



AVSOFT OCTOPUS

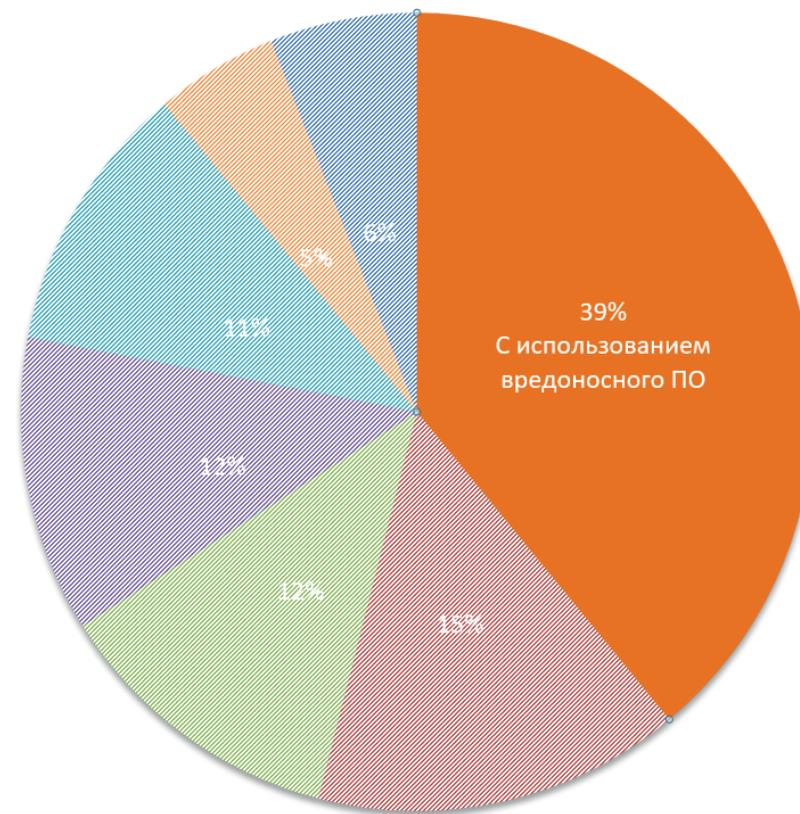
Система комплексной
антивирусной проверки ПО

УГРОЗЫ

Целенаправленные кибератаки и новые вирусы быстро совершенствуются уже более 12 лет. За последнее время самыми масштабными из них были **WannaCry, Petya, Bad Rabbit**, которые дестабилизировали корпоративные информационные системы с целью похищения конфиденциальных сведений, шантажа, остановки рабочих процессов, выведения из строя критических объектов, нанесения финансового и репутационного ущерба.

В 2017 году основная масса атак была проведена с использованием вредоносного ПО, ущерб от которого составил более 1,5 млрд долл. США*

Методы атак



* По данным компании Positive Technologies

ПРОБЛЕМА



Использование одного антивируса в компании повышает риск проникновения новых вирусов в информационную инфраструктуру.

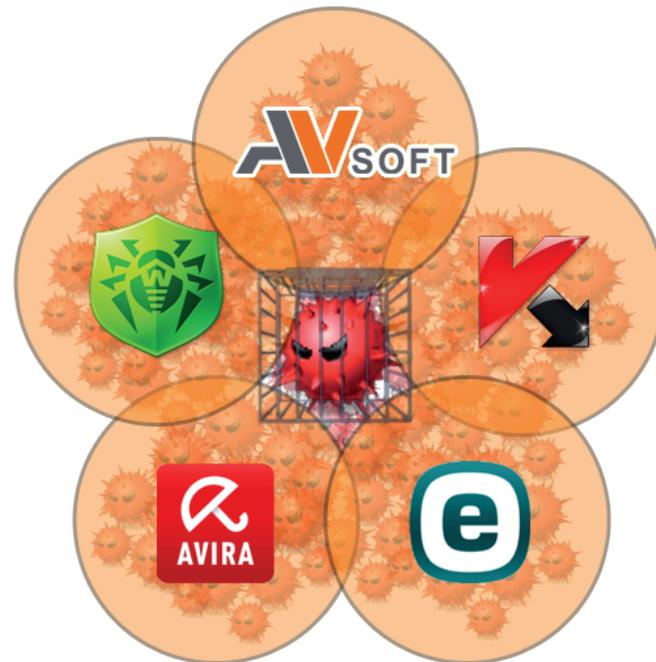
Один вендор антивирусного продукта не способен обеспечить своевременное отражение всех новых вирусов в своих базах и отсутствие ложных срабатываний.



РЕШЕНИЕ ПРОБЛЕМЫ

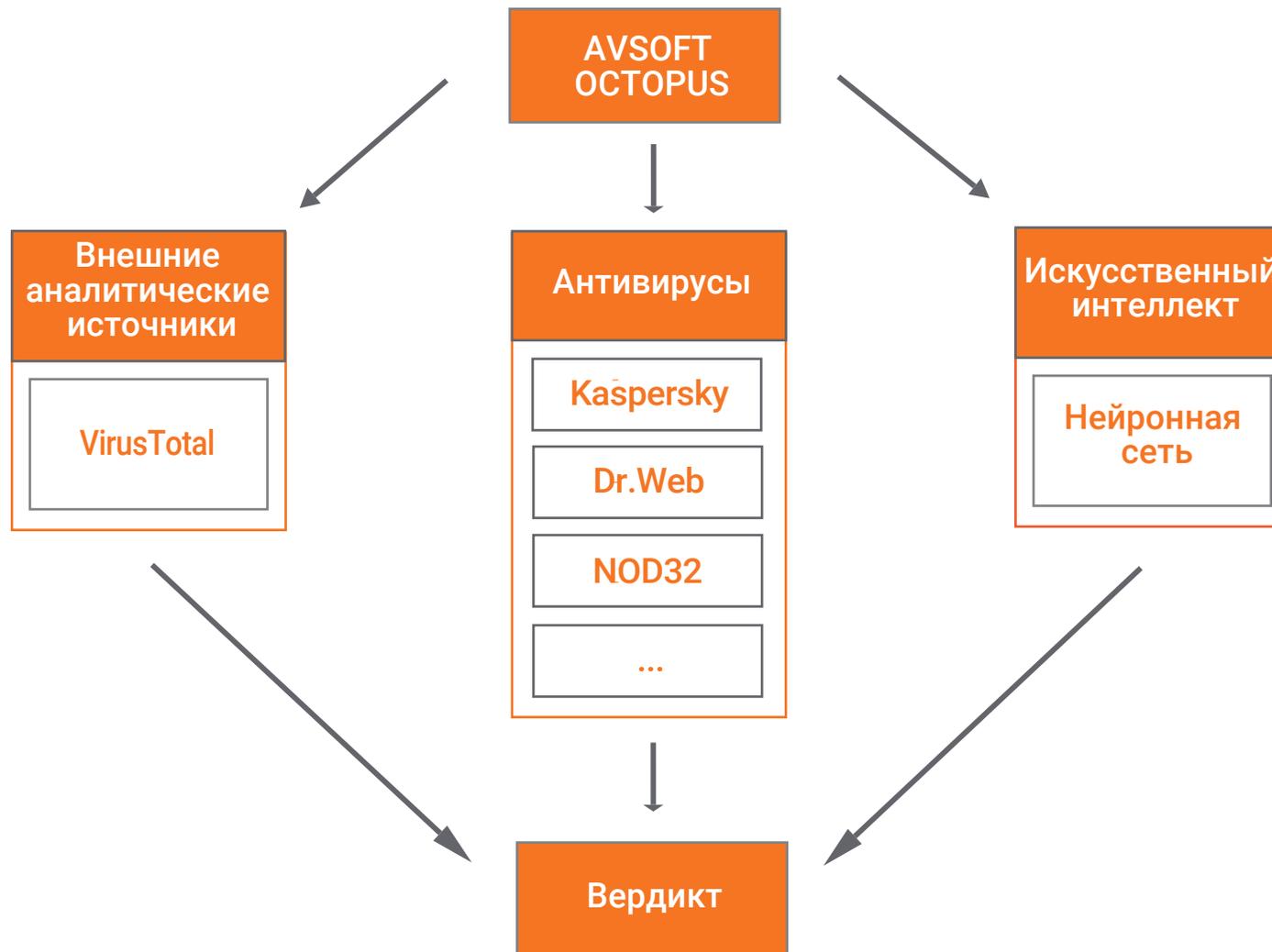
Для снижения риска проникновения новых вирусов в инфраструктуру компании необходимо выполнять параллельную проверку всех поступающих файлов различными антивирусными средствами и аналитическими инструментами:

- внешние аналитические ресурсы (VirusTotal)
- искусственный интеллект (нейронная сеть)



AVSOFT OCTOPUS

Система «AVSOFT OCTOPUS» усиливает защиту информационной инфраструктуры от вирусов нулевого дня. Каждый файл проходит проверку в модуле антивирусной проверки (более 10 антивирусов), в модуле внешних аналитических источников и в модуле нейронной сети.



ОСНОВНЫЕ ВОЗМОЖНОСТИ AVSOFT OCTOPUS



Анализ различных типов файлов

Офисные документы, исполняемые файлы, приложения и т.д.



Анализ почтового трафика

Выявление вредоносных вложений в письмах до получения адресатом



Ретроспективный анализ

Пере проверка при обновлении баз данных антивирусов



Интеграция с другими системами для отправки файлов

Присутствует API-интерфейс, который позволяет отправлять файлы на проверку из других систем

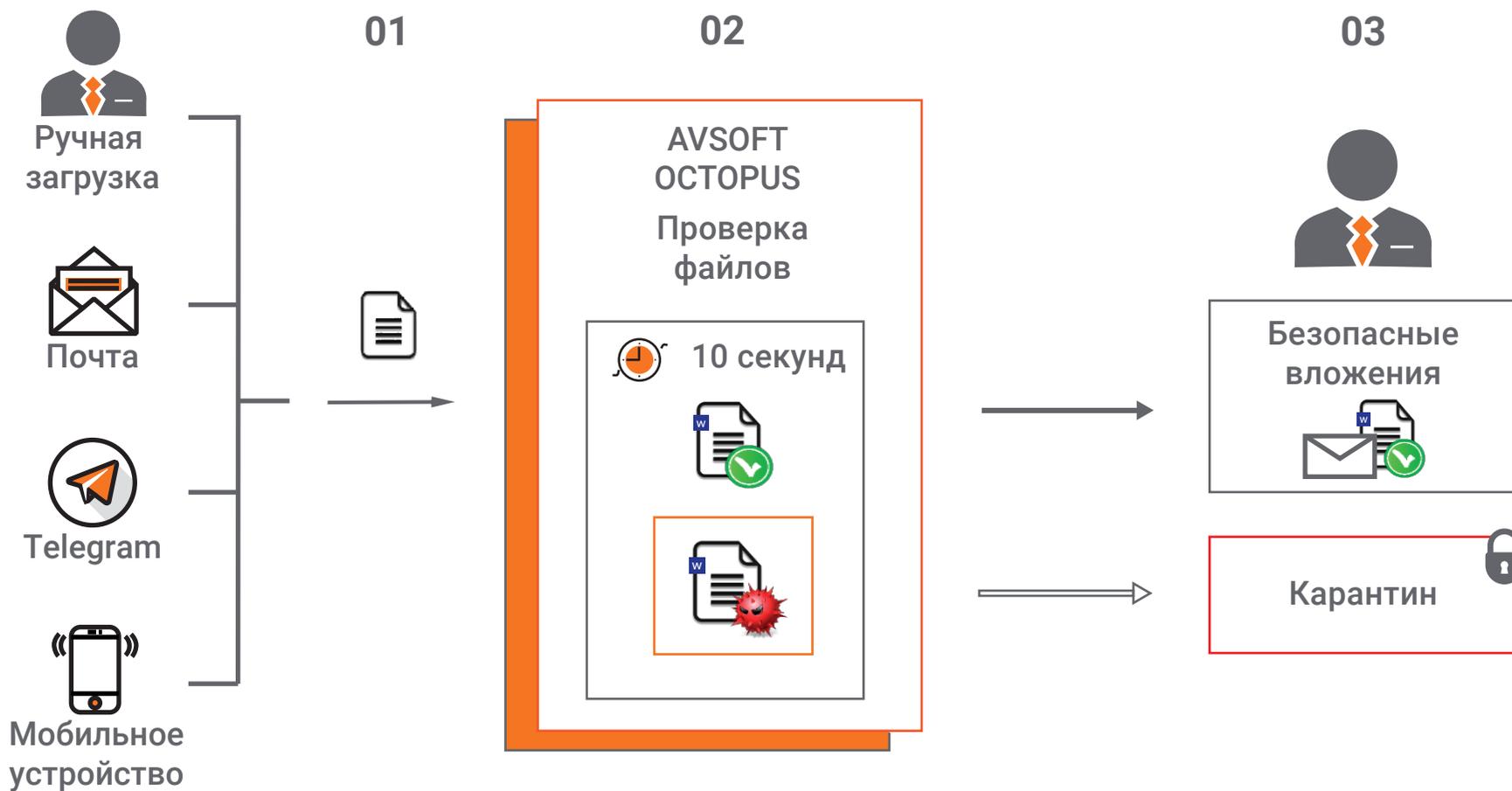


Интеграция в существующую инфраструктуру

Не требует установку дополнительного оборудования

ОБЩАЯ СХЕМА РАБОТЫ

Система «AVSOFT OCTOPUS» способна одновременно проверять файлы из различных каналов поступления данных.



ОТЧЕТ ПО ФАЙЛУ

Система «AVSOFT OCTOPUS» предоставляет подробный отчет с ключевой информацией по результатам проверки файла.

СТАТИСТИКА | ПОЧТОВЫЙ ТРАФИК | МОБИЛЬНЫЕ УСТРОЙСТВА | **ФАЙЛЫ** | ИССЛЕДОВАНИЯ | РЕСУРСЫ | СПРАВОЧНИКИ | НАСТРОЙКИ | ЖУРНАЛЫ

ФАЙЛЫ СОЗДАТЬ ИССЛЕДОВАНИЕ ПЕЧАТЬ

ИНФОРМАЦИЯ О ФАЙЛЕ

Имя:	Dino.exe	Дата загрузки образа:	19.07.2018 12:55:22
Размер:	476 Кб	Образ:	30BD27B122C117FABF5FBFB0A6CDD7EE.exe
Sha256:	7BA09403E9D7122A20FA510DE11F7809822E6E11EFB164414E2148B762CF4E75	Sha1:	BF551FBDCF5A982705C01094436883A6AD3B75BD
Md5:	30BD27B122C117FABF5FBFB0A6CDD7EE	Ssdeep:	6144:qntbWMPHyMz2+qcE0glzW2o6JQZGrt7qI3AmvXAAMXquPQcEY/0H.Ar1pyU2+qcEJoOQm+8
MIME тип:	application/x-dosexec	MIME описание:	PE32 executable (GUI) Intel 80386, for MS Windows
Расширение:	exe	Архитектура:	Athena.Data.Models.StaticResearchFileTypeArch
Операционная система:	Windows	Версия ОС:	4.0

Версия документа:

Вердикт: **ВРЕДНОСНЫЙ**

История вердиктов

СТАТИЧЕСКИЙ АНАЛИЗ

Антивирусы

Virus Total

СТАТИЧЕСКИЙ АНАЛИЗ

Антивирусы

Экспорт

Элементов на странице: 10

Дата проверки	Состояние	Вердикт
19.07.2018 12:55:22	Проверка завершена	Вредоносный

Антивирус	Версия	Версия вирусной базы	Дата обновления	Комментарий	Вердикт
AVG	13.0.3114	4793/15825	20180717	/malware/30BD27B122C117FABF5FBFB0A6CDD7EE.exe Trojan horse Generic_f_FNG;	Вредоносный
Sophos	5.47.0	5.53	20180717	Troj/Dino-A	Вредоносный
Comodo	1.1		20180717		Безопасный
Bitdefender	7.141118		20180717	Gen.Variant.Zusy.188407	Вредоносный
Avira	8.3.52.22		20180717	HEUR/AGEN.1011711	Вредоносный
ESET	7.0-20		20180717		Безопасный
Avast	2.2.0	18071700	20180717	/malware/30BD27B122C117FABF5FBFB0A6CDD7EE.exe/Win32.Dino-A [Spy];	Вредоносный
Fsecure			20180717		Безопасный
Fprot	4.6.5.141		20180717		Безопасный
Clamav	0.99.4		20180717	Win.Trojan.Dino-1	Вредоносный

Страница 1 из 1 (Всего элементов: 10)

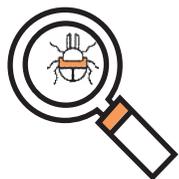
ПРОВЕРКА МОБИЛЬНЫХ УСТРОЙСТВ



О КОМПАНИИ

Компания «АВ Софт» существует с 2010 года.

Основными направлениями нашей деятельности являются разработка программного обеспечения и консалтинг в сфере информационной безопасности.



Анализ
вредоносного ПО



Расследование
инцидентов ИБ



Консалтинг в
области ИБ



Разработка ПО

КОНТАКТЫ



+7 (495) 988-92-25



office@avsw.ru



127106, Москва,
ул. Гостиничная, д.5



www.avsw.ru