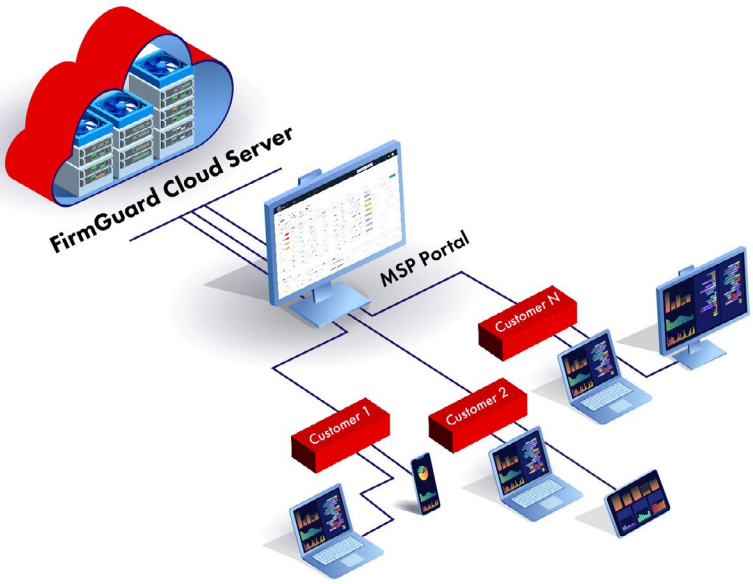
SOLUTION BRIEF

FirmGuard® SecureBeat

MONITOR ENDPOINT CONNECTIVITY

Introduction

SecureBeat is the mechanism by which the FirmGuard endpoint agent and the FirmGuard Cloud Server (hosted in AWS) communicate. A secure, encrypted tunnel is established and that is used to pass all relevant information back and forth to facilitate the various other FirmGuard features such as SecureCheck, SecureConfig, SecureWipe and SecureSense. The amount of data passed via SecureBeat will vary depending on the actions being performed. But as a general rule of thumb, we might expect 20MB or more per day which may grow in the future as more features are added to FirmGuard.



Examples of the types of data that are sent back and forth via SecureBeat are as follows and the interval over which this data is transmitted can be set and typically varies between 1 to 5 minutes.

- **Telemetry updates sent to the Cloud Server** - During the course of a day, there is a constant stream of data flowing up to the Cloud Server. This stream includes system metrics, heart beats, and more detailed information such as reports about the state of the BIOS. During any given hour, this is likely to be the bulk of the data transmitted/received from the Cloud Server.
- **Endpoint Commands** - When actions are initiated on the endpoint (e.g., updating BIOS settings, or wiping drives), information must be communicated down to the endpoint and then status must be communicated back up. This would typically be a minority of the data transmitted/received.
- **Endpoint Updates** - Currently, the FirmGuard installer is 46 MB, so during updates (or even during initial installs) this data is likely to be most of the traffic. This only applies to those specific use cases and is under the control of the administrator who is logged into FirmGuard.

phoenix technologies

rev. 06.17.24