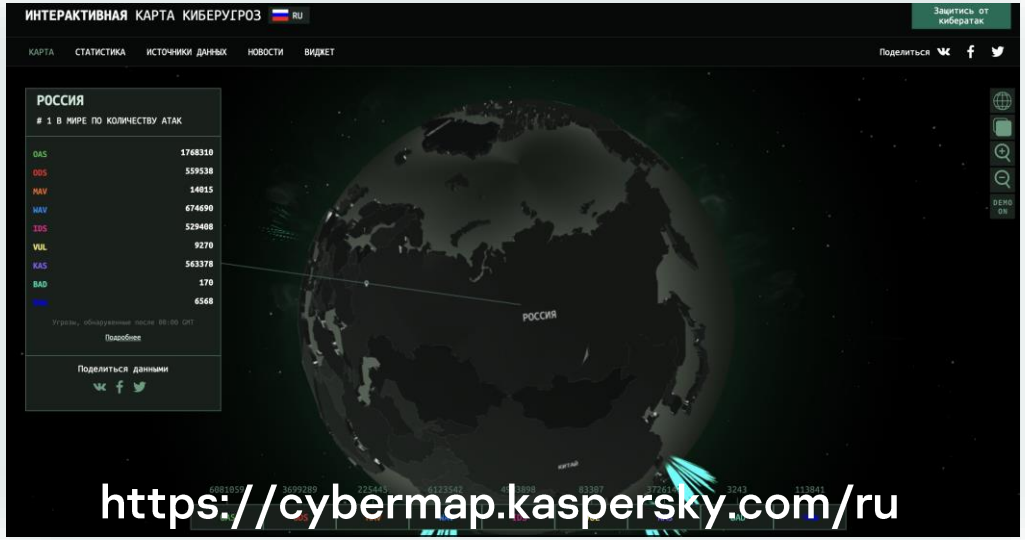
Киберзащита бизнеса в России: как обеспечить стабильность бизнеса в новых условиях

kaspersky

Новая реальность

- Неопределенность
- Больше рисков
- Поиск решения



Усложнение атак

Количество киберинцидентов в российских компаниях увеличилось в 4 раза (Q1 2021 vs Q12022)*

Киберагрессия

Россия номер 1 в мире по количеству атак

Срочное замещение

Ряд различных защитных ИБ-решений становятся менее эффективными, риски пропустить сложную кибератаку значительно повышаются

*По данным центра реагирования на инциденты «Лаборатории Касперского»

Каждодневные информационные новости

Fortinet® (NASDAQ: FTNT), мировой лидер в области комплексных, интегрированных и автоматизированных решений в области кибербезопасности, объявила сегодня о прекращении операций в России. Компания остановила все продажи, поддержку и профессиональные услуги Fortinet. Fortinet продолжает следовать всем протоколам безопасности, а также законам и рекомендациям правительства США и других стран.

Cisco ушла из России. Будущее ее устройств под угрозой

Американская корпорация Cisco прекращает поставки своей продукции в Россию и Белоруссию. Остановлена также работа сервиса Webex и Сетевой академии Cisco. Работоспособность уже приобретенных устройств, требующих подписку, под вопросом.

Из России сбежала Microsoft. Россияне остались без Windows, MS Office и Azure

Microsoft свернула все операции в России на неопределенный срок, сославшись на американские санкции против России из-за ситуации на Украине. Россияне лишатся доступа к ее облачным сервисам, а также, возможно, к игровым приставкам и обновлениям Windows и Office.

Защита от массовых угроз

В первую очередь, необходимо обратить внимание на замещение решений на базе превентивных технологий, которые стоят на передовой защиты (узлы, почта, сеть)

Защита от сложных угроз

Во вторую очередь, обратить внимание на замещение продвинутых технологий противодействия сложным атакам (EDR, SIEM, NTA, Anti-APT, Sandbox, XDR и пр.)

Управляемая защита MDR

Оперативно разворачиваемая управляемая защита от «Лаборатории Касперского» для тех, кто не располагает временем на осознанный выбор необходимых ИБ решений

Превентивные средства защиты

Антивирус для корпоративной сети

Решение	Статус
TrendMicro Apex One (Япония)	
ESET Protect (Словакия)	
Symantec Endpoint Protection (США)	
Microsoft Defender (США)	
McAfee Endpoint Security (США)	

Ключевые возможности

Основа любой системы ИБ для компаний любой величины и сферы деятельности для автоматического отражения массовых киберугроз.

- Огромное количество компонентов защиты в одном исполнении для разных платформ и операционных систем;
- Уникальные технологии по оперативному выявлению и блокированию шифровальщиков
- Инструменты контроля для управления доступом к приложениям, ресурсам сети Интернет или подключенным устройствам
- Встроенные средства по поиску и закрытию уязвимостей ОС и приложений сторонних вендоров
- Инструменты системного администрирования для автоматизации развертывания приложений и операционных систем
- Поддержка частичного и полнодискового шифрований , управление встроенными в операционную систему функциями шифрования
- Полная поддержка функционирования системы на отечественных ОС и базах данных

Антивирусная защита виртуальных сред и облаков

Решение	Статус
Trend Micro Hybrid Cloud Security (Япония)	
McAfee MOVE AntiVirus (США)	
Eset Virtualization Security (Словакия)	

Легкий агент и защита без агента

Light Agent

- Поддержка всех самых популярных гипервизоров
- Облегченный агент добавляет критичные возможности безопасности, сохраняя высокую плотность виртуальных машин
- Веб-контроль, Контроль устройств и приложений на основе политик
- Анализ поведения и защита от эксплойтов

Agentless

- Тесно интегрируется с VMware NSX Vsphere и vShield
- Отсутствие дублирования, сохранение коэффициентов консолидации и высокой плотности виртуальных машин
- Простота администрирования и развертывания для мгновенной защиты и безопасности

Ключевые возможности

Помогает эффективно защищать виртуальные и облачные среды, позволяет управлять IT-инфраструктурой и обеспечивает ее прозрачность, не влияя на производительность системы и не мешая работе пользователей.

- Несколько вариантов исполнения, включая как безагентную защиту, так и на базе сверхлегкого агента
- Поддержка большого количества производителей сред виртуализация, включая платформы отечественного рынка
- Поддержка защиты гостевых систем на базе Windows, Linux, а также отечественных ОС
- Высокий уровень оптимизации затрат ресурсов гипервизоров в пользу работы бизнес-задач клиента.
- Гибкая схема лицензирования решения по CPU, ядрам или защищаемым ОС
- Наличие государственных сертификации

Антивирусная защита промышленных сетей

Решение	Статус
Trend Micro Industrial Endpoint Security (Япония)	
McAfee Endpoint Security (США)	
Symantec endpoint Protection (США)	

Ключевые возможности

Создано специально для защиты промышленной инфраструктуры организации от киберугроз, предназначено для защиты промышленных панелей оператора, рабочих станций и серверов.

- Незначительное влияние на защищаемое устройство за счет минимального потребления ресурсов и модульной архитектуры решения
- Контроли целостности ПЛК и файлов SCADA
- Расширенная защита от вредоносного ПО: шифровальщиков, эксплойтов, руткитов и т.д. Встроенные средства анализа журналов и управления сетевым экраном.
- Инструменты контроля для управления доступом к приложениям, подключенным устройствам и Wi-Fi сетям
- Высокий уровень совместимости с решениями вендоров АСУ-ТП, подтвержденный наличием сертификатов совместимости после совместных испытаний
- Поддержка Windows, Linux, включая устаревшие ОС на низкопроизводительном оборудовании.
- Наличие государственной сертификации

Защита веб-трафика

Решение	Статус
Checkpoint Secure Web Gateway (Израиль)	
Fortinet FortiGate (США)	
Cisco WSA (США)	
ForcePoint Web Security - Websense (США)	
Kerio Control (США)	
TrendMicro Web Security (Япония)	
Symantec BlueCoat (США)	

Ключевые ВОЗМОЖНОСТИ

Корпоративный шлюз Web безопасности с расширенными средствами анализа и защиты, предлагает средства антивирусной защиты, динамического анализа веб страниц и мощный категоризатор веб ресурсов

- Продвинутые технологии антивирусной защиты (AM-движок, интеграция с KATA)
- Инспекция SSL трафика
- URL/IP репутация
- Контроль доступа к Web-ресурсам, предопределенные списки категорий
- Анализ контента, обнаружение вредоносных скриптов
- Настройки доступа для приложений (по user агенту)

- Поддержка работы в кластере
- Несколько вариантов развертывания (готовый Virtual Appliance или интеграция с существующим Proxy)
- Ролевая модель доступа к элементам управления
- Разделение на рабочие области

Защита почтового трафика

Решение	Статус
Fortinet FortiMail (США)	
Cisco IronPort (США)	
Barracuda Email Security Gateway (США)	
TrendMicro Email Security (Япония)	

Ключевые возможности

Kaspersky Security для почтовых серверов защищает корпоративную почту от вредоносного ПО, программ-вымогателей, спама, фишинга и BEC-атак

- Продвинутые технологии блокирования вредоносных объектов (интеграция с KATA)
- Защита от фишинга, спама и компрометации корпоративной электронной почты
- Фильтрация почтовых вложений
- Предотвращение попыток обмануть пользователей с помощью методов социальной инженерии
- Соответствие требованиям регуляторов, поддержка отечественных ОС (KLMS)

Релиз KSMG 2.0

- Кластерная архитектура для масштабирования решения
- Ролевое разграничение прав доступа, интеграция с AD;
- Централизованный поиск по хранилищу событий;
- Усилены технологии детектирования (IP-репутация, look-like, выявление спуфинговых атак и т.д.)

Продвинутые решения выявления сложных угроз

Endpoint Detection and Response (EDR)

Решение	Статус
Cisco AMP (США)	
Microsoft ATP (США)	
PaloAlto EDR (США)	
Fortinet FortiEDR (США)	
TrendMicro Apex One (Япония)	
Checkpoint Sandblast Agent (Израиль)	

Ключевые возможности

Решение класса EDR экспертного уровня для обнаружения, расследования и реагирования на сложные угрозы и целевые атаки на уровне конечных точек (защищаемых устройств)

- Продвинутые технологии обнаружения (AM-движок, Sandbox, IoC, IoA)
- Обновляемые правила автоматического детектирования на основе MITRE
- Автоматизированный и ручной поиск угроз (Threat hunting)
- Автоматическое и ручное реагирование (Response) на защищаемых устройствах (изоляция устройств, остановка процессов, изъятие объекта и др)
- API для реагирования из сторонних систем
- Дополнение NDR-решений до класса XDR (защитой уровня конечных точек (EDR))
- Поддержка Windows и Linux систем, включая отечественные ОС.
- Интеграция с антивирусным решением для обмена информацией и кросс-сценариев.

Защита от целенаправленных атак (NTA, Sandbox, AntiAPT)

Решение	Статус
Checkpoint Sandblast (Израиль)	
Cisco Sandbox (США)	
FireEye NX, EX, FX (США)	
PaloAlto WeldFire (США)	
TrendMicro Deep Discovery Inspector (Япония)	
Fortinet FortiSandbox (США)	

Kaspersky Anti Targeted Attack (KATA)

Ключевые возможности

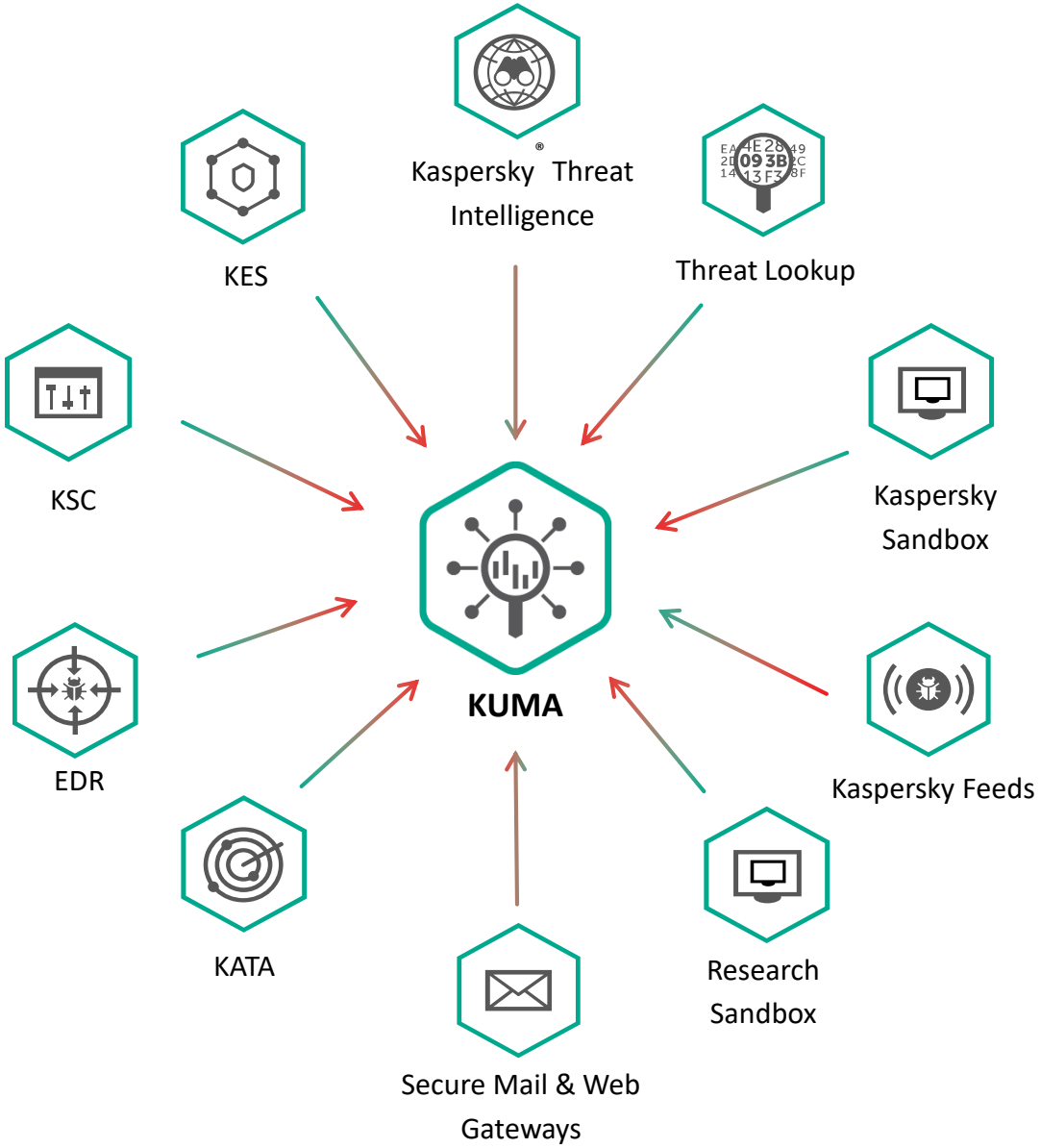
Решение класса NTA/NDR для обнаружения, расследования и реагирования на сложные угрозы и целевые атаки на уровне сети

- Различные варианты интеграции в инфраструктуру (inline, mirror)
- Быстрое масштабирование, поддержка различных схем развертывания
- Продвинутые технологии обнаружения на уровне сети (AM-движок, IDS Sandbox)
- Встроенный инструментарий для написания своих собственных правил обнаружения(Yara, IDS)
- Автоматическое и ручное реагирование (Response) на веб и почтовых шлюзах (интеграция с KSMG и KWTS)
- Получение по API объектов на проверку из сторонних систем
- Дополнение EDR-решений до класса XDR (защитой уровня сети (NDR))

Security information and event management (SIEM)

Решение	Статус
IBM Qradar (США)	
Fortinet FortiSIEM (США)	
MicroFocus ArcSight ESM (США)	
ELK	

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Производительность
300k+ EPS на одну ноду

Низкие системные требования

Гибкая архитектура
Современная микросервисная архитектура

Интеграция «из коробки»
С решениями «Лаборатории Касперского» и сторонних поставщиков

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

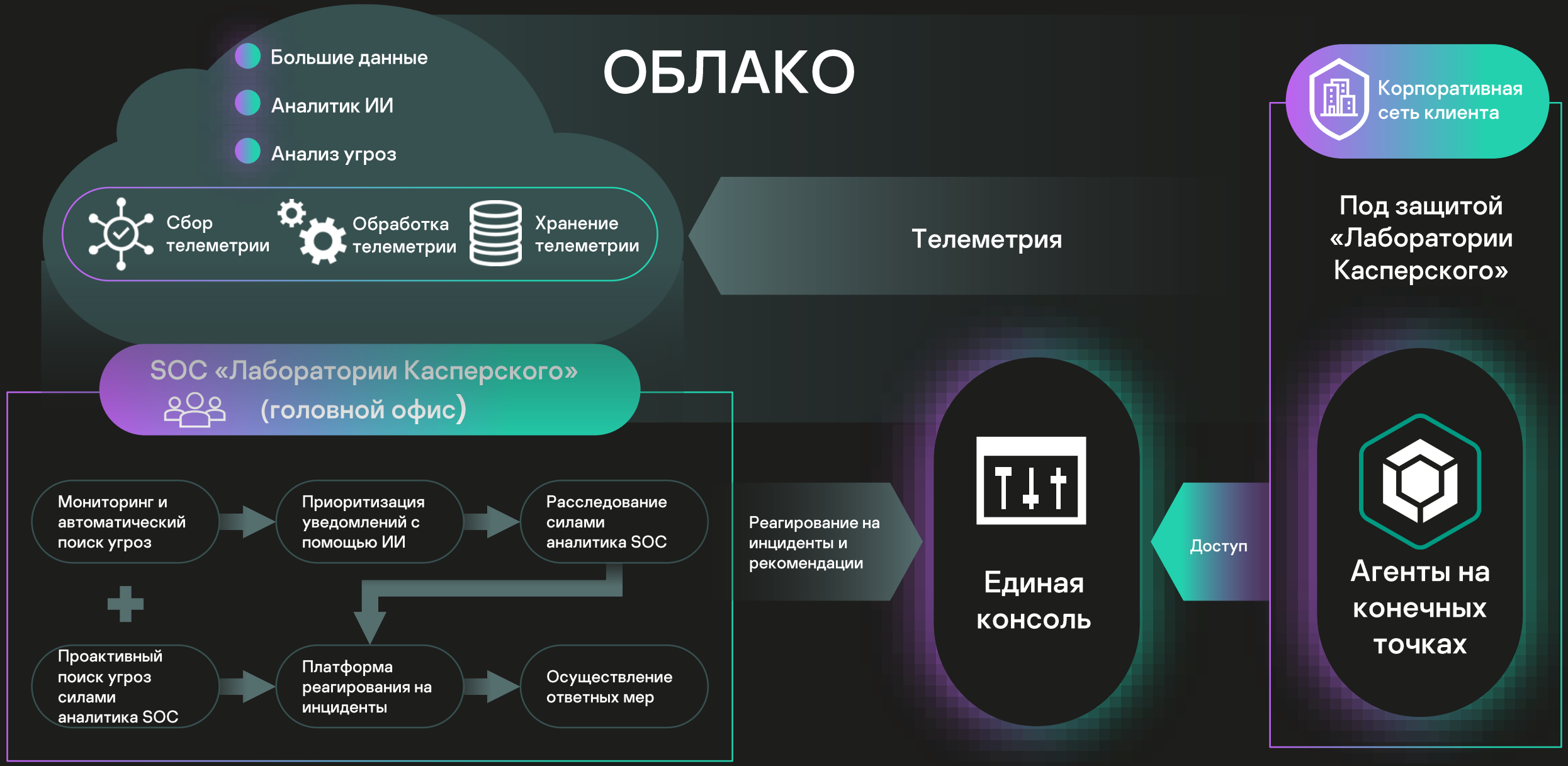
Ключевые ВОЗМОЖНОСТИ

KUMA SIEM - это центральный элемент единой платформы безопасности от «Лаборатории Касперского», который взаимодействует как с решениями ЛК, так и с разработками сторонних поставщиков.

- Ситуационная осведомлённость и аналитика - дашборды и отчёты по актуальному состоянию ИБ для отслеживания трендов (C-level) и операционной работы по поиску аномалий
- Мониторинг безопасности - непрерывная корреляция потока событий от источников для выявления инцидентов ИБ
- Реагирование на инциденты - единая консоль позволяет обогатить карточки инцидентов дополнительной информацией (по индикаторам компрометации, активам, пользователям) и запустить задачи реагирования через KES, EDR, ASAP и другие решения
- Проактивный поиск угроз - быстрый поиск ClickHouse по всей собранной информации с использованием возможностей SQL-запросов или применение ретроспективной корреляции для выявления подозрительных цепочек событий
- Соответствие требованиям - KUMA имеет сертификат ФСТЭК, свидетельство о регистрации, включена в реестр отечественного ПО и позволяет выполнять требования 187-ФЗ, приказа ФСТЭК России № 239, рекомендаций ЦБ и других НПА.
- Поддержка отечественной ОС (Astra Linux)

Kaspersky MDR

Kaspersky Managed Detection and Response



Мигрируй

https://migration.kaspersky.ru/