# Middleware 11.23

# Features

- Whitelist Updates
  - Implemented the ability to create an exception with the parent program path and arguments
  - Implemented the ability to create an exception to match extortion responses when there are only trusted certs, match only when there are no related injections, and match only when there is no modified memory
  - Implemented the ability to create an exception to match specific file access triggers
- Implemented group setting for automatically freeing licenses for inactive agents
  - Updated Group model to have setting for when to free licenses from inactive agents in the group. Options are 30/60/90 days, or have this setting turned off
  - Updated Agent model to have new inactive status
  - Implemented service to automatically free inactive agents' licenses according to their group setting
- Updated the endpoint for the retrieving extortion responses to include the parent program path and arguments
  - The parent program path and arguments are now also included in the unique extortion response counts for the Web Application, Security Notification alerts, and Executive Summaries
- Updated our Executive Summary Reports to separate out the Licenses slide to individual Desktop and Server Licenses slides
- Updated Security Email Notification model and the Security Notification service to include two new alert types
  - Behavioral Model Tuned
  - New Agent Version
    - When a group’s managed update settings are changed to have auto update turned off, a New Agent Version notification is automatically created for the group
- User Role/Permission Updates
  - Updated the Role model Incident Manager permissions to now only have view/edit for whitelists and silent response rules
  - Groups now have 3 default roles that are not user editable:
    - Admin
    - Read Only
    - Guest
  - Users added to a group by default are assigned the Guest Role
- Implemented endpoints for the Web Application Browser Utility Process Tuning Modal to easily manage how agents in groups should respond to chrome utility processes

- Updated the endpoint for the Agents page chart to be able to limit counts to agents that have called in over the past 30/60/90 days
- Updated the Security Notification Ransomware Activity email alert to include a link that will automatically redirect users to the Extortion Responses page with the a filter to show the responses the alert was for
- Implemented group setting for agents in a group to run in safe mode or not
- Implemented a powershell script option for installing agents
- Upgrading our Spring Boot to the latest version
- Various updates to our list of default data + identity + cert whitelists for AVs

---

Revision #1
Created 2026-07-13 18:49:51 UTC by Dennis Underwood
Updated 2026-07-13 18:49:51 UTC by Dennis Underwood