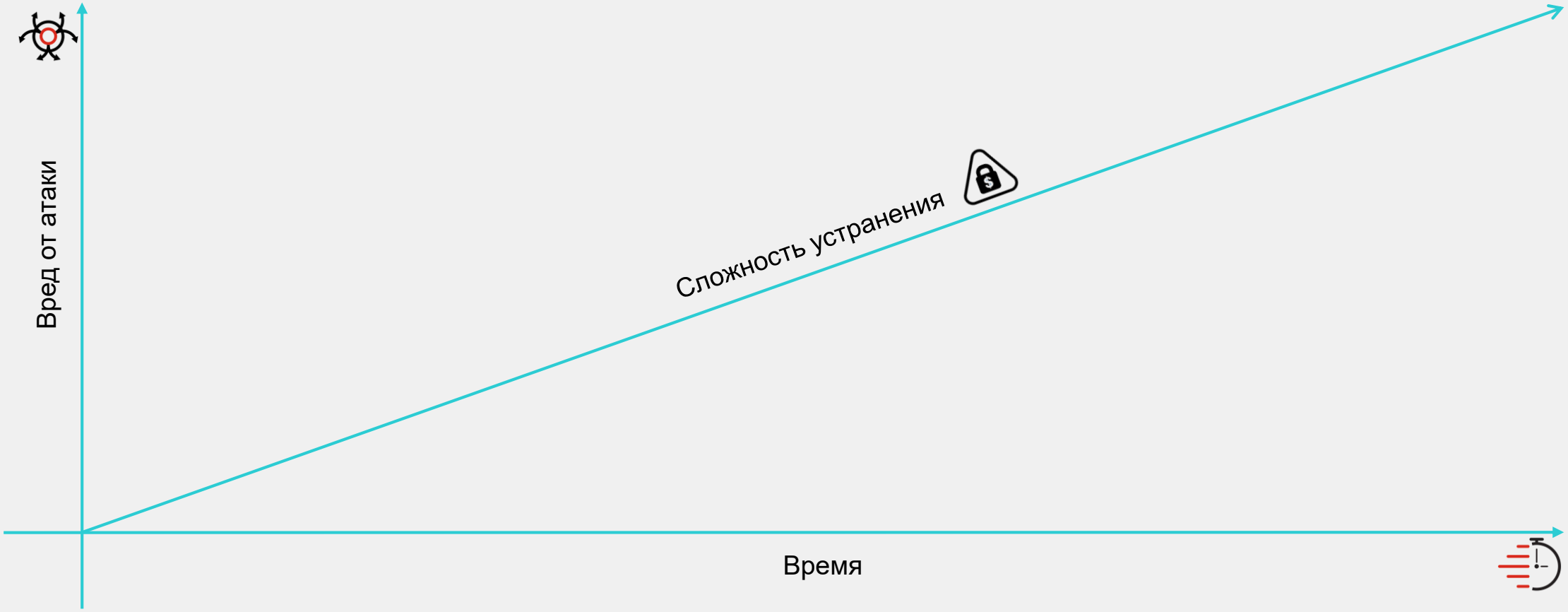
Решения и сервисы Fortinet для защиты конечных узлов от комплексных кибератак

Кирилл Михайлов, системный инженер EDR/XDR

kmikhaylov@fortinet.com

Снижение издержек от кибератак



Fortinet: автоматизация

FortiGuard Security Services

SOC & NOC

- Content Security
- Web Security
- Advanced SOC/NOC

User Security

- User Security
- Device Security
- Bundled Security

Fabric Management Center - SOC

Endpoint

- FortiEDR
- FortiXDR

Breach

- FortiSandbox
- FortiDeceptor
- FortiAI

Incident Response

- FortiAnalyzer
- FortiSIEM
- FortiSOAR
- FortiGuard MDR Service

Fabric Management Center - NOC

- FortiManager
- FortiCloud
- FortiMonitor

Open Ecosystem

- Connector
- Fabric API
- DevOps
- Extended Fabric Ecosystem

Zero Trust Access

- FortiClient
- FortiNAC
- FortiVoice
- FortiToken
- FortiAuthenticator
- FortiCamera

Security-Driven Networking

LAN Edge

- FortiAP
- FortiSwitch

WAN Edge

- FortiGate SD-WAN
- FortiExtender

DC Edge

- FortiGate
- FortiProxy

Cloud Edge

- FortiSASE
- FortiIsolator

Adaptive Cloud Security

Network

- FortiGate VM
- Cloud Networking
- FortiDDos
- FortiSegment

Platform

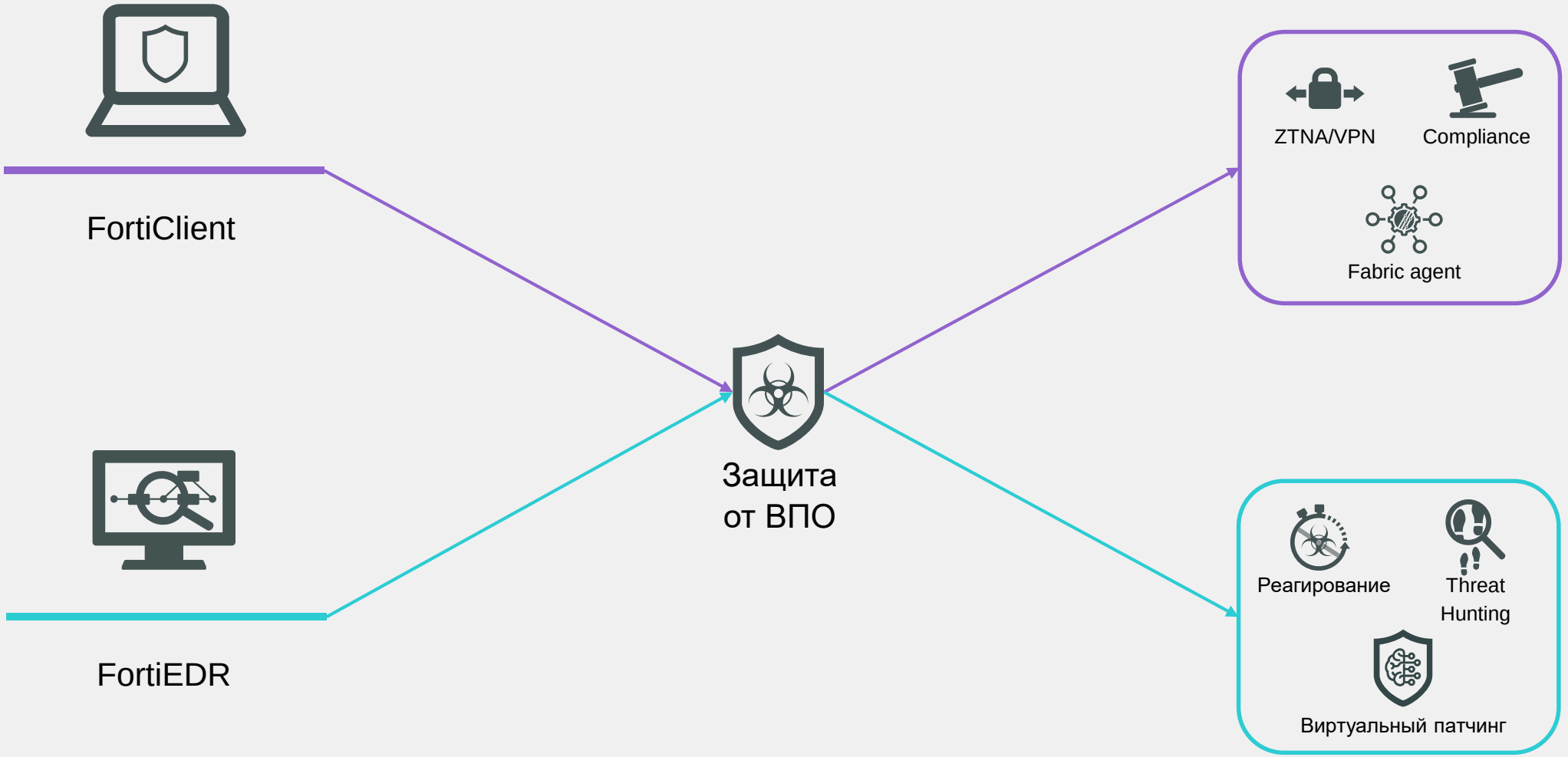
- FortiCASB
- FortiCWP
- AWS Native
- Azure Native

Applications

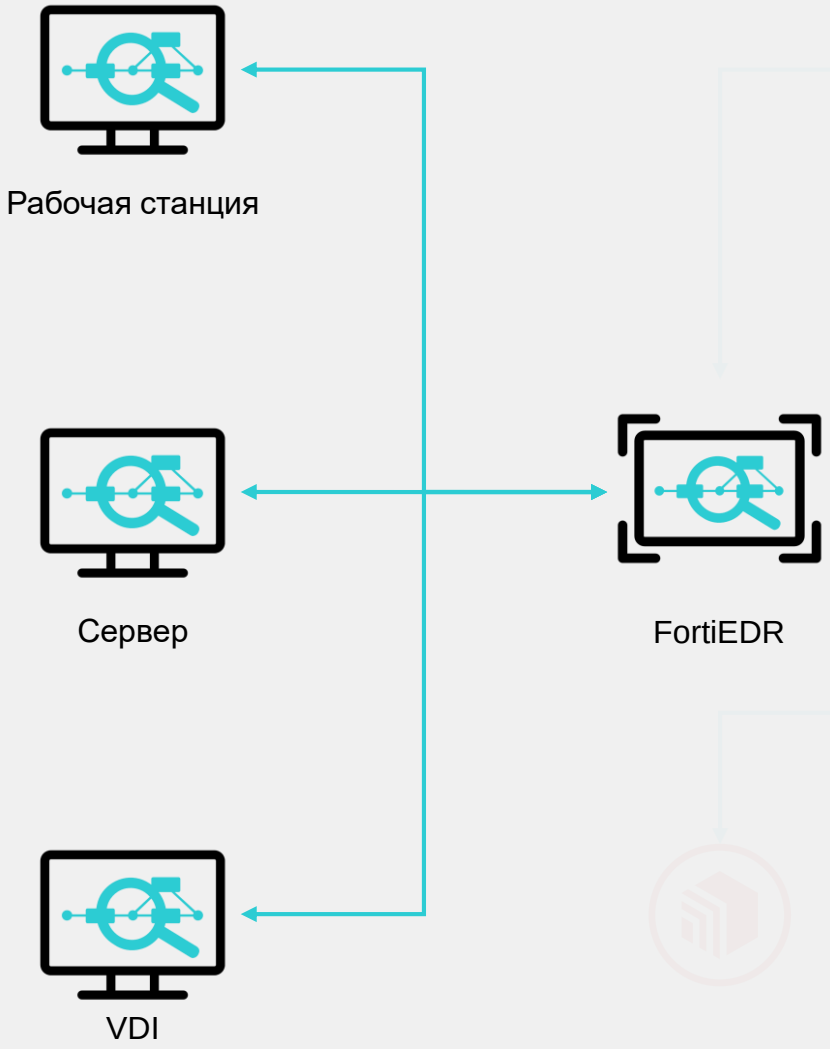
- FortiWeb
- FortiMail
- FortiADC
- FortiGSLB

Appliance | VM | Hosted | Cloud | Software | Container

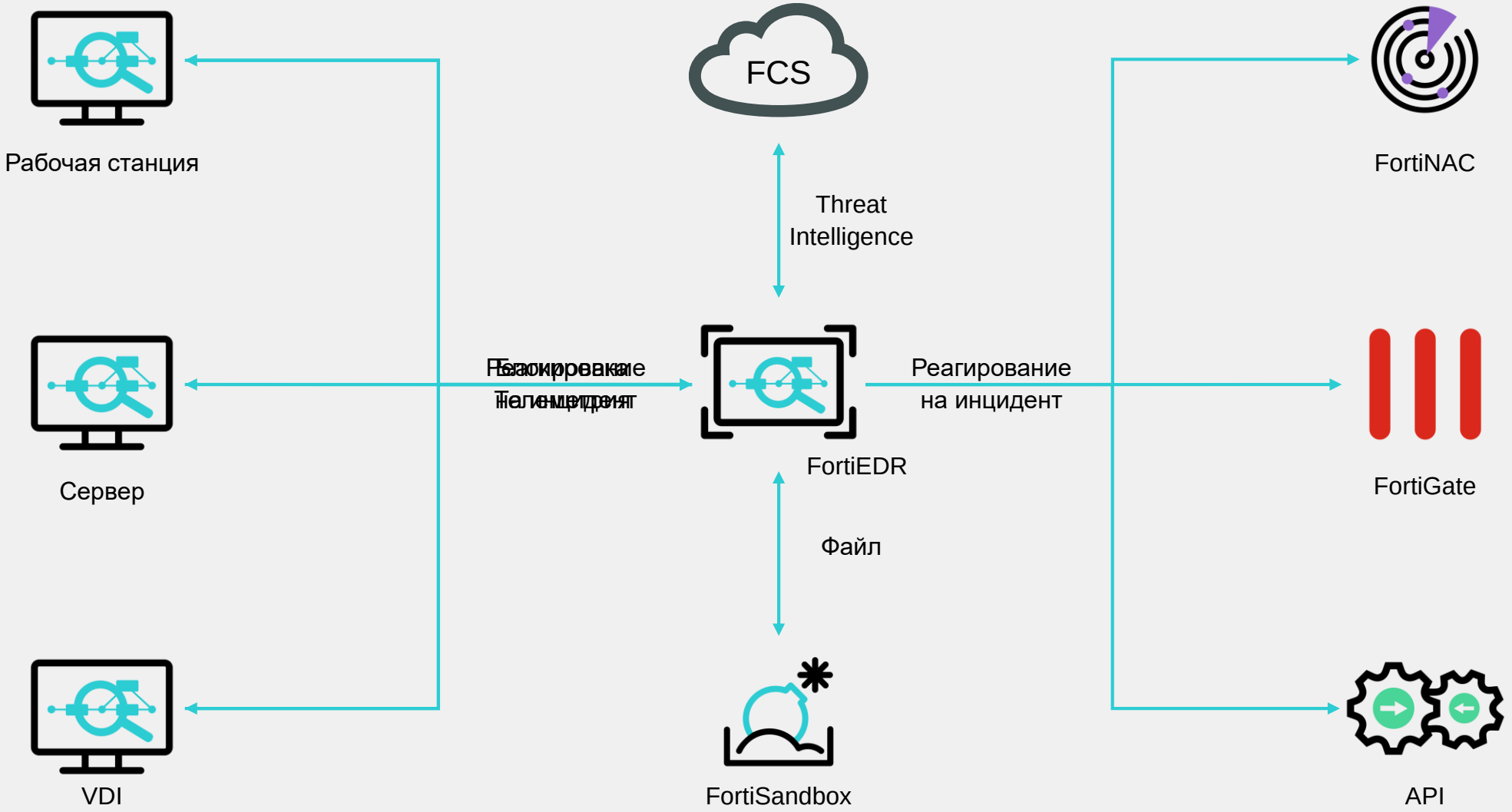
EDR и/или EPP?



FortiEDR

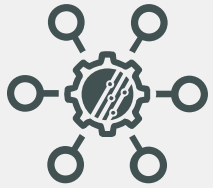


FortiEDR


Рабочая станция
Сервер
VDI
FCS
Threat
Intelligence
FortiEDR
Файл
FortiSandbox
Реагирование
на инцидент
FortiNAC
FortiGate
API

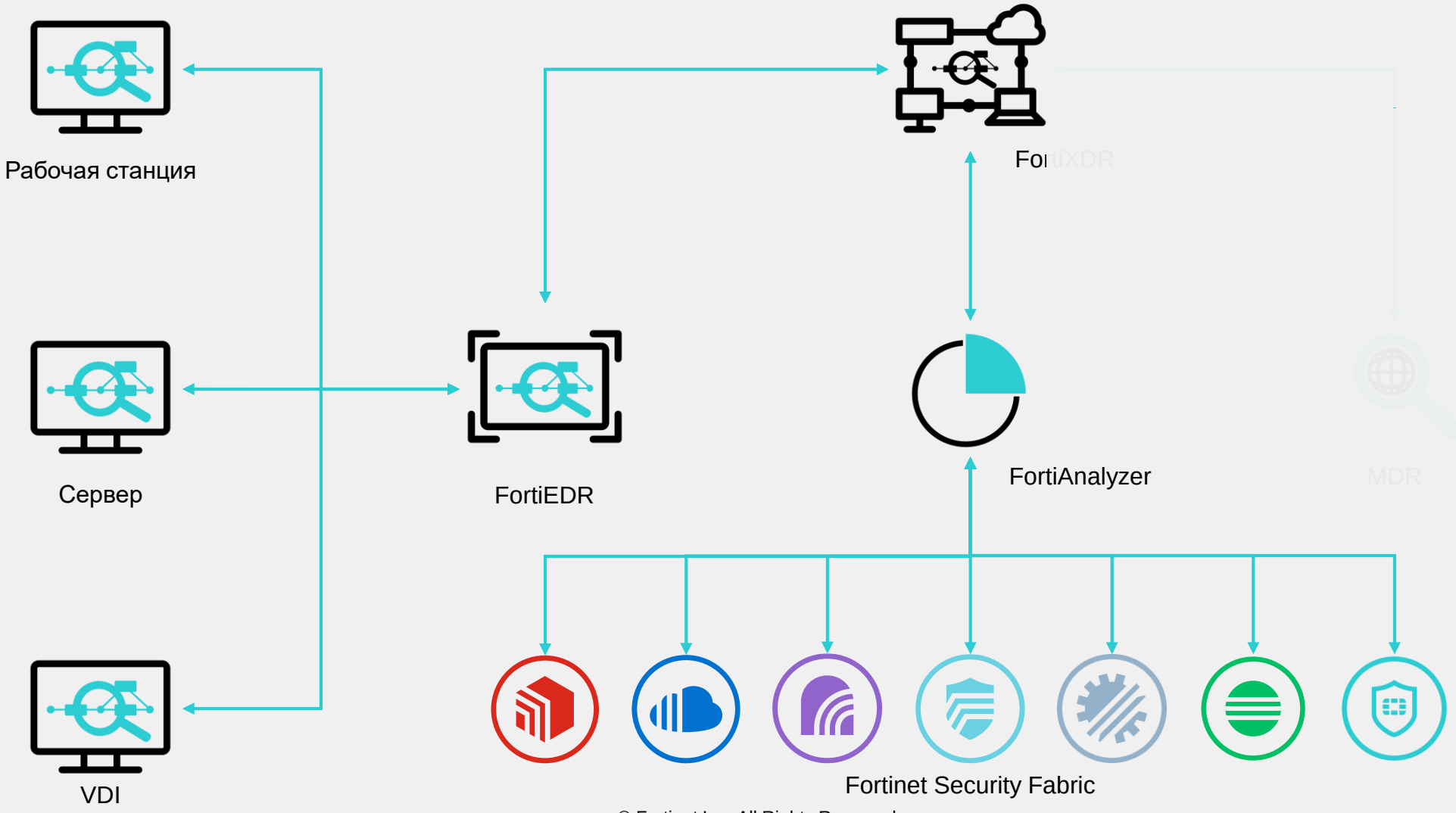
Расширенные обнаружение и реагирование

FortiEDR

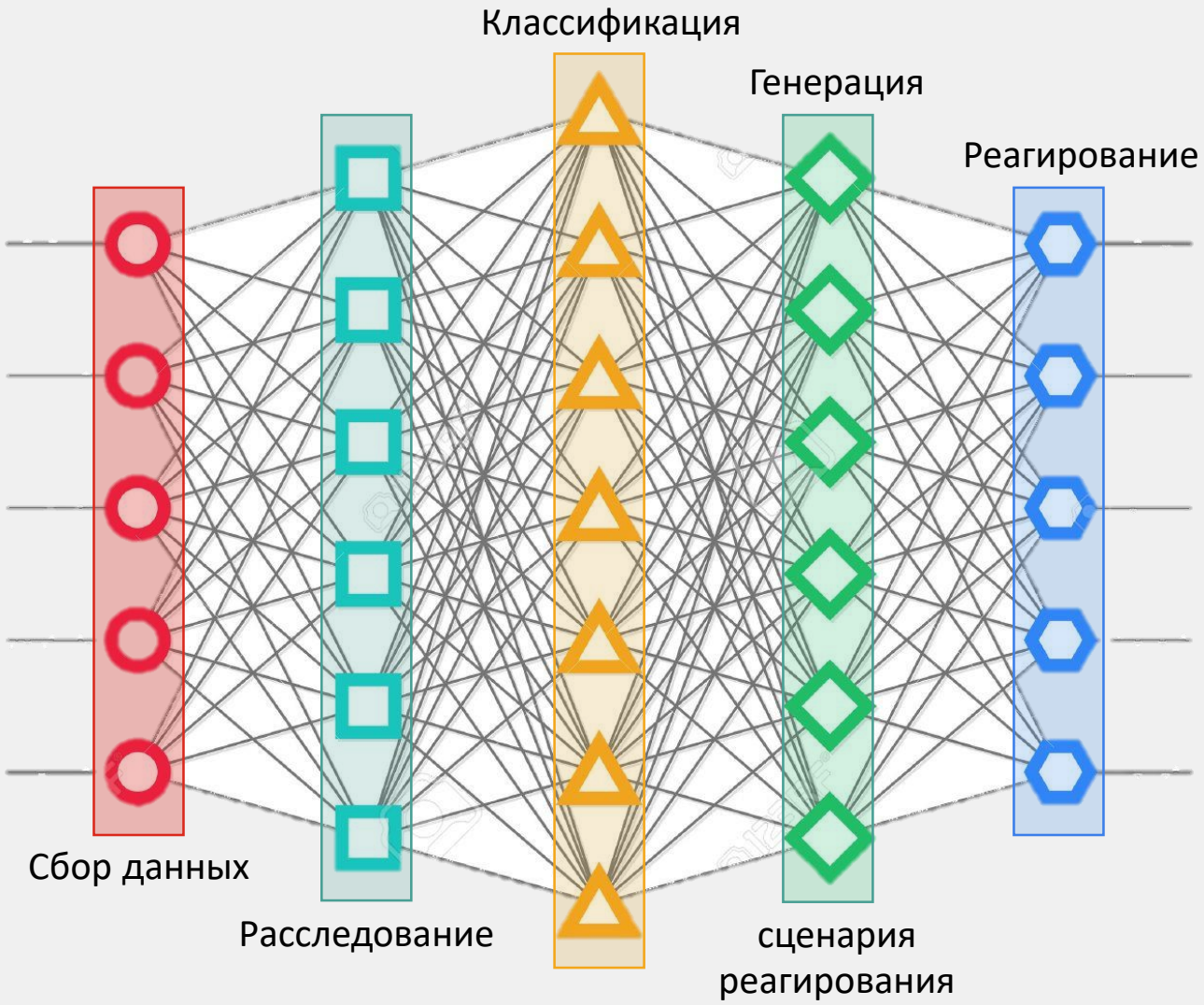


Fortinet Security Fabric

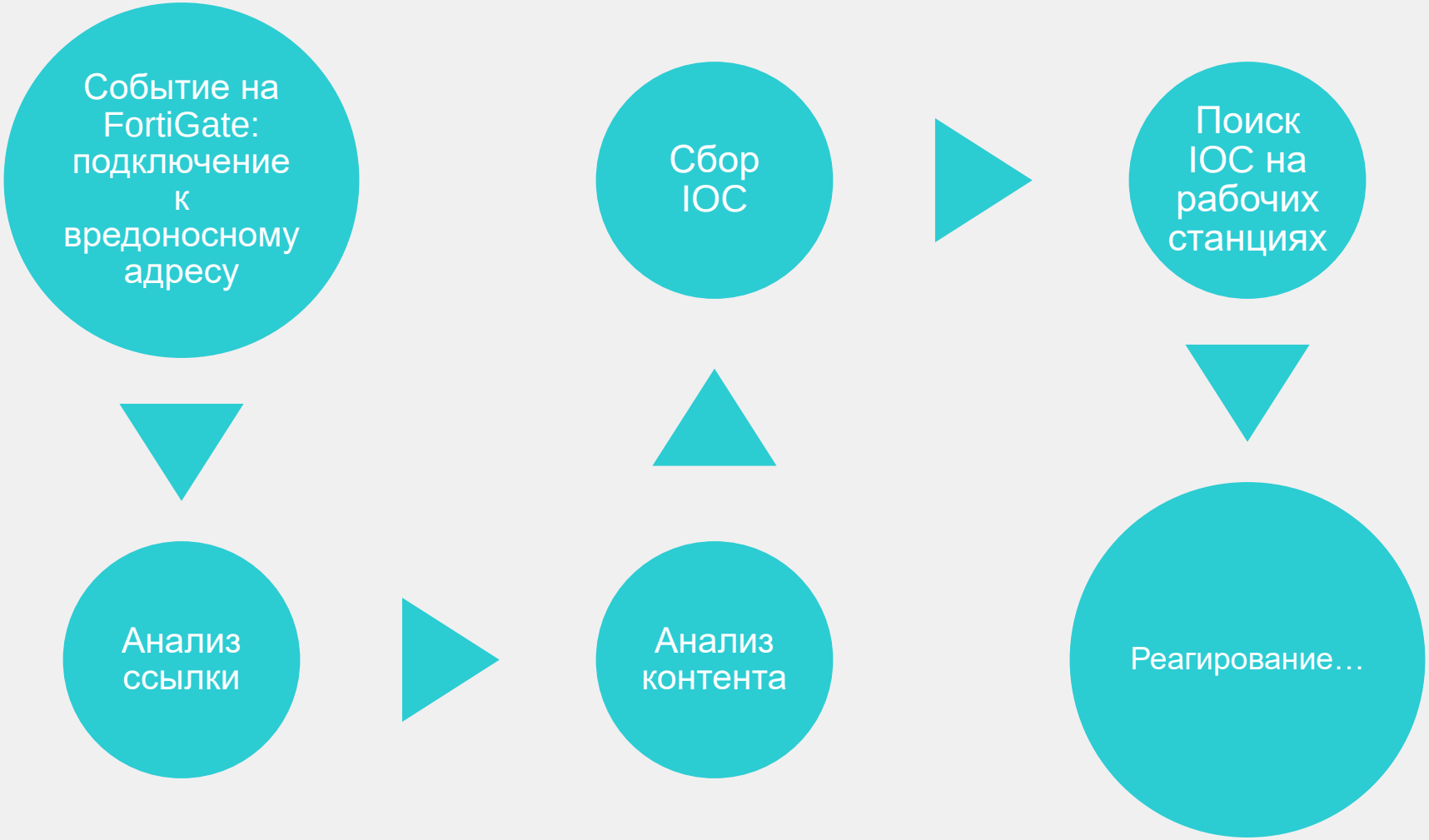
FortiXDR



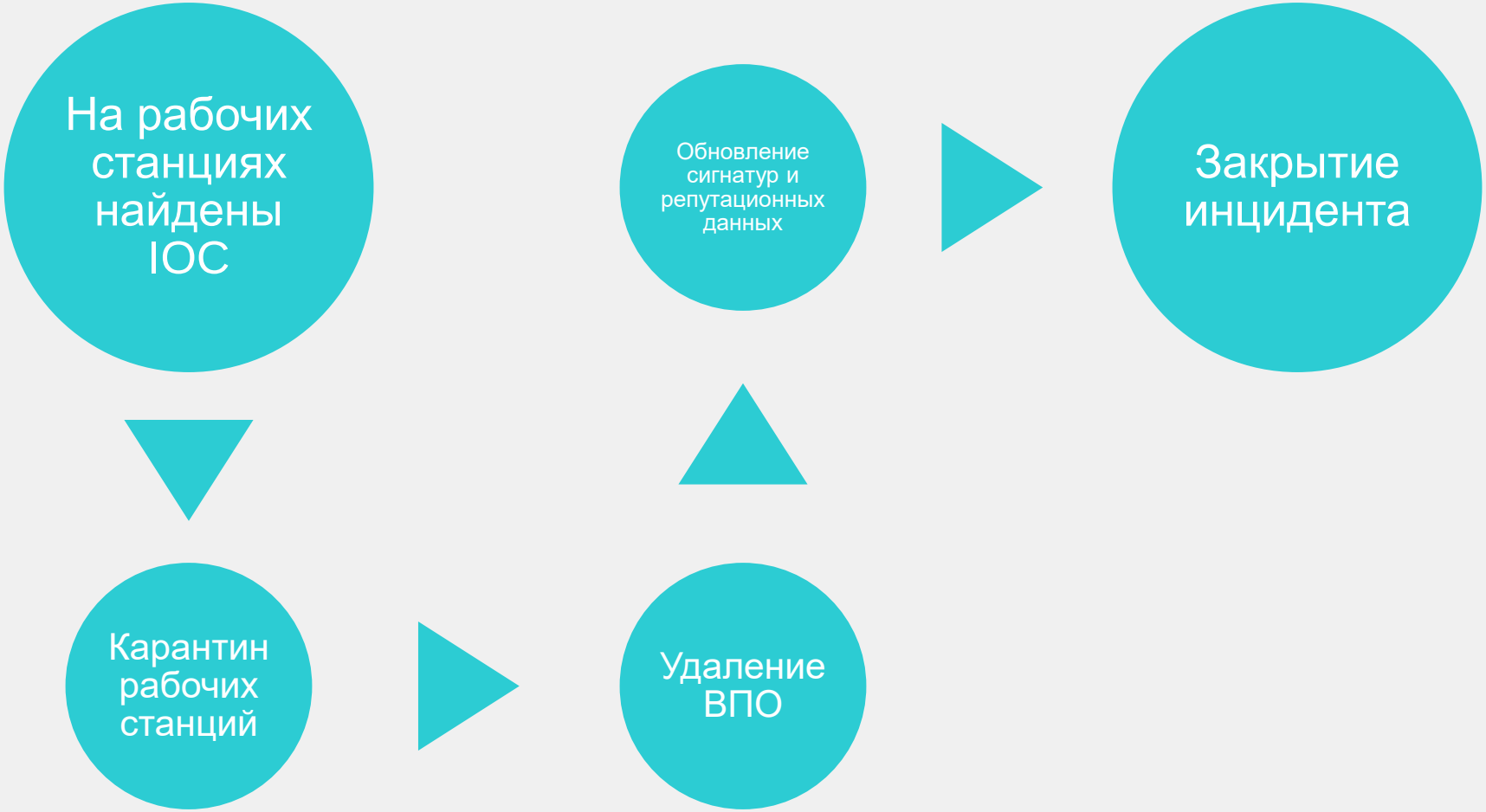
ANN



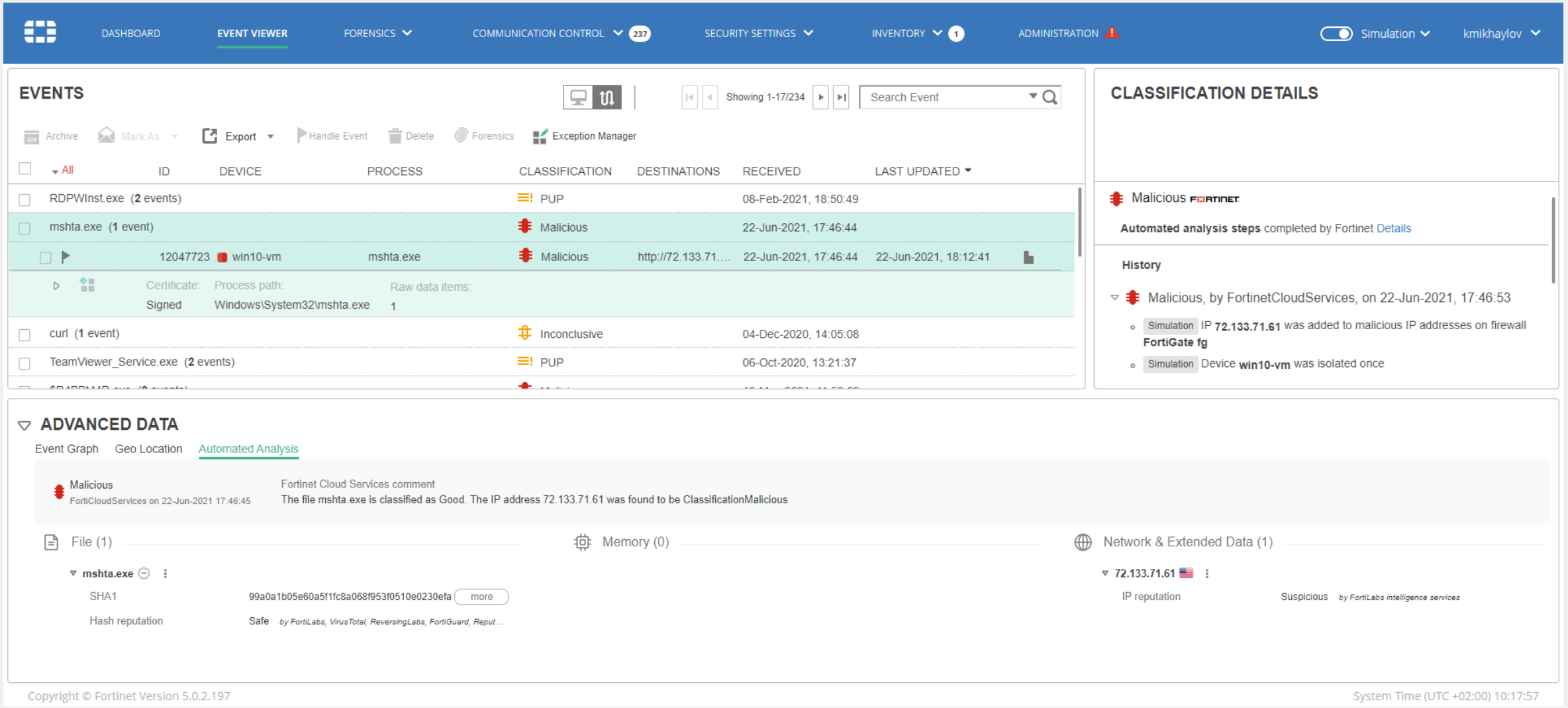
FortiXDR: пример расследования



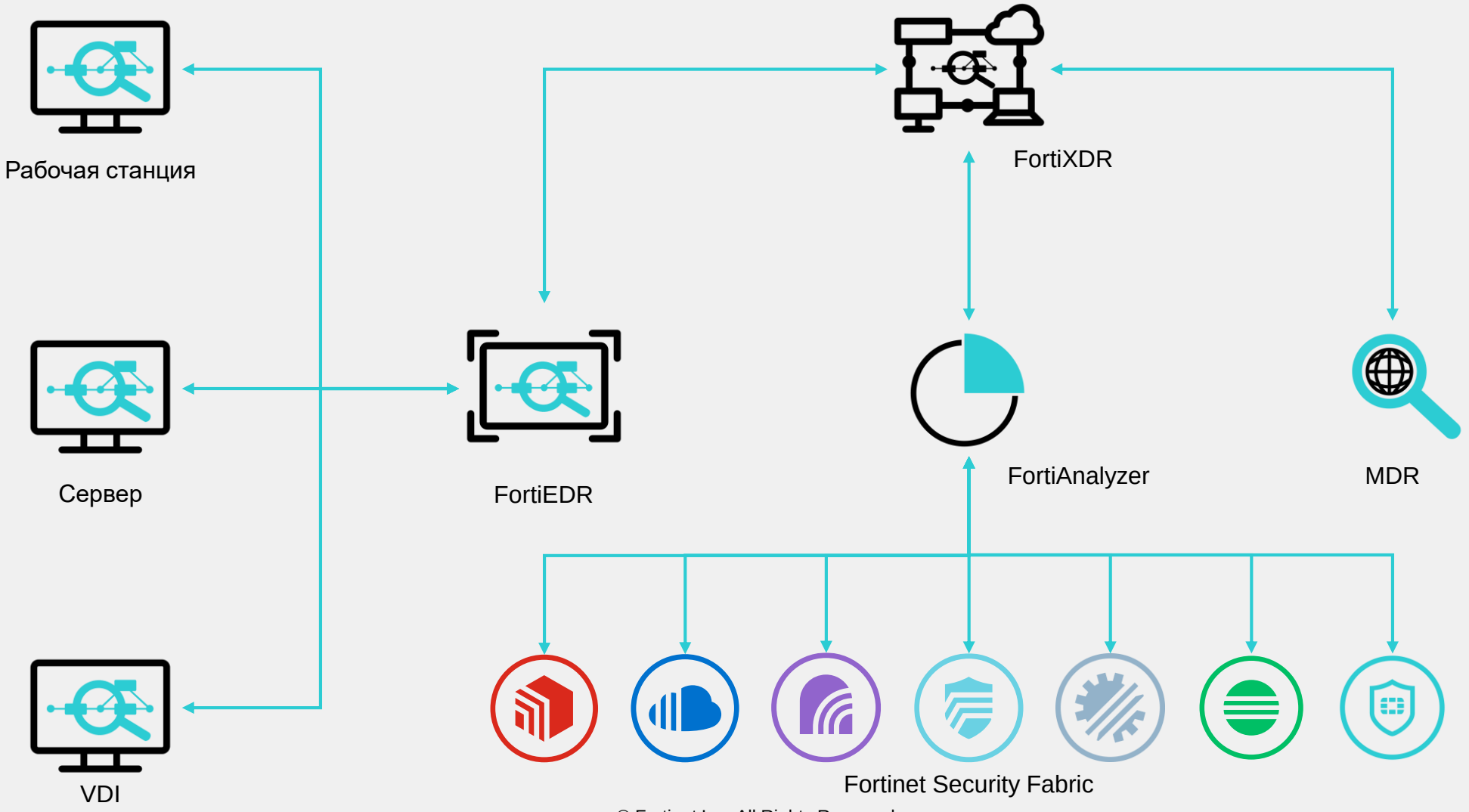
FortiXDR: пример реагирования



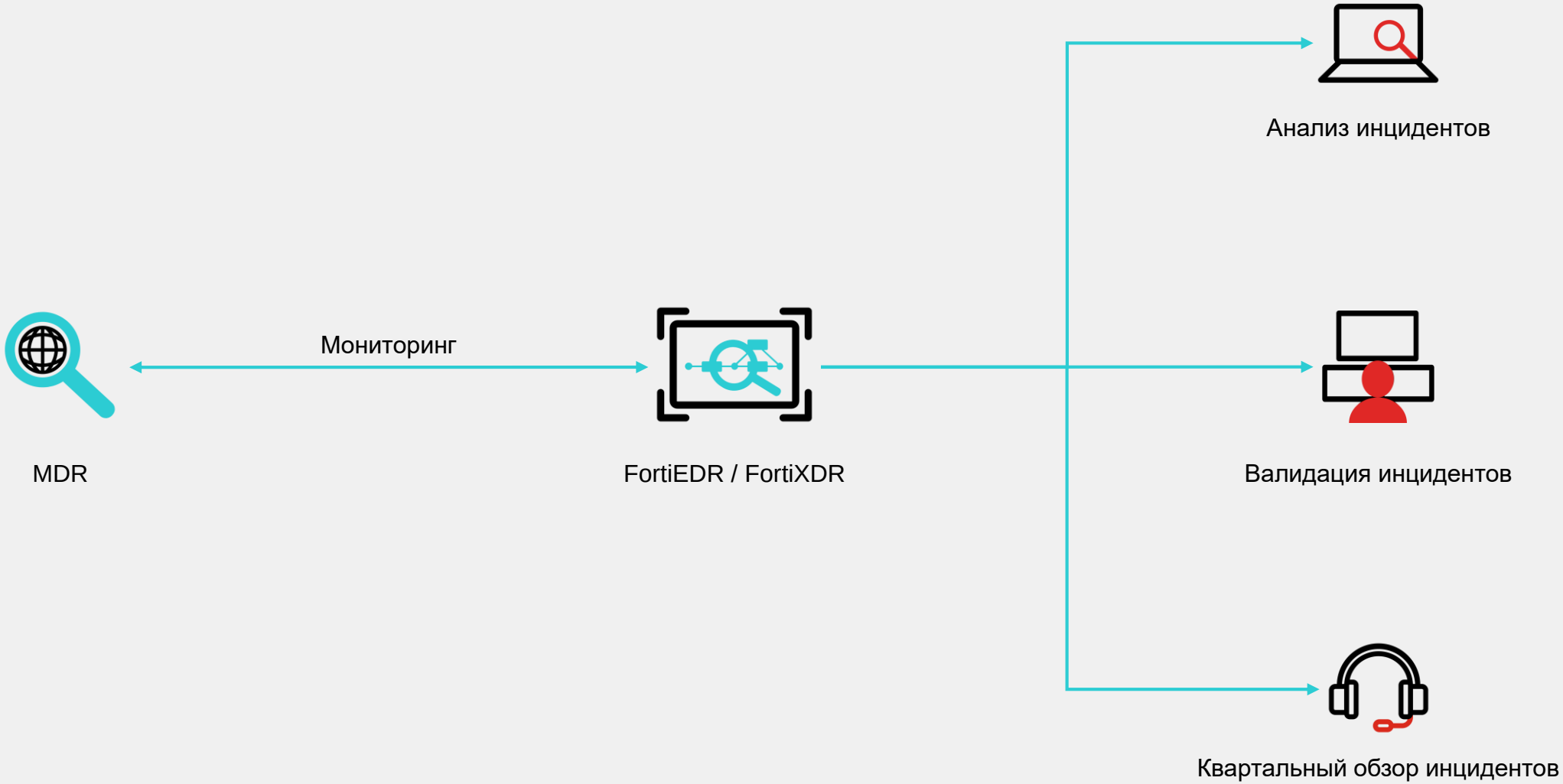
FortiXDR



FortiEDR



Сервис MDR


Анализ инцидентов
Мониторинг
MDR
FortiEDR / FortiXDR
Валидация инцидентов
Квартальный обзор инцидентов

Независимое

тестирование

Тестирование EDR решений

- Новость: https://therecord.media/state-of-the-art-edrs-are-not-perfect-fail-to-detect-common-attacks/?__cf_chl_jschl_tk__=4HIL4eDYh2NMoRJdiRj5Q1QoR.it9suyOxI9BSIXLCU-1642758123-0-gaNycGzNCiU

- Вебкаст: https://www.fortinet.com/resources-campaign/ai-driven-security-operations/webcast-hear-it-yourself-researchers-cover-their-edr-assessment?bypassCta=

EDR	CPL	HTA	EXE	DLL
BitDefender GravityZone Plus	✗	✗	✓	✗
Carbon Black Response	•	✗	✓	✓
Check Point Harmony	✗	◇	✗	✓
Cisco AMP	✗	✗	✓	⊙
Comodo OpenEDR	✗	✓	✗	✓
CrowdStrike Falcon	✓	✓	✗	✓
Elastic EDR	✗	✓	✓	✗
F-Secure Elements Endpoint Detection and Response	◇	†	✓	✗
FortiEDR	✗	✗	✗	✗
Microsoft Defender for Endpoints	⋆	✗	✗	✓
Panda Adaptive Defense 360	✗	✓	⋆	✓
Sentinel One (without test features)	✓	✓	✓	✗
Sentinel One (with test features)	✗	✗	✗	✗
Sophos Intercept X with EDR	✗	✗	✓	-
Trend micro Apex One	•	•	✓	✓
Endpoint Protection				
ESET PROTECT Enterprise	✗	✗	✓	✓
F-Secure Elements Endpoint Protection Platform	✓	✓	✓	✓
Kaspersky Endpoint Security	✗	✗	✗	✓
McAfee Endpoint Protection	✗	✗	✓	✓
Symantec Endpoint Protection	✓	✗	✓	✓

Table 1: Aggregated results of the attacks for each tested solution.
Notation: ✓: Successful attack,◇ Successful attack, raised medium alert, •: Successful attack, raised minor alert, ⋆: Successful attack, alert was raised ○:Unsuccessful attack, no alert raised, ✗: failed attack, alerts were raised. † In two experiments supplied by the vendor, in the first it was detected after five hours, in the second it was detected after 25 minutes. ⊙ Initial test was blocked due to file signature, second one was successful with another application.


FORTINET