**Monitoring**

Partnet is using Nagios® Core (<https://www.nagios.org/projects/nagioscore>) as our monitoring platform. The monitoring is broken up into 3 categories: server monitoring, process monitoring, and accessibility monitoring.

**Server Monitoring**

Host alive check

Disk Usage

Server Load

**Process Monitoring**

Nginx processes

Docker Process

**Accessibility Monitoring**

SSH access to the server

DNS resolution

**ERRATA Management**

Weekly errata script run with report mailed to server admins

Subscription to US-CERT mailing list

Subscription to RedHat and CentOS errata mailing lists

**Server Management**

Server configs managed via Puppet

Puppet process monitored by nagios

Daily LogWatch reports sent from server to admins

**Server Baseline**

A number of specific security measures are present in the environment:

1. A network security profile is configured limiting port access only to needed application and administrative ports. The nginx proxy server provides a translation between packets destined for reserved low ports (e.g. HTTP:80) and non-privileged high ports under which the application is configured to run.
2. A distinct application account is created to host the application distinct from any other accounts. Access to this account is restricted via SUDO.
3. All application processes are managed in user space. No basic application activity (e.g. deployment, starting/stopping processes) requires privileged root access.