FORTINET SECURITY DAY

VIRTUAL

Подходы к реализации решений

Endpoint Detection and Response

Кирилл Михайлов

Агенты для защиты

рабочих станций

EDR замена EPP?

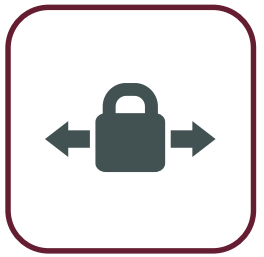
Ба[illegible]ля
[illegible]ы ра[illegible]
[illegible]станций

Решение Endpoint
Detection and Response

Функционал EPP

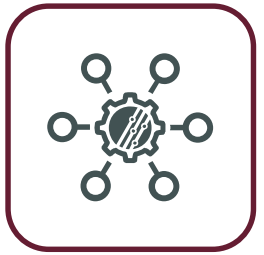
Базовое решение для защиты рабочих станций

Антивирусный модуль



Модуль VPN

Модуль Compliance



Модуль интеграции со сторонними системами

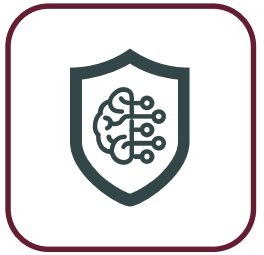
Функционал EDR

Решение Endpoint
Detection and Response

Антивирусный модуль

Модуль анализа активности

Модуль реагирования и восстановления системы



Модуль анализа и закрытия уязвимостей

EDR – замена EPP?

Базовое решение Endpoint Detection and Response

Защита рабочих станций

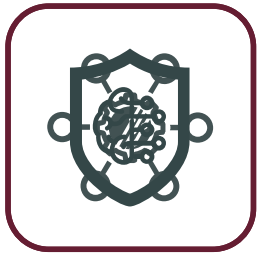
Антивирусный модуль

Модуль анализа активности

Модуль VPN

Модуль Compliance и восстановления системы

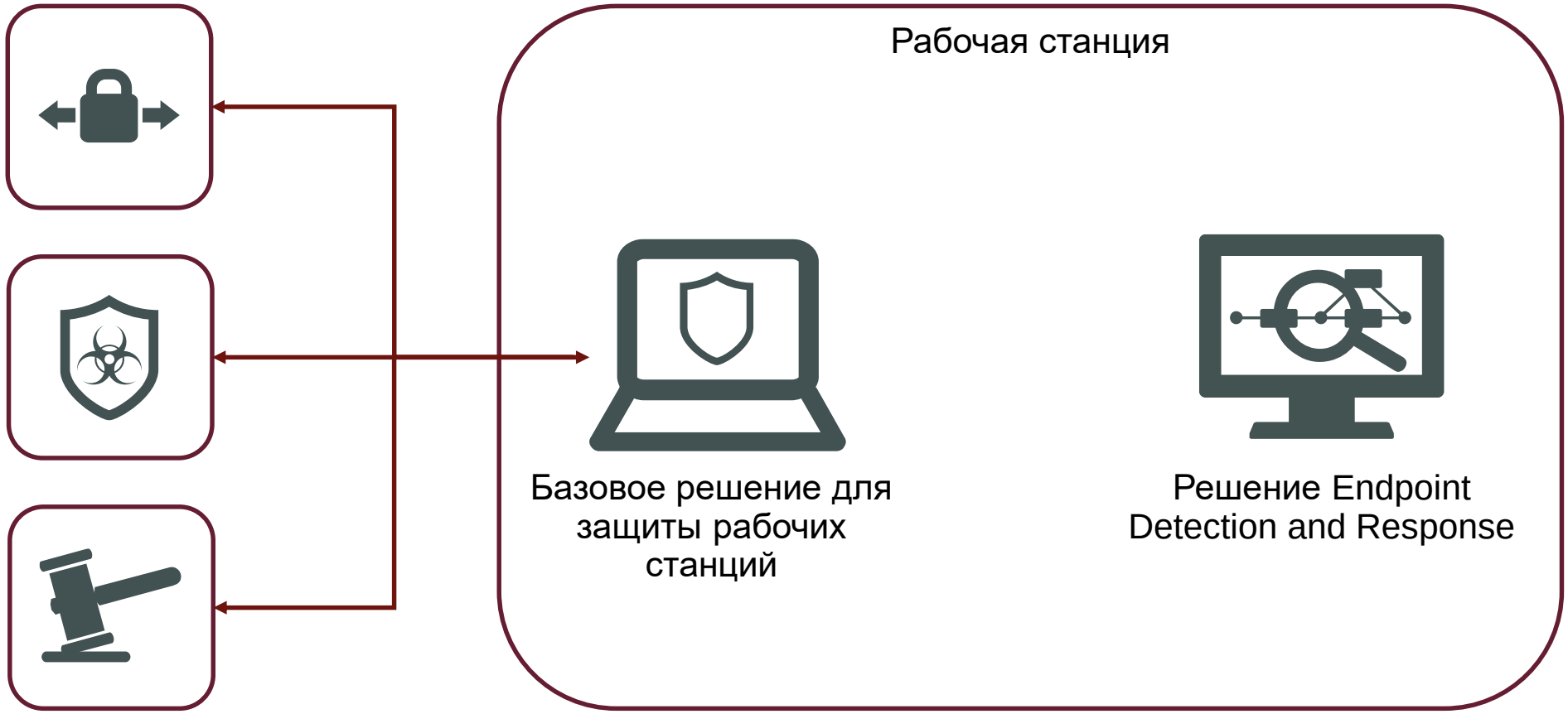
Модуль реагирования



Модуль интеграции со сторонними системами

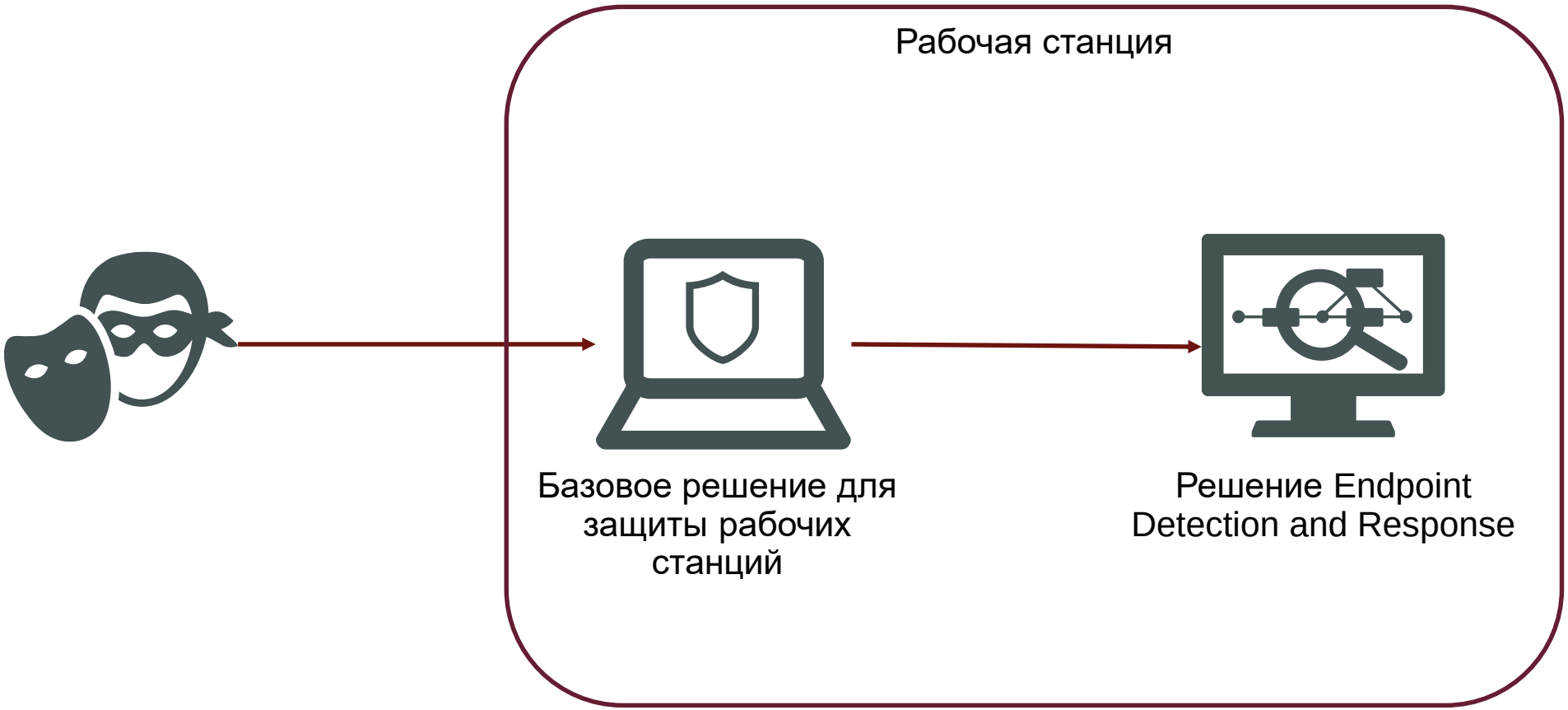
Модуль анализа уязвимостей

EPP: Фильтрация угроз



EPP: Фильтрация угроз

EDR: обнаружение сложных угроз



EDR замена EPP?

Ба[illegible]ля
[illegible]ы ра[illegible]
[illegible]станций

Решение Endpoint
Detection and Response

Подходы к реализации EDR

Архитектура

Компоненты

Агент

Центральный сервер

Облачный сервис

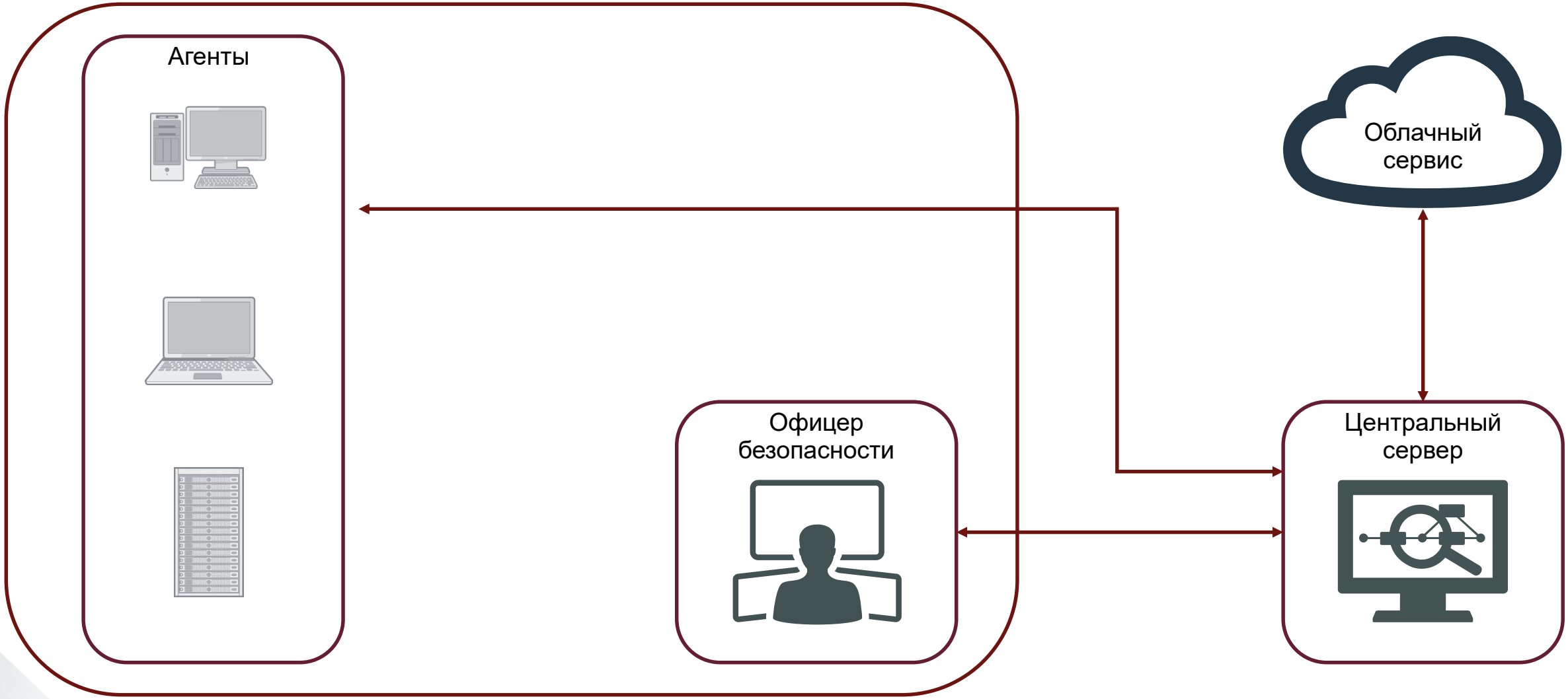
Типы архитектуры

Облачная

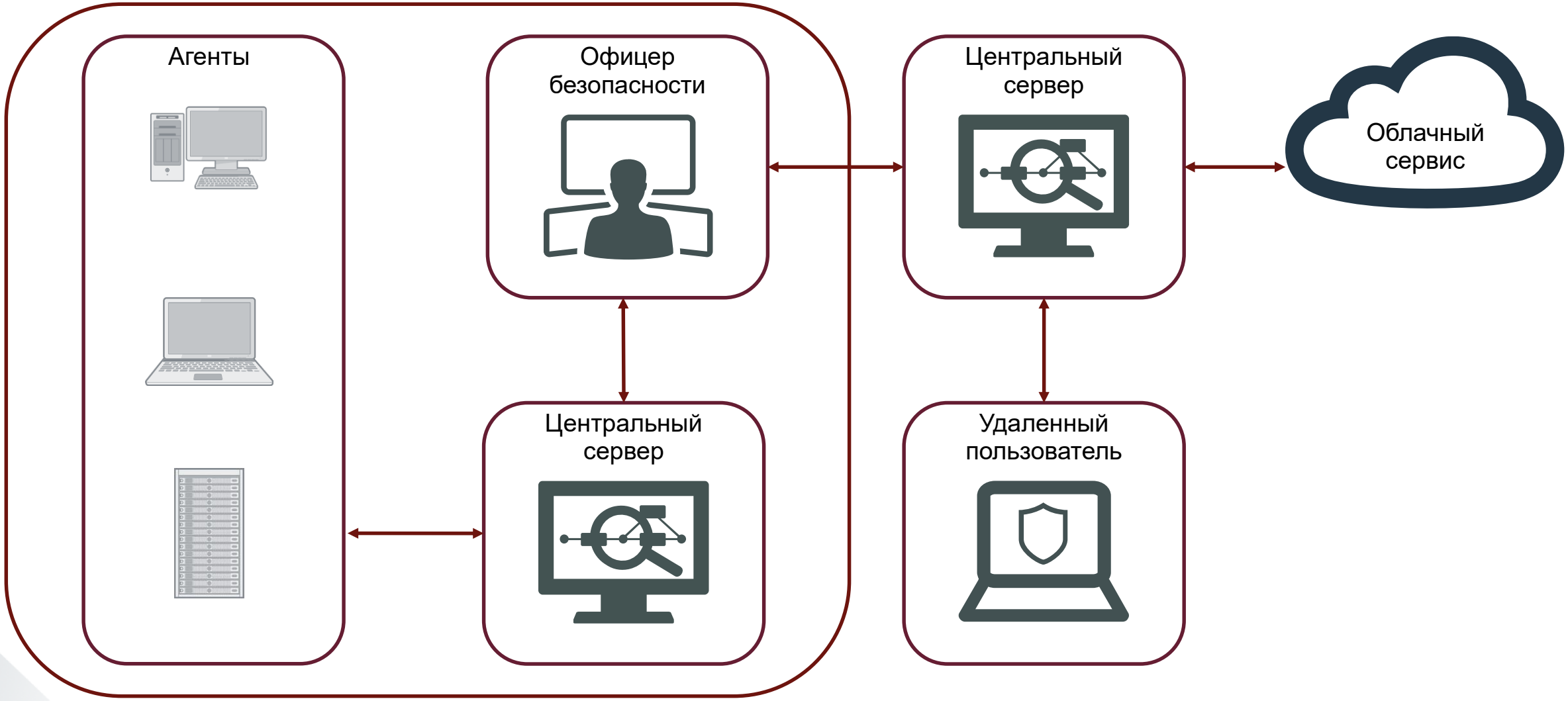
Гибридная

Локальная

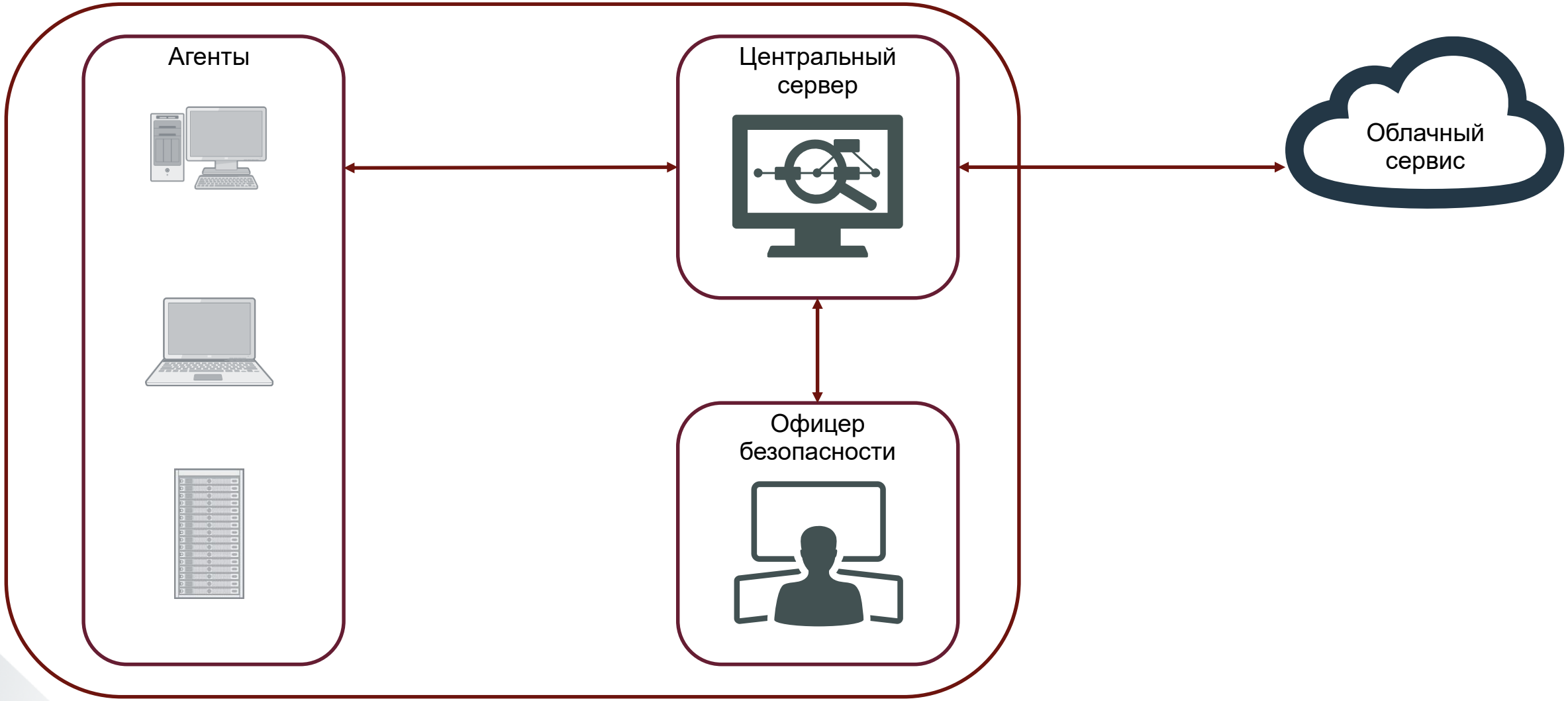
Облачная архитектура



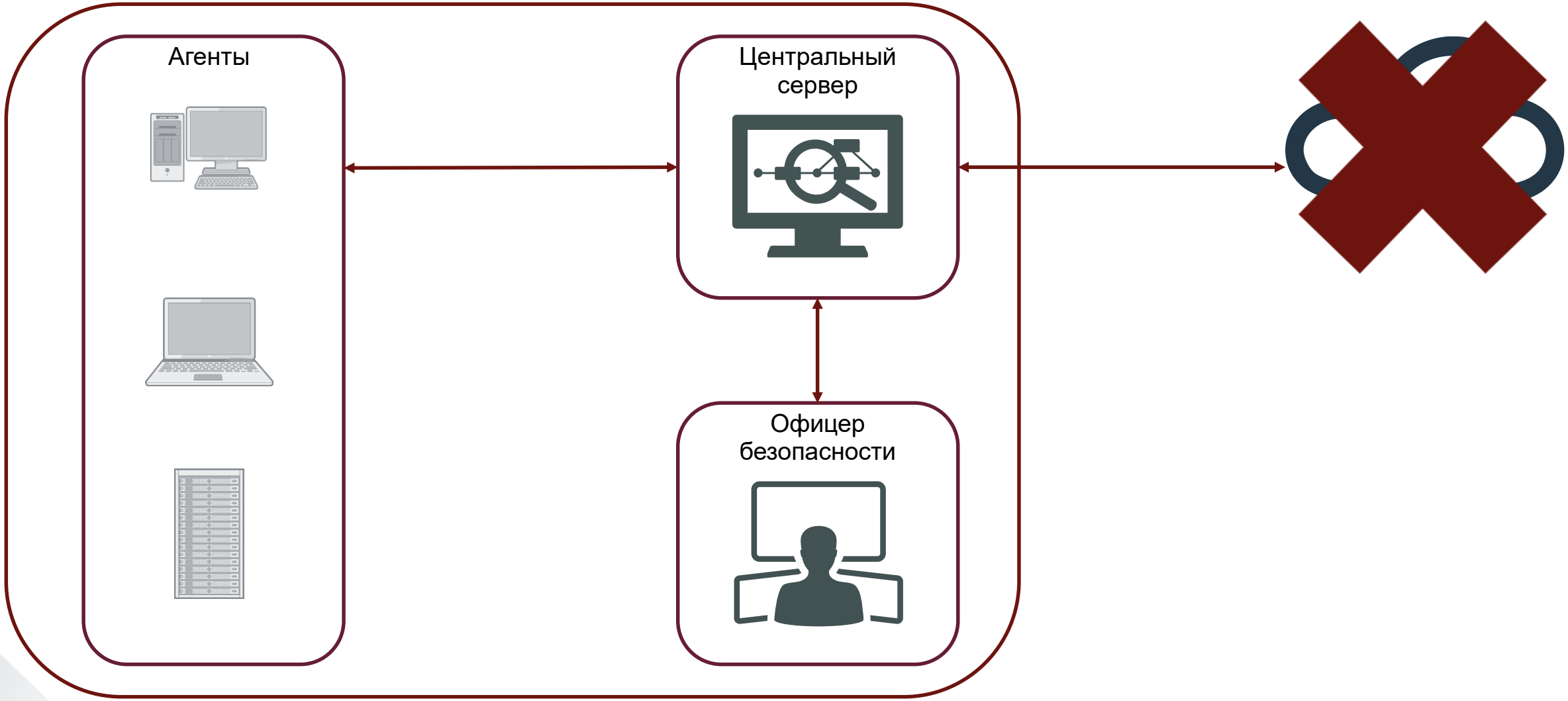
Гибридная архитектура



Локальная архитектура



Полная изоляция



Подходы к реализации EDR

Сбор данных

Сбор данных

Сбор всей телеметрии

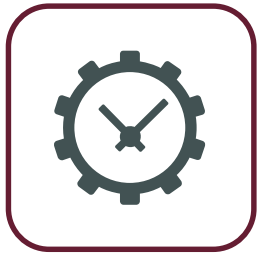
Сбор событий безопасности

Сбор всей телеметрии

Сбор всей телеметрии

Задержки в обнаружении

Повышенная нагрузка на каналы связи



Задержки в реагировании на инциденты

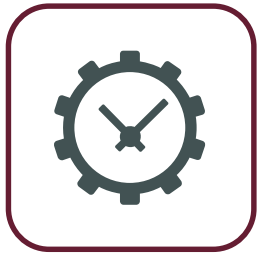
Повышенные аппаратные требования

Сбор события ИБ

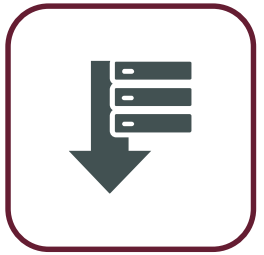
Сбор событий безопасности

Обнаружение угроз в кратчайшие сроки

Снижение нагрузки на каналы связи



Ускоренная реакция на инциденты



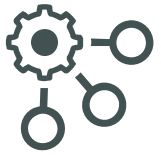
Снижение аппаратных требований

Подходы к реализации EDR

Реагирование

Автоматизировать?

Ручное реагирование
на инциденты



Автоматизированное
реагирование на
инциденты

Автоматизировать?

Заключение

EDR – инструмент офицера безопасности

Офицер безопасности

Endpoint Detection and Response


FORTINET