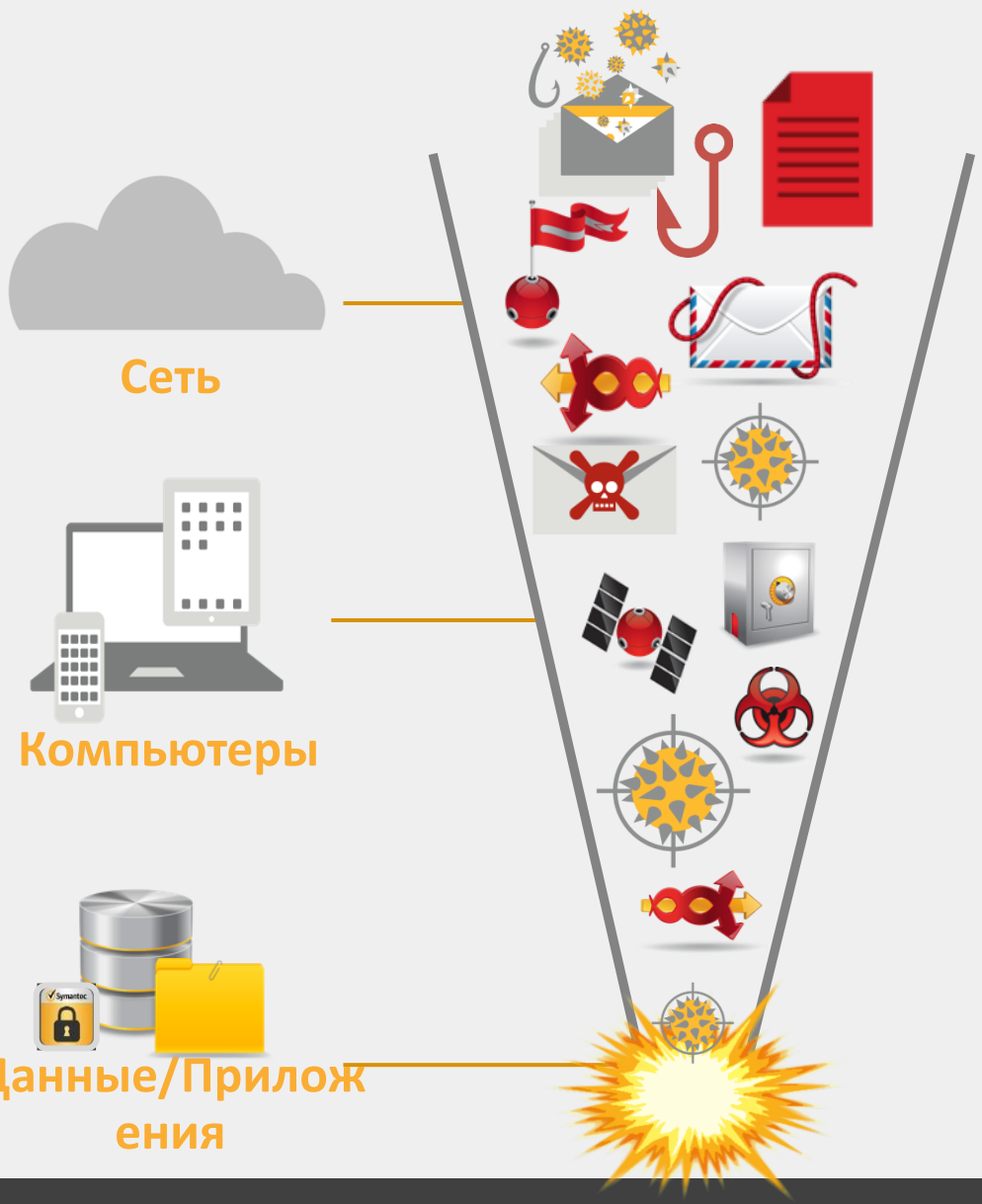
Защита от направленных атак

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-инциеднты

Время реагирования не устраивает бизнес

Среднее время реакции от недель до месяцев!

У вас больше не будет вирусов…

Copyright © 2014 Symantec Corporation

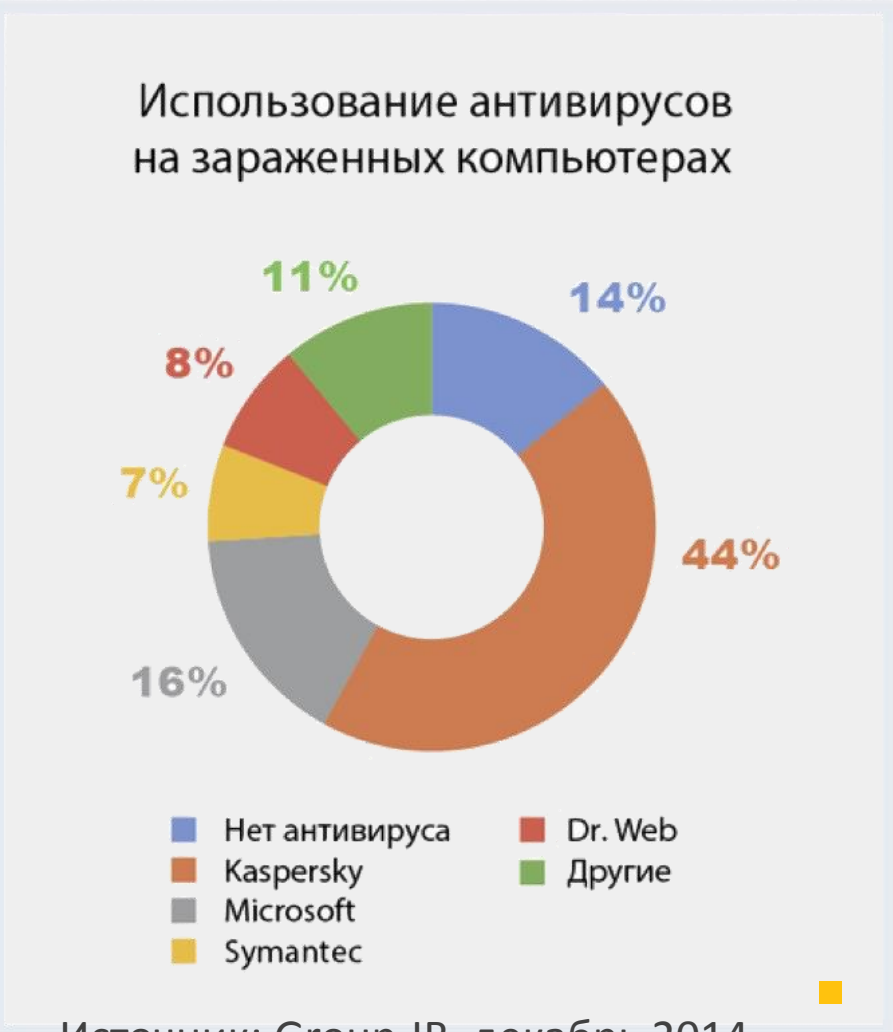
Результаты разбора инцидентов

86%

зараженных машин имеют установленное антивирусное средство

1.5 млн

компьютеров в России заразил ботнет Carberp

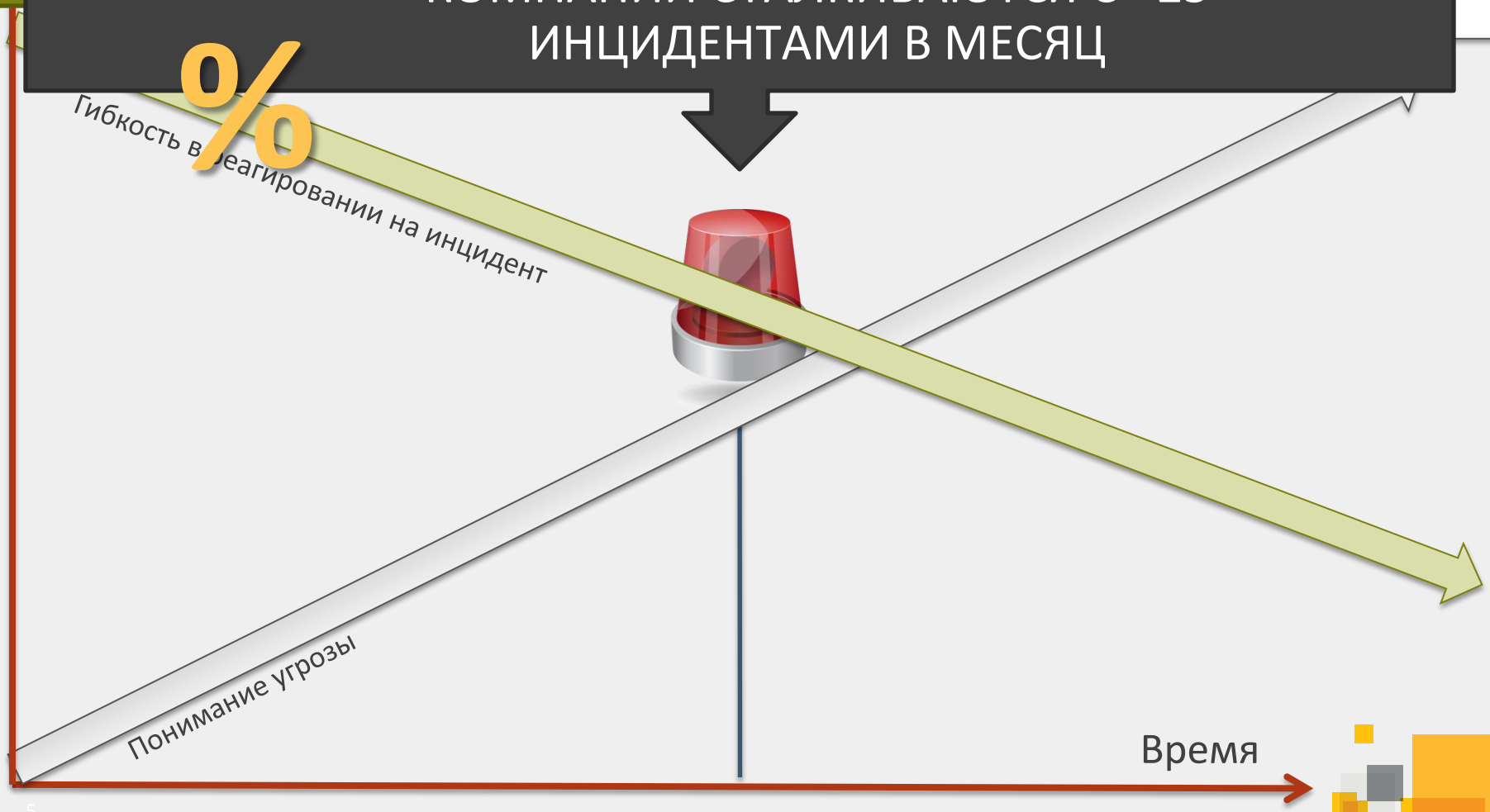


Источник: Group-IB, декабрь 2014

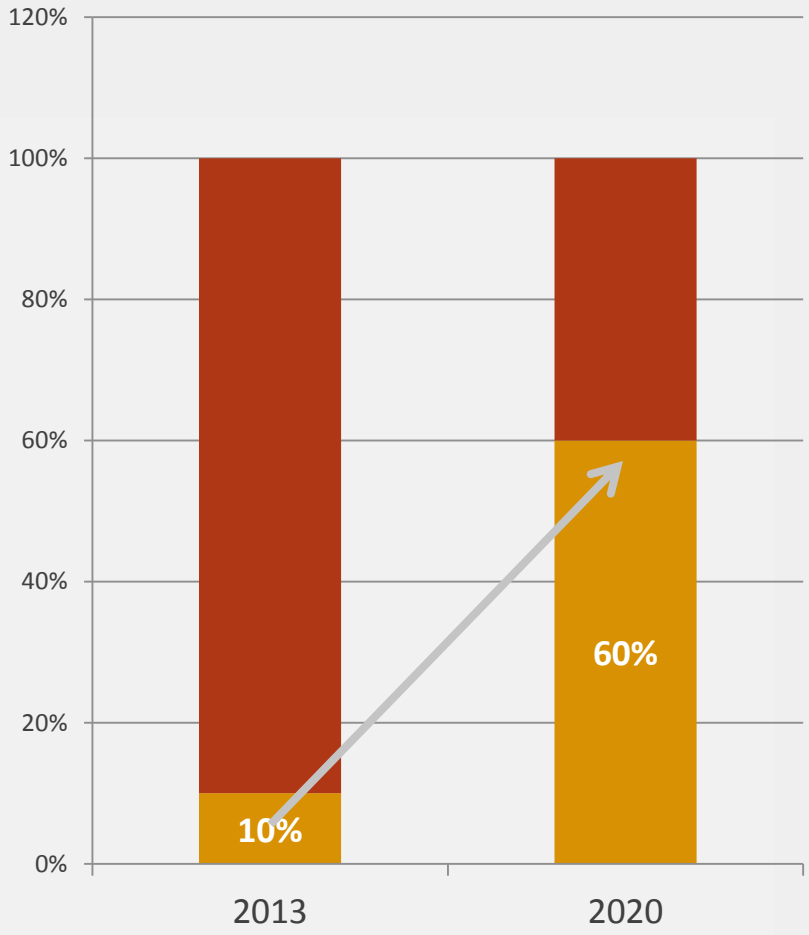
Copyright © 2014 Symantec Corporation

Без пересмотра подхода к ИБ нельзя

60% КОМПАНИЙ СТАЛКИВАЮТСЯ С >25 ИНЦИДЕНТАМИ В МЕСЯЦ



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

Copyright © 2014 Symantec Corporation

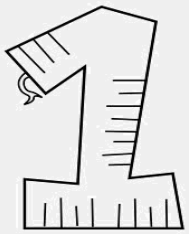
Волны ATP-решений

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

Copyright © 2014 Symantec Corporation

Защита от направленных атак на конечных точках

3 важные причины



Рабочие станции и сервера – цель направленных атак

Здесь хранится информация, на которую охотится злоумышленник

*Ponemon Institute: 2014 State of Endpoint Risk

Рабочие станции и мобильные устройств – до 90% всей инфраструктуры

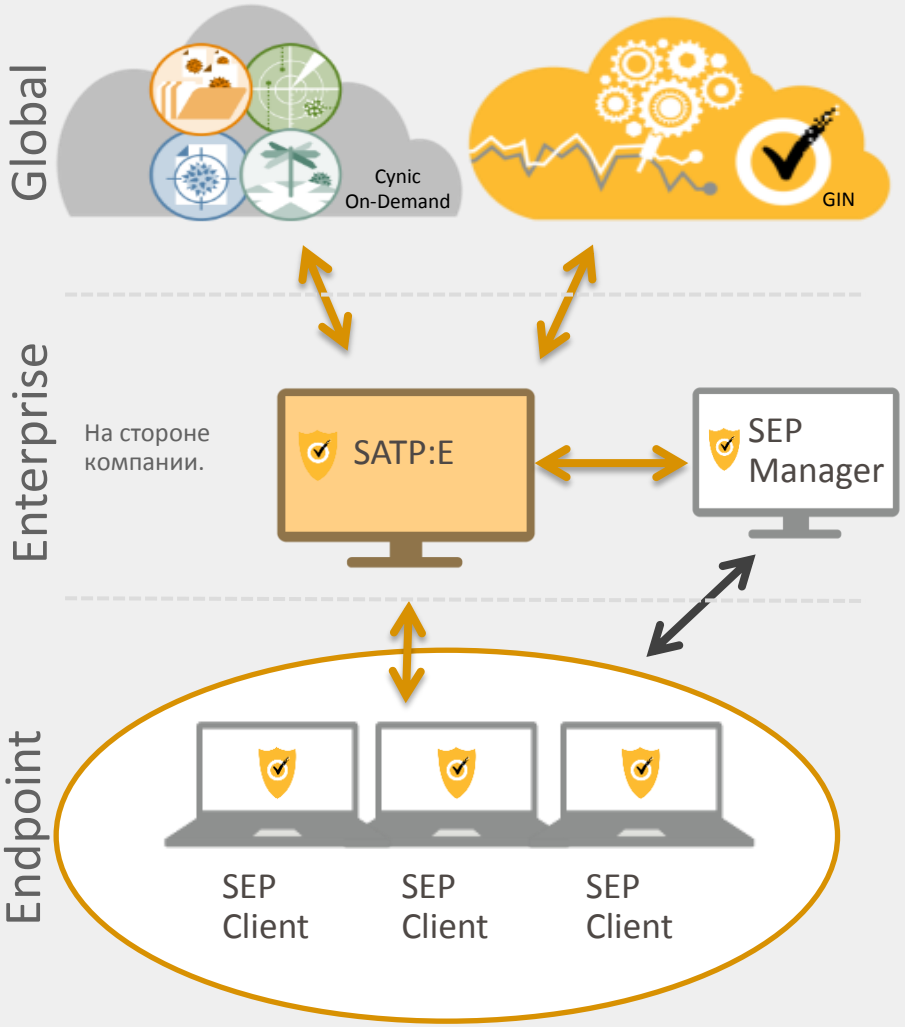
Необходимо контролировать эту часть и за периметром

Необходимо понять, что на самом деле произошло

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

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

Механизмы защиты от направленных атак, работающие на уровне рабочих станций



Аккуратное обнаружение

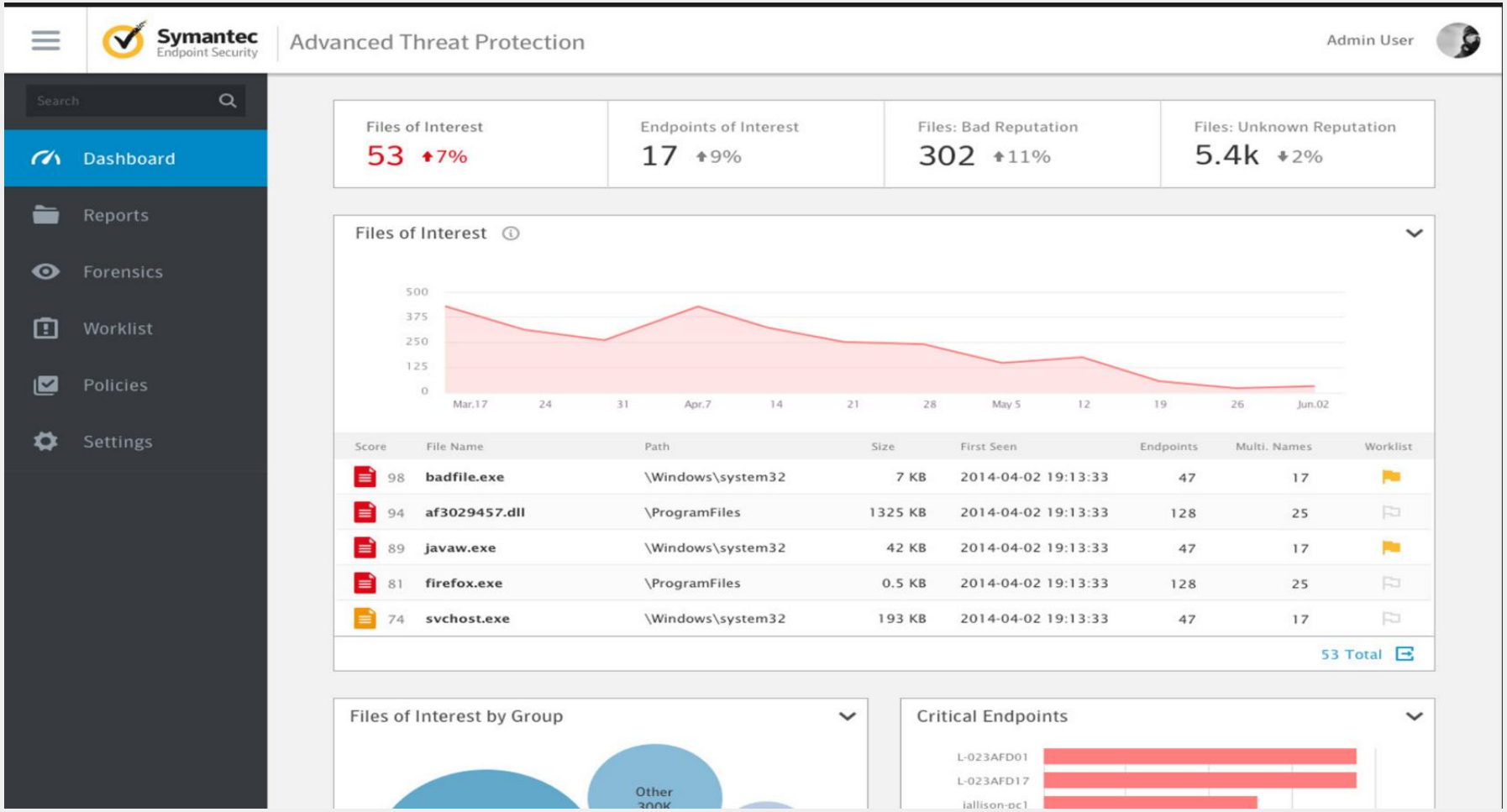
Быстрый анализ

Уверенное реагирование

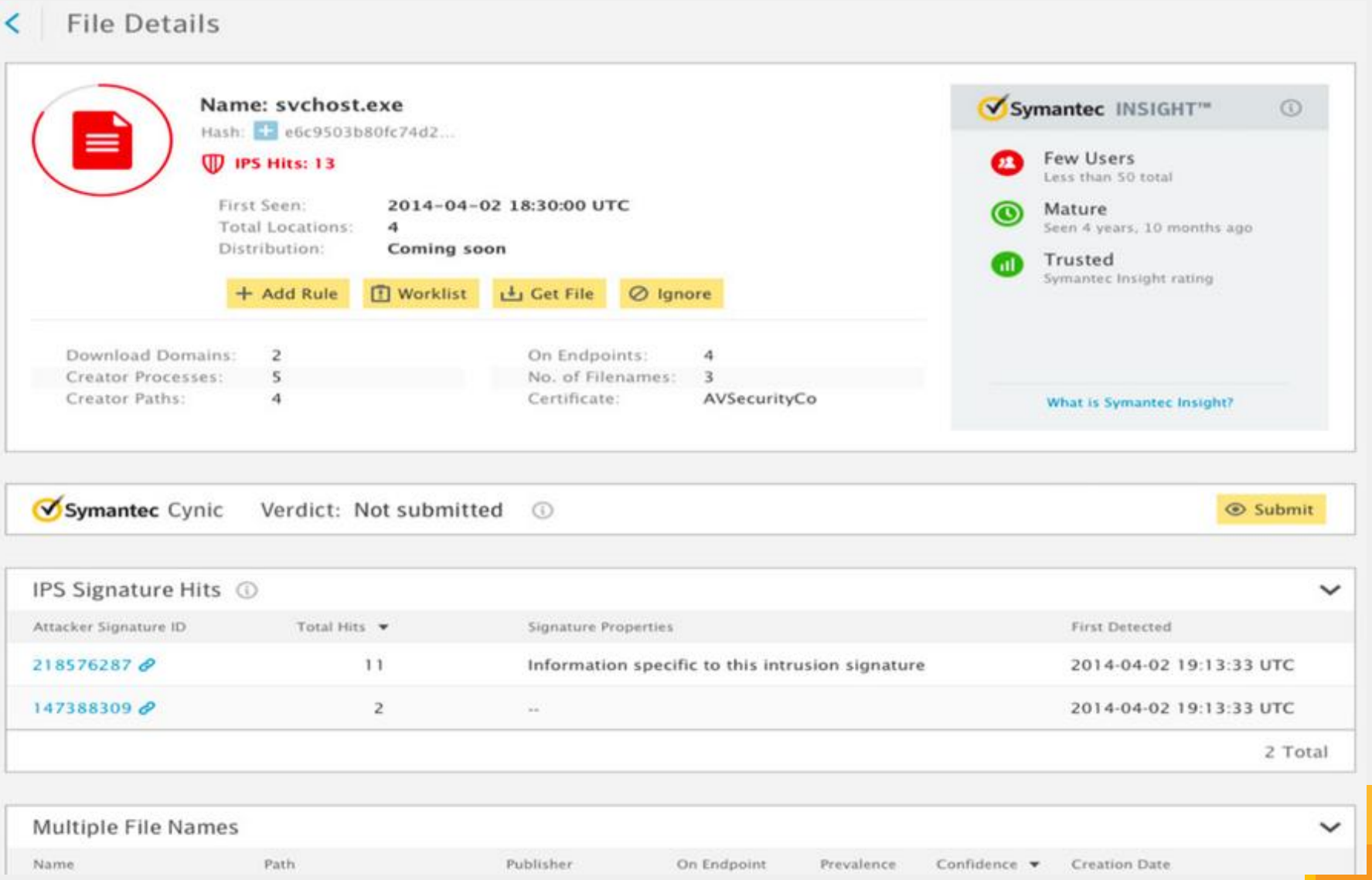
Почему решение от Symantec:

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

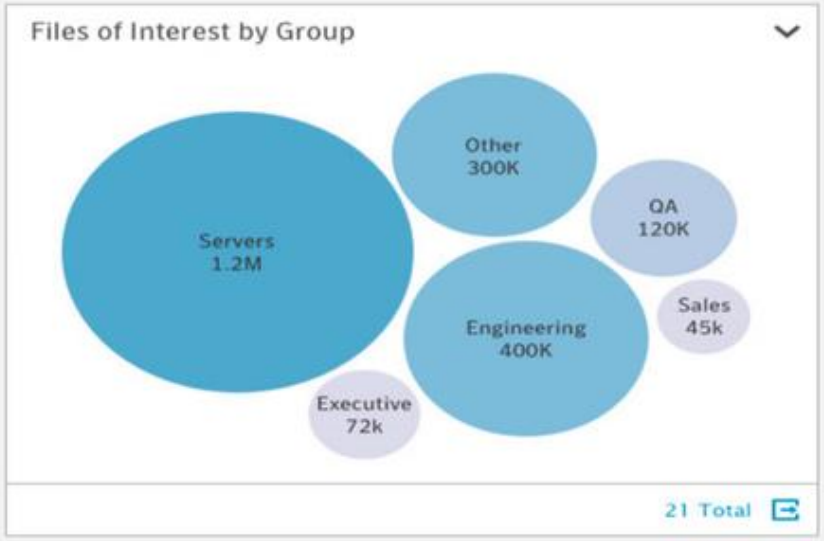
Обнаружение подозрительных ситуаций

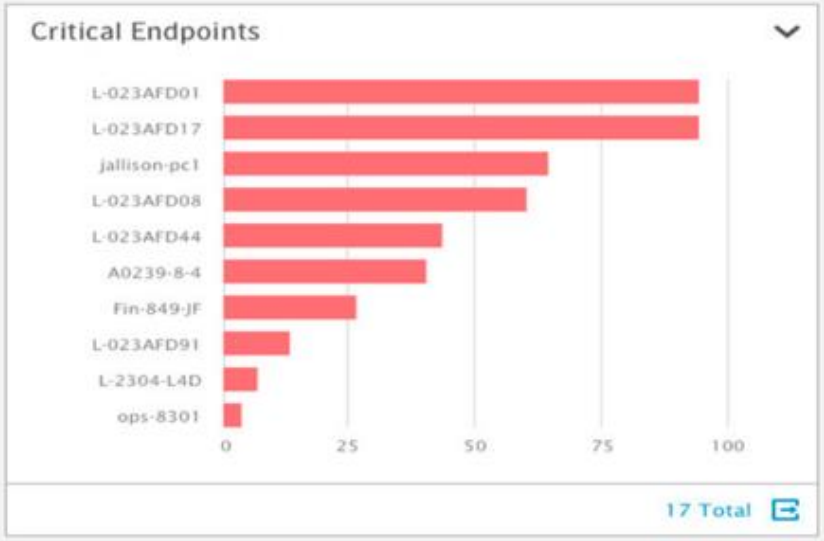


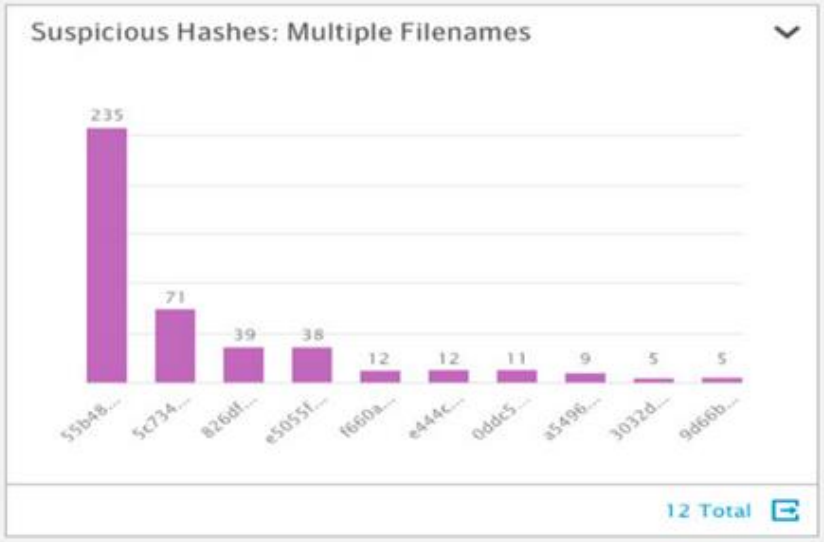
Быстрый анализ и реагирование



Категоризация по компонентам инфраструктуры







Один в поле не воин!

Copyright © 2014 Symantec Corporation

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.