Топ-5 критериев для выбора современного EPP-решения



Защита конечных устройств – это краеугольный камень стратегии информационной безопасности. Все понимают ее важность. Точно так же все осознают, что одного антивируса сегодня недостаточно. Именно поэтому многие вендоры называют свои решения платформами для защиты рабочих мест (EPP). Но что скрывается за этими заявлениями?

Наш простой чек-лист призван помочь вам оценить и сделать обоснованный выбор решения класса EPP, которое обеспечит надёжную защиту сегодня и будет соответствовать вызовам завтрашнего дня. Отметьте те пункты, которым соответствует решение, которое вас заинтересовало, и вам будет гораздо проще определиться с выбором.

1. Поддержка всех платформ

Чек-лист:

- ☐ Windows
- ☐ macOS
- ☐ Linux
- ☐ Android/iOS
- ☐ Виртуальные инфраструктуры
- ☐ VDI

Современные EPP-решения должны обеспечивать комплексную защиту всех типов операционных систем и различных сред развертывания. Современный ИТ-ландшафт обычно представляет собой смесь из разнородных систем, где каждая представляет собой отдельный вектор атаки и требует специфической защиты. Выбор EPP, ограниченного лишь одной основной ОС, создает «слепые зоны» в безопасности организации.

2. Обнаружение массовых и сложных угроз

Чек-лист:

- [ ] Файловый антивирус
- [ ] Веб-антивирус
- [ ] Почтовый антивирус
- [ ] Защита от сетевых угроз (IDS)
- [ ] Поведенческий анализ
- [ ] Защита от эксплойтов
- [ ] Защита от шифровальщиков
- [ ] Проактивная защита (HIPS)
- [ ] Машинное обучение
- [ ] Эмуляция (Sandbox)

Традиционные антивирусные решения, ориентированные исключительно на сигнатурный анализ вредоносного кода, больше не способны обеспечить адекватный уровень защиты в условиях современных киберугроз. Современная платформа класса EPP должна реализовывать стратегию многоуровневой защиты, выходя за рамки простого сопоставления с базой известных угроз. В современном детектировании ключевая роль отведена технологиям искусственного интеллекта и поведенческого анализа. Решения, использующие множество постоянно обновляемых моделей машинного обучения, способны выявлять аномальную активность и атаки на ранних стадиях, не полагаясь на сигнатуры.

3. Репутационный анализ

Чек-лист:

- [ ] Возможность подключения устройств, защищенных EPP, к глобальной репутационной базе с широким географическим покрытием.

Система репутационного анализа использует глобальную телеметрию с миллионов устройств, чтобы оценивать файлы на основе распространенности, времени первого появления, источника происхождения и цифровых подписей. Это позволяет обнаруживать целевые и малораспространенные угрозы, проактивно блокировать угрозы на этапе проникновения, повышать точность обнаружения и оптимизировать производительность.

4. Проактивное сокращение поверхности атаки

Чек-лист:

- [ ] Сетевой экран (уровня узла)
- [ ] Веб-контроль
- [ ] Контроль устройств и приложений
- [ ] Контроль целостности
- [ ] Патч-менеджмент
- [ ] Шифрование данных

Современные EPP-решения помимо обнаружения угроз создают комплексную превентивную среду, максимально сужая «окно возможностей» злоумышленника. Именно совокупность превентивных механизмов, дополняющих движки обнаружения угроз, превращает EPP-решение в комплексную систему, способную противостоять современным угрозам не только путем их обнаружения, но и путем проактивного ограничения поля деятельности нарушителя.

5. Интеграция с EDR/MDR

Чек-лист:

- ☐ Возможность работы агента EPP в режиме EDR
- ☐ Возможность работы агента EPP в режиме MDR
- ☐ Возможность бесшовного наращивания функциональности EPP → EDR → MDR

По мере развития компании и усложнения ИТ-инфраструктуры закономерно меняются и требования к системе защиты информации в организации. Для перехода от EPP к EDR или MDR ключевым условием является единый агент, умеющий одновременно выполнять функции EPP и EDR/MDR, а также единая консоль управления. Это позволяет подключать расширенную функциональность без установки дополнительного ПО, дополнительных перезагрузок и риска конфликтов совместимости.

Kaspersky Endpoint Security для бизнеса
Расширенный Плюс

Kaspersky Endpoint Security для бизнеса Расширенный Плюс – это комплексное предложение для компаний до 1000 узлов по защите рабочих мест и корпоративной почты, а также для безопасного управления мобильными ресурсами.

Подробнее о решении

www.kaspersky.ru

© 2026 АО «Лаборатория Касперского» Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.