

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



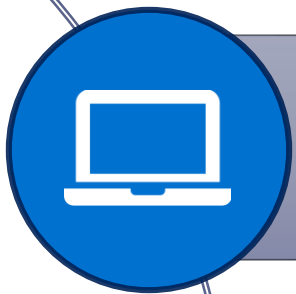
Objectives

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

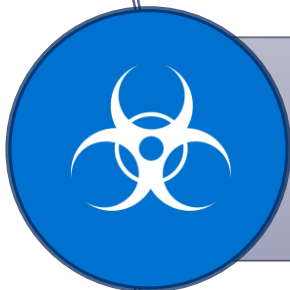
Конечные точки – сценарии использования

Потребность в видимости, контроле и защите

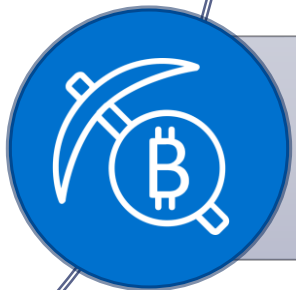
Конечные точки остаются целью атак



44% опрошенных компаний признали, что за последние 24 месяца была взломана одна или несколько конечных точек¹



30% нарушений включают вредоносное ПО²



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

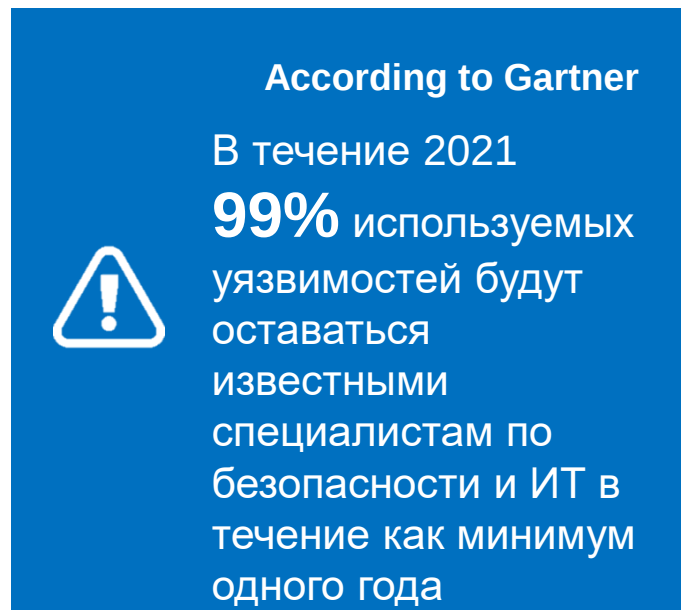
³ FortiGuard Labs Quarterly threat report, Q1 2018

© Fortinet Inc. All Rights Reserved.

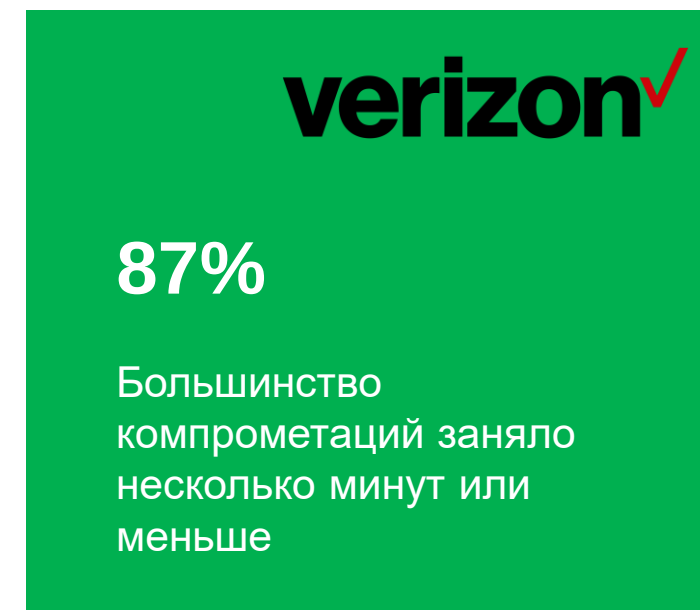
Пробелы в безопасности конечных точек



Недостаток видимости



Уязвимости



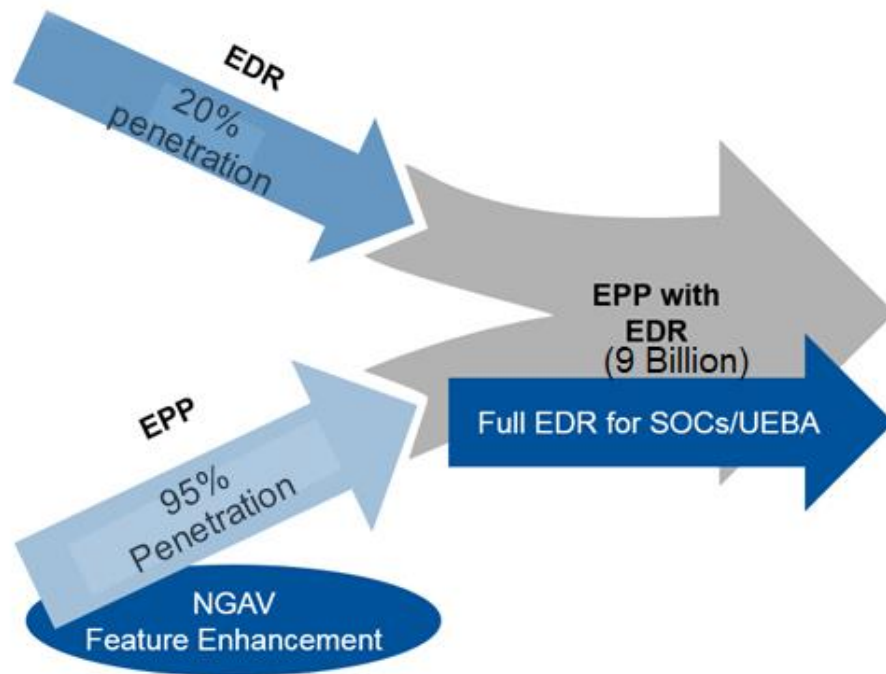
Атаки происходят быстро

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

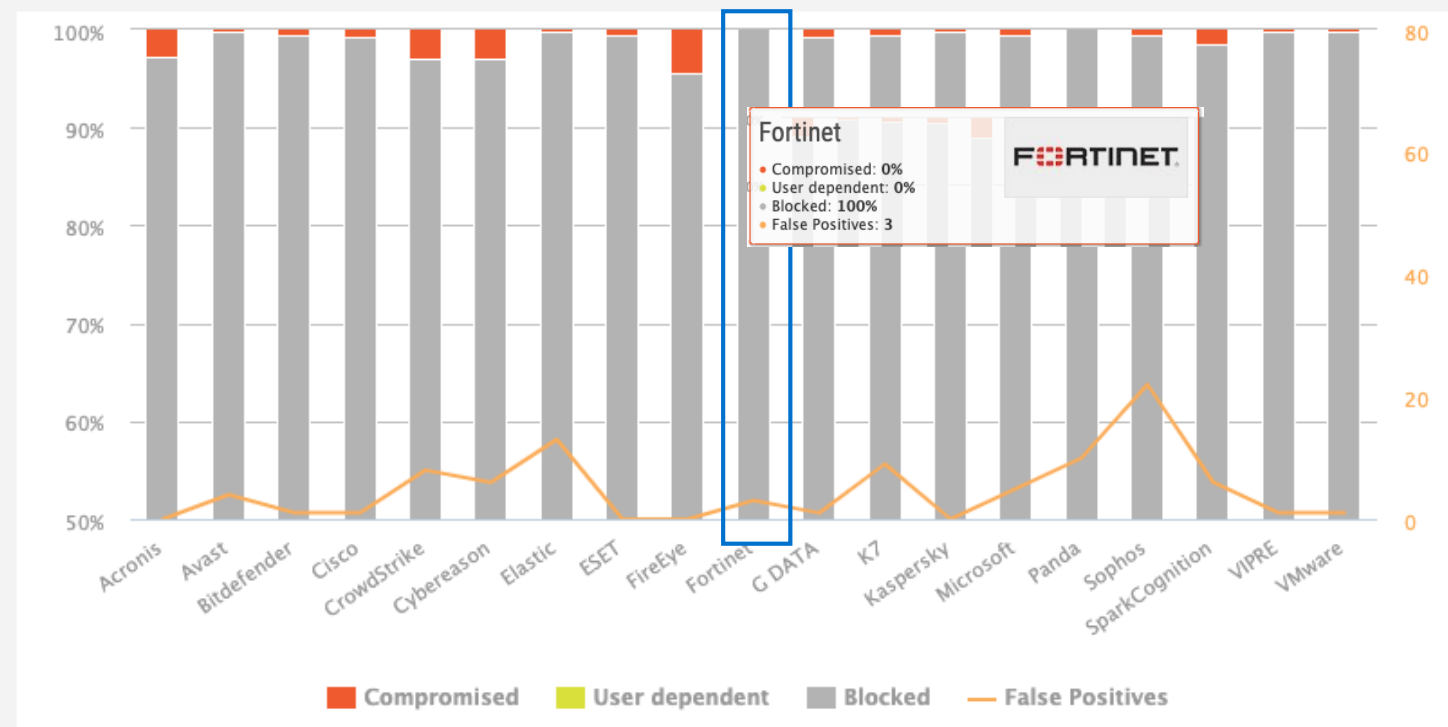
✓ Наименьшее количество
false positive (3)

NSS Labs – рейтинг AA

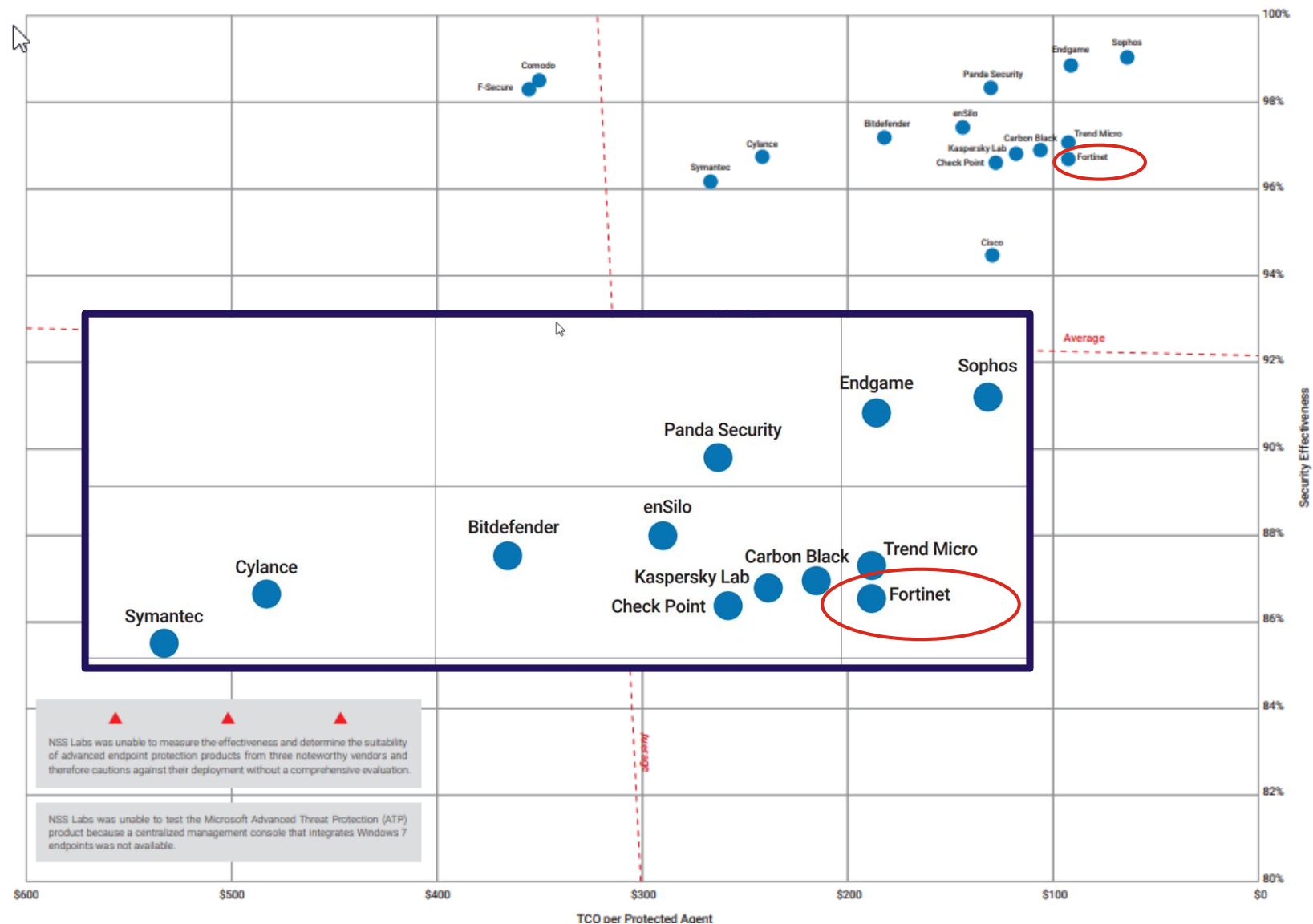
Test Results

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



Безопасность конечных точек и ландшафт угроз

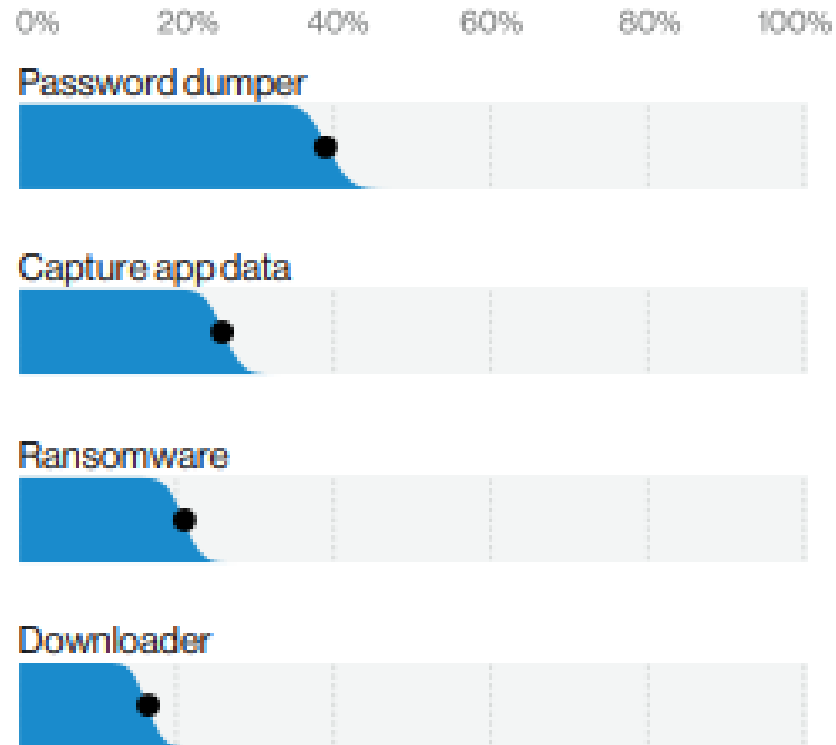


Figure 16. Top Malware varieties in breaches (n = 506)

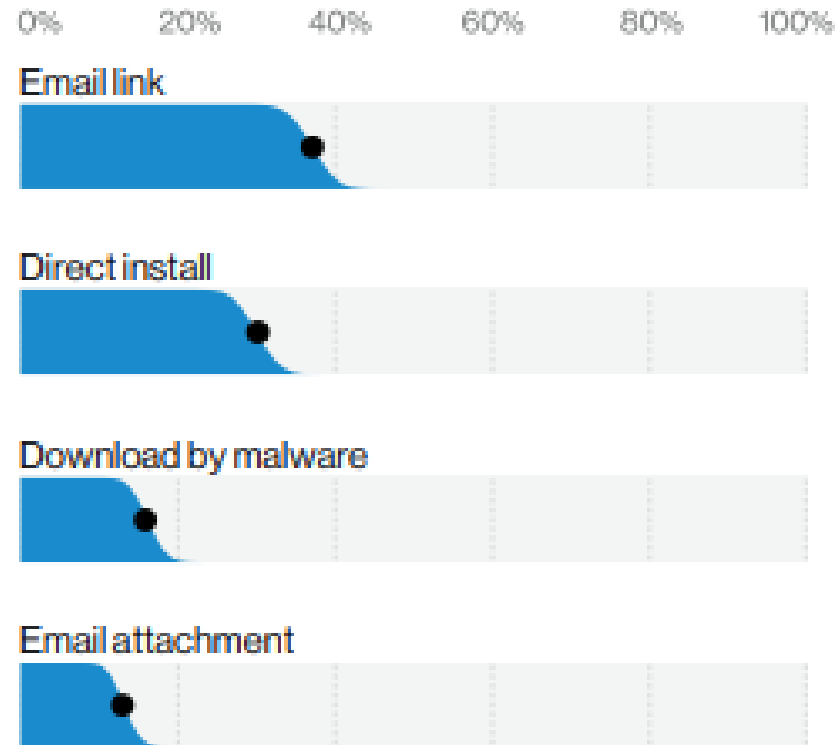


Figure 17. Top Malware vectors in breaches (n = 360)

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

2

1

ENDPOINT PROTECTION (EPP)

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



ADVANCED THREAT PROTECTION

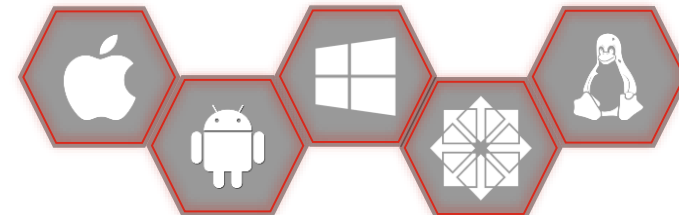
Sandbox Integration

SECURE REMOTE ACCESS

SSL & IPSec VPN, SSO

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



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

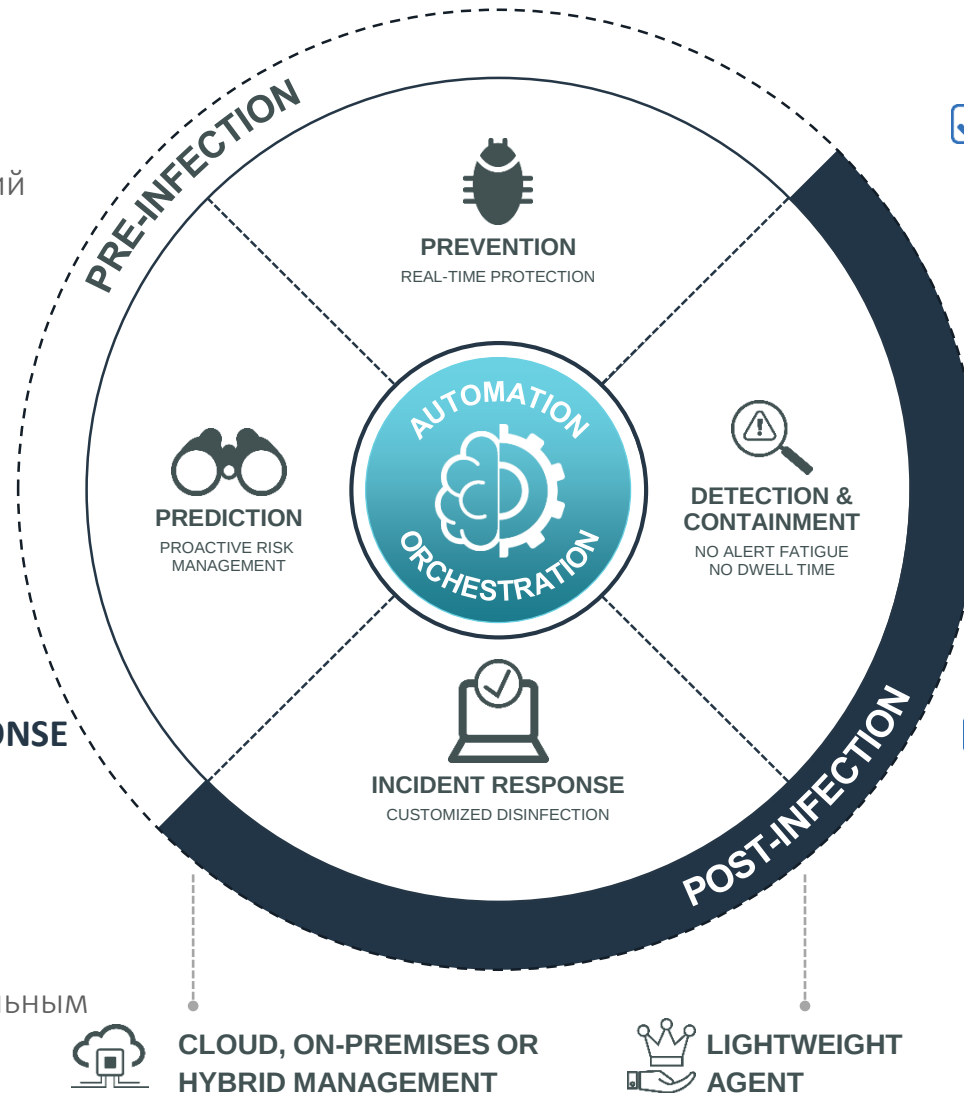
Автоматическая безопасность в реальном времени с организованным реагированием на инциденты

✓ 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 ORCHESTRATED INCIDENT RESPONSE

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



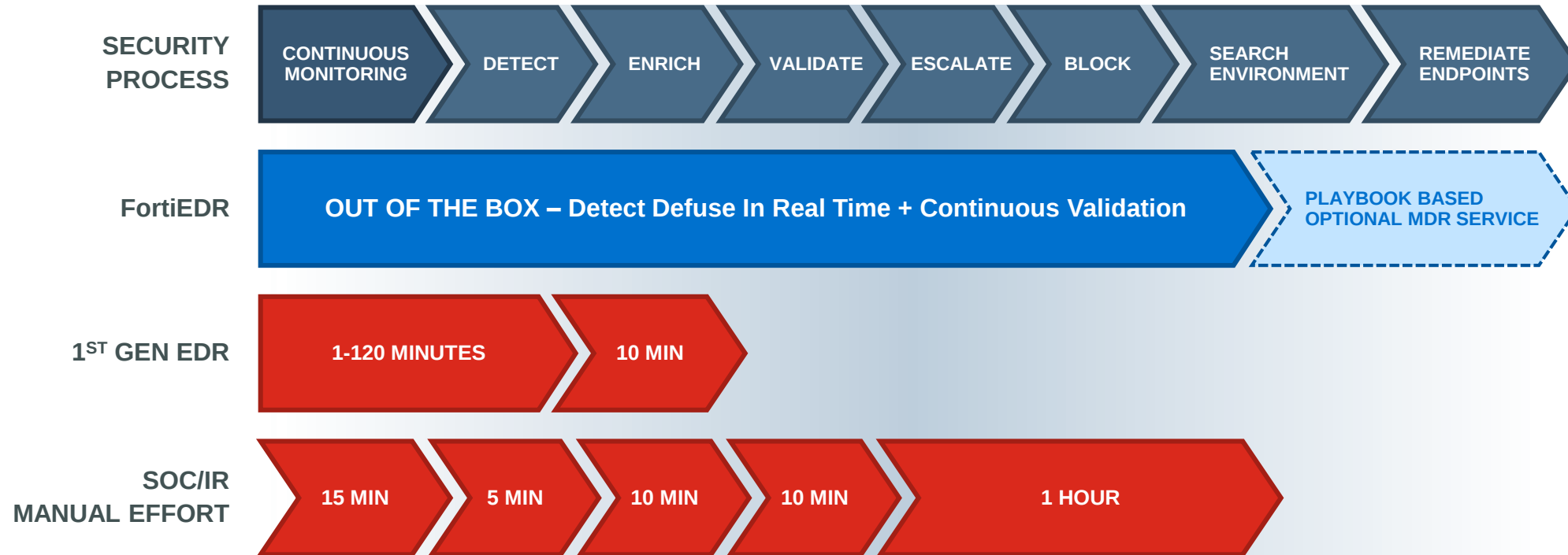
✓ REAL-TIME PREVENTION

- 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 DETECTION AND CONTAINMENT

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

Ручное реагирование vs. Автоматическое реагирование



Уменьшение шума и повышение зрелости SOC

EVENTS

Archive

Mark As

Export

Handle Event

Delete

Forensics

Exception Manager

☐ Unhandled

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
ensw-lap117 (1 event)			Suspicious		31-Dec-2018, 02:10:21	
☐	1167471	ensw-lap117	MSIE585.tmp	Safe	Modify OS Settin...	31-Dec-2018, 02:10:21 31-Dec-2018, 02:10:48
Certificate: Unsigned			Process path: \Device\HarddiskVolume3\Windows\Installer\MSIE585.tmp		Raw data items: 2	
☐	DESKTOP-BS09MQF (1 event)		Suspicious		18-Nov-2018, 15:37:07	
☐	ensw-lap151 (1 event)		Inconclusive		28-Oct-2018, 03:32:11	
☐	ensw-lap146 (2 events)		Suspicious		25-Oct-2018, 10:47:03	
☐	ENSW-LAP108 (3 events)		Malicious		10-Oct-2018, 01:57:50	
☐	ensw-lap-152 (3 events)		Malicious		04-Oct-2018, 08:02:28	

CLASSIFICATION DETAILS

Safe

By ReversingLaos

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Safe, by enSiloCloudServices, on 08-Nov-2018, 06:21:11

Inconclusive, by enSilo, on 08-Nov-2018, 06:21:07

EVENTS

Showing 1-4/4

Search Event

ArchiveMark As...ExportHandle EventDeleteForensicsException Manager

	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 **FEARTNET**
By [ReversingLabs](#)
Threat name: Win32.Trojan.Gandcrab
Threat family: Gandcrab
Threat type: Trojan

History

ADVANCED DATA

[Event Graph](#)

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...



Автоматическая переклассификация



DASHBOARD

EVENT VIEWER 465

FORENSICS ▾

COMMUNICATION CONTROL ▾ 2018

SECURITY SETTINGS ▾

INVENTORY ▾ 14

ADMINISTRATION 1179

 Protection

EVENTS

 Unarchive

 Mark As...

 Export ▾

 Handle Event

 Delete

 Forensics

 Exception Manager

☐ Archived

ID

DEVICE

PROCESS

CLASSIFICATION ▴

DESTINATIONS

RECEIVED ▾

LAST UPDATED

☐ BEN-PC (104 events)

 Malicious

23-Mar-2020, 08:10:24

1-10/104

☐	1756436	BEN-PC	net.technipack.launcher...	 Likely Safe	2 destinations	23-Mar-2020, 08:10:24	23-Mar-2020, 08:10:31	
☐	1752680	BEN-PC	RemotrService.exe	 Safe	2 destinations	21-Mar-2020, 20:20:51	21-Mar-2020, 20:21:02	
▶  User: BEN-PC\ben Certificate: Signed Process path: \Device\HarddiskVolume2\Program Files (x86)\Remotr\RemotrService.exe Raw data items: 2								
☐	1752622	BEN-PC	RemotrService.exe	 Safe	Service Access	21-Mar-2020, 20:20:49	21-Mar-2020, 20:20:49	
☐	1752609	BEN-PC	RemotrService.exe	 Safe	6 destinations	21-Mar-2020, 20:20:49	21-Mar-2020, 20:20:52	
☐	1709408	BEN-PC	DiscordHookHelper.exe	 Likely Safe	93.184.220.29	05-Mar-2020, 19:45:04	05-Mar-2020, 19:45:04	
☐	1705725	BEN-PC	org.gradle.launcher.dae...	 Likely Safe	5 destinations	04-Mar-2020, 16:57:47	04-Mar-2020, 16:59:43	
☐	1696154	BEN-PC	DiscordHookHelper.exe	 Likely Safe	File Execution ...	27-Feb-2020, 11:16:27	29-Feb-2020, 11:47:51	

CLASSIFICATION DETAILS

 Safe  FORTINET

By [ReversingLabs](#)

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

 Safe, by FortinetCloudServices , on 21-Mar-2020, 20:21:10

 Inconclusive, by Fortinet , on 21-Mar-2020, 20:20:59

Управляемый интерфейс с обогащением данных

The screenshot displays the Fortinet SIEM interface, which is divided into several sections:

- EVENTS:** A table listing security events. The table has columns for 'Source', 'Process', 'Classification', 'Destination', 'Revised', and 'Last Updated'. The first event is a 'Malicious' event from '1542111' (DESKTOP-PKQ1M6) to 'NO-40.exe' on '13-Dec-2018, 14:55:24'. Other events include 'File Write Access', 'Modify OS Service', 'File Creation', 'File Service Access', and 'File Deletion'.
- CLASSIFICATION DETAILS:** A section on the right providing details for the selected event. It includes the 'Malicious' classification, the file path 'C:\Windows\System32\cmd.exe', and a 'History' section showing the event was detected by 'm500' on '13-Dec-2018, 14:55:24'.
- Triggered Rules:** A section on the right listing rules that triggered the event. It includes 'SMB Techniques' (T1196, T1197, T1198) and 'Unmapped Executable - Executable File Without a Correlation'. The text explains that an executable running in memory does not have a corresponding file in the file system, which is a technique used by malware to evade detection.
- ADVANCED DATA:** A section at the bottom showing a network diagram. It illustrates a sequence of events: '1 Create' (Process), '2 Create' (Process), '3 Create' (Process), '4 Create' (Process), and '5 Create' (Process). The diagram shows the flow of data between these processes and a central 'Network' node.

Расширенный ответ за счет Fabric-интеграции



Default

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 23

SECURITY SETTINGS

INVENTORY 2

ADMINISTRATION 10

Protection

admin

LICENSING

ORGANIZATIONS

USERS

DISTRIBUTION LISTS

EXPORT SETTINGS

TOOLS

SYSTEM EVENTS

IP SETS

INTEGRATIONS

CONNECTORS

+ Add connector

Firewall

Details

Name FGT001-Server_2 Type FortiGate Host 10.51.122.63 Port 443 User name Admin Password/Key *****

Actions

Block Destination Address Address group FortiEDR_BL

+ Add action

Test connector Save Cancel Delete

NAC: FGT001-Server

Sandbox: SB001

Active Directory: dc01.tech.local

Обнаружение вредоносных IP-адресов

Default

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 23

SECURITY SETTINGS

INVENTORY 2

ADMINISTRATION 10

Protection

admin

EVENTS

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception Manager

☐	All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
☐		powershell.exe (1 event)			Malicious		07-May-2020, 20:38:41	
☐		21722	Einat-PC-0-Test_1	powershell.exe	Malicious	216.239.36.29	07-May-2020, 20:38:41	11-May-2020, 15:38:40
User: ZSARIC-TEST\Victim Certificate: Signed Process path: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe Raw data items: 1								
☐		TeamViewer.exe (1 event)			Safe		07-May-2020, 20:46:15	
☐		WinBio.dll (1 event)			Malicious		07-May-2020, 20:51:00	

CLASSIFICATION DETAILS

Malicious

By ReversingLabs

Threat name: Win32.Trojan.Zbot

Threat family: Zbot

Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 11-May-2020, 15:39:03

Process ...1.0\powershell.exe\ with PID 108 was terminated at device Einat-PC-0-Test_1 2 times

IP 216.239.36.29 was added to malicious IP addresses on firewall Fortigate 10.51.122.63

Triggered Rules

Exfiltration Prevention

Malicious File Detected

Suspicious Application - Connection Attempt from a Suspi...

ADVANCED DATA

Контекстные сценарии реагирования на инциденты FortiEDR

Default

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 147

Protection

admin

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Clone Playbook

Set Mode

Assign Collector Group

Delete

NAME

Default Playbook

Fortinet

NOTIFICATIONS

sent in protection and simulation modes

Send mail notification

SMTP must be defined under [Hoster Admin](#) settings

Send syslog notification

Syslog must be defined under [Admin](#) settings

Open ticket

Open ticket must be defined under [Admin](#) settings

INVESTIGATION

Isolate device

Move device to the High Security group

REMEDiation

Terminate process

Delete file

Clean persistent data

Block address on Firewall

Firewall-1, Firew...

All Firewalls

Firewall-2

Firewall-1

ASSIGNED COLLECTOR GROUPS

Unassign Group

High Security Collector Group (0 collectors included)

Default Collector Group (2 collectors included)

Интеграция с межсетевым экраном

FortiGate VM64 FGVM02TM20002532

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

Authentication Rules

Local In Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shapers

Traffic Shaping Policy

Traffic Shaping Profile

Security Profiles

VPN

User & Device

WiFi & Switch Controller

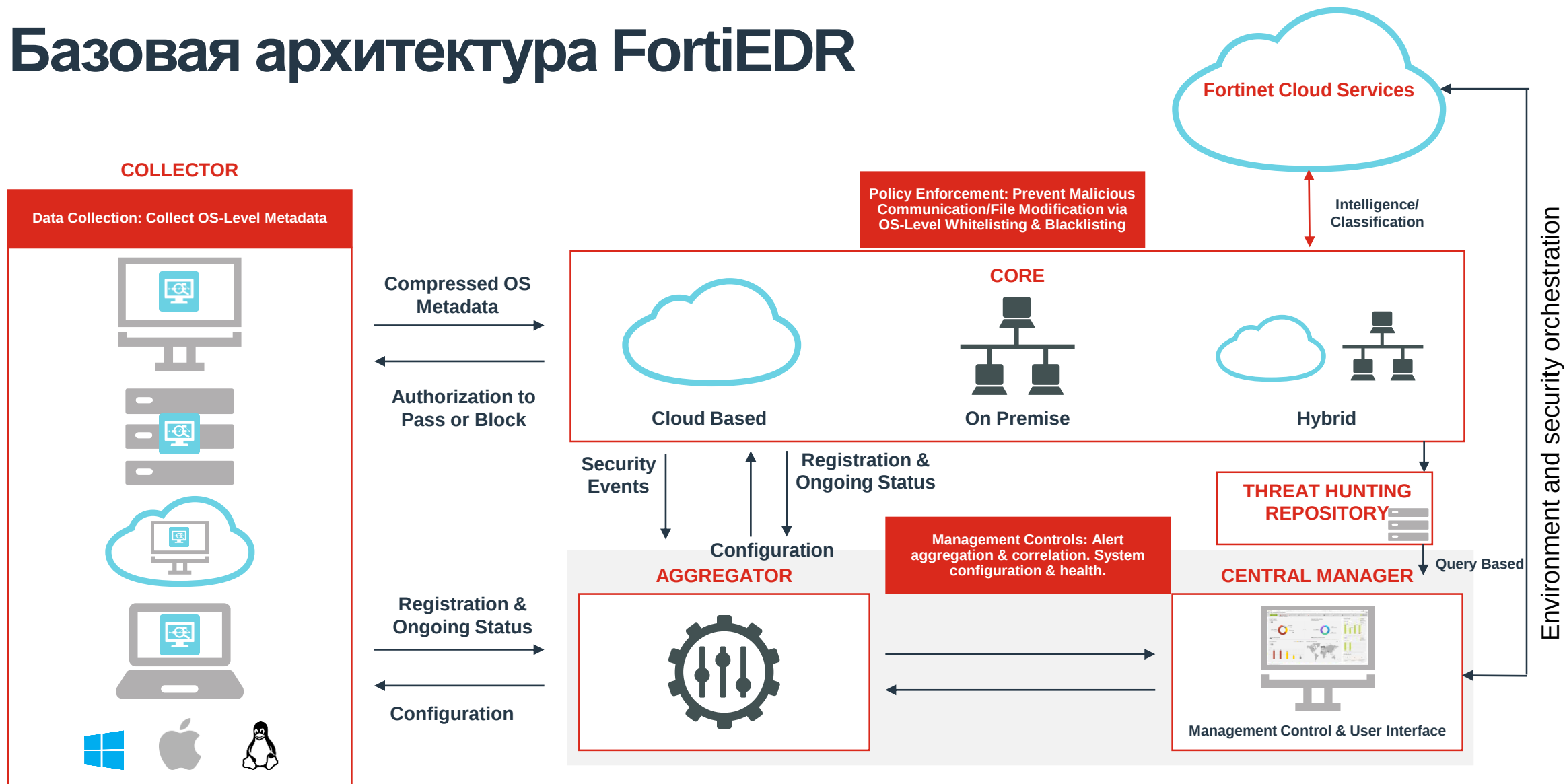
Log & Report

Monitor

Create New Edit Clone Delete Search

Name	Type	Details	Interface	Visibility	Ref.
Address 12					
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
FortiEDR_216.239.36.29	IP Range	216.239.36.29 - 216.239.36.29		Hidden	1
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	2
all	Subnet	0.0.0.0/0		Visible	1
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	1
wildcard.dropbox.com	FQDN	*.dropbox.com		Visible	0
wildcard.google.com	FQDN	*.google.com		Visible	1
Address Group 4					
FortiEDR_BL	Address Group	FortiEDR_216.239.36.29		Visible	1
G Suite	Address Group	gmail.com wildcard.google.com		Visible	0
Microsoft Office 365	Address Group	login.microsoftonline.com login.microsoft.com login.windows.net		Visible	0
test_group	Address Group	none		Visible	0

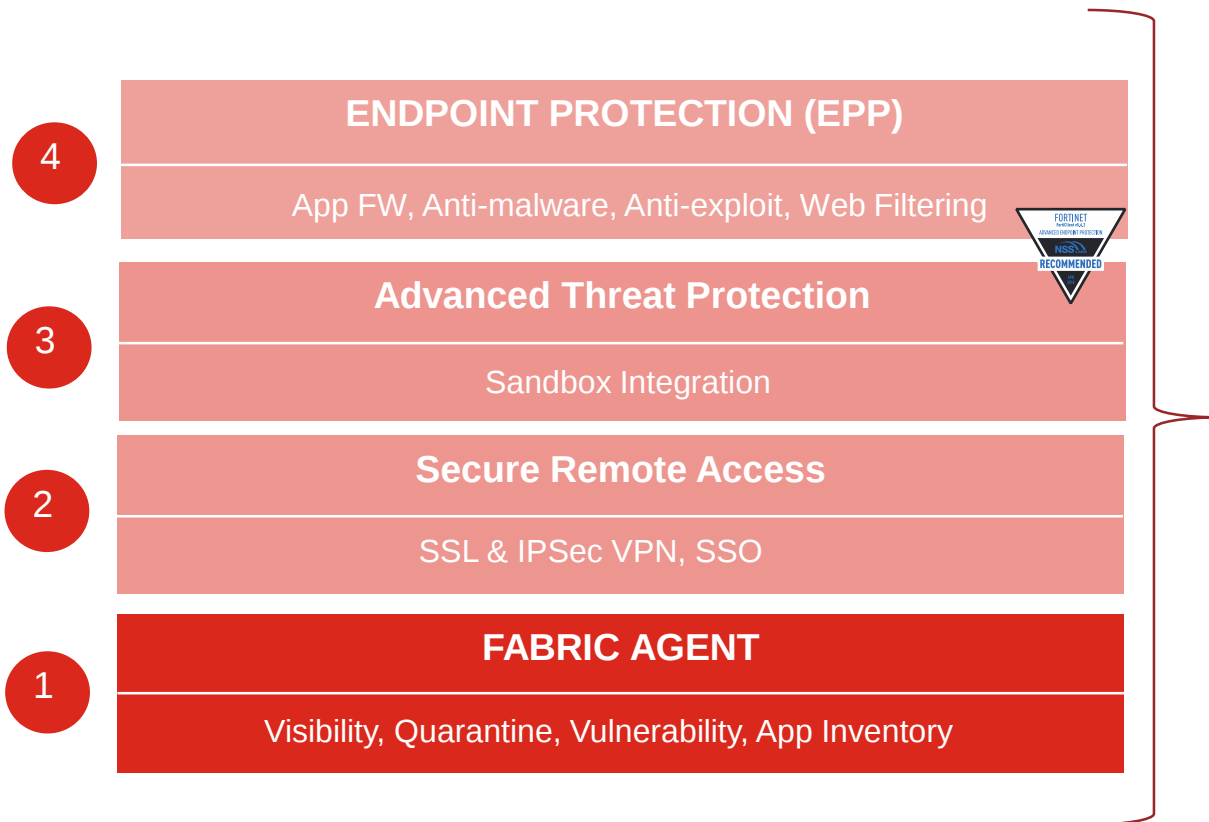
Базовая архитектура FortiEDR



FortiClient Fabric Agent

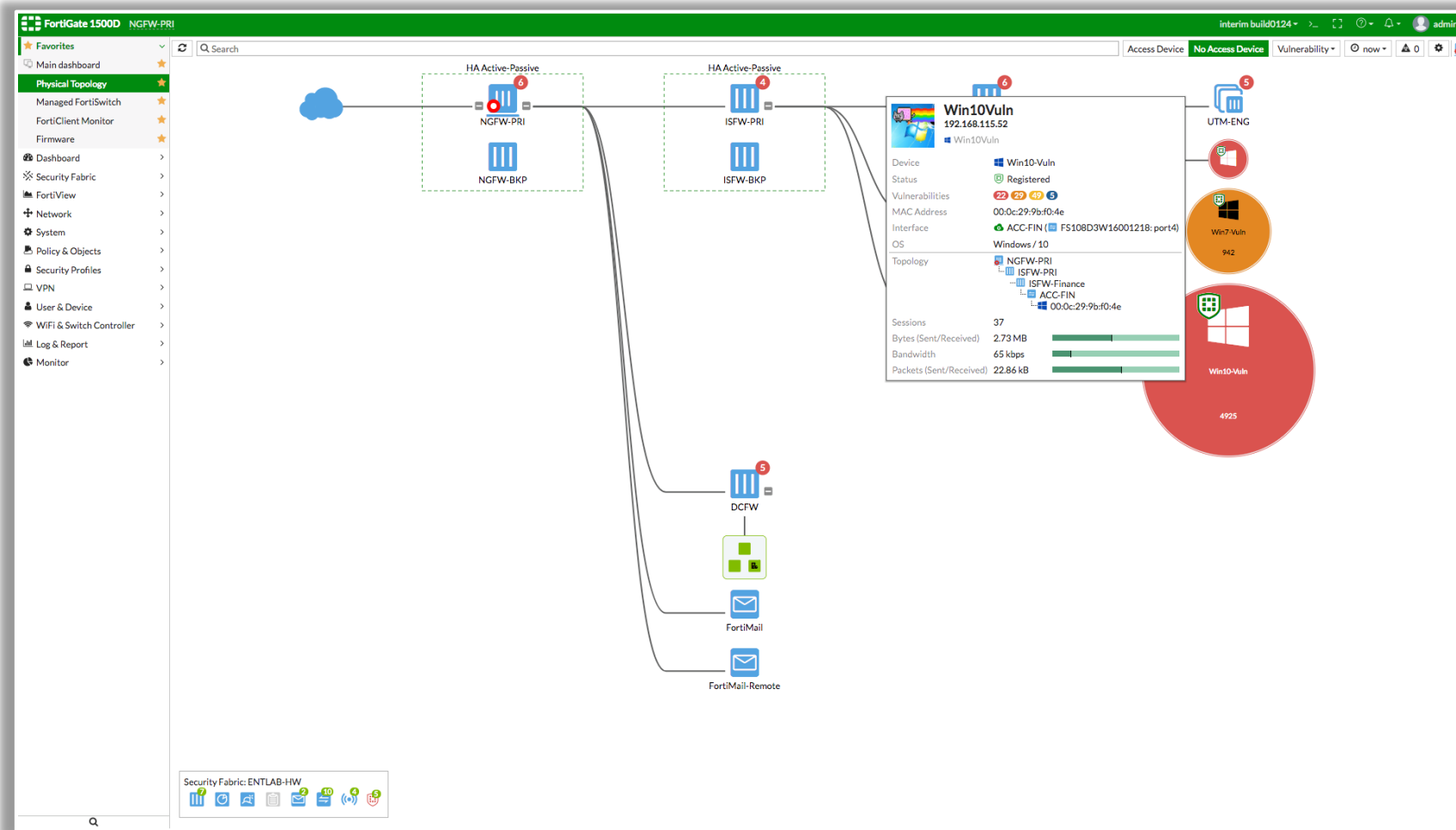
Видимость, контроль и автоматизация для конечных точек

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

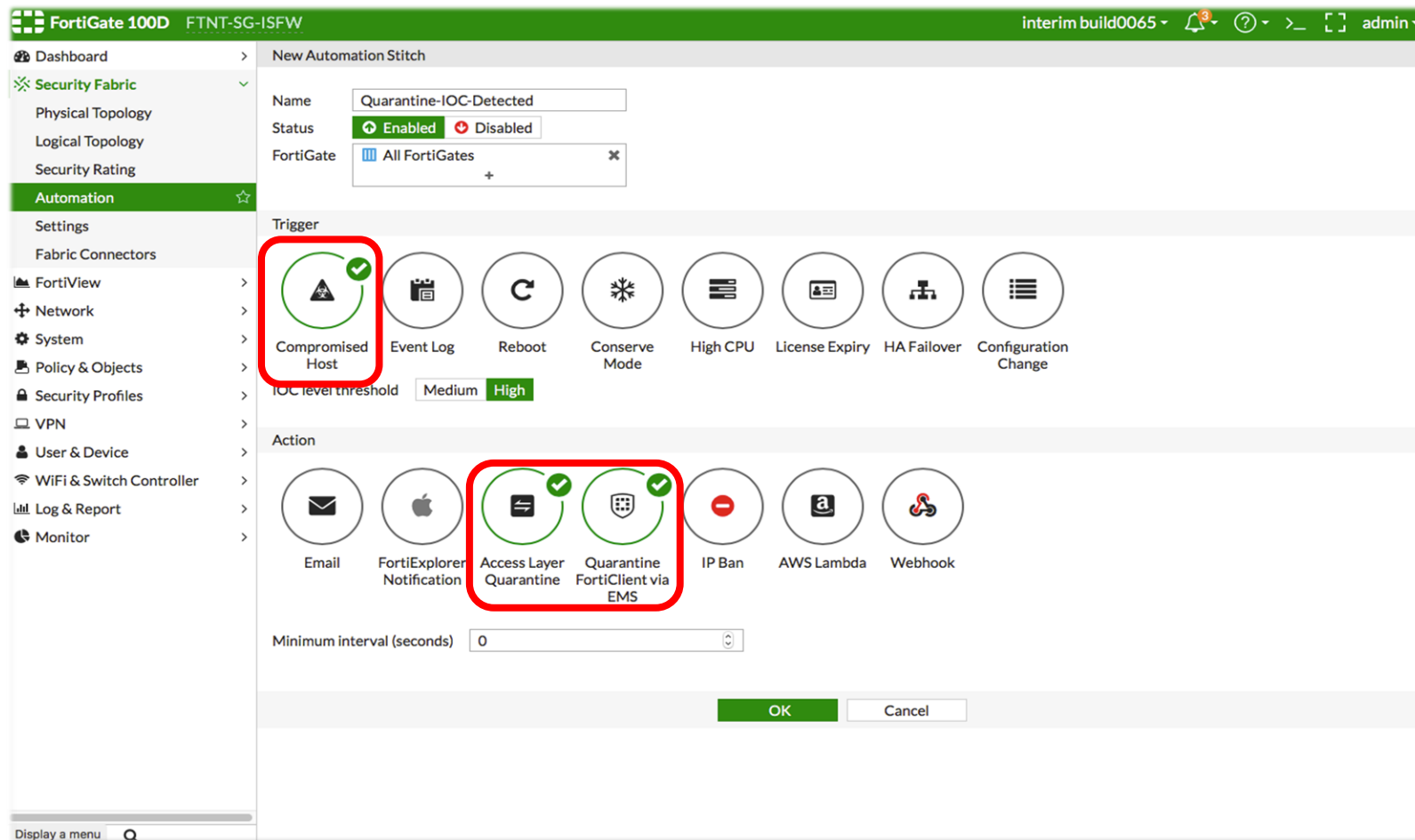
Наглядность уровня риска



- 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

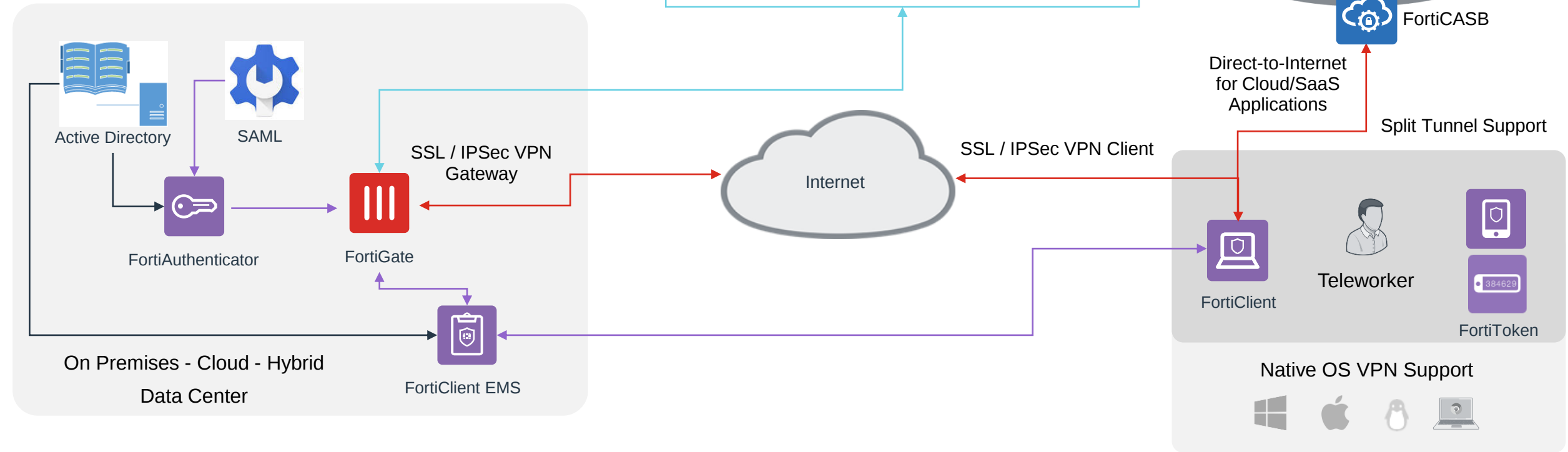


Безопасный удаленный доступ

Интегрированный, Always-on VPN

Single Sign on

Teleworker Access



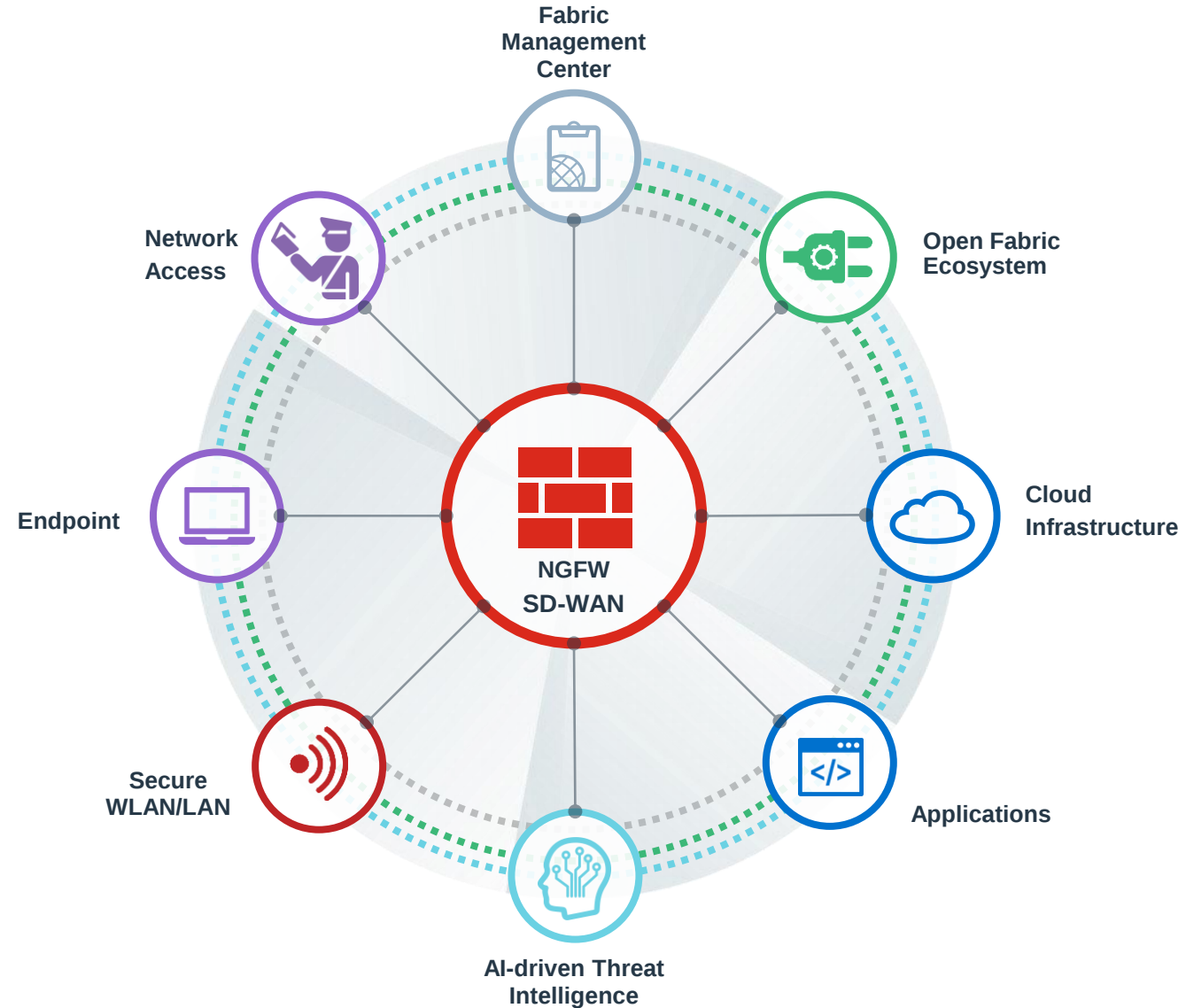
FortiClient EMS

FortiClient Enterprise Management Server

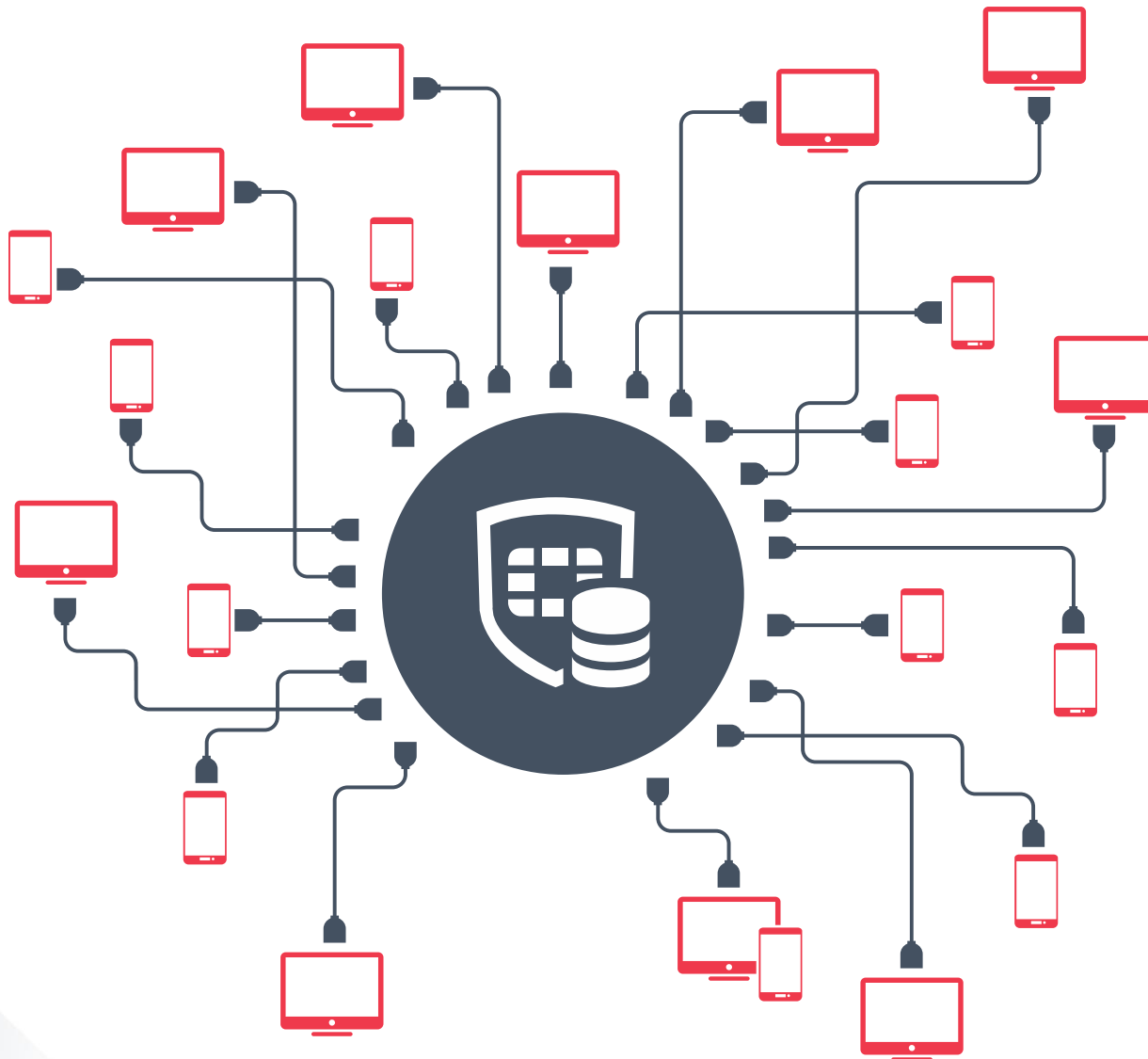
FortiClient EMS

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



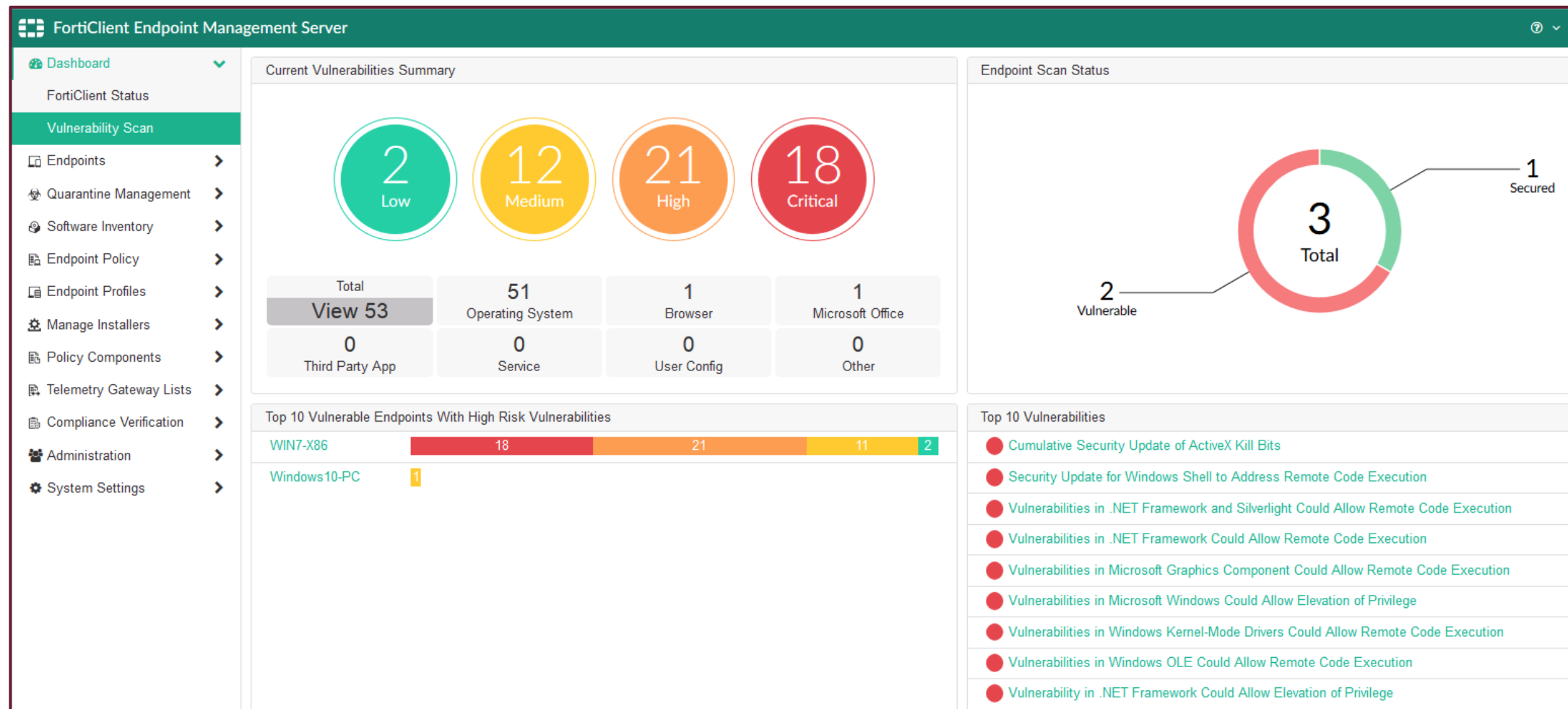
Централизованное управление с помощью EMS



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

FortiClient Endpoint Management Server							?	▼				
Dashboard	>	 15 Total Applications		 9 Total Vendors		 10 New Detections						
Endpoints	>											
Quarantine Management	>	Display by Vendor ▼										
Software Inventory	▼	Name	▼	Vendor	▼	Version	▼	First Detected	▼	Last Installed	▼	Install Count
Applications		▼ Adobe Systems Incorporated (1)										
Hosts		 Adobe Flash Player 18 NPAPI		Adobe Systems Incorporated		18.0.0.194		2018-09-29		2017-11-15		1
Endpoint Policy	>	▼ Fortinet Technologies Inc (2)										
Endpoint Profiles	>	 FortiClient		Fortinet Technologies Inc		6.0.5.0209		2019-02-12		2019-02-12		1
Manage Installers	>	 FortiClient		Fortinet Technologies Inc		6.2.2.0877		2019-11-21		2019-11-21		1
Policy Components	>	▼ Google LLC (2)										
Telemetry Gateway Lists	>	 Google Chrome		Google LLC		78.0.3904.97		2019-11-21		2019-11-12		1
Compliance Verification	>	 Google Update Helper		Google LLC		1.3.35.341		2019-11-21		2019-11-08		1
Administration	>	▼ Microsoft Corporation (2)										
System Settings	>	 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

The screenshot displays the FortiClient Endpoint Management Server interface. The left sidebar shows the navigation menu with 'Local Profiles' expanded and 'Default' selected. The main panel shows the 'Web Filter' settings for the 'Default' profile. The 'Web Filter' toggle is turned on. Under the 'General' tab, several options are enabled: 'Client Web Filtering When On-Net', 'Log All URLs', 'Log User Initiated Traffic', 'Enable Web Browser Plugin for Web Filtering', 'Sync Mode', 'Check User Initiated Traffic Only', and 'Enable Safe Search'. The 'Site Categories' section is also enabled. A red box highlights the 'Site Categories' list, and a red arrow points from the 'Adult/Mature Content' category in the main panel to a detailed view of the categories in the right panel.

FortiClient Endpoint Management Server

Profile Name: Default

Malware | Sandbox | **Web Filter** | Firewall | VPN | Vulnerability

Web Filter ☒

General

- ☒ Client Web Filtering When On-Net ⓘ
- ☒ Log All URLs
- ☒ Log User Initiated Traffic
- ☒ Enable Web Browser Plugin for Web Filtering ⓘ
- ☐ Sync Mode ⓘ
- ☐ Check User Initiated Traffic Only ⓘ
- ☒ Enable Safe Search

☒ **Site Categories** ⓘ

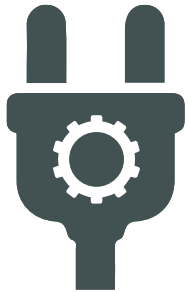
- + Adult/Mature Content
- + Bandwidth Consuming
- + General Interest - Business
- + General Interest - Personal
- + Potentially Liable

Site Categories ⓘ

- Adult/Mature Content
- Abortion
- Advocacy Organizations
- Alcohol
- Alternative Beliefs
- Dating
- Gambling
- Lingerie and Swimsuit
- Marijuana
- Nudity and Risque
- Other Adult Materials
- Pornography
- Sex Education
- Sports Hunting and War Games
- Tobacco
- Weapons (Sales)

Fabric EMS коннектор

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



FortiGate VM64 FortiGate-Edge

Dashboard > New Fabric Connector

Security Fabric >

- Physical Topology
- Logical Topology
- Security Rating
- Automation
- Settings

Fabric Connectors ☆

- FortiView >
- Network >
- System >
- Policy & Objects >
- Security Profiles >

SSO/Identity

- FortiClient EMS
- FortiNAC
- Fortinet Single Sign-On Agent
- Symantec Endpoint Protection
- Poll Active Directory Server
- RADIUS Single Sign-On Agent

Name ⓘ To Internet

Incoming Interface ISFW Network (port2)

Outgoing Interface Edge Network (port1)

Source FCTEMS0000101980_User_Spec

Destination all

Schedule always

Service ALL

Action ACCEPT DENY

Select Entries

Address	User	Internet Service
FCTEMS0000101980_User_Spec		
FCTEMS0000101980_Trusted_PC_TAG		
FCTEMS0000101980_User_Specified_Tag		
FCTEMS_ALL_FORTICLOUD_SERVERS		
Finance_Network		
FIREWALL_AUTH_PORTAL_ADDRESS		
FortiClient-EMS-Server		
gmail.com		
HR_Network		

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

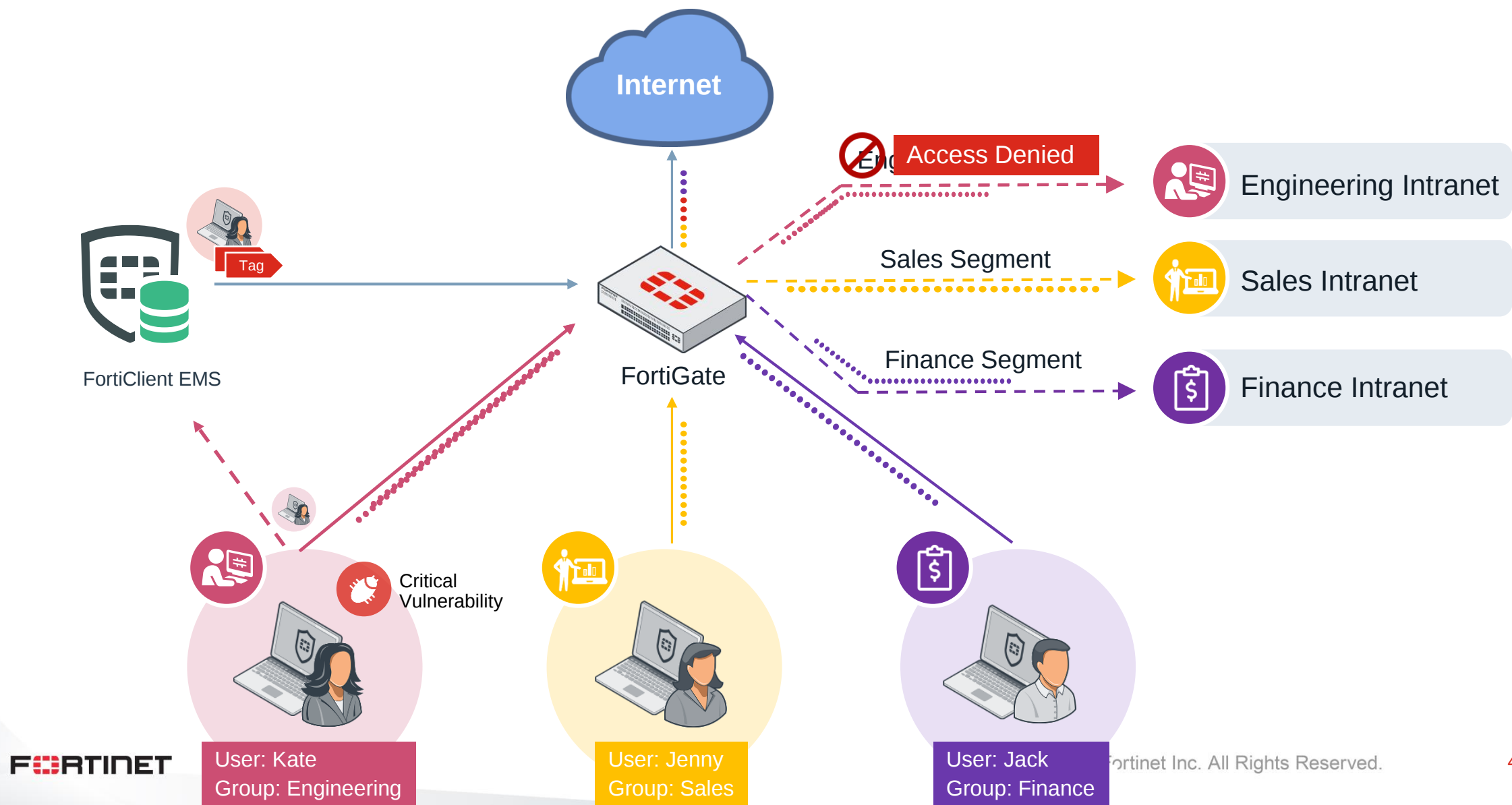
The screenshot displays the FortiClient Enterprise Management Server interface. The top section shows a table of compliance rules. The bottom section shows the Host Tag Monitor, which lists endpoints and their associated tags.

Name	OS	Feature	Value	Assign to	Host Tag	Status
Windows Domain check	Windows	Logged in Domain	fortinet-us.com or fortinet-ca.com or fortinet-cn.com	All	Local User	✓

Endpoint	User	OS	IP	List	Tagged on
BYOD (7)					
ayang-x220	ayang	Windows 7	172.28.1.107	Host Verification List 2	2018-03-12 14:06:34
All Groups/PM					
AHarris	Andrew Harris	Windows 8	172.27.2.209	Host Verification List 1	2018-03-12 09:36:12
All Groups/Docs					
Carrie-PC	Carrie Zhao	Windows 10	172.27.3.200	Host Verification List 2	2018-03-11 11:46:28
All Groups/Designer					
Desktop-3IBDT2	tbirdi	Windows 8	172.28.1.111	Host Verification List 2	2018-03-11 07:22:54
All Groups/test					
Desktop-5DRQ9	In Hye Lee	Windows 8	172.27.2.202	Host Verification List 3	2018-03-11 17:09:11
All Groups/test					
km-lab-pc1	Kunal	Windows 8	172.28.1.105	Host Verification List 3	2018-03-11 15:12:26
All Groups/PM					
LauraW-PC	LauraW	Windows 10	172.27.2.200	Host Verification List 2	2018-03-10 21:11:35
All Groups/Docs					
Vulnerable Endpoints (45)					
Guest Devices (85)					
Corporate Devices (120)					
Insecure Endpoints (86)					

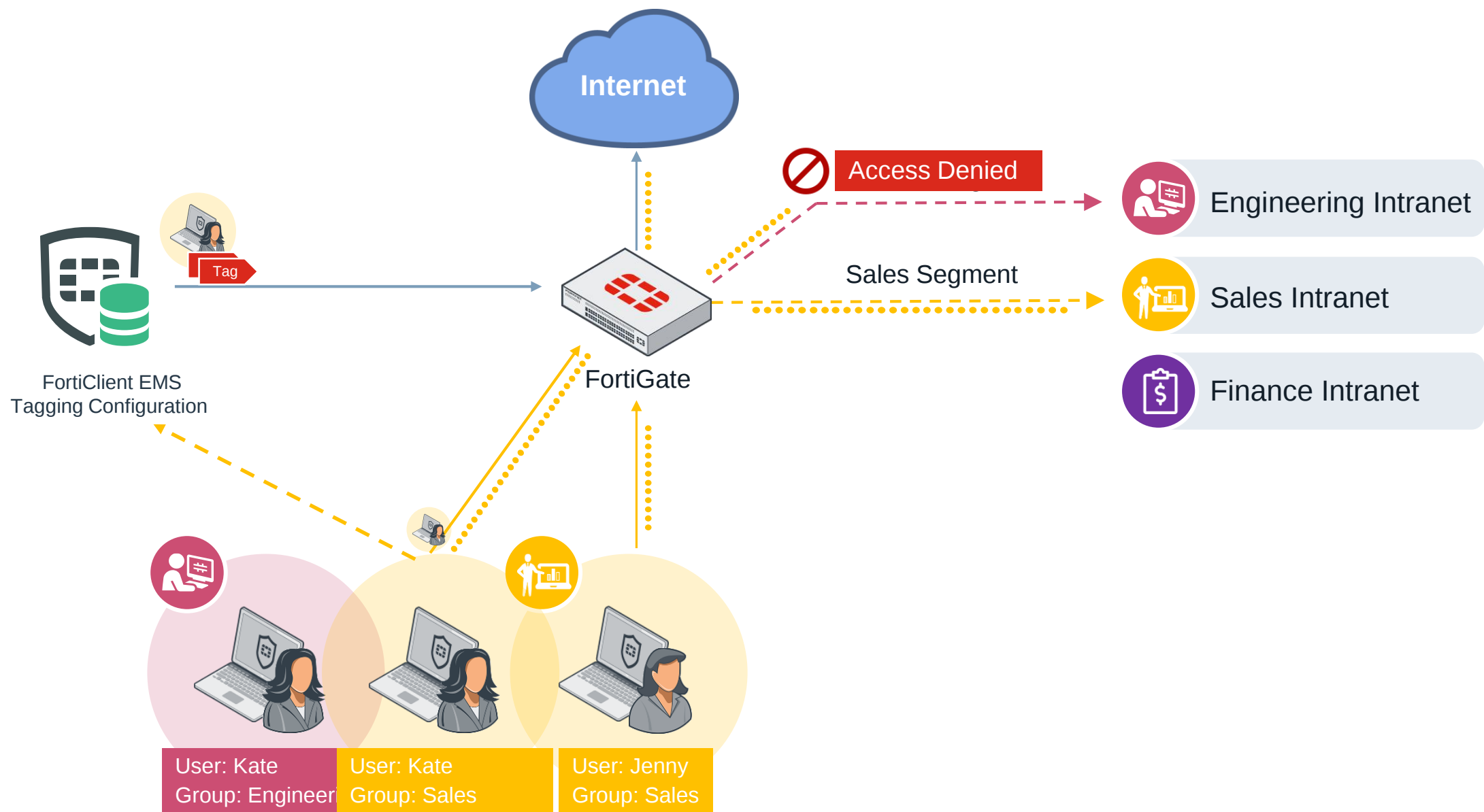
Динамический контроль доступа (сегментация на основе намерений)

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



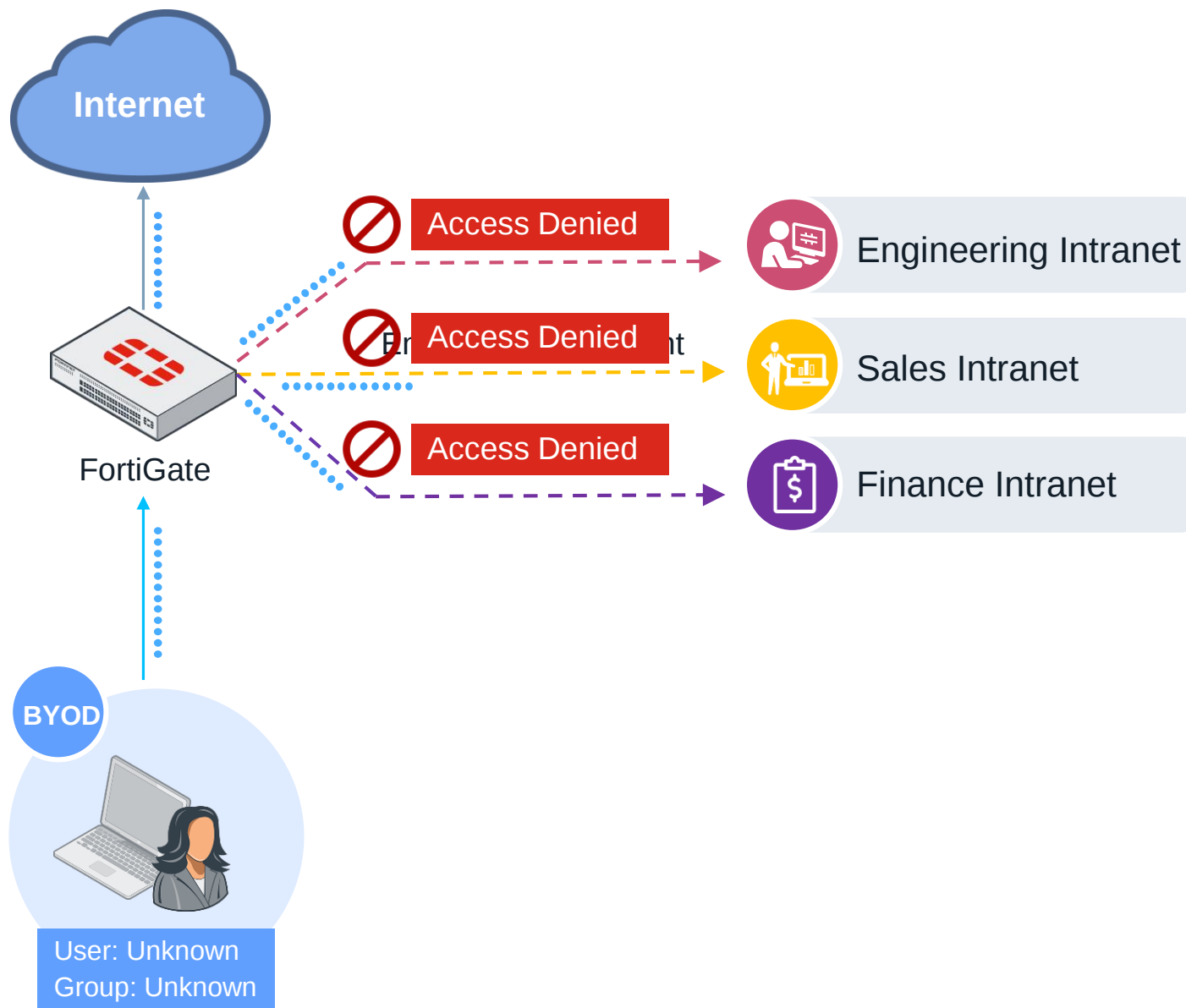
Динамический контроль доступа (сегментация на основе намерений)

Use Case: Доступ на основе групп AD



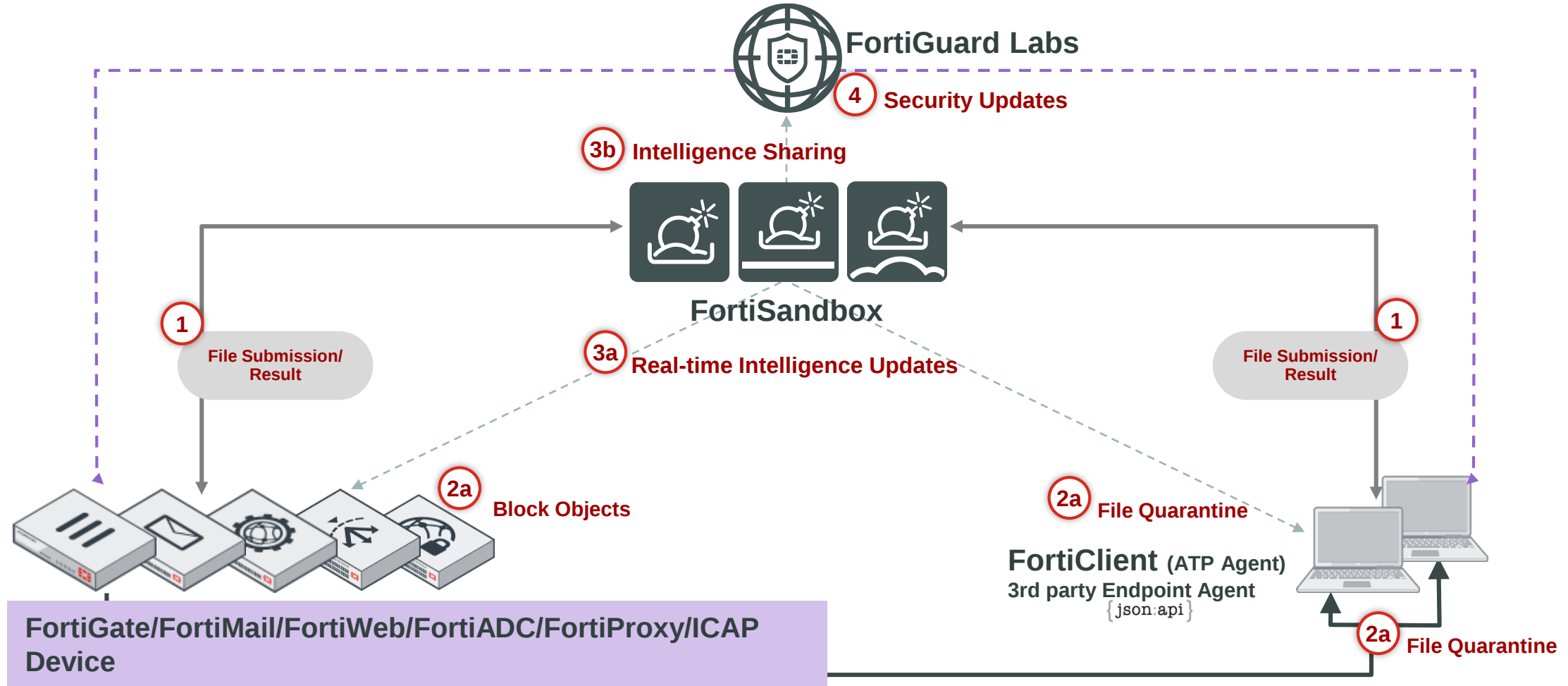
Динамический контроль доступа (сегментация на основе намерений)

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

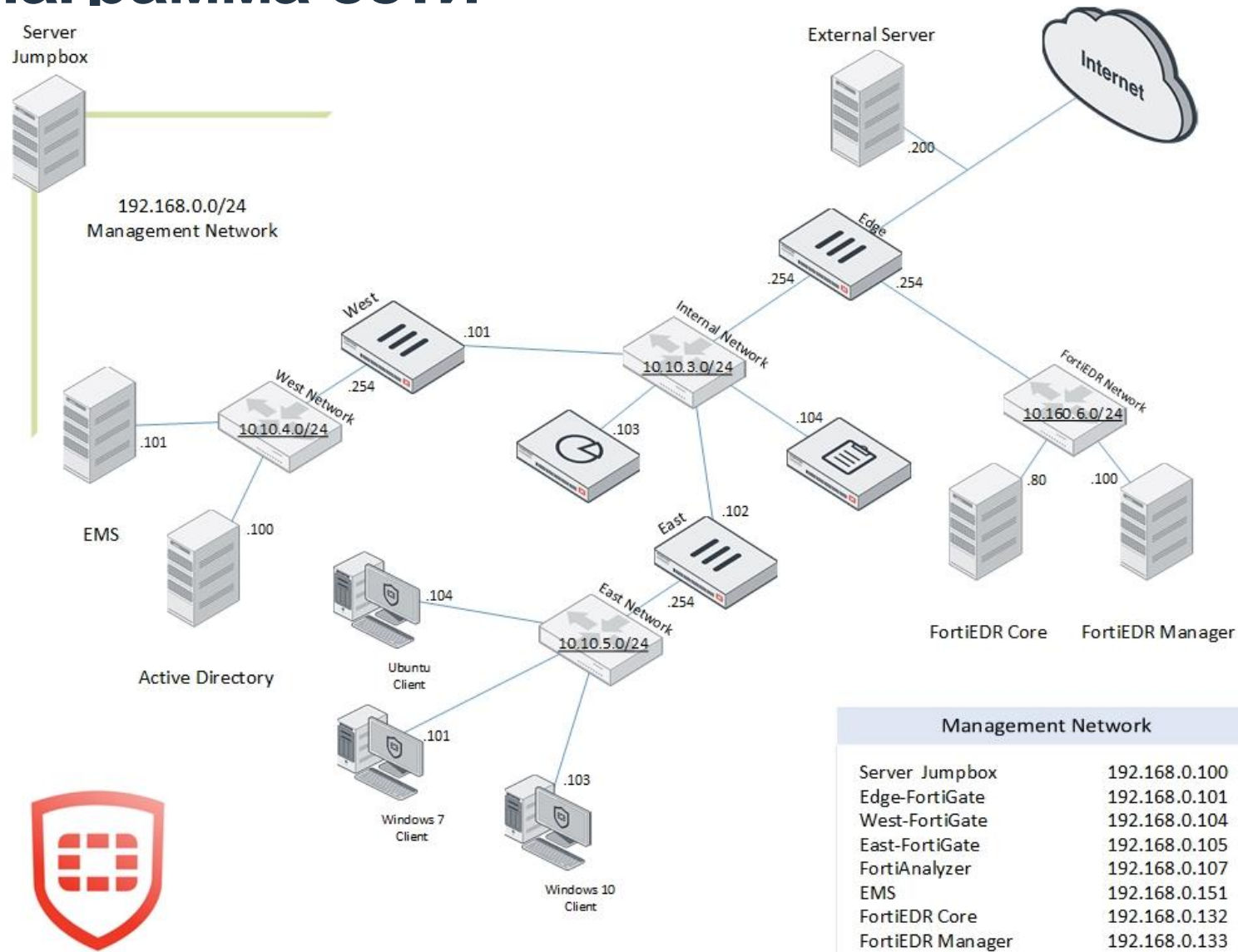
- Защита конечных точек от Ransomware
 - AV на основе ML + на основе поведения
 - Обнаружение / защита от безфайловых атак
 - Обнаружение приложений
 - Сканирование уязвимостей / Виртуальное исправление
 - Защита данных
- Обнаружение и защита от угроз
 - Уменьшение поверхности атаки – Virtual patching
 - 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



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

CloudShare Training Portal

Class Environments

POWERED BY cloudshare

Access your class environment

Enter the credentials supplied by your instructor to start working with your environment.

Login

* indicates required field

Email: *

Class Passphrase: *

Fortinet1!

Name : *

Chris

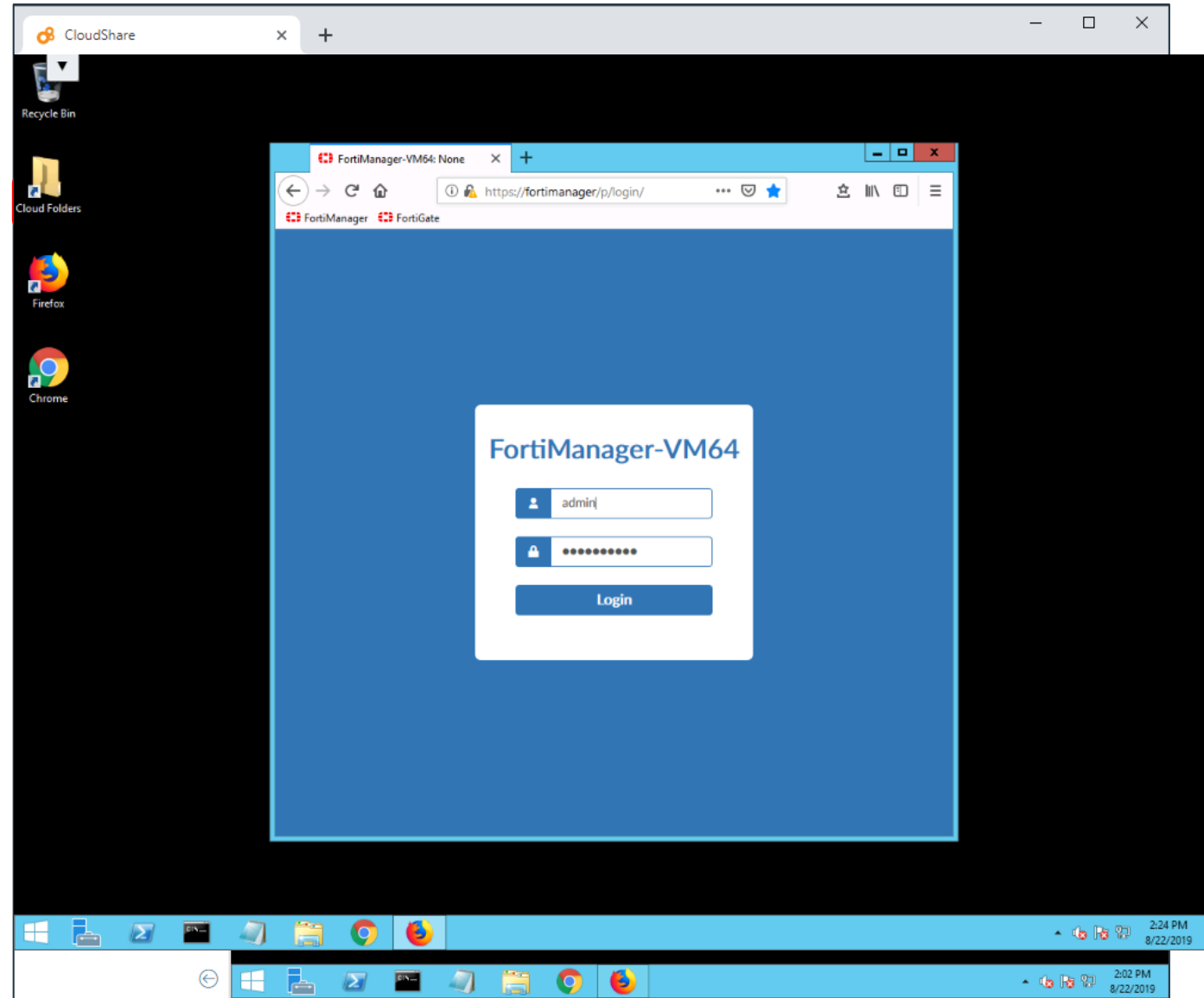
Pratico

Register and Login

[About CloudShare](#) [Terms of use](#) [Support](#) [Contact Us](#)

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

The screenshot displays the FortiFIED Interactive Lab interface. At the top, a green banner reads "Centralized Management with FortiManager" with a "Score: 0 (10)" indicator on the right. Below the banner, a section titled "Add Devices to FortiManager" contains a description of the lab scenario and a list of steps. Step 1 includes a "Jumpbox Server" link and login credentials (Username: admin, Password: Fortinet1!). Step 4 includes a "Discover" button and the same login credentials. A "Scale Text" slider is located in the top right corner. On the right side, a list of objectives is shown, including "1.0: FortiManager and FortiAnalyzer FastTrack" and "2.0: Centralized Management with FortiManager". At the bottom, a "Request Hint" button is on the left, and a "Continue" button is on the right. The status bar at the very bottom shows "Ready" and "Possible: 9 Points Values: 10/-1 Points".

0.0.0.0

Centralized Management with FortiManager

Score: 0 (10)

Add Devices to FortiManager

Description Hint 1

Add Devices to FortiManager

AcmeCorp has decided to utilize FortiManager to centrally provision and manage its devices. At its head office in Ottawa AcmeCorp has a core FortiGate, FortiGate-HQ. FortiGate-HQ is the root for the Security Fabric group, AcmeCorp. There are currently two FortiGate devices which are operationally but not yet fully configured at the Toronto and Vancouver branches.

Add Devices to FortiManager

You must add devices to FortiManager in order to centrally manage them. There are multiple ways to add devices. In this lab, you use the Add Device wizard.

1. To connect to FortiManager, use the **Jumpbox Server** and open a browser. Browse to <http://192.168.0.120> or use the browser shortcut. Log in using the following credentials:
Username: admin
Password: Fortinet1!
2. Click **Device Manager**.
3. Click **Devices and Groups** and click **Add Device**.
4. Select **Discover** and enter the following information:
IP address: 10.10.3.254
Username: admin
Password: Fortinet1!

Add Device

☐ a. It has been imported successfully but you have to configure its password in order for FortiManager to push updates

☒ d. It indicates that it is the root of the AcmeCorp Security Fabric group

☐ b. It has been imported but there is a duplicate device with the same name

☐ c. It requires user intervention

Request Hint

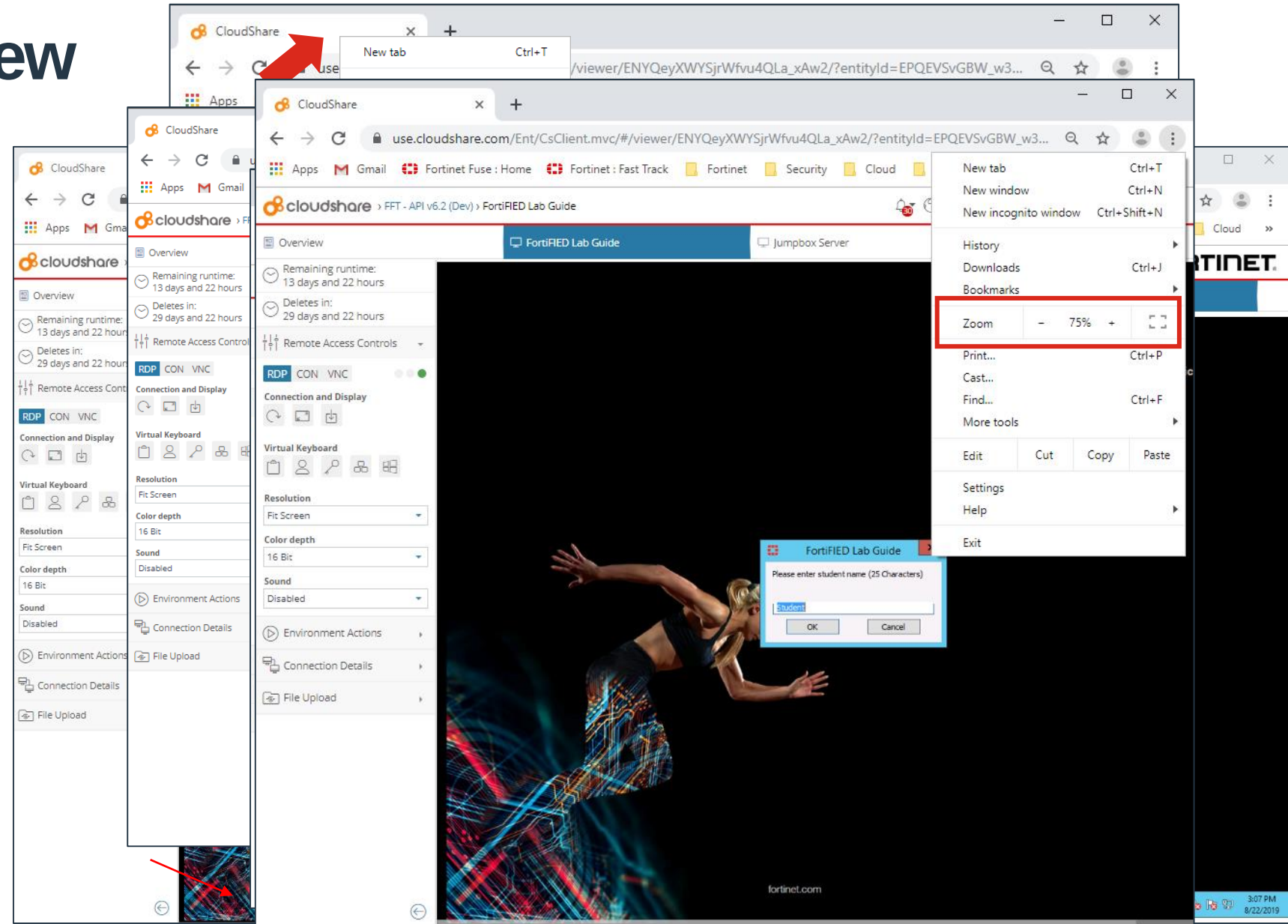
Continue

Ready

Possible: 9 Points Values: 10/-1 Points

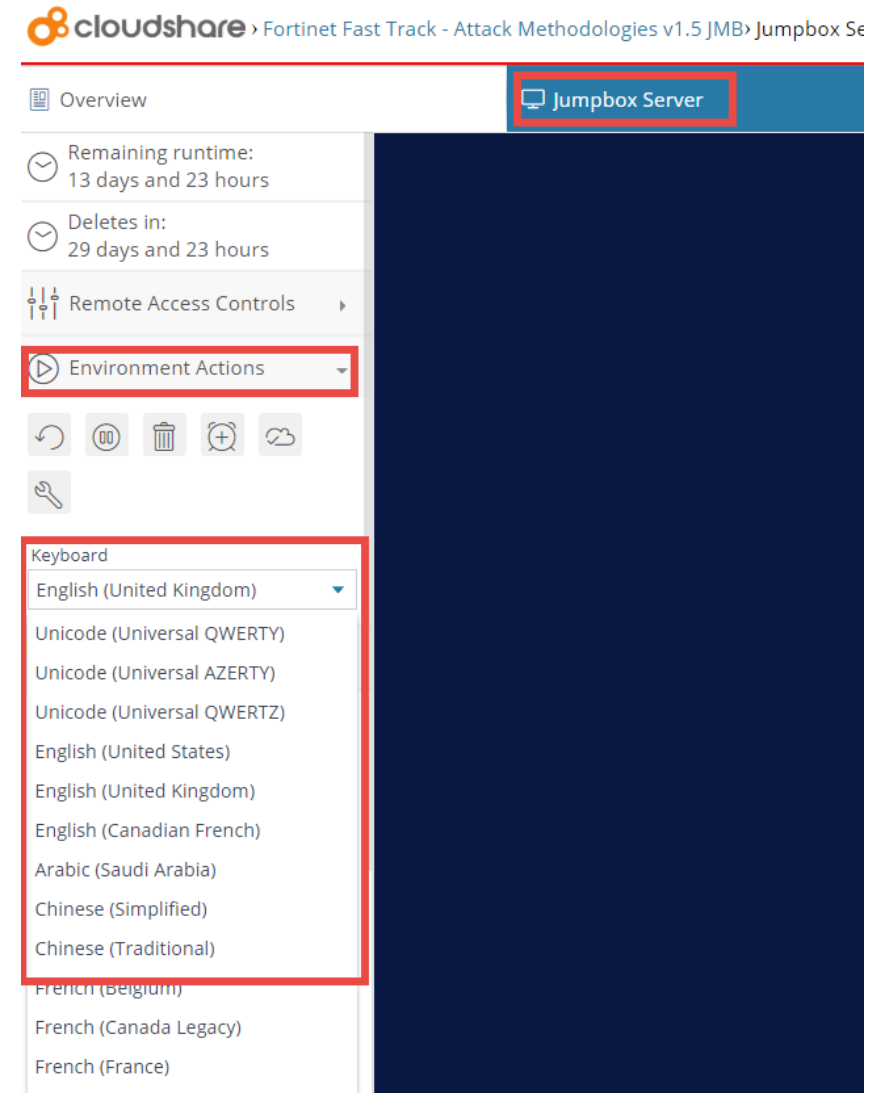
Adjusting the View

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



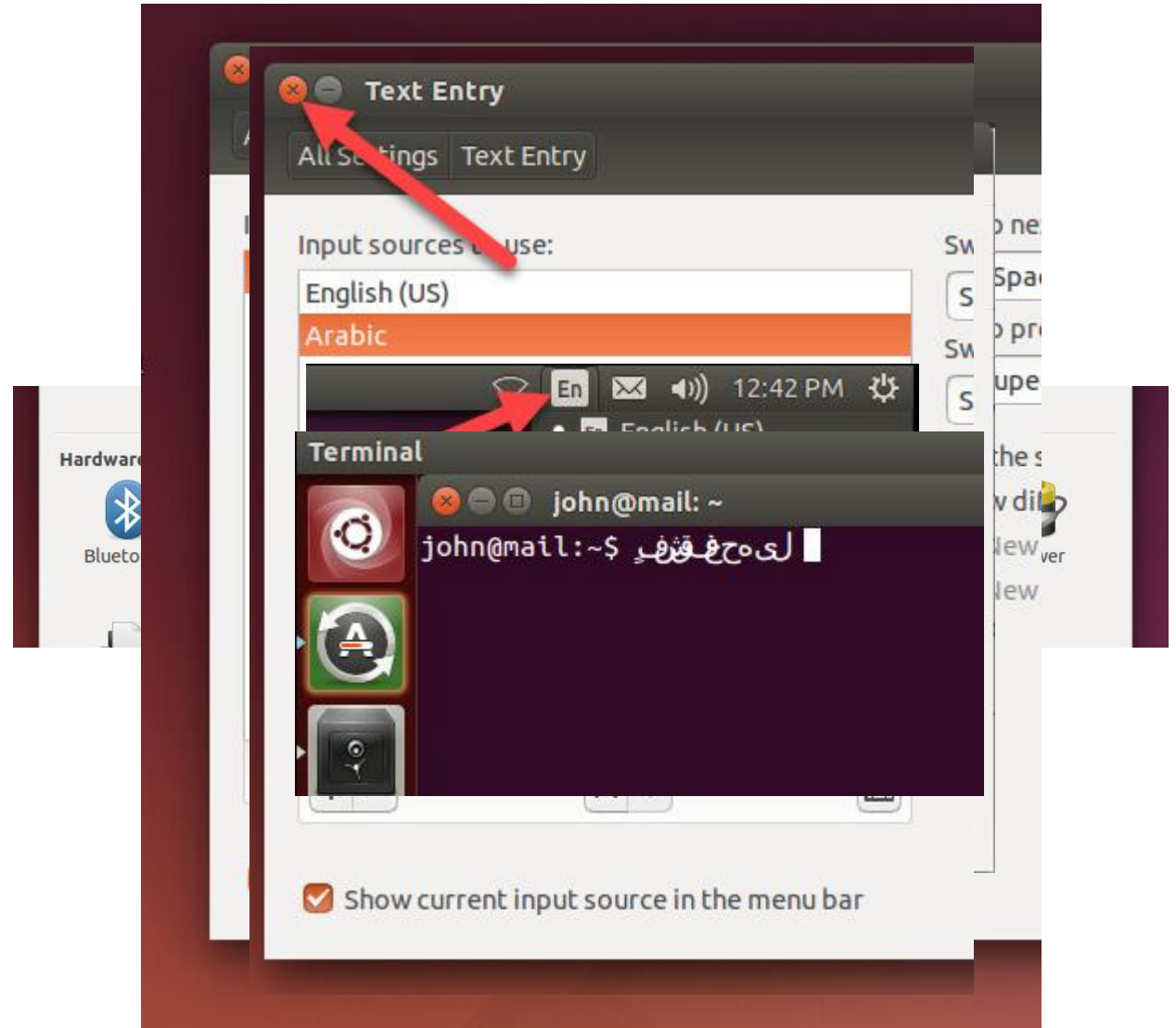
Keyboard Layouts

- 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)

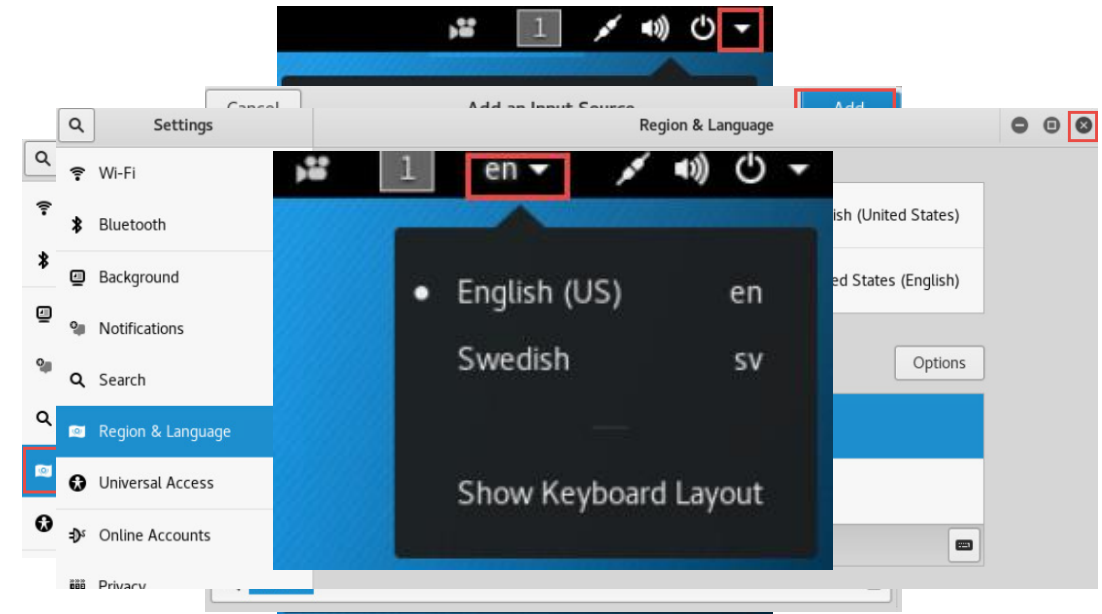
- Ubuntu 14.04 (NGFW)
 1. Must be done from inside the host
 2. Log in, click the gear icon on the top right and click **System Settings...**
 3. Click **Keyboard**
 4. Click **Text Entry**
 5. Click +
 6. Select a keyboard layout and click **Add**
 7. Close the window
 8. Click the **Keyboard Layout** icon on top right and click the new layout



Keyboard Layouts

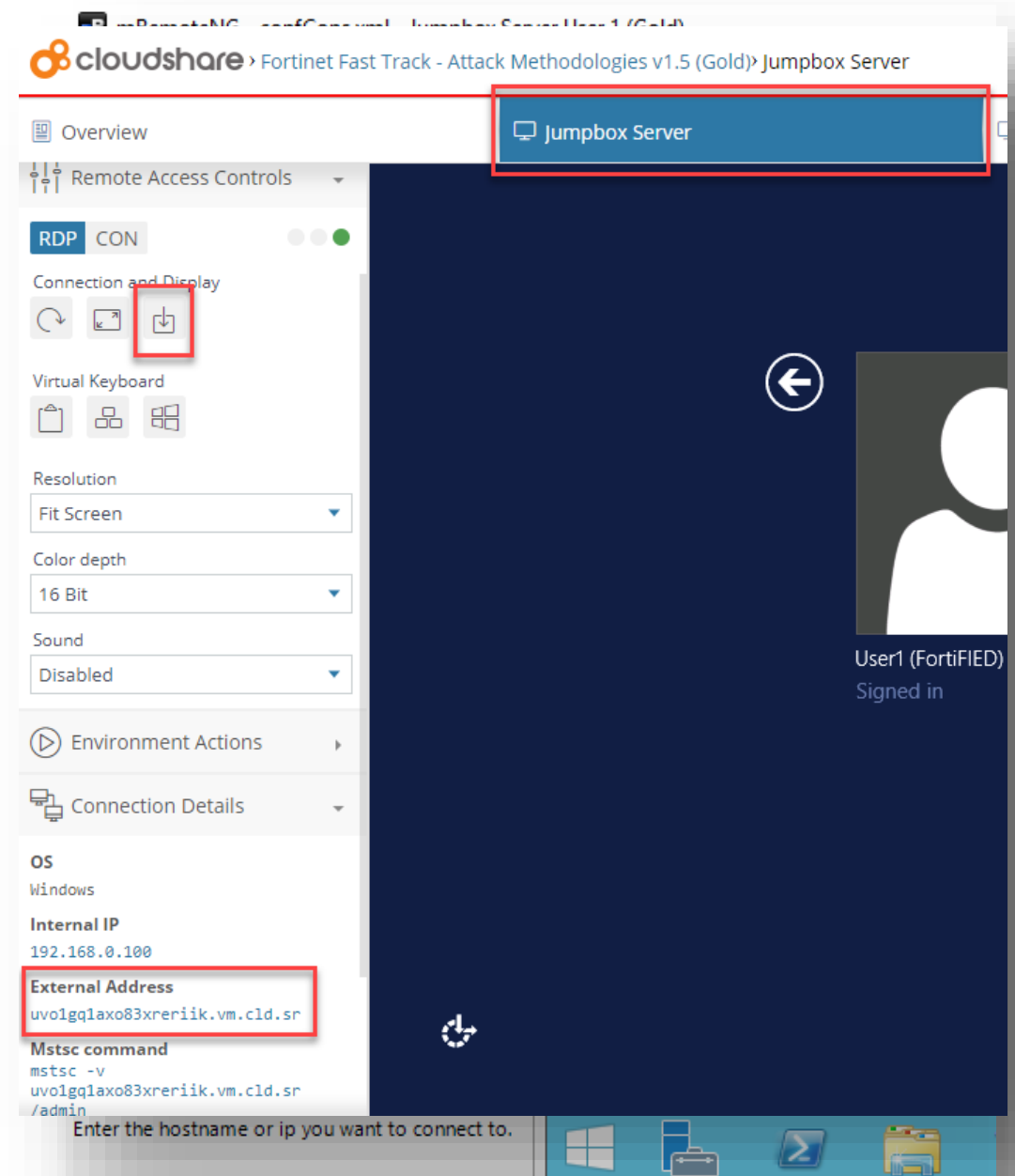
- Ubuntu 18.04 & Kali Host (Security Fabric & FortiWeb)

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

