Kaspersky Security System

Современные информационные системы, зачастую управляющие жизненно важными, а иногда и критическими объектами инфраструктуры, подвержены большому количеству различных киберугроз. Нередко информационную защиту таких систем обеспечивают средства, не отвечающие актуальным требованиям по безопасности. Как правило, это сторонние решения, которые добавляются к системе, но не интегрируются с ней в полной мере. Их применение не всегда дает приемлемый результат, так как они не позволяют описать соответствующую индивидуальным требованиям конкретной системы политику безопасности и принять все меры для ее надежной реализации.

История создания

В рамках своей глобальной инициативы «Лаборатория Касперского» разрабатывает комплекс решений для защиты критически важных объектов инфраструктуры. Одним из таких решений стала KasperskyOS — безопасная операционная система. KasperskyOS создавалась с учетом мировых практик и стандартов безопасности, которые позволяют гарантировать конфиденциальность и целостность данных.

Kaspersky Security System разрабатывалась как один из основных компонентов KasperskyOS, реализующий возможность применения в операционной системе различных моделей обеспечения безопасности. Однако в процессе разработки стало понятно, что Kaspersky Security System можно использовать не только в рамках KasperskyOS, но и как основу безопасности других информационных систем. Так платформа была выделена в самостоятельный проект и стала доступна для защиты других информационных систем с повышенными требованиями к безопасности.

Текущая реализация

Платформа Kaspersky Security System представлена в виде OEM-компонента.

Именно необходимостью создания интегрируемого решения обусловлена разработка Kaspersky Security System — инновационной платформы, предназначенной для защиты различных информационных систем с повышенными требованиями к безопасности, примерами которых могут служить:

- Корпоративные информационные системы
- Информационные системы специального назначения
- Интернет вещей
- Интеллектуальные сети распределения и генерации электроэнергии
- Системы управления технологическими процессами
- Системы управления критически важными объектами инфраструктуры
- Системы управления транспортом

Преимущества

- В основу Kaspersky Security System заложен принцип изоляции компонента безопасности от функциональных компонентов информационной системы. Это **обеспечивает безопасную работу системы независимо от того, как реализованы ее функциональные компоненты, что позволяет строить доверенные системы из недоверенных компонентов**. Политика безопасности при этом может быть скорректирована без изменения функциональных компонентов.
- Kaspersky Security System дает возможность комбинировать разные модели безопасности – например, сочетая базовые и специализированные политики.
- При соблюдении определенных условий Kaspersky Security System может использоваться в информационных системах, работающих в режиме реального времени.
- Архитектура Kaspersky Security System обеспечивает реализацию правил безопасности в соответствии с индивидуальными требованиями конкретной информационной системы без необходимости поддерживать ненужные клиенту механизмы и сложные конфигурации.

Целевая аудитория

- Производители программно-аппаратного обеспечения
- Системные интеграторы
- Разработчики операционных систем и программного обеспечения специального назначения

Процесс внедрения

Интеграция Kaspersky Security System осуществляется в два этапа и сопровождается набором специализированных сервисов.

Этап №1. Предпроектная подготовка
1. Анализ информационной системы
2. Выработка рекомендаций по адаптации Kaspersky Security System под архитектуру информационной системы
3. Формирование политик обеспечения безопасности

Этап №2. Внедрение
4. Интегрирование Kaspersky Security System в информационную систему
5. Внедрение ранее сформированных политик безопасности

Совместимость

В настоящее время платформа Kaspersky Security System доступна для информационных систем на базе[1]:

- KasperskyOS[2]
- Linux

Сопроводительная документация

Включает набор архитектурных шаблонов и рекомендованные практики безопасной разработки программного обеспечения, а также правила использования Kaspersky Security System для достижения высокого уровня безопасности.

Патенты

Технологии, на основе которых разработана платформа Kaspersky Security System, защищены рядом патентов:

US 7386885 B1, US 7730535 B1,
US 8370918 B1, EP 2575318 A1,
US 8522008 B2, US 20130333018 A1,
US 8381282 B1, EP 2575317 A1,
US 8370922 B1, EP 2575319A1,
US 9015797 B1, DE 202014104595 U1.

Основные функции

- Контроль взаимодействия программных компонентов внутри информационной системы, основанный на объединении компонентов в домены с одинаковыми свойствами безопасности
- Описание свойств безопасности для каждого домена и правил взаимодействия между компонентами, принадлежащими к разным доменам
- Классификация ресурсов информационной системы с точки зрения политики безопасности
- Вынесение вердиктов, соответствующих политике безопасности и текущему контексту безопасности
- Протоколирование и ведение журнала событий

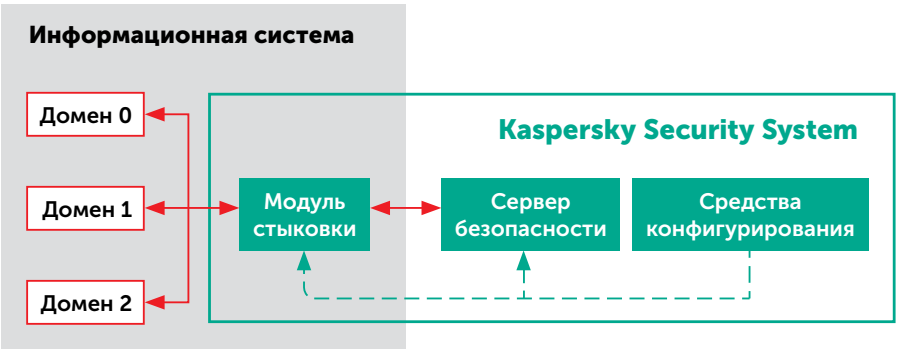
Режим эксплуатации

Kaspersky Security System предусматривает два режима эксплуатации:

- **Базовый** – включает широкий набор базовых политик обеспечения безопасности информационной системы, которого достаточно для большинства сценариев использования;
- **Расширенный** – в дополнение к базовому набору, позволяет разрабатывать и настраивать специализированные политики безопасности в соответствии с индивидуальными требованиями информационной системы и спецификой решаемых задач.

Компоненты

- **Модуль стыковки** — программный модуль, отвечающий за процесс взаимодействия между информационной системой и сервером безопасности; осуществляет доставку запросов и применение вердиктов «запрещено/разрешено».
- **Сервер безопасности** — программный модуль, ответственный за вынесение вердикта «запрещено/разрешено». Сервер безопасности определяет вердикт, основываясь на двух составляющих:
  - **Набор правил безопасности**, определяющих политику безопасности конкретной системы.
  - **Контекст**: сервер безопасности хранит контексты безопасности, описывающие текущее состояние системы.
- **Средства конфигурации** – программный модуль, позволяющий настроить политики безопасности и интегрировать их в информационную систему.



Пример архитектуры решения, использующего Kaspersky Security System. **Модуль стыковки**, интегрированный в информационную систему, перехватывает взаимодействия между доменами и исполняет решение о доступе. **Сервер безопасности** предоставляет вердикт модулю стыковки в соответствии с установленной политикой безопасности. Политика безопасности может быть сформирована с использованием **Средств конфигурации**.

1 Идет работа над поддержкой других операционных систем, в том числе ОС, работающих в режиме реального времени

2 Тесная интеграция дополняющих друг друга технологий (KasperskyOS + Kaspersky Security System) позволяет добиться их максимальной эффективности и производительности, а также дает надежный и гибкий инструмент управления безопасностью информационных систем, включая технологические сети.

www.kaspersky.ru

Find out more at os.kaspersky.com
All about Internet security: www.securelist.com