ЛИНЕЙКА ПРОДУКТОВ
INFOWATCH ARMA

для защиты сетевой инфраструктуры

InfoWatch в цифрах и фактах

22
года на рынке информационной безопасности

20+
программных технологий и патентов

500+
сотрудников в компании

30%
ежегодный рост инвестиций в разработку

4000
проектов из 12 отраслей

135+
аналитических отчётов в год

100+
технологических партнёров

5000+
обученных специалистов ИБ

Рекомендовано АРПП «Отечественный софт»

Аккредитация ЦБ РФ

Легенды Инфобеза — 2025
Премия CIPR Digital

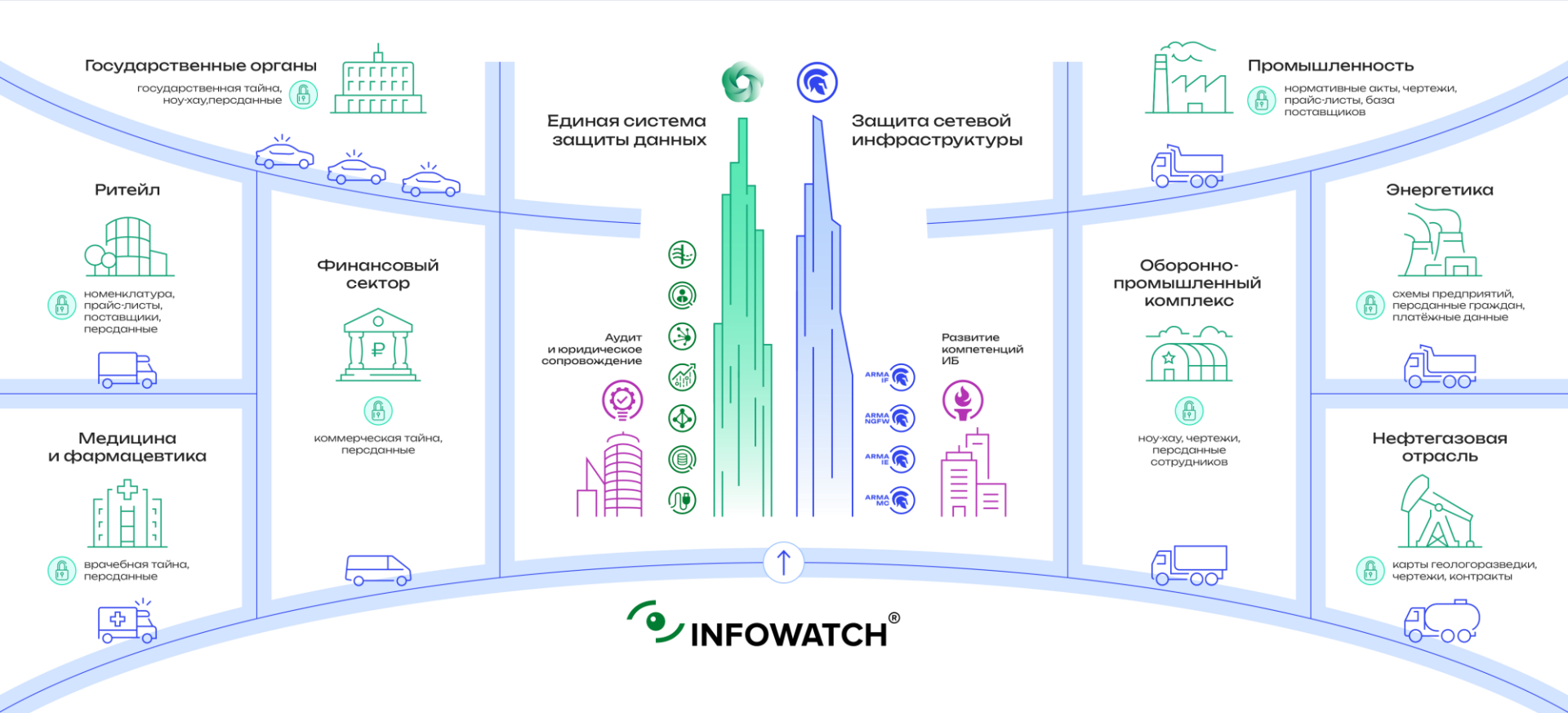
Национальная банковская премия
2023 и 2024

Инновация года в ИБ, 2022
CNews FORUM Кейсы

Лучшее ИБ-решение, 2021
TAdviser

DLP Market Guide
первое российское DLP-решение, вошедшее в Gartner Magic Quadrant и удерживающее признание более 10 лет

Карта решений InfoWatch



Решения InfoWatch

защита данных

InfoWatch Центр расследований

все продукты InfoWatch для защиты данных в едином окне — расследования проходят в 3 раза быстрее

- InfoWatch Traffic Monitor / мониторинг трафика
- InfoWatch Activity Monitor / мониторинг действий за ПК
- InfoWatch Vision / интерактивная визуальная аналитика
- InfoWatch Prediction / поведенческая аналитика
- InfoWatch Data Discovery / аудит хранения файлов
- InfoWatch Data Access Tracker / контроль изменений прав доступа
- InfoWatch Device Control / контроль устройств

кибербезопасность АСУ ТП

InfoWatch ARMA Industrial Firewall

защита АСУ ТП на сетевом уровне и соответствие требованиям ФСТЭК России

InfoWatch ARMA Industrial Endpoint

средство защиты информации рабочих станций и серверов SCADA

InfoWatch ARMA Management Console

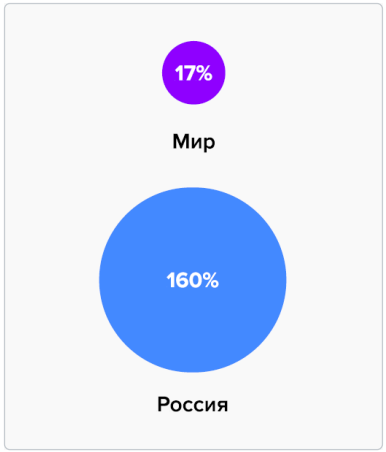
единый центр управления системой защиты InfoWatch ARMA и инцидентами ИБ

сетевая безопасность

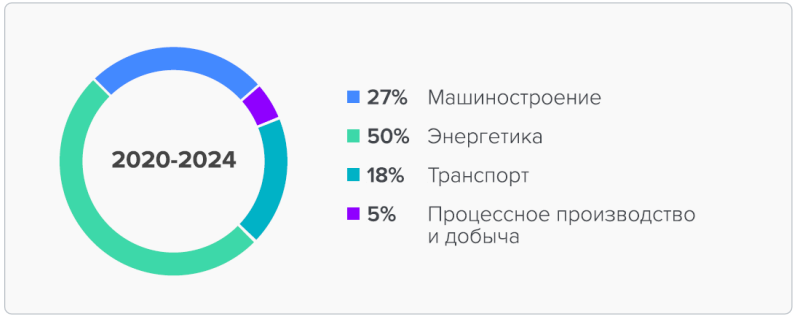
InfoWatch ARMA Стена (NGFW)

межсетевой экран нового поколения для корпоративных сетей

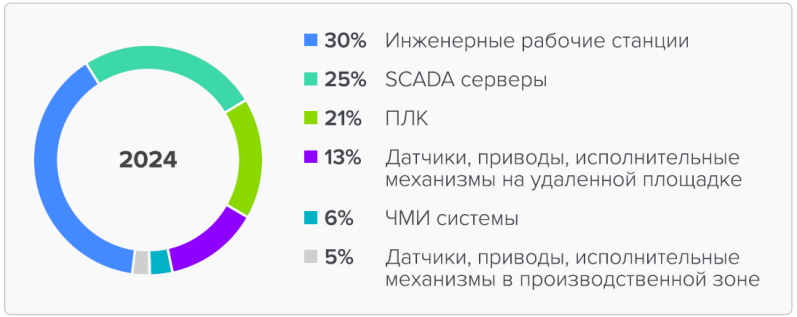
Почему защита сети — это важно?



рост числа инцидентов ICS / OT, 2022–2024



распределение атак APT-группировок по отраслям



наиболее часто атакуемые устройства АСУ ТП

Источник — ЭАЦ InfoWatch, отчёт «Тенденции развития киберинцидентов АСУ ТП»

Почему защита сети — это важно?

Приказ ФСТЭК России № 31

ИБ АСУ ТП вне КИИ, или незначимые объекты КИИ

Приказ ФСБ о ГосСОПКА № 368

о необходимости взаимодействия с ГосСОПКА

Приказ ФСБ о ГосСОПКА № 282

о деталях взаимодействия с ГосСОПКА

Приказ ФСТЭК России № 239

технические меры и сопутствующие процессы для критичных объектов КИИ (187-ФЗ)

Указ президента РФ № 250

повышение защищённости КИИ за счёт отечественного ПО и выделения заместителя гендиректора по ИБ

Нормативная база

187-ФЗ «О безопасности КИИ»: выполнение требований нормативных документов, относящихся к данному ФЗ

Карта реализации технических мер приказа № 239 ФСТЭК России

Какие бизнес-задачи помогает решить InfoWatch ARMA

1. Обеспечить соответствие требованиям регуляторов
2. Обеспечить эшелонированную защиту от внешних угроз с единым центром управления
3. Предотвратить штрафы и уголовную ответственность руководителей
4. Предотвратить финансовые потери, связанные с простоем и остановкой производства
5. Повысить эффективность предприятия

Помогаем конкретным предприятиям

INFOWATCH® ARMA

Госпредприятия с объектами КИИ в составе (187-ФЗ)

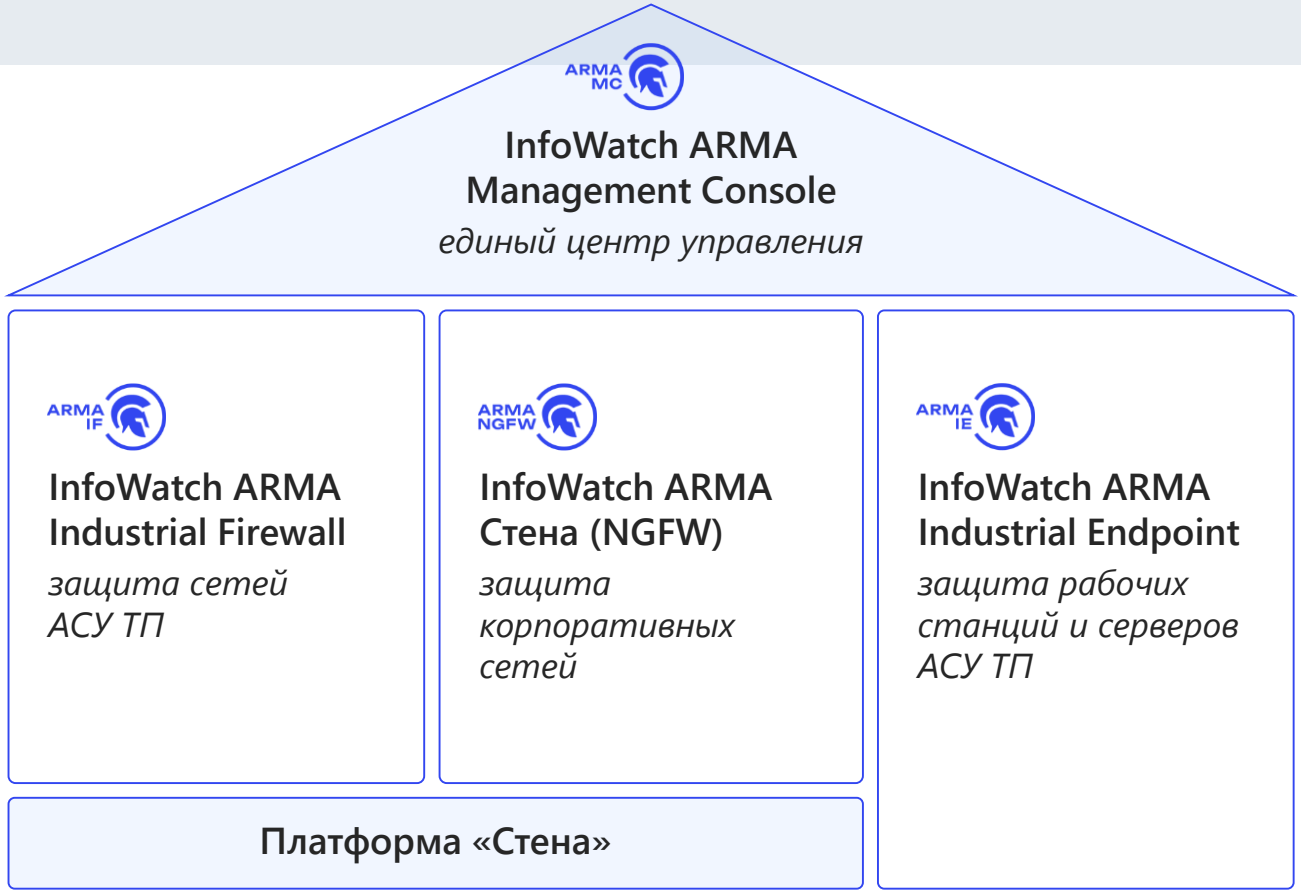
предприятия с объектами критической информационной инфраструктуры (КИИ)

Предприятия с промышленной сетью

где политики безопасности остаются неизменными или меняются не чаще раза в месяц

- энергетика
- нефтегазовая отрасль
- металлургия
- машиностроение
- управление движением
- водоотведение
- водоподача

Портфель решений InfoWatch ARMA



Защита сетевой инфраструктуры

INFOWATCH® ARMA

INFOWATCH ARMA СТЕНА (NGFW)

межсетевой экран нового поколения для защиты корпоративной сети

ngfw.infowatch.ru

Сертифицированный, отечественный NGFW для защиты корпоративной сети

INFOWATCH® ARMA

ПО и ПАК российского производства

Пропускная способность до 10 Гбит/с

Быстрые поставки ПАК — до 4 недель

Сертифицирован ФСТЭК России МЭ типа «Б» и «Д» 4 класса защиты, СОВ 4 класса защиты

Задачи и возможности

Решаемые задачи

Фильтрация сетевого трафика

Управления доступом пользователей и приложений

Обнаружение и предотвращение атак

Основные возможности

— Обнаружение и предотвращение вторжений (IPS / IDS)

— Разбор промышленных протоколов до уровня команд

— URL-фильтрация

— Журналирование событий

— Контроль приложений

— Маршрутизация трафика VPN на подсети

— Работа в отказоустойчивом кластере (VRRP)

— Аутентификация пользователей (basic, ntlm-v2, kerberos)

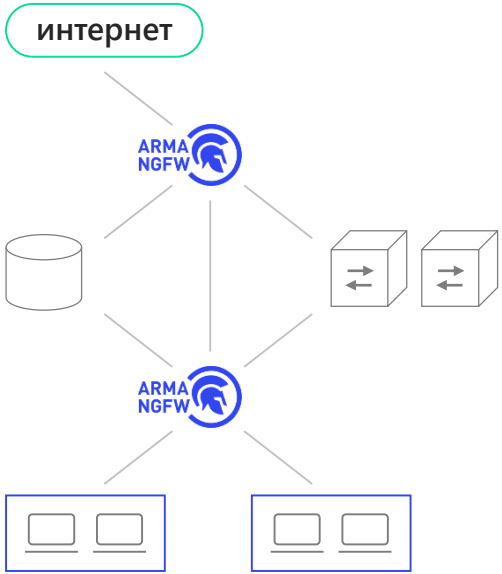
— Интеграция с InfoWatch ARMA Management Console

— GeoIP, QoS, Stunnel, snmp, Reverse Proxy

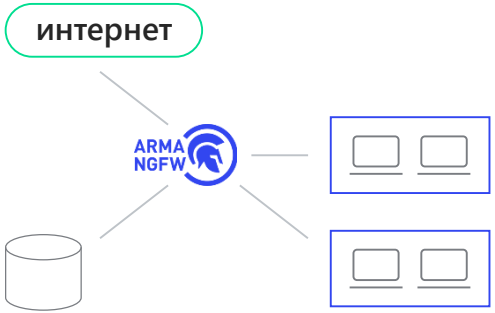
Типовые сценарии применения

Защита всей компании

Защита центрального офиса



Защита филиала



Показатели производительности

8 Гбит/с

при 35 000 правил IPS
и 100 правилах МЭ

Внутренние тесты InfoWatch

6,2 Гбит/с

при 65 000 правил IPS
и 200 правилах МЭ

*Независимое тестирование
«Инфосистем Джет»*

Аппаратные платформы в наличии

на складе

ARMA Стена K10000

до 10 Гбит/с

2 × Intel Xeon Silver 4310 (12C / 24T)
12 × RJ45, 8 × SFP и 2 × SFP+

ARMA Стена K1000

до 1 Гбит/с

Intel Xeon D-1537 (8C / 16T)
8 × RJ45 и 8 × SFP

ARMA Стена K100

до 1 Гбит/с

Intel Atom X6425E 2.00 GHz (4C / 4T)
8 × RJ45

ARMA BOX-6E

до 1 Гбит/с
Intel Core i7-8700
6 × RJ45

ARMA BOX-4E

до 1 Гбит/с
Intel Atom E3930
4 × RJ45

INFOWATCH®

ARMA

ARMA IF

ARMA IE

ARMA MC

INDUSTRIAL FIREWALL

Защита промышленной сети

arma-firewall.infowatch.ru

Как защищает Industrial Firewall?

Межсетевое экранирование

Позволяет блокировать неавторизованные действия и запрещать недопустимые операции с ПЛК (перепрошивку, изменение ПО, запись информации в ПЛК и др.)

VPN

Обеспечивает безопасность информации при объединении в единую сеть филиалов предприятия, удалённом подключении к производственной площадке или при работе технической поддержки

QoS

Позволяет настроить приоритизацию трафика, тем самым управлять нагрузкой и обеспечить стабильную работу сети

DPI промышленных протоколов

Обнаруживает вторжения по специализированным промышленным протоколам благодаря глубокому разбору трафика до уровня команд

СОВ

Обнаруживает и блокирует вредоносное ПО, компьютерные атаки и попытки эксплуатации уязвимостей ПЛК на сетевом и прикладном уровнях. Сигнатурные базы обновляются регулярно

Proxy

Защищает от базовых атак

Потоковый антивирус

Сканирует и анализирует трафик промышленной сети в реальном времени. При обнаружении вредоносных объектов блокирует их на сетевом уровне

Все необходимые возможности для защиты промышленной сети

INFOWATCH® ARMA

Межсетевое экранирование
— Разделение групп пользователей и устройств на основе белых списков доступа и политик обмена данными
— Встроенный функционал NAT / PAT
— Quality of service (QoS)

IDS / IPS
— Встроенная СОВ
— Сигнатурные базы постоянно обновляются
— Можно дополнять собственными правилами СОВ

DPI промышленных протоколов
Наибольшее количество разбираемых полей протоколов

Потоковый антивирус
— Антивирусные базы постоянно обновляются
— Можно настроить интеграцию с любым антивирусом по ICAP

VPN
— IPsec
— OpenVPN
— OpenVPN-ГОСТ (шифрование на базе сертифицированного ФСБ России СКЗИ)

Динамическая маршрутизация трафика
— OSPF
— RIP
— BGP

— Modbus TCP
— Modbus TCP x90 func. code (UMAS)
— IEC 60870-5-104
— IEC 61850-8-1 MMS
— IEC 61850-8-1 GOOSE
— OPC UA
— OPC DA
— S7 Communication
— S7 Communication plus
— KRUG
— ADS TCP
— EtherCAT
— DNP3
— Fanuc Focas
— ENIP / CIP
— Alpha.Link

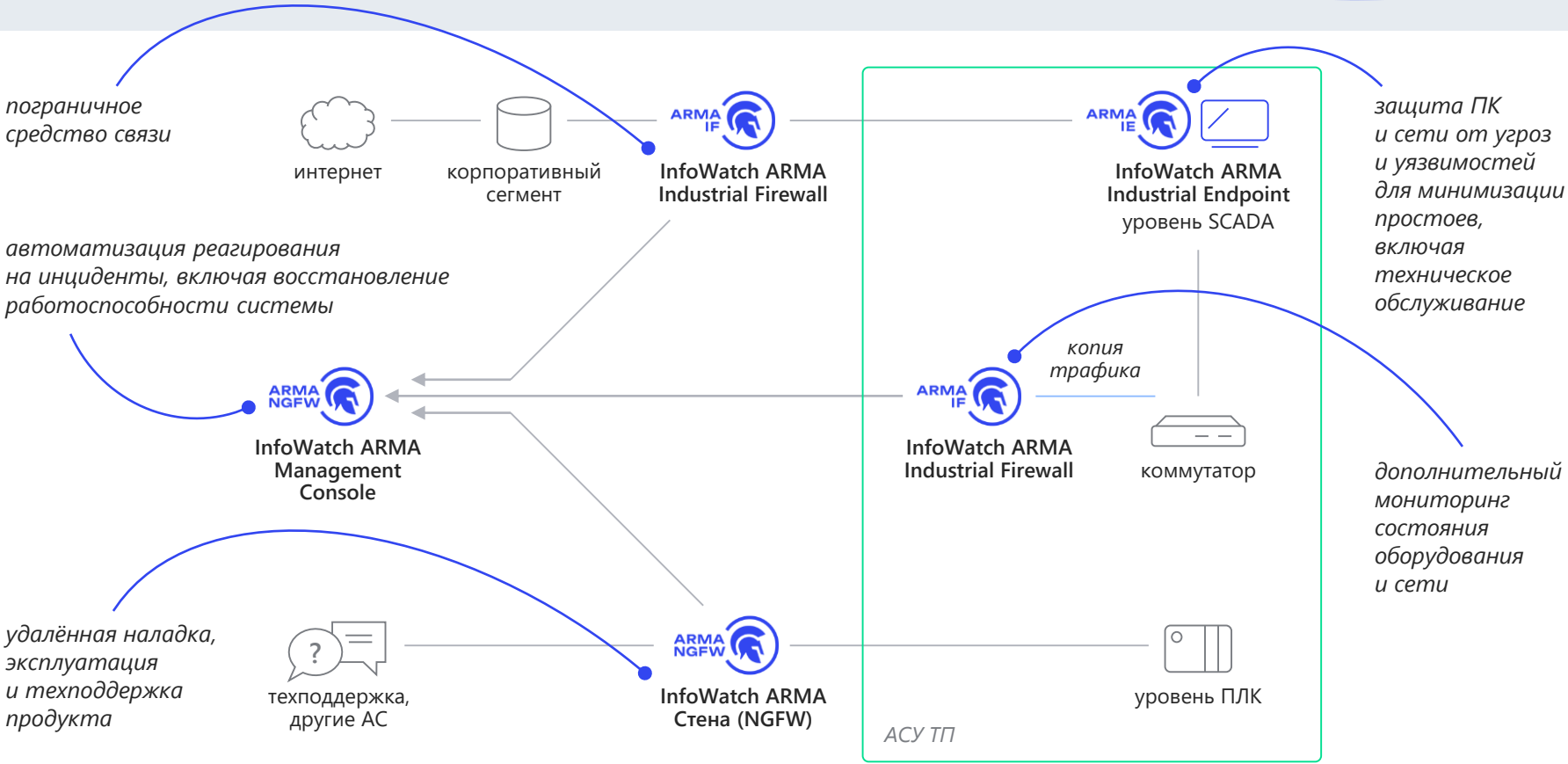
ARMA MC

InfoWatch ARMA Management Console
— Централизованное управление и администрирование группами МЭ
— Сбор событий безопасности в едином центре управления
— Управление инцидентами ИБ и их расследование

Сертификат ФСТЭК России МЭ тип «Д», УД4; СОВ, УД4

Включён в единый реестр российского ПО Минкомсвязи РФ

Сценарии применения InfoWatch ARMA Industrial Firewall



INFOWATCH®

ARMA

ARMA IF

ARMA IE

ARMA MC

INDUSTRIAL ENDPOINT

Защита рабочих станций
и серверов АСУ ТП

arma-endpoint.infowatch.ru

InfoWatch ARMA Industrial Endpoint защищает рабочие станции и сервера АСУ ТП

INFOWATCH® ARMA

Контролирует целостность файлов

непрерывно следит за неизменностью среды рабочих станций и серверов АСУ ТП — файлов и папок

Контролирует запуск приложений по «белому списку»

разрешает доступ только к тем исполняемым файлам, которые необходимы специалистам для работы

Контролирует USB-устройства

разрешает доступ только выбранным классам устройств или конкретным USB-устройствам из списка

INFOWATCH®

ARMA

ARMA IF

ARMA IE

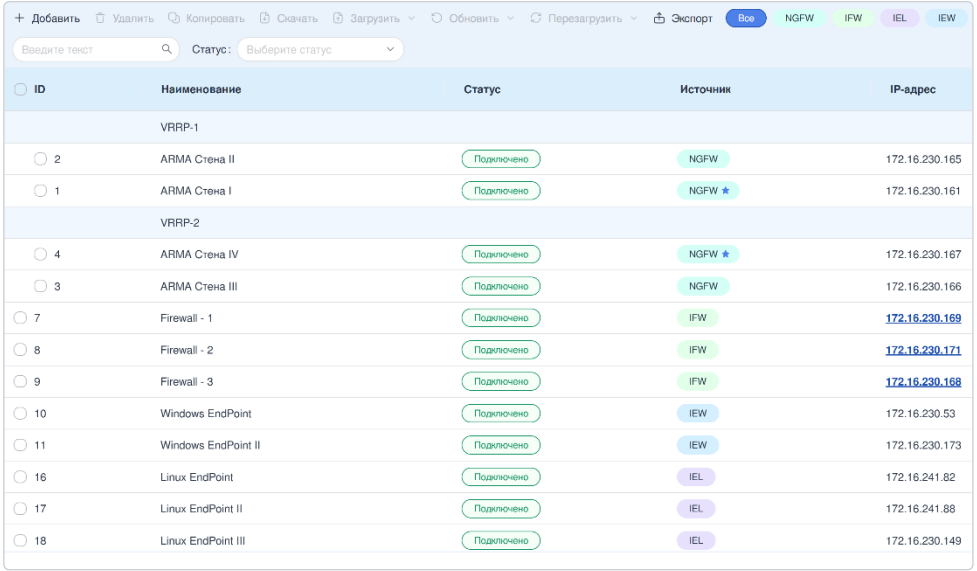
ARMA MC

MANAGEMENT CONSOLE

Единый центр управления СЗИ ARMA
и инцидентами ИБ

arma-console.infowatch.ru

InfoWatch ARMA Management Console управляет системой защиты InfoWatch ARMA



ID	Наименование	Статус	Источник	IP-адрес
	VRRP-1			
2	ARMA Стена II	Подключено	NGFW	172.16.230.165
1	ARMA Стена I	Подключено	NGFW ★	172.16.230.161
	VRRP-2			
4	ARMA Стена IV	Подключено	NGFW ★	172.16.230.167
3	ARMA Стена III	Подключено	NGFW	172.16.230.166
7	Firewall - 1	Подключено	IFW	172.16.230.169
8	Firewall - 2	Подключено	IFW	172.16.230.171
9	Firewall - 3	Подключено	IFW	172.16.230.168
10	Windows EndPoint	Подключено	IEW	172.16.230.53
11	Windows EndPoint II	Подключено	IEW	172.16.230.173
16	Linux EndPoint	Подключено	IEL	172.16.241.82
17	Linux EndPoint II	Подключено	IEL	172.16.241.88
18	Linux EndPoint III	Подключено	IEL	172.16.230.149

Пример интерфейса InfoWatch ARMA Management Console

Управляйте безопасностью без расширения штата

1. автоматизируйте рутину вместо набора сотрудников
2. используйте все возможности защиты в одном окне
3. управляйте всеми средствами защиты удалённо

Возможности Management Console

Централизованное управление InfoWatch ARMA

Industrial Firewall: управление конфигурацией, обновление правил СОВ и перезагрузка устройств

Стена (NGFW): настройка интерфейсов, правил, сервисов, балансировки нагрузки и системные настройки

Industrial Endpoint (Linux и Windows): управление конфигурацией, настройки контроля целостности, приложений и устройств

Работа с событиями и инцидентами

- Сбор событий по CEF со всех СЗИ в единый список
- Создание инцидентов на основе событий
- Расследование инцидентов, назначение ответственных
- Управление инцидентами: изменение статусов
- Передача рекомендаций по решению инцидента
- Отправка инцидентов в SIEM-системы

Другие возможности

- Оперативный контроль важной информации в виджетах
- Журналирование всех действий, произведённых пользователями в консоли
- Автоматическая реакция на инцидент: блокировка угрозы и её источника
- Настройка протокола TLS для криптографического шифрования канала связи
- Работа с правилами корреляции: использование встроенных пакетов правил, создание пользовательских правил
- Взаимодействия с ГосСОПКА: отправка инцидентов и взаимодействие с сотрудниками НКЦКИ в онлайн-режиме
- Работа с устройствами сети: визуализация состояния сетевой инфраструктуры на карте сети и в виде списка

Почему выбирают InfoWatch ARMA?

InfoWatch ARMA Industrial Firewall

единственный межсетевой экран с разбором 16+ промышленных протоколов до уровня команд

InfoWatch ARMA Industrial Endpoint

лёгкий и быстрый, не нагружает рабочие станции

InfoWatch ARMA Management Console

единый центр управления продуктами ARMA с возможностью передачи данных в ГосСОПКА

Выполнение технических требований приказа ФСТЭК России № 239

INFOWATCH® ARMA

СПАСИБО
ЗА ВНИМАНИЕ!

arma.infowatch.ru /InfoWatchOut /InfoWatch