



МЫ — ЗНАЕМ!

ЭВОЛЮЦИЯ. ОТ АНТИВИРУСА К EDR

Сергей Голубев
Заместитель руководителя
Управление анализа и минимизации рисков



ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

- ✗ Классический антивирус
- ✗ Endpoint Protection – дальнейшее развитие классических антивирусов
- ✗ Что такое EDR?
- ✗ Функциональные возможности EDR
- ✗ Вопросы?



КЛАССИЧЕСКИЙ АНТИВИРУС

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

[Общие](#)

Защита

[Производительность](#)

[Проверка](#)

[Дополнительно](#)



Файловый Антивирус

Проверка всех открываемых, сохраняемых и запускаемых файлов.

Вкл



Веб-Антивирус

Проверка входящего веб-трафика и предс...



Контроль программ

Контроль действий всех установленных на...



Сетевой экран

Фильтрация сетевой активности и обеспеч...



Защита от сбора данных

Защищает от сбора информации о вашей...



Защита веб-камеры

Предотвращает наблюдение за вами чере...



Обновление программ

Помогает обновить программы на вашем...



Анти-Баннер

Блокирование показа баннеров на веб-страницах и в интерфейсе...

Выкл



Параметры Файлового Антивируса

Файловый Антивирус

Проверка всех открываемых, сохраняемых и запускаемых файло...

Уровень безопасности

- Высокий (максимальная защита при работе в опасной с...
- Рекомендуемый (оптимальная защита, рекомендуется б...
- Низкий (минимальная защита при высоком быстродейст...

Действие при обнаружении угрозы:

Выбирать действие автоматически ▾



Дополнительные параметры

Типы файлов

- Все файлы
- Файлы, проверяемые по формату
- Файлы, проверяемые по расширению

Изменить область защиты

Методы проверки

- Сигнатурный анализ
- Эвристический анализ:

- Глубокий
- Средний
- Поверхностный

Оптимизация проверки

- Проверять только новые и измененные файлы

ENDPOINT PROTECTION – ДАЛЬНЕЙШЕЕ РАЗВИТИЕ КЛАССИЧЕСКИХ АНТИВИРУСОВ

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

Ключевые отличия решений класса Endpoint Protection от антивирусов:

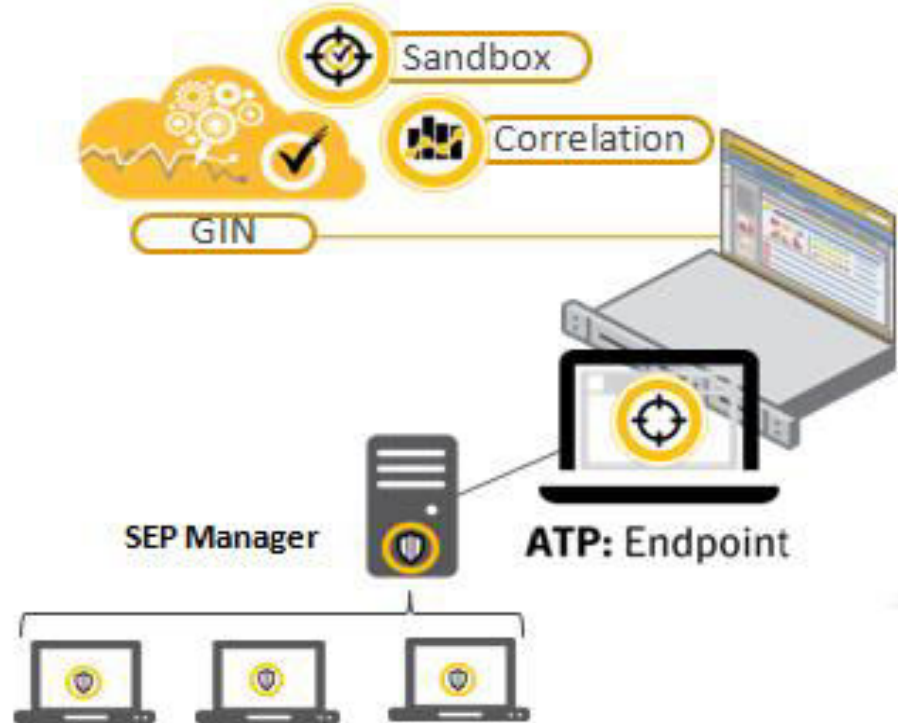
1. Единая консоль управления всеми агентами;
2. Расширенный инструментарий выявления активности вредоносного ПО (от брандмауэра до встроенного эмулятора загрузки);
3. Интеграция с SIEM и DLP системами, прокси и антиспам серверами, а так же различными облачными системами безопасности (CASB, Cloud SOC).


								
БРАНДМАУЭР И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ	КОНТРОЛЬ ПРИЛОЖЕНИЙ И УСТРОЙСТВ	ЗАЩИТА ОТ ЭКСПЛОЙТОВ В ПАМЯТИ	АНАЛИЗ РЕПУТАЦИИ	МАШИННОЕ ОБУЧЕНИЕ	ЭМУЛЯТОР	АНТИВИРУС	МОНИТОРИНГ ПОВЕДЕНИЯ	БРАНДМАУЭР И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ
Контроль трафика и превентивная блокировка вредоносного кода	Контроль файлов, реестра и устройств; черные и белые списки.	Блокировка эксплойтов нулевого дня в известном программном обеспечении	Выявление опасных файлов и сайтов с помощью сообщества	Заблаговременное выявление новых и эволюционирующих угроз	Виртуальная машина для выявления угроз, скрытых с помощью упаковщиков	Сканирование на вредоносные программы и удаление их из системы	Отслеживание и блокирование файлов с подозрительным поведением	Контроль трафика и превентивная блокировка вредоносного кода

ЧТО ТАКОЕ EDR?

EDR (Endpoint Detection & Response) – это дальнейшее развитие решений класса Endpoint Protection, когда при интеграции решения Endpoint Protection и решений класса ATP (например, песочниц) мы получаем новый функционал, который не может дать каждое решение по отдельности.

Ключевым компонентом EDR является ATP Endpoint Module, который проводит корреляцию данных, получаемых с агентов Endpoint Protection и решений ATP, и переносит в карантин/удаляет все файлы с вредоносным ПО и низким рейтингом.



ca_setup.exe 



Bad
DISPOSITION

Not Available
CYNIC VERDICT

No
TARGETED ATTACK

SecurityRisk.BL
AV SIGNATURE NAME

f98bc99cb8160d4e7f19fb76410ca4fab37c3d3dbfef6123b54c6c...
SHA256

ea2ef30c99ecec1eda9aa128631ff31
MD5

Not Signed
CERTIFICATE

Unknown
FILE TYPE

File Overview

6
RELATED EVENTS

0
RELATED INCIDENTS

0
EMAIL DETECTIONS

0
CYNIC MODIFICATIONS

1
EXTERNAL MACHINES ACCESSED

Global Reputation

Years ago
FIRST SEEN

Tens of thousands of users
PREVALENCE

Local Reputation


Weeks ago
FIRST SEEN


2 internal endpoints
PREVALENCE

Further actions



Add to Blacklist 

Add to Whitelist 

Submit to Cynic 

Submit to VirusTotal 

Copy to file store 

Delete 

П

