«Инфозонт» внедряет Kaspersky Smart для защиты объектов КИИ в сегменте среднего и малого бизнеса

Использование Kaspersky Smart позволяет вывести защиту информационных систем в сегменте SMB на новый уровень за счёт использования более продвинутых инструментов обнаружения кибератак и реагирвоания на них, по сравнению с традиционными решениями для защиты рабочих устройств.

kaspersky

ИнфоЗонт

Предыстория

Компания «Инфозонт» — российский поставщик решений в области информационной безопасности, основанный в 2017 году. Головной офис «Инфозонта» расположен в Иннополисе (Республика Татарстан), а география бизнес-деятельности охватывает весь Приволжский федеральный округ. В команде работает около 50 специалистов, имеющих опыт в построении систем ИБ для высоконагруженных ИТ-сред и критически важных инфраструктур.

Основной фокус деятельности — услуги для организаций среднего и малого бизнеса в области защиты критической информационной инфраструктуры и цифровых систем от киберугроз. Компания разрабатывает собственные технологии для мониторинга, анализа и реагирования на инциденты ИБ, а также оказывает услуги по консалтингу, аудиту и поставке сторонних решений в области ИБ.

Компании сегмента SMB работают в условиях высоких киберрисков, актуальным остается весь ландшафт киберугроз: скам, использование социальной инженерии, фишинг, шифровальщики. При этом одно предприятие в случае пропущенной кибератаки теряет в среднем более 5 млн рублей.

Для комплексной защиты информационных систем от сложных кибератак в сегменте SMB компания «Инфозонт» использует решение Kaspersky Smart, систему мониторинга событий информационной безопасности с возможностями реагирования и обнаружения на уровне конечных точек.

Kaspersky Smart

Решение

Kaspersky Smart — линейка решений для умной защиты среднего бизнеса. Она делает экспертные инструменты доступными для небольших организаций (250–1000 рабочих мест) и открывает новые возможности для киберзащиты. Технологии SIEM и EDR в составе решений содержат множество автоматизированных функций и предоставляют отделу ИБ всю необходимую информацию для отражения самых сложных и актуальных кибератак. Решения из линейки Kaspersky Smart легко интегрируются с существующими информационными системами и другими защитными средствами, а также помогают соответствовать растущим требованиям регуляторов.

Преимущества Kaspersky Smart

- **Уникальный стек** технологий экспертного уровня.
- **Минимальные требования** к аппаратным мощностям и возможность установки на виртуальные машины.
- **Интеграция «из коробки»** с распространёнными источниками данных и ИТ-системами.
- **Соответствует** многим **регуляторным требованиям.**
- **Подойдёт компаниям с критической инфраструктурой** и чувствительными данными.

Ключевые особенности

Kaspersky Smart I — SIEM

Помогает осуществлять комплексный мониторинг и потоковую корреляцию событий ИБ из различных источников данных по всей инфраструктуре. Это позволяет оперативно обнаруживать даже сложные угрозы и предпринимать базовые действия по реагированию. А благодаря централизованному хранению данных решение имеет сертификаты соответствия требованиям регулирующих органов.

Kaspersky Smart II — SIEM + EDR

Помимо SIEM содержит технологию класса EDR, которая открывает возможность проактивного обнаружения сложных угроз на уровне хостов, автоматизированного реагирования на них, а также обеспечивает полную видимость для анализа первопричин и расследования инцидентов.

Возможности Kaspersky Smart

Kaspersky Smart	Smart I	Smart II
Технологии	SIEM	SIEM и EDR
Комплексный мониторинг и корреляция событий ИБ	•	•
Базовые действия по реагированию	•	•
Готовая интеграция с распространёнными источниками данных	•	•
Помощь в соответствии требованиям регуляторов	•	•
Контроль и визуализация происходящего на уровне конечных точек		•
Передовое обнаружение и расследование сложных угроз		•
Расширенные действия по реагированию на хостах		•

Соответствие решения требованиям регуляторов

- Входит в реестр отечественного ПО Минцифры России.
- Сертифицировано ФСТЭК России.
- Соответствует требованиям приказов № 17, 21, 239 ФСТЭК России.
- Соответствует требованиям приказа № 196 ФСБ России.
- Позволяет реализовать меры ГОСТ Р 57580.1-2017.
- Помогает во взаимодействии с НКЦКИ — даёт возможность получения и отправки данных об инцидентах.

Результат

Благодаря Kaspersky Smart «Инфозонт» помогает небольшим компаниям выстраивать комплексные системы защиты продвинутого уровня. В пользу выбора решения «Лаборатории Касперского» говорят такие преимущества, как низкие системные требования, единый удобный интерфейс, высокий уровень поддержки, глубокая экспертиза вендора и достаточный экспертный опыт в применении SIEM-технологий, низкий порог входа для клиента.

«Мы остановились на линейке Kaspersky Smart, так как она помогает соответствовать требованиям регуляторов и подходит тем компаниям, которые работают с КИИ или персональными данными. Кроме того, на выбор повлияла репутация «Лаборатории Касперского» как надёжного вендора по ИБ-решениям, с которым мы работаем с 2017 года и продолжаем пилотировать новые решения».

Тимур Назмутдинов

генеральный директор ООО «Инфозонт»

«Компании среднего размера по большей части уже обладают фундаментальной защитой на уровне конечных устройств и задумываются о защите от сложных атак. Востребованность систем анализа и управления ИБ-событиями, а также EDR-решений растёт, поскольку с усложнением ландшафта киберугроз возникает необходимость реагировать на инциденты быстрее, качественнее, с меньшими усилиями. Линейка Kaspersky Smart делает доступным для среднего бизнеса комплексный продукт уровня enterprise и помогает соответствовать требованиям законодательства».

Анна Кулашова

вице-президент «Лаборатории Касперского» по развитию бизнеса в России и странах СНГ