



Защита от направленных атак

Шабуров Олег

Руководитель направления ИБ

Защита от направленных атак: почему тяжело?



Это произойдет...

Традиционный подход устарел. Не «если», а «когда» будет инцидент!

Слишком много времени на детектирование

229 дней в среднем тратится на обнаружение инцидента!

Мало знаний

70% признаются в недостатке ресурсов, умеющих реагировать на кибер-инциденты

Время реагирования не устраивает бизнес

Среднее время реакции от недель до месяцев!

У вас больше не будет вирусов...



Результаты разбора инцидентов

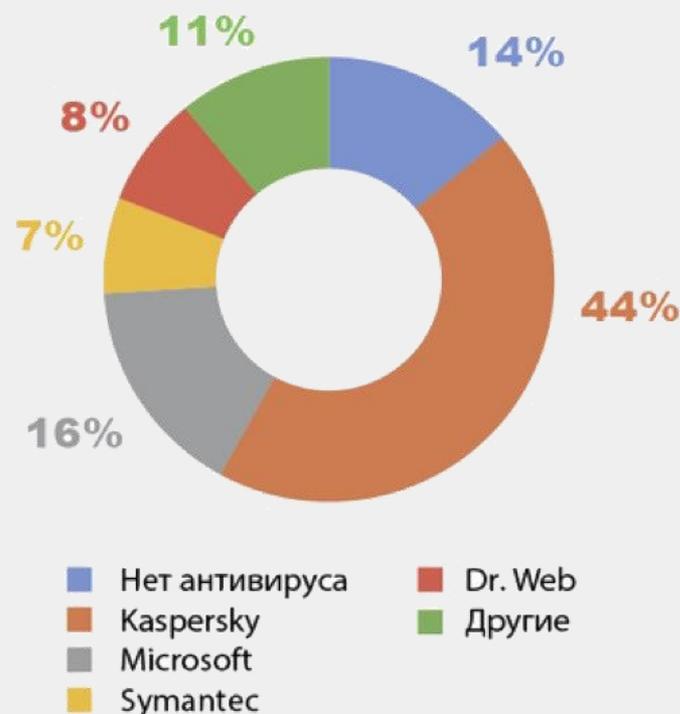
86%

зараженных машин
имеют установленное
антивирусное средство

1.5 МЛН

компьютеров в России
заразил ботнет Carberp

Использование антивирусов на зараженных компьютерах



Источник: Group-IB, декабрь 2014

Без пересмотра подхода к ИБ нельзя

60

КОМПАНИЙ СТАЛКИВАЮТСЯ С >25
ИНЦИДЕНТАМИ В МЕСЯЦ

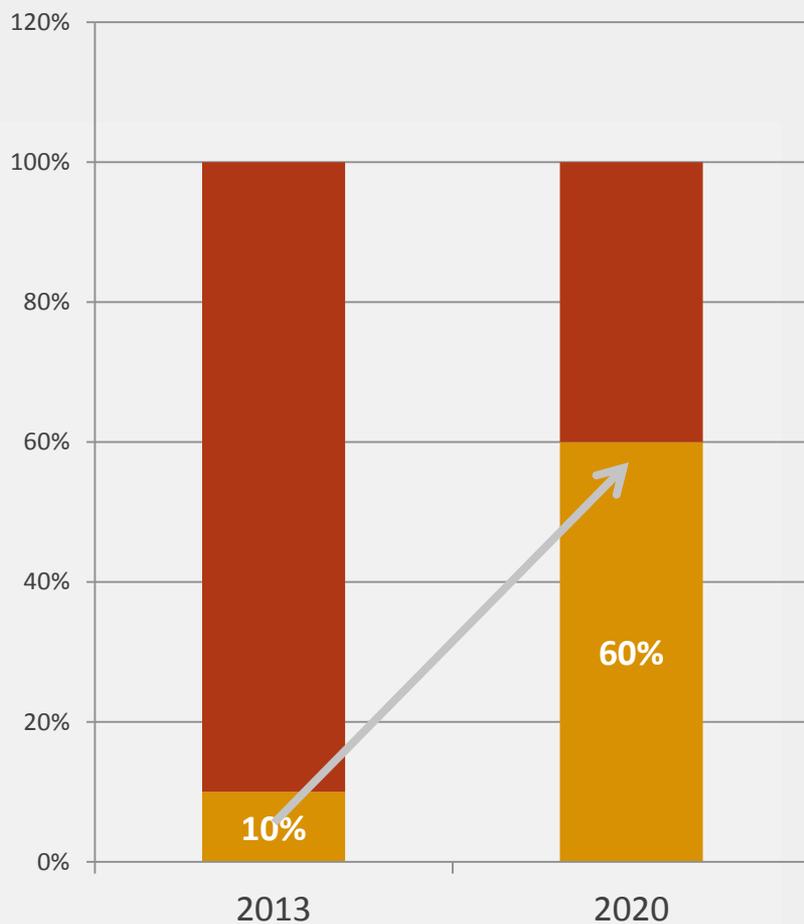
%

Гибкость в реагировании на инцидент

Понимание угрозы

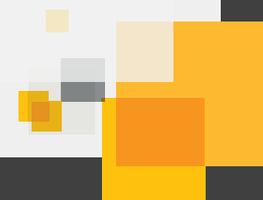
Время

Динамика рынка ведет к перераспределению бюджетов



*“К 2020 году **60%** корпоративных ИБ бюджетов будут потрачены на быстрое обнаружение и реагирование (менее чем 10% в 2013).”*

Gartner.



Волны АТР-решений

- Первая волна – сетевые решения
- Вторая волна – на рабочих станциях и серверах
- Необходима интеграций решений, работающих на разных уровнях



Защита от направленных атак на конечных точках

3 важные причины

1

**Рабочие станции и сервера –
цель направленных атак**

*Здесь хранится информация,
на которую охотится
злоумышленник*



*Ponemon Institute: 2014 State of Endpoint Risk

2

**Рабочие станции и
мобильные устройств – до
90% всей инфраструктуры**

*Необходимо контролировать
эту часть и за периметром*



Источник: Gartner - Endpoint Threat Detection and Response Tools and Practices, 2013

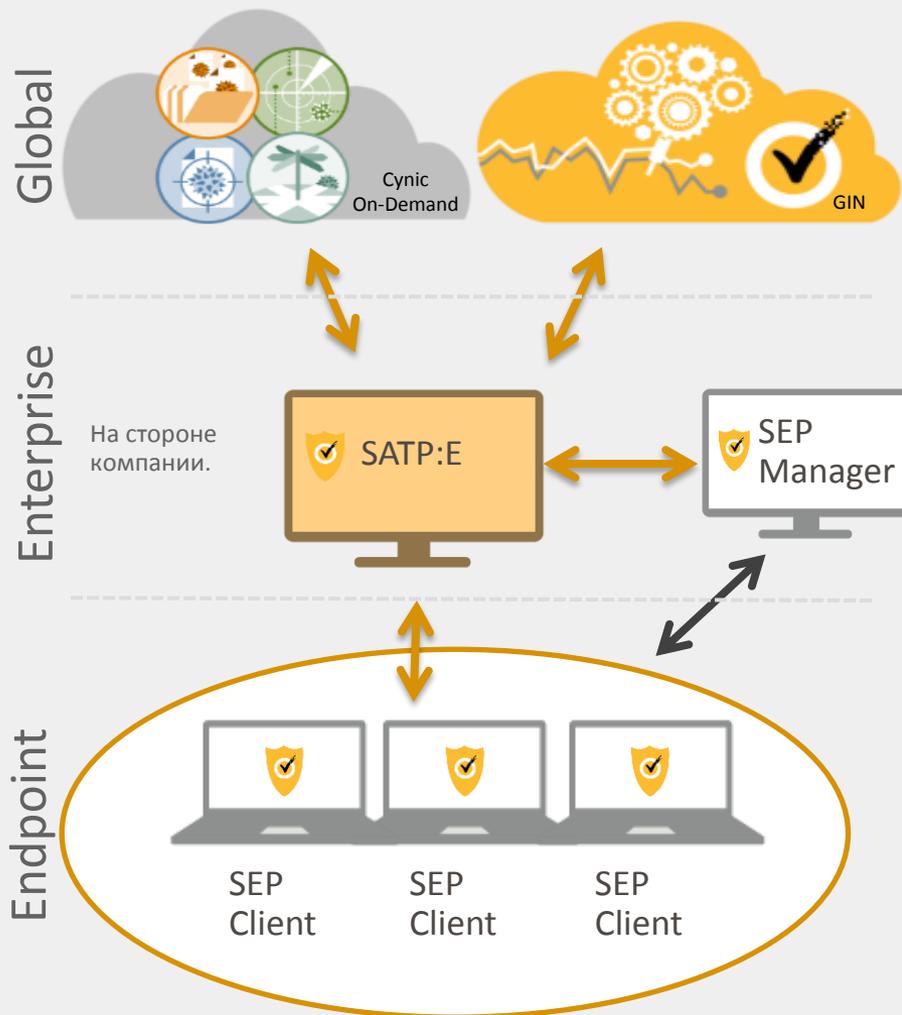
3

**Необходимо понять, что на
самом деле произошло**

*“Организациям необходимо
оценить решения для рабочих
станций и ускорить их
внедрение” (Gartner)*



Механизмы защиты от направленных атак, работающие на уровне рабочих станций



Аккуратное обнаружение

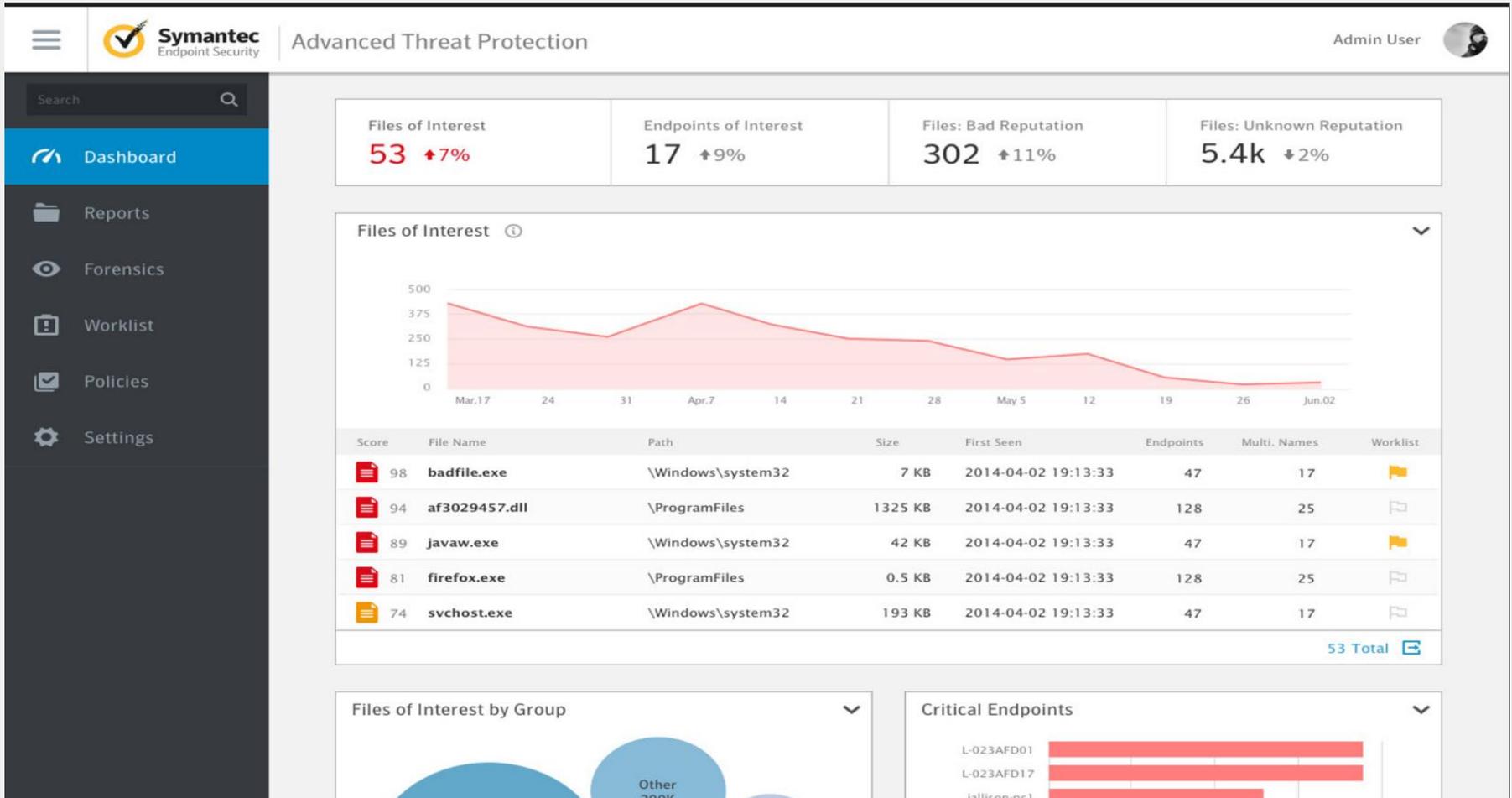
Быстрый анализ

Уверенное реагирование

Почему решение от Symantec:

- Глубокая интеграция с антивирусным продуктом.
- Высокоточная приоритезация подозрительной активности с использованием машинного обучения
- Информация о признаках подозрительной активности для обоснованного реагирования.

Обнаружение подозрительных ситуаций



Быстрый анализ и реагирование

< File Details



Name: svchost.exe

Hash: [+](#) e6c9503b80fc74d2...

IPS Hits: 13

First Seen: **2014-04-02 18:30:00 UTC**

Total Locations: **4**

Distribution: **Coming soon**

[+ Add Rule](#) [Worklist](#) [Get File](#) [Ignore](#)

Download Domains: **2**

Creator Processes: **5**

Creator Paths: **4**

On Endpoints: **4**

No. of Filenames: **3**

Certificate: **AVSecurityCo**

Symantec INSIGHT™ ⓘ

Few Users
Less than 50 total

Mature
Seen 4 years, 10 months ago

Trusted
Symantec Insight rating

[What is Symantec Insight?](#)

Symantec Cynic Verdict: Not submitted ⓘ

[Submit](#)

IPS Signature Hits ⓘ

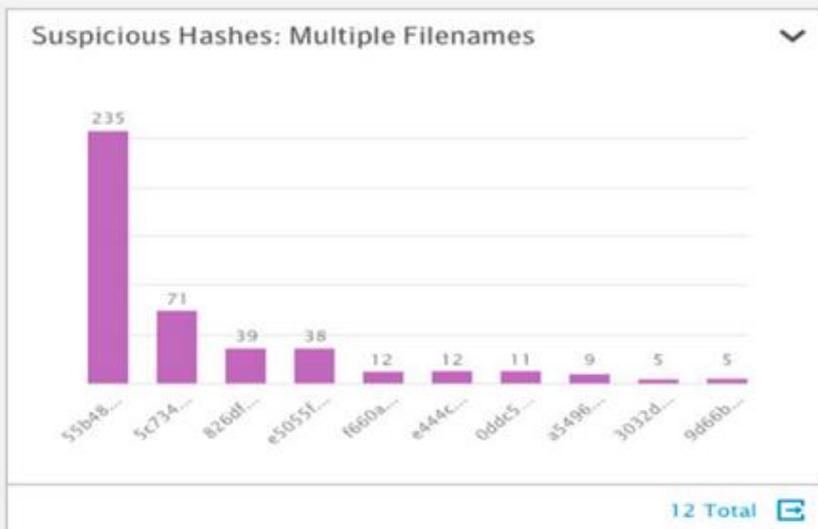
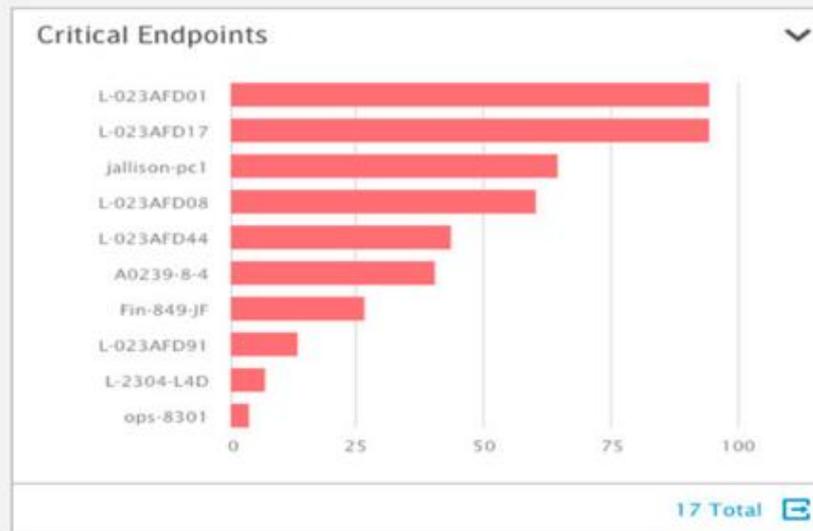
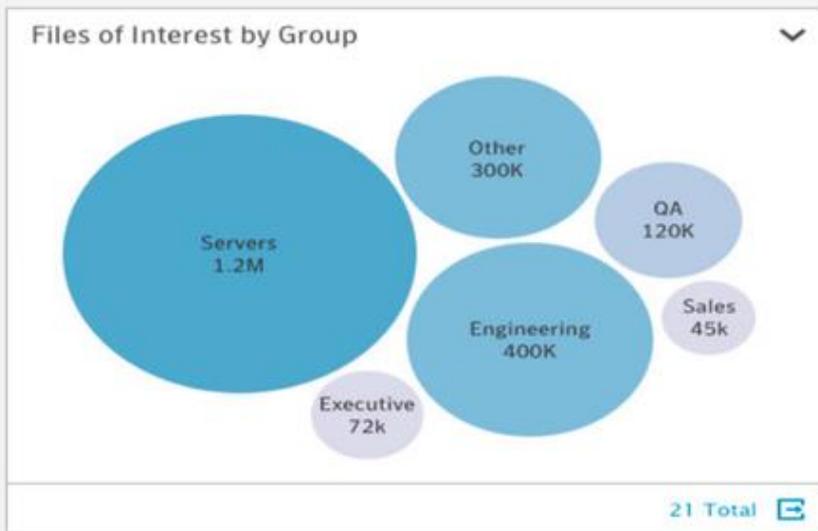
Attacker Signature ID	Total Hits	Signature Properties	First Detected
218576287	11	Information specific to this intrusion signature	2014-04-02 19:13:33 UTC
147388309	2	--	2014-04-02 19:13:33 UTC

2 Total

Multiple File Names

Name	Path	Publisher	On Endpoint	Prevalence	Confidence	Creation Date
------	------	-----------	-------------	------------	------------	---------------

Категоризация по компонентам инфраструктуры



Один в поле не воин!





Спасибо за внимание!

Олег Шабуров

oleg_shaburov@symantec.com

+7-916-924-8006

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.