kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky OT CyberSecurity

Экосистема промышленной кибербезопасности

Угрозы на компьютеры АСУ

По данным Kaspersky ICS CERT, 39,2% компьютеров АСУ в России были атакованы вредоносным программным обеспечением во втором полугодии 2022 года; их количество постоянно растет.

Kaspersky ICS CERT,
март 2023 г.

Киберугрозы для АСУ и промышленных предприятий

Рост интереса хактивистов к системам автоматизации, увеличение числа APT-угроз в промышленном сегменте, уход зарубежных вендоров с российского рынка, ослабление уровня защищенности, новые регуляторные требования — 2022 год был богат на события кибербезопасности. Он доставил много проблем для владельцев и операторов промышленных инфраструктур.

Наиболее значимые изменения в ландшафте угроз для промышленных предприятий и OT-инфраструктур будут теперь определяться прежде всего геополитическими и связанными с ними макроэкономическими факторами.

По данным Kaspersky ICS CERT, в числе мишеней атак все чаще будут встречаться организации из следующих секторов экономики:

Сельское хозяйство, производство удобрений, сельхозтехники и продуктов питания

Ввиду маячащих продовольственных кризисов и переделов продовольственных рынков

Энергетика, добыча и обработка полезных ископаемых, цветная и черная металлургия, химическая промышленность, судостроение, приборо- и станкостроение

Поскольку доступность продукции этих компаний и их технологий входят в фундамент экономической безопасности стран и политических альянсов

Хайтек-компании, фармацевтика и производство медицинского оборудования

Поскольку они необходимы для обеспечения технологической независимости

Логистика и транспорт (включая транспорт энергоресурсов)

Ввиду начавшихся глобальных перестроений логистических цепочек

Среди основных целей APT будет прослеживаться и традиционный фокус на следующее:

Критическая инфраструктура

Атаки с целью закрепиться на «черный день», а в некоторых случаях и с целью нанесения прямого ущерба

Госучреждения

Атаки для сбора всевозможного рода информации об инициативах и проектах государства, связанных с развитием промышленных секторов экономики

Предприятия ВПК

Главные факторы активности атакующих — геополитическая напряженность

Устойчивое развитие промышленных предприятий и объектов критической инфраструктуры напрямую зависит от стабильности производственных и бизнес-процессов и защиты важных активов. В эпоху четвертой промышленной революции число атак на промышленные системы, в частности на системы АСУ ТП и SCADA, продолжает расти. При этом традиционные решения не способны защитить промышленные среды от новых киберугроз. Постоянно меняющаяся ИБ-реальность и необходимость соответствовать требованиям регулирующих органов побуждают организации к внедрению специализированных средств киберзащиты промышленных инфраструктур.

Именно поэтому сегодня как никогда важен выбор надежного партнера, который обладает экспертизой на стыке промышленной и корпоративной кибербезопасности и готов предложить полный арсенал расширенных защитных технологий.

Единая концепция промышленной безопасности

Знания

Аналитика об угрозах

- Kaspersky ICS Threat Intelligence

Повышение осведомленности

- Kaspersky Security Awareness

Тренинги для специалистов

- Kaspersky ICS CERT Training

Достоверная аналитика угроз в АСУ ТП и специальные тренинги

Технологии

Основные

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks

Фокусные

- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN
- Kaspersky Antidrone
- Kaspersky Unified Monitoring and Analysis Platform

Решения на базе KOS

- Kaspersky IoT Infrastructure Security
- Kaspersky Secure Remote Workspace

Полный арсенал защитных решений, протестированных вендорами АСУ ТП

Экспертиза

Анализ защищенности

- Kaspersky ICS Security Assessment

Управляемая защита

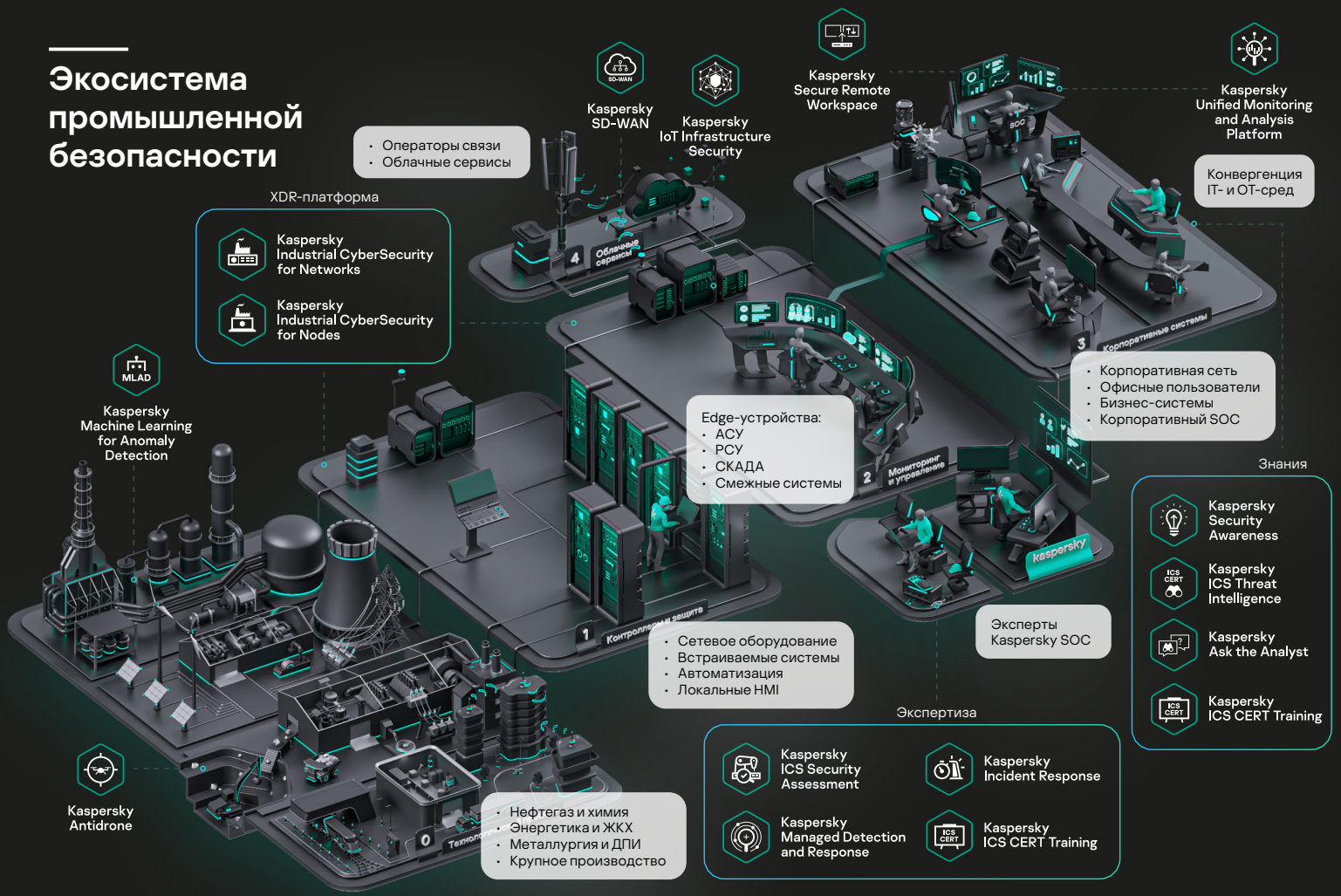
- Kaspersky Managed Detection and Response

Скорая помощь

- Kaspersky Incident Response
- Kaspersky Industrial Emergency Kit

Набор экспертных сервисов для комплексной промышленной кибербезопасности

Экосистема промышленной безопасности



Платформа XDR для промышленности

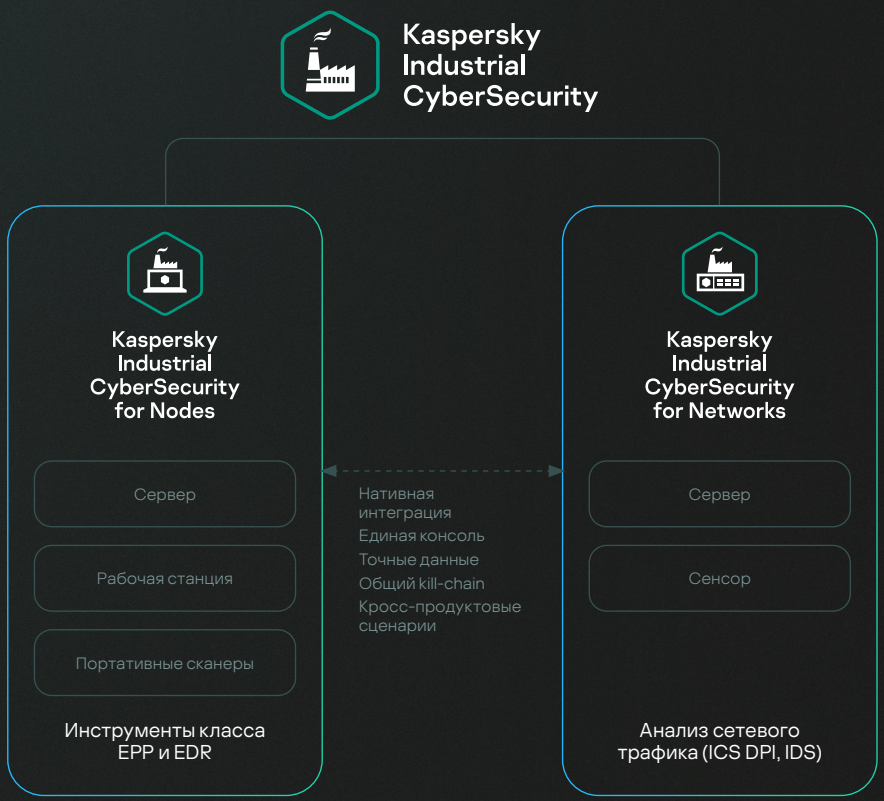
- Показывает скрытые угрозы, аномалии, уязвимости и попытки вторжений задолго до того, как это стало опасным
- Сертифицировано вендорами АСУ ТП и регуляторами
- Не влияет на технологический процесс, исключает недопустимый ущерб
- Помогает управлять сложной распределенной инфраструктурой автоматизации и реагировать на инциденты

Преимущества

Полное покрытие инфраструктуры АСУ. Защита Linux, Windows, изолированных или приносимых компьютеров, обнаружение сетевых аномалий и угроз

Аудит узлов, опрос сетевых устройств, централизованное управление рисками, политиками безопасности и активами на всех уровнях АСУ

Непревзойденная прозрачность при расследовании нарушений. Визуализация развития инцидента в сети и на узлах



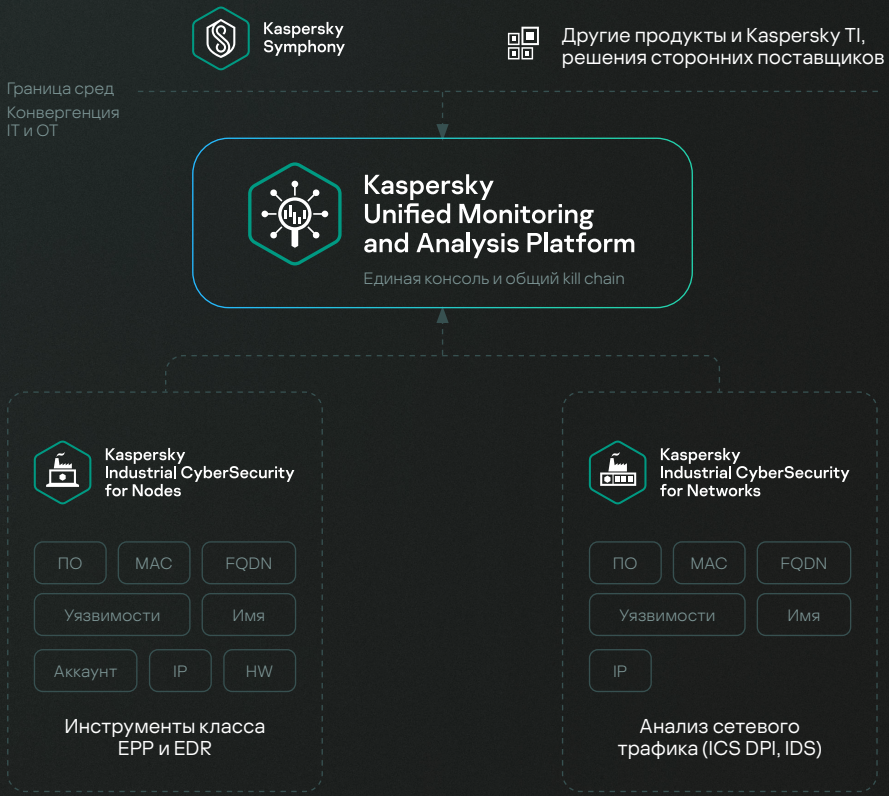
Единая киберзащита одного предприятия

Благодаря тесной интеграции с SIEM-системой Kaspersky Unified Monitoring and Analysis Platform XDR-платформа Kaspersky Industrial CyberSecurity позволяет:

- реализовывать больше сценариев по расследованию и реагированию на инциденты в промышленной сети
- защищать бизнес не только в промышленной среде, но и в той части, где промышленная среда пересекается с корпоративной, тесно взаимодействуя с корпоративной XDR-платформой Kaspersky Symphony
- команды безопасности могут сформировать целостную картину развития инцидента и определить его первопричины для предупреждения подобных инцидентов в будущем

Примеры ответных действий

- Сканирование и обновление баз
- Запуск файла, установка патча
- Смена статуса авторизации
- Изоляция узла и запрет запуска



О продукте

Обзор

Связаться

Раннее обнаружение аномалий и аналитика

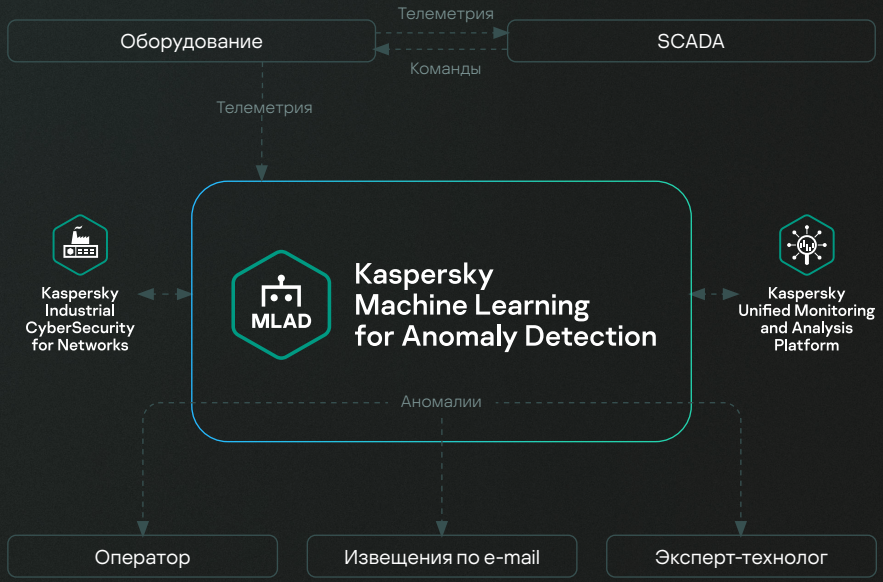
- Обнаруживает дефекты оборудования или ошибки персонала задолго до критической стадии — поможем предотвратить отказ, аварию или выпуск бракованной продукции
- Выявляет нетипичные действия сотрудников или операции с оборудованием — признаки специализированной атаки или саботажа
- Сочетает обнаружение аномалий с предиктивным анализом состояния и срока службы оборудования

Работа в экосистеме и искуственный интеллект

Использует ИИ для анализа телеметрии технологического процесса и событий, связанных с действиями персонала

Интеграция с KICS for Networks и KUMA: получает из систем телеметрию и события, обратно отправляет извещения об обнаруженных аномалиях

Применяет диагностические правила для заранее известных симптомов проблемы, а машинное обучение — для обнаружения любых отклонений от нормального поведения оборудования



Единое решение для надежности промышленных сетей

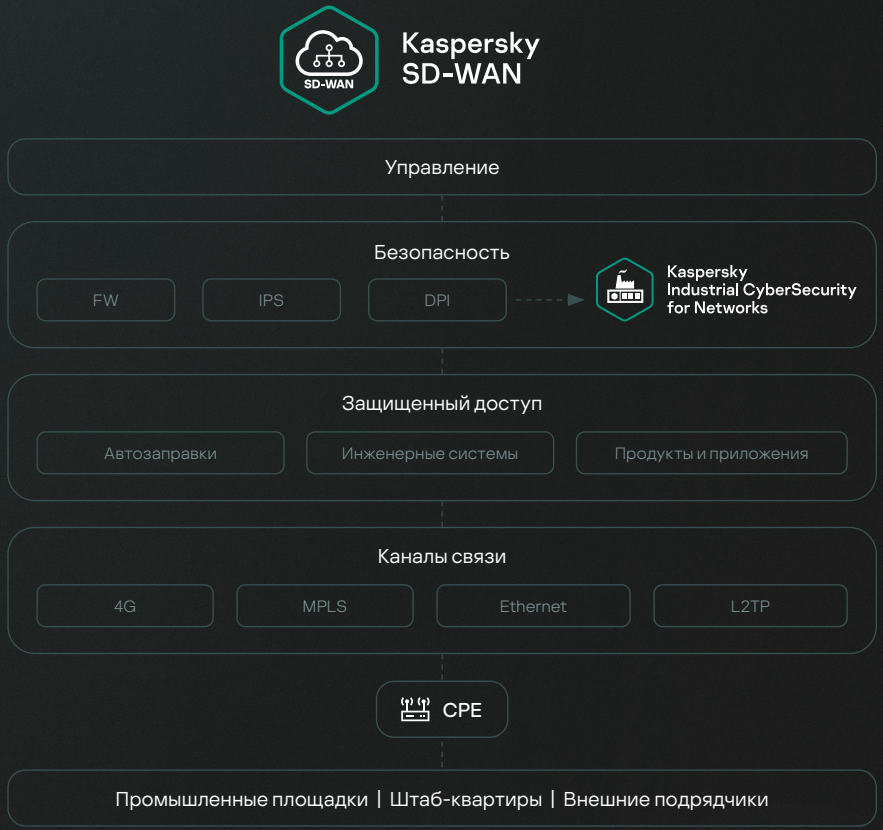
- Построить отказоустойчивую территориально распределенную сеть с централизованным управлением, а также обеспечить непрерывность производственных процессов.
- Архитектура Kaspersky SD-WAN позволяет легко интегрировать средства защиты «Лаборатории Касперского» и других производителей непосредственно в решение
- Использование инфраструктуры SD-WAN решением KICS for Networks позволяет организовать систему централизованного мониторинга и защиты в условиях большого количества распределенных промышленных объектов

Простая масштабируемость сети

Легкое управление

Оптимизация расходов

Централизованная безопасность



О продукте

Обзор

Связаться

Защита от дронов

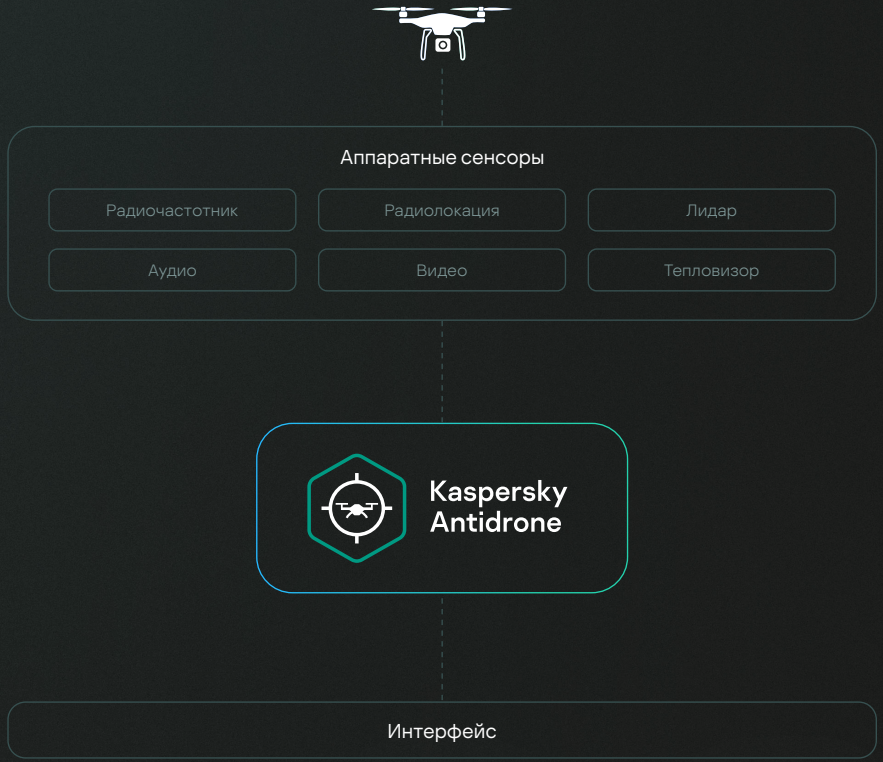
- Kaspersky Antidrone сокращает вероятность остановки процессов промышленных предприятий, исключая проникновение на их территорию несанкционированных дронов
- Система в автоматическом режиме сканирует воздушное пространство, обнаруживая и классифицируя беспилотники. Информация о происходящем выводится в единый интерфейс. В случае опасности и при наличии соответствующих разрешений оператор может нейтрализовать беспилотный летальный аппарат
- Решение Kaspersky Antidrone является модульным и может быть применимо на объекте любого масштаба
- Система также поддерживает режим работы «свой/чужой», что позволяет использовать ее на предприятиях

Ключевые функции

Обнаружение и трекинг дронов

Классификация дронов при помощи нейронных сетей

Возможность интеграции узконаправленных и всенаправленных модулей нейтрализации



О продукте

Обзор

Связаться

Данные для развития бизнеса 4.0

Решение состоит из кибериммунных шлюзов Kaspersky IoT Secure Gateway на базе KasperskyOS, а также из консоли централизованного управления Kaspersky Security Center. Шлюзы безопасно собирают и передают данные с оборудования на цифровые платформы (например, 1С:ERP) для качественной бизнес-аналитики, которая позволяет оптимизировать производства и предотвращать инциденты. Консоль позволяет интегрировать Kaspersky IoT Infrastructure Security с другими решениями Kaspersky.

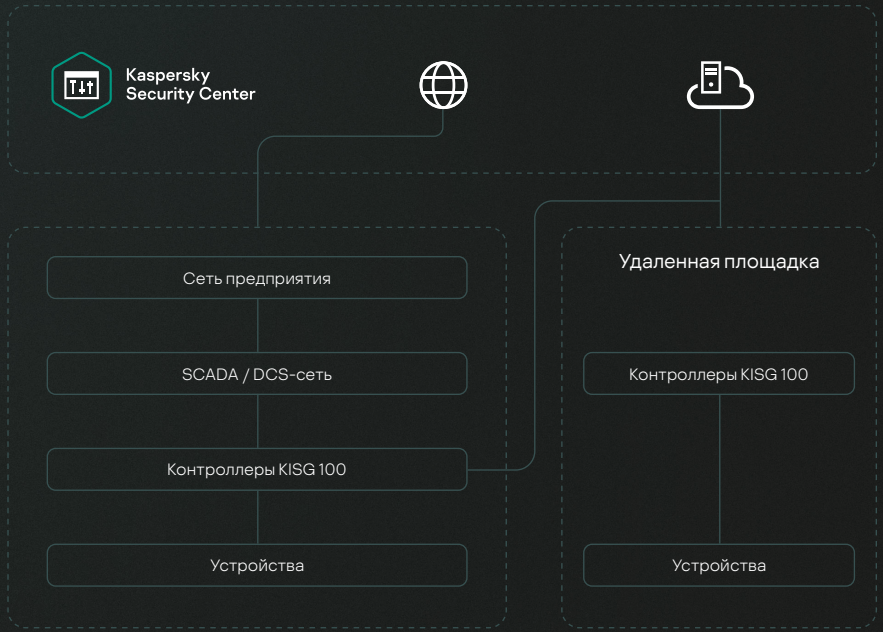
Ключевые функции

Безопасный прямой сбор и транспорт данных с оборудования на цифровые платформы и облака

Прозрачность инфраструктуры и централизованное управление событиями

Кибериммунитет на базе KasperskyOS — исходная киберзащита шлюзов и передаваемых данных, а также функции защиты инфраструктуры

Kaspersky IoT Infrastructure Security



aprotech Развитием и внедрением решения занимается НПО «Адаптивные промышленные технологии» (Апротех, дочерняя компания «Лаборатории Касперского»)

О продукте | Обзор | Демо | Связаться

Кибериммунная инфраструктура тонких клиентов

Кибериммунные тонкие клиенты в составе Kaspersky Secure Remote Workspace обеспечивают защищенное подключение к виртуальным рабочим столам, в т. ч. доверенную зону подключения пользователей к промышленной инфраструктуре

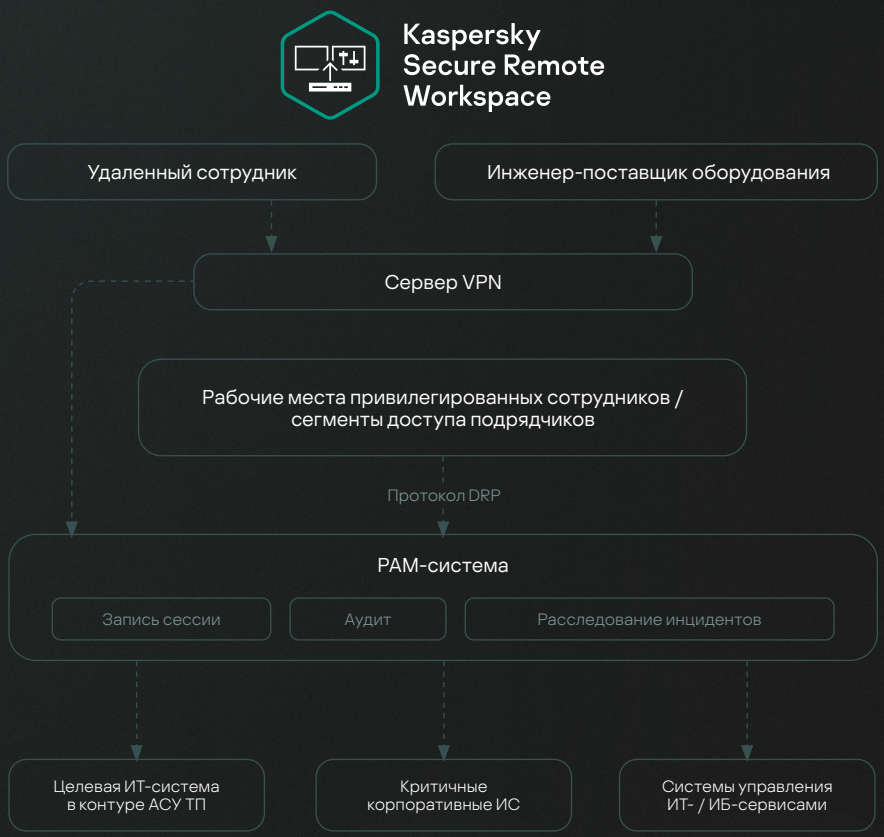
Применение продукта

Риск

Рабочая станция пользователя — одна из самых распространенных целей для кибератак

Решение

Kaspersky Secure Remote Workspace (KSRW) — решение для построения кибериммунной, управляемой и функциональной инфраструктуры тонких клиентов на базе микроядерной ОС «Лаборатории Касперского» — KasperskyOS



Всестороннее понимание угроз и уязвимостей

Услуги категории Threat Intelligence для оценки рисков, успешного расследования инцидентов и реагирования. Сервис подкреплен глубокой экспертизой и опытом Kaspersky ICS CERT — первого частного CERT в промышленной кибербезопасности.

Ландшафт угроз для АСУ ТП России

Подробнее

Ключевые возможности

Быстрое обнаружение угроз и широкие аналитические возможности

Повышение эффективности расследований и активного поиска угроз

Исчерпывающая информация по угрозам и уязвимостям для принятия взвешенных решений

Kaspersky ICS Malware Data Feed

Регулярно обновляемый поток данных об актуальных угрозах для систем АСУ ТП, позволяющий упростить и автоматизировать обнаружение и расследование атак. Основан на телеметрии с более чем 1 млн узлов, относящихся к АСУ ТП

Kaspersky ICS Threat Intelligence

ICS CERT

Kaspersky ICS Threat Intelligence Reporting

Отчеты и оповещения о кибератаках на промышленные предприятия и об уязвимостях в промышленном ПО и оборудовании, а также регулярные обзоры угроз для систем промышленной автоматизации, доступные через web-портал или API

Kaspersky ICS Vulnerability Data Feed

Регулярно обновляемый поток проверенных и уточненных данных об уязвимостях в ПО и оборудовании для АСУ ТП в машиночитаемом формате

Что получает клиент

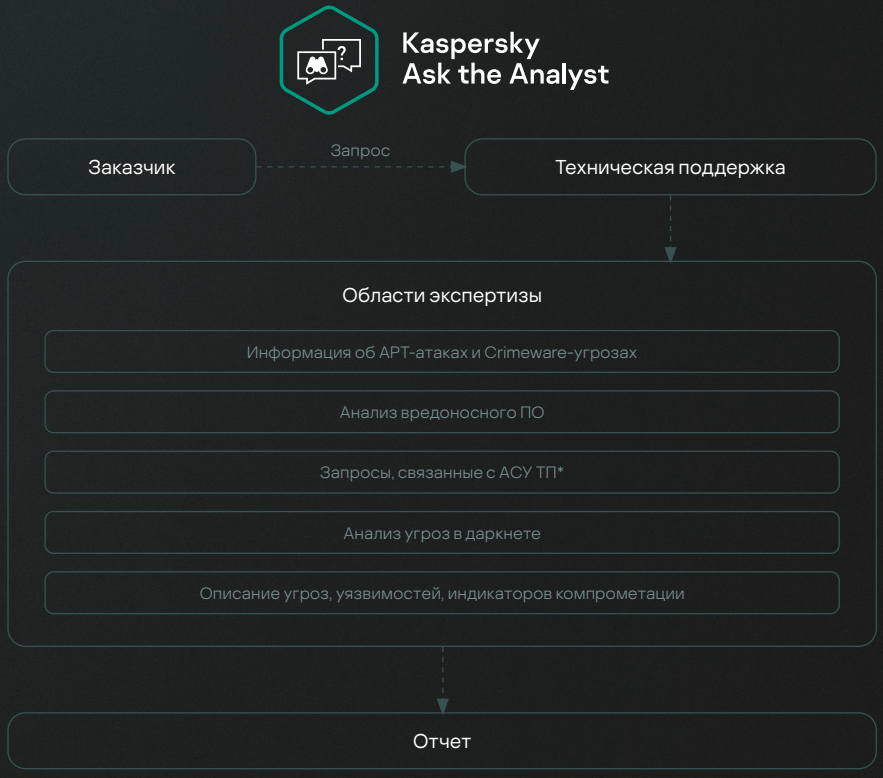
Kaspersky Ask the Analyst дополняет наш портфель сервисов Kaspersky Threat Intelligence. С помощью этого сервиса вы можете обращаться к экспертам за поддержкой и полезной информацией по конкретным угрозам и уязвимостям, с которыми вы сталкиваетесь или которые вас интересуют. Используя эти данные, вы сможете усовершенствовать систему защиты против угроз, нацеленных как на вашу организацию в целом, так и на вашу промышленную инфраструктуру.

Ключевые преимущества

Подробные инструкции наших экспертов для оперативного реагирования на обнаруженные угрозы и уязвимости

Персонализированная и подробная контекстная информация для эффективных расследований

Доступ к ведущим threat intelligence экспертам, включая экспертов промышленной безопасности Kaspersky ICS CERT



*Дополнительная информация об опубликованных отчетах, информация об уязвимостях АСУ ТП, статистика угроз АСУ ТП и новые тенденции по регионам и отраслям, анализ вредоносных программ, нацеленных на АСУ ТП, информация, касающаяся нормативных требований и стандартов

Постоянное повышение киберграмотности сотрудников промышленных организаций

Kaspersky Security Awareness

Геймифицированные тренинги

Kaspersky Interactive Protection Simulation (KIPS)

Интерактивная командная игра позволяет симулировать возможные последствия кибератак и связанные с ними решения руководства на сценариях, специально проработанных для конкретных отраслей: ТЭС, ГЭС, нефтегаз и химия и др.

Kaspersky Gamified Assessment Tool (GAT)

Быстрый и увлекательный способ оценки навыков сотрудников в области кибербезопасности. По итогам оценки для сотрудника формируются рекомендации, которые можно учесть при составлении программы обучения для конкретной группы сотрудников в ASAP.

Интерактивные онлайн-платформы

Платформа Kaspersky Automated Security Awareness Platform (ASAP)

Автоматизированный эффективный инструмент для повышения осведомленности сотрудников по всем основным темам IT-безопасности, включая «Кибербезопасность промышленных систем». Помогает выработать у сотрудников полезные и практичные навыки кибергигиены.

Cybersecurity for IT Online (CITO)

Интерактивный онлайн-тренинг для ИТ-специалистов общего направления, где они получат практические навыки распознавания возможного сценария атаки при якобы безобидном инциденте и сбора данных об инцидентах для передачи их в службу IT-безопасности.

Очные тренинги от экспертов по промышленной кибербезопасности

Kaspersky
ICS CERT Training

Основы кибербезопасности АСУ ТП

2-дневный курс с инструктором из Kaspersky ICS CERT

Тренинг о важнейших аспектах промышленной кибербезопасности повышает общий уровень осведомленности о безопасном поведении на всех уровнях организации — от OT- и IT-специалистов до управленцев, а также учитывает специфику конкретной отрасли. Продолжительность тренинга может быть скорректирована по запросу заказчика.

Расследование инцидентов

5-дневный курс по цифровой криминалистике в АСУ ТП

Участники тренинга смогут изучить все аспекты и тонкости цифровой криминалистики в АСУ ТП, начиная с установления факта инцидента и сбора улик и заканчивая анализом данных и подготовкой отчета о расследовании. Курс создан для специалистов по информационной безопасности и безопасности систем АСУ ТП.

Поиск уязвимостей

3-дневный курс по поиску уязвимостей в IoT-устройствах

Обучение проведению полного и всестороннего исследования устройств интернета вещей (IoT) на уязвимости и подготовке экспертных рекомендаций по принятию мер для исправления выявленных недочетов. Тренинг будет интересен специалистам по тестированию, разработчикам и исследователям проблем безопасности.

3-дневный курс по поиску уязвимостей в ПО методом фаззинга

Изучение на примере практических заданий современных методик, подходов, инструментов и техники для выявления ошибок и возможных критических уязвимостей в программном обеспечении. Тренинг будет полезен всем, кто участвует в процессе проектирования, создания и тестирования приложений под Linux и Windows.

Анализ защищенности промышленной инфраструктуры

Комплексный подход к выявлению уязвимостей и недостатков систем безопасности в инфраструктурах АСУ ТП, включая: поверхность атаки, уровень безопасности промышленной сетевой инфраструктуры, РСУ и промышленных устройств, риски компрометации критически важных систем.

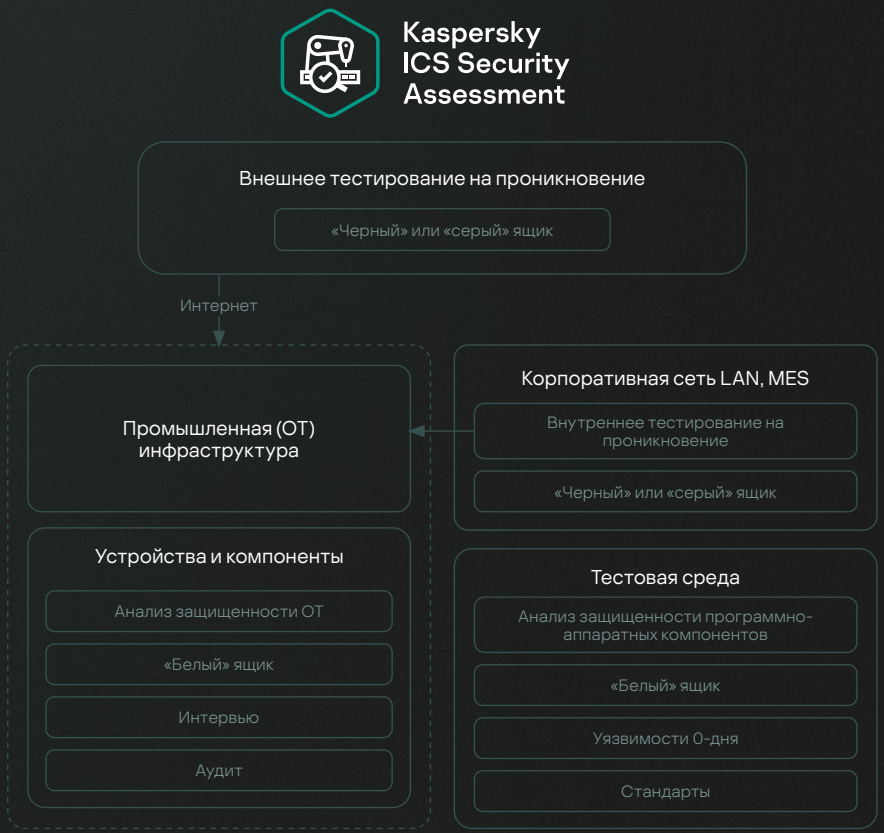
Проверка критических компонентов

Сетевой трафик, в том числе в промышленных протоколах

Компоненты АСУ ТП: SCADA, ПЛК, интеллектуальные счетчики и др.

Физическое оборудование АСУ ТП

Сетевая архитектура, включая сети АСУ ТП



О продукте

Обзор

Связаться

Kaspersky Managed Detection and Response

Непрерывный поиск, обнаружение и устранение угроз, направленных на промышленное предприятие

Ключевые особенности

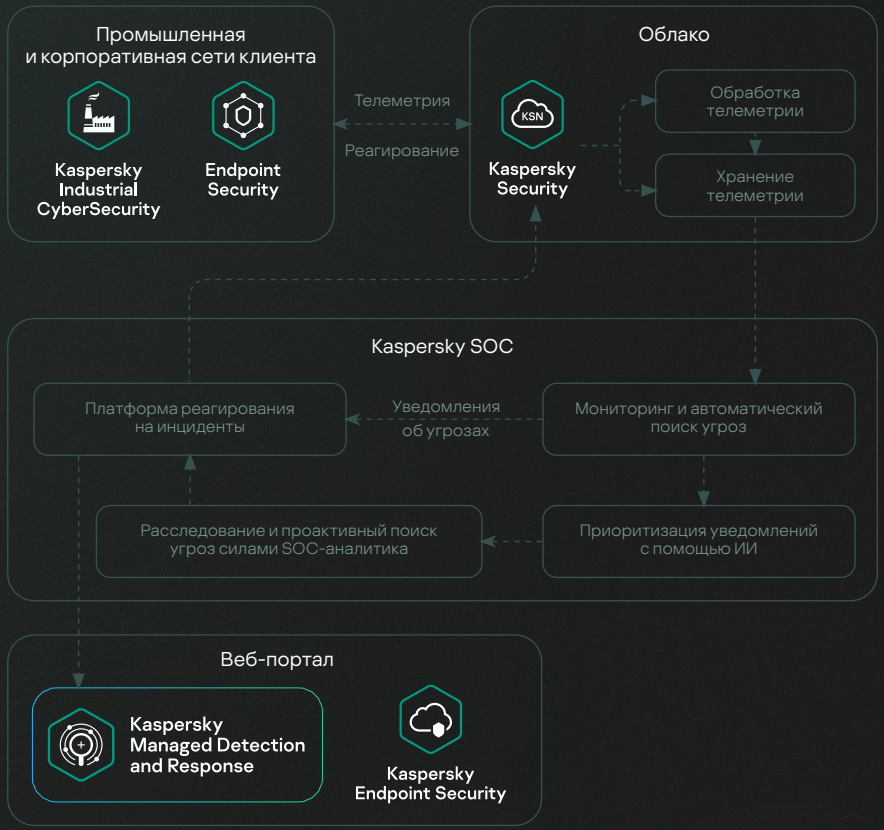
Проактивный поиск угроз: запатентованные индикаторы атак помогают отследить незаметные угрозы в АСУ ТП

Сокращение расходов на безопасность из-за отсутствия необходимости нанимать новых ИБ-специалистов

Знания и опыт экспертов в кибербезопасности АСУ ТП: поддержка от опытной команды по активному поиску угроз

Возможность пользоваться ключевыми преимуществами центра SOC, не имея его внутри предприятия

Автоматизированное и управляемое реагирование: полностью управляемые инструменты для предотвращения и сдерживания угроз в АСУ ТП



О продукте

Обзор

Связаться

Реагирование на инциденты

Риск

Одной уязвимости достаточно, чтобы киберпреступники смогли получить контроль над промышленными системами

Решение

- Быстрая ликвидация последствий инцидента
- Анализ причин, источников и последствий инцидента
- Подробное представление о вредоносном ПО
- Поддержка командой экспертов ICS CERT

Kaspersky
Incident Response

Состав сервиса

Реагирование на инциденты: расследование, ликвидация угрозы безопасности

Цифровая криминалистика: анализ цифровых улик

Анализ вредоносного ПО: подробное представление об использованных в атаке файлах

О продукте | Обзор | Связаться

Кибераптечка для промышленных организаций

Безопасность объектов КИИ каждый день испытывают на прочность все большее количество атакующих. Чтобы не потерять контроль над собственной инфраструктурой, важно оценить текущий уровень защищенности

Kaspersky
Industrial
Emergency Kit

Фронт работ на 3 месяца

Оценить текущий уровень защищенности АСУ ТП

Повысить осведомленность сотрудников в области промышленной кибербезопасности

Получить рекомендации экспертов «Лаборатории Касперского», как усилить информационную безопасность промышленной инфраструктуры

Сократить количество потенциальных векторов атаки и рисков ИБ для организации благодаря предоставленной аналитике об угрозах

О продукте | Обзор | Связаться

Партнер, которому можно доверять

Глобальное присутствие, опыт и знания мирового уровня

Высокий статус в индустрии безопасности IT-/OT-систем

Более 80 сертификатов о совместимости с решениями вендоров АСУ ТП

Доказанная эффективность технологий и соответствие стандартам

ICS CERT

Собственное международное подразделение ICS CERT

Клиенты по всему миру

РОСАТОМ, НОРНИКЕЛЬ, Северсталь, KAMAZ, TATNEFT, РОССЕТИ, НЛМК, alperia, PacificLight, КазМунайГаз

Kaspersky OT CyberSecurity

Подробнее

А также предлагаем единый подход
для комплексной безопасности бизнеса

Kaspersky Symphony

Подробнее

Получите консультацию по продуктам и сервисам,
коммерческое предложение, бесплатное демо

Получить консультацию

www.kaspersky.ru