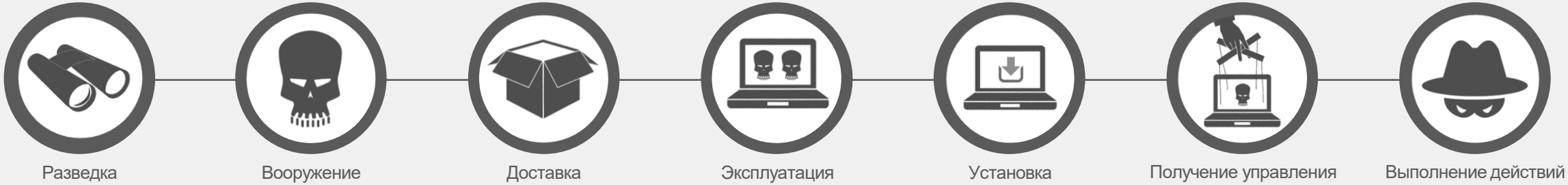
FortiEDR/FortiXDR

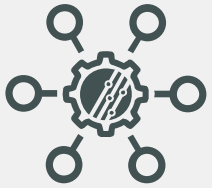
Кирилл Михайлов, системный инженер

kmikhaylov@fortinet.com

Минимизация издержек



Инструменты обнаружения и предотвращения



Fortinet Security Fabric

Рабочие станции / серверы

Видимость и контроль

конечных узлов

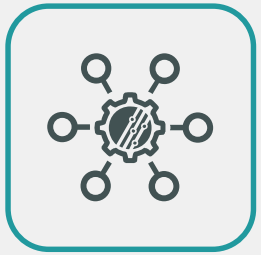
Функционал EPP

FortiClient

Модуль защиты от ВПО

Модуль VPN

Модуль Compliance



Модуль интеграции со сторонними системами

Функционал EDR

FortiEDR

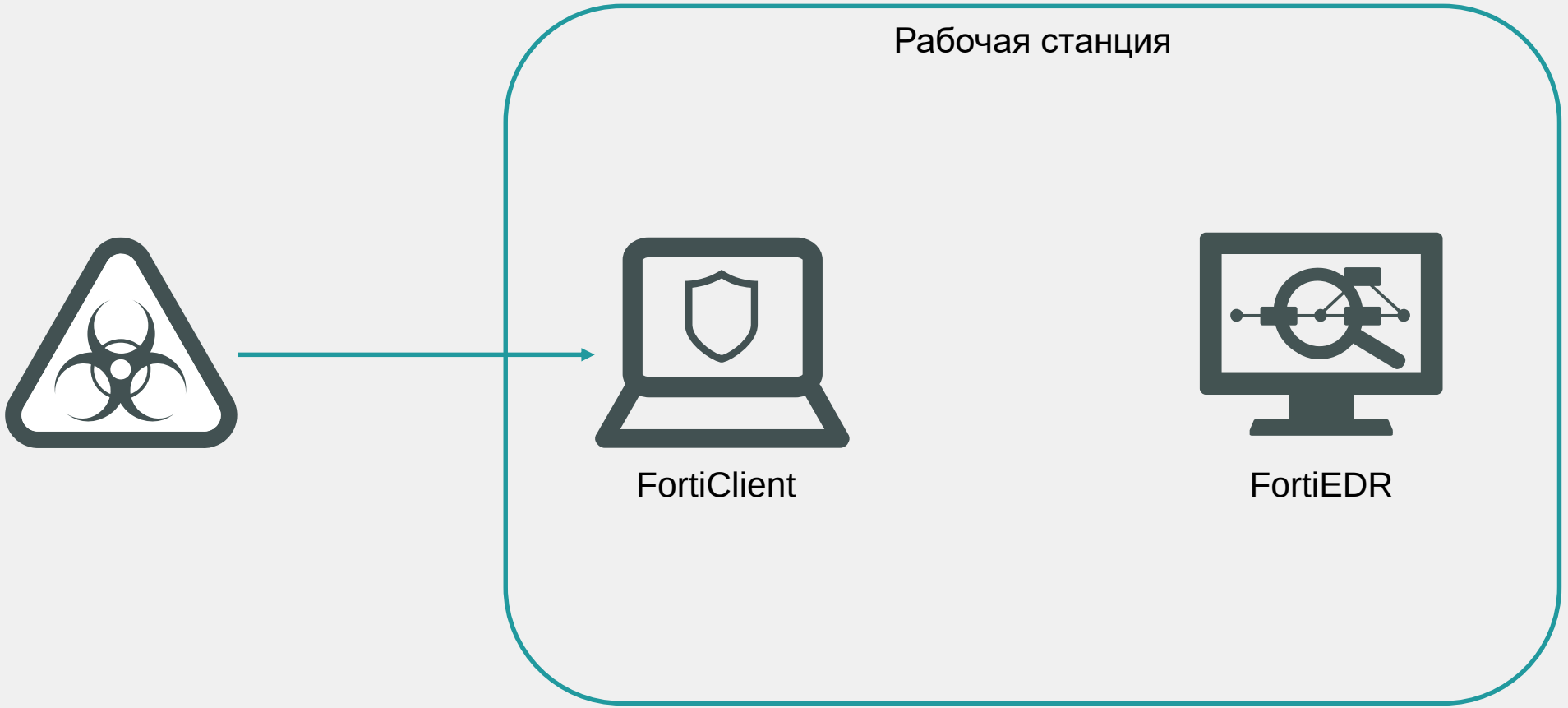
Антивирусный модуль

Модуль анализа активности

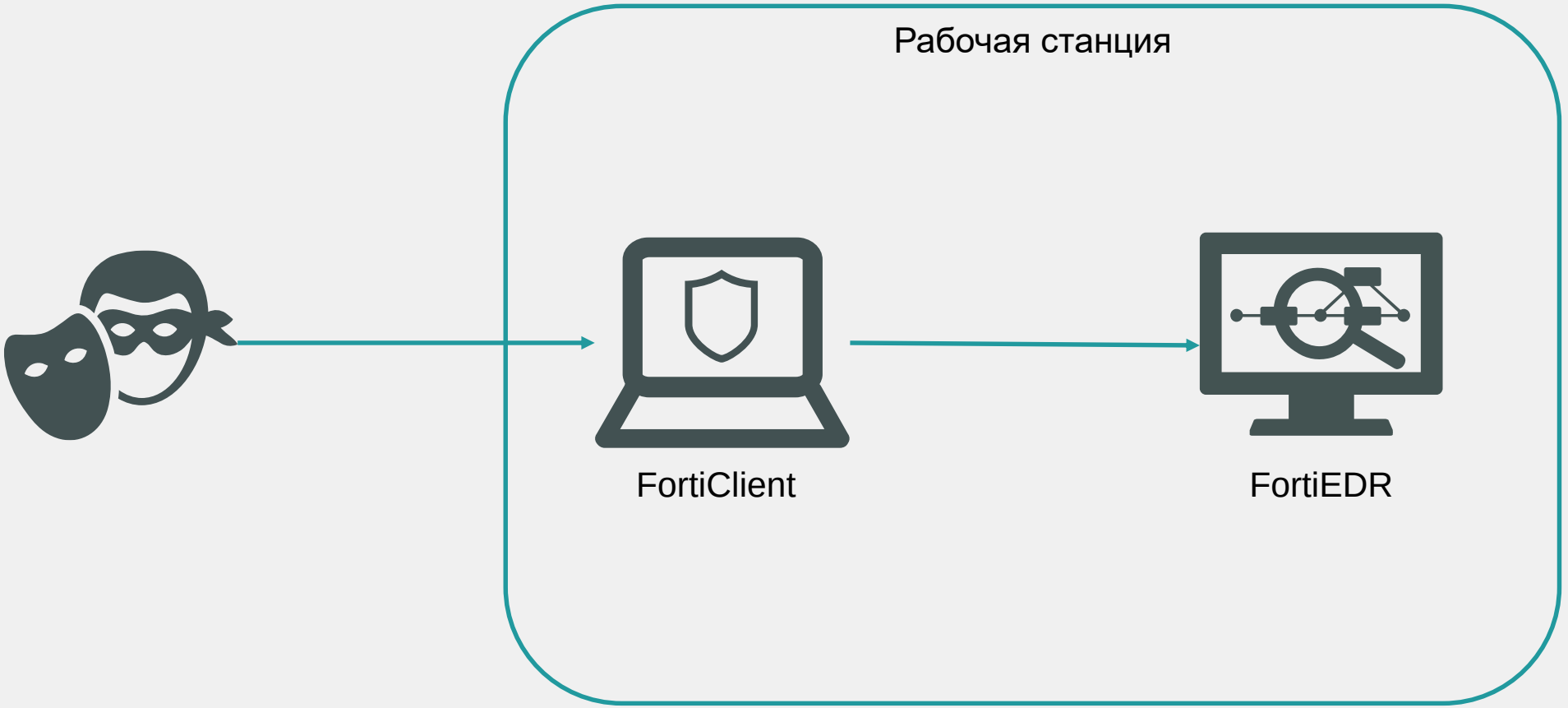
Модуль реагирования и восстановления системы

Модуль анализа и закрытия уязвимостей

EPP: защита от известных угроз



EDR: обнаружение продвинутых атак



EDR замена EPP?

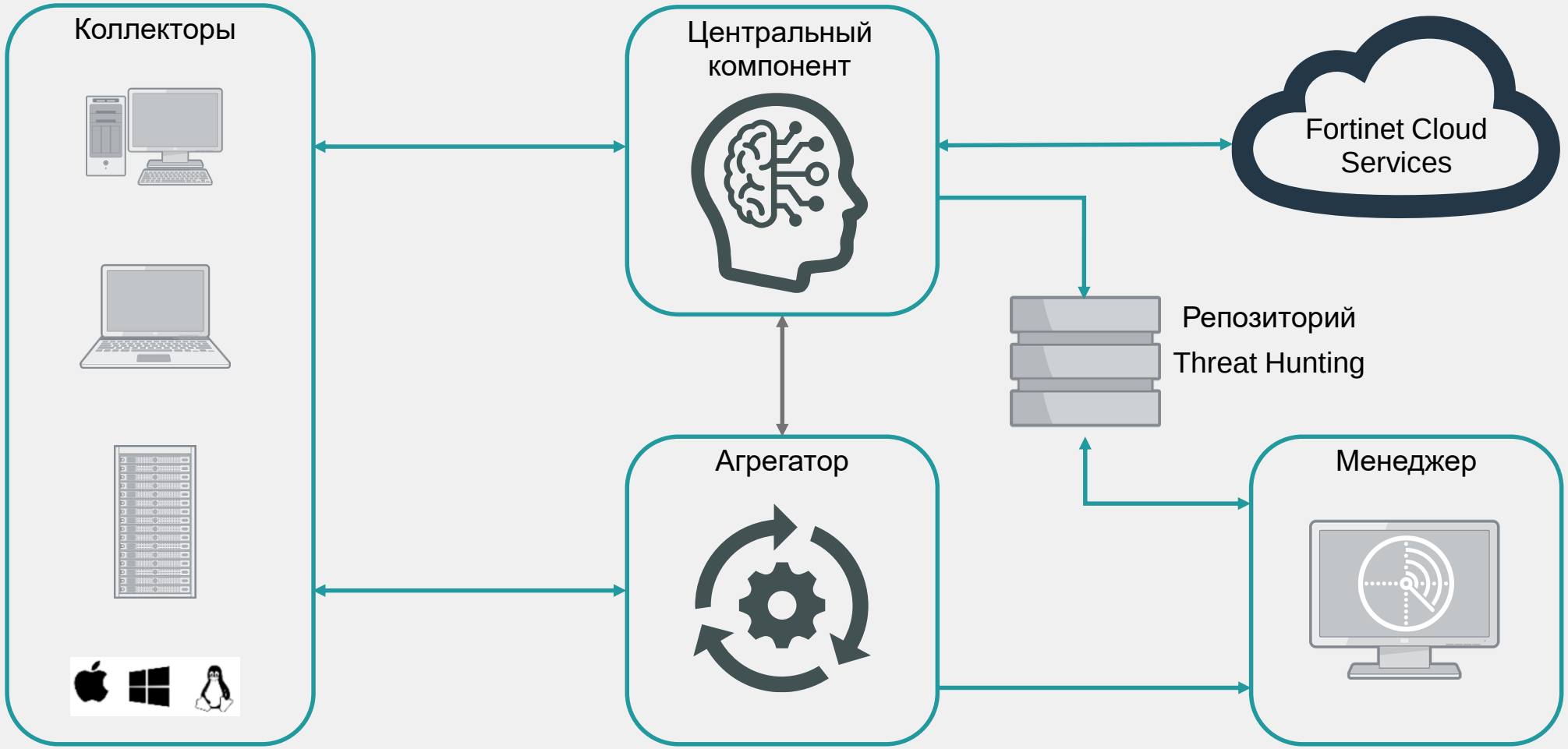
FortiClient

FortiEDR

FortiEDR

Компоненты и архитектура

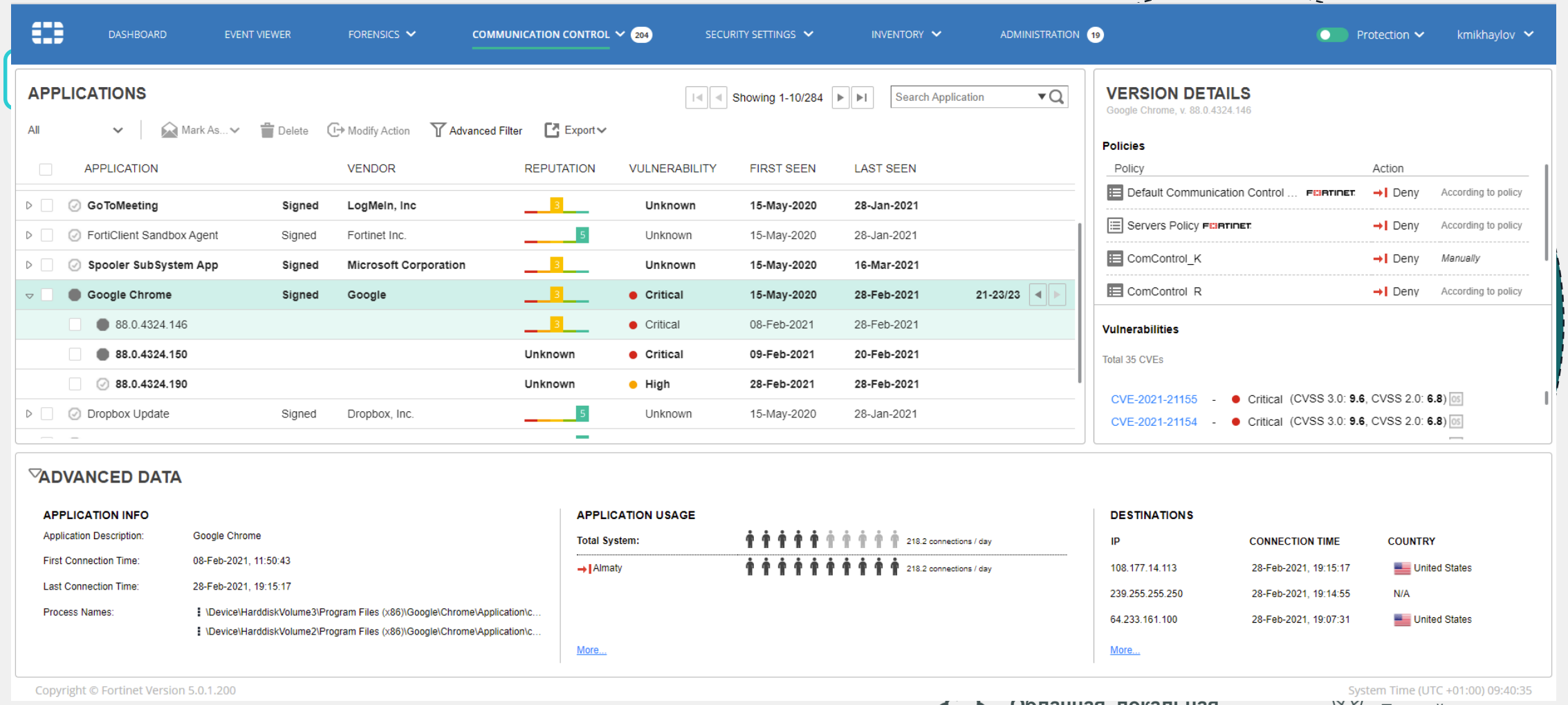
FortiEDR: архитектура



FortiEDR

Технологии обнаружения и реагирования

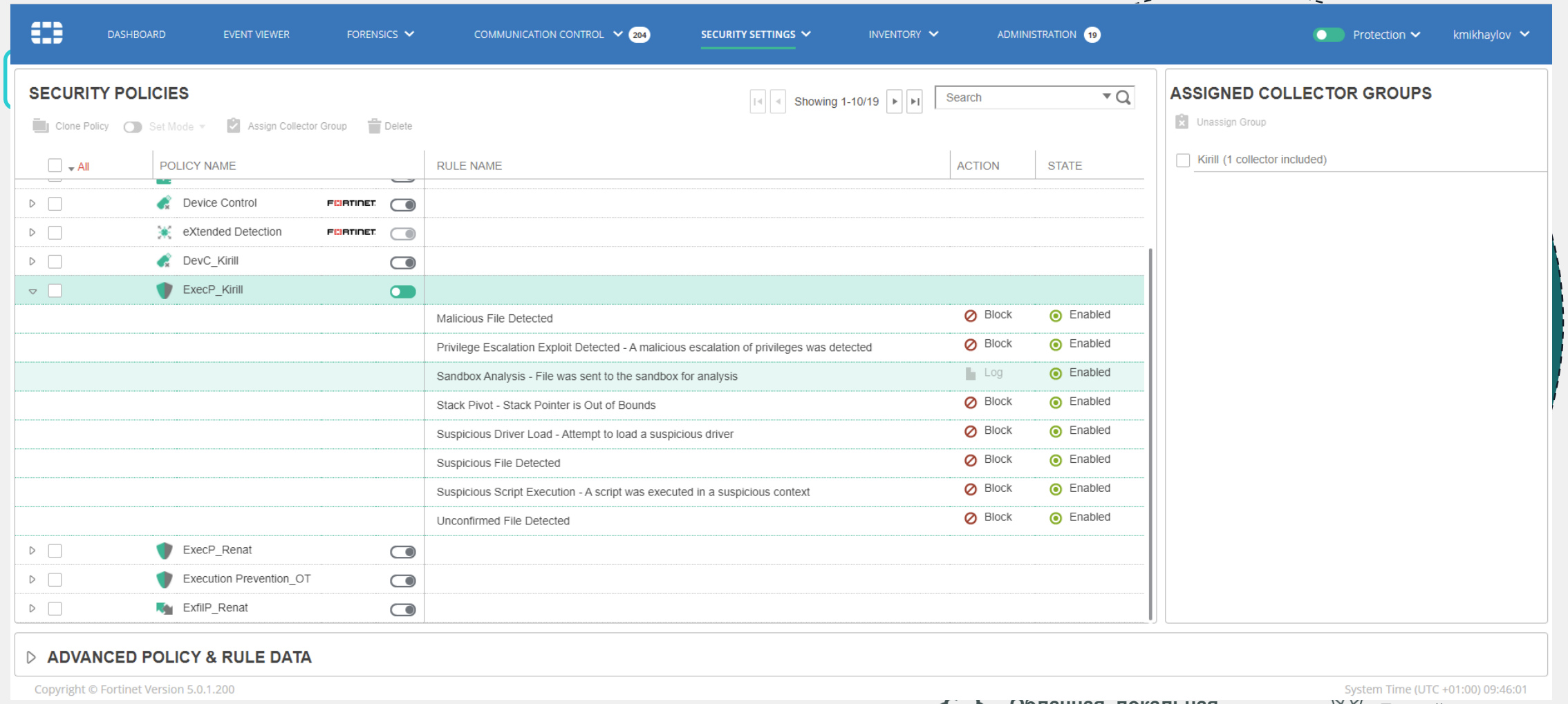
FortiEDR: блокировка



Облачная, локальная, Гибридная архитектура

Легкий агент

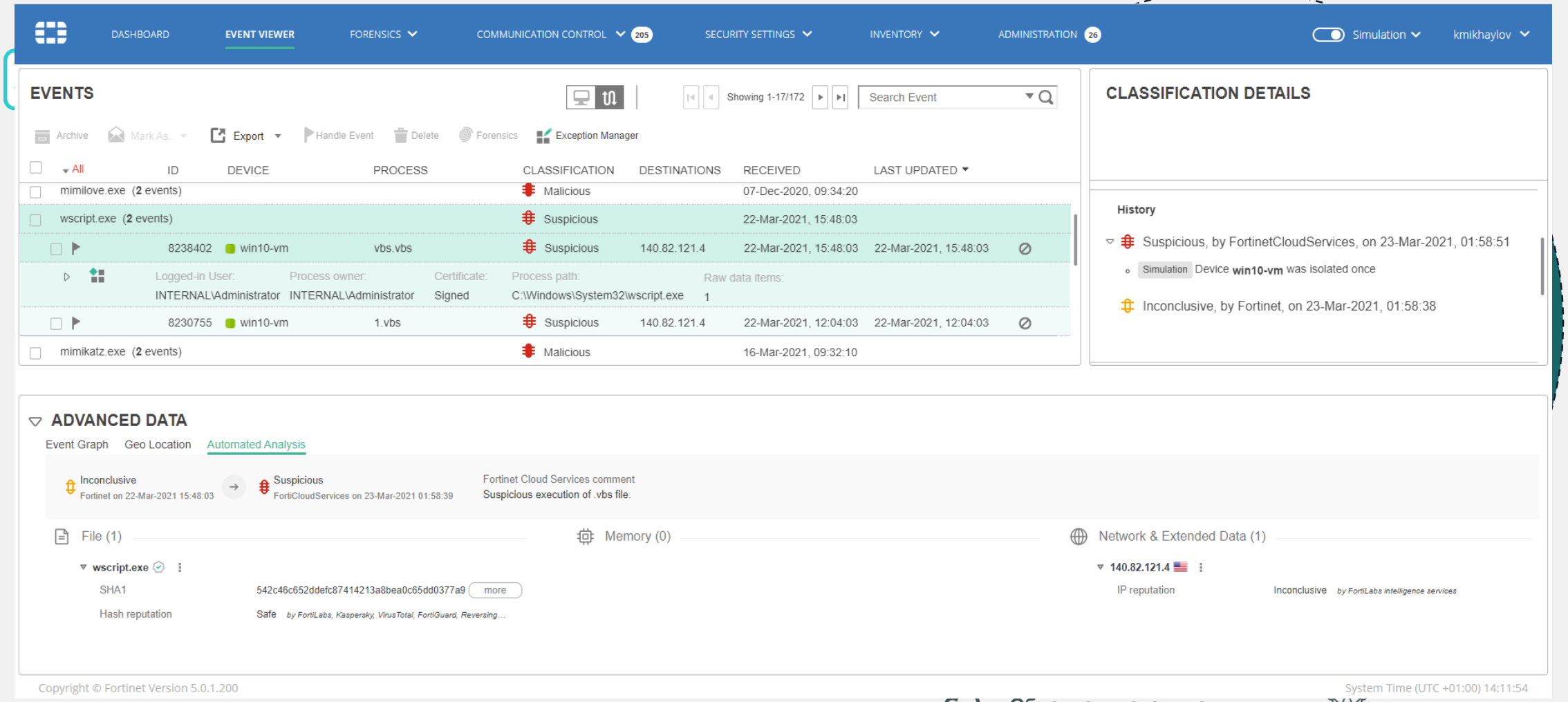
FortiEDR: блокировка



Облачная, локальная, Гибридная архитектура

Легкий агент

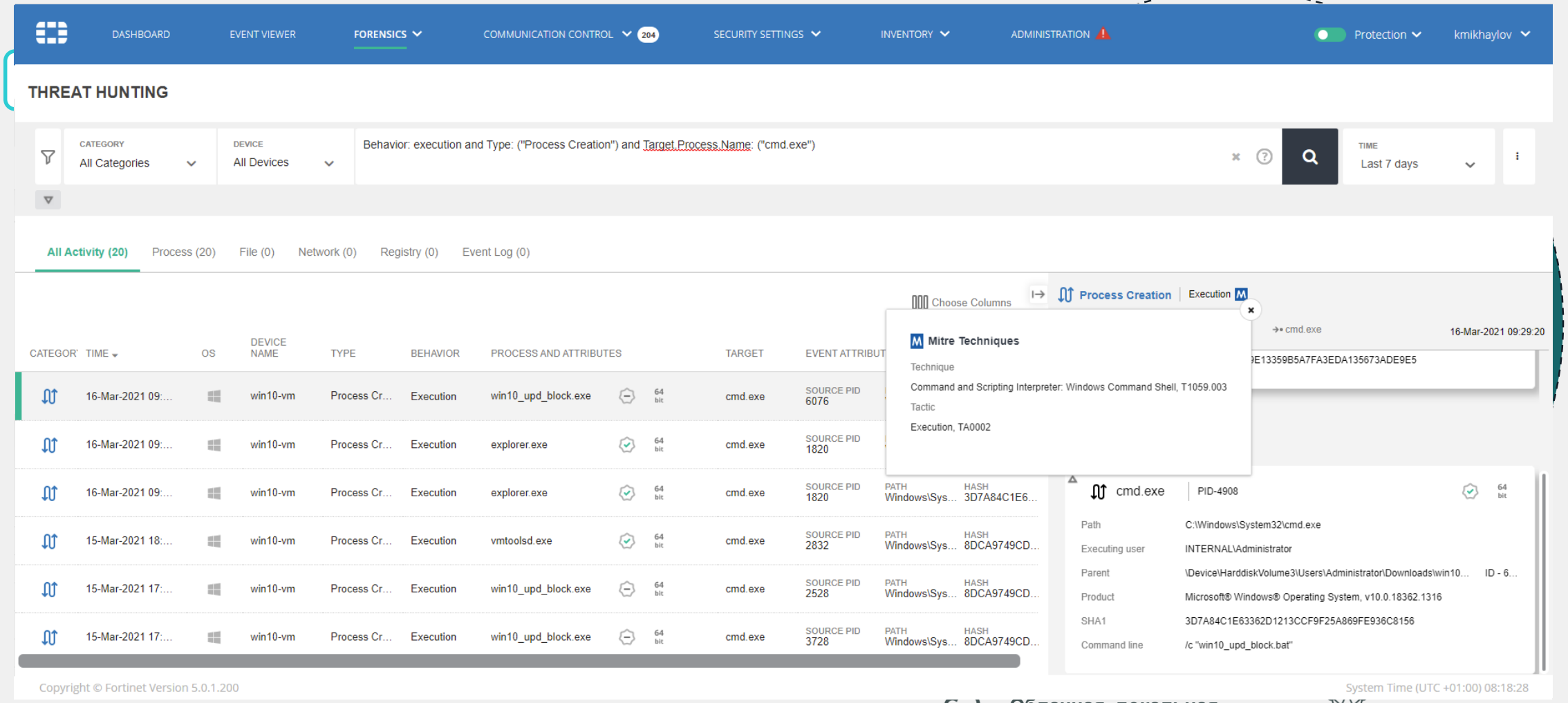
FortiEDR: обнаружение



Облачная, локальная, Гибридная архитектура

Легкий агент

FortiEDR: реагирование



Облачная, локальная, Гибридная архитектура

Легкий агент

Расширенные обнаружение и реагирование

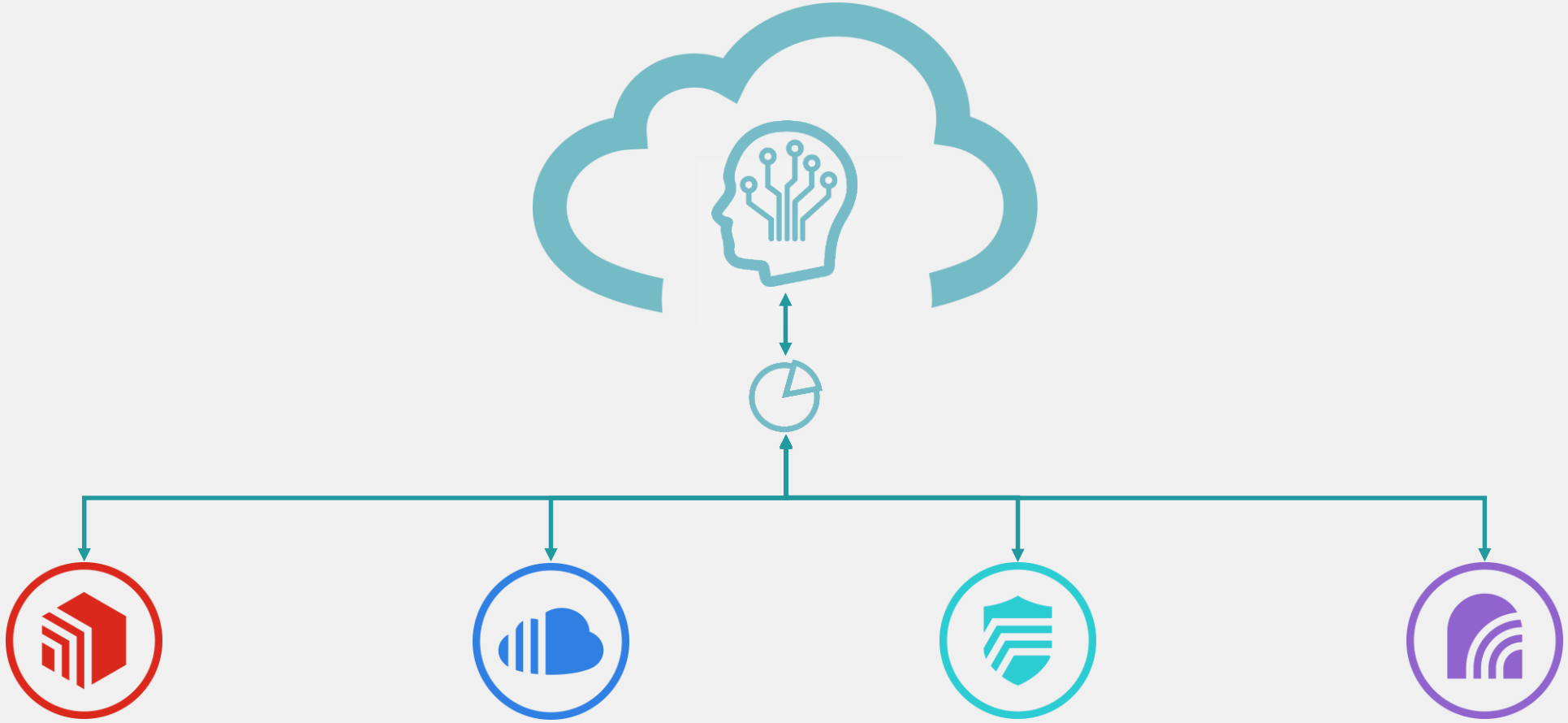
FortiEDR

Fortinet Security Fabric

Расширение автоматизации

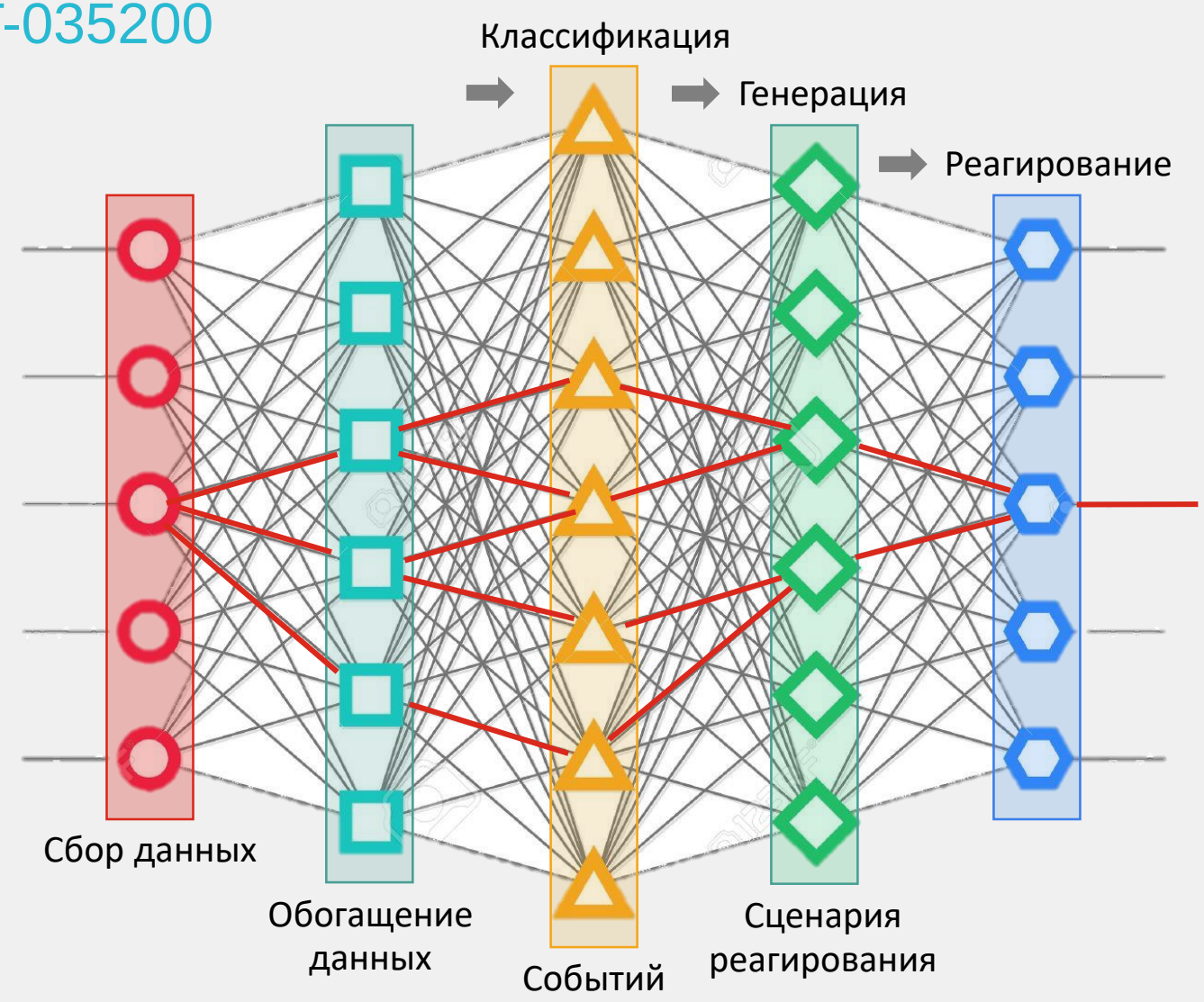
Обнаружения и реагирования на угрозы

FortiXDR



FortiXDR: ANN

Патент: #FORT-035200

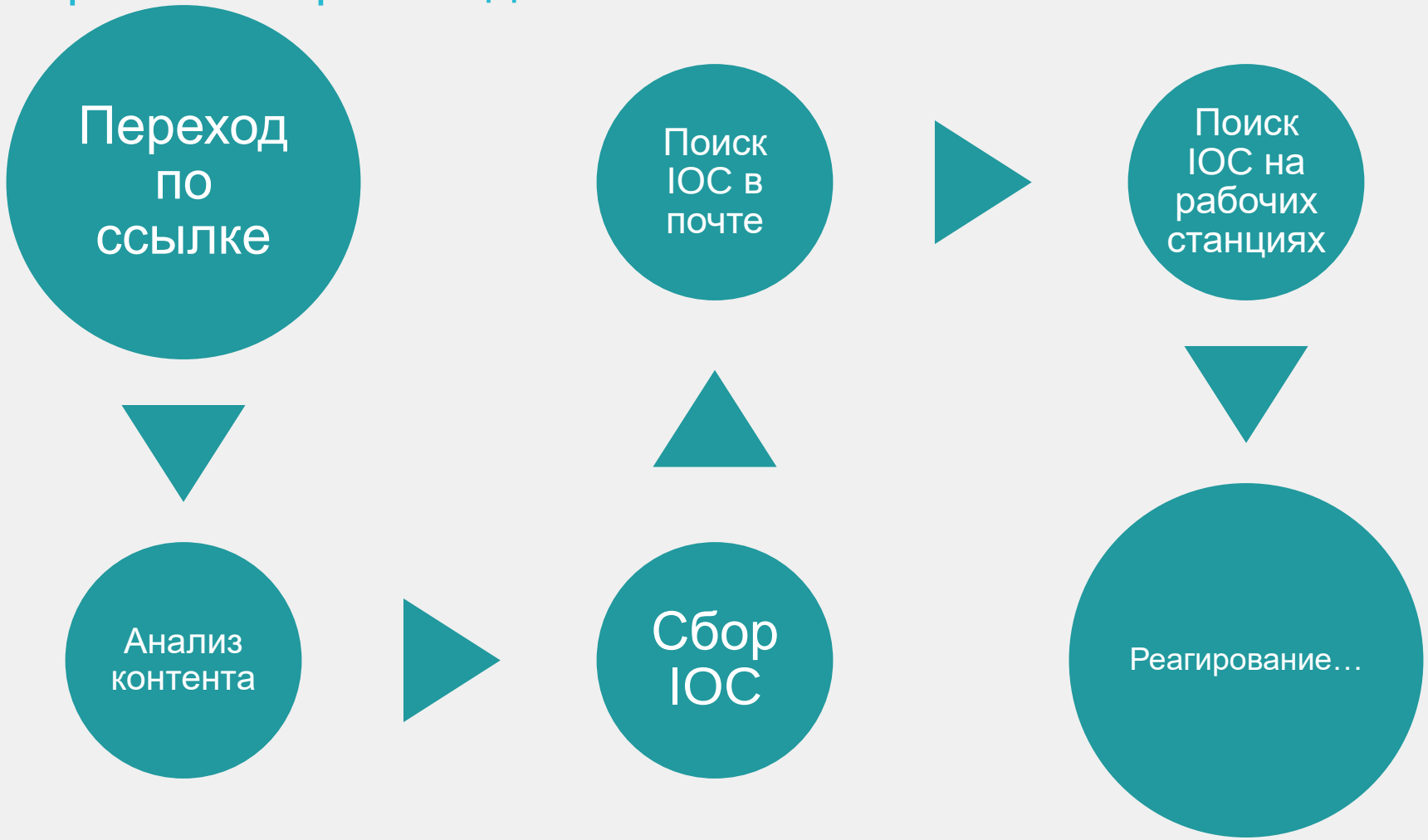


FortiXDR

Пример: целевой фишинг

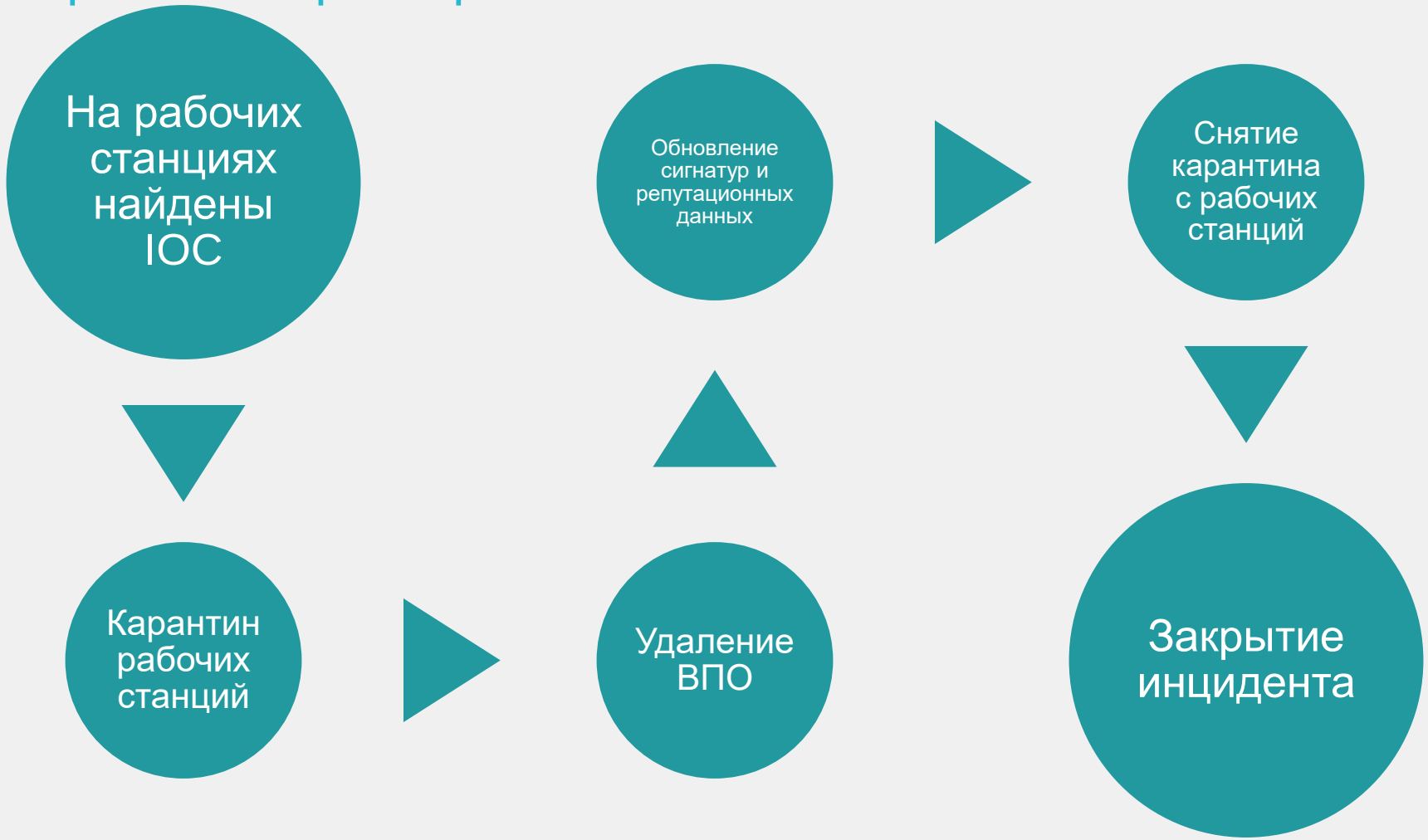
FortiXDR

Автоматизированное расследование



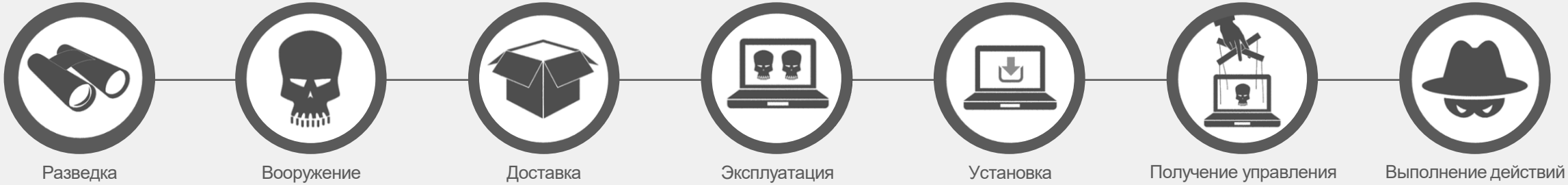
FortiXDR

Автоматизированное реагирование



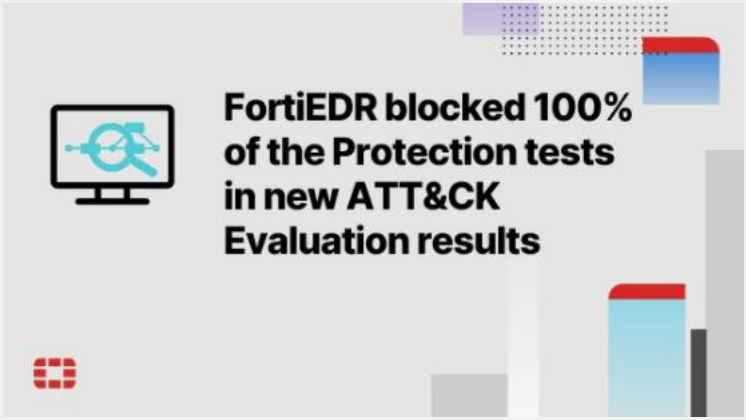
Заключение

Минимизация издержек



FortiEDR: MITRE

“The results showed that FortiEDR has:
- The ability to block 100% of the Protection tests, used by Carabank, FIN 7 and other similar campaigns; past, present and future.
- Precise tracing and assessment of granular system activity, for comprehensive detection of the techniques and tactics in the scope of evaluation as well as confident blocking at the optimal time of the campaign.
- A clear picture of conscious design principles, especially the balance between effectiveness and accuracy, valuable vs. overwhelming information.” *



* https://www.fortinet.com/blog/business-and-technology/interpreting-mitre-evaluations-to-better-understand-endpoint-security-solutions


FORTINET