МЫ — ЗНАЕМ!

ЭВОЛЮЦИЯ. ОТ АНТИВИРУСА К EDR

Сергей Голубев
Заместитель руководителя
Управление анализа и минимизации рисков

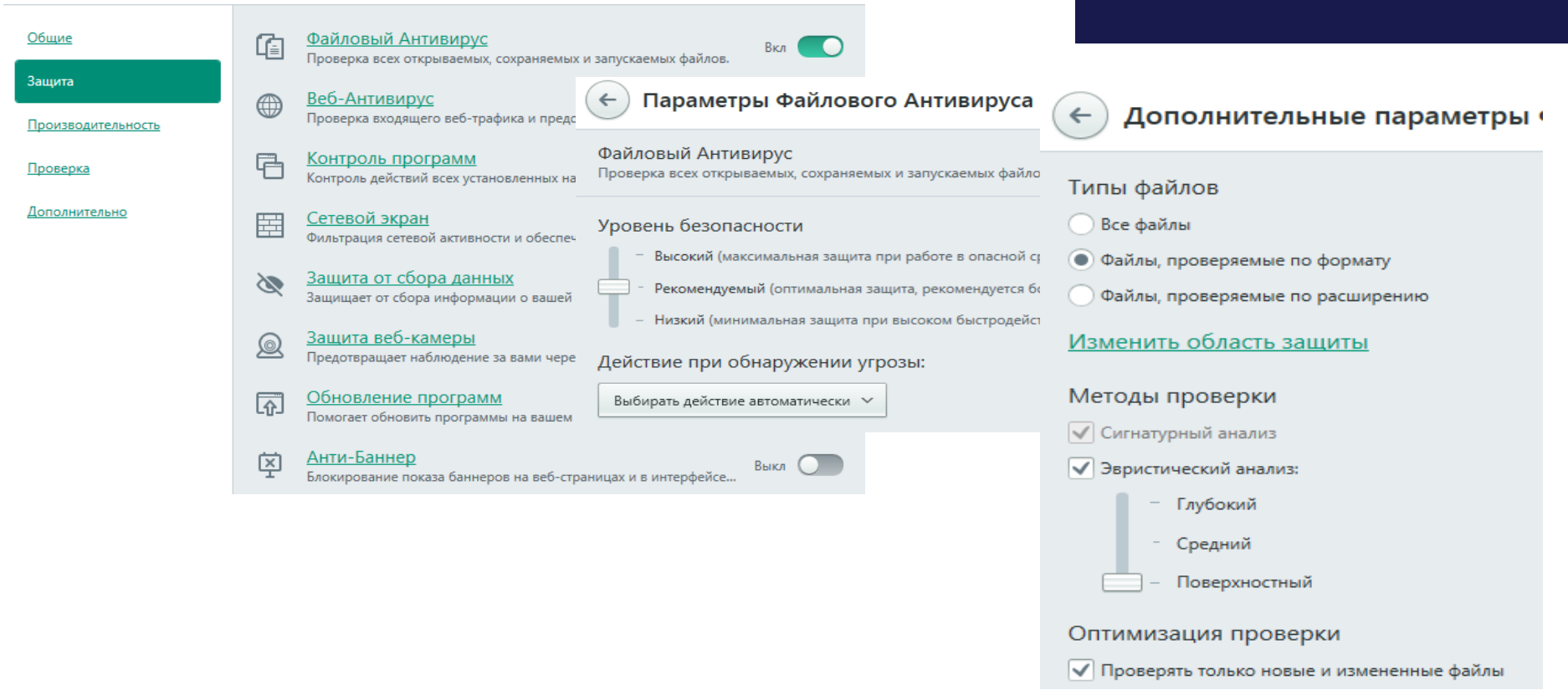
ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

ОГЛАВЛЕНИЕ

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

КЛАССИЧЕСКИЙ АНТИВИРУС

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ



ENDPOINT PROTECTION – ДАЛЬНЕЙШЕЕ РАЗВИТИЕ КЛАССИЧЕСКИХ АНТИВИРУСОВ

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

Ключевые отличия решений класса Endpoint Protection от антивирусов:

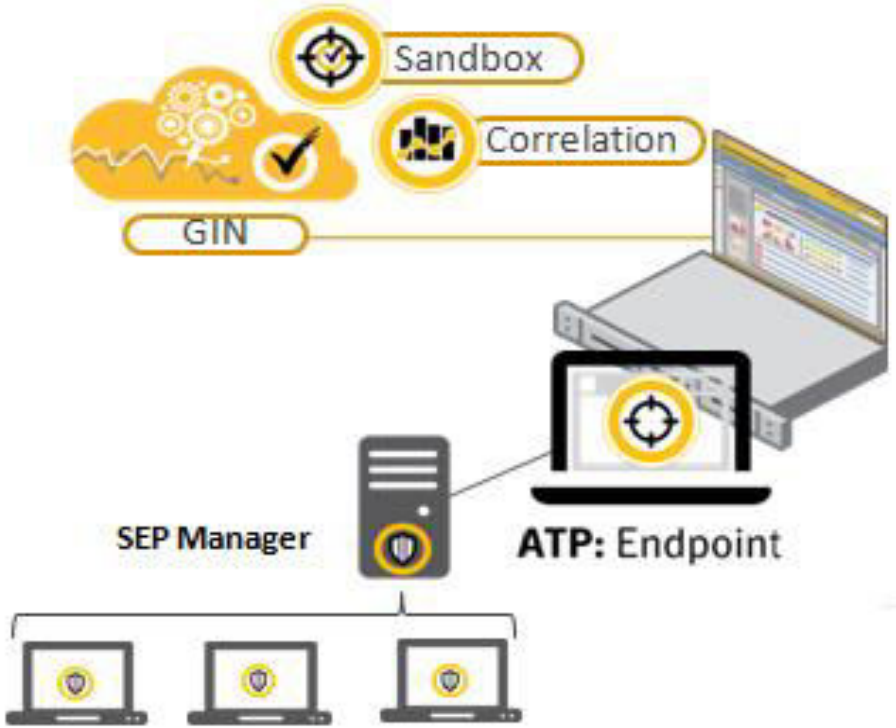
1. Единая консоль управления всеми агентами;
2. Расширенный инструментарий выявления активности вредоносного ПО (от брандмауэра до встроенного эмулятора загрузки);
3. Интеграция с SIEM и DLP системами, прокси и антиспам серверами, а так же различными облачными системами безопасности (CASB, Cloud SOC).

ЧТО ТАКОЕ EDR?

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

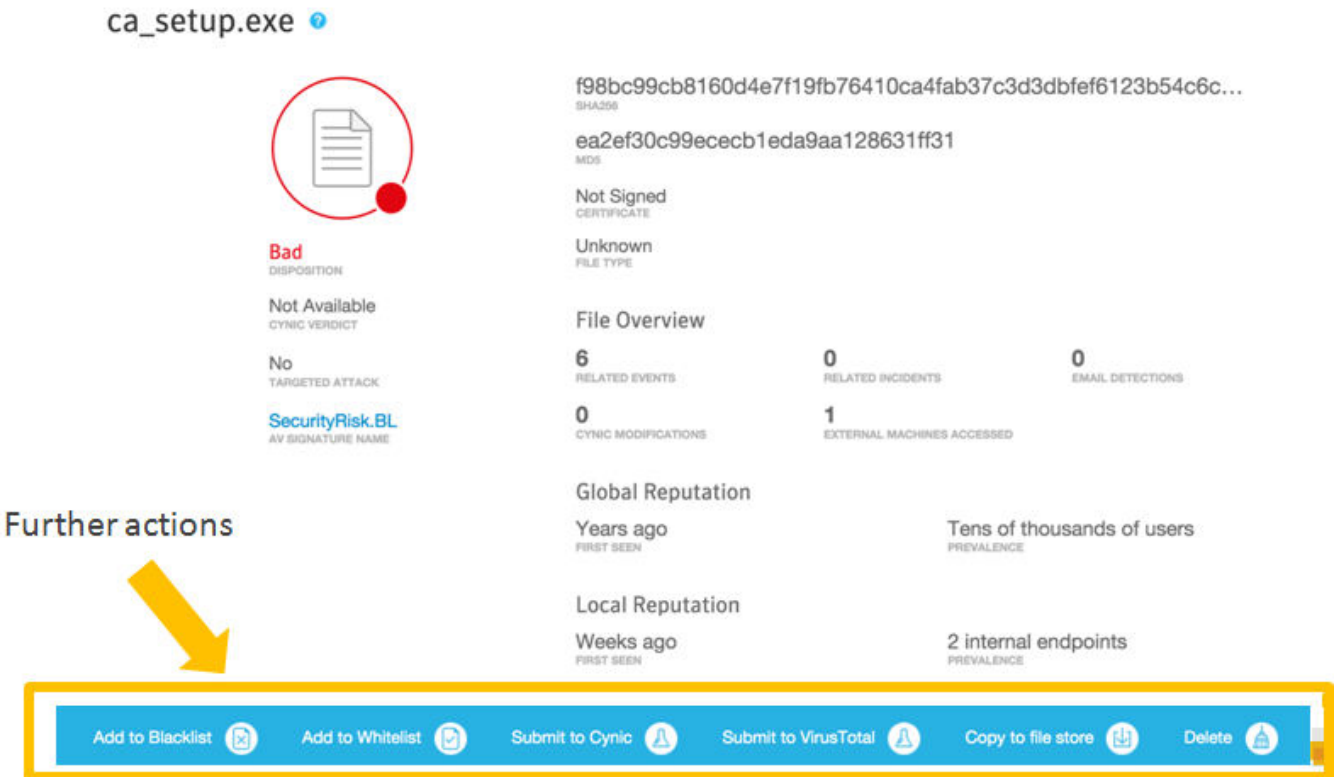
EDR (Endpoint Detection & Response) – это дальнейшее развитие решений класса Endpoint Protection, когда при интеграции решения Endpoint Protection и решений класса ATP (например, песочниц) мы получаем новый функционал, который не может дать каждое решение по отдельности.

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.



ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ EDR

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ



ВОПРОСЫ

ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ

П