INFOWATCH ARMA INDUSTRIAL ENDPOINT 3.0

what's new

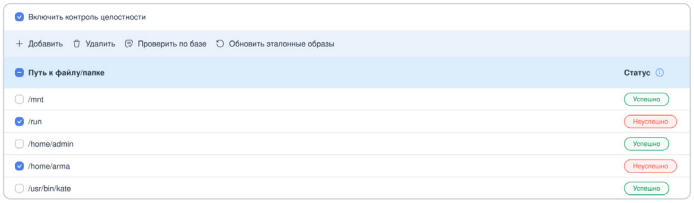
Версия 3.0 совместима с Astra Linux SE версий 1.7 и 1.8, что позволяет использовать продукт в отечественной инфраструктуре. Для защиты данных доступны возможности контроля целостности файлов и папок, запуска приложений и подключения устройств. Отправка событий в сторонние системы и настройка логирования стали более гибкими. Управлять продуктом теперь можно с помощью Management Console. Активация лицензии доступна как онлайн, так и в офлайн-режиме.

Новые возможности

Поддержка отечественных дистрибутивов Linux

InfoWatch ARMA Industrial Endpoint теперь совместим с Astra Linux SE версий 1.7 и 1.8, что позволяет использовать его в инфраструктуре клиентов с отечественными операционными системами.

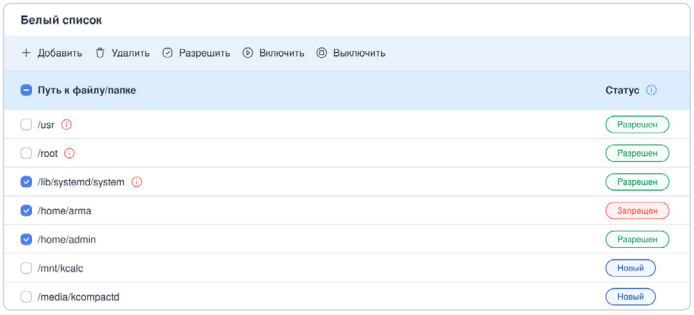
Контроль целостности файлов и папок



Появилась возможность отслеживать изменения в файлах и папках, указанных в настройках, в реальном времени. Это помогает оперативно выявлять несанкционированные изменения данных. Сравниваются текущее состояние объектов и эталонный образ, зафиксированный ранее.

Эталонный образ создаётся при постановке объекта на контроль и может обновляться вручную. Администратор может в любой момент запустить проверку контролируемых объектов. Для удобства доступны поиск, сортировка и отслеживание статуса объектов.

Контроль запуска приложений



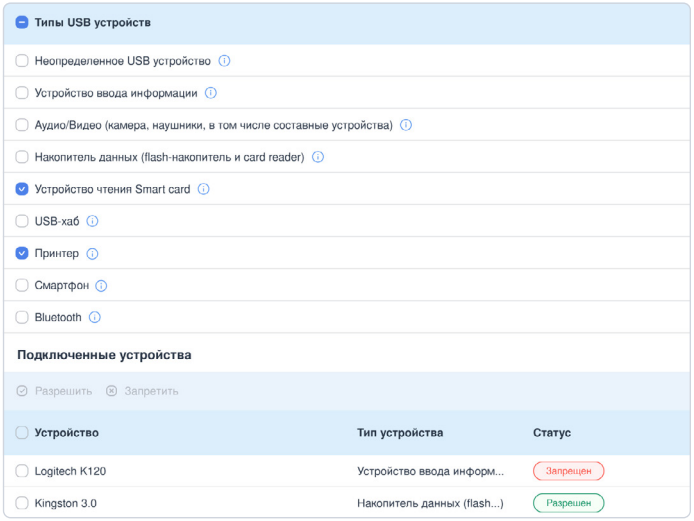
Стало возможно управлять запуском приложений на рабочих станциях, ограничивая доступ к ненужным или потенциально опасным программам. Это снижает риски заражения устройств и утечки данных.

Настройка выполняется через белый список, куда можно добавить отдельные файлы или директории, разрешённые к запуску. Все остальные приложения запускаться не будут.

Для удобства есть режим обучения — он автоматически собирает данные о запущенных процессах за заданный период и формирует предварительный список разрешённых приложений.

В окне контроля приложений теперь можно выбрать путь или файл и сразу включить для него контроль целостности. Если целостность пути из белого списка нарушена, запуск файлов из него блокируется
Для удобства доступны поиск, сортировка и отслеживание статуса контролируемых приложений.

Контроль подключённых устройств

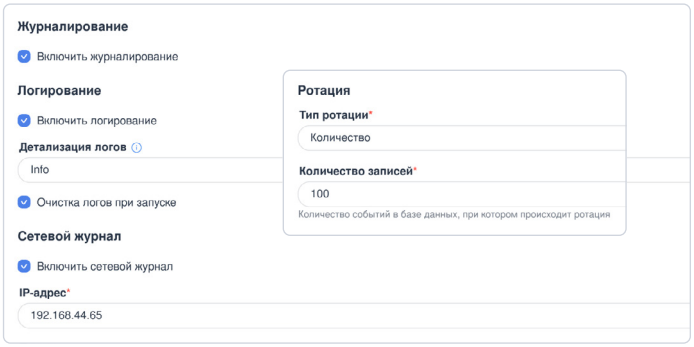


Появилась возможность управлять доступом к USB-устройствам (устройства ввода, накопители, камеры, микрофоны и т. д.) и CD / DVD, подключённым к рабочим станциям. Это позволяет предотвратить заражение, утечку или потерю данных.

Гибкие настройки позволяют разрешать или запрещать устройства по типу, параметрам VID / PID или выбрать конкретное устройство из списка подключённых.

В интерфейсе отображаются подключённые когда-либо устройства с информацией о названии, типе, серийном номере и параметрах VID / PID. Для удобства доступны поиск, сортировка, отслеживание статуса и состояния устройств.

Отправка событий в другие системы, ротация и логирование



InfoWatch ARMA Management Console — единый центр управления средствами защиты InfoWatch ARMA и инцидентами ИБ. Позволяет своевременно обнаружить и заблокировать угрозы, настроить автоматическое реагирование на инциденты.

В новой версии InfoWatch ARMA Industrial Endpoint появилась возможность отправлять данные в InfoWatch ARMA Management Console и сторонние SIEM-системы. Это позволяет оперативно выявлять угрозы и принимать обоснованные решения.

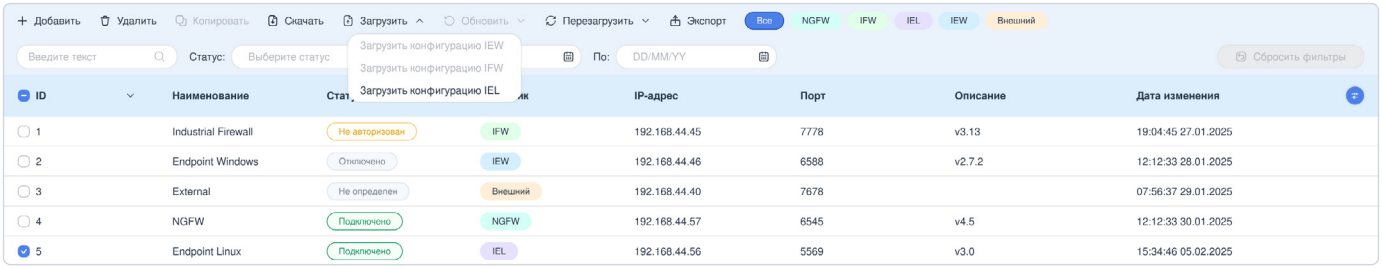
События модулей контроля целостности, приложений, устройств и изменения файлов конфигураций теперь записываются в базу данных. Журналирование можно включить или отключить в настройках. Все события InfoWatch ARMA Industrial Endpoint автоматически передаются в InfoWatch ARMA Management Console. Доступна возможность отправлять события в сторонние системы в формате CEF.

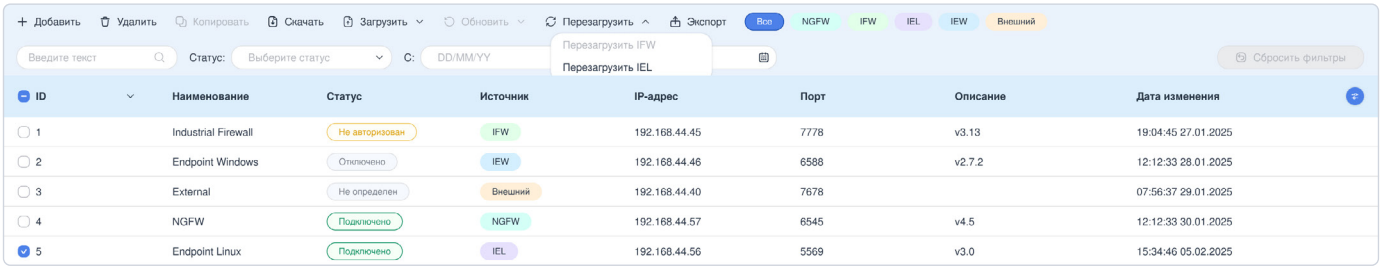
Появилась ротация событий по количеству записей и времени для предотвращения перегрузки базы данных. Ротированные записи сохраняются в отдельный файл. Ротации подвергаются только события, отправленные в InfoWatch Management Console, что исключает потерю данных.

Стала доступна настройка уровня детализации логирования с возможностью очистки лога при запуске.

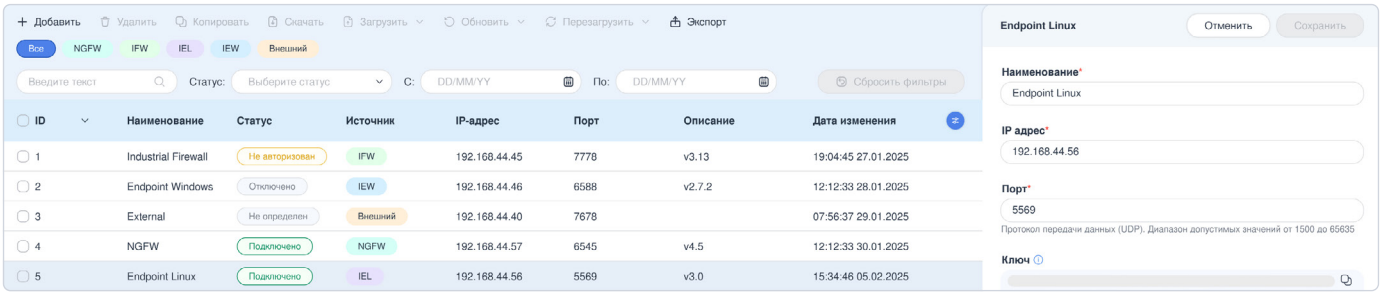
Управление из интерфейса InfoWatch ARMA Management Console

Появилось централизованное управление и настройка сразу нескольких защищённых станций через InfoWatch ARMA Management Console. Теперь можно загружать и скачивать конфигурационные файлы InfoWatch ARMA Industrial Endpoint для одной или нескольких рабочих станций одновременно. Стал доступен удалённый перезапуск InfoWatch ARMA Industrial Endpoint без необходимости прямого доступа к рабочим станциям.





Лицензирование



Теперь управление лицензиями стало проще и доступнее. Появилась возможность активировать лицензию InfoWatch ARMA Industrial Endpoint в онлайн- или офлайн-режиме через CLI. информацию о лицензии и версии ПО теперь можно просматривать в интерфейсе Management Console.