



Kaspersky Unified Monitoring and Analysis Platform

Создавая безопасность

Более 20 лет практического опыта «Лаборатории Касперского» в области создания средств защиты информации, противодействия целевым атакам и анализа вредоносного ПО легли в основу решения Kaspersky Unified Monitoring and Analysis Platform.

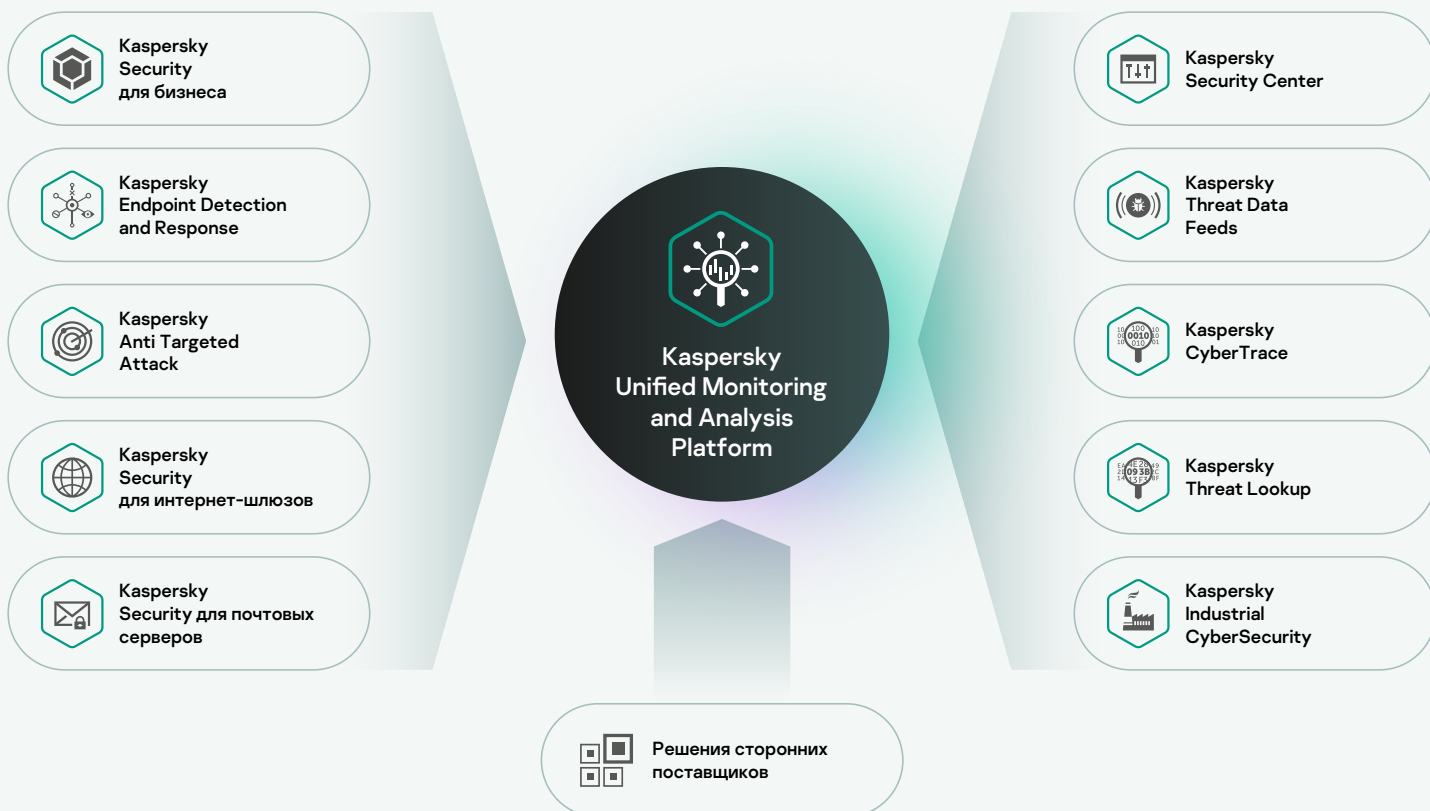
Единая консоль мониторинга и анализа инцидентов ИБ

Центральный элемент единой платформы безопасности

Надежная защита данных, безопасность ИТ-инфраструктуры, в том числе критической информационной инфраструктуры (КИИ), стабильность бизнес-процессов и соблюдение требований законодательства — обязательные условия устойчивого развития современного бизнеса. Чтобы выполнить эти условия, недостаточно просто установить защитные решения — необходимо обладать всей полнотой информации о состоянии безопасности комплексной ИТ-инфраструктуры и подготовить инструменты для своевременного выявления и нейтрализации возможных угроз.

Разрозненные и неинтегрированные средства защиты малоэффективны против хорошо скоординированных современных атак в условиях сложной инфраструктуры. «Лаборатория Касперского» предлагает решение **Kaspersky Unified Monitoring and Analysis Platform (KUMA)** — один из ключевых компонентов на пути к реализации единой платформы кибербезопасности. Решение обеспечивает гибкий комплексный подход к противодействию сложным угрозам и целевым атакам, помогает обеспечить соответствие требованиям внешних регулирующих органов и готово встроиться в существующую ИТ- и ИБ-инфраструктуру.

Kaspersky Unified Monitoring and Analysis Platform — это решение класса SIEM (Security Information and Event Management), предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации. Решение предоставляет единую консоль мониторинга, анализа и расследования инцидентов ИБ, объединяя как решения «Лаборатории Касперского», так и сторонних производителей.



Ключевые преимущества Kaspersky Unified Monitoring and Analysis Platform

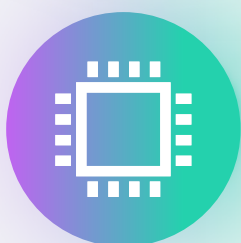
1



Масштабируемая архитектура и низкие системные требования

Решение разработано для работы в современных динамично изменяющихся и высоконагруженных ИТ-средах. Модульная микросервисная архитектура решения позволяет легко изменять конфигурацию системы, обеспечивая масштабируемость, отказоустойчивость и гибкость вариантов развертывания.

2



Высокая производительность

Высокопроизводительный потоковый движок корреляции обеспечивает производительность более 300 тысяч событий в секунду (EPS) на один узел корреляции. Модульная архитектура решения позволяет еще больше увеличить общую производительность за счет балансировки и распределения нагрузки между компонентами.



3



Потоковая корреляция в реальном времени

Kaspersky Unified Monitoring and Analysis Platform обеспечивает централизованный сбор и анализ журналов регистрации, корреляцию событий ИБ в реальном времени и своевременное оповещение об инцидентах.

4



Автоматический сбор информации о конечных точках и реагирование

Автоматический сбор инвентаризационной информации (установленное ПО, уязвимости, оборудование, владелец актива, и т. д.) может использоваться для корреляции событий ИБ с учетом контекста, а также при расследовании инцидентов. Управление агентами на рабочих местах помогает в процессе реагирования на выявленные инциденты.

5



Тесное взаимодействие с Kaspersky Threat Intelligence

«Лаборатория Касперского» является одним из лидеров в области сервисов оперативного информирования о киберугрозах. Решение Kaspersky Unified Monitoring and Analysis Platform тесно интегрировано с богатым портфолио сервисов Kaspersky Threat Intelligence что позволяет выявлять и приоритизировать угрозы и в один клик получать доступ к контекстной информации по новым атакам, индикаторам компрометации, тактикам и техникам злоумышленников.

6



Обеспечение соответствия требованиям регуляторов: интегрированный модуль ГосСОПКА

Решение помогает организациям соответствовать действующему законодательству РФ в сфере безопасности объектов КИИ. В частности, оно позволяет выполнить требования в части обнаружения, предупреждения и ликвидации последствий атак, информирования о компьютерных инцидентах, а также установления причин и условий их возникновения. Встроенный модуль ГосСОПКА напрямую обменивается данными об инцидентах с НКЦКИ.

Интеграция «из коробки»

Kaspersky Unified Monitoring and Analysis Platform поддерживает встроенную интеграцию со следующими решениями:

Лаборатория Касперского

- Kaspersky Security для бизнеса
- Kaspersky Security Center
- Kaspersky EDR для бизнеса Оптимальный
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack Platform
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace
- Kaspersky Threat Lookup
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Network



Стороннее взаимодействие

- Программное обеспечение с открытым исходным кодом (Unbound, Dovecot, Nginx, Apache, DNS BIND, pfSense (с OpenVPN), Exim, Squid, Postfix и др.)
- Операционные системы (Windows, Linux, FreeBSD)
- Ключевые продукты от различных поставщиков (Microsoft, Palo Alto Networks, Cisco, VMWare, Код безопасности, CheckPoint, R-Vision, Fortinet, Positive Technologies, Infotecs, InfoWatch, Бастион, Huawei, Oracle, MikroTik, Бифит, TrendMicro и др.)
- Другое (Netflow, Kafka, Nats, SQL, TCP, UDP, HTTP, Files, SNMP, WMI)

Благодаря наличию у решения гибкого API, возможна интеграция с широким набором продуктов сторонних поставщиков, в том числе с платформой реагирования на инциденты, системой регистрации и учета заявок, сканером защищенности и многими другими продуктами.

Интеграция с продуктами «Лаборатории Касперского»

Kaspersky Unified Monitoring and Analysis Platform обменивается информацией с решениями и технологиями «Лаборатории Касперского», что позволяет связать установленные у вас продукты «Лаборатории Касперского» в единую систему и сделать их работу еще эффективнее.

Решение

Как связано с KUMA

Kaspersky Security Center

Автоматический сбор инвентаризационной информации: установленное ПО, уязвимости, оборудование, владелец актива, и т. д.

Агрегация оповещений об угрозах, а также управление агентами на рабочих местах для реагирования на выявленные инциденты

Kaspersky Security для бизнеса

Оповещения об угрозах, обнаруженных на рабочих станциях

Kaspersky Endpoint Detection and Response

Централизованный сбор оповещений о продвинутых угрозах и АРТ-атаках на уровне рабочих мест

Kaspersky Anti Targeted Attack

Централизованный сбор оповещений о продвинутых угрозах и АРТ-атаках на уровне сети

Kaspersky Security для интернет-шлюзов

Оповещения об угрозах, обнаруженных веб-шлюзом

Kaspersky Security для почтовых серверов

Оповещения об угрозах, обнаруженных почтовым шлюзом

Kaspersky CyberTrace

Потоковое обогащение событий ИБ контекстом и представление информации в интерфейсе Kaspersky Unified Monitoring and Analysis Platform. Накопление собственных знаний об угрозах, полученных в процессе расследования инцидентов и управление этими знаниями

Kaspersky Threat Lookup

Источник контекстной информации по новым угрозам, индикаторам компрометации, тактикам и техникам злоумышленников, а также доступ к аналитическим отчетам об АРТ-угрозах, об угрозах для финансовых организаций и промышленных предприятий

Kaspersky Industrial CyberSecurity

Оповещения об угрозах, обнаруженных в промышленных технологических сетях

Ценность решения для бизнеса

Объединение в целостную экосистему безопасности интегрированных решений «Лаборатории Касперского» и сторонних производителей

Повышение продуктивности работы ИБ-служб по выявлению, расследованию и реагированию на сложные киберинциденты

Обеспечение помощи в соответствии требованиям внутренних политик безопасности и внешних регулирующих органов (в частности, требованиям ФЗ-187 и приказа ФСТЭК России №239)

Снижение рисков информационной безопасности

Сокращение прямых потерь от целенаправленных действий злоумышленников



**Kaspersky
Unified Monitoring
and Analysis
Platform**

[Узнать больше](#)

www.kaspersky.ru

© 2021 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

