

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

Включить контроль целостности	
+ Добавить Удалить Проверить по базе Обновить эталонные образы	
Путь к файлу/папке	Статус
<input type="checkbox"/> /mnt	Успешно
<input checked="" type="checkbox"/> /run	Неуспешно
<input type="checkbox"/> /home/admin	Успешно
<input checked="" type="checkbox"/> /home/arma	Неуспешно
<input type="checkbox"/> /usr/bin/kate	Успешно

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

Белый список	
+ Добавить Удалить Разрешить Включить Выключить	
Путь к файлу/папке	Статус
<input type="checkbox"/> /usr	Разрешен
<input type="checkbox"/> /root	Разрешен
<input checked="" type="checkbox"/> /lib/systemd/system	Разрешен
<input checked="" type="checkbox"/> /home/arma	Запрещен
<input checked="" type="checkbox"/> /home/admin	Разрешен
<input type="checkbox"/> /mnt/kcalc	Новый
<input type="checkbox"/> /media/kcompactd	Новый

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

Типы USB устройств

☐ Неопределённое USB устройство

☐ Устройство ввода информации

☐ Аудио/Видео (камера, наушники, в том числе составные устройства)

☐ Накопитель данных (flash-накопитель и card reader)

☒ Устройство чтения Smart card

☐ USB-хаб

☒ Принтер

☐ Смартфон

☐ Bluetooth

Подключённые устройства

☒ Разрешить

☒ Запретить

Устройство	Тип устройства	Статус
Logitech K120	Устройство ввода информ...	Запрещен
Kingston 3.0	Накопитель данных (flash...)	Разрешен

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

Журналирование

☒ Включить журналирование

Логирование

☒ Включить логирование

Детализация логов

Info

Очистка логов при запуске

Сетевой журнал

☒ Включить сетевой журнал

IP-адрес

192.168.44.65

Ротация

Тип ротации

Количество

Количество записей

100

Количество событий в базе данных, при котором происходит ротация

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.

+

Добавить

Удалить

Копировать

Скачать

Загрузить

Обновить

Перезагрузить

Экспорт

Введите текст

Q

Статус:

Выберите статус

По:

DD/MM/YY

Сбросить фильтры

Загрузить конфигурацию IEL

Загрузить конфигурацию IFW

ID	Наименование	Статус	Источник	IP-адрес	Порт	Описание	Дата изменения
<input type="checkbox"/>	Industrial Firewall	Не авторизован	IFW	192.168.44.45	7778	v3.13	19:04:45 27.01.2025
<input type="checkbox"/>	Endpoint Windows	Отключено	IEW	192.168.44.46	6588	v2.7.2	12:12:33 28.01.2025
<input type="checkbox"/>	External	Не определен	Внешний	192.168.44.40	7678		07:56:37 29.01.2025
<input type="checkbox"/>	NGFW	Подключено	NGFW	192.168.44.57	6545	v4.5	12:12:33 30.01.2025
<input checked="" type="checkbox"/>	Endpoint Linux	Подключено	IEL	192.168.44.56	5569	v3.0	15:34:46 05.02.2025

+

Добавить

Удалить

Копировать

Скачать

Загрузить

Обновить

Перезагрузить

Экспорт

Введите текст

Q

Статус:

Выберите статус

С:

DD/MM/YY

По:

DD/MM/YY

Сбросить фильтры

Перезагрузить IFW

Перезагрузить IEL

ID	Наименование	Статус	Источник	IP-адрес	Порт	Описание	Дата изменения
<input type="checkbox"/>	Industrial Firewall	Не авторизован	IFW	192.168.44.45	7778	v3.13	19:04:45 27.01.2025
<input type="checkbox"/>	Endpoint Windows	Отключено	IEW	192.168.44.46	6588	v2.7.2	12:12:33 28.01.2025
<input type="checkbox"/>	External	Не определен	Внешний	192.168.44.40	7678		07:56:37 29.01.2025
<input type="checkbox"/>	NGFW	Подключено	NGFW	192.168.44.57	6545	v4.5	12:12:33 30.01.2025
<input checked="" type="checkbox"/>	Endpoint Linux	Подключено	IEL	192.168.44.56	5569	v3.0	15:34:46 05.02.2025

Лицензирование

+

Добавить

Удалить

Копировать

Скачать

Загрузить

Обновить

Перезагрузить

Экспорт

Введите текст

Q

Статус:

Выберите статус

С:

DD/MM/YY

По:

DD/MM/YY

Сбросить фильтры

ID	Наименование	Статус	Источник	IP-адрес	Порт	Описание	Дата изменения
<input type="checkbox"/>	Industrial Firewall	Не авторизован	IFW	192.168.44.45	7778	v3.13	19:04:45 27.01.2025
<input type="checkbox"/>	Endpoint Windows	Отключено	IEW	192.168.44.46	6588	v2.7.2	12:12:33 28.01.2025
<input type="checkbox"/>	External	Не определен	Внешний	192.168.44.40	7678		07:56:37 29.01.2025
<input type="checkbox"/>	NGFW	Подключено	NGFW	192.168.44.57	6545	v4.5	12:12:33 30.01.2025
<input checked="" type="checkbox"/>	Endpoint Linux	Подключено	IEL	192.168.44.56	5569	v3.0	15:34:46 05.02.2025

Endpoint Linux

Отменить

Сохранить

Наименование*

Endpoint Linux

IP адрес*

192.168.44.56

Порт*

5569

Протокол передачи данных (UDP). Диапазон допустимых значений от 1500 до 65535

Ключ

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.