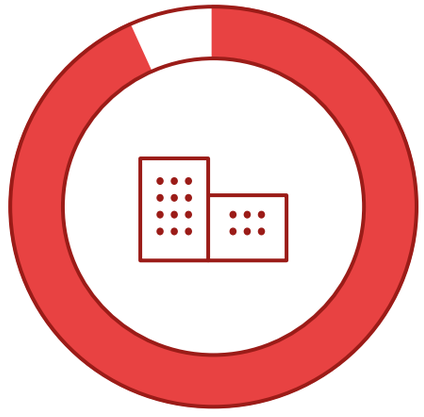
pandasecurity.com

Практическое руководство по безопасности

для предотвращения кибер-вымогательств

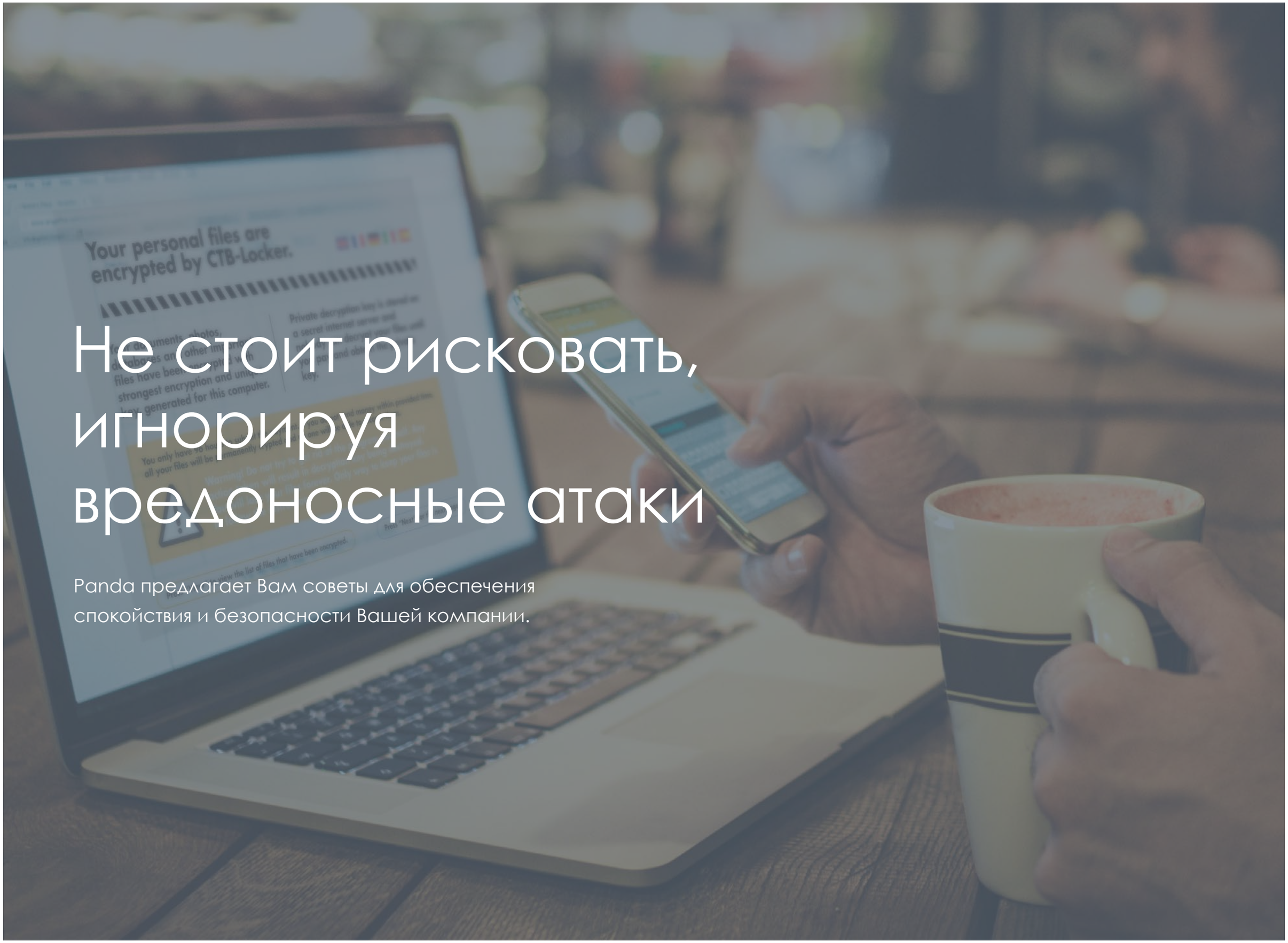
Европейские компании чаще всего сталкиваются с кражей критически важных данных.

Согласно прогнозу на 2016 год, **Европа и дальше будет подвергаться риску кибер-атак**.



91% малых и средних предприятий были объектами IT-атак

Источник: Shopper Software Security in SMBs. Nielsen, April 2015



Не стоит рисковать, игнорируя вредоносные атаки

Panda предлагает Вам советы для обеспечения спокойствия и безопасности Вашей компании.

Что такое кибер-вымогательства?

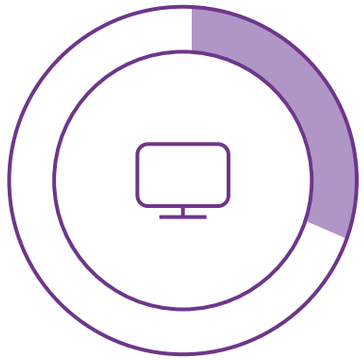
Кибер-вымогательство - это форма шантажа, когда жертвы IT-атаки вынуждены платить во избежание его последствий.

Один из самых распространеных методов кибер-вымогательства - это шифровальщики (ransomware). Такая атака шифрует информацию жертвы, а затем требует выкуп для ее расшифровки и возврата.

Став жертвой вымогательства и заплатив выкуп кибер-преступникам, жертва обычно получает письмо с кодом для расшифровки информации. Для оплаты, как правило, используют цифровую валюту Bitcoin (1 Bitcoin = 380$). На самом деле, этот метод платежа используется для того, чтобы его нельзя было отследить. Однако, оплата не гарантирует предприятию, что оно не будет в будущем атаковано снова.

Другие подобные атаки, использующие такой тип вымогательства, заражают Ваш ПК и получают доступ к его веб-камере, после чего Вас шантажируют публикацией видео.

Большинство атак начинаются с писем, которые содержат вложенные документы, или с посещения небезопасных веб-сайтов.



39%

Небезопасные и мошеннические веб-сайты

23%

Скачивание программ

19%

Вредоносные программы, полученные по электронной почте

Источники заражений
Источник: Shopper Software Security in SMBs. Nielsen, April 2015

Как кибер-преступники используют шифровальщики для атак?

Такие шифровальщики как Cryptolocker, Cyptowall или Coinvault угрожают целостности файлов, которые находятся на ПК или доступных сетевых устройствах.

Эти угрозы шифруют данные, расшифровка которых возможна только с помощью ключа. Злоумышленники его могут предоставить только после получения выкупа от своей жертвы.

Если Ваша компания пострадала от шифровальщиков, то, как правило, Вам предоставляется от 48 до 72 часов на выплату выкупа. Если Вы не заплатите в течение указанного времени, то стоимость расшифровки может возрасти.

Если Вы не заплатите и в дополнительный период времени, то скорее всего ключ будет уничтожен, а значит данные уже нельзя будет восстановить.

Даже если платеж осуществлен, то нет никакой гарантии, что Ваши данные будут возвращены. Это вызвано тем, что программа, разработанная преступниками, может содержать ошибки, которые приведут к сбоям процесса дешифрации. Кроме того, правоохранительные органы постоянно пытаются нарушить инфраструктуру вымогателей.

Что делать, если Вы стали жертвой кибер-вымогательства?

Не поддавайтесь на шантаж преступников

Нет гарантий, что выполнение их требований решит проблему.

Фактически, во многих случаях жертвы шантажа оплачивали выкуп, но они либо не получали ключ, либо получали его поврежденным. В этих случаях невозможно получить назад зашифрованную информацию.

Встречается и неоднократный шантаж. После возврата информации, злоумышленники запускали процессы, которые вскоре начинали снова шифровать корпоративные данные.

В других случаях кибер-преступники требовали более значимую сумму, чем запрашивали изначально, в зависимости от ощущения отчаяния жертвы или финансового положения компании.

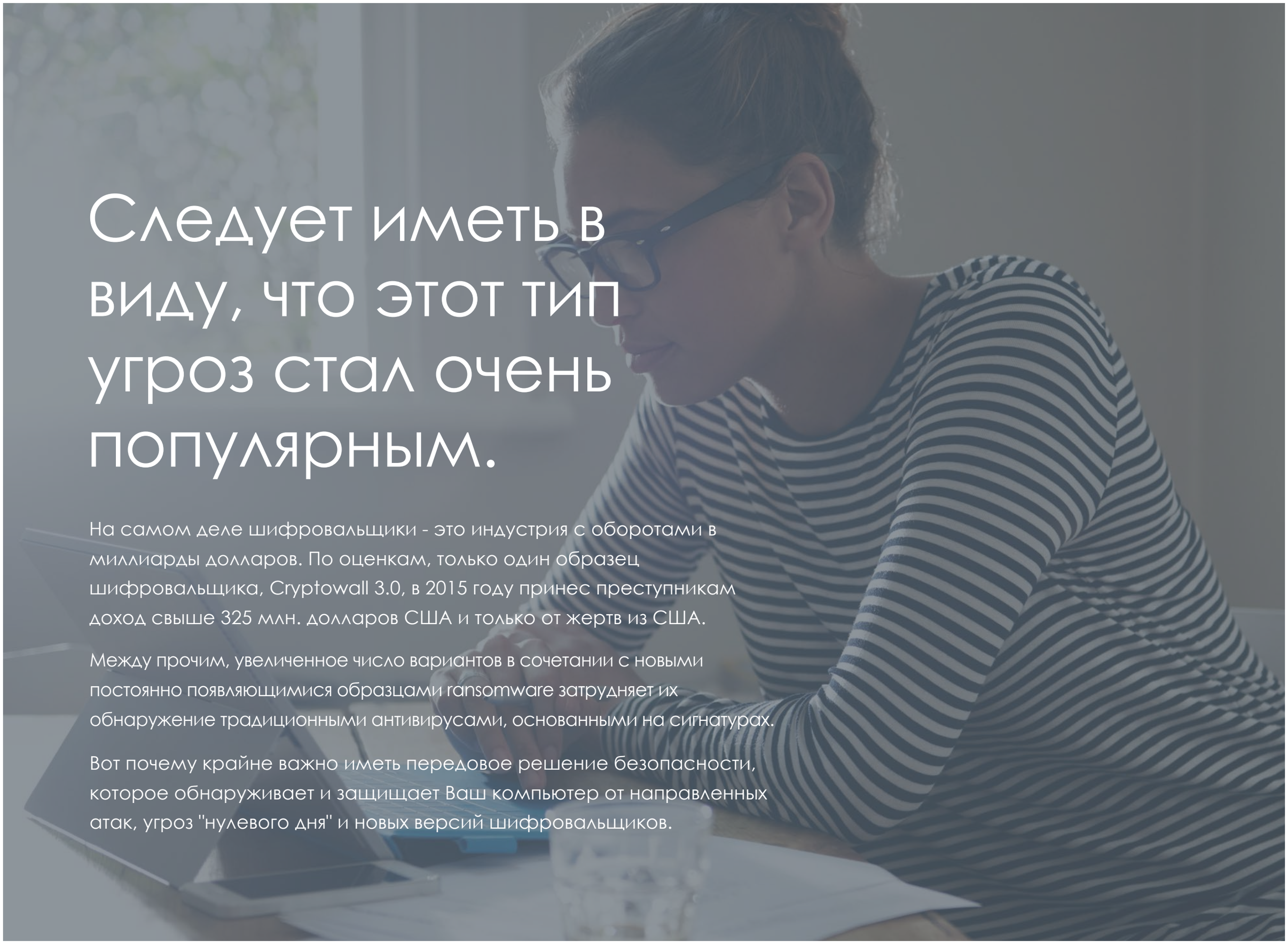
Полностью сотрите все следы зловреда с Ваших компьютеров

Для этого Panda рекомендует использовать **Cloud Cleaner** в оффлайновом режиме - решение, которое специализируется на удалении всех следов современных вирусов с зараженных компьютеров.

Восстановите все Ваши зашифрованные файлы

Для этого необходимо предварительно активировать Историю файлов (в Windows 8.1 и 10) или Защиту системы (Windows 7 и Vista), которые позволят Вам отменить изменения в файлах с данными, сделанные вредоносными программами.

Также рекомендуется периодически делать резервные копии критически важных файлов. Если у Вас есть свежий бэкап Ваших важных документов, то мы советуем Вам проверять их на любые остатки вредоносных программ перед их восстановлением.



Следует иметь в виду, что этот тип угроз стал очень популярным.

На самом деле шифровальщики - это индустрия с оборотами в миллиарды долларов. По оценкам, только один образец шифровальщика, Cryptowall 3.0, в 2015 году принес преступникам доход свыше 325 млн. долларов США и только от жертв из США.

Между прочим, увеличенное число вариантов в сочетании с новыми постоянно появляющимися образцами ransomware затрудняет их обнаружение традиционными антивирусами, основанными на сигнатурах.

Вот почему крайне важно иметь передовое решение безопасности, которое обнаруживает и защищает Ваш компьютер от направленных атак, угроз "нулевого дня" и новых версий шифровальщиков.

Что относится к вредоносным программам и какие основные их типы?

К ним относится любая вредоносная программа или IT-код, предназначенные для проникновения в сети или на компьютеры для причинения ущерба, шпионажа и кражи информации. Самые опасные типы вредоносных программ:

RANSOMWARE (ШИФРОВАЛЬЩИКИ)

Блокируют ПК, перехватывая контроль пользователя, шифруют файлы и требуют выкуп за доступ к ним.

ЭКСПЛОЙТ

Используют брешь безопасности или уязвимость в коммуникационных протоколах для проникновения на Ваш ПК.

ШПИОНЫ

Собирают данные доступа, имена пользователей и пароли, другую информацию о Вашей компании.

ФИШИНГ

Создает ложные адреса сайтов для получения Ваших персональных и регистрационных данных, часто с целью кражи денег с Вашего банковского счета.

ТРОЯН

Устанавливает различные приложения, чтобы хакеры могли контролировать компьютер. Они контролируют Ваши файлы и осуществляют кражу Вашей конфиденциальной информации.

APT (ПОСТОЯННЫЕ УГРОЗЫ ПОВЫШЕННОЙ СЛОЖНОСТИ)

Это компьютерный процесс, который пронизывает Вашу систему безопасности для ее контроля и мониторинга, чтобы иметь возможность постоянно извлекать информацию для коммерческих или политических целей.

МОШЕННИЧЕСТВО

Обман с помощью ложных промо-акций (например, лотереи), которые просят от Вас денег за доступ к "призу".

БЭКДОР

Открывает “заднюю дверь” для получения контроля над Вашей системой.

КЕЙЛОГГЕР

Собирает и отправляет все нажатия клавиш пользователя.

БОТ

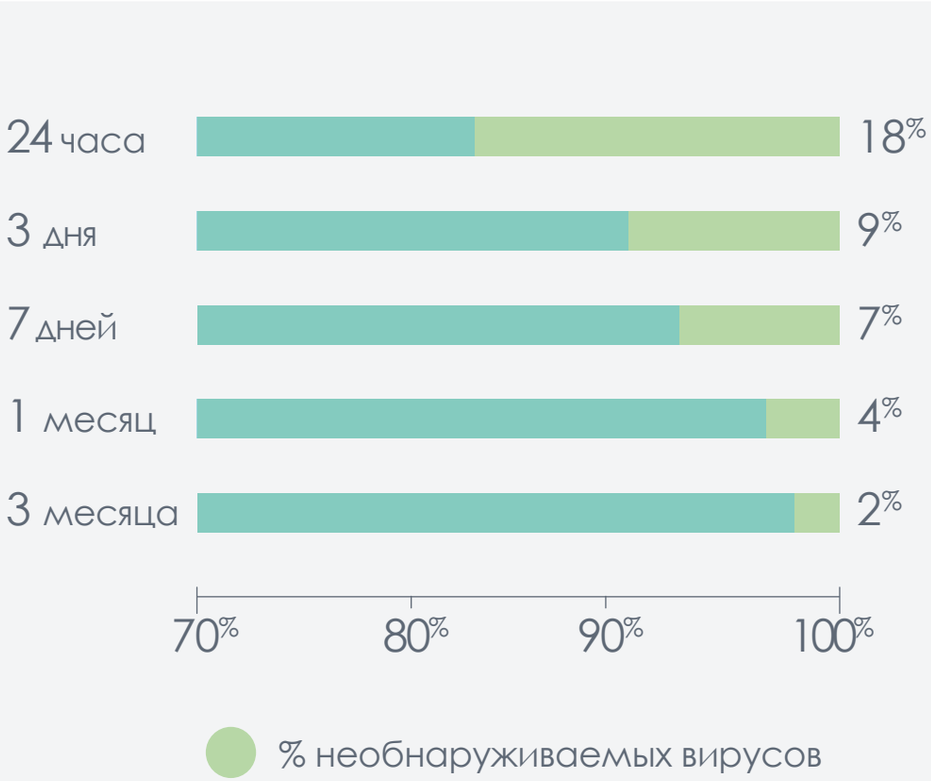
Программа, которая удаленно контролирует Ваш ПК.

ЧЕРВЬ

Заражает все Ваши компьютеры, замедляя работу сети и даже блокируя доступ к коммуникациям.

Эволюция вредоносных программ: сложность и изощренность.

Технологии, используемые традиционными антивирусами (сигнатуры, эвристика), реактивны. **18% новых угроз не обнаруживаются традиционными антивирусами в первые 24 часа, а 2% оставались таковыми и спустя 3 месяца**.



Могут ли эти антивирусы остановить сложные угрозы?

Антивирус не может этого сделать. Существуют сайты, где Вы можете увидеть, обнаруживается ли конкретная вредоносная программа антивирусом. **Хакеры запускают свой вредоносный код после того, как они убедились, что он не обнаруживается антивирусами**.

5 рекомендаций Panda Security для предотвращения кибер-атак

1

Ваши сотрудники должны быть в курсе

Убедитесь, что Ваши сотрудники знают о рисках фишинга, о недопустимости скачивания неизвестных программ (или тех, что не были предложены в компании), а также запрете на посещение сайтов, не вызывающих доверие.

2

Будьте осторожны с Интернетом

Установите политики работы в Интернете, способные контролировать репутацию веб-сайтов, которые могут быть доступны.

3

Решение для Ваших потребностей

Убедитесь, что у Вас есть решение безопасности, в котором нуждается Ваша компания, и оно обновляется.

Решение с различными уровнями безопасности, которое способно обнаруживать и блокировать сложные угрозы.

4

Разработайте внутренние протоколы

Установите протоколы и меры безопасности для контроля установки и запуска любых программ. Вам также следует регулярно осуществлять инвентаризацию Ваших приложений.

5

Обновляйте Ваши системы и приложения

Определите политику для обновления Ваших приложений и их блокировки или удаления, если в них нет потребности для предприятия.

Очень важно защититься от приложений, которые могут иметь уязвимости или дыры безопасности, используемые кибер-преступниками, даже если такие приложения являются летитимными (например, Java, Office, Chrome, Mozilla или Adobe).

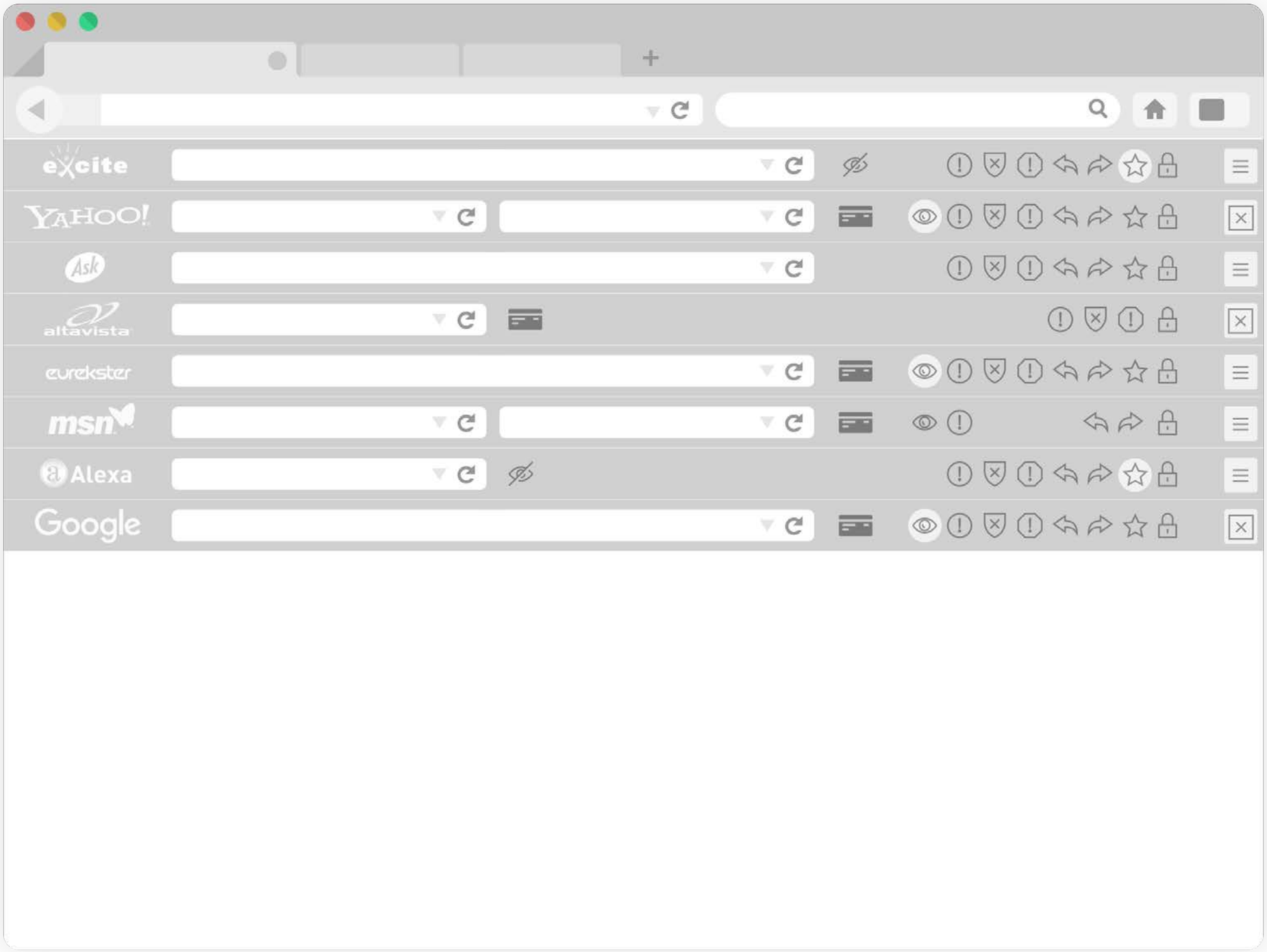


Рисунок: Тулбары представляют серьезный риск безопасности.

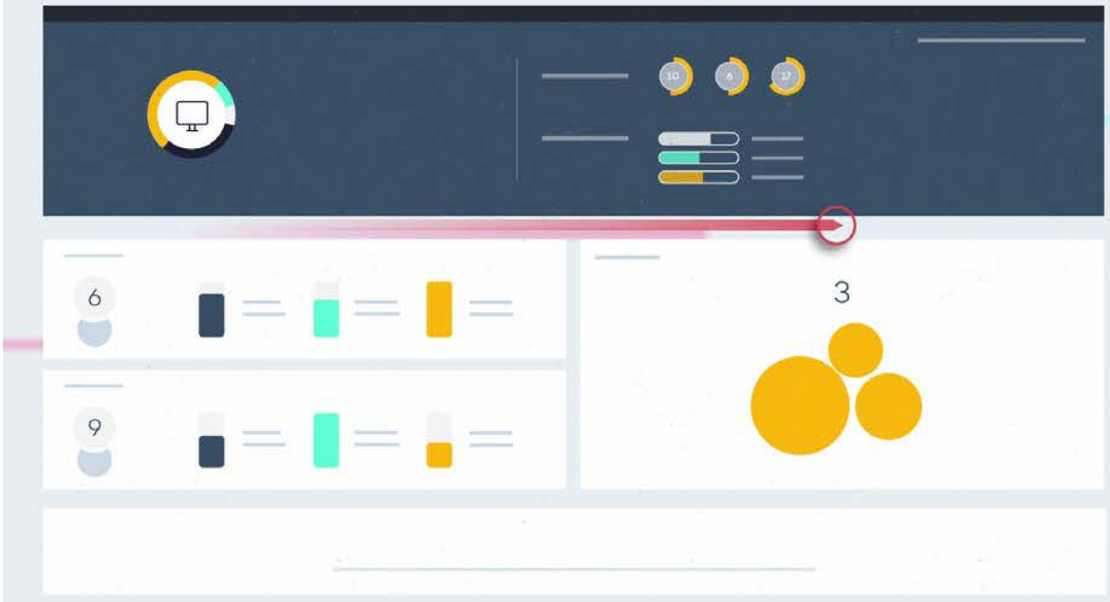
Как Вы можете реально защитить Вашу компанию?

Panda Security разработала первое решение, которое гарантирует непрерывный мониторинг 100% активных процессов.

Panda Security разработала единственное решение кибер-безопасности, которое способно защитить Вашу компанию от направленных атак, угроз "нулевого дня" и других типов сложных угроз, включая шифровальщики.

Это первый продукт на рынке, который гарантирует полноценную защиту компьютеров и серверов благодаря нерерывному мониторингу 100% процессов на конечных точках.

Adaptive Defense 360

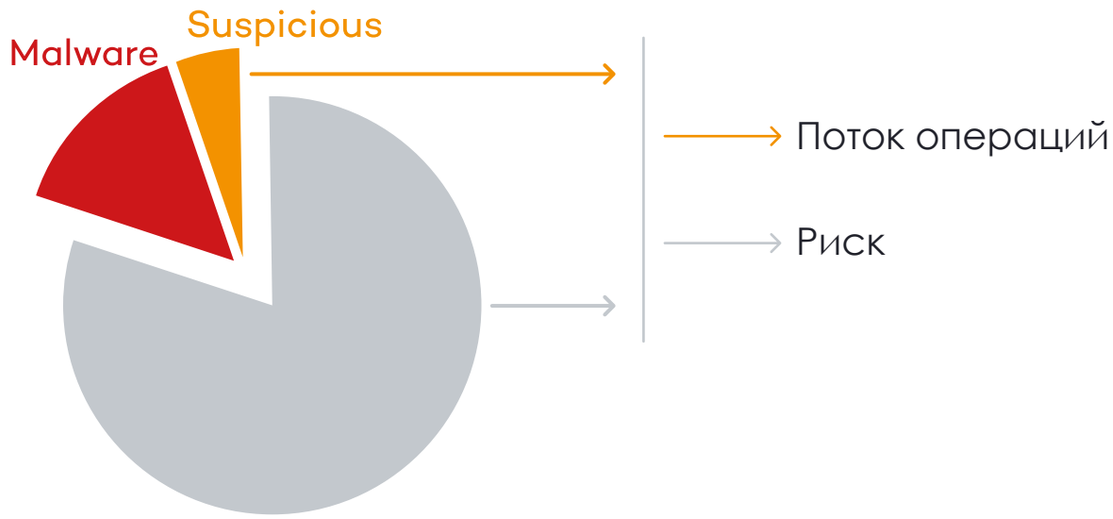


Adaptive Defense 360 предлагает максимально доступные уровни безопасности, превышающие возможности любых антивирусов, представленных на рынке.

Adaptive Defense 360 отслеживает, регистрирует и классифицирует 100% запущенных приложений, что в сочетании с функциями EDR позволяет нам обнаруживать и блокировать вредоносные программы, которые другие системы защиты даже не видят.

Традиционные антивирусы

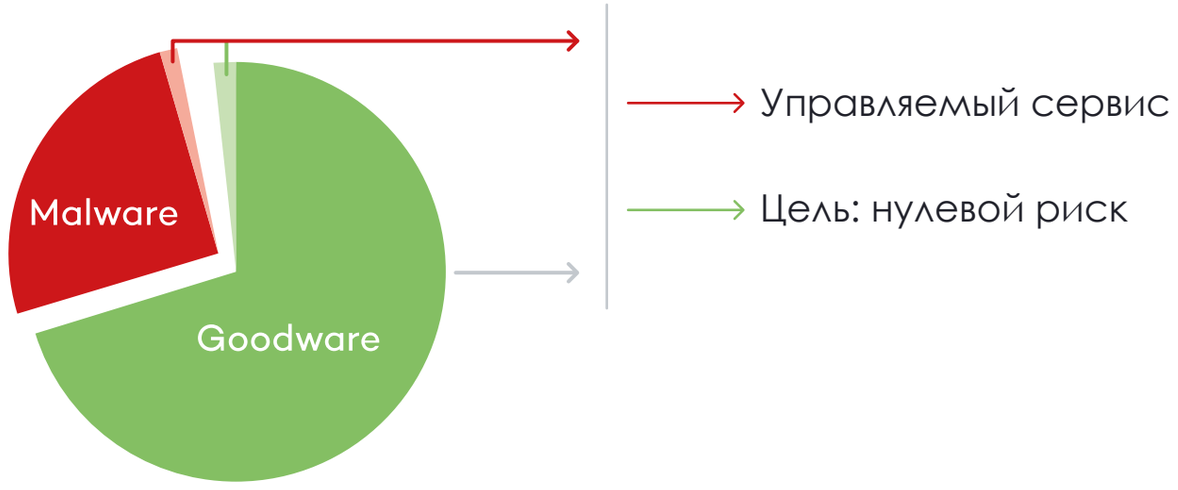
Они только распознают вредоносные программы, но не более.



Т.к. они не могут классифицировать что-либо подозрительное, такие атаки представляют огромную проблему безопасности для традиционных антивирусов (особенно со стороны направленных атак и угроз "нулевого дня").

Adaptive Defense 360

Отслеживает абсолютно все активные процессы.



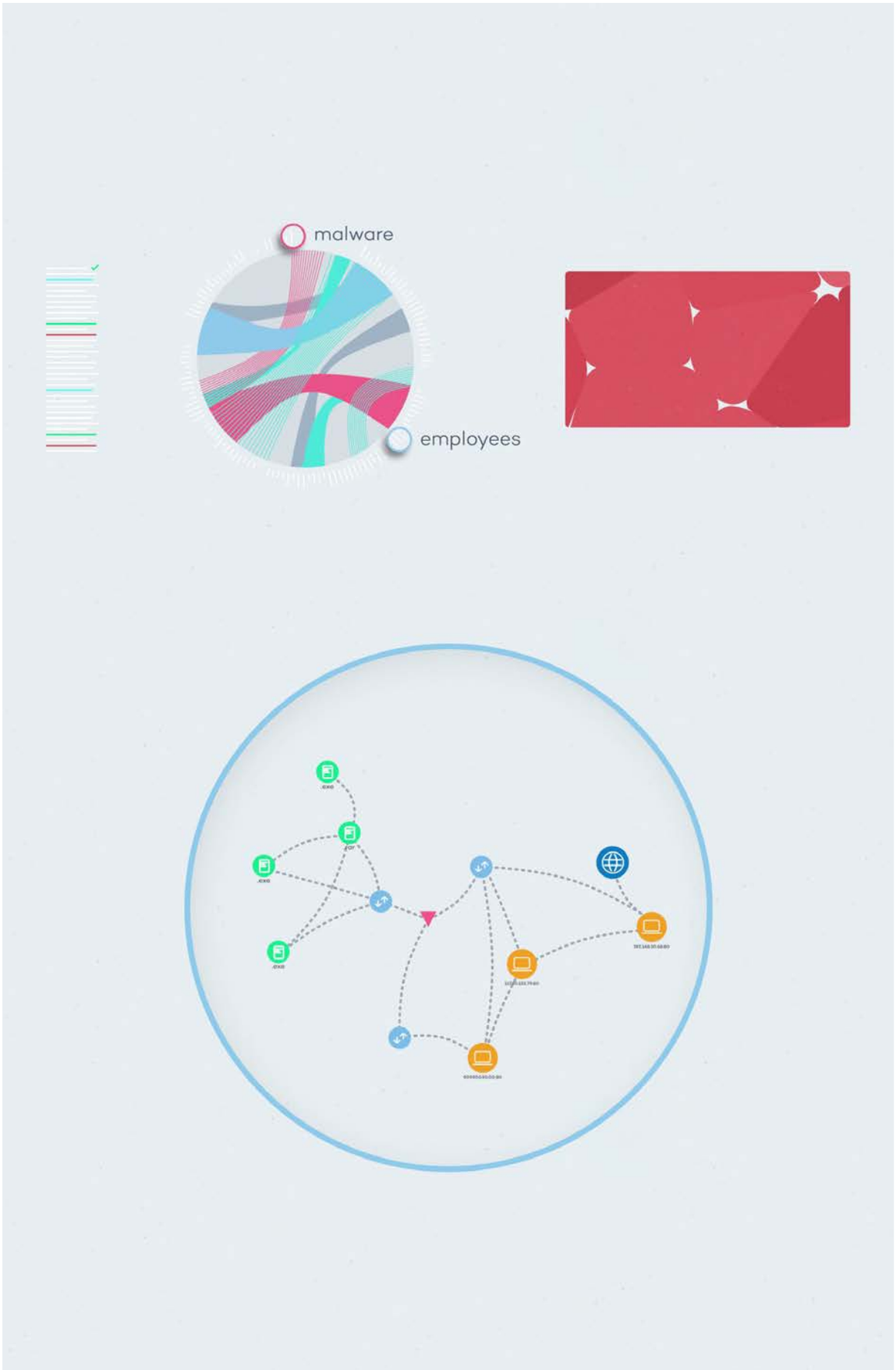
Adaptive Defense 360 точно знает, является ли процесс вредоносным или нет. Он классифицирует абсолютно все, чтобы не было ничего подозрительного.

Способность контролировать все, что происходит на Ваших компьютерах, позволяет Вам:

Обнаруживать утечку информации в результате действия вредоносной программы или сотрудников предприятия в отношении любого файла с данными (pdf, word, excel, txt,...).

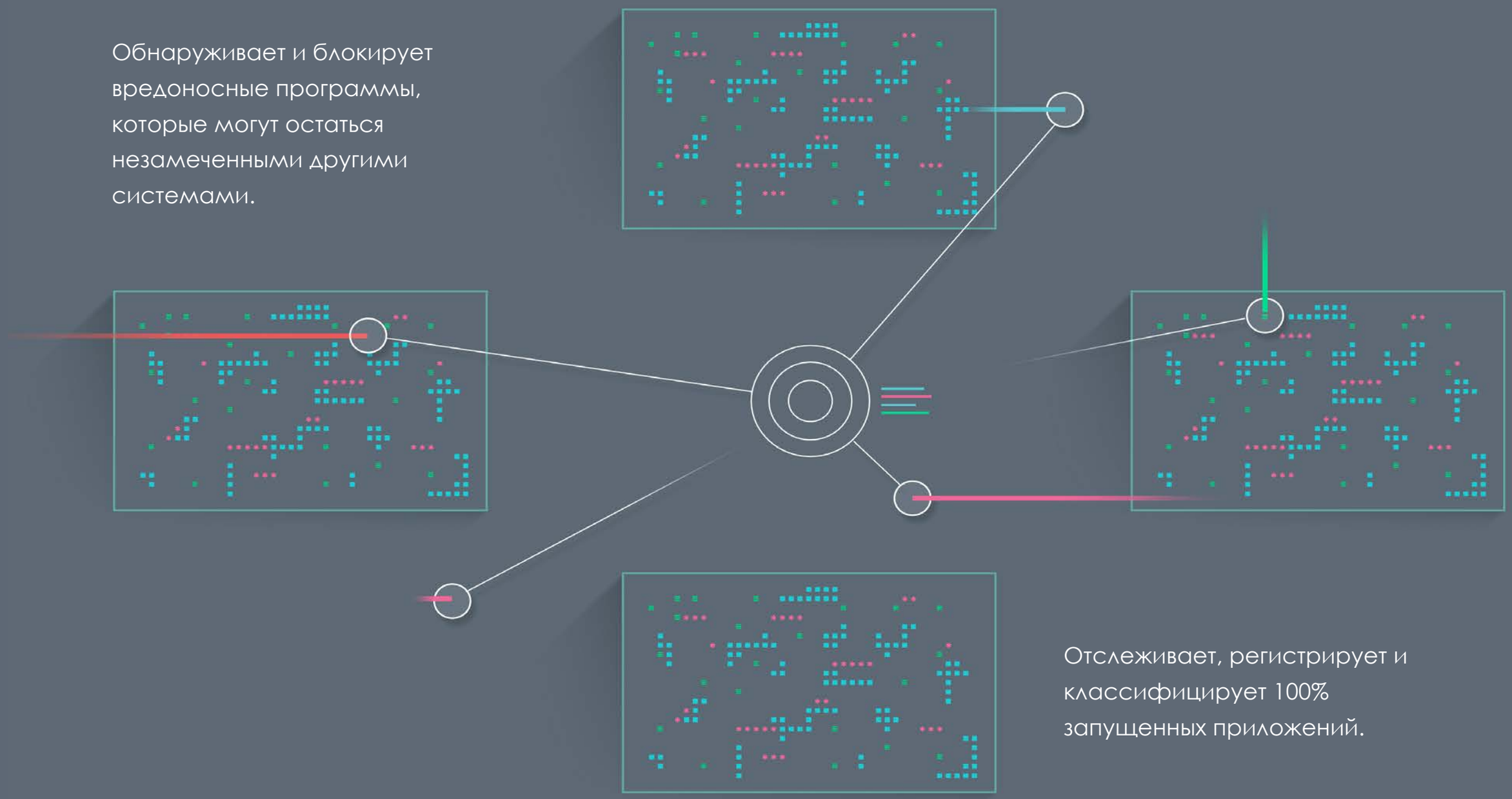
Обнаруживать и закрывать уязвимости в Ваших системах и приложениях, и предотвращать использование нежелательных программ.

Обнаруживать атаки, направленные непосредственно на Ваши системы.



Неограниченная видимость, абсолютный контроль

Обнаруживает и блокирует вредоносные программы, которые могут остаться незамеченными другими системами.



Отслеживает, регистрирует и классифицирует 100% запущенных приложений.

Adaptive Defense 360 в числах

500K

Защищает свыше 500 000 компьютеров и серверов в мире.

1.5M

Классифицировано свыше 1,5 миллиардов приложений.

1,1M

Отразил свыше 1 100 000 нарушений безопасности в 2015 году.

550K

Сэкономлено свыше 550 000 часов IT-ресурсов, что означает примерную экономию в 34,8 миллионов евро.

100%

Обнаружил вредоносные программы в 100% сетей, где он был установлен, независимо от наличия механизмов защиты.

Данные за 2015 г.

Более того, решение опирается на **25-летний опыт компании Panda Security**, что делает нас пионером в обнаружении вредоносных программ и внедрении инновационных решений безопасности.

Не говоря уже о том, что **свыше 30 миллионов конечных точек в мире уже защищены решениями Panda.**

Свяжитесь с нами для получения дополнительной информации

РОССИЯ

+7 495 105 94 51
sales@rus.pandasecurity.com