КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

22 мая 2018 г.
г. Баку

#CODEIB

ОБНАРУЖЕНИЕ И ЗАЩИТА ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК

КОТ ИБ corporation

КОТ ИБ

Вадим Лещинский,
Softprom by ERC

ТЕЛЕФОН: +3 8(044) 230-34-74

EMAIL: fortinet@softprom.com

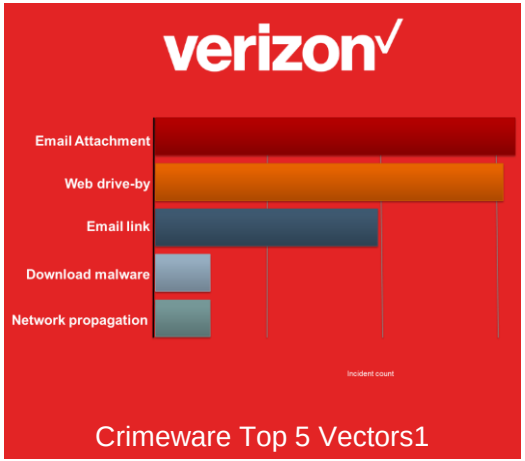
Agenda

- Текущая ситуация
  - ✓Уязвимости и приоритеты
  - ✓Почему Sandboxing
- Обзор FortiSandbox
  - ✓Что такое FortiSandbox
  - ✓Ключевые компоненты
- Что делает FortiSandbox отличительным
  - ✓Fortinet Advanced Threat Protection
  - ✓Fortinet Security Fabric

Текущая ситуация

FORTINET

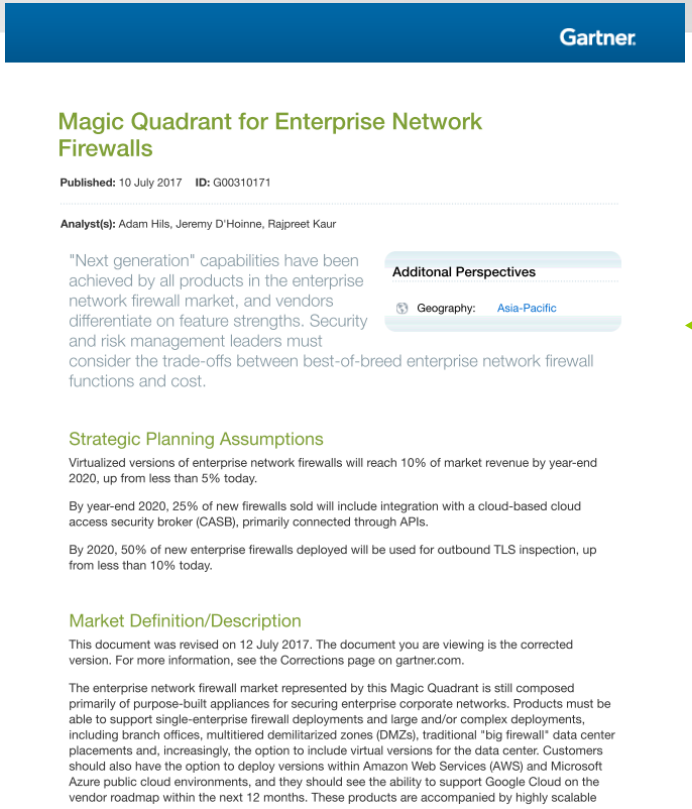
Традиционные методы защиты неэффективны



Notes/Sources:

1. Verizon 2016 Data Breach Report.
2. Verizon 2016 Data Breach Report.
3. Enterprise Strategy Group. Cybersecurity Skills Shortage: A State of Emergency. 2016.

Gartner рекомендует Sandbox



Gartner

Magic Quadrant for Enterprise Network Firewalls

Published: 10 July 2017 **ID:** G00310171

Analyst(s): Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur

"Next generation" capabilities have been achieved by all products in the enterprise network firewall market, and vendors differentiate on feature strengths. Security and risk management leaders must consider the trade-offs between best-of-breed enterprise network firewall functions and cost.

Additonal Perspectives

Geography: Asia-Pacific

Strategic Planning Assumptions

Virtualized versions of enterprise network firewalls will reach 10% of market revenue by year-end 2020, up from less than 5% today.

By year-end 2020, 25% of new firewalls sold will include integration with a cloud-based cloud access security broker (CASB), primarily connected through APIs.

By 2020, 50% of new enterprise firewalls deployed will be used for outbound TLS inspection, up from less than 10% today.

Market Definition/Description

This document was revised on 12 July 2017. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

The enterprise network firewall market represented by this Magic Quadrant is still composed primarily of purpose-built appliances for securing enterprise corporate networks. Products must be able to support single-enterprise firewall deployments and large and/or complex deployments, including branch offices, multitiered demilitarized zones (DMZs), traditional "big firewall" data center placements and, increasingly, the option to include virtual versions for the data center. Customers should also have the option to deploy versions within Amazon Web Services (AWS) and Microsoft Azure public cloud environments, and they should see the ability to support Google Cloud on the vendor roadmap within the next 12 months. These products are accompanied by highly scalable

"В стремлении защититься от продвинутой угрозы, клиенты все чаще обращаются к своим поставщикам брандмауэров для потребностей в Sandbox"

1. Gartner Magic Quadrant for Enterprise Network Firewalls, July, 2017

Как вирус остается незаметным? Уникальный код.

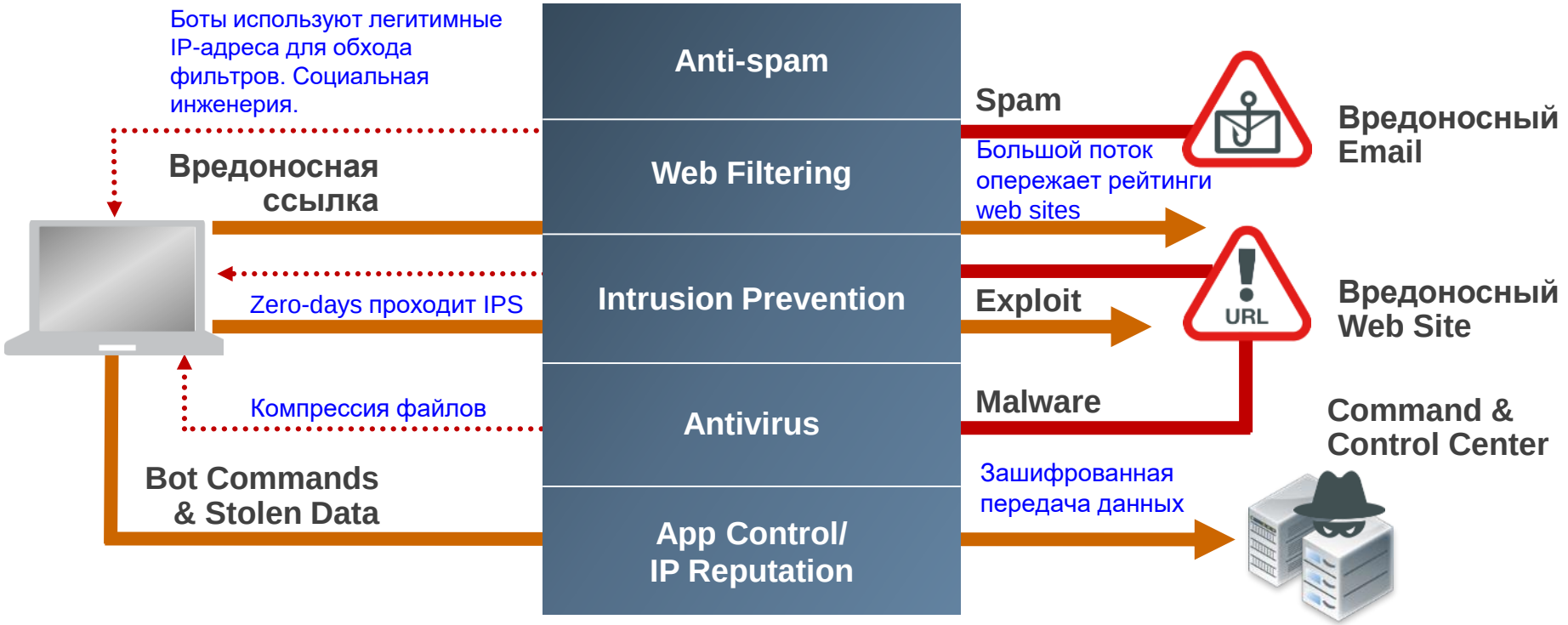
99.5%

Of Malware samples are Unique to an Organization

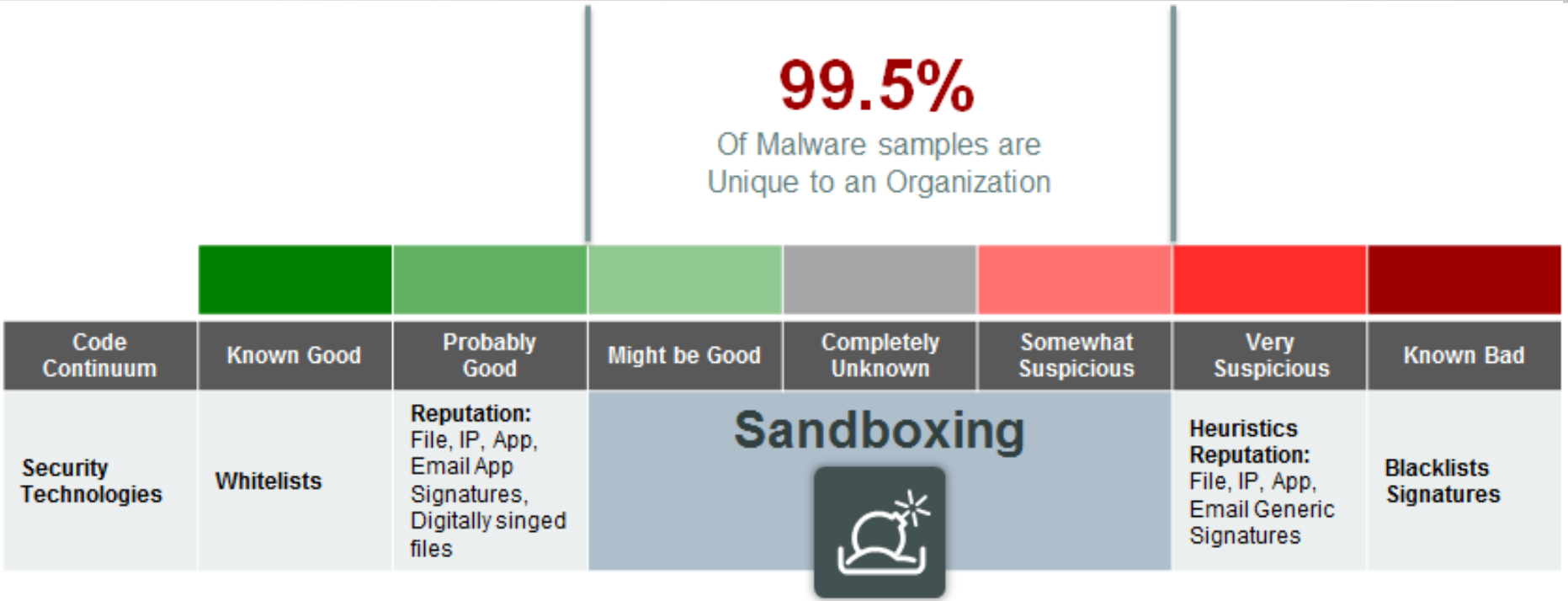
Code Continuum	Known Good	Probably Good	Might be Good	Completely Unknown	Somewhat Suspicious	Very Suspicious	Known Bad
Security Technologies	**Whitelists**	**Reputation:** File, IP, App, Email App Signatures, Digitally singed files				**Heuristics Reputation:** File, IP, App, Email Generic Signatures	**Blacklists Signatures**

Source:
Verizon 2016 Data Breach Investigations Report, April 2016

Kill Chain продвинутой атаки

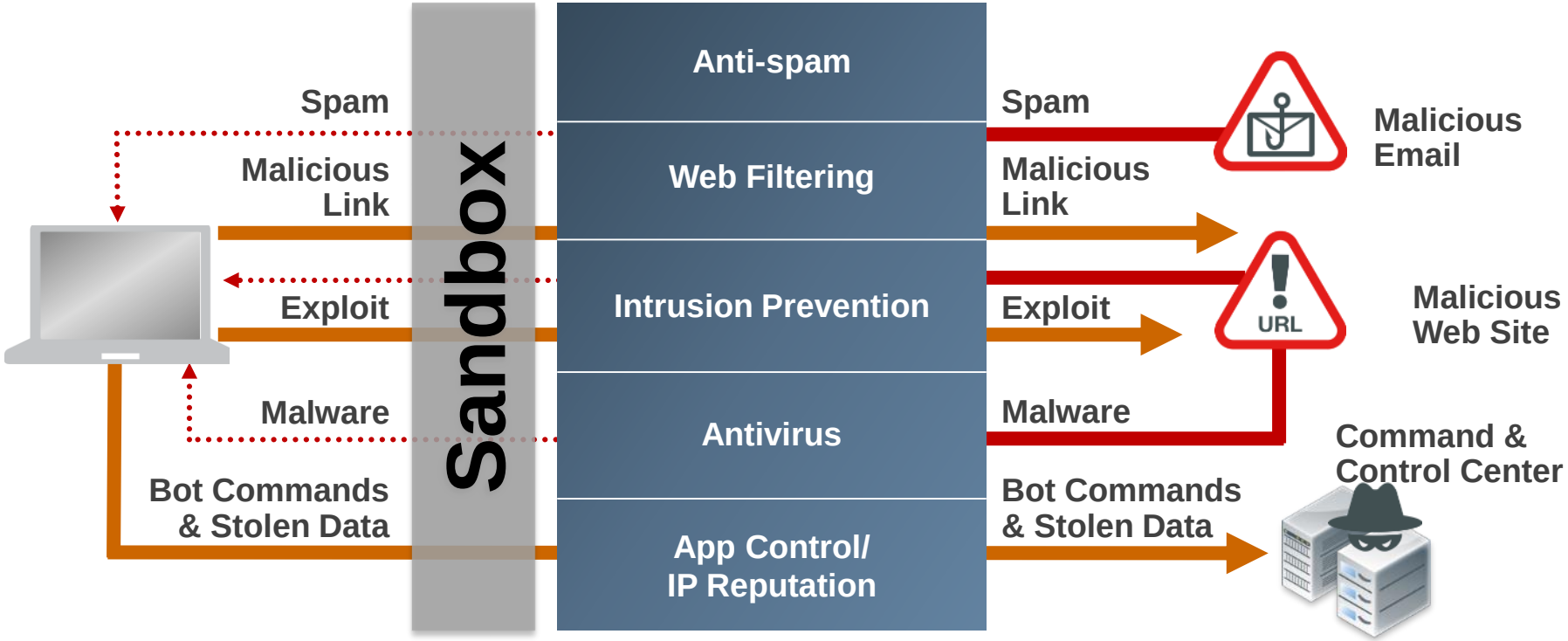


Sandboxing



Source:
Verizon 2016 Data Breach Investigations Report, April 2016

Sandboxing

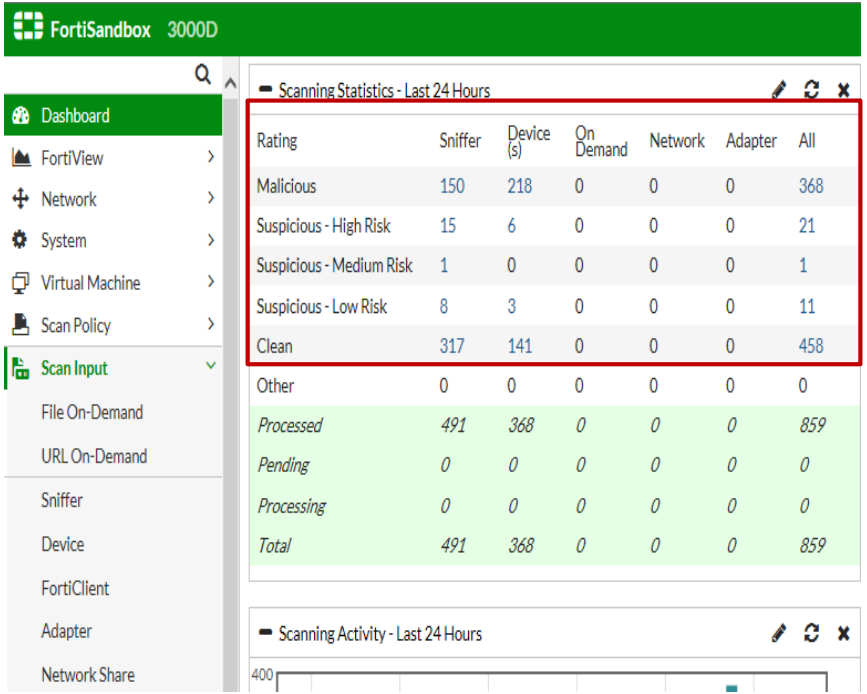

Spam
Malicious Link
Exploit
Malware
Bot Commands & Stolen Data
Sandbox
Anti-spam
Web Filtering
Intrusion Prevention
Antivirus
App Control/ IP Reputation
Spam
Malicious Link
Exploit
Malware
Bot Commands & Stolen Data
Malicious Email
URL
Malicious Web Site
Command & Control Center

FortiSandbox

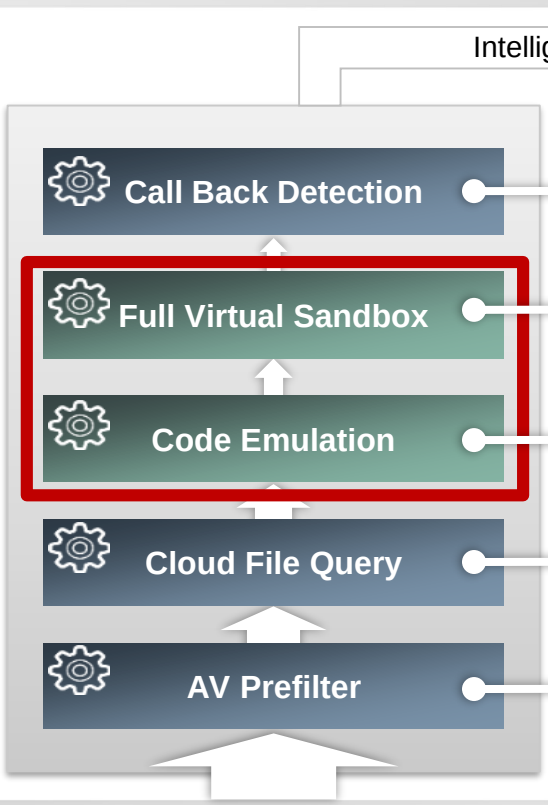
FORTINET

Обзор FortiSandbox

«Песочница» анализирует динамическую активность, а не статические атрибуты, для выявления ранее неизвестных вредоносных программ



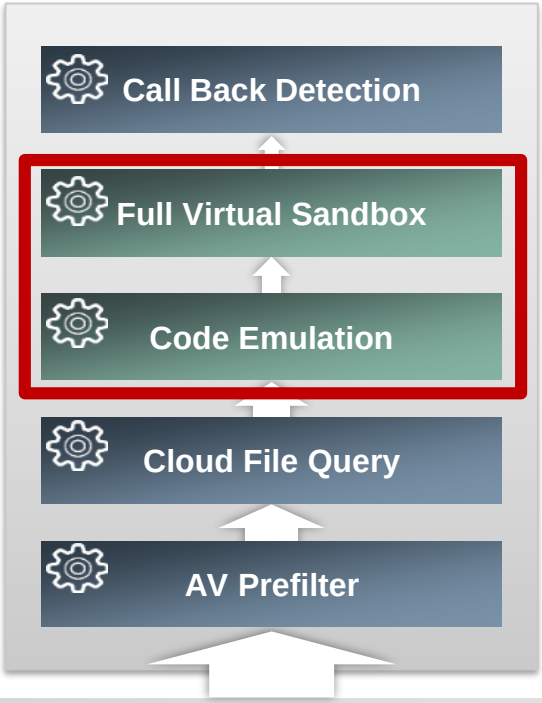
Ключевые компоненты FortiSandbox



- Распространение обновлений в реальном времени
- Дополняет глобальную систему

- Определяет конечную цель и call back
- Изучает в реальном времени активность и полный жизненный цикл файла для проявления угрозы
- Быстро имитирует предполагаемую деятельность
- Распространенные ОС
- Проверка репутации файла в глобальной системе
- Применяет сигнатурный антивирусный анализ

Что именно FortiSandbox показывает Вам



High Risk Unknown

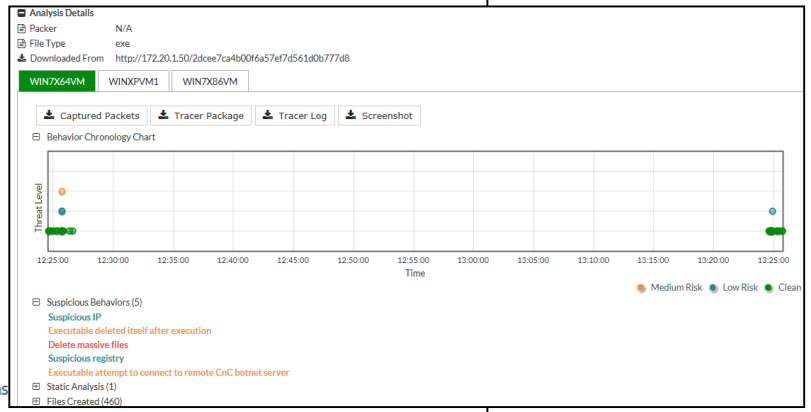
Mark as clean (false positive)

Received	May 20 2016 13:28:32
Started	May 20 2016 13:28:35
Status	Done
Rated By	VM Engine
Submit Type	FortiGate
Source IP	172.20.2.50
Destination IP	172.20.1.50
Digital Signature	No
Scan Bypass Configuration	N/A

More Details

Behavior Summary

This file visit webpage with certain URL
This file connect to certain IP Addresses
This file has network traffic
This file dropped files
This file modified files
This file deleted files
This file tried to delete massive files
This file applied autostart registry modifications
This file spawned process(es)
This file query DNS with certain domain names



Продуктовая линейка FortiSandbox

Hardware Appliances

- 4 models
- 480 – 3,600 real-world throughput (objects/hr)

vmware KVM

Virtual Appliances

- CPU-based
- 4 – 792 VMs*

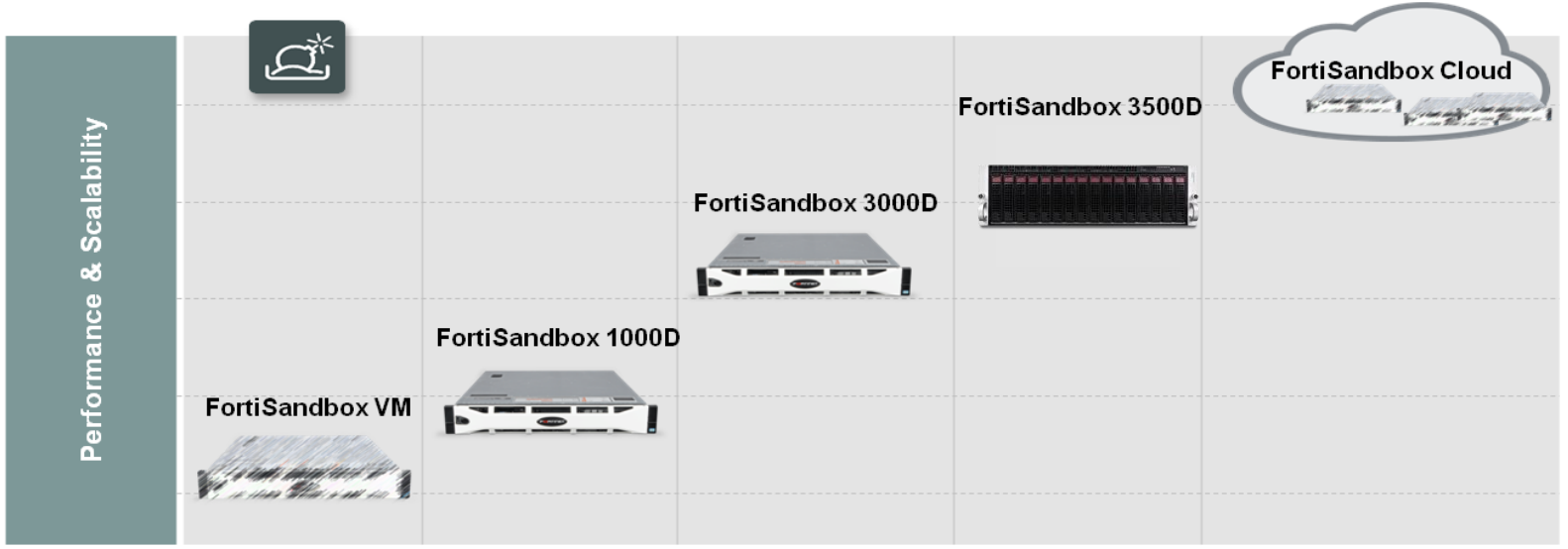
FORTINET

Cloud

- Fortinet managed
- Supports FortiGate, FortiMail, FortiWeb
- Available as a add-on service or in a bundle

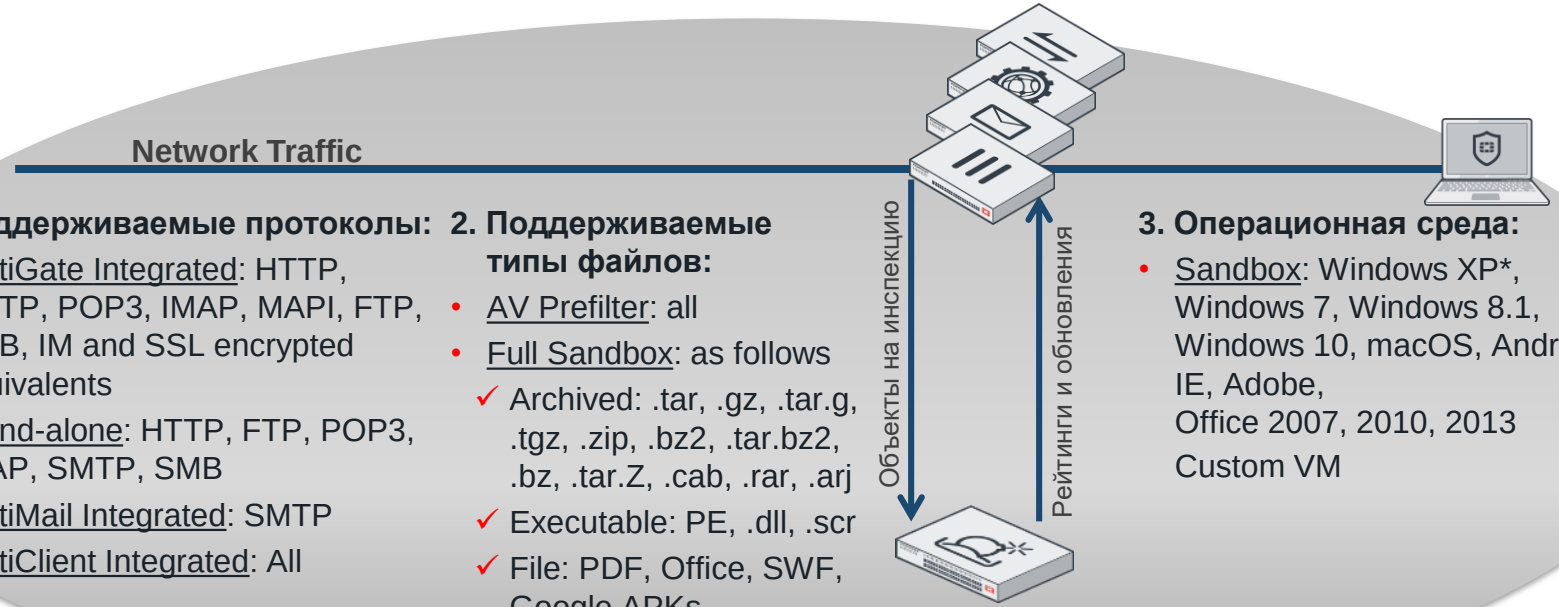
*8 VMs/node and up to 99 nodes/cluster

Форм-фактор FortiSandbox



VMs	2+	8	28	64	As needed
Sandboxing (Files/hr)	Depends on hardware	160	560	1280*	As needed
AV Scanning (files/hr)	Depends on hardware	6,000	15,000	48,000*	As needed

Подробнее о FortiSandbox



1. Поддерживаемые протоколы:

- FortiGate Integrated: HTTP, SMTP, POP3, IMAP, MAPI, FTP, SMB, IM and SSL encrypted equivalents
- Stand-alone: HTTP, FTP, POP3, IMAP, SMTP, SMB
- FortiMail Integrated: SMTP
- FortiClient Integrated: All

2. Поддерживаемые типы файлов:

- AV Prefilter: all
- Full Sandbox: as follows
  - ✓ Archived: .tar, .gz, .tar.g, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
  - ✓ Executable: PE, .dll, .scr
  - ✓ File: PDF, Office, SWF, Google APKs
  - ✓ URLs

3. Операционная среда:

- Sandbox: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, Android
  IE, Adobe,
  Office 2007, 2010, 2013
  Custom VM

Гибкие варианты развертывания FortiSandbox

Гибкие варианты развертывания

- Наиболее подходящая реализация зависит от требований и инфраструктуры
- Позволяет защищать инвестиций, поддерживая разные режимы развертывания по мере изменения требований
- Быстрая инспекция, распознавание и блокировка вирусов при интеграции с продуктами Fortinet

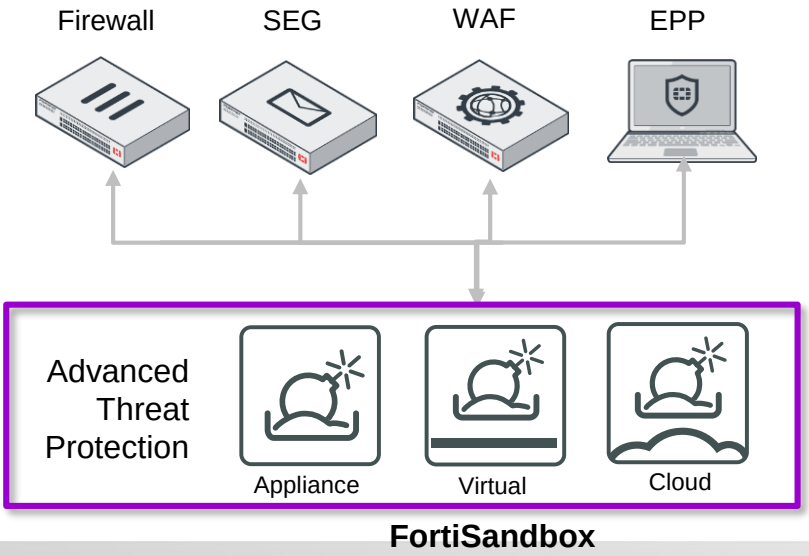
Fortinet Advanced Threat Protection Solution

FORTINET

Интегрированная защита от продвинутых угроз для Сети, Почты, Веб и Конечных точек

FortiSandbox

Advanced Threat Detection

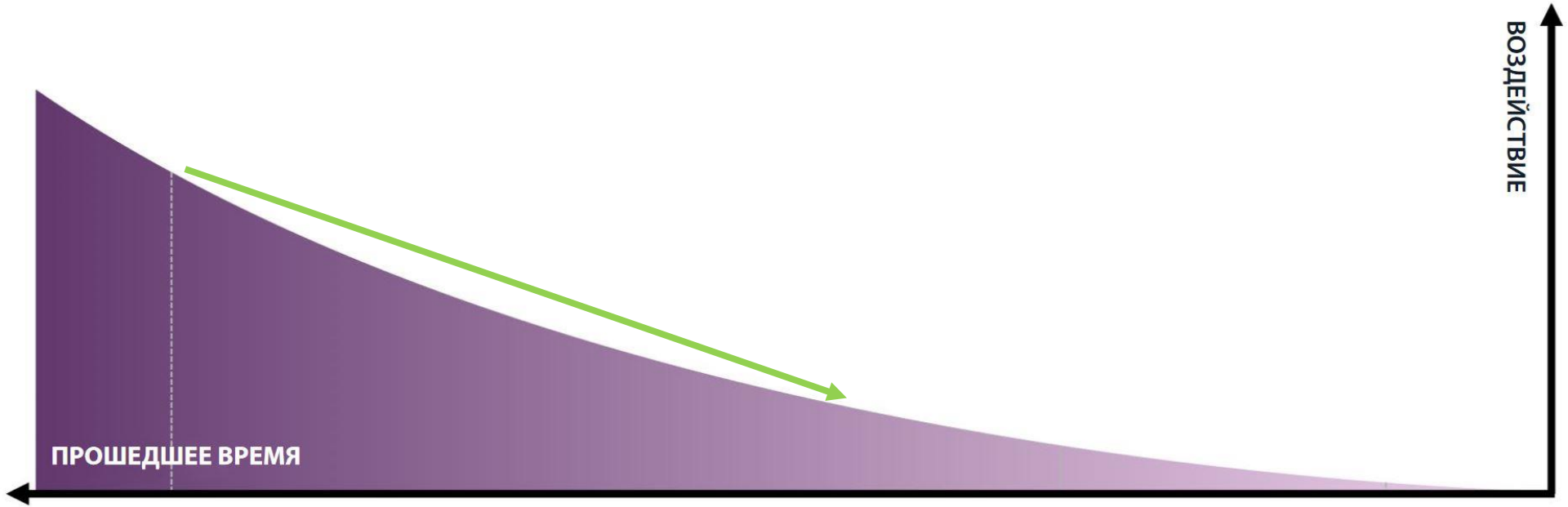


FortiSandbox

- **Интеграция** с FortiGate, FortiMail, FortiWeb, FortiClient и не-Fortinet компонентами безопасности для защиты от всех векторов атаки
- **Автоматизация** защиты от продвинутых атак
- **Лучшие** продукты безопасности согласно независимых сторонних тестов

Идентификация и реагирование на вирусы-вымогатели, фишинг и целенаправленные атаки, которые могут привести к нанесению финансового и репутационного вреда организации, простоям, нормативным санкциям и т. д.

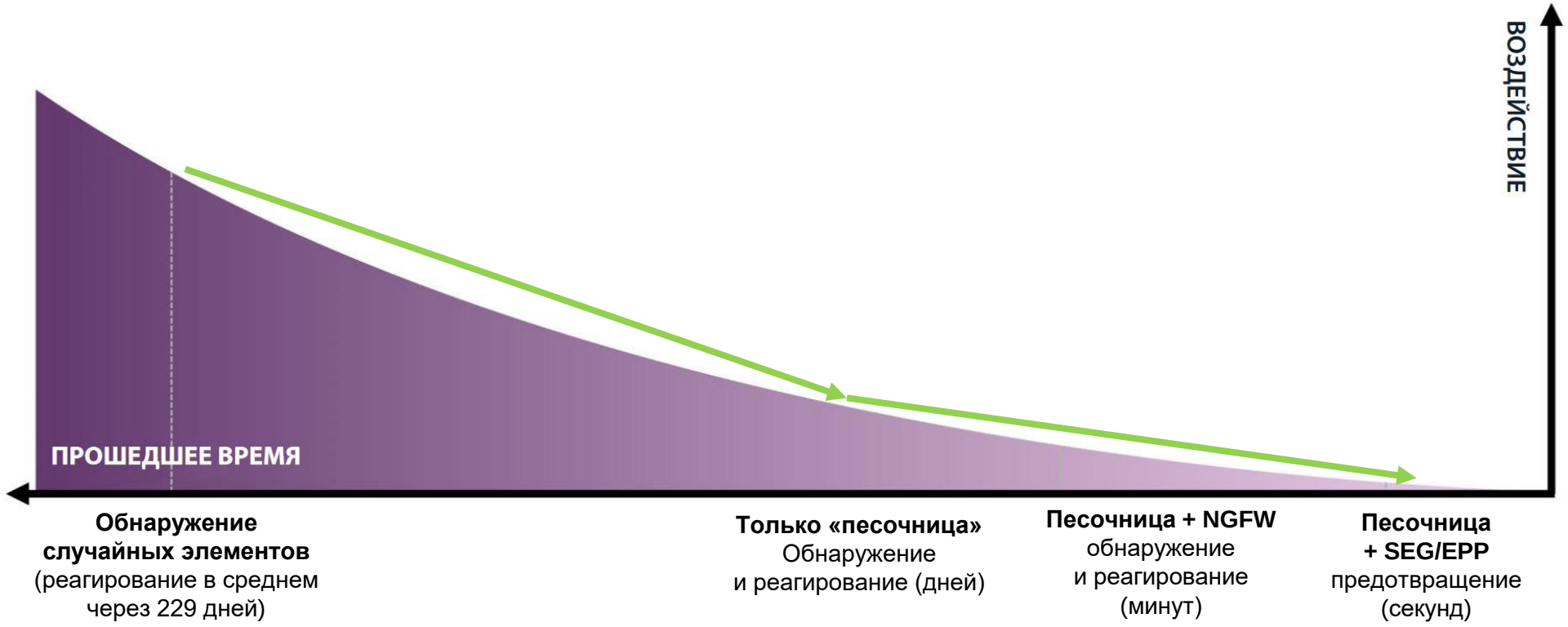
Польза FortiSandbox



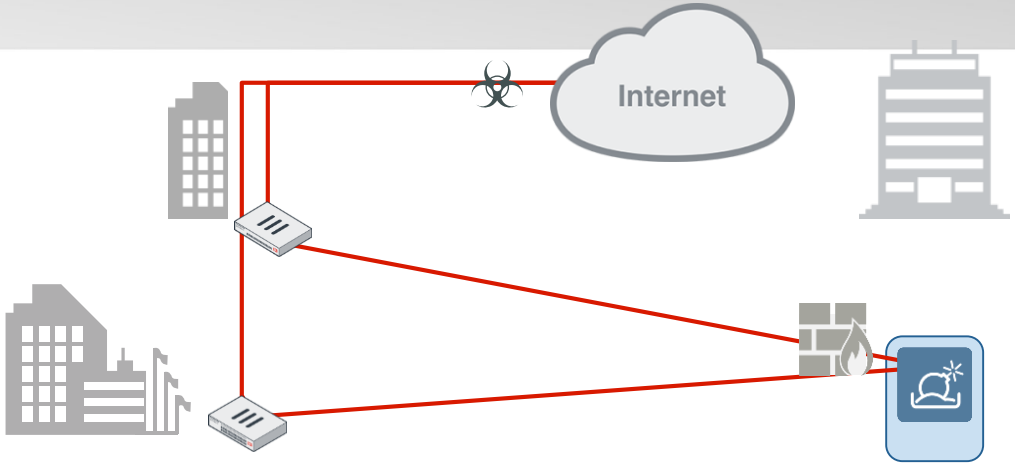
Обнаружение случайных элементов
(реагирование в среднем через 229 дней)

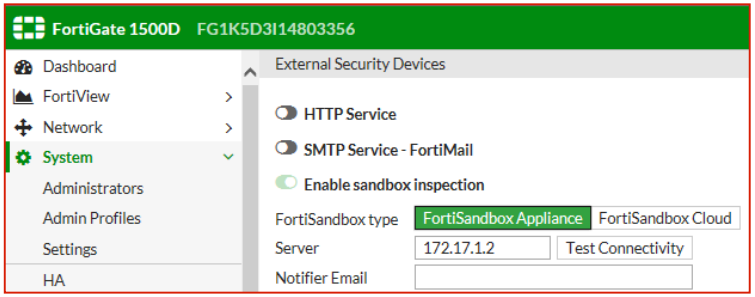
Только «песочница»
Обнаружение
и реагирование (дней)

Польза FortiSandbox



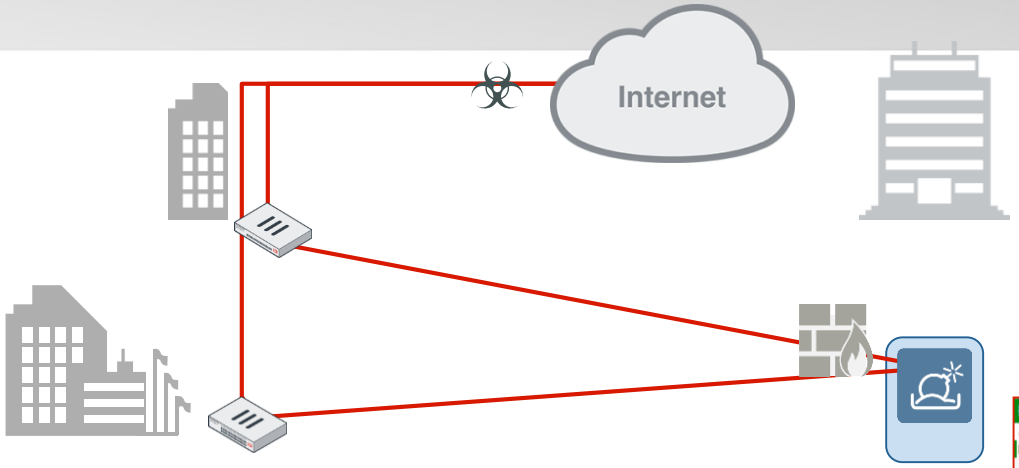
#1 Использование ATP: NGFW + Sandbox

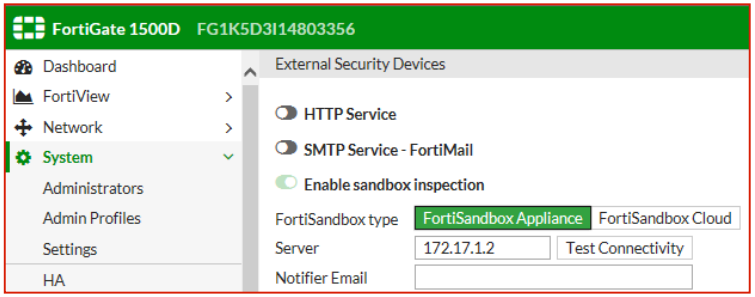


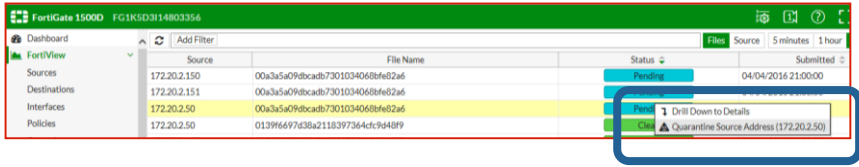


- FortiGate blocks as much as it can, routes remaining objects to FortiSandbox
- FortiSandbox returns ratings and updates
- FortiGate admin quarantines device, FortiGate starts blocking new threats

#1 Использование ATP: NGFW + Sandbox

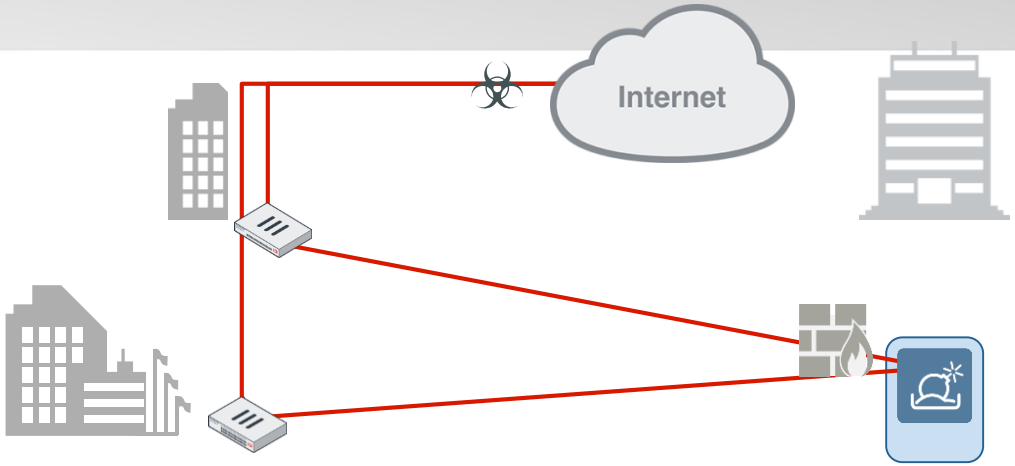




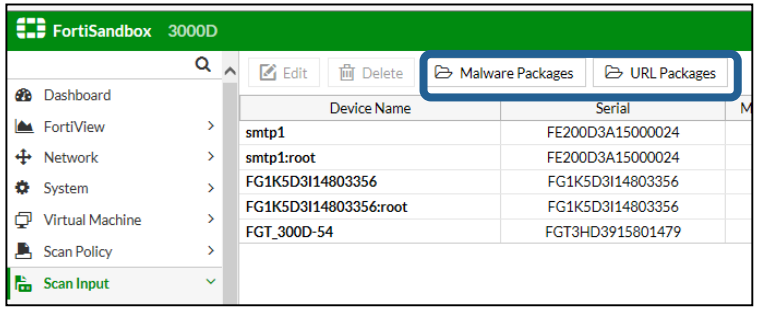


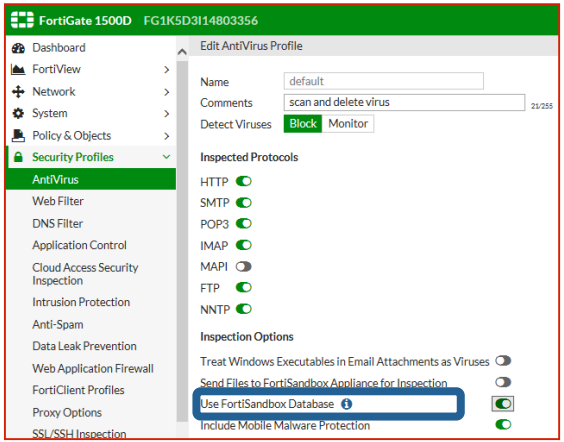
- FortiGate blocks as much as it can, routes remaining objects to FortiSandbox
- FortiSandbox returns ratings and updates
- FortiGate admin quarantines device, FortiGate starts blocking new threats

#1 Использование ATP: NGFW + Sandbox

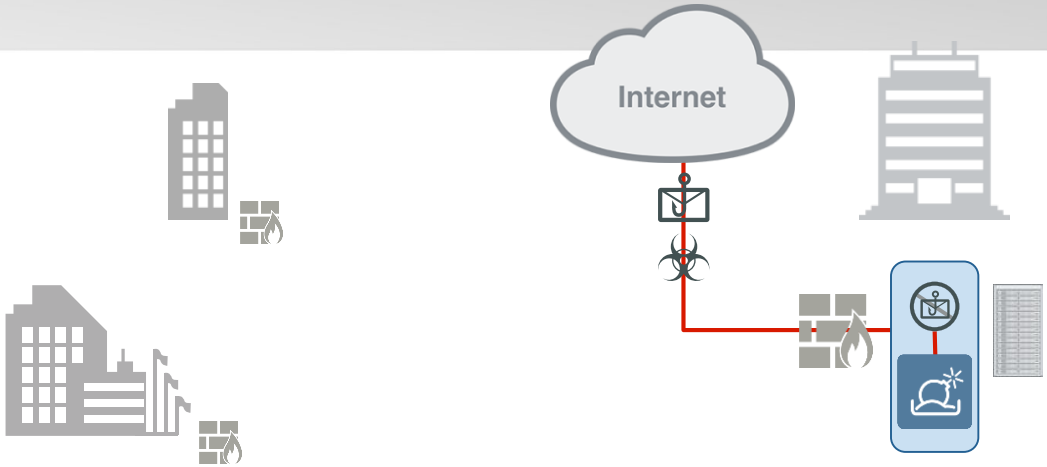


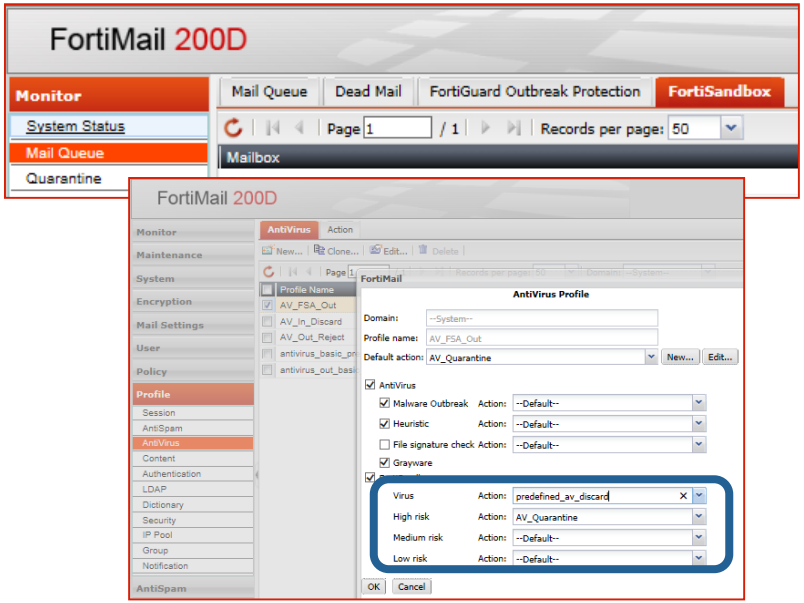
- FortiGate blocks as much as it can, routes remaining objects to FortiSandbox
- FortiSandbox returns ratings and updates
- FortiGate admin quarantines device, FortiGate starts blocking new threats





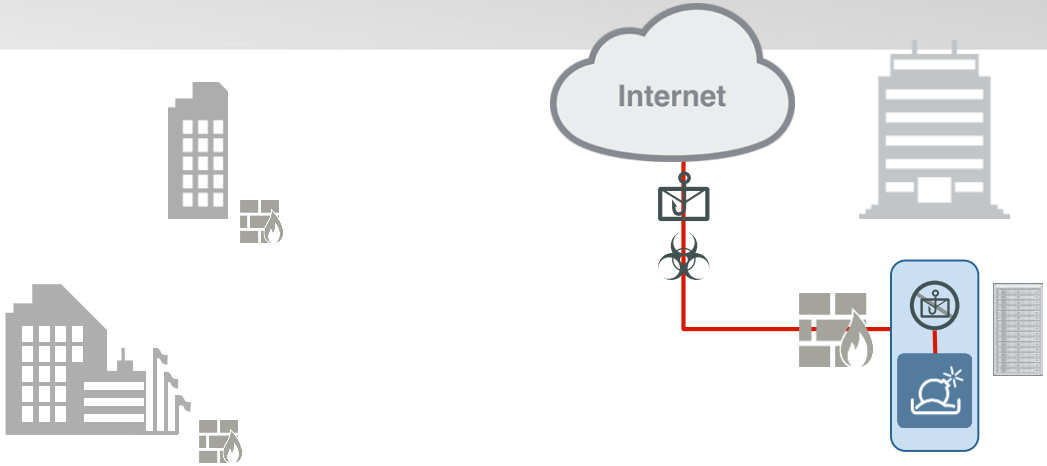
#2 Использование : SEG + Sandbox Hold and Analyze

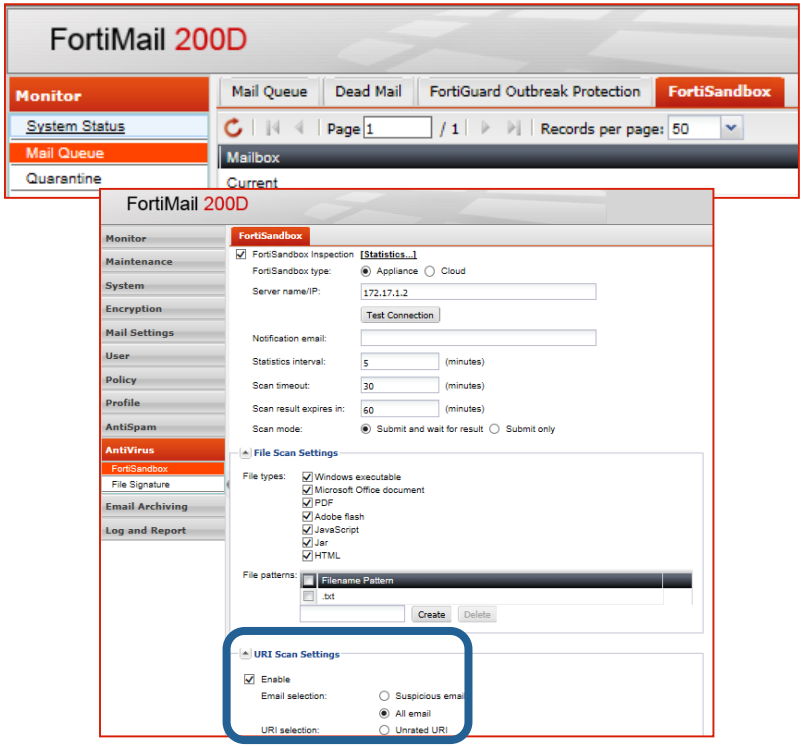




- FortiMail blocks as much as possible, queues messages for additional FortiSandbox analysis
- Quarantine or Deliver based on result
- Send URLs as well as attachments

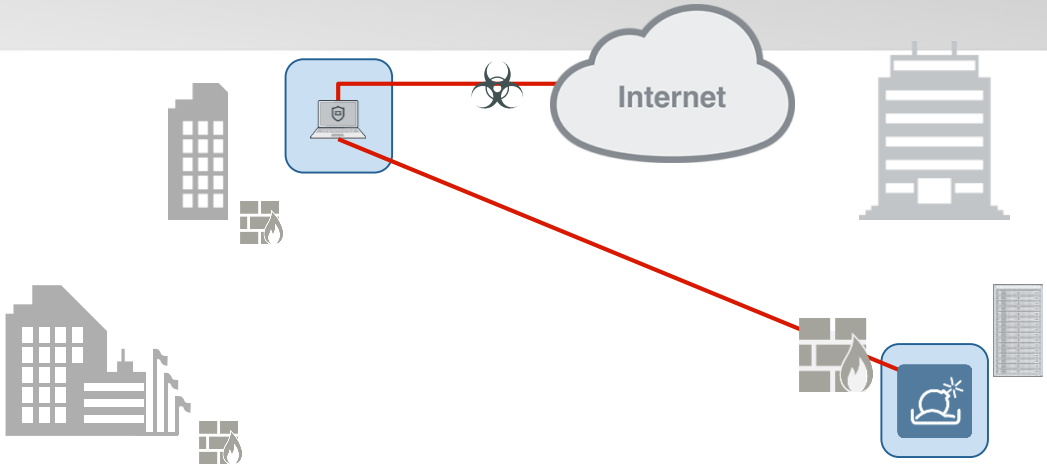
#2 Использование: SEG + Sandbox

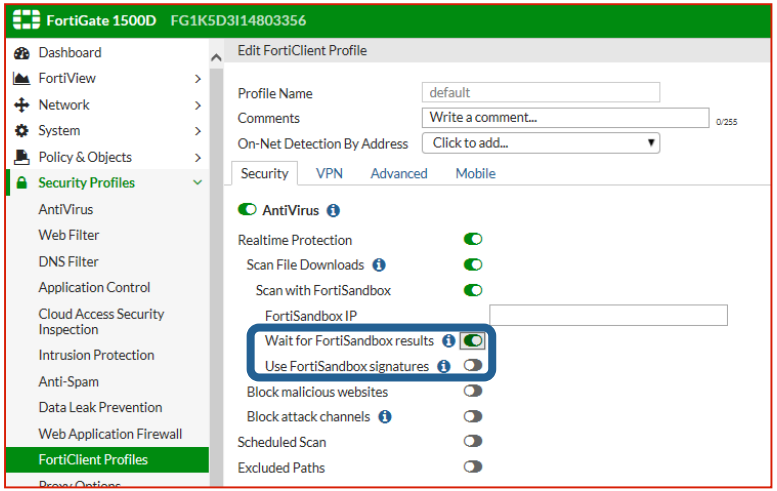




- FortiMail blocks as much as possible, queues messages for additional FortiSandbox analysis
- Quarantine or Deliver based on result
- Send URLs as well as attachments

#3 Использование : Client + Sandbox





- FortiClient sends files to FortiSandbox
- Hold for Rating or Install and Quarantine
- Receive FortiSandbox Updates to Block

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

22 мая 2018 г.
г. Баку

#CODEIB

КОТ ИБ
corporation

КОТ ИБ

Вадим Лещинский,
Softprom by ERC

ТЕЛЕФОН: +3 8(044) 230-34-74

EMAIL: fortinet@softprom.com