INFOWATCH®

КИБЕРБЕЗОПАСНОСТЬ АСУ ТП

ARMA

INFOWATCH ARMA

arma.infowatch.ru

Комплексная система InfoWatch ARMA

Защита АСУ ТП от современных кибератак на IT- и OT-системы в эпоху цифровой трансформации

Развитие Индустрии 4.0 привело к тому, что к традиционным моделям угроз OT-сетей добавились новые способы атак через уязвимости операционных систем со стороны IT. Главными барьерами оперативному реагированию на вторжения и атаки стало то, что средства защиты устанавливаются точечно, слабо интегрированы между собой и не имеют единого центра управления.

InfoWatch ARMA — отечественная система для обеспечения кибербезопасности АСУ ТП

Защищает критическую информационную инфраструктуру от угроз, которые возникают при смешении IT- и OT-контуров, и исходят как от внутренних, так и от внешних нарушителей.

Позволяет закрыть ~90% технических мер ФСТЭК России (Приказы №235 и №239).

Состав системы InfoWatch ARMA

InfoWatch ARMA Industrial Firewall

Промышленный межсетевой экран нового поколения (NGFW)

InfoWatch ARMA Industrial Endpoint

Средство защиты рабочих станций и серверов SCADA

InfoWatch ARMA Management Console

Инструмент для автоматического реагирования на инциденты и централизованного управления СЗИ

Все компоненты системы InfoWatch ARMA интегрированы между собой и позволяют обеспечить комплексную кибербезопасность.

InfoWatch ARMA Industrial Endpoint

Средство защиты рабочих станций и серверов SCADA

InfoWatch ARMA Industrial Firewall

Промышленный межсетевой экран нового поколения (NGFW)

InfoWatch ARMA

InfoWatch ARMA Management Console

Инструмент для автоматического реагирования на инциденты и централизованного управления СЗИ

InfoWatch ARMA Industrial Firewall

Отечественный промышленный межсетевой экран нового поколения (NGFW)

InfoWatch ARMA Industrial Firewall позволяет своевременно обнаружить и заблокировать атаки на промышленные сети, защитить от несанкционированного доступа и обеспечить соответствие требованиям законодательства.

Какие задачи решает

Защита АСУ ТП от вредоносного ПО и компьютерных атак

Помимо функции межсетевого экранирования, обладает встроенной системой обнаружения вторжений с базой решающих правил СОВ для АСУ ТП и VPN.

Соответствие требованиям регулятора

Позволяет реализовать меры защиты значимых объектов КИИ, согласно требованиям ФСТЭК России. Проходит сертификацию по типу «Д» и 4 классу защиты, в том числе как СОВ. Включён в единый реестр российского ПО Минкомсвязи РФ.

Обеспечение непрерывной работы АСУ ТП уровня Индустрии 4.0

Защищает сети в смешанных средах, благодаря конфигурации active-passive, фильтрации пакетов промышленных протоколов по полям до уровня команд, и организации безопасного удалённого подключения.

Почему профессионалы доверяют защиту АСУ ТП InfoWatch ARMA Industrial Firewall?

Своевременное обнаружение и предотвращение вторжений зависит от способности средства защиты анализировать содержание пакетов промышленного трафика.

InfoWatch ARMA Industrial Firewall глубоко инспектирует пакеты промышленных протоколов. Предоставляет полную информацию о событиях безопасности в промышленной сети и позволяет детально работать с трафиком.

Глубокая инспекция пакетов промышленного трафика

- **Определяет протоколы на основе содержания пакетов промышленного трафика, а не только номера порта**

  Так вы получаете данные трафика, в том числе с нестандартных портов. Это значительно расширяет видимость промышленной сети и позволяет своевременно реагировать на любые угрозы.

- **Позволяет фильтровать протоколы по полям до уровня отдельных команд и их значений**

  Вы можете запрещать или разрешать отдельные команды по протоколам, усиливая защиту специфических АСУ ТП.

Работа с трафиком на уровне команд позволяет настроить защиту под свои задачи. Вот некоторые сценарии, которые используют наши клиенты

- **Контроль действий пользователей**

  Назначайте пользователям права, чтобы контролировать легитимность действий в сети. Например, ограничьте права оператора до функции чтения.

- **Ограничение промышленного трафика на уровне отдельных промышленных протоколов**

  Усилить защиту специфических и даже обособленных АСУ ТП можно благодаря работе с отдельными протоколами. Например, для непрерывного монторинга трафика только проприетарного протокола промышленной системы конкретного вендора, запретите трафик других протоколов.

- **Контроль недопустимых операций с ПЛК**

  Установите запрет на перепрошивку ПЛК, чтобы своевременно реагировать на нежелательные изменения в системе и, в частности, в ПЛК.

- **Расширение зоны видимости сети**

  Своевременно реагировать на угрозы помогают данные трафика, которые поступают со всех типов портов, в том числе нестандартных.

Какие протоколы инспектирует InfoWatch ARMA Industrial Firewall

Позволяет фильтровать по полям до уровня команд и их значений	Обнаруживает вторжения и осуществляет мониторинг
S7 Communication	S7 Communication
	S7 Communication plus
Modbus TCP	Modbus TCP
Modbus TCP x90 func. code (UMAS)	Modbus TCP x90 func. code (UMAS)
OPC DA	OPC DA
OPC UA	OPC UA
IEC 61850-8-1 MMS	IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE	IEC 61850-8-1 GOOSE
IEC 60870-5-104	IEC 60870-5-104
	ENIP / CIP
	Profibus
	DNP3

Встроенная система обнаружения и предотвращения вторжений

Обнаруживает и блокирует вредоносное ПО, компьютерные атаки и попытки эксплуатации уязвимостей ПЛК на сетевом и прикладном уровне.

Результаты пилотных проектов показывают, что наша СОВ обнаруживает больше типов атак, чем известные аналоги*

- **Содержит базу решающих правил СОВ для АСУ ТП, которая обновляется ежедневно**

  Можно самостоятельно дополнять предустановленную базу СОВ собственными пользовательскими правилами для максимальной защиты конкретных АСУ ТП.

- **Использует функцию фильтрации пакетов промышленных протоколов**

  Благодаря детальному разбору трафика до уровня команд и их значений можно настроить автоматическую блокировку вредоносных пакетов в трафике или информационных потоков от источника угрозы.

Межсетевое экранирование для промышленных объектов

Контролирует доступ к сетевым ресурсам, защищает от несанкционированного действия в промышленной сети и регистрирует все информационные потоки.

Почему наше межсетевое экранирование можно использовать на промышленных объектах?

- **Позволяет ограничить использование сервисных функций промышленного трафика**

  Запрещает перепрошивку ПЛК, изменение ПО ПЛК или запись информации в ПЛК. А также даёт возможность устанавливать срок действия учётной записи и гибко назначать права доступа.

- **Использует функцию фильтрации пакетов промышленных протоколов**

  С помощью отдельных команд протоколов можно блокировать неавторизованные действия и запрещать недопустимые операции с ПЛК: подключение к сети АСУ ТП, доступ к параметрам ПЛК или управление ПЛК по сети.

Безопасное удалённое подключение через VPN

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

**По результатам пилотных проектов InfoWatch ARMA, 2019–2020*

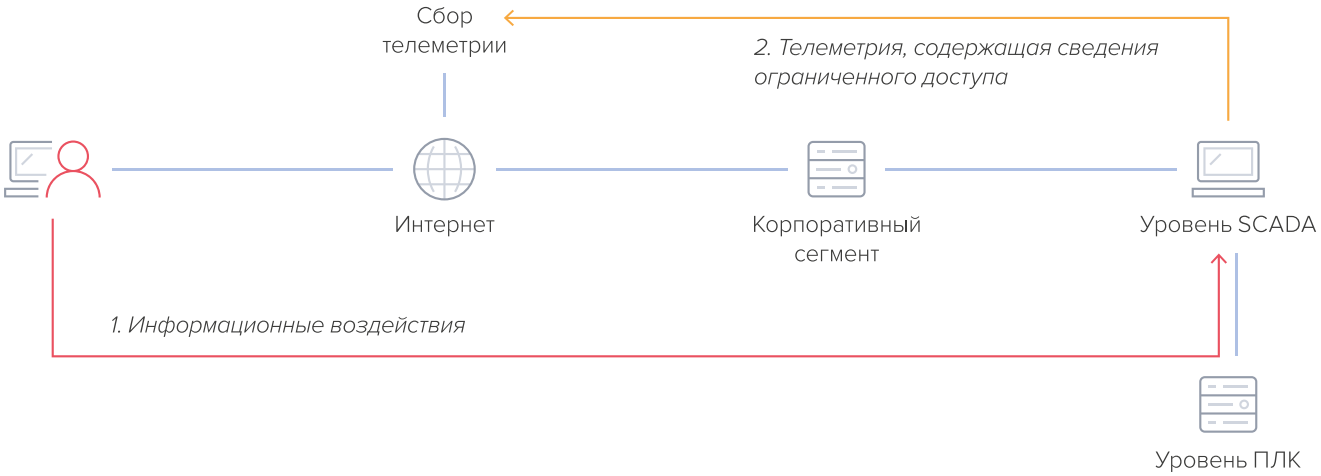
Примеры установки InfoWatch ARMA Industrial Firewall

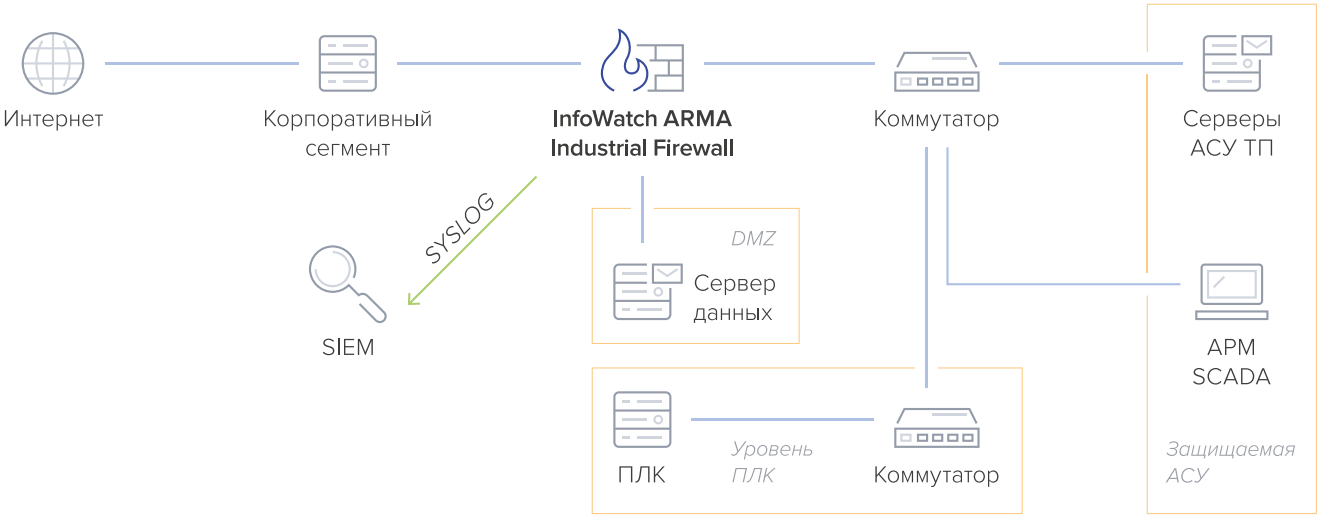
Шесть способов защиты от распространённых типов угроз.

Защищайте АСУ ТП на границе с корпоративным сегментом

- **Угрозы**

  Современная архитектура АСУ ТП не изолирована от корпоративной сети. Вторжение в промышленную сеть возможно через фишинг, заражённое ПО или в результате перехода на заражённый веб-сайт и далее в промышленную сеть.





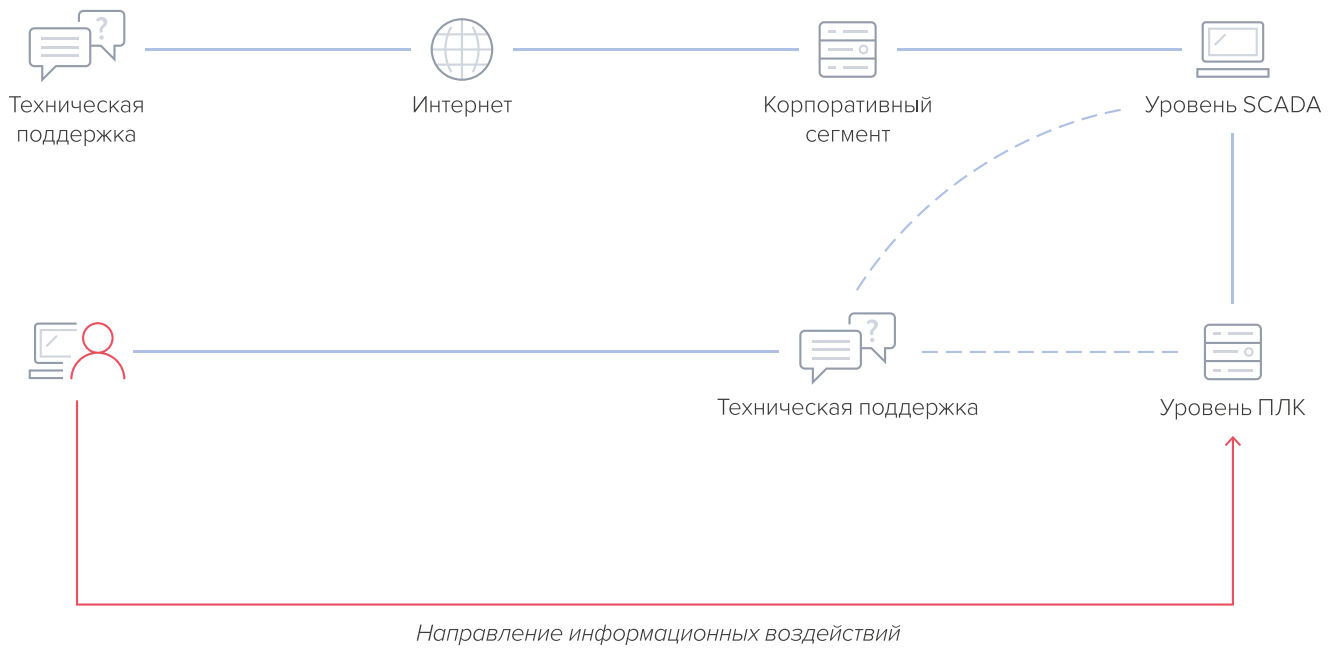
- **Сегментируйте сеть между корпоративным сегментом и АСУ ТП**

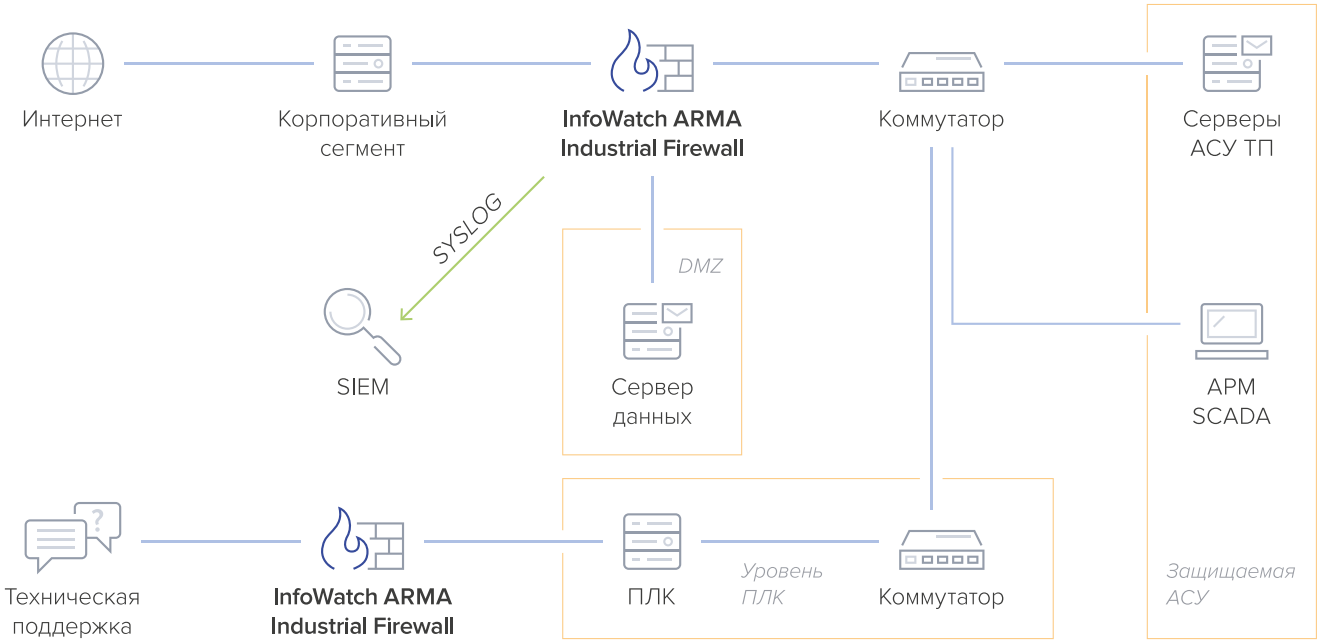
  Аутентифицируйте пользователей, блокируйте атаки с помощью IPS, ограничивайте информационные потоки из корпоративной сети на уровень АСУ ТП.

Защищайте АСУ ТП на границе с каналом технической поддержки

Угрозы

Незащищённый канал технической поддержки может способствовать проникновению вредоносного ПО или предоставить киберпреступникам удалённый доступ к промышленной сети.





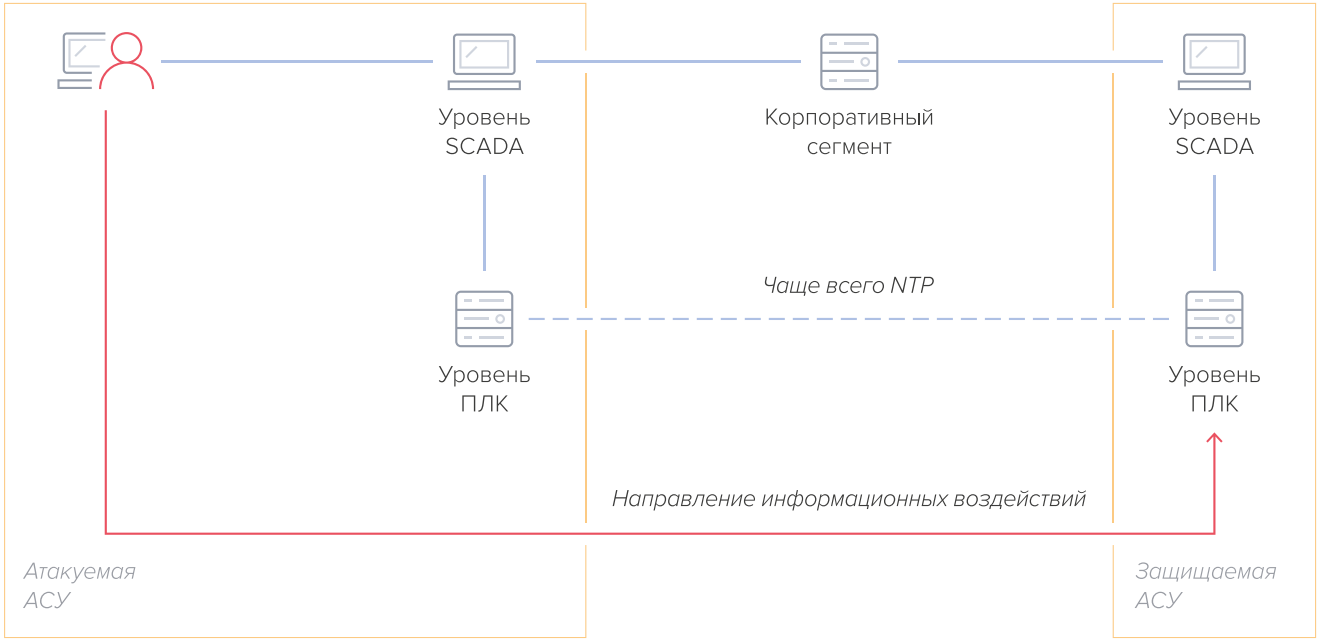
Сегментируйте сеть между технической поддержкой и АСУ ТП

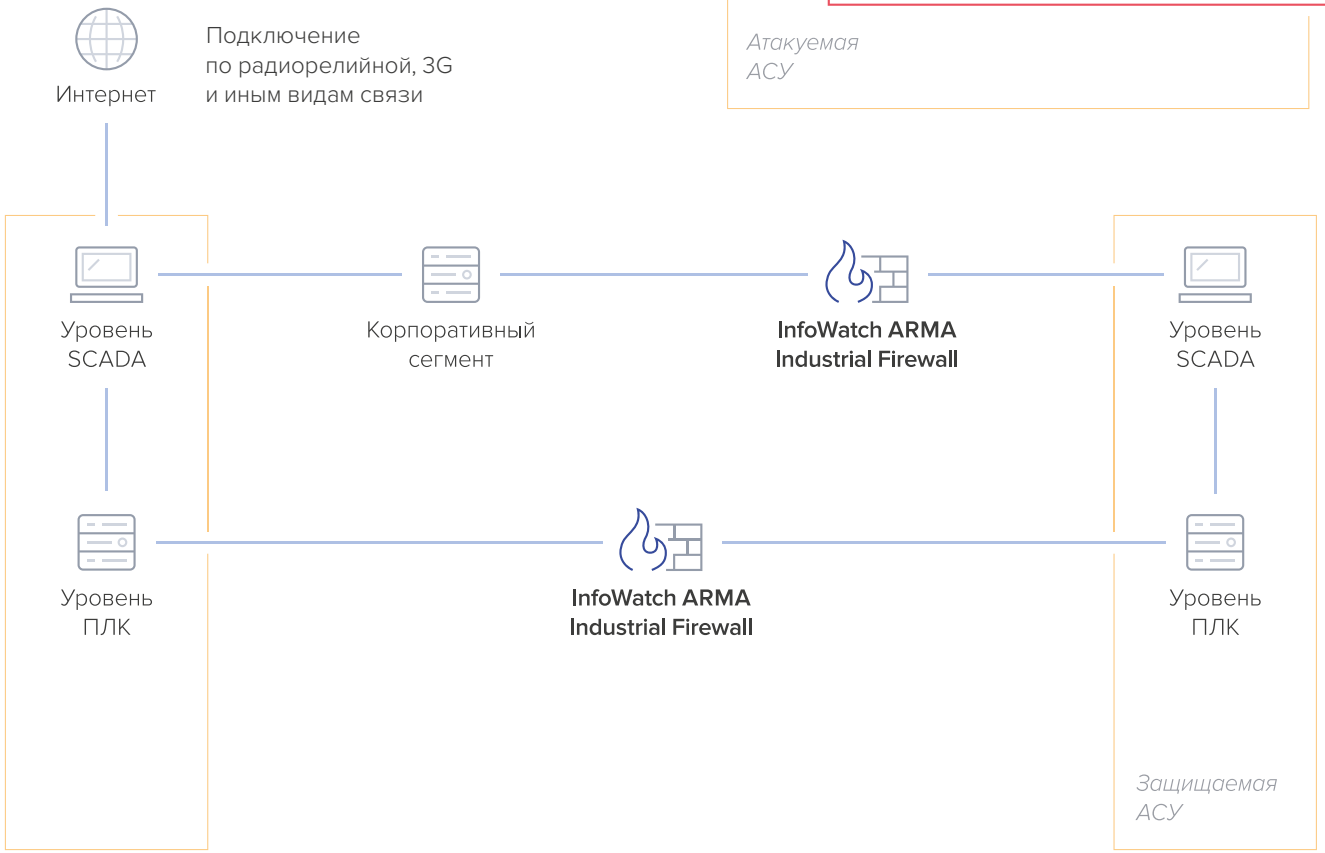
Блокируйте неразрешённые действия технической поддержки по установленным заранее правилам и правам для пользователей, журналируйте все происходящие действия, выявляйте атаки и распространение вредоносного ПО.

Защищайте взаимосвязанные АСУ ТП

Угрозы

Если киберпреступник атаковал одну АСУ через уязвимости ПЛК её уровня, он может получить доступ к смежной АСУ через корпоративный сегмент или смежный уровень ПЛК.





Сегментируйте сеть между смежными АСУ ТП

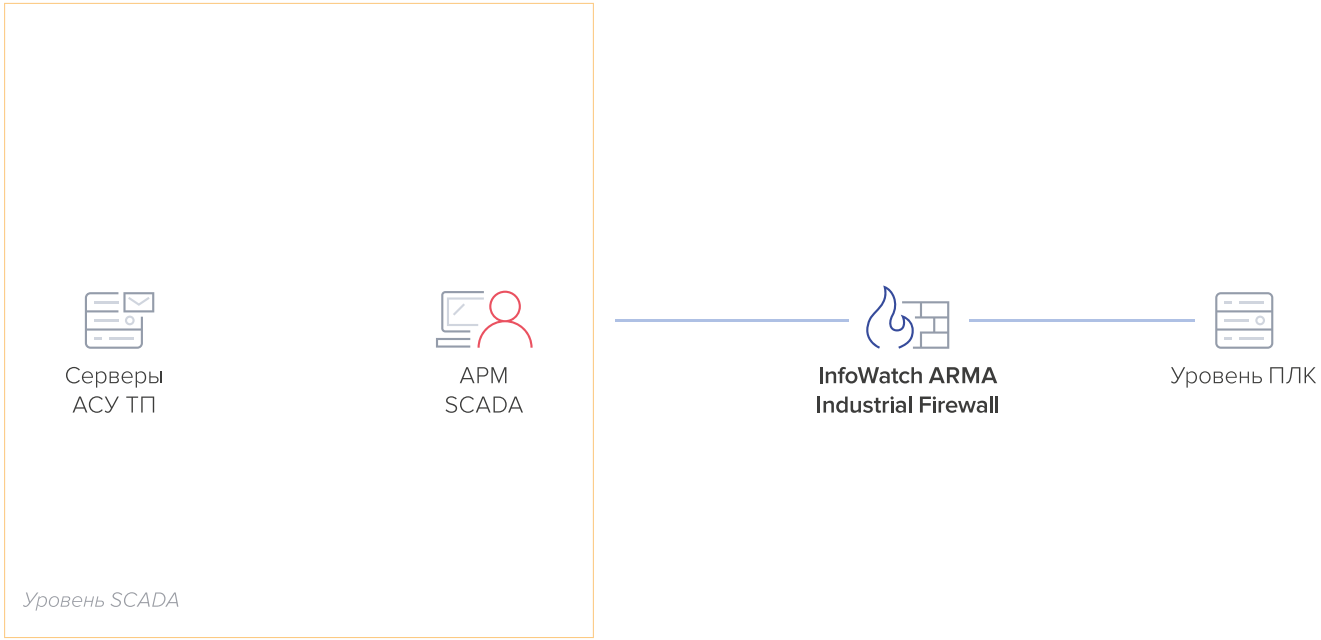
Установите правила и политики взаимодействия АСУ ТП, разного уровня защищённости, а также ограничьте трафик сети внутри обособленных или смежных АСУ ТП.

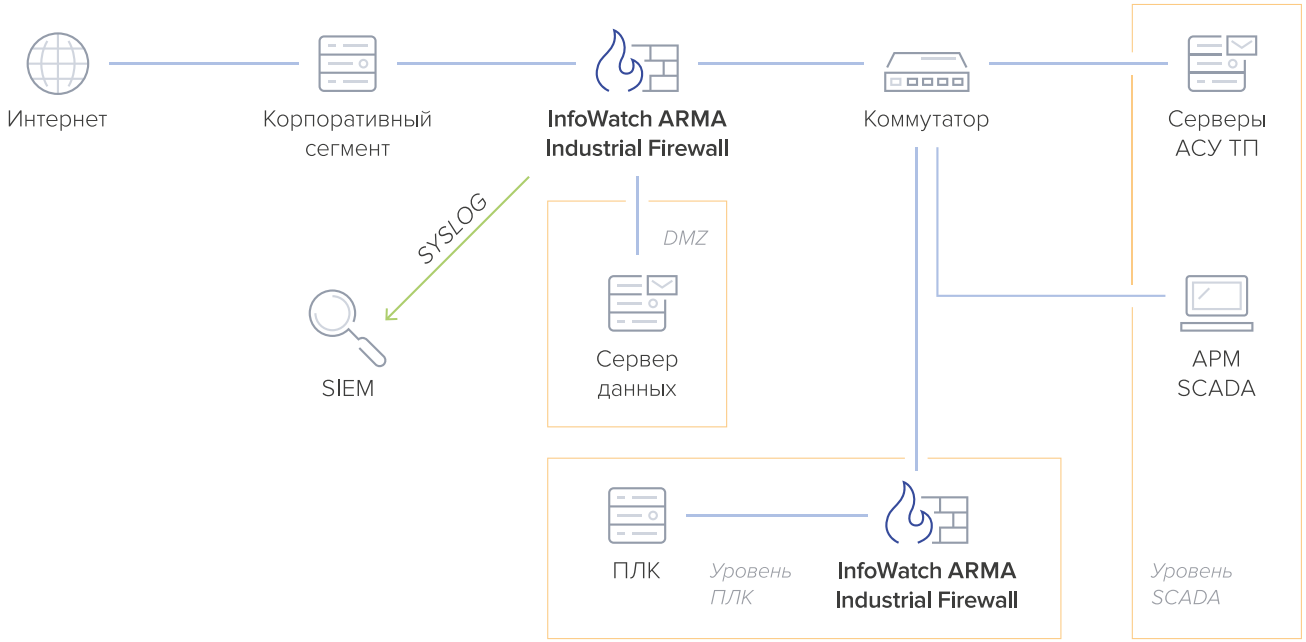
Это может быть особенно актуально, если одна из АСУ ТП подключена к внешней системе передачи данных.

Защищайте сеть между SCADA и ПЛК

Угрозы

Проникновение вредоносного ПО, несанкционированное подключение устройств и даже действия операторов могут нанести ущерб АСУ ТП внутри периметра.





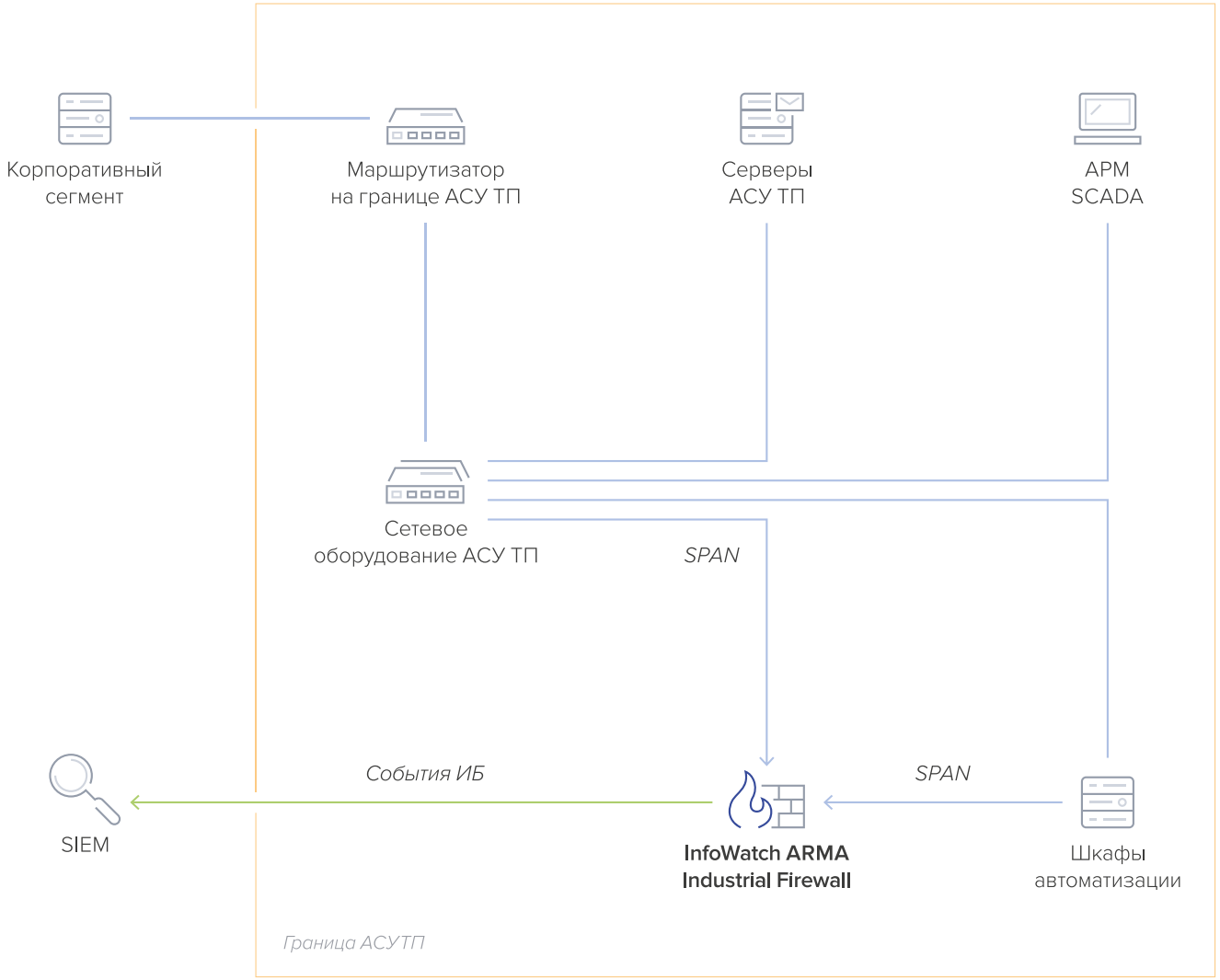
Сегментируйте сеть между SCADA и ПЛК

Установка межсетевого экрана между SCADA и ПЛК позволит построить дополнительный эшелон защиты и разделить права пользователей.

Дополнительные сценарии защиты

Обеспечьте мониторинг трафика внутри АСУ ТП

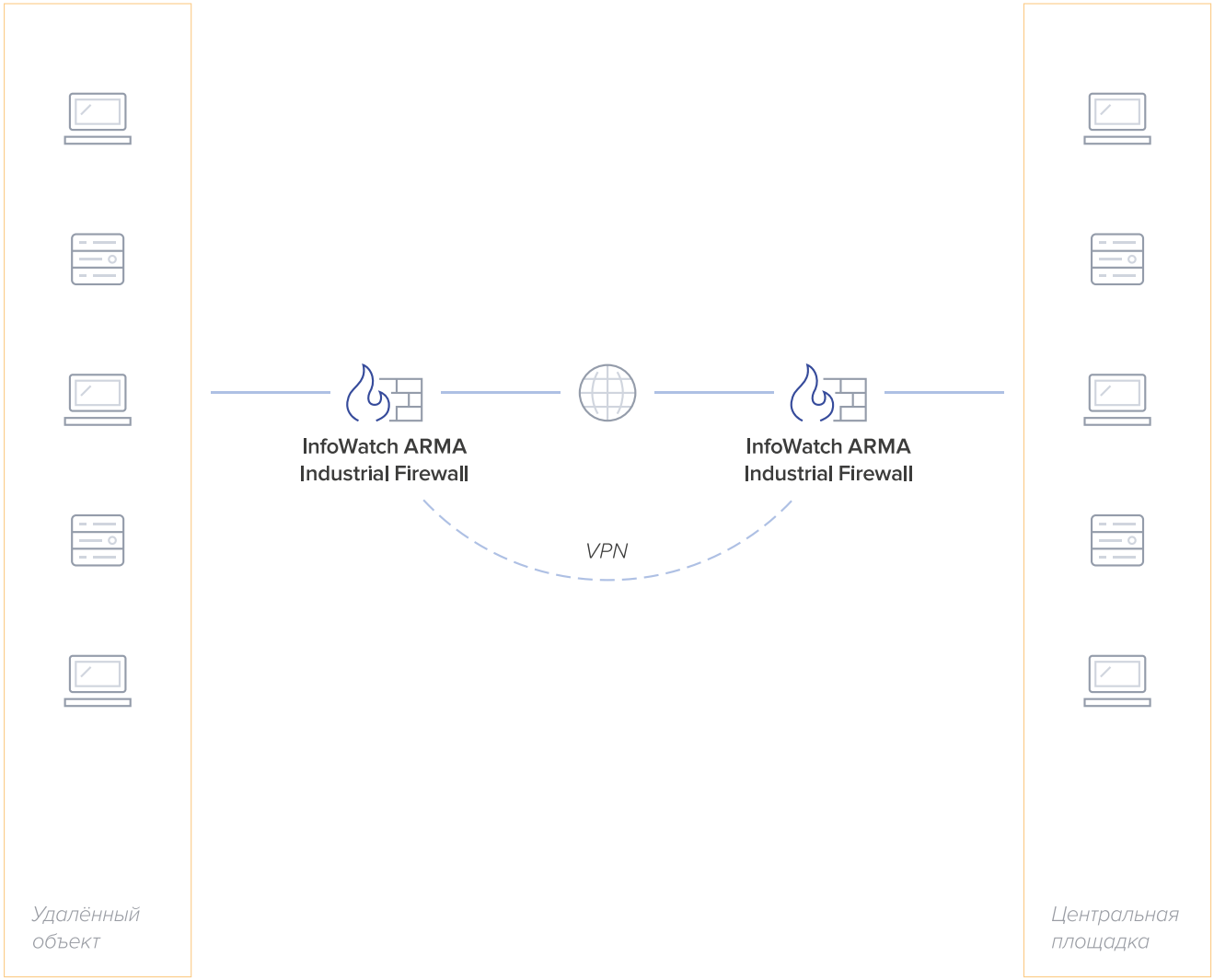
Если не требуется блокировать атаки, то установите **InfoWatch ARMA Industrial Firewall** в режиме мониторинга сети и получайте информацию об аномалиях и действиях пользователей.



Дополнительные сценарии защиты

Защищайте удалённое подключение

Обеспечивайте безопасность информации при объединении в единую сеть филиалов предприятия, удалЁнном подключении к производственной площадке или при работе технической поддержки.



Варианты установки и режимов работы

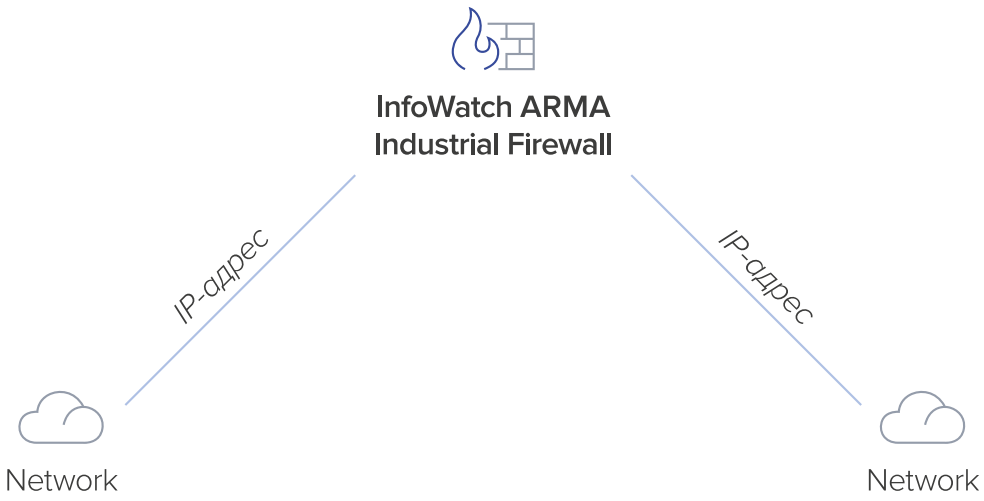
InfoWatch ARMA Industrial Firewall может устанавливаться в сеть в одном из двух типов режимов работы. Первый — в режиме маршрутизации, прозрачного моста, отказоустойчивого кластера или мониторинга. Второй — комбинированным способом.

Режим маршрутизации

Обнаружьте вторжения и заблокируйте атаки в сетях с разными адресами

В режиме маршрутизации **InfoWatch ARMA Industrial Firewall** функционирует как межсетевой экран с функциями обнаружения и предотвращения вторжений, обеспечивая защиту передачи информации на уровне L3.

Может использоваться при объединении подсетей, имеющих разное адресное пространство.



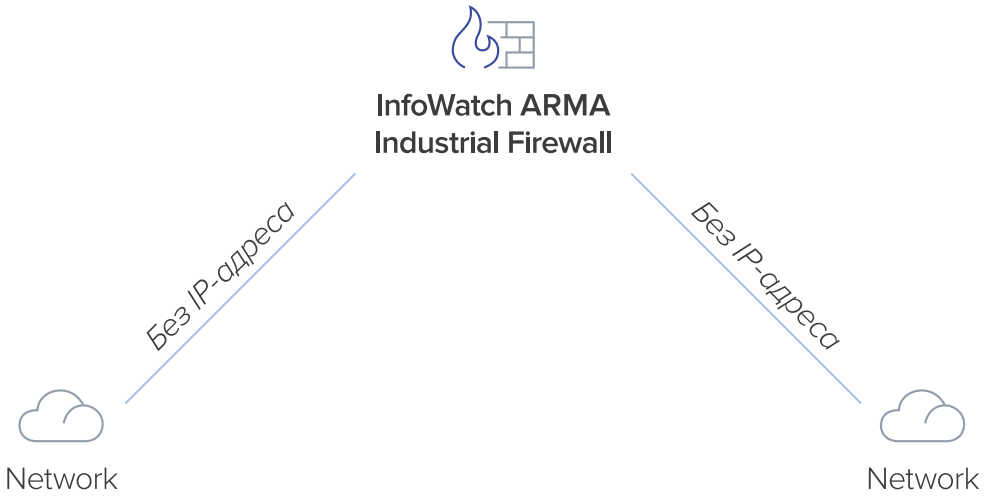
Режим прозрачного моста

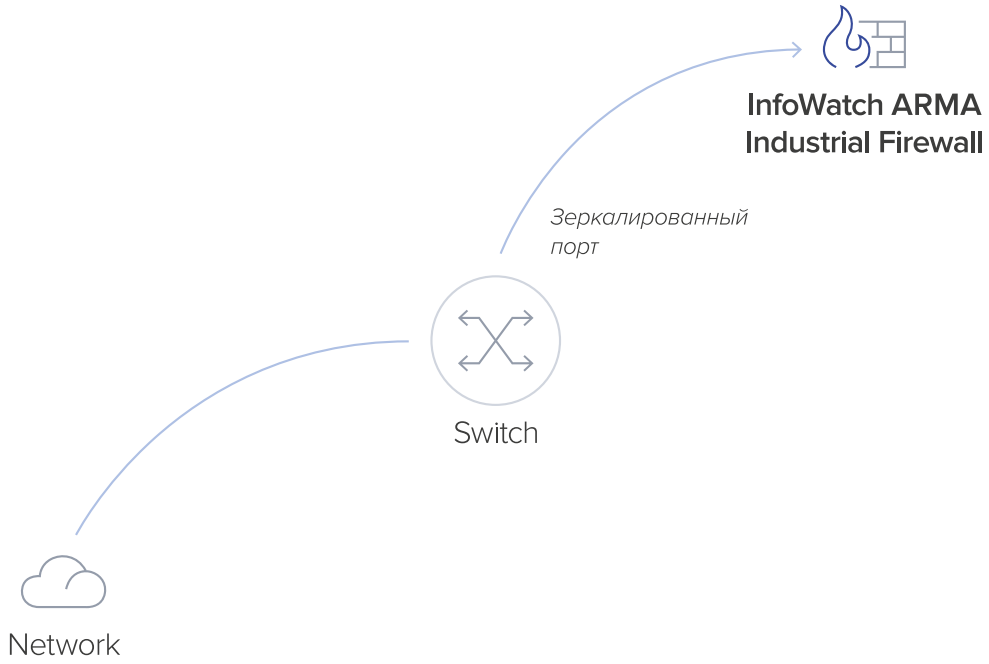
Обнаружьте вторжения и заблокируйте атаки в сетях с общим адресом

InfoWatch ARMA Industrial Firewall работает как система обнаружения и предотвращения вторжений в прозрачном режиме с возможностью блокировки вредоносных пакетов между сетями одного адресного пространства.

Интерфейсы при этом соединены в сетевой мост.

При обнаружении подозрительного либо вредоносного трафика, информация о нём отправляется на веб-интерфейс для информирования пользователей, а при необходимости — блокируется.



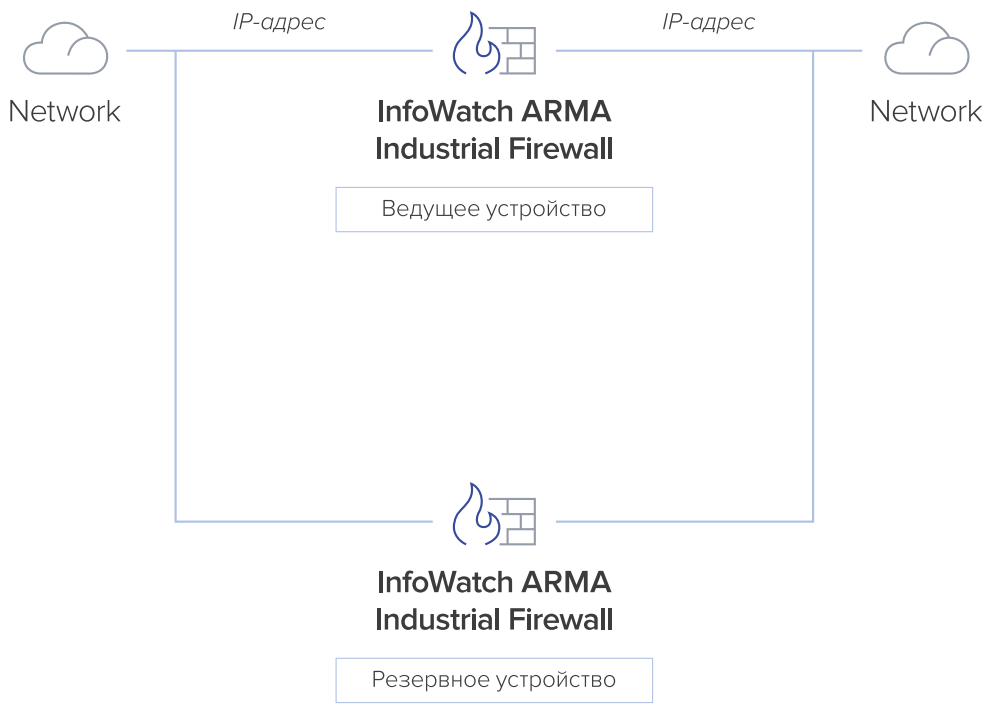


Режим мониторинга с глубоким анализом пакетов трафика (DPI)

Обнаружьте вторжения в копии сетевого трафика с зеркалированного порта

В режиме sniffing mode (мониторинга) **InfoWatch ARMA Industrial Firewall** работает в качестве системы обнаружения вторжений, которая анализирует копии сетевого трафика, снятого с зеркалированного порта.

Проводит глубокий анализ пакетов (DPI) и, в случае необходимости, уведомляет специалиста ИБ АСУ ТП о событиях информационной безопасности.



Режим отказоустойчивого кластера в конфигурации active-passive

Обеспечьте непрерывность и надёжность работы АСУ ТП

В режиме отказоустойчивого кластера несколько **InfoWatch ARMA Industrial Firewall** объединяются в единый кластер в режиме active-passive.

Весь трафик в кластере обрабатывает ведущее устройство, а резервное — непрерывно синхронизирует с ним свою конфигурацию и берёт на себя функцию обработки трафика, в случае, если ведущее устройство выключится.

Варианты поставок и аппаратные конфигурации

Варианты поставок

InfoWatch ARMA Industrial Firewall поставляется в виде образа виртуальной машины или как программно-аппаратный комплекс.

Виртуальные машины

InfoWatch ARMA Industrial Firewall может работать со всеми популярными системами виртуализации:

- VMware
- ORACLE VirtualBox
- Microsoft Hyper-V

Программно-аппаратный комплекс

Серверное и промышленное исполнение предусмотрено без движущих частей:

- Серверы Intel x86 / x64
- Промышленные компьютеры

Аппаратные конфигурации

ПАК InfoWatch ARMA представлен как в промышленном, так и серверном исполнениях без движущих частей для монтажа в стойку или на DIN-рейку.

Монтаж в 19-дюймовую стойку

ARMAIF-RUGRACK

ARMAIF-19RACK

Монтаж на DIN-рейку или в 19-дюймовую стойку

ARMAIF-DIN

ARMAIF-BOX

Лицензии и опции масштабирования

Вы можете выбрать лицензию на один из трёх наборов функций, который решит ваши задачи именно сейчас. Наращивайте функции поэтапно с нашей гибкой системой лицензирования без крупных единовременных инвестиций.

Работа по промышленным протоколам доступна в каждом виде лицензий. Опции лицензирования позволяют расширять функциональность системы без замены оборудования. Например, на первом этапе система может использоваться только на критических объектах, а затем масштабироваться на все процессы промышленной сети.

С полной лицензией вы можете вести работу по промышленным протоколам, пользоваться базой сигнатур и тонко настраивать правила.

Виды лицензий на ПО

1. **Межсетевой экран и VPN**
2. **Система обнаружения вторжений**
3. **Межсетевой экран нового поколения (NGFW)***

*Межсетевой экран с системой обнаружения вторжений и VPN

Технические характеристики

Всё оборудование представлено в базовой комплектации

ARMAIF-RUGRACK

Преимущества

- Работает при температурах от −10 до +55°C
- Степень защиты корпуса — IP 20
- Монтаж в 19-дюймовую стойку

Исполнение	Промышленное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	До 6
Пассивное охлаждение	Да
Питание	2 × 100 Вт
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 4
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 500
Межсетевой экран, пакетов / сек	До 1 800 000
Межсетевой экран, количество одновременных соединений (сессий)	До 2 000 000
Габаритные размеры (Ш × Г × В), мм	1U
Вес, кг	12

ARMAIF-19RACK

Преимущества

- Оборудование без движущихся частей
- При необходимости комплектуется платой bypass
- Монтаж в 19-дюймовую стойку

Исполнение	Серверное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	4 в конфигурации ARMAIF-19RACK-4E, 8 в конфигурации ARMAIF-19RACK-8E
Пассивное охлаждение	Нет
Питание	2 × 450 Вт, с возможностью горячей замены
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 6
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 500
Межсетевой экран, пакетов / сек	До 2 000 000
Межсетевой экран, количество одновременных соединений (сессий)	До 8 500 000
Работает при температурах	От 0 до +40°C
Работает при влажности	От 10 до 95% (без конденсата)
Габаритные размеры (Ш × Г × В), мм	444 × 615 × 44
Вес, кг	16

ARMAIF-DIN

Преимущества

- Степень защиты корпуса — IP 30
- Монтаж на DIN-рейку или настольное исполнение

Исполнение	Промышленное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	До 4
Пассивное охлаждение	Да
Питание	От 12 до 24 В, внешний блок питания
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 1
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 80
Межсетевой экран, пакетов / сек	До 120 000
Межсетевой экран, количество одновременных соединений (сессий)	До 250 000
Работает при температурах	От −20 до +70°C
Работает при влажности	От 5 до 95%
Работает при вибрации	2G, от 10 до 150 Гц, амплитуда — 0.35 мм
Работает при ударе	25G, полусинусоида, продолжительность — 11 мс
Габаритные размеры (Ш × Г × В), мм	155 × 110 × 79
Вес, кг	1,15

ARMAIF-BOX

Преимущества

- При возможности может комплектоваться платой bypass
- Монтаж на DIN-рейку или настольное исполнение

Исполнение	Промышленное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	До 6
Пассивное охлаждение	Да
Питание	2 × 24 В, встроенные блоки питания с резервированием (без возможности горячей замены)
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 2
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 180
Межсетевой экран, пакетов / сек	До 1 100 000
Межсетевой экран, количество одновременных соединений (сессий)	До 1 000 000
Работает при температурах	От −10 до +40°C
Работает при влажности	От 5 до 95% (без конденсата)
Работает при вибрации	3G, от 5 до 500 Гц
Работает при ударе	20G, IEC-68-2-27, полусинусоида, продолжительность — 11 мс
Габаритные размеры (Ш × Г × В), мм	192 × 230 × 127
Вес, кг	4,1

InfoWatch ARMA Industrial Endpoint

Средство защиты информации рабочих станций и серверов SCADA

InfoWatch ARMA Industrial Endpoint — программное обеспечение, которое защищает АСУ ТП от угроз на диспетчерском уровне. Создаёт замкнутую безопасную среду, блокирует запуск недоверенных программ и контролирует целостность ПО рабочих станций и серверов АСУ ТП.

Какие задачи решает

- **Контроль подключения съёмных носителей**

  Позволяет предотвратить угрозы от заражённых съёмных устройств, в том числе портативных — например, смартфонов.

- **Блокировка любого недоверенного ПО**

  Создаёт безопасную замкнутую среду с помощью белого списка программ. Не позволяет исполнять любые файлы, которые не входят в белый список, в том числе вредоносное ПО, например, вирусы-шифровальщики.

- **Контроль целостности файлов и ПО рабочих станций и серверов АСУ ТП**

  Запрещает вносить любые нелегитимные изменения в программную среду рабочей станции или сервера АСУ ТП.

InfoWatch ARMA Management Console

Инструмент для автоматического реагирования на инциденты и централизованного управления СЗИ

InfoWatch ARMA Management Console позволяет своевременно обнаружить и заблокировать угрозы, настроить автоматическое реагирование на инциденты и централизованно управлять обновлениями продуктов комплексной системы **InfoWatch ARMA.**

Какие задачи решает

- ### Централизованное управление продуктами InfoWatch ARMA

  Позволяет централизовано управлять конфигурацией и обновлениями промышленного межсетевого экрана нового поколения — **InfoWatch ARMA Industrial Firewall** и средства защиты конечных устройств АСУ ТП — **InfoWatch ARMA Industrial Endpoint,** а также базами промышленных сигнатур и решающими правилами СОВ.

- ### Управление и расследование инцидентов

  Позволяет расследовать инциденты ИБ, поступающие из промышленной сети, средств защиты других производителей и продуктов комплексной системы **InfoWatch ARMA,** в едином веб-интерфейсе.

- ### Сбор событий ИБ и предоставление инцидентов в SOC- и SIEM-системы

  Собирает события безопасности, коррелирует их в инциденты и отправляет их по протоколу syslog в SOC- или SIEM-системы.

- ### Автоматическая блокировка угрозы на всех средствах защиты

  Позволяет автоматически сформировать реакцию на инцидент. Например, сформировать правило блокировки и настроить по нему средства защиты, как только получит информацию об атаке и её источнике. Специалист ИБ АСУ ТП может использовать предустановленные правила или задать собственный сценарий реагирования.

- ### Визуализация сети

  Позволяет отображать активы на карте сети, видеть все инциденты и взаимосвязь событий. Сотрудник ИБ АСУ ТП может создавать индивидуальные карты любой конфигурации и масштаба.

INFOWATCH®

arma.infowatch.ru

/InfoWatchOut

/infowatchnews

/InfoWatch

Попробуйте на вашем предприятии

Команда **InfoWatch** предусмотрела несколько вариантов тестирования **InfoWatch ARMA.** Процесс стал удобным и необременительным. Начать можно с демонстрации работы, а дальше выбрать, нужно ли пригласить специалистов InfoWatch для проведения пилотного проекта или самостоятельно развернуть решение на ваших мощностях. Мы в любом случае вас поддержим.

sales@infowatch.ru

+7 495 22 900 22

InfoWatch — ведущий российский разработчик решений для обеспечения информационной безопасности организаций. С 2003 года мощная академическая база, лучшие инженеры, математики и лингвисты обеспечивают технологическое преимущество InfoWatch в области защиты предприятий от современных киберугроз, информационных и инсайдерских атак.

Признанный эксперт и лидер рынка России и СНГ в области защиты корпоративных данных, InfoWatch успешно выполнил более 2000 проектов для коммерческих и государственных организаций в 20-ти странах мира.

Две трети из 50-ти крупнейших компаний России (в соответствии с рейтингом «Эксперта») доверили InfoWatch выполнение масштабных и, зачастую, нестандартных проектов, связанных с информационной безопасностью. Причина такого доверия не только в качестве и уникальности технологий, но и в чувстве уверенности, которое даёт InfoWatch, когда сопровождает своих клиентов на всех этапах проектных работ.

Федеральная налоговая служба

Федеральная таможенная служба

Министерство обороны РФ

Фонд социального страхования