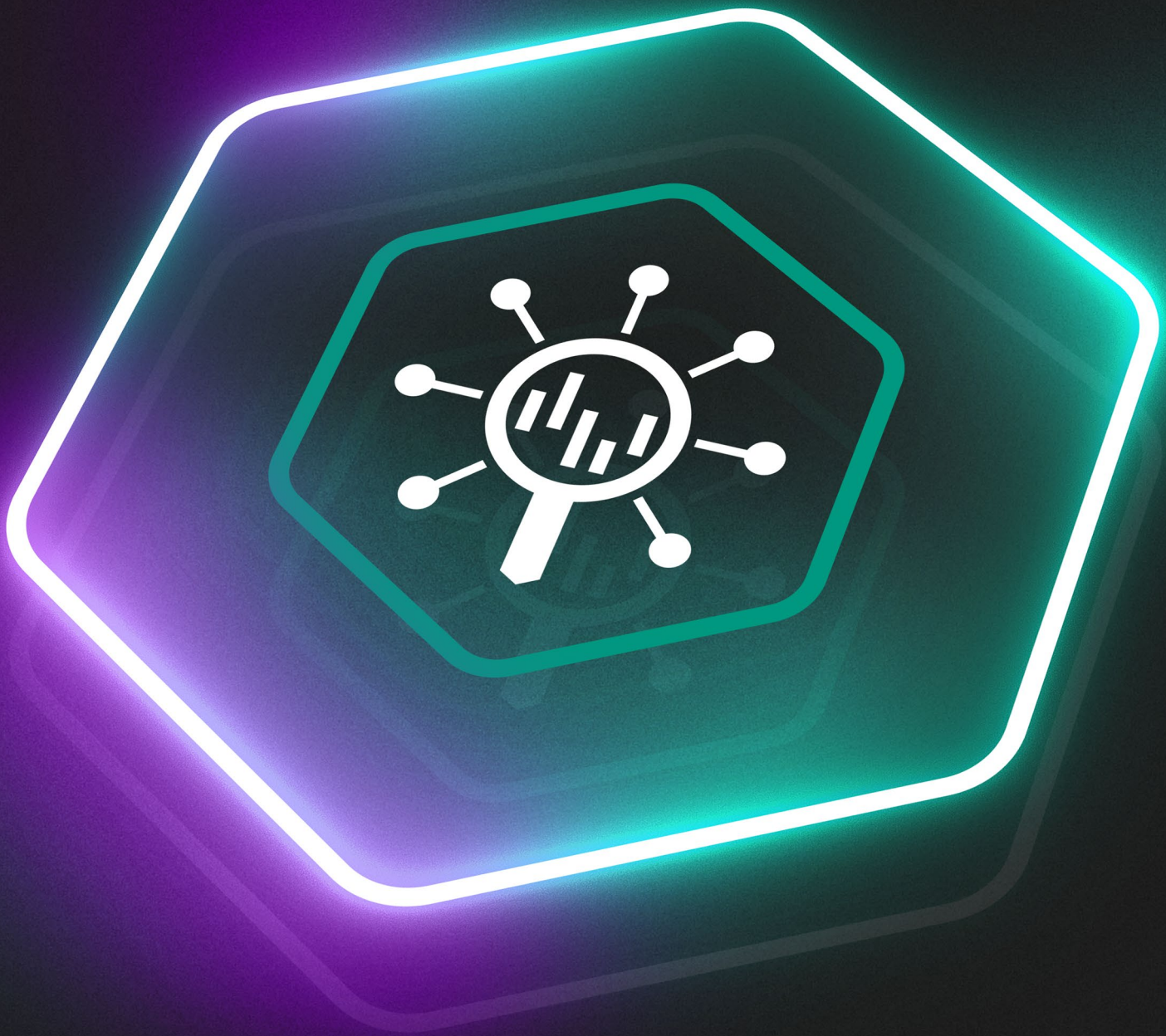


Kaspersky Unified Monitoring and Analysis Platform

kaspersky АКТИВИРУЙ БУДУЩЕЕ

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 Unifed Monitoring and Analysis Platform.

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 событиях информационной безопасности и выстроить экосистему на основе интегрированных между собой технологий.

Разрозненные и неинтегрированные средства защиты малоэффективны против хорошо скоординированных современных атак. «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.

Единая консоль мониторинга и анализа инцидентов ИБ

Ключевые преимущества Kaspersky Unified Monitoring and Analysis Platform

1

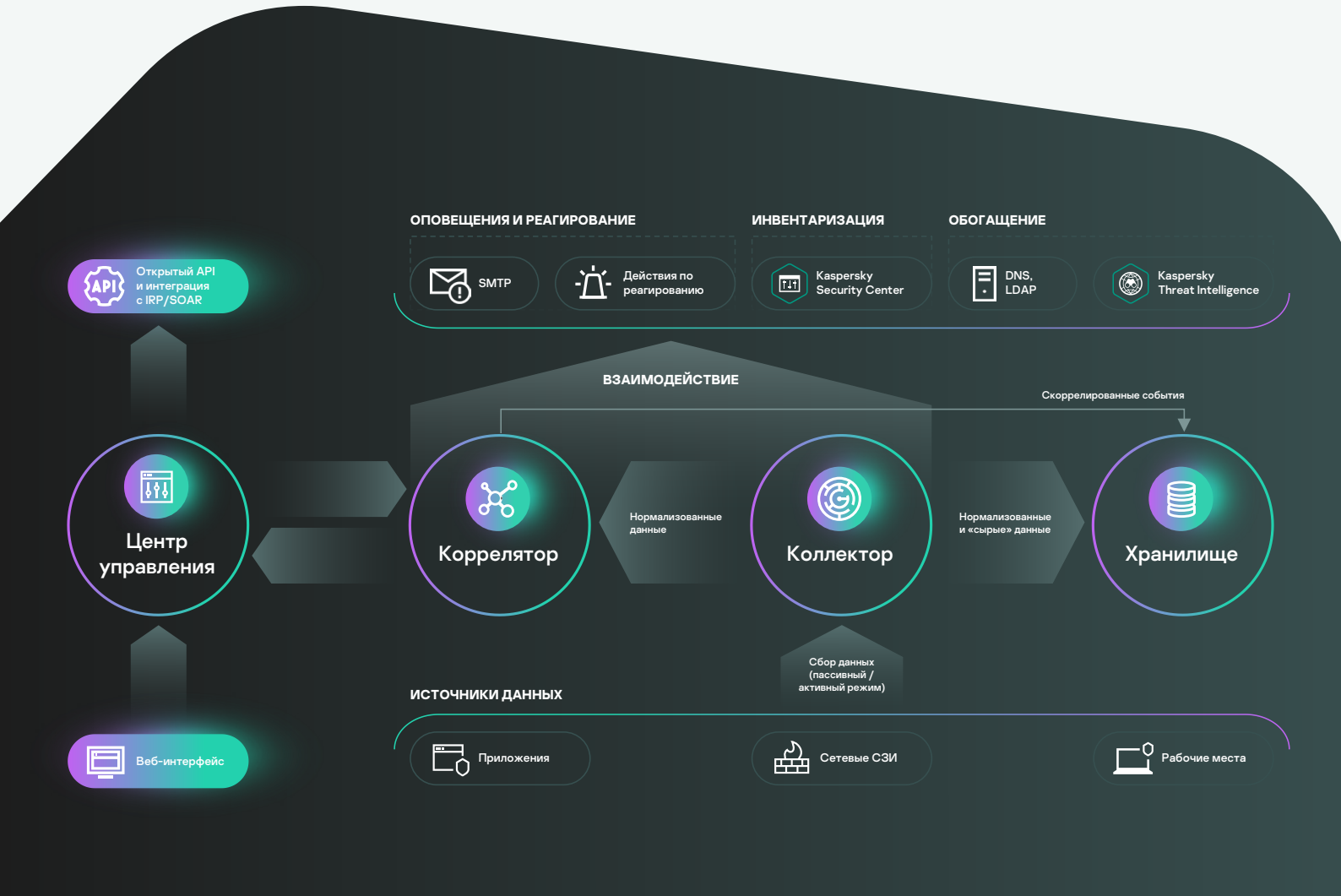
Масштабируемая архитектура и низкие системные требования

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.

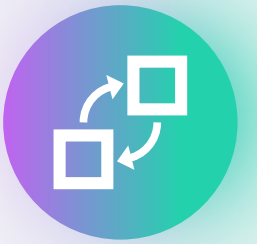
2

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



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

Сторонние поставщики

- Palo Alto NGFW & Panorama
- FortiGate UTM
- FortiAnalyzer
- Windows OS (Windows Event Log)
- CheckPoint IPS, Firewall (CEF)
- Netflow v5/v9/IPFIX (v10)
- Cisco ASA, Cisco IOS (R&S), Cisco WSA
- ViPNetCoordinator 4.x
- Unbound
- Dovecot
- Nginx
- Apache
- DNS BIND
- pfSense (OpenVPN)
- Linux (auth,rights, owner,FW)
- FreeBSD (auth,rights, owner,FW)
- Microsoft DNS, Microsoft DHCP
- BIFIT Mitigator (CEF)
- R-Vision Incident Response Platform

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

4

Автоматический сбор информации о конечных точках

Одна из самых актуальных проблем при расследовании инцидентов – недостаток контекста и информации об информационных активах организации. Автоматизированное обнаружение и инвентаризация хостов в сети позволяет решить эту проблему. С помощью агента Kaspersky Endpoint Security в автоматизированном режиме получает полную информацию о конечных точках (в том числе сведения об уязвимостях на рабочих станциях), а также любых изменениях, произошедших с ними. Данная информация может использоваться для корреляции событий ИБ с учетом контекста, а также при расследовании инцидентов.

5

Тесное взаимодействие с Kaspersky Threat Intelligence

«Лаборатория Касперского» обладает одной из наиболее полных и достоверных баз данных об угрозах Threat Intelligence. Kaspersky Unified Monitoring and Analysis Platform тесно интегрирован с платформой Kaspersky CyberTrace для автоматического обогащения данными Threat Intelligence, а также с Kaspersky Threat Lookup для расследования инцидентов и анализа угроз.

6

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.

7

Обеспечение соответствия требованиям регуляторов

Решение помогает организациям соответствовать действующему законодательству РФ в сфере безопасности объектов КИИ. Оно позволяет выполнить требования в части обнаружения, предупреждения и ликвидации последствий атак, информирования о компьютерных инцидентах, а также установления причин и условий их возникновения.

8

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 APT-атаках на уровне рабочих мест
Kaspersky Anti Targeted Attack	Централизованный сбор оповещений о продвинутых угрозах и APT-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 APT-угрозах, об угрозах для финансовых организаций и промышленных предприятий
Kaspersky Industrial CyberSecurity	Оповещения об угрозах, обнаруженных в индустриальных технологических сетях

Ценность решения для бизнеса

- Предоставляет возможность построить экосистему безопасности на основе интегрированных продуктов «Лаборатории Касперского»
- 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 закона 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