Fast Track Program

Проактивная защита конечных точек: защита, видимость и контроль критически важных активов

Aleksey Maltsev, Olesya Tarabrina

11.12.20

CIS

Проактивная защита конечных точек: защита, видимость и контроль критически важных активов

Objectives

- Конечные точки – сценарии использования
- Доказанная в отрасли эффективность
- FortiEDR
- FortiClient Endpoint
- FortiClient EMS

Конечные точки – сценарии использования

Потребность в видимости, контроле и защите

Конечные точки остаются целью атак

44% опрошенных компаний признали, что за последние 24 месяца была взломана одна или несколько конечных точек[1]

30% нарушений включают вредоносное ПО[2]

От WannaCry к WannaMine.

Влияние вредоносного ПО класса «криптоджекинг» удваивается до **28%**[3]

Sources:
[1] SANS Institute Stage of Endpoint Security survey 2016
[2] Verizon DBIR 2020 – out of 157,525 incidents
[3] FortiGuard Labs Quarterly threat report, Q1 2018

Пробелы в безопасности конечных точек

Ponemon INSTITUTE

63% компаний не могут отслеживать конечные точки вне сети, более половины не могут определить статус их соответствия требованиям безопасности

Недостаток видимости

According to Gartner

В течение 2021 **99%** используемых уязвимостей будут оставаться известными специалистам по безопасности и ИТ в течение как минимум одного года

Уязвимости

verizon

87%

Большинство компрометаций заняло несколько минут или меньше

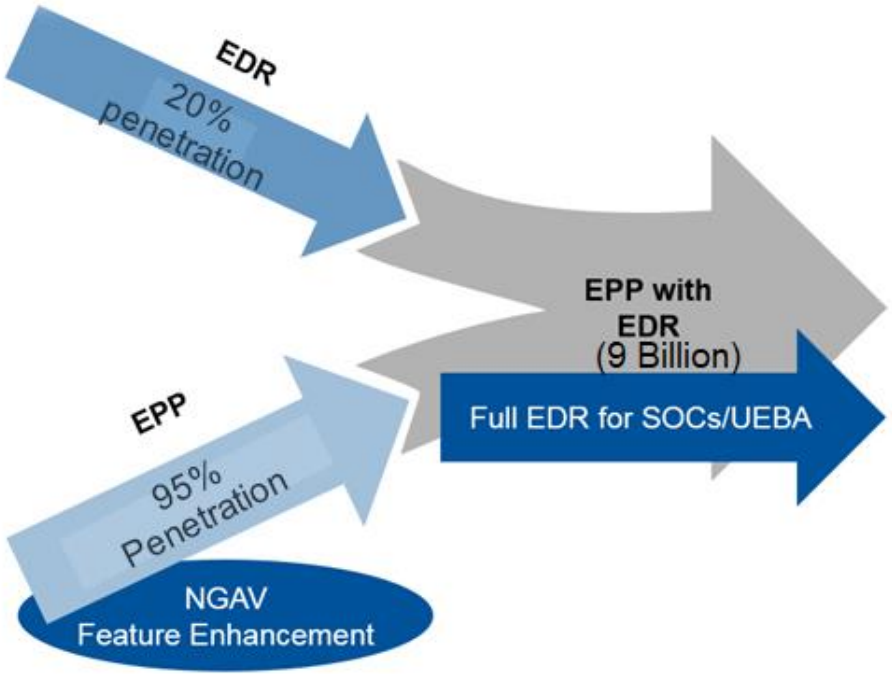
Атаки происходят быстро

Sources:

1. The Cost Of Insecure Endpoints, Ponemon Institute, 2017
2. Gartner, How to Respond to the 2018 Threat Landscape, Greg Young, 28 November, 2017
3. Breach Investigation Report, Verizon, 2018

Обзор технологий

Платформа Advanced Endpoint Protection Platform (EPP) с функциями автоматического обнаружения и реагирования



Endpoint Detection and Response (EDR)

1. Запись и сохранение поведения и событий с конечных точек
2. Обнаружение инцидентов безопасности
3. Реагирование –
    1. Сдерживание и исправление/восстановление
    2. Форензика - расследование инцидентов безопасности, анализ первопричин

Endpoint Protection Platform (EPP)

1. Предотвращение ВПО на основе файлов
2. **Обнаружение** и блокирование вредоносных действий доверенных и ненадежных приложений
3. Обеспечение функциональности расследования и восстановления с целью **реагирования** на инциденты безопасности и предупреждения

Доказанная в отрасли эффективность

Результат стороннего тестирования

#1 в последних сравнительных рейтингах AV Comparatives

Fortinet - No.1 в тесте
AV Comparative Real World Test

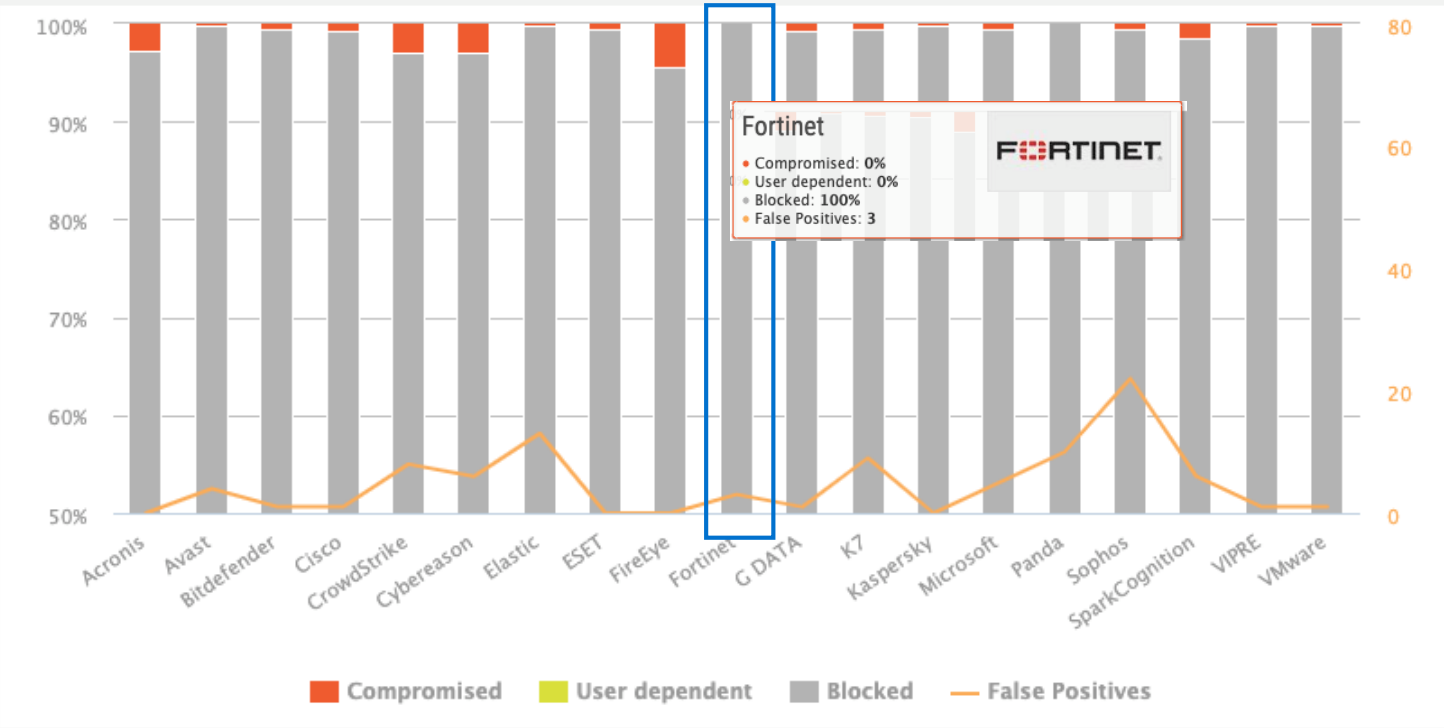
- ✓ 100% - рейтинг блокировки
- ✓ Наименьшее количество false positive (3)

NSS Labs – рейтинг AA

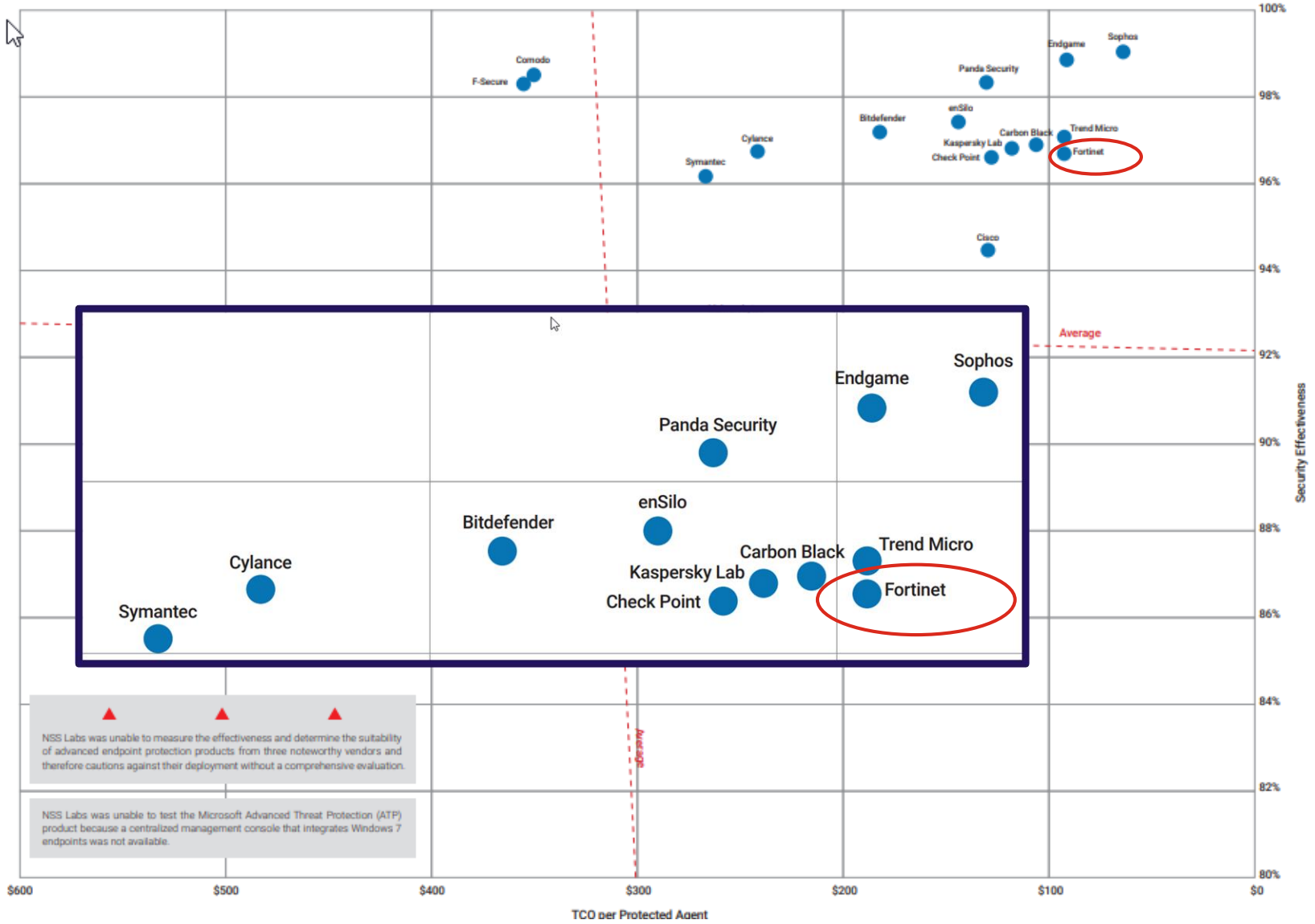
Test Results

Real-World Protection Test (March-April)

This fact sheet gives a brief overview of the results of the Business Real-World Protection Test run in March and April 2020. The overall business product reports (each covering four months) will be released in July and December. For more information about this Real-World Protection Test, please read the details available at https://www.av-comparatives.org. The results are based on a test set consisting of **403** test cases (such as malicious URLs), tested from the beginning of March till the end of April.



AEP 2.0 Security Value Map 2019



FORTINET
FortiClient v5.6.2
ADVANCED ENDPOINT PROTECTION
NSS LABS
RECOMMENDED
APR 2018

Безопасность конечных точек и ландшафт угроз

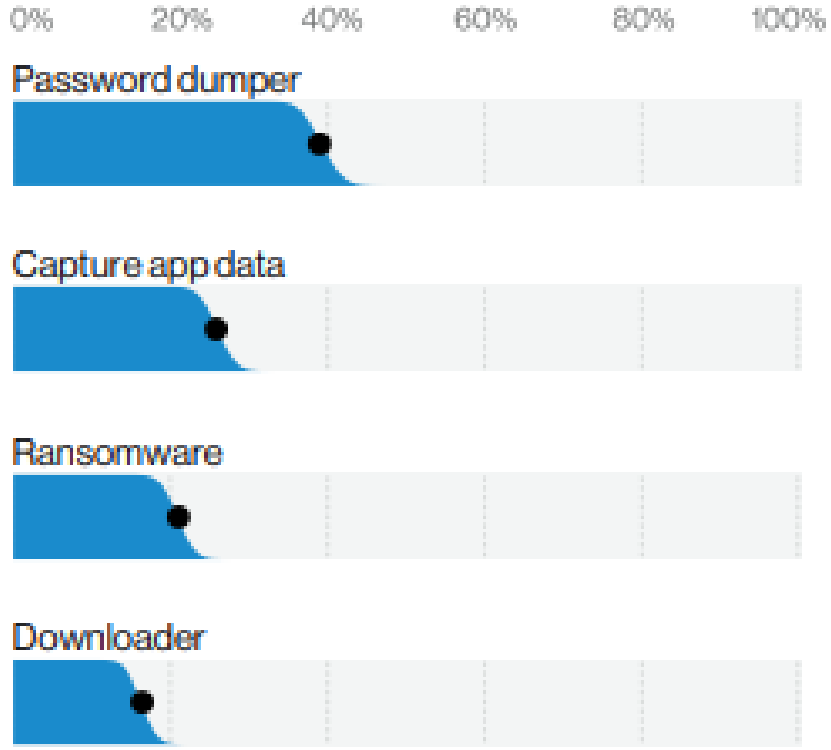


Figure 16. Top Malware varieties in breaches (n = 506)

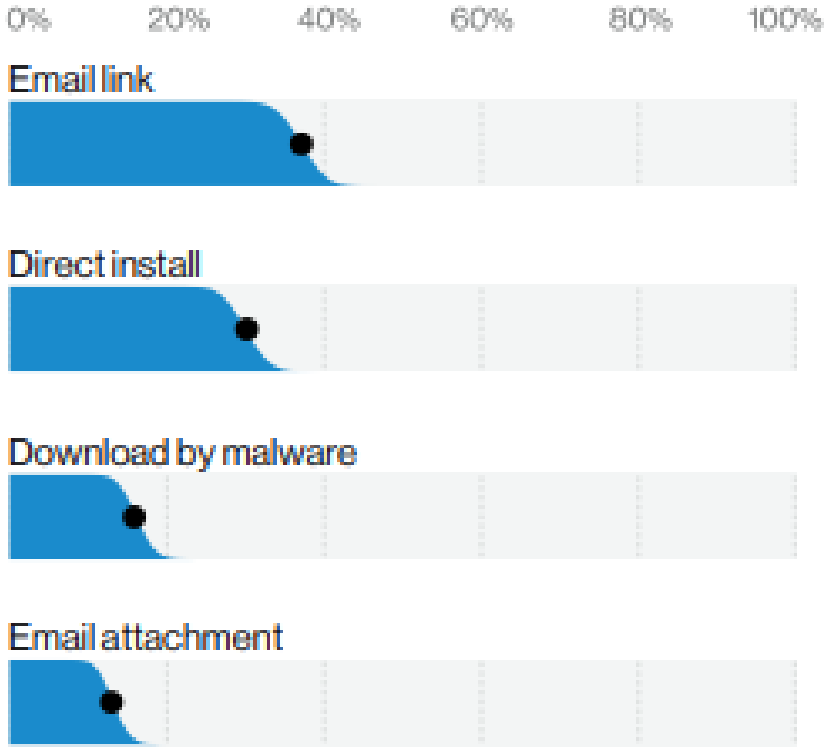


Figure 17. Top Malware vectors in breaches (n = 360)

Результаты тестирования FortiClient NSS Labs AEP:
Exploits: 100%
HTTP: 100%
Evasions: 100%

Source: Verizon DBIR 2020
NSS Labs AEP Test 2019

Компоненты и варианты использования Endpoint Security

Fortinet Security Fabric Integration

FortiGate, FortiSandbox, FortiAnalyzer, FortiAuthenticator

FortiGuard Services

CPRL AV, Web Filtering, App Firewall, Vulnerability Management

1	2	3
Видимость конечных точек / IoT и контроль соответствия	**Безопасный удаленный доступ**	**Защита конечных точек / Расширенная защита от угроз**
FortiClient Fabric Agent **FortiGate** **FortiNAC** **FortiAnalyzer** **Fabric Partners**	**FortiClient** **FortiGate** **FortiAuthenticator**	**FortiClient** **FortiGate** **FortiSandbox**

3

ENDPOINT PROTECTION (EPP)

App FW, Anti-malware, Anti-exploit, Web Filtering

ADVANCED THREAT PROTECTION

Sandbox Integration

2

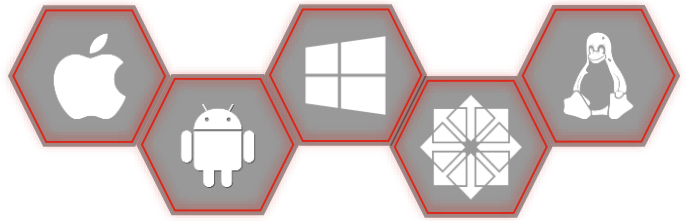
SECURE REMOTE ACCESS

SSL & IPSec VPN, SSO

1

FABRIC AGENT

Telemetry, Quarantine, Vulnerability, App Inventory



ENDPOINT DEVICES **HOSTS / SERVERS**

FortiEDR

Автоматическое обнаружение угроз и реагирование на них в режиме реального времени

FortiEDR – В реальном времени & Автоматически

Самовосстановление конечных точек

Pre-Infection

Discover & Predict

Проактивное снижение рисков

- Обнаружение мошеннических устройств & IoT
- Уязвимости
- Виртуальное исправление

Prevent

Защита до исполнения

- Уровень ядра
- Машинное обучение AV

Post-Infection/ Post Execution

Detect

Безфайловые и сложные угрозы

- На основе поведения
- Обнаружение атак на основе памяти
- Классификация угроз

Defuse

Остановка взлома и действий программ-вымогателей

- Блокировка вредоносных действий
- Предотвращение потери данных
- Нулевое время пребывания

Respond & Investigate

Полная видимость атаки

- Автоматизация с использованием playbook
- Форензика
- Threat hunting
- Аналитика больших данных

Remediate & Roll back

Автоматическая дезинфекция

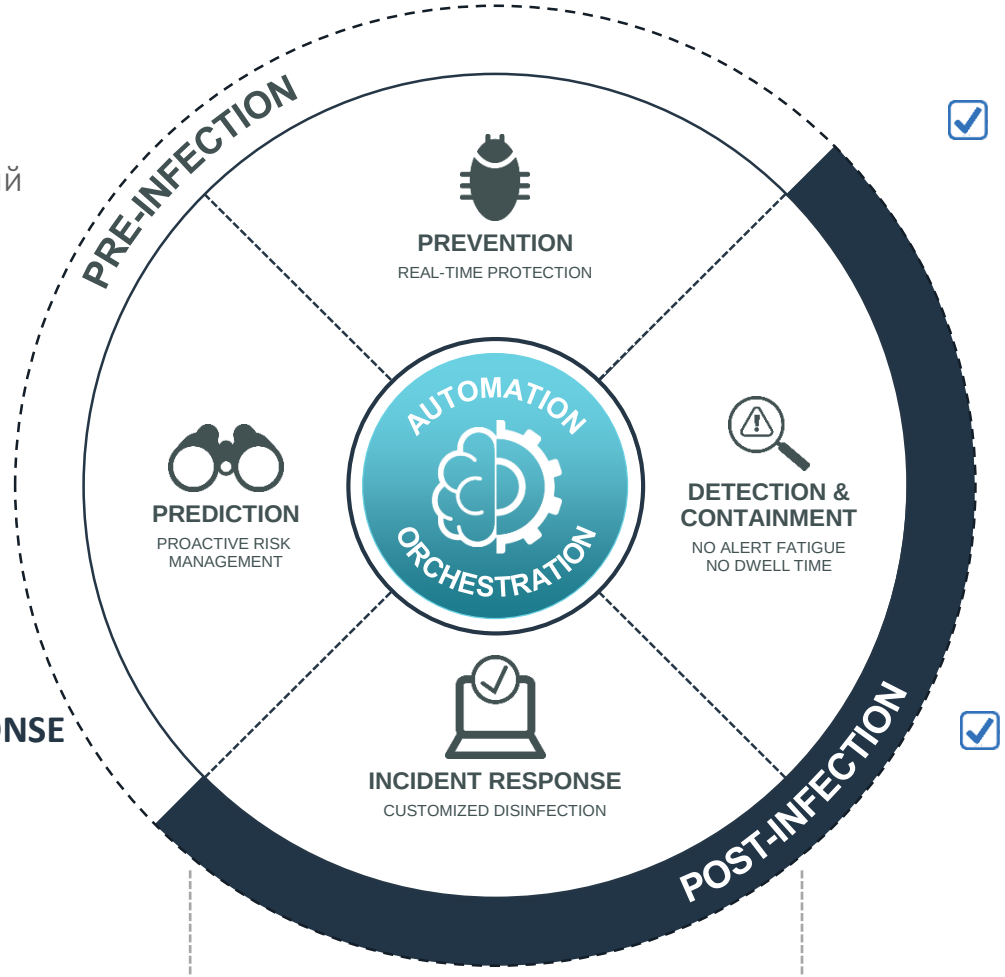
- Очистка / возврат к исходному состоянию
- Исключение перезаливки / пересборки
- Минимизация прерывания бизнеса

Automation | Cloud/Hybrid/air-gap deployment | OS coverage

Автоматическая безопасность в реальном времени с организованным реагированием на инциденты

REAL-TIME PROACTIVE RISK MITIGATION

- Обнаружение и отслеживание приложений и IoT-устройств
- Обогащение данных о CVE и рейтинге приложений
- Проактивные политики, основанные на рисках, позволяющие уменьшить поверхность атаки



REAL-TIME PREVENTION

- Машинное обучение, AV следующего поколения на основе ядра
- Фиды из постоянно обновляемой облачной базы данных
- Автоматическое предотвращение шифрования программами-вымогателями в реальном времени

REAL-TIME ORCHESTRATED INCIDENT RESPONSE

- Автоматическая классификация событий
- Автоматическое исправление (уведомить пользователей, изолировать устройство, исправить устройство, открыть заявку)
- Автоматическое расследование с минимальным прерыванием для пользователя

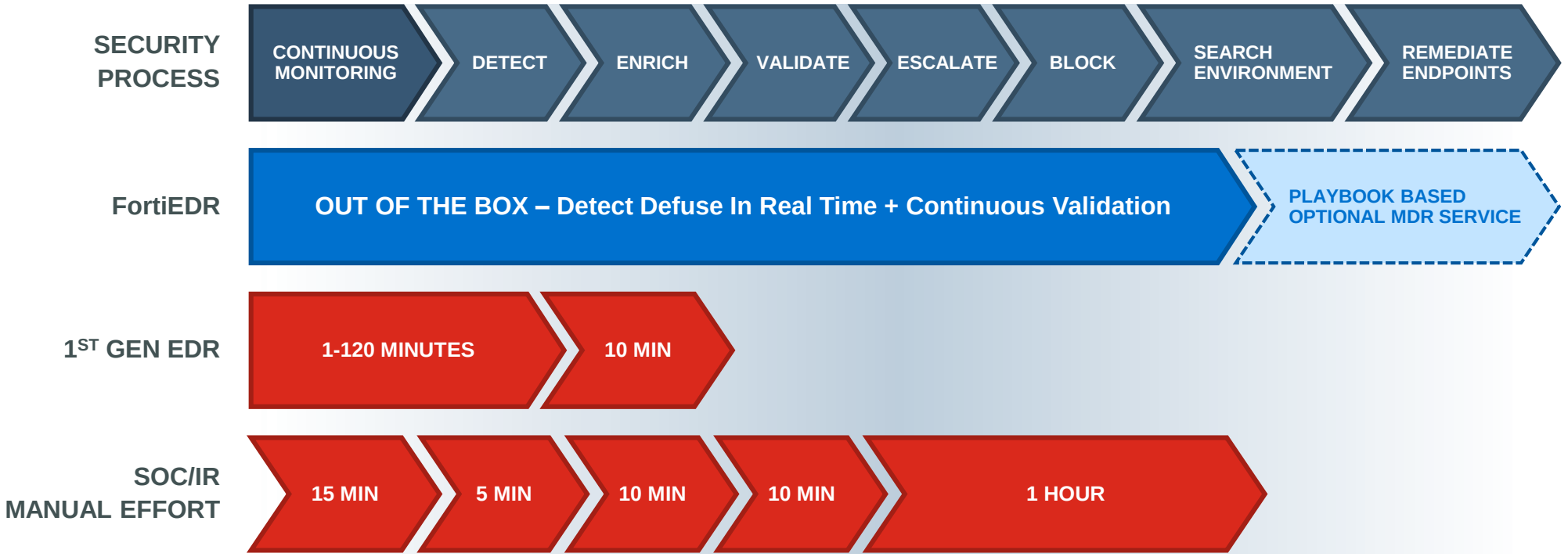
REAL-TIME DETECTION AND CONTAINMENT

- Автоматическое обнаружение и блокировка заражения
- ОС-ориентированная технология
- Анализ всей истории журнала
- Хирургическая защита

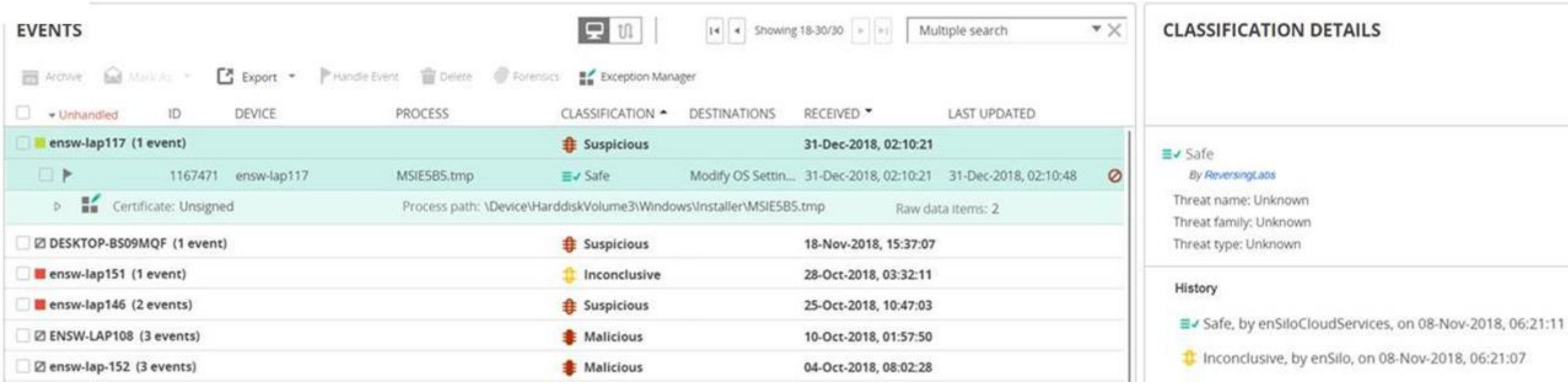
CLOUD, ON-PREMISES OR HYBRID MANAGEMENT

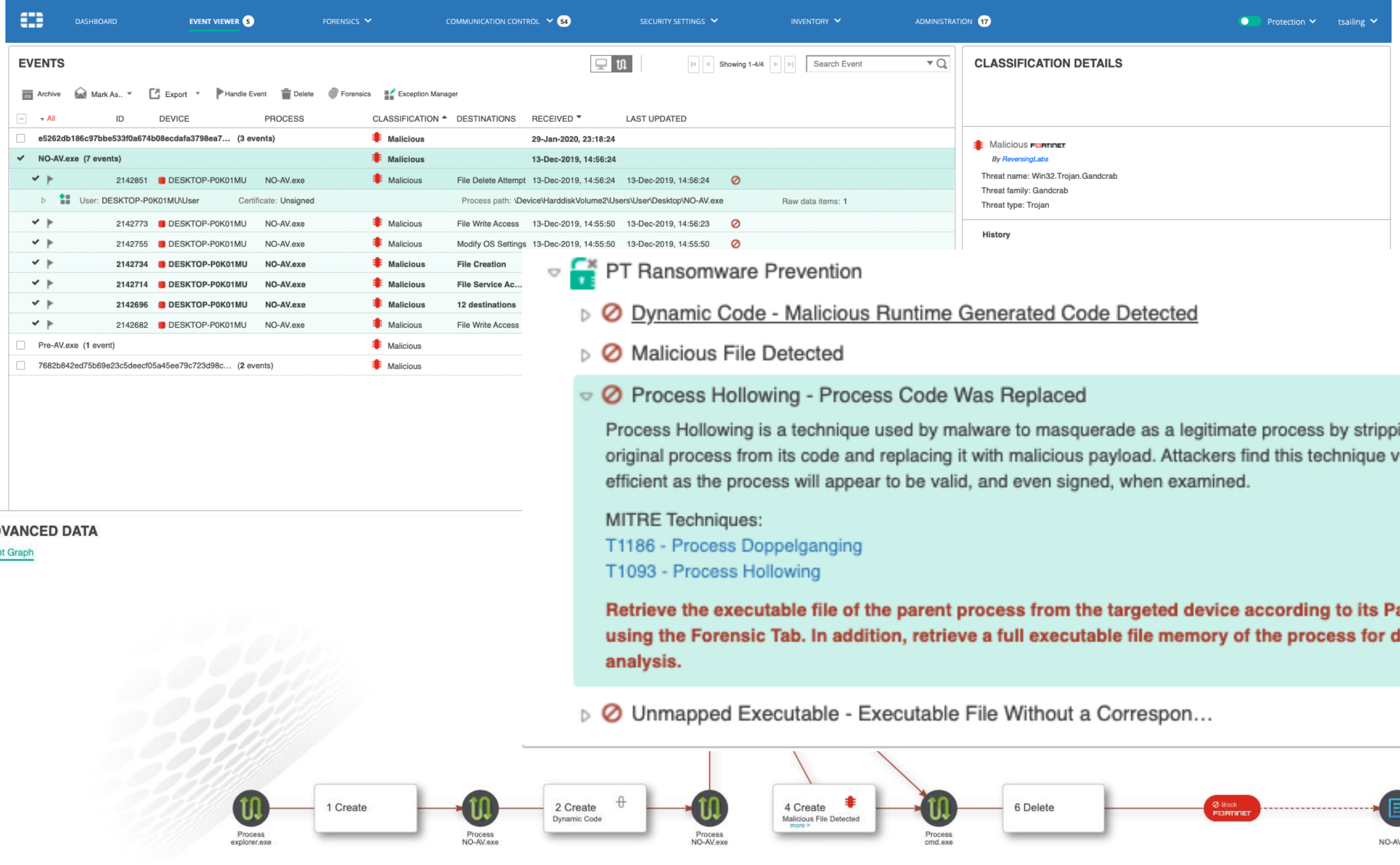
LIGHTWEIGHT AGENT

Ручное реагирование vs. Автоматическое реагирование

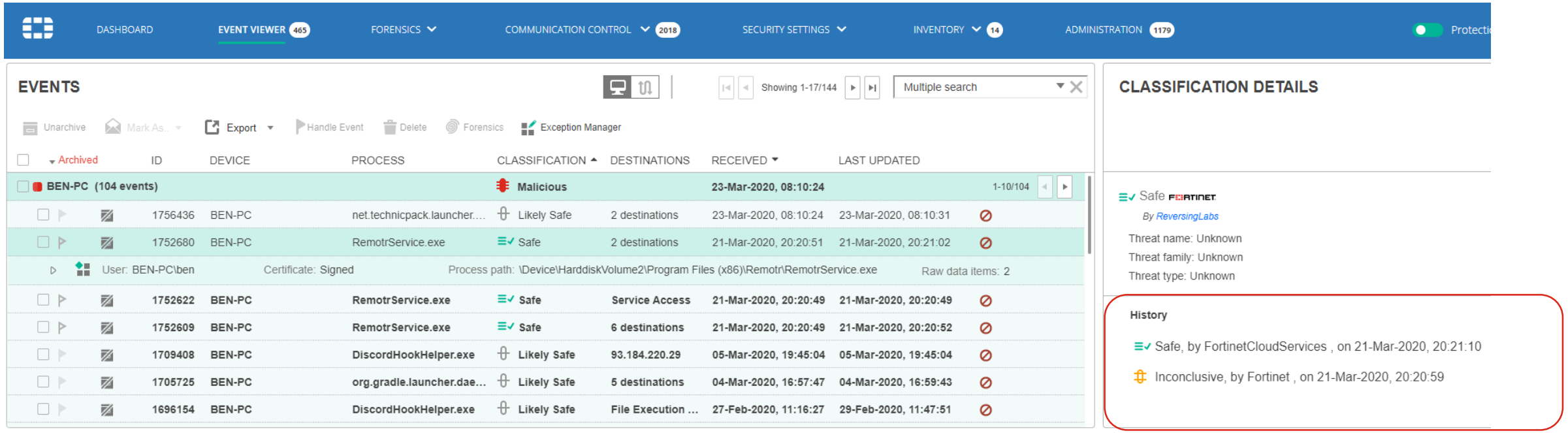


Уменьшение шума и повышение зрелости SOC

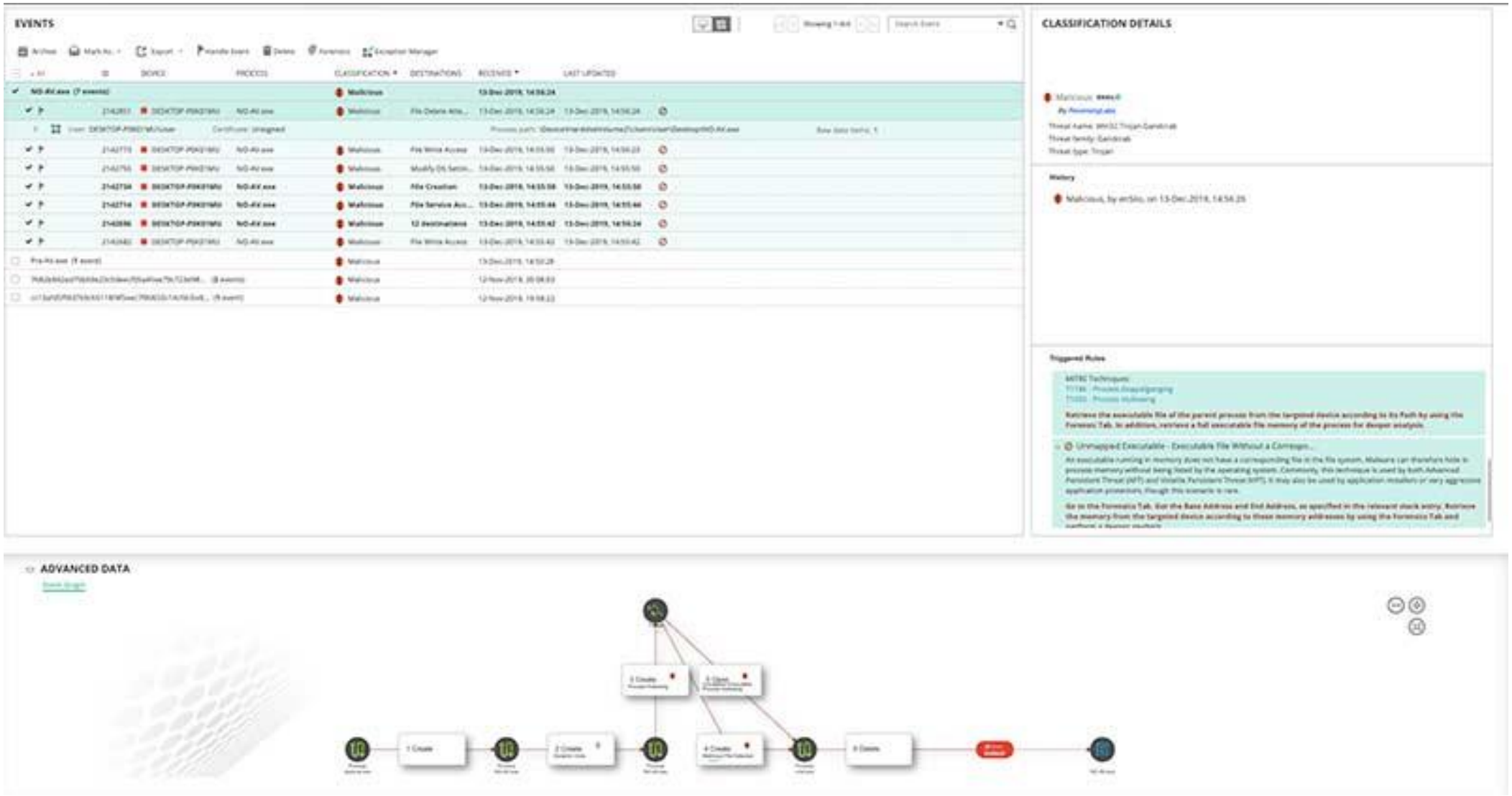



DASHBOARD
EVENT VIEWER 5
FORENSICS
COMMUNICATION CONTROL 54
SECURITY SETTINGS
INVENTORY
ADMINISTRATION 17
Protection
tsailing
EVENTS
Showing 1-4/4
Search Event
Archive
Mark As..
Export
Handle Event
Delete
Forensics
Exception Manager
All
ID
DEVICE
PROCESS
CLASSIFICATION
DESTINATIONS
RECEIVED
LAST UPDATED
e5262db186c97bbe533f0a674b08ecdafa3798ea7... (3 events)
Malicious
29-Jan-2020, 23:18:24
NO-AV.exe (7 events)
Malicious
13-Dec-2019, 14:56:24
2142851 DESKTOP-P0K01MU NO-AV.exe Malicious File Delete Attempt 13-Dec-2019, 14:56:24 13-Dec-2019, 14:56:24
User: DESKTOP-P0K01MU\User
Certificate: Unsigned
Process path: \Device\HarddiskVolume2\Users\User\Desktop\NO-AV.exe
Raw data items: 1
2142773 DESKTOP-P0K01MU NO-AV.exe Malicious File Write Access 13-Dec-2019, 14:55:50 13-Dec-2019, 14:56:23
2142755 DESKTOP-P0K01MU NO-AV.exe Malicious Modify OS Settings 13-Dec-2019, 14:55:50 13-Dec-2019, 14:55:50
2142734 DESKTOP-P0K01MU NO-AV.exe Malicious File Creation
2142714 DESKTOP-P0K01MU NO-AV.exe Malicious File Service Ac...
2142696 DESKTOP-P0K01MU NO-AV.exe Malicious 12 destinations
2142682 DESKTOP-P0K01MU NO-AV.exe Malicious File Write Access
Pre-AV.exe (1 event)
Malicious
7682b842ed75b69e23c5deecf05a45ee79c723d98c... (2 events)
Malicious
CLASSIFICATION DETAILS
Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Gandcrab
Threat family: Gandcrab
Threat type: Trojan
History
PT Ransomware Prevention
Dynamic Code - Malicious Runtime Generated Code Detected
Malicious File Detected
Process Hollowing - Process Code Was Replaced
Process Hollowing is a technique used by malware to masquerade as a legitimate process by stripping the original process from its code and replacing it with malicious payload. Attackers find this technique very efficient as the process will appear to be valid, and even signed, when examined.
MITRE Techniques:
T1186 - Process Doppelganging
T1093 - Process Hollowing
Retrieve the executable file of the parent process from the targeted device according to its Path by using the Forensic Tab. In addition, retrieve a full executable file memory of the process for deeper analysis.
Unmapped Executable - Executable File Without a Correspon...
ADVANCED DATA
Event Graph
Process explorer.exe
1 Create
Process NO-AV.exe
2 Create
Dynamic Code
Process NO-AV.exe
4 Create
Malicious File Detected
more >
Process cmd.exe
6 Delete
Block FORTINET
NO-AV.exe

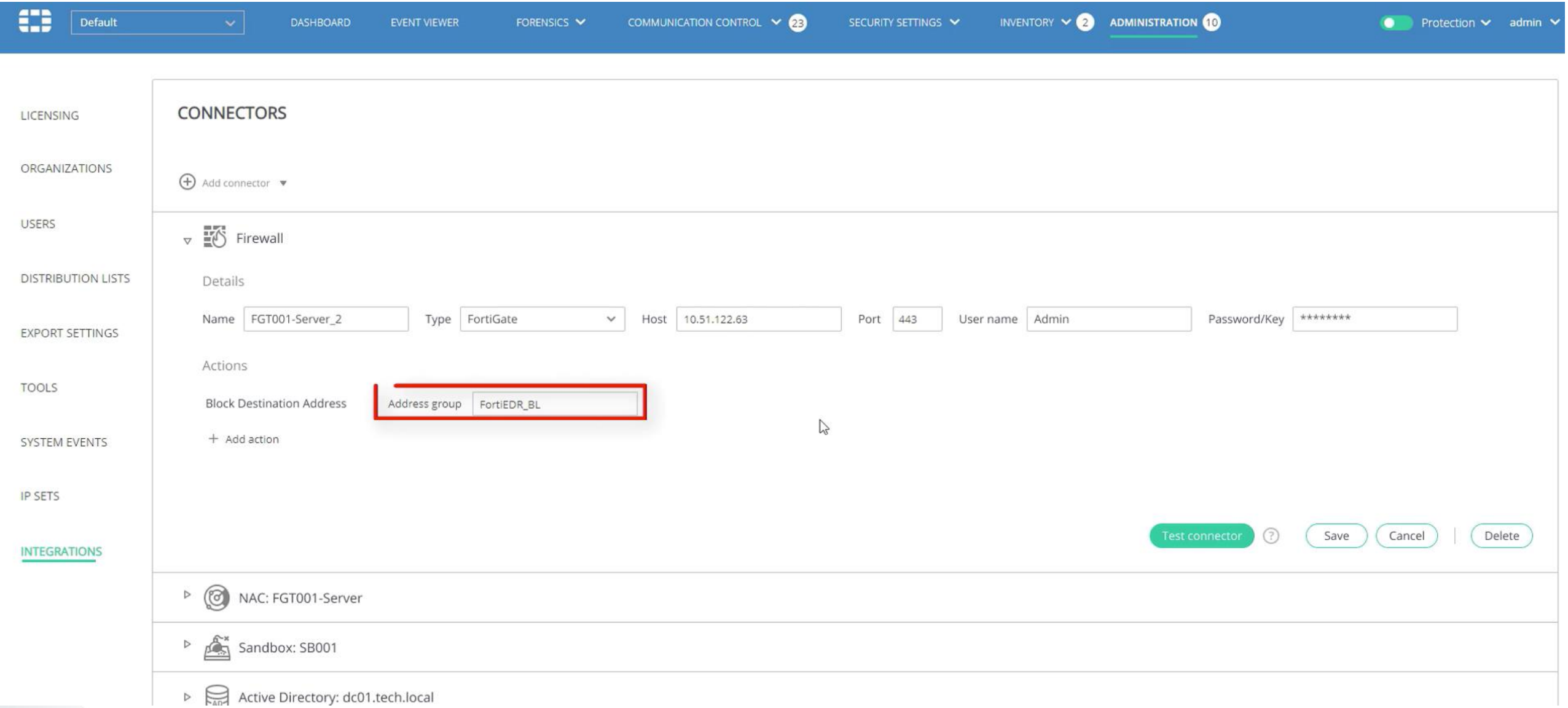
Автоматическая переклассификация



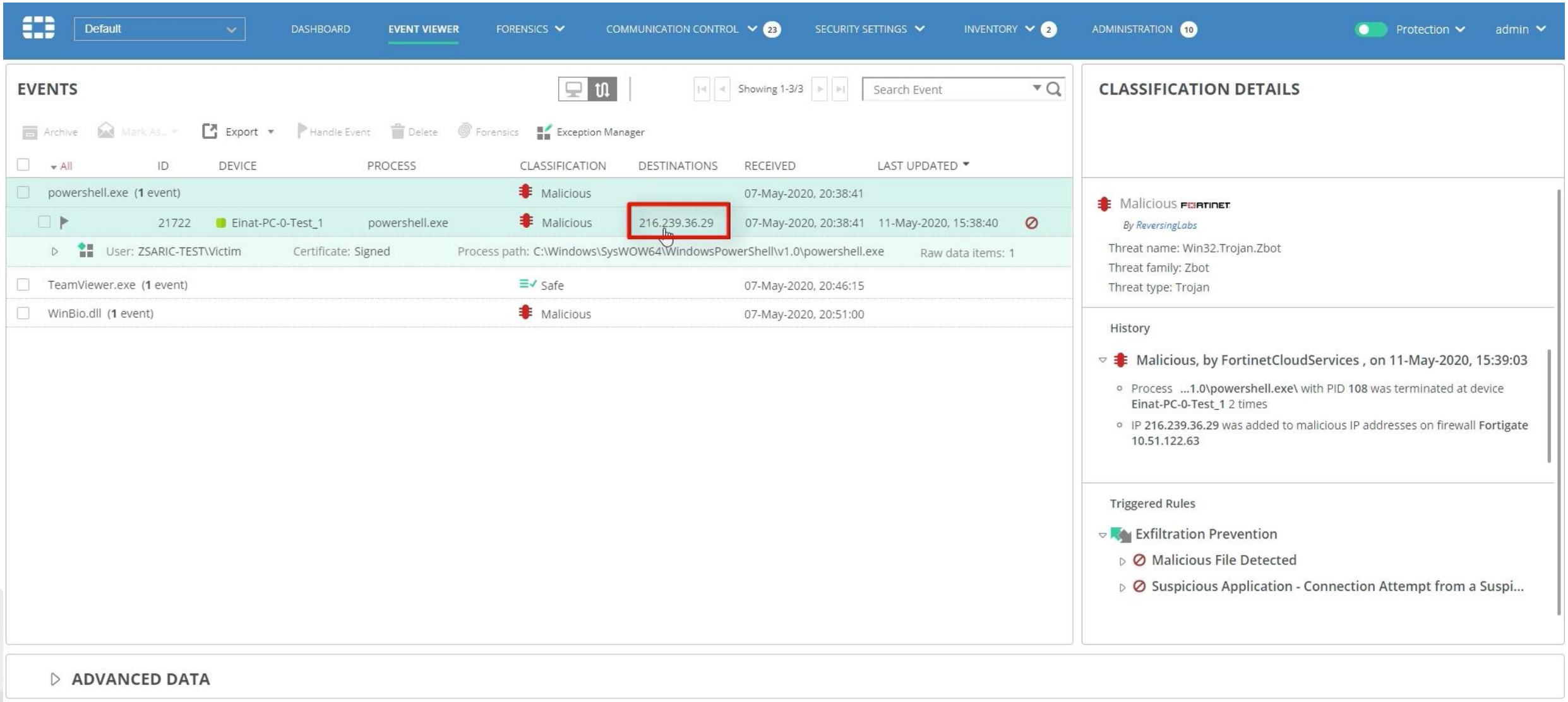
Управляемый интерфейс с обогащением данных



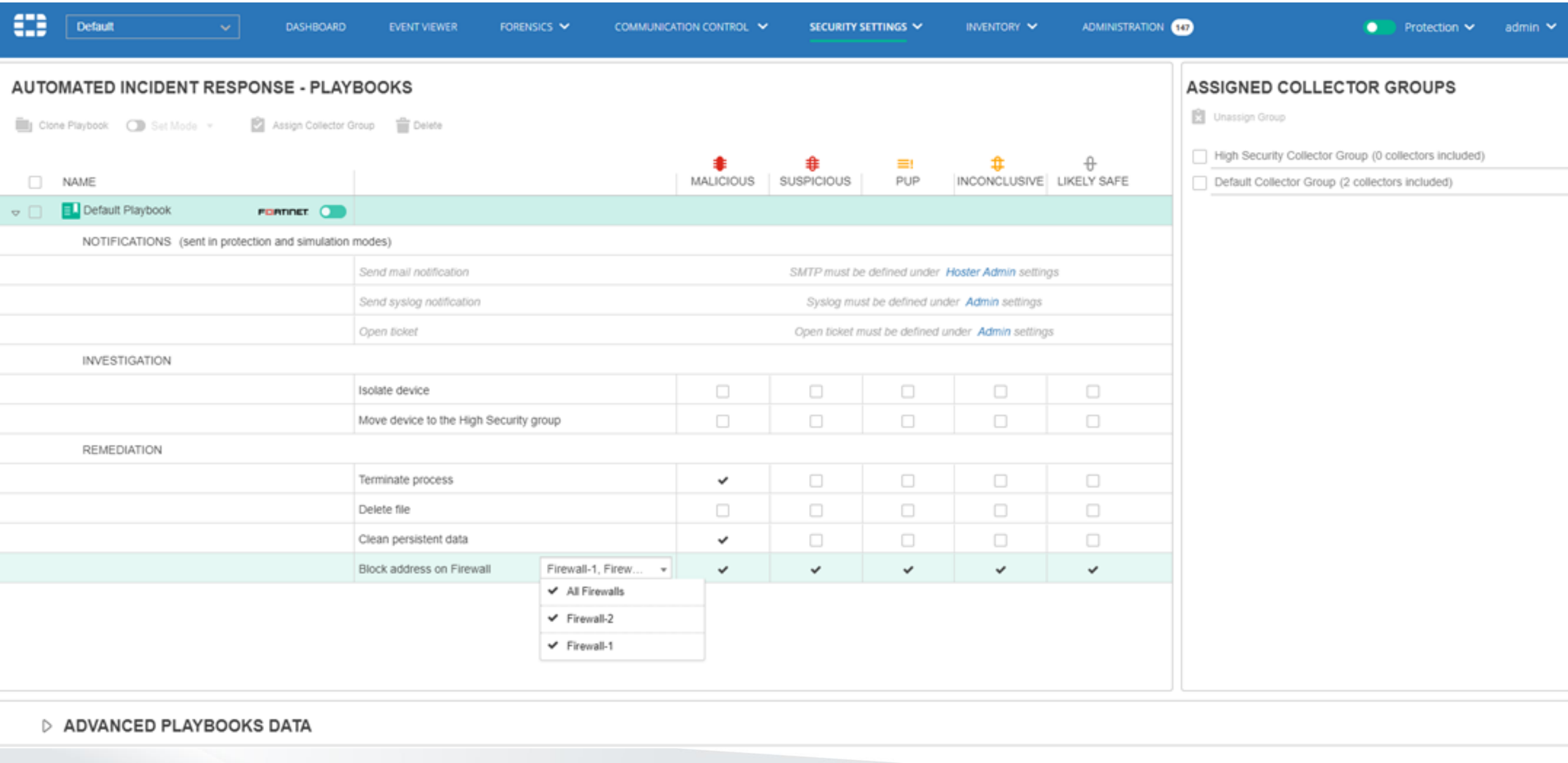
Расширенный ответ за счет Fabric-интеграции



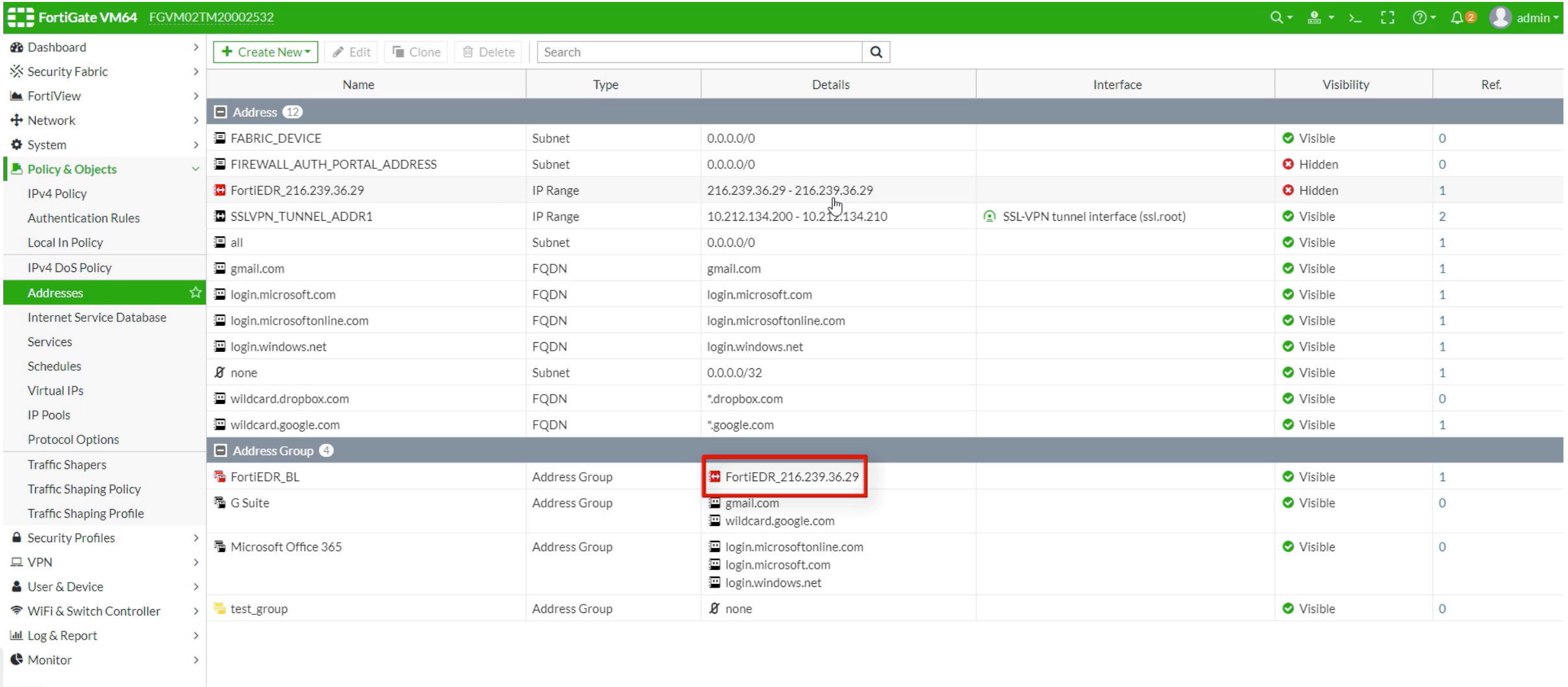
Обнаружение вредоносных IP-адресов



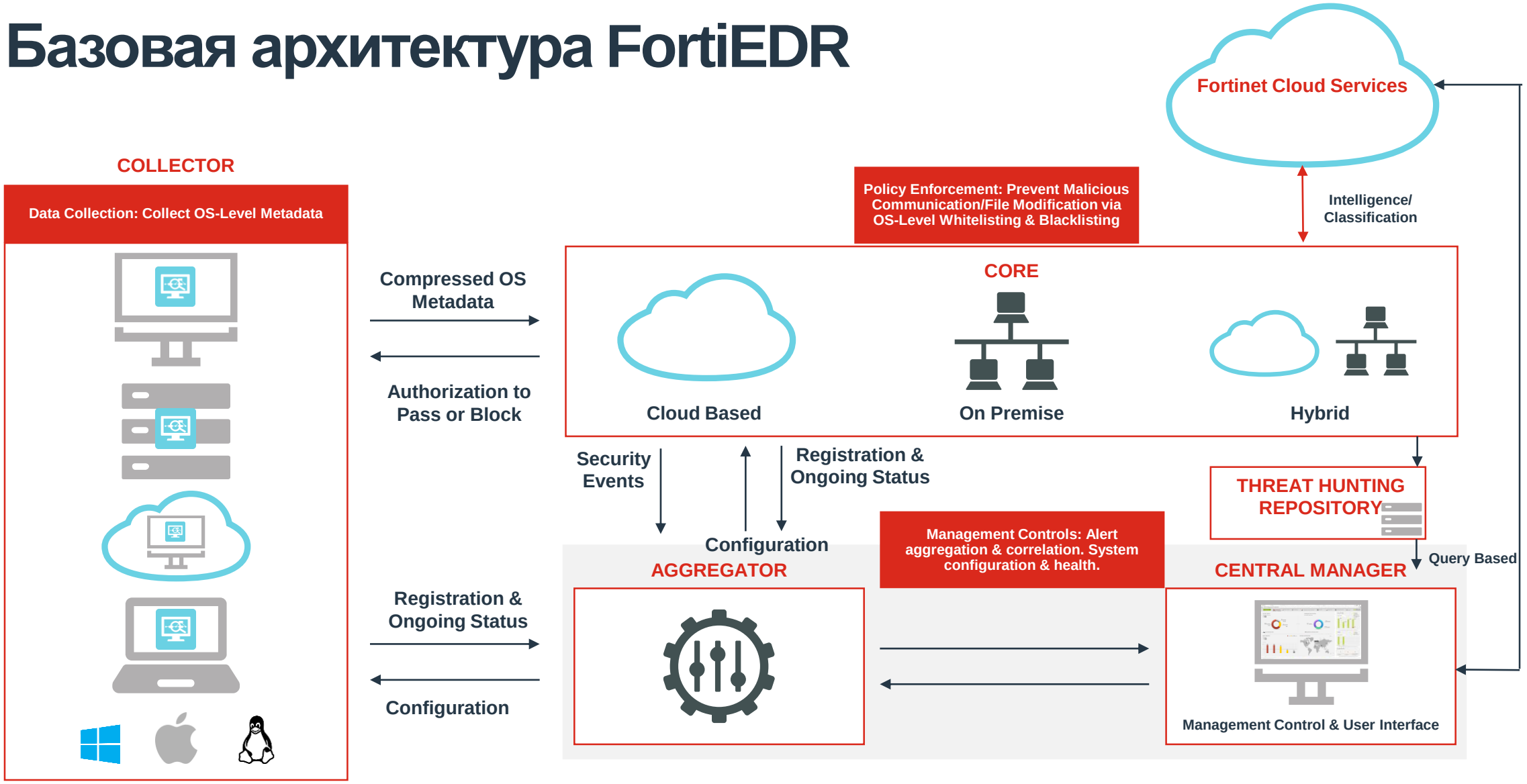
Контекстные сценарии реагирования на инциденты FortiEDR



Интеграция с межсетевым экраном



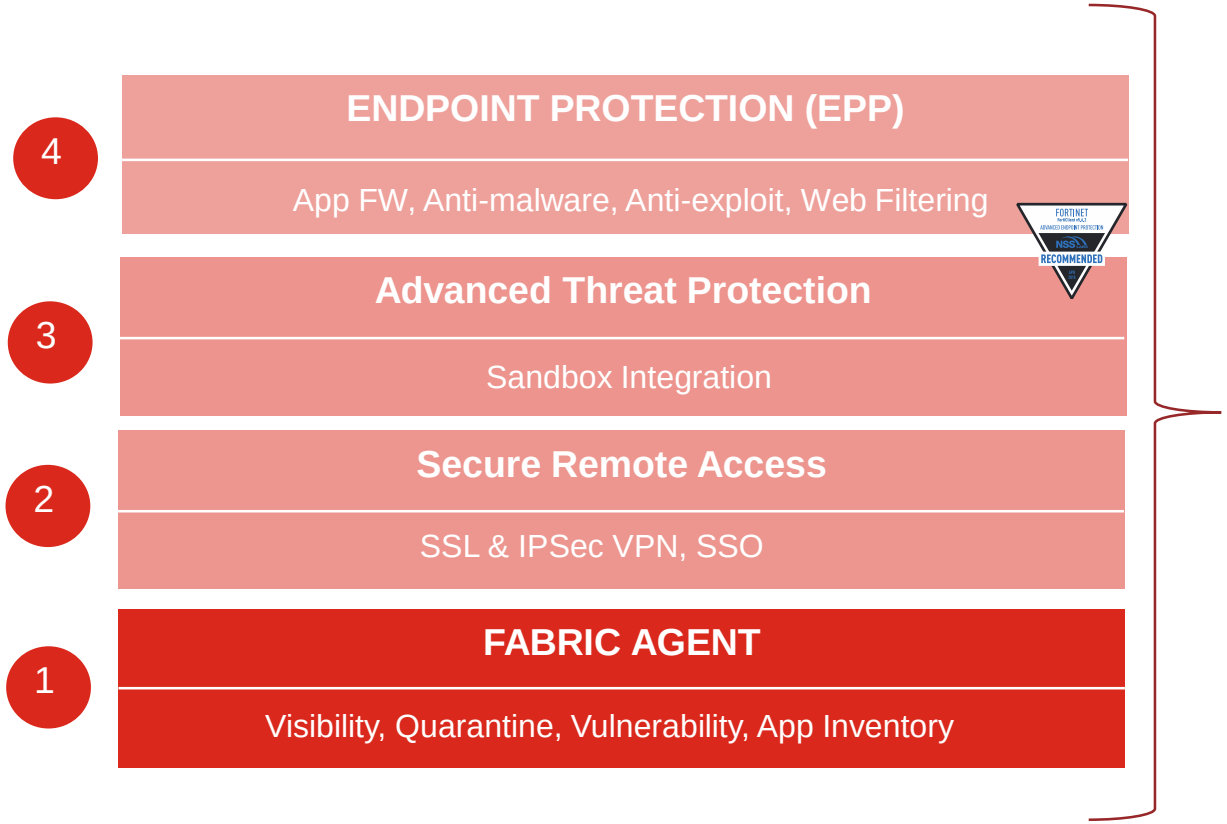
Базовая архитектура FortiEDR



FortiClient Fabric Agent

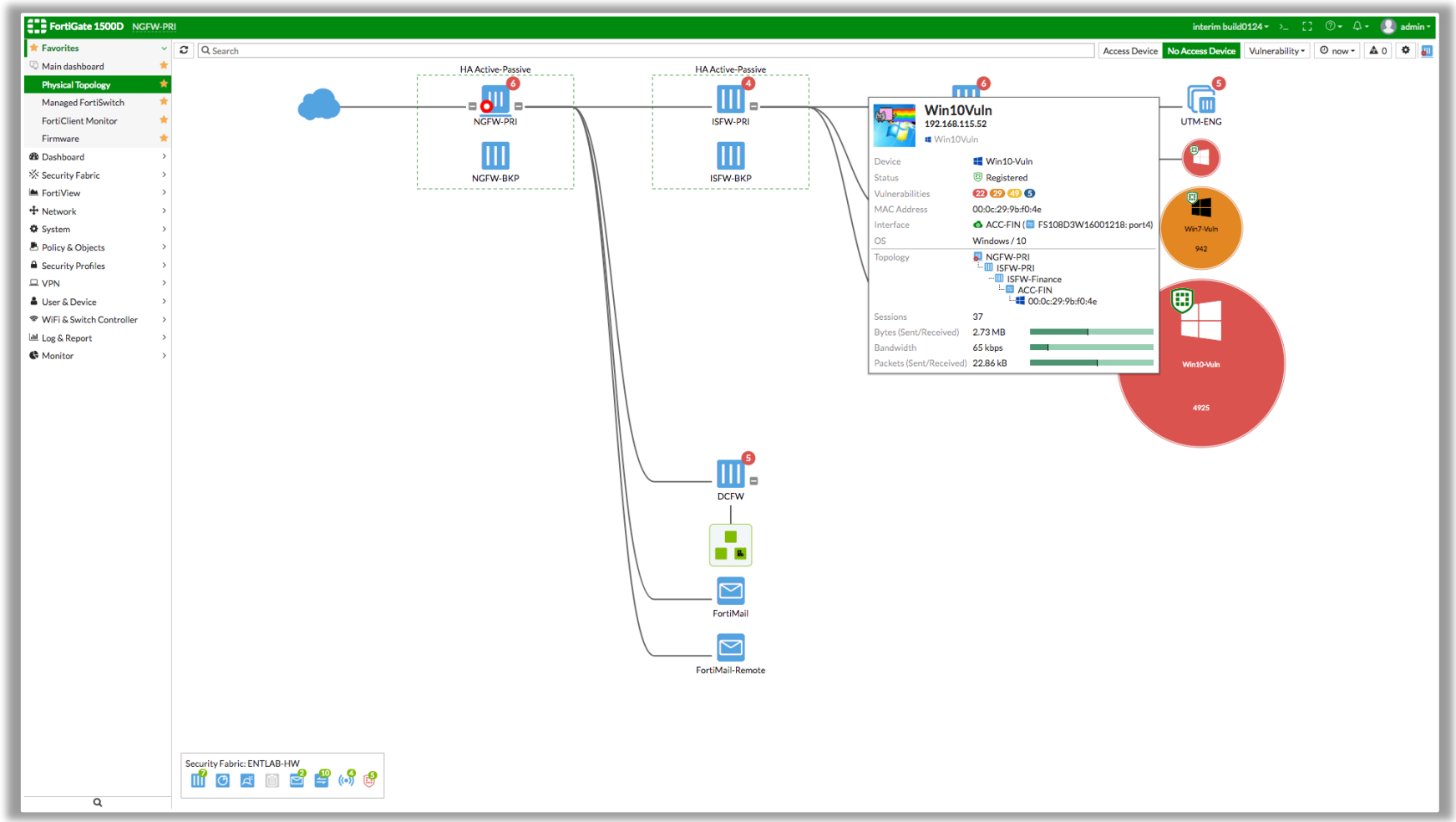
Видимость, контроль и автоматизация для конечных точек

FortiClient Fabric Agent



- Видимость конечных точек
- Обмен телеметрией с Security Fabric
- Обеспечение соответствия конечных точек требованиям безопасности
- Сканирование уязвимостей и патчинг
- Оценка риска конечных точек - рейтинг безопасности
- Инвентаризация приложений
- Поддержка Windows, Mac и Linux

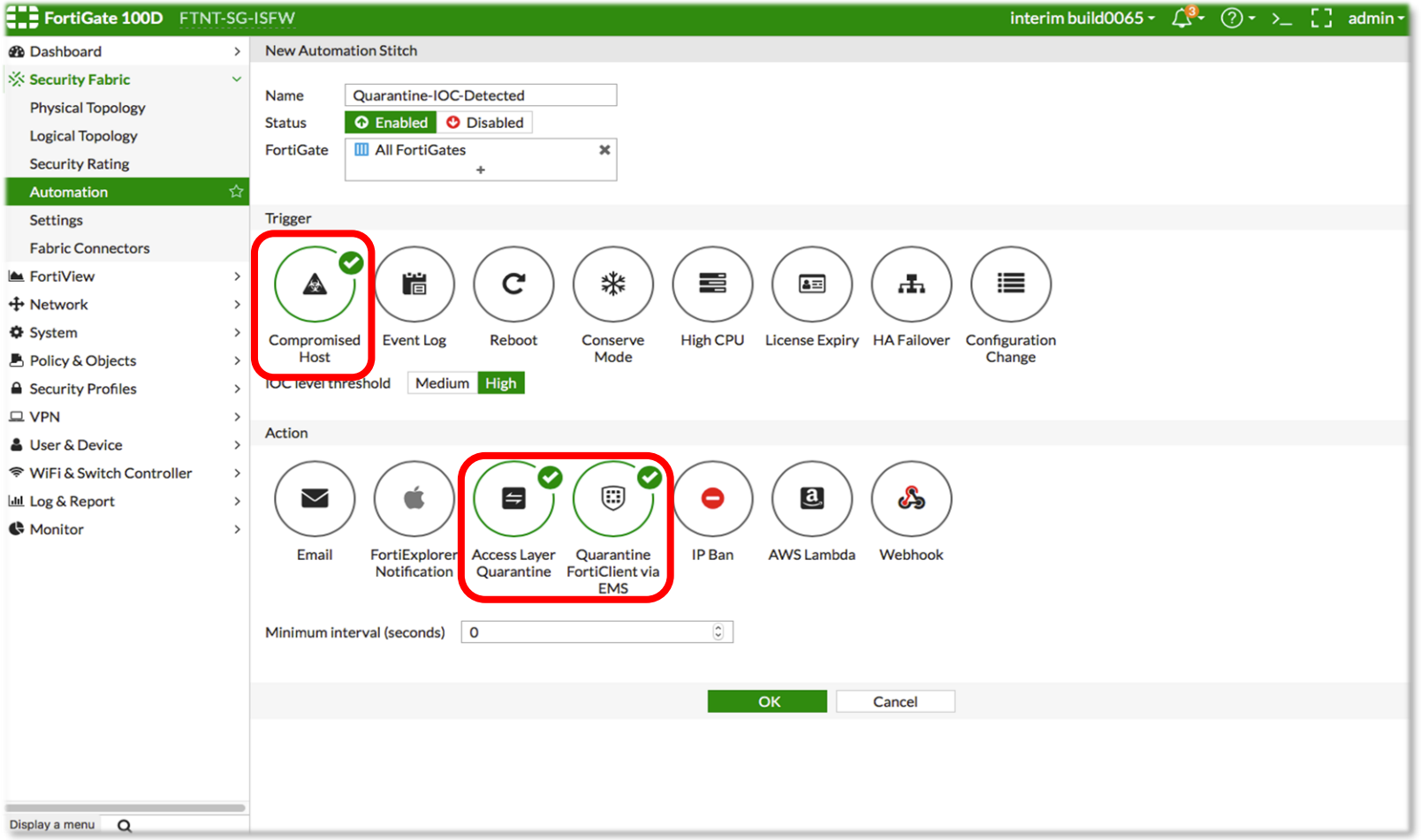
Наглядность уровня риска



- Информация об устройстве
  - ОС
  - Связывание нескольких MAC
- Статус FortiClient
- Уязвимости конечных точек
- Авторизованные пользователи
- Аватар пользователя
- Социальные идентификаторы
- Online/Off-line
- События и журналы конечной точки

Автоматизация

- Файловый карантин
- Анализ в песочнице
- Автоматический патчинг
- Оценка соблюдения требований
- Карантин конечной точки

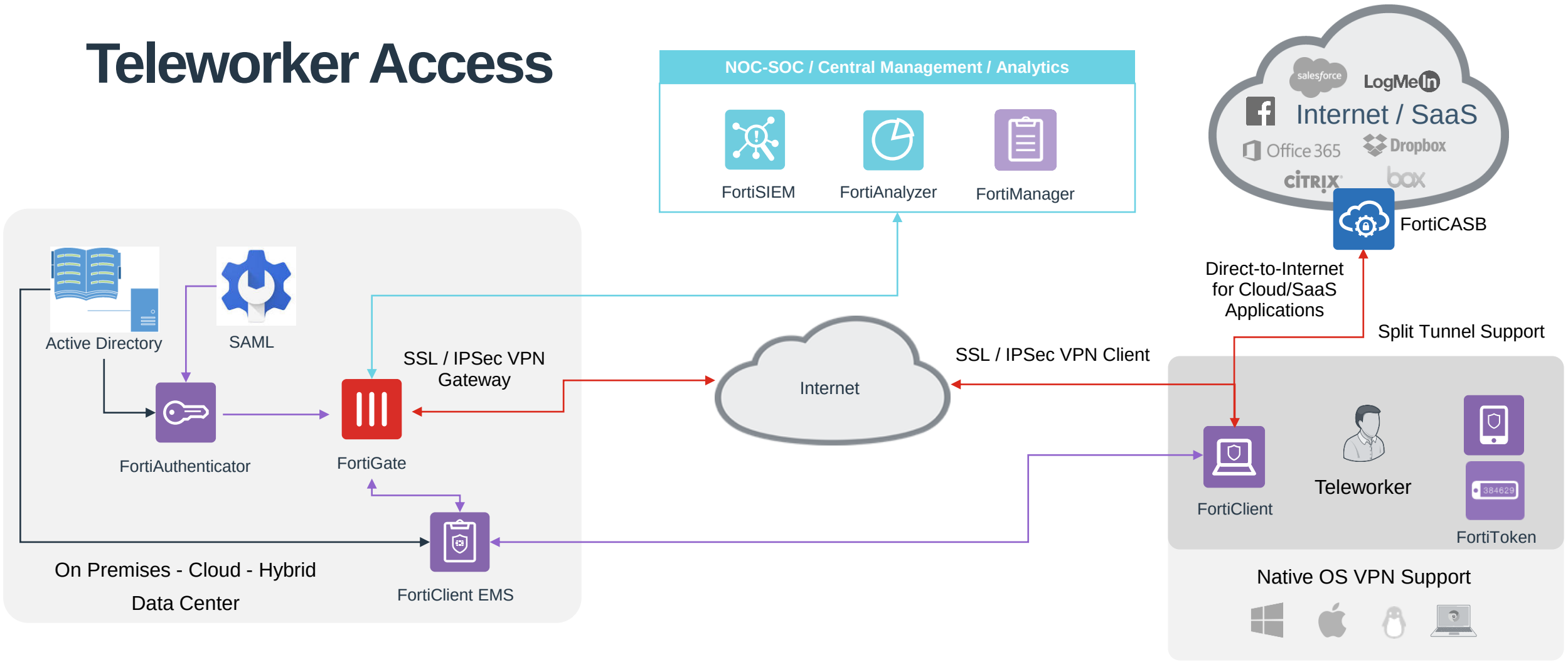


Безопасный удаленный доступ

Интегрированный, Always-on VPN

Single Sign on

Teleworker Access



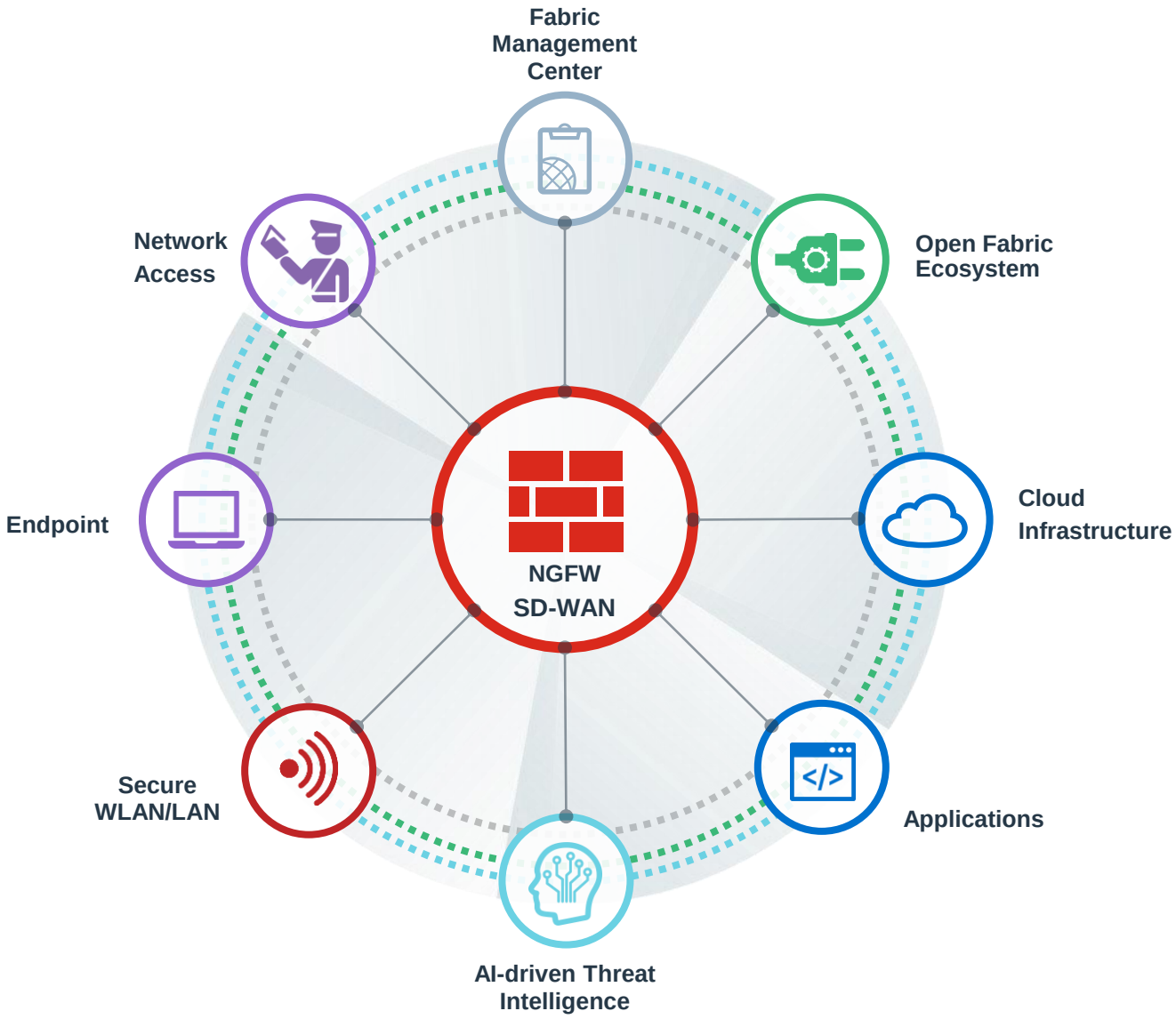
FortiClient EMS

FortiClient Enterprise Management Server

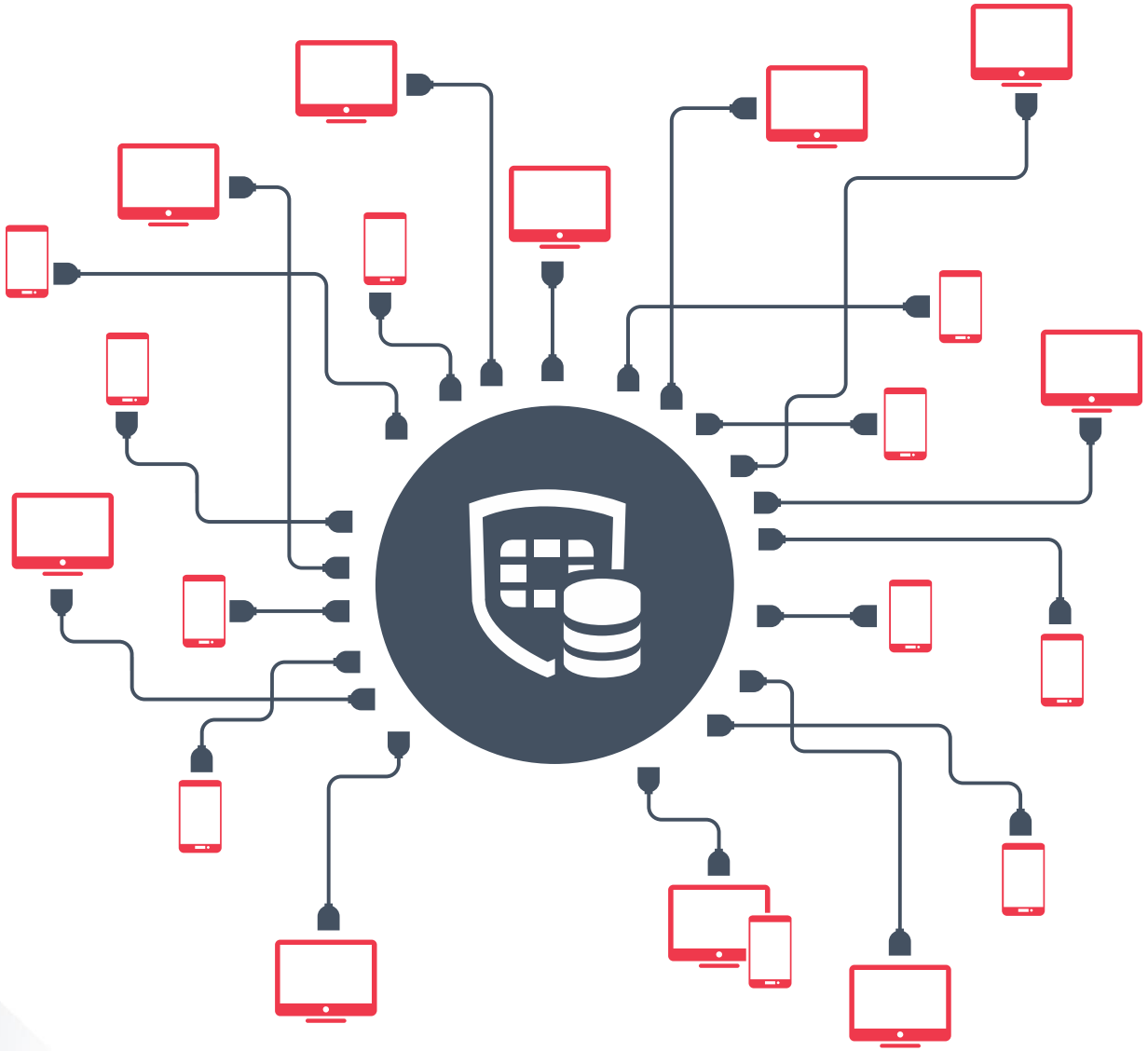
FortiClient EMS

Защита конечных точек на базе Fabric обеспечивает…

- интегрированную видимость конечных точек и контроль соответствия
- проактивную защиту конечных точек
- автоматизированное сдерживание угроз и контроль эпидемий
- безопасный удаленный доступ



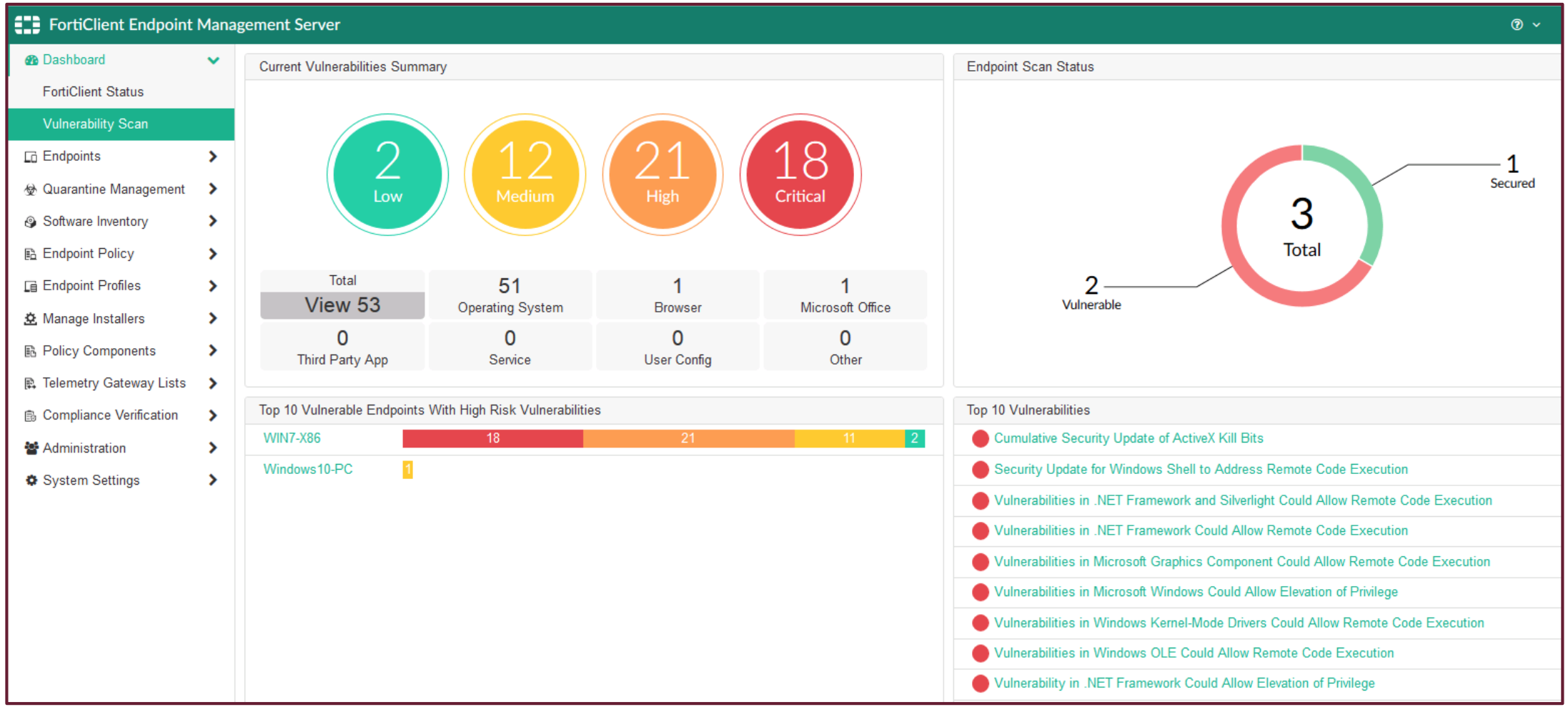
Централизованное управление с помощью EMS



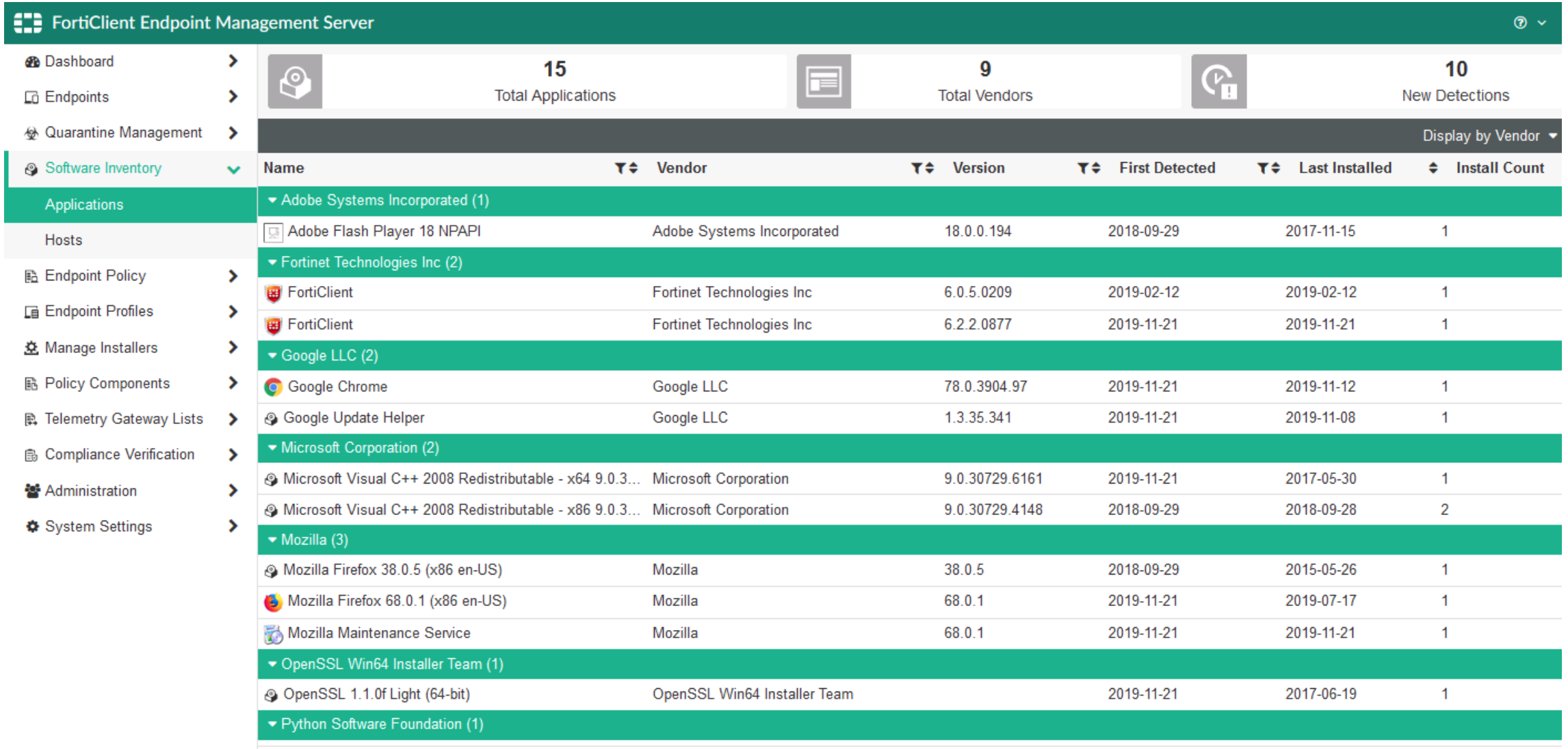
Enterprise Management Server (EMS)

- Настройка, развертывание и управление FortiClient
  - Интеграция с LDAP, Active Directory и другими корпоративными системами
- Мониторинг конечных точек в реальном времени
- Сводка угроз, предупреждение и уведомление
- Удаленные действия
  - Антивирусное сканирование
  - Сканирование уязвимостей
  - Карантин конечной точки
- Инвентаризация программного обеспечения
- Управление файловым карантином
- Высокая масштабируемость

Сканирование уязвимостей

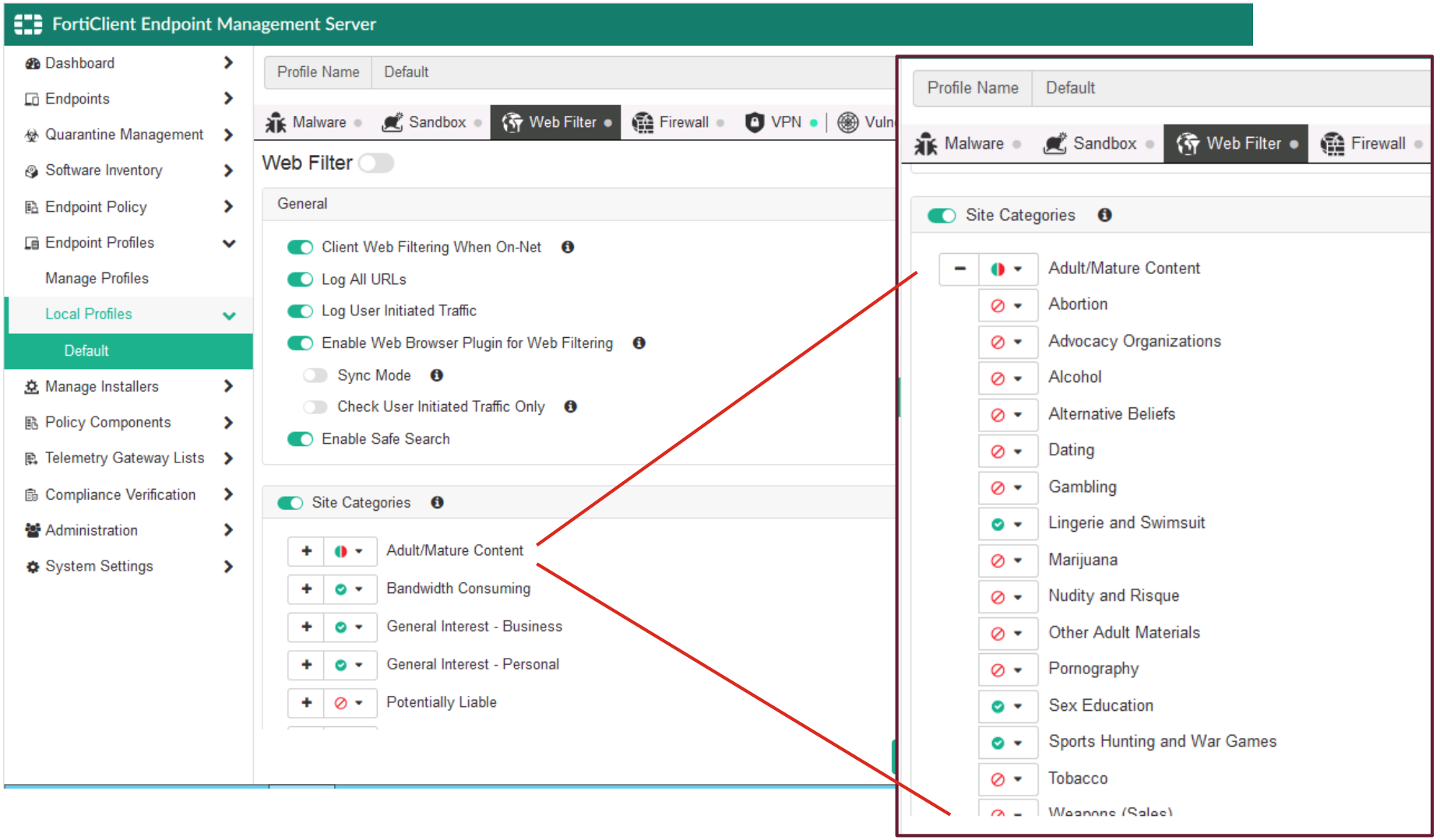


Инвентаризация программного обеспечения



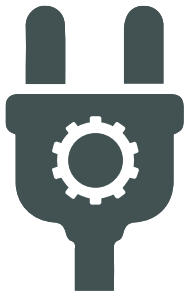
Name	Vendor	Version	First Detected	Last Installed	Install Count
Adobe Systems Incorporated (1)					
Adobe Flash Player 18 NPAPI	Adobe Systems Incorporated	18.0.0.194	2018-09-29	2017-11-15	1
Fortinet Technologies Inc (2)					
FortiClient	Fortinet Technologies Inc	6.0.5.0209	2019-02-12	2019-02-12	1
FortiClient	Fortinet Technologies Inc	6.2.2.0877	2019-11-21	2019-11-21	1
Google LLC (2)					
Google Chrome	Google LLC	78.0.3904.97	2019-11-21	2019-11-12	1
Google Update Helper	Google LLC	1.3.35.341	2019-11-21	2019-11-08	1
Microsoft Corporation (2)					
Microsoft Visual C++ 2008 Redistributable - x64 9.0.3...	Microsoft Corporation	9.0.30729.6161	2019-11-21	2017-05-30	1
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	9.0.30729.4148	2018-09-29	2018-09-28	2
Mozilla (3)					
Mozilla Firefox 38.0.5 (x86 en-US)	Mozilla	38.0.5	2018-09-29	2015-05-26	1
Mozilla Firefox 68.0.1 (x86 en-US)	Mozilla	68.0.1	2019-11-21	2019-07-17	1
Mozilla Maintenance Service	Mozilla	68.0.1	2019-11-21	2019-11-21	1
OpenSSL Win64 Installer Team (1)					
OpenSSL 1.1.0f Light (64-bit)	OpenSSL Win64 Installer Team		2019-11-21	2017-06-19	1
Python Software Foundation (1)					

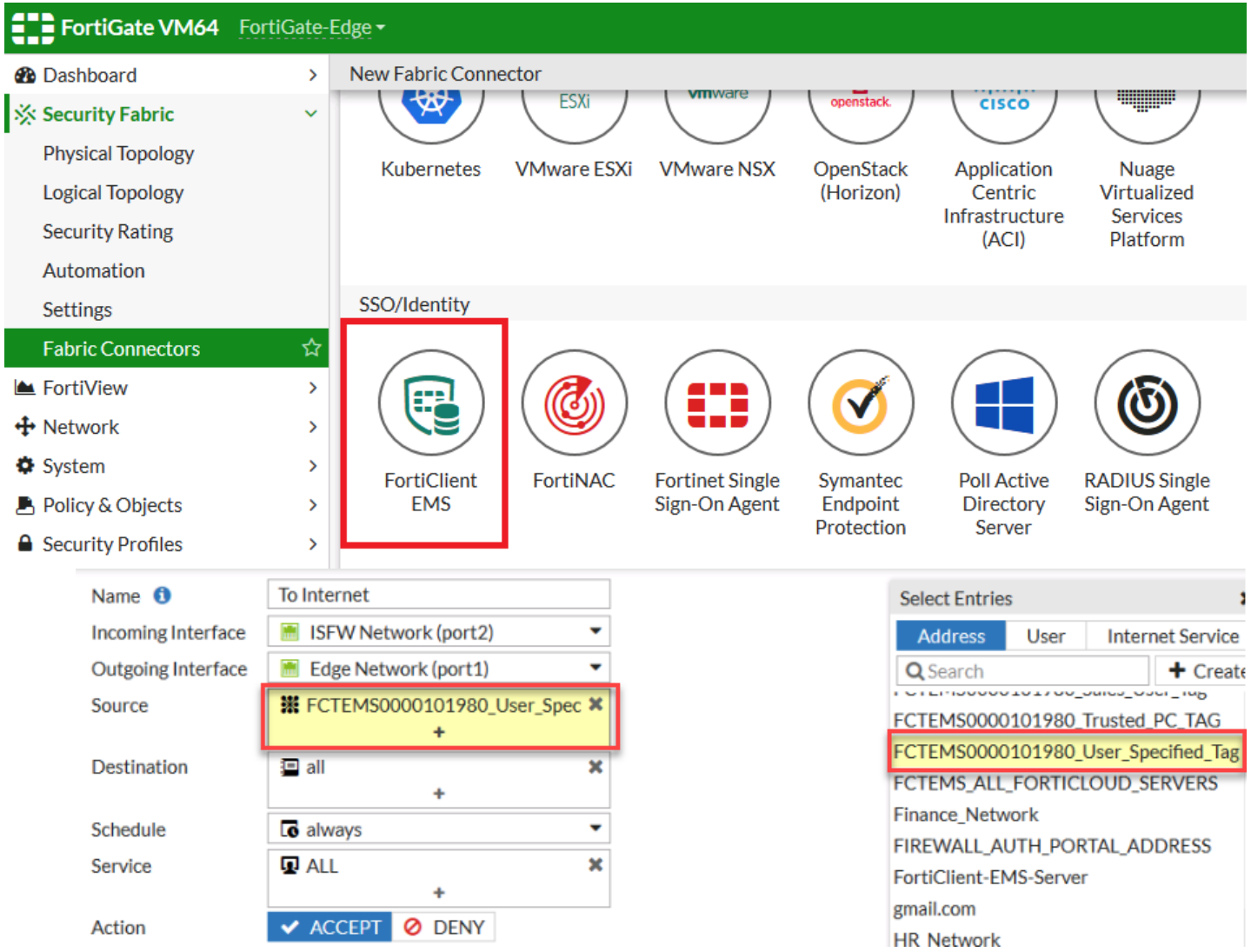
База данных FortiGuard Web Filter



Fabric EMS коннектор

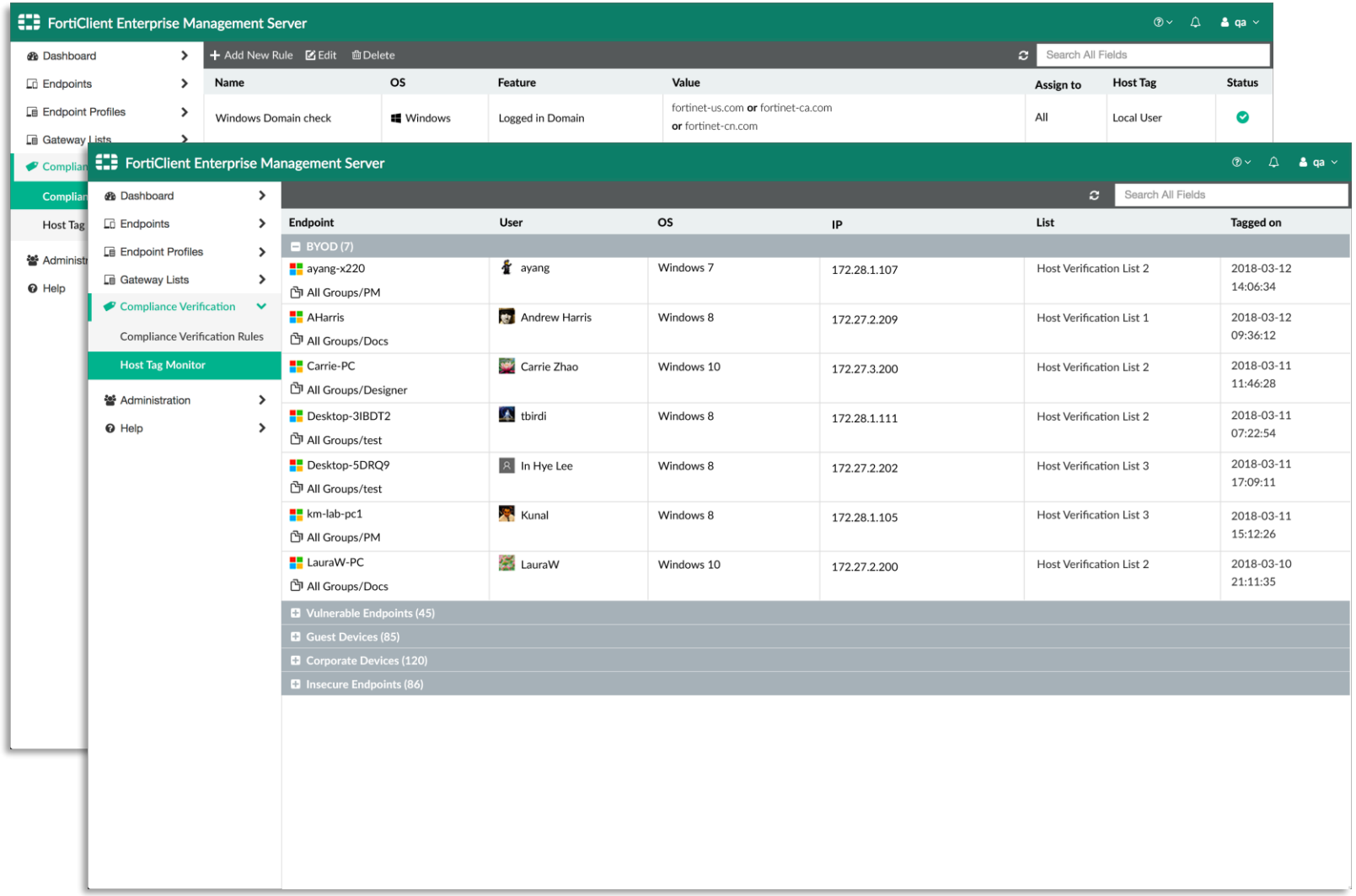
- Обеспечение связи между FortiClient EMS и FortiGate
- Получение EMS-тэгов
- Применение политик FortiGate
- Обеспечение compliance





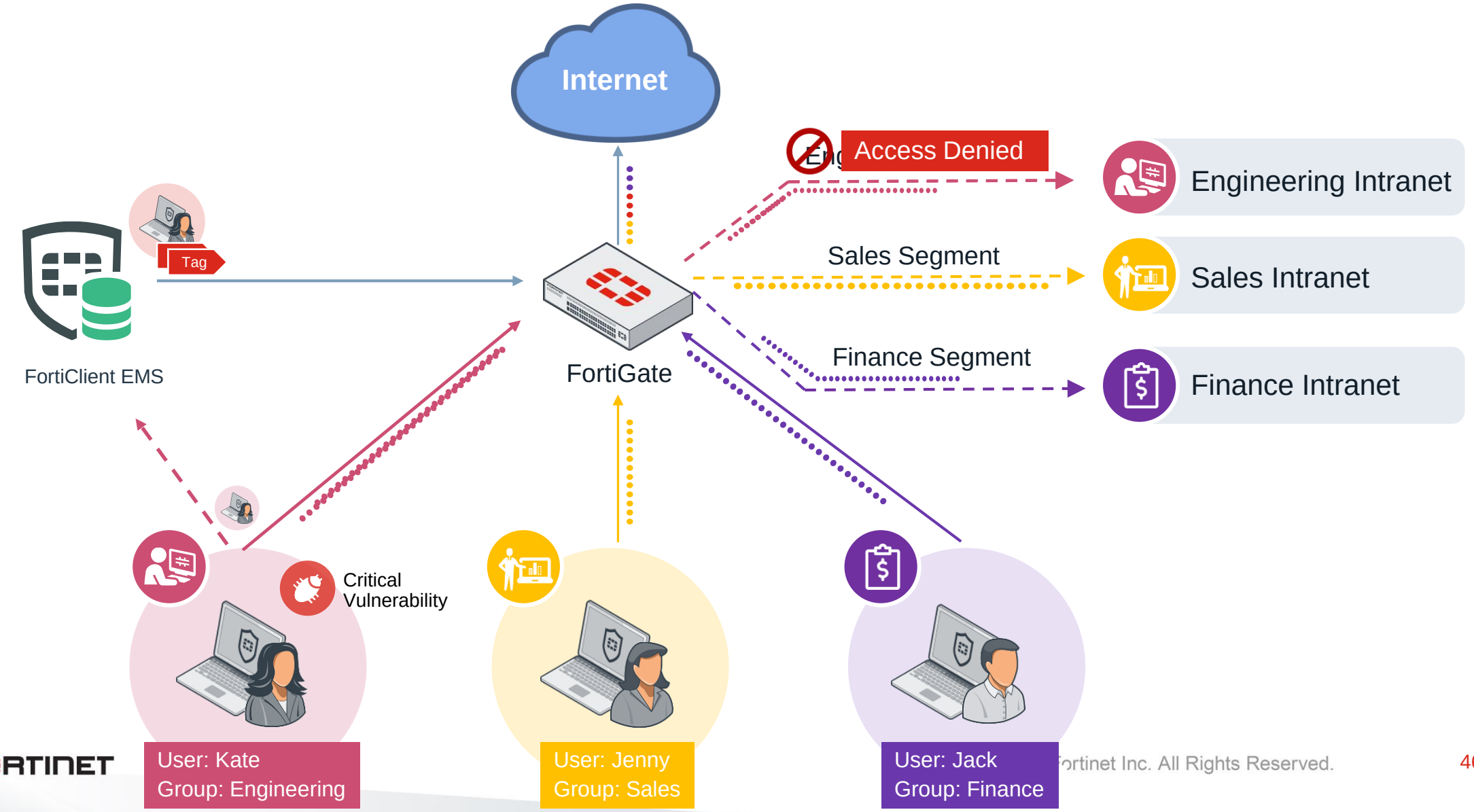
Правила и тэги для проверки соответствия

- Правила соответствия могут использоваться для применения тэгов к конечным точкам
- Тэги могут использоваться политиками FortiGate для динамического контроля доступа



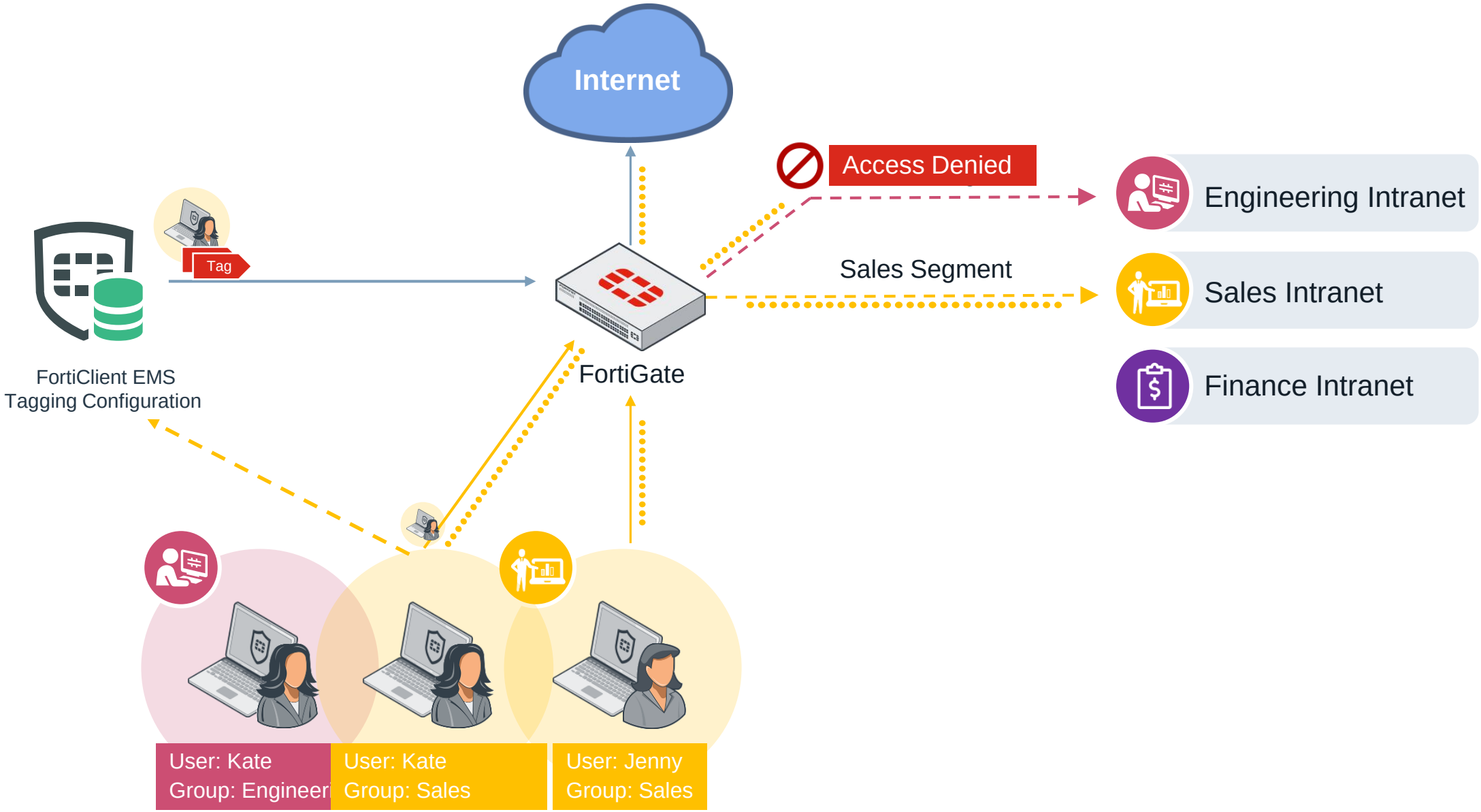
Динамический контроль доступа (сегментация на основе намерений)

Use Case : заблокировать доступ для конечных точек с выявленной угрозой безопасности



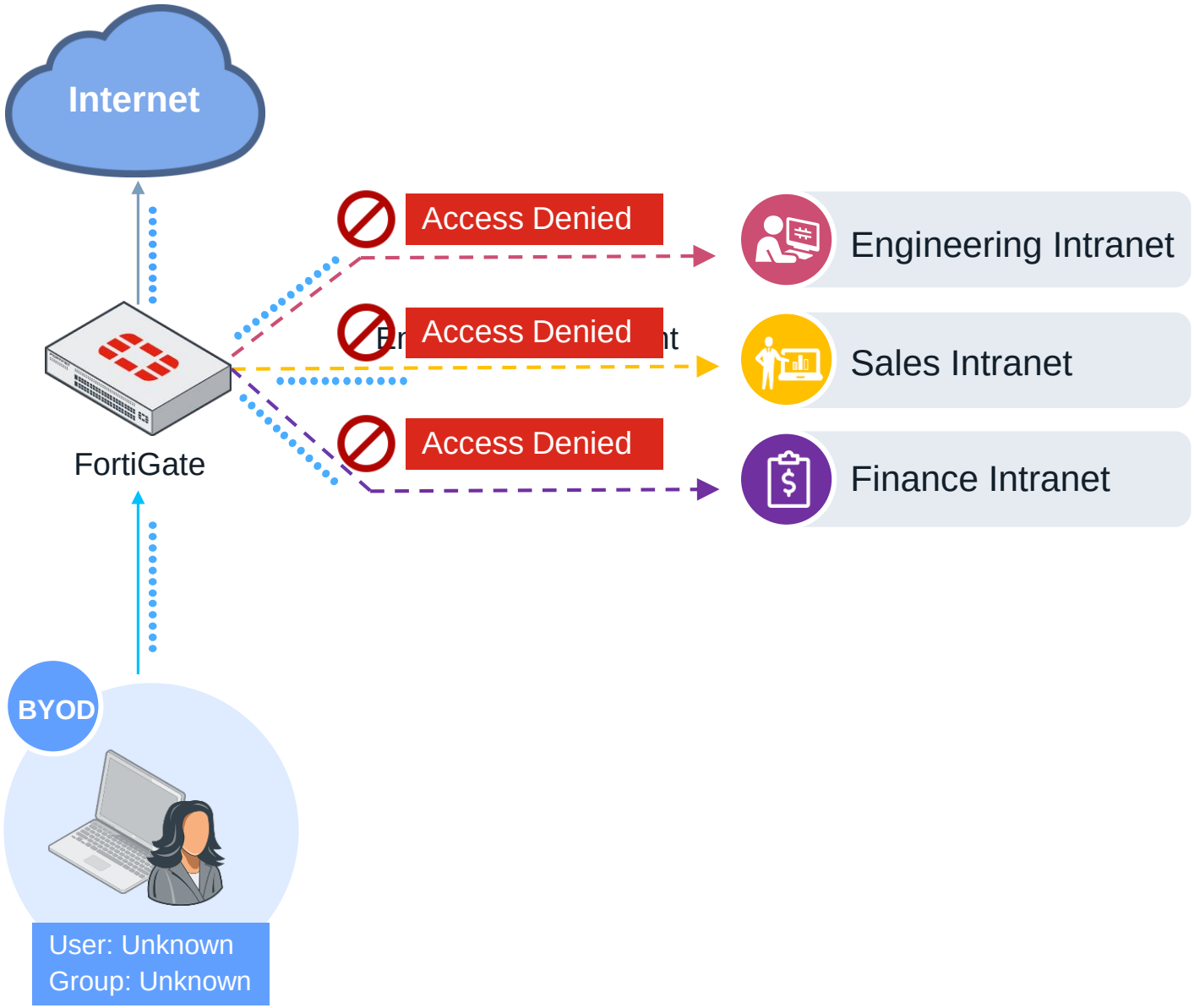
Динамический контроль доступа (сегментация на основе намерений)

Use Case: Доступ на основе групп AD



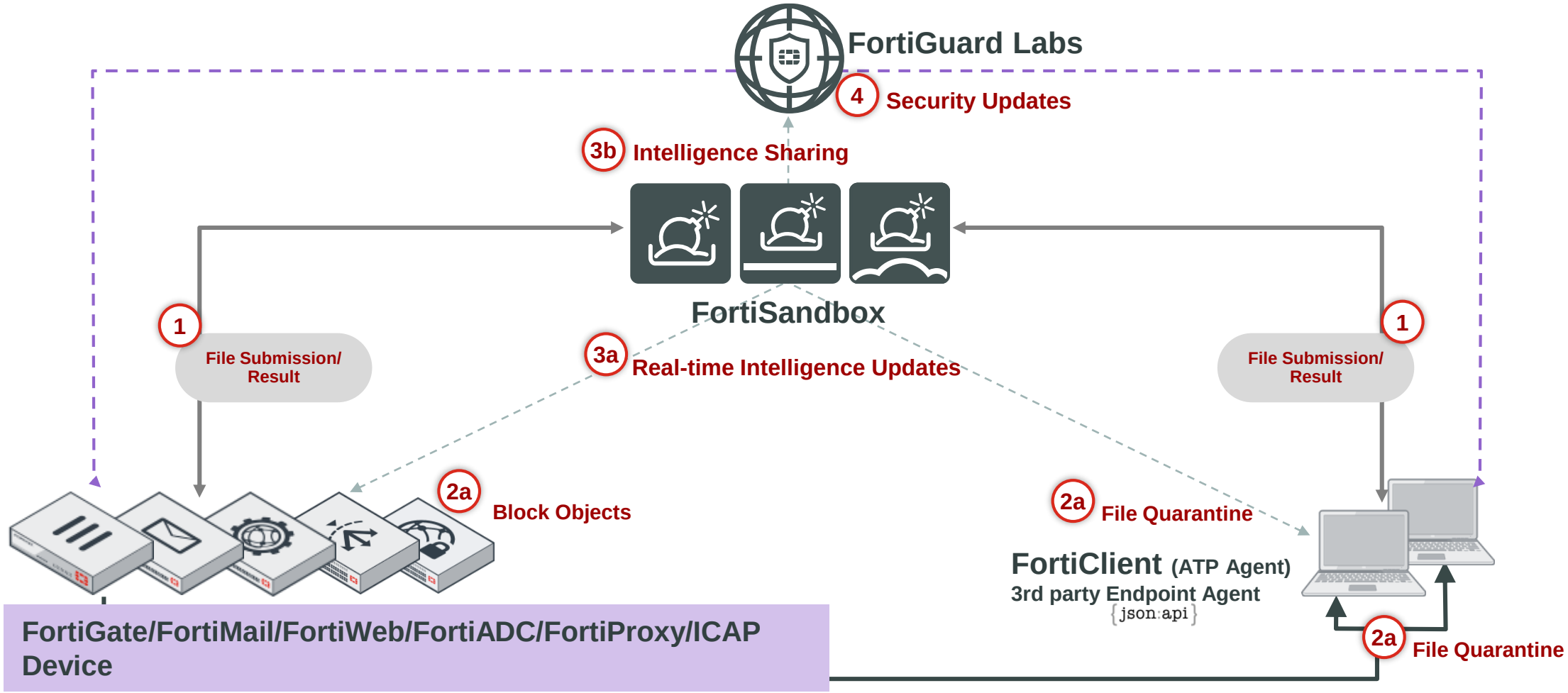
Динамический контроль доступа (сегментация на основе намерений)

Use Case: Ограниченный доступ для неизвестных конечных точек



FortiSandbox – Обмен аналитическими данными об угрозах

AUTOMATED



Обзор: FortiClient and FortiEDR

Ключевые варианты использования

FortiClient

- Взаимодействие с Fabric Agent
  - Сбор телеметрии с конечной точки
  - Инвентаризация приложений
  - Динамический контроль доступа
- Безопасный удаленный доступ
  - VPN Agent
  - SSO
- Защита конечных точек
  - Сканирование / исправление уязвимостей
  - CPRL – AV
  - Anti-Exploit
  - Web filtering
  - Application firewall (SaaS Control)

FortiEDR

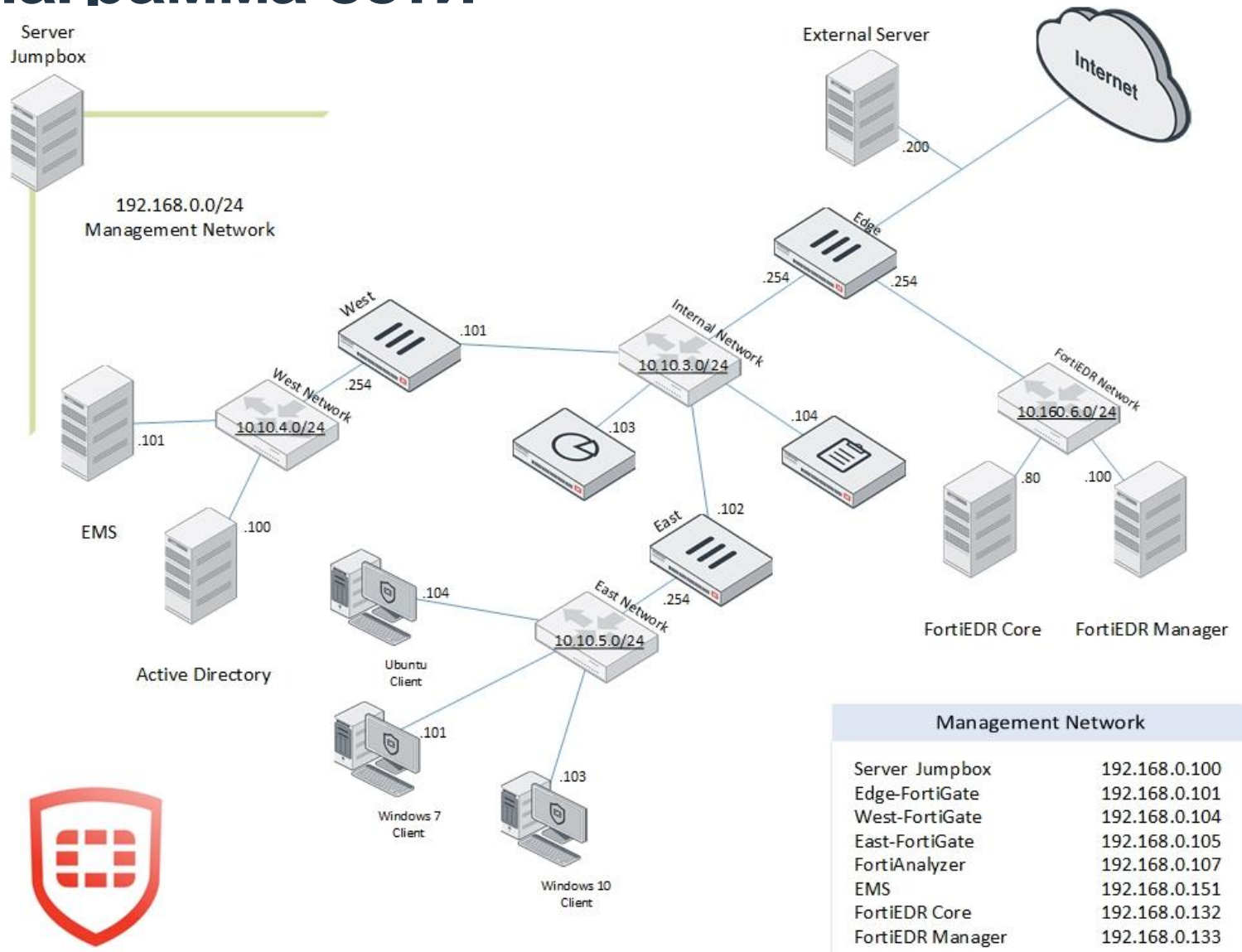
- Защита конечных точек от Ransomware
  - AV на основе ML + на основе поведения
  - Обнаружение / защита от безфайловых атак
  - Обнаружение приложений
  - Сканирование уязвимостей / Виртуальное исправление
  - Защита данных
- Обнаружение и защита от угроз
  - Уменьшение поверхности атаки – Virtual patching
  - Post-execution detection (behavioral-based)
  - Автоматическое сдерживание угроз, remediation /roll back
- Криминалистические данные (форензика)
- Threat hunting
- Сервис MDR (FortiResponder)

Минимальное перекрытие

Элементы AV – защита до выполнения| Интеграция с песочницей |Уменьшение поверхности атаки - сканирование уязвимостей

Лабораторная работа: Endpoint Workshop

LAB – Диаграмма сети



Management Network	
Server Jumpbox	192.168.0.100
Edge-FortiGate	192.168.0.101
West-FortiGate	192.168.0.104
East-FortiGate	192.168.0.105
FortiAnalyzer	192.168.0.107
EMS	192.168.0.151
FortiEDR Core	192.168.0.132
FortiEDR Manager	192.168.0.133

Proactive Advanced Endpoint Protection, Visibility and Control for Critical Assets Workshop Exercise

- В этих упражнениях вы узнаете, как:
  - FortiClient EMS защищает конечные точки и интегрируется в Fortinet Security Fabric для повышения видимости и контроля сети.
  - FortiEDR обеспечивает защиту конечных точек для сценариев до и после заражения с обширным мониторингом событий, предупреждениями и возможностями криминалистического расследования.

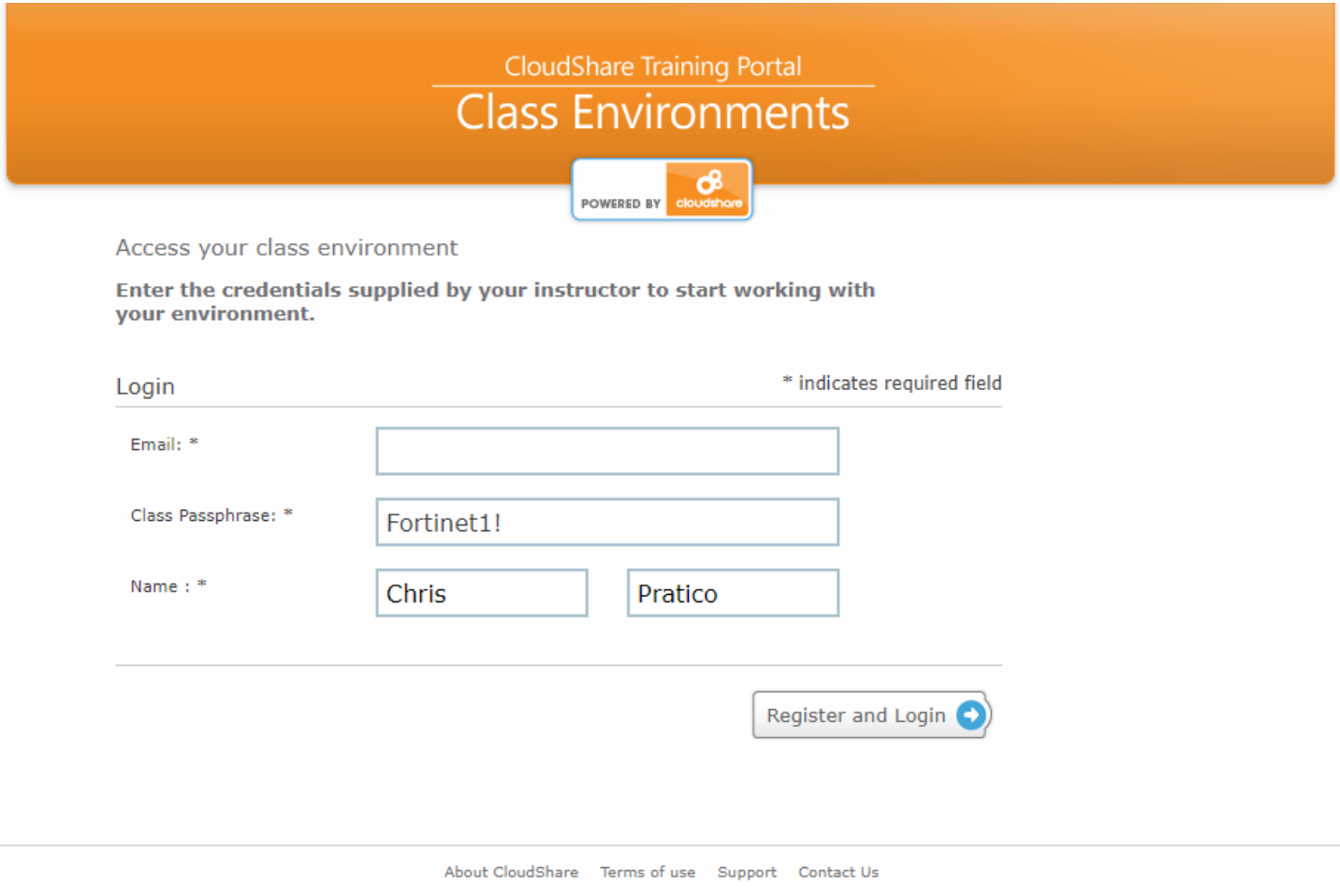
FORTINET

Instructor Notes

- The following slides are optional and can be used for the following:
  - To remind instructors how to interact with the Fast Track labs
  - To help students get started using the hands-on lab
- Feel free to use some, all, or none of the slides as part of your session
- It is recommended to keep the initial instruction short and then assist students individually as needed
- It is suggested to use no more than the first four of the following slides and only use the others on a case-by-case basis

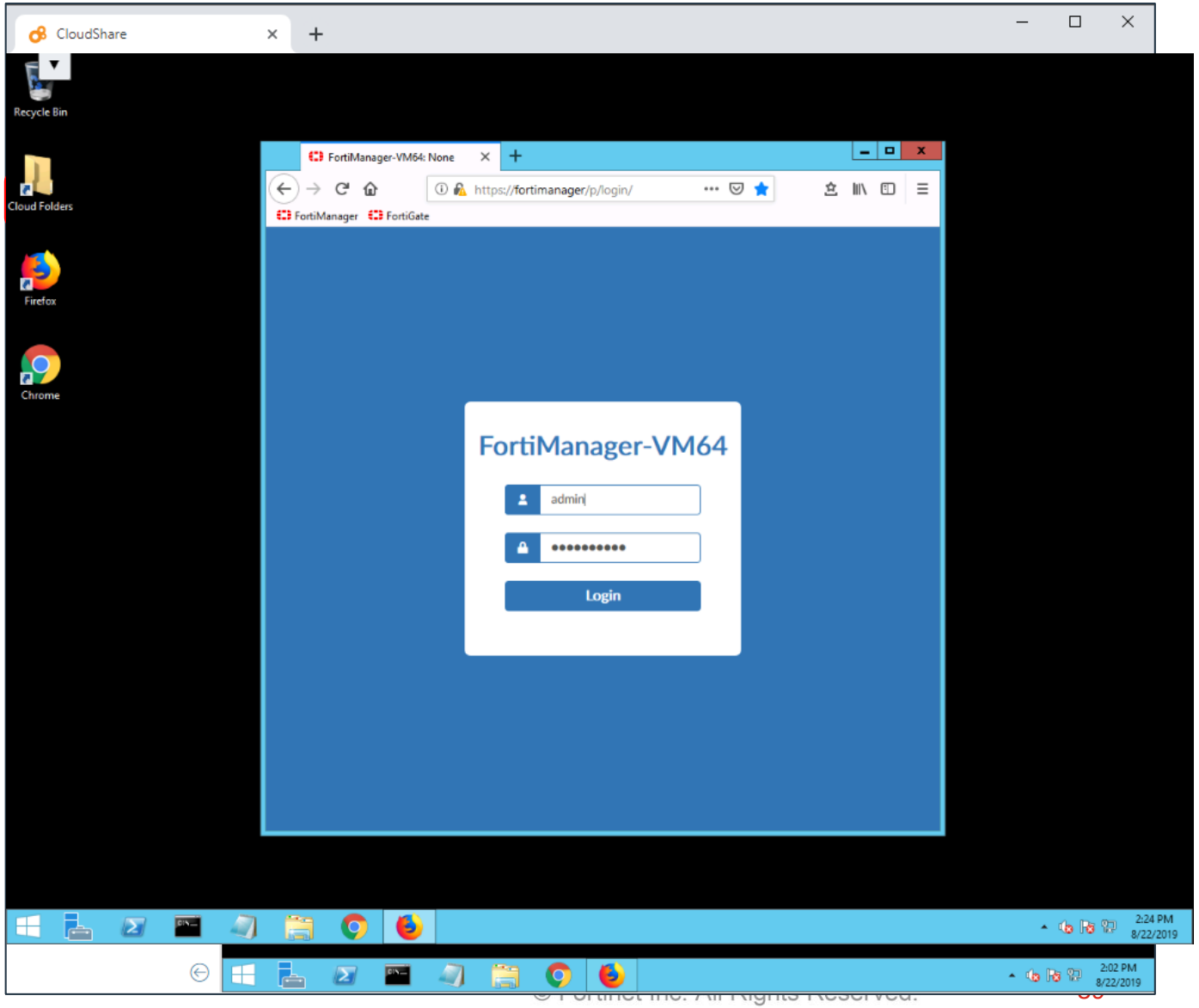
Student Access

- Classroom URL and password are provided by your instructor



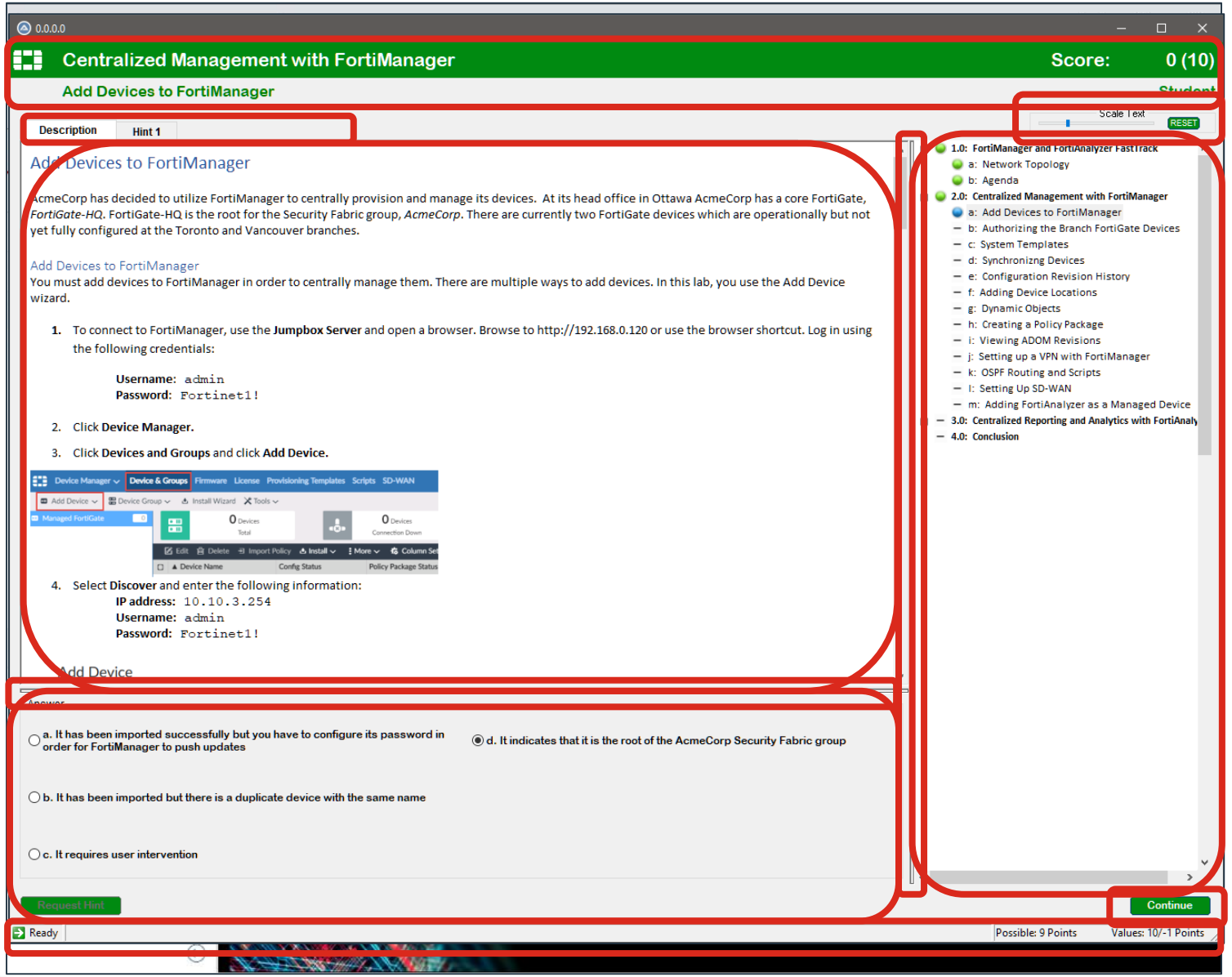
Student Classroom Portal

- View tabs across the top provide access to lab devices
- **FortiFIED Lab Guide:** an interactive lab guide providing tasks and validating results
- **Jumpbox Server:** provides access to links, software, and tools necessary to complete tasks
- **Full Screen Button:** makes current view full screen



FortiFIED Interactive Lab Guide

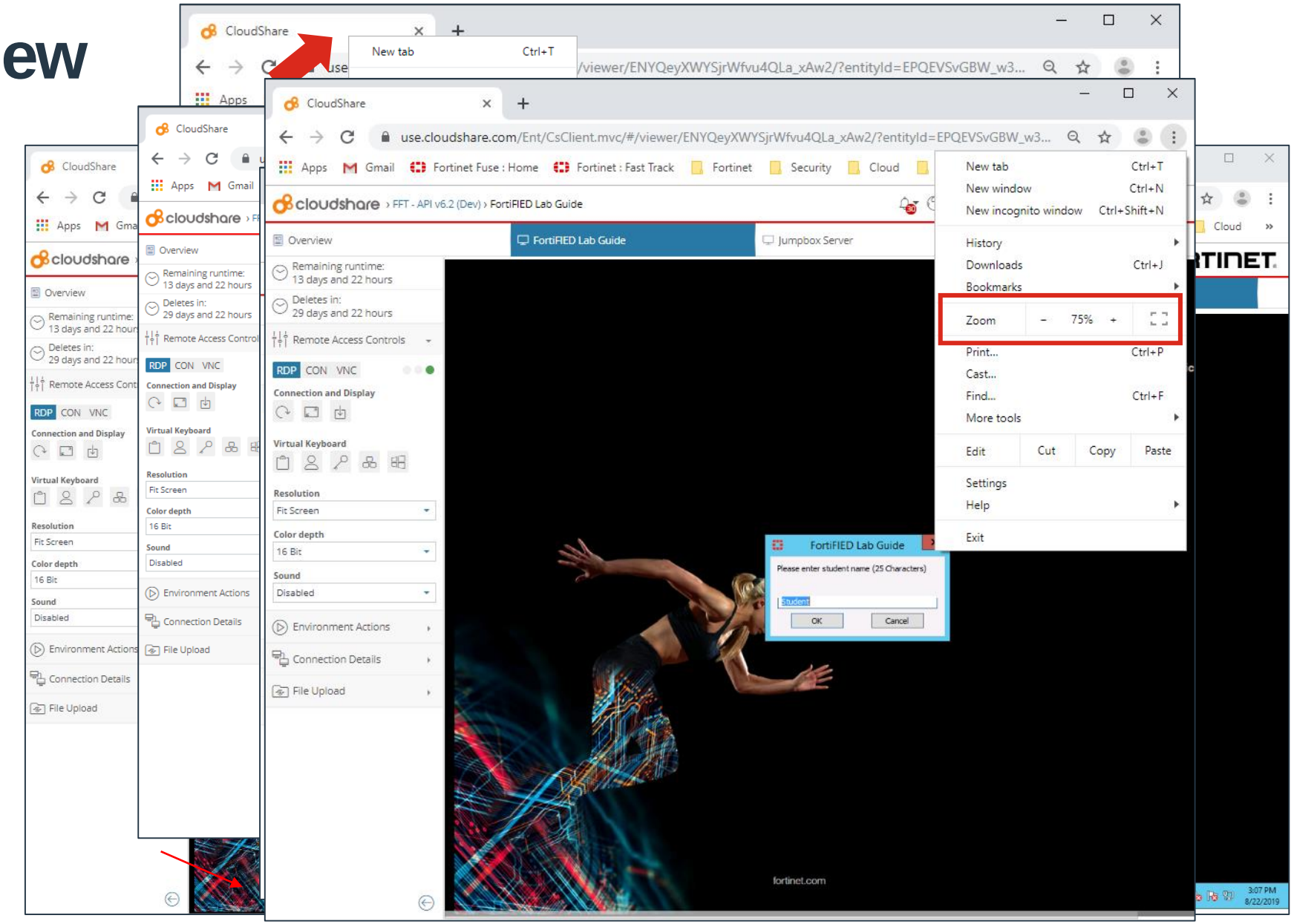
- Enter a Name
- Application banner
- Objectives list
- Display tabs
- Rich text
- Answer choice
- Continue button
- Status bar
- Scale text slider
- Resize display bar



Adjusting the View

1. Right-click the browser tab and select **duplicate** from drop-down menu
2. Tear off the browser tab by clicking it and dragging the tab away from the browser
3. Arrange the browser windows side by side, based on personal preference
4. Use the browser zoom to adjust resolution of views based on preference

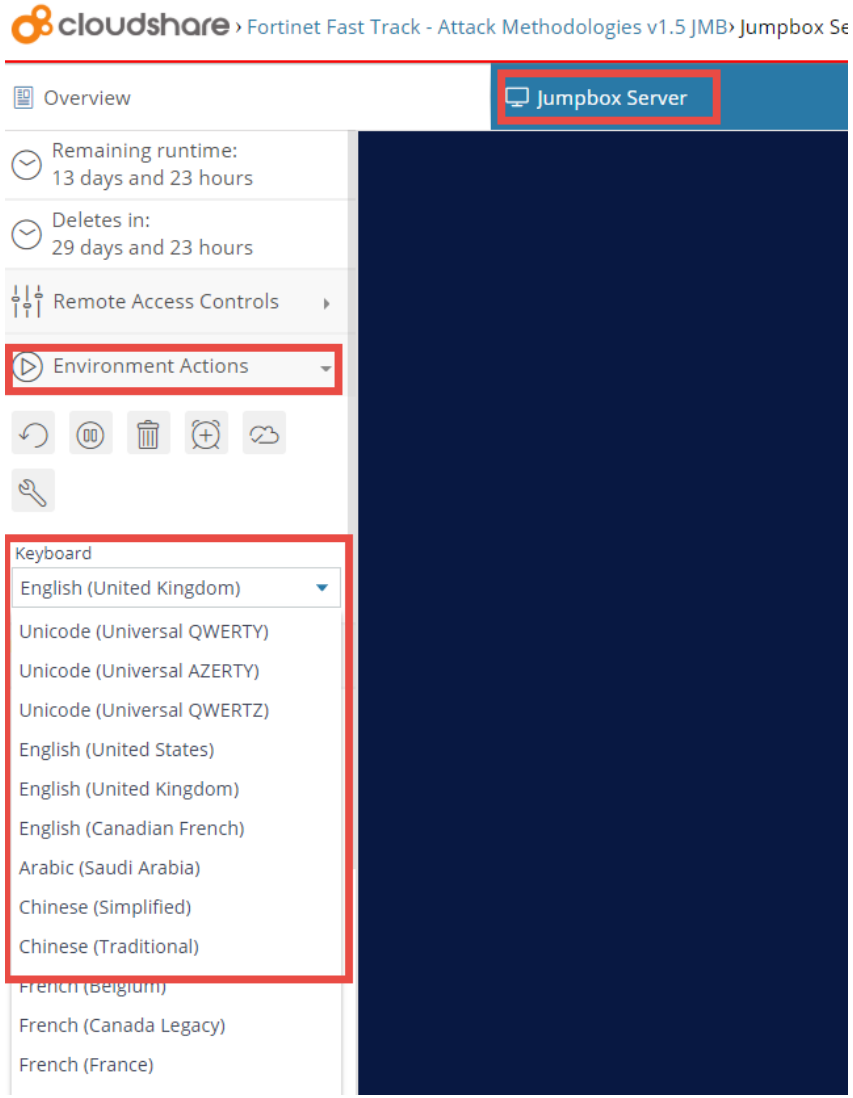
- These same steps can be used to place a second browser window on a separate monitor



Keyboard Layouts

- Keyboards on Windows and Linux hosts can be changed for non-US keyboard environments

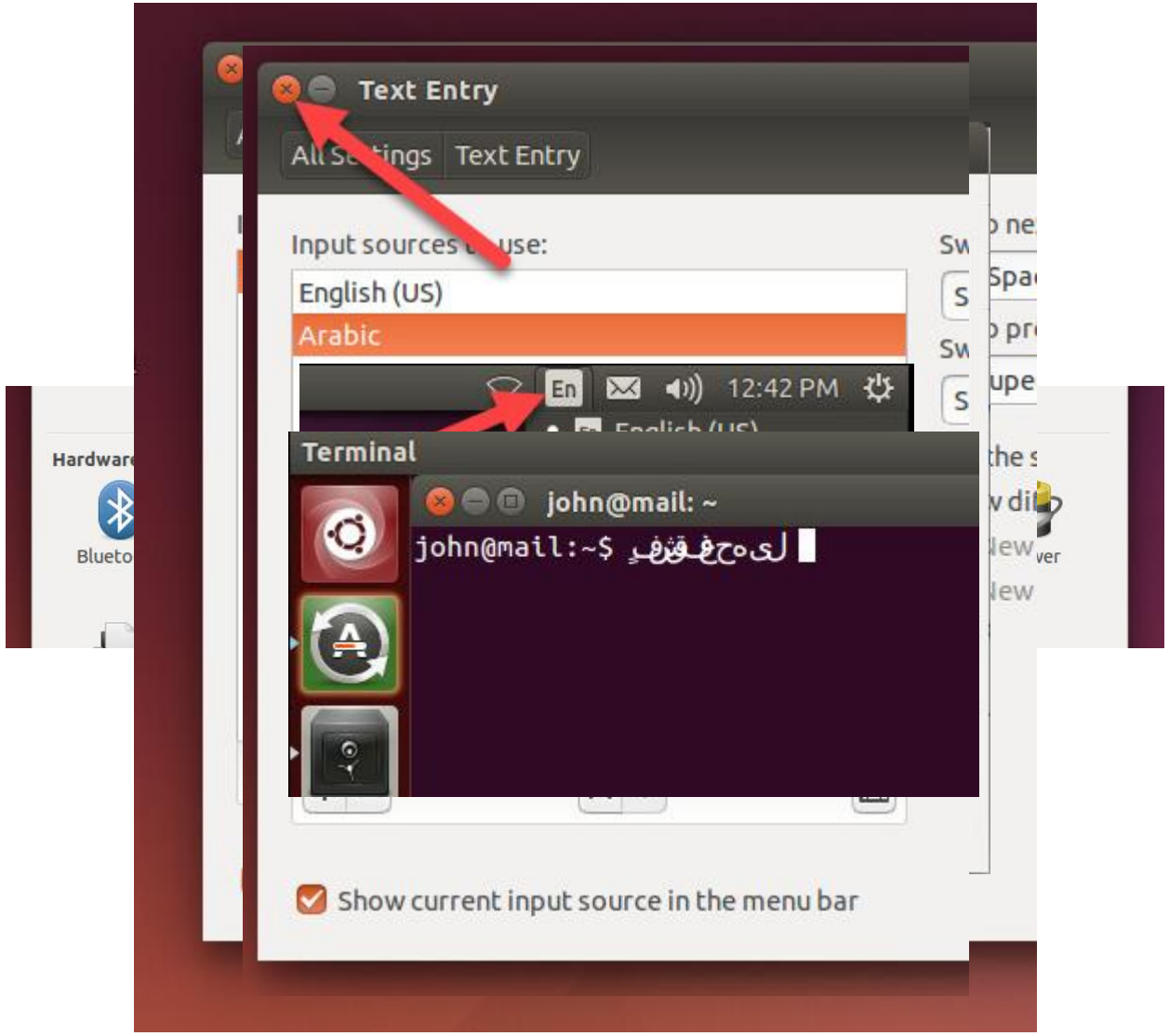
- Windows host:
  1. Under **Environment Actions,** use the keyboard drop-down list to select a keyboard
  2. To apply the new keyboard, log out of Jumpbox, then log back in



Keyboard Layouts (cont)

- Ubuntu 14.04 (NGFW)

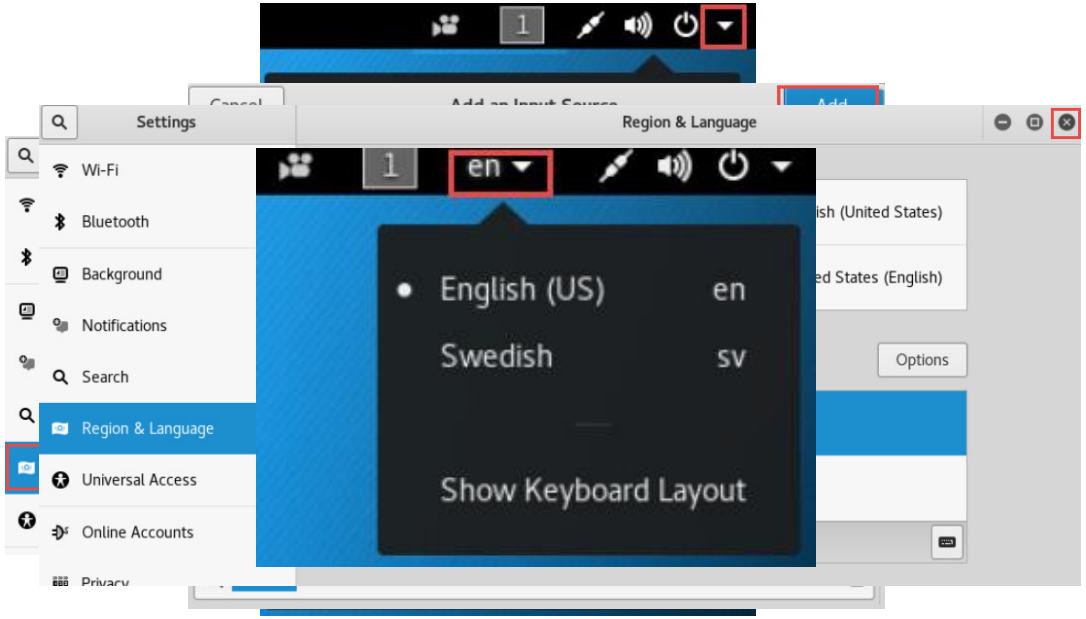
1. Must be done from inside the host
2. Log in, click the gear icon on the top right and click **System Settings…**
3. Click **Keyboard**
4. Click **Text Entry**
5. Click **+**
6. Select a keyboard layout and click **Add**
7. Close the window
8. Click the **Keyboard Layout** icon on top right and click the new layout



Keyboard Layouts

- Ubuntu 18.04 & Kali Host (Security Fabric & FortiWeb)

1. Must be done from inside the host
2. Log in, click the drop-down list on the top right and select the **Settings** icon
3. Click **Region and Language** and click the + icon under **Input Sources**
4. If required, use the button on the bottom of the window to search for a keyboard
5. Click the keyboard and click **Add**
6. Close the window
7. Click the **Keyboard Layout** icon on top right and click the new layout panel

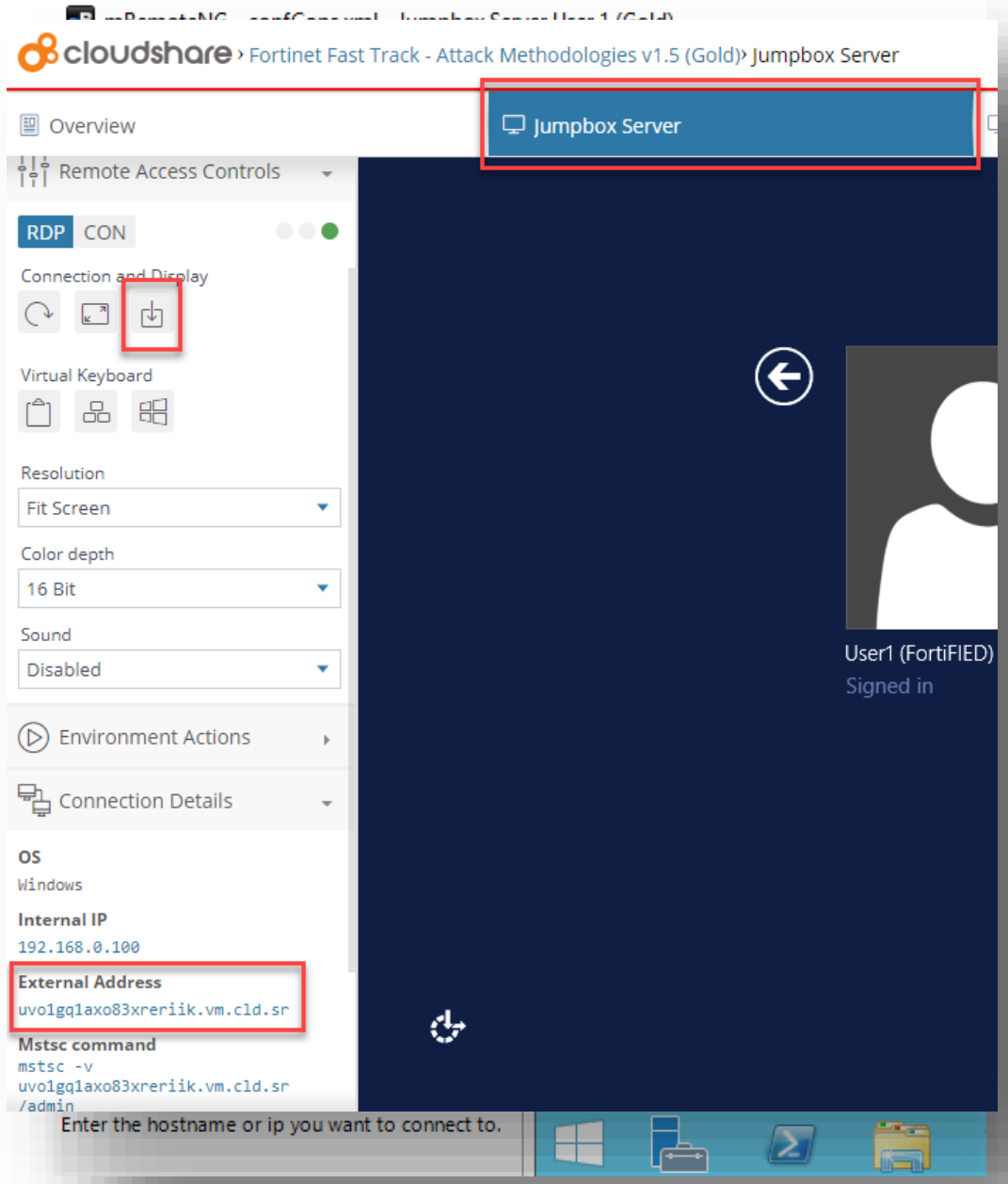


Extended RDP Access

- Easiest and quickest access is through the browser interface

- RDP client access provided
  - RDP config download
  - External address link

- Benefits
  - Allows students to use an interface that is most familiar to them
  - Custom configuration
  - Lets students use a tablet as a secondary screen



Use Tablet as a Secondary Screen

- Install an RDP client on tablet (for example Parallels)
- Email or transfer the CloudShare external access link to tablet
- Tablets works well for Jumpbox access and the FortiFIED app
- Secondary VMs still require using the web portal interface