websense®

# ПЯТЬ НЕОБХОДИМЫХ ВЕЩЕЙ ДЛЯ ЗАЩИТЫ

# ОТ **ПОСТОЯННЫХ УГРОЗ ПОВЫШЕННОЙ СЛОЖНОСТИ (APT)**

websense
TRITON®

# ПЯТЬ НЕОБХОДИМЫХ ВЕЩЕЙ ДЛЯ ЗАЩИТЫ ОТ **ПОСТОЯННЫХ УГРОЗ ПОВЫШЕННОЙ СЛОЖНОСТИ (APT)**

Постоянные угрозы повышенной сложности (англ. advanced persistent threat, APT) стали одной из основных проблем для ИТ-специалистов по безопасности во всем мире. В последнее время атакам подвергалось множество различных компаний. В этой статье описывается характер рисков, связанных с APT, и даются рекомендации по более надежной защите организаций. В частности, настоящая статья:

- дает практическое понятие об APT для профессионалов информационной безопасности;
- раскрывает наиболее эффективную стратегию и тактику защиты от APT;
- описывает уникальные средства Websense для защиты от APT.

## ОБЗОР

Термин APT первоначально относился к краже данных государствами или причинение ими вреда другим государствам для получения стратегической выгоды. Затем понятие было расширено вендорами безопасности и СМИ, и теперь оно охватывает случаи кражи данных злоумышленниками у предприятий с целью получения прибыли. Посредством APT злоумышленники пытаются получить данные о клиентах, инженерную документацию, дорожные карты, исходные коды и другую конфиденциальную информацию.

С практической точки зрения специалистам в сфере ИБ следует понимать, что злоумышленники бизнес-уровня используют для кражи данных у предприятий те же техники, которые ранее использовались на высшем уровне межгосударственного шпионажа.

### НИЖЕ ПРИВЕДЕН ЧАСТИЧНЫЙ ПЕРЕЧЕНЬ APT-АТАК.

- **Атаки на финансовый сектор.** В сентябре 2013 года финансовые учреждения FOREX на Ближнем Востоке, в Пакистане и Непале подверглись атаке в виде нацеленной рассылки вредоносных электронных сообщений. Электронные сообщения содержали ZIP-вложения с исполняемыми файлами. Дополнительные сведения см. в блоге Websense Security Labs™.

- **Атаки на новостные агентства.** В начале 2013 года издания The New York Times и Wall Street Journal сообщили об изощренных кибератаках, в которых использовалось сочетание направленного фишинг-мошенничества и 45 экземпляров специального вредоносного ПО. Щелкните здесь для получения дополнительных сведений.

- **Атаки на предприятия различных отраслей.** В блоге Websense Security Labs в феврале 2013 года было отмечено, что с 2011 года против предприятий всех основных отраслей было зафиксировано более 2000 уникальных атак APT1 (определенное семейство угроз). В публикации также была показана неэффективность традиционных (основанных на сигнатурах) средств защиты против APT.

- **Направленные атаки ставят под вопрос безопасность т.н. надежных доменных имен. В августе 2013 года мир узнал об атаках типа waterholing, использующих техники APT:** сперва компрометируются вполне надежные Интернет-сервисы, которые затем поражают вредоносным ПО пользователей только определенного профиля, устанавливая программы для хищения данных. Щелкните здесь для получения дополнительных сведений.

Список примеров бесконечен. Суть в том, что как на уровне государства, так и на уровне бизнеса специалисты ИБ должны четко понимать методики атак повышенной сложности и способы противодействия им. Традиционные средства защиты при этом зачастую неэффективны.

## ХАРАКТЕРИСТИКИ ПОСТОЯННЫХ УГРОЗ ПОВЫШЕННОЙ СЛОЖНОСТИ

**Направленность**

Угрозы APT нацелены на конкретные организации с целью кражи конкретных данных или нанесения определенного урона.

**Постоянство**

APT-угрозы реализуются в несколько этапов в течение длительного периода времени. До момента фактической атаки злоумышленники знают только жертву и преследуемую цель. Чтобы похитить данные, злоумышленнику требуется выявить уязвимости, оценить существующие меры безопасности, получить доверенный доступ к привилегированным хостам целевой сети, найти нужные данные и, наконец, извлечь данные из сети. Весь процесс может занимать несколько месяцев или даже лет.

**Неуловимость**

Инструменты APT систематически перестраиваются с целью обхода традиционных средств безопасности, на которые большинство организаций полагаются в течение многих лет.

**Сложность**

В основе APT-угроз — сложный набор методик атаки, нацеленных на различные уязвимости внутри организации. Например, APT могут использовать: социальную инженерию по телефону для выявления нужных людей в организации; отправку этим людям поддельных сообщений по email со ссылками на сайт со специальными кодами JavaScript для установки программы-шпиона; командную машину для управления шпионом (либо специально сделанная, либо собранная из доступных комплектов вредоносных утилит); а также особые технологии шифрования.

# ПРОЦЕСС APT СООТВЕТСТВУЕТ СЕМИЭТАПНОЙ МОДЕЛИ АТАКИ

APT, как и прочие сложные угрозы, реализуются в виде серий нападений, разделенных на семь этапов. Не во всех угрозах обязательно присутствует каждый этап. Кроме того, возможны переходы на предыдущие этапы, что существенно расширяет семиэтапный процесс. Это позволяет киберпреступникам создавать и проводить атаки на протяжении длительного периода сотнями и даже тысячами различных способов.

## Этап 1: разведка

На этапе РАЗВЕДКИ киберпреступники изучают своих предполагаемых жертв, используя все виды социальных сетей. Злоумышленники ищут информацию, помогающую им создать благонадежные с виду «приманки», содержащие ссылки на взломанные сайты, находящиеся под их контролем. Иногда в качестве приманки используется информация о недавних стихийных бедствиях, общественных скандалах или о смерти знаменитостей, то есть приманки опираются на человеческое любопытство.

## Этап 2: приманка

Используя информацию, собранную на этапе разведки, киберпреступники создают безобидные на вид приманки, которые могут мотивировать пользователя перейдти по ссылке, ведущую на взломанный веб-сайт. Приманки распространяются по электронной почте, через публикации в социальных сетях или через иное содержимое, которое, как кажется пользователю, поступает из надежных источников.

## Этап 3: перенаправление

В приманках злоумышленники используют ссылки, которые перенаправляют пользователей к безопасно выглядящим или скрытым веб-страницам с наборами эксплойтов, отдельными вредоносными кодами или обфусцированными сценариями. При перенаправлении выполняется анализ целевой системы или же пользователю предлагается обновить программное обеспечение.

## Этап 4: набор эксплойтов

После того как пользователь перейдет по ссылке на вредоносный сайт, программное обеспечение, называемое набором эксплойтов, сканирует систему жертвы с целью поиска открытых уязвимостей или угроз «нулевого дня». Эти бреши — открытая дверь для доставки вредоносных программ, клавиатурных шпионов и других современных инструментов, которые позволяют злоумышленникам глубже проникнуть в сеть.

## Этап 5: файл-инъекция

После того как набор эксплойтов найдет путь для доставки вредоносного ПО, злоумышленник передает файл-инъекцию (как правило, с другого взломанного сервера), чтобы заразить систему жертвы. Инъекция содержит ПО, исполняемое на системе жертвы для запуска поиска и извлечения ценных данных. Некоторые инъекции не активизируются в течение недели, чтобы избежать обнаружения, и содержат загрузчики, которые через какое-то время привносят в систему вредоносное ПО.

## Этап 6: соединение с сервером злоумышленников

После заражения целевой системы инъекция совершает «звонок домой» на управляющий сервер для загрузки дополнительных программ, инструментов или инструкций. Это первый момент, когда устанавливается прямое соединение между злоумышленником и зараженной системой.

## Этап 7: хищение данных

Конечная фаза большинства современных атак — этап хищения данных — завершает серию нападений. Киберпреступники похищают интеллектуальную собственность, личную информацию и другие ценные данные для получения финансовой выгоды или для использования в других атаках.

**Дополнительные сведения о семи этапах см. на сайте** **http://www.websense.com/sevenstages**

## ТРЕБОВАНИЯ К ЗАЩИТЕ ПРОТИВ APT

Проанализировав вышеприведенные характеристики APT, можно описать ключевые требования к эффективному решению для обеспечения безопасности.

- **Учет характера содержимого.** Так как APT постоянно прорывают оборону сетевых экранов, встраивая эксплойты в содержимое, которое переносится через разрешенные протоколы, то в решениях для защиты от APT требуется тщательный учет характера содержимого на всех семи этапах серии нападений.

- **Учет контекста.** Поскольку в большинстве APT используется специально разработанный код или целевые атаки на уязвимости «нулевого дня», ни одна система предотвращения вторжений или антивирус на базе сигнатур не смогут точно определить угрозу. В отсутствие точных сигнатур атак необходимо опираться на менее конкретные признаки. Одного подозрительного признака недостаточно, чтобы идентифицировать атаку, однако если оценивать каждый из них в контексте других признаков, можно собрать достаточно доказательств, чтобы надежно идентифицировать вредоносную активность.

- **Учет данных.** Учет данных. Хотя организации никогда точно не знают, к какому виду относятся отдельные APT (все они уникальны), большинство организаций могут определить свои собственные конфиденциальные данные. Поэтому в качестве уровня защиты для этапа 7 (см. выше) можно применить технологию предотвращения утечки данных (DLP) с целью определения конфиденциальных данных и запрета исходящей передачи этих данных. Также для защиты против APT важно обнаружение специальных видов шифрования исходящего интернет-трафика.

## СТРАТЕГИИ УЛУЧШЕНИЯ ЗАЩИТЫ ПРОТИВ APT

В большинстве современных организаций основная часть бюджета, выделяемого на ИТ-безопасность, расходуется на антивирусные программы, сетевые экраны, системы обнаружения и предотвращения вторжений. Однако в новостях то и дело появляются истории о целевых атаках — в том числе APT-типа, — которым такие средства защиты не страшны. Против современных угроз традиционные меры безопасности не работают. Пока не будут внедрены новые принципы безопасности, еще немало атак на основе методов APT успешно поразят свои цели. Но традиционные средства защиты, такие как сетевые экраны и антивирусные программы, все же необходимы, так как они блокируют известные направления угроз. Впрочем, одних их недостаточно, и следует всегда помнить об ограниченности таких методов защиты и при необходимости их корректировать.

Для грамотной защиты от APT необходимо контролировать входящий и исходящий трафик с учетом характера содержимого, контекста и данных; причем как для электронной почты, так и для веб-коммуникаций. В частности, защитная система должна контролировать исходящую из сети информацию для обнаружения признаков, характерных для кражи данных. Вот несколько возможных признаков вредоносной активности, которые встречаются в исходящей из сети информации: трафик к центрам управления ботнетов; запросы к динамическим DNS-хостам; запросы известных неблагонадежных веб-сайтов; передача конфиденциальных файлов, которые никогда не должны отправляться за пределы организации (например, база данных SAM), а также использование специальных видов шифрования.

Исследуя передовой опыт по  минимизации угроз APT, аналитики отмечают, что комплексная стратегия для борьбы и предотвращения APT должна распространяться на сети, краевые устройства, рабочие места и средства защиты данных. Иными словами, стратегия должна включать в себя правильное сочетание технологий, а именно безопасные веб-шлюзы с аналитикой реального времени и DLP-технологией, а также решения для мониторинга угроз с наличием изолированной среды анализа («песочницы») и возможностью создания экспертных отчетов.

- Безопасные веб-шлюзы являются краеугольным камнем эффективной защиты против угроз повышенной сложности и кражи данных. Они анализируют весь входящий и исходящий трафик (в том числе SSL).

- Решения для мониторинга угроз, которые иногда называются системами обнаружения брешей (BDS), также являются важным компонентом в борьбе с APT. Эти службы предоставляют специалистам по безопасности ценную информацию об уровнях угрозы и о поведении вредоносных программ, а также обеспечивают полноценный экспертный анализ с легкой для чтения отчетностью. Надежное решение для мониторинга угроз предоставляет ИТ-отделам знания и инструменты, позволяющие снизить воздействие угроз на сети.

# ПЯТЬ НЕОБХОДИМЫХ ВЕЩЕЙ ДЛЯ ЗАЩИТЫ ОТ **ПОСТОЯННЫХ УГРОЗ ПОВЫШЕННОЙ СЛОЖНОСТИ (APT)**

**ДЛЯ ЭФФЕКТИВНОЙ ЗАЩИТЫ ОТ ПОСТОЯННЫХ УГРОЗ ПОВЫШЕННОЙ СЛОЖНОСТИ РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДОЛЖНЫ ОБЛАДАТЬ ПЯТЬЮ СЛЕДУЮЩИМИ ФУНКЦИЯМИ.**

1. **Анализ угроз в реальном времени**

   Традиционные средства защиты опираются на сигнатуры, что делает их в значительной степени неэффективными для борьбы с современными угрозами повышенной сложности. Для защиты от целевого фишинг-мошенничества, наборов эксплойтов, динамического перенаправления и аналогичных компонентов APT-атаки необходимо проводить дополнительный анализ в реальном времени и оценивать трафик по степени риска.

2. **Получение данных о глобальных угрозах**

   Любое решение для обеспечения безопасности может извлечь существенную пользу из крупной сети, содержащей информацию об обнаружения угроз. Чем крупнее сеть, тем больше осведомленность решения об угрозах и выше его возможности защиты.

3. **Возможности предотвращения утечек данных (DLP)**

   Конечной целью APT является кража данных. Учитывая сложность APT, крайне важно не только защищаться от угроз, которые могут содержаться в исходящем трафике, но и иметь в распоряжении передовые технологии, обнаруживающие кражи данных в исходящем трафике. Одного сопоставления с шаблонами недостаточно — скорее, требуется развернуть DLP-решение, полностью учитывающее контекст, чтобы защитить конфиденциальные данные от просачивания наружу.

4. **Исполнение в изолированной среде**

   Кибербезопасность стала практической проблемой для ИТ-специалистов и экспертов по безопасности. Решающее значение приобрели эффективная отчетность и анализ в отношении вредоносных программ и угроз повышенной сложности. Чтобы лучше защитить ресурсы своих компаний, специалистам по безопасности требуется понимание того, как ведут себя вредоносные программы и как они влияют на их сети. Такую возможность обеспечивает хорошее решение для исполнения файлов в изолированной среде.

5. **Экспертные отчеты и отчеты о поведении угроз**

   Рука об руку с развертыванием любого решения для безопасности идет необходимость в качественных экспертных отчетах и отчетах о поведении угроз. Ключевым компонентом любого решения для безопасности являются отчеты, позволяющие принимать необходимые меры. Они содержат ценную информацию о поведении угроз, их опасном воздействии, а также экспертные сведения. Чем больше информации для принятия мер дает отчет, тем полезнее он для ИТ-специалиста или эксперта по безопасности.

## РЕШЕНИЯ WEBSENSE ДЛЯ ЗАЩИТЫ ОТ APT

Websense предлагает полный набор продуктов, которые обеспечивают тщательную защиту от APT и других угроз повышенной сложности. Портфель продуктов состоит из следующих групп продуктов.

- **Продукты для защиты.** Продукты Websense TRITON® включают в себя решения на основе прокси-шлюзов для защиты веб-трафика, электронной почты, конфиденциальных данных и мобильных устройств. Все они обеспечивают следующее:
  - **Обнаружение и защита от угроз повышенной сложности в реальном времени.** Подсистема Websense ACE (Advanced Classification Engine) использует семь областей оценки защиты и более чем 10 000 аналитических единиц . Она проводит анализ угроз интернет-трафика в режиме реального времени.
  - **Получение данных о глобальных угрозах.** Сеть Websense ThreatSeeker® Intelligence Cloud объединяет более 900 млн рабочих мест и анализирует 3–5 млрд запросов в день, обеспечивая получение данных о глобальных угрозах и предоставляя жизненно важные аналитические материалы для ACE.
  - **Обнаружение краж и утечек данных.** DLP-средства Websense обнаруживают и блокируют утечку данных для зарегистрированных и описанных данных. В число передовых функций Websense DLP входит оптическое распознавание текста в изображениях, поддержка геолокационных сведений, обнаружение отправки зашифрованных файлов, а также обнаружение кражи паролей и медленных утечек данных.
- **Решение для анализа файлов в изолированной среде.** Websense TRITON ThreatScope™ обеспечивает непревзойденные возможности исполнения файлов в изолированной среде и их анализа. Это позволяет специалистам по безопасности изучать вредоносное ПО, содержащееся в файлах и на веб-сайтах, с учетом его поведения. (См. приложение A.)
- **Решения для мониторинга угроз.** Websense TRITON RiskVision™ — это полное решение для мониторинга угроз, гарантирующее эффективное обнаружение угроз самой высокой сложности (включая APT) и попыток кражи данных. Экспертные отчеты и отчеты о поведении угроз предоставляют специалистам по безопасности необходимые данные для принятия мер по снижению рисков, связанных с угрозами.

# ПРИЛОЖЕНИЕ А. ИЗОЛИРОВАННАЯ СРЕДА, УЧИТЫВАЮЩАЯ ПОВЕДЕНИЕ УГРОЗ

## Изолированная среда Websense, учитывающая поведение угроз, гарантирует непревзойденные возможности анализа в реальном времени

Защита от сегодняшних целевых атак повышенной сложности требует гораздо более тщательного подхода к безопасности, чем даже пару лет назад. Компания Gartner Inc. рекомендует «использовать комплексный подход, так как ни одна технология не остановит целевые атаки повышенной сложности в одиночку»1. Такой подход включает в себя защиту веб и почтового трафика с помощью различных признанных и новых технологий, включая исполнение в изолированной среде («песочнице»).

О «песочницах» в последнее время говорят все чаще, так как они позволяют осуществлять мониторинг активности вредоносного ПО в виртуальной среде, полностью отделенной от пользовательских сетей. Позволяя специалисту по безопасности увидеть, какие вредоносные изменения происходят в виртуальной среде, «песочница» снабжает его информацией, необходимой для лучшего понимания характера угрозы.

Однако не все решения для исполнения файлов в изолированной среде одинаково эффективны. Многие из них продолжают использовать статические списки, содержащие известные вредоносные действия в отношении системы и признаки вредоносного обмена данными (либо подобные списки на основе сигнатур). Проблема в том, что вредоносные программы все время меняются и адаптируются. Даже небольшого изменения существующей вредоносной программы достаточно, чтобы она ускользнула от многих традиционных средств защиты.

Отсюда возникает вопрос: как защититься от чего-то, что ранее никто не видел?

Ответ: с помощью изолированной среды, учитывающей поведение угроз. Она в реальном времени соотносит активность вредоносных программ с аналитическими данными о глобальных угрозах, обеспечивая непревзойденную защиту даже от самых сложных угроз.

## Как работает изолированная среда

После получения файла через Интернет или электронную почту «песочница» запускает его в виртуальной среде, которая полностью отделена от всех других сред и сетей. Это позволяет полностью выполнить файл и проконтролировать весь жизненный цикл заражения в изолированной среде. Типовая изолированная среда содержит не только стандартную операционную систему, но и наиболее часто используемые бизнес приложения. От Microsoft Windows до Microsoft Office и Adobe Acrobat Reader — любая изолированная среда эмулирует наиболее типичную бизнес-среду, чтобы сымитировать максимально вероятные цели для вредоносного ПО, тем самым увеличивая вероятность застать его «на месте преступления».

Для мониторинга жизненного цикла заражения вредоносным ПО требуется анализ как действий в системе, так и последующего обмена данными. Действия в системе включают в себя любые изменения, начиная от модификации процессов и файловой системы и заканчивая изменениями в реестре. Поскольку для каждого анализа используется новая виртуальная среда, исполнение файлов в «песочнице» всегда начинается с одной и той же точки, что позволяет при каждом последующем анализе совершенно точно определять изменения. Знание конкретного перечня изменений в системе очень важно для специалистов по безопасности, так как за счет него они могут понять природу вредоносного ПО и устранить заражение.

Не менее важным для понимания действий в системе является мониторинг вредоносного обмена данными. Действия в системе закладывают основу для реального ущерба, обычно путем загрузки дополнительных компонентов или кражи данных. В обоих случаях необходим анализ всех протоколов связи, целевых IP-адресов или хостов, DNS-запросов и типов передаваемых данных.

Отслеживание действий в системе и обмена данными необходимо для понимания полного жизненного цикла заражения — но это всего лишь отправная точка.

1 Gartner, Inc. «Практические рекомендации по снижению опасности угроз повышенной сложности» (Best Practices for Mitigating Advanced Persistent Threats). Авторы: Lawrence Pingree, Neil MacDonald, Peter Firstbrook. 12 сентября 2013 г.

## Изолированная среда, учитывающая поведение угроз, обеспечивает аналитику в реальном времени

Чтобы перейти от обыкновенной изолированной среды к «песочнице», учитывающей поведение угроз, нужно в реальном времени соотносить действия вредоносного ПО с известными подозрительными действиями. Поддержание статического списка известных вредоносных действий по-прежнему ценно для обеспечения немедленного реагирования на вредоносные программы, однако наиболее сложное вредоносное ПО, лежащее в основе самых опасных постоянных угроз повышенной сложности (APT), скорее всего, в такое списке не обнаружить.

Наиболее эффективное распознавание вредоносного ПО, лежащего в основе сложных целевых атак и APT, достигается за счет комплексного анализа, осуществляемого двумя технологиями Websense®: Websense ACE (Advanced Classification Engine) и Websense ThreatSeeker® Intelligence Cloud. Ежедневно анализируя до 5 млрд запросов от 900 млн рабочих мест с применением свыше 10 000 аналитических материалов, компания Websense может соотнести информацию о действиях вредоносного ПО из крупнейшей в мире сети аналитики безопасности с действиями вредоносной программы, отслеживаемой в изолированной среде. И даже во время выполнения вредоносной программы в этой среде технологии Websense продолжают собирать новую информацию и делают ее доступной для сравнения с действиями этой программы.

## Преимущества развертывания изолированной среды в облаке

Многие решения для организации изолированной среды поставляются в виде локального приложения, и это создает определенные проблемы. Во-первых, мощность изолированной среды самоограничивается имеющимися ресурсами. В условиях большого трафика изолированные среды на базе АПК оказываются не в состоянии анализировать все подозрительные действия, и тогда, по мере увеличения их загруженности, приходится отдавать приоритет только наиболее существенным угрозам. С другой стороны, у изолированных сред в облаке нет проблем с мощностью, и они легко масштабируются для мониторинга всех возможных угроз вне зависимости от объемов трафика.

Второй, не менее важной проблемой является обмен информацией между несколькими АПК. Даже при небольшом количестве АПК иногда возникают задержки при обновлении аналитических данных об угрозах. А даже самые короткие задержки могут привести к неправильной классификации вредоносного ПО «нулевого дня», грозящего потенциальным заражением системы. Чтобы решить эту проблему, Websense автоматически распространяет получаемые в реальном времени аналитические данные о глобальных угрозах на все изолированные среды Websense. В результате собираются самые актуальные аналитические данные и обеспечивается самое быстрое обучение, что дает основу для настоящей защиты реального времени против сложных целевых атак и APT.

## Необходимость в экспертной отчетности

Чтобы специалисты по безопасности получали нужную информацию и проводили восстановительные мероприятия, изолированные среды, учитывающие поведение угроз, должны включать функции экспертной отчетности. При этом экспертные отчеты должны быть простыми для понимания и в то же время содержать подробную информацию о вредоносных действиях и обмене данными — иными словами, это должны быть отчеты, опираясь на которые можно принять необходимые меры. Экспертные отчеты в изолированной среде Websense содержат подробную информацию об обнаруженных действиях, изменениях в системе и обмене данными между вредоносным ПО. Они автоматически создаются для всех вредоносных файлов, выявляемых изолированной средой.

## Решения Websense для работы в изолированной среде

**Изолированная среда Websense, учитывающая поведение угроз, доступна в двух инновационных решениях:**

- TRITON ® ThreatScope™ — добавочная служба, предоставляющая дополнительную защиту против самых сложных целевых угроз «нулевого дня» и APT-угроз, которые проникают через электронную почту или веб.

- TRITON ® RiskVision™ — непревзойденное решение для мониторинга угроз, которое обеспечивает оперативный просмотр информации об угрозах повышенной сложности, краже данных и зараженных системах за счет объединения четырех основных средств защиты в одном АПК.

## О КОРПОРАЦИИ WEBSENSE

Websense, Inc. — ведущий поставщик систем информационной безопасности, чьи продукты эффективно защищают организации от новейших видов кибератак и краж данных. Комплексные решения Websense TRITON объединяют в себе средства обеспечения безопасности интернет-трафика, электронной почты и мобильных устройств, а также системы предотвращения утечки данных (DLP). Десятки тысяч организаций доверяют Websense TRITON охрану от непрерывно развивающихся киберугроз, целевых атак и от все более изощренного вредоносного ПО. Решения Websense эффективно предотвращают хищение интеллектуальной собственности и сбои в системах защиты данных, одновременно способствуя внедрению единых стандартов и лучших практических методик обеспечения безопасности. Международная сеть партнеров по распространению позволяет Websense успешно поставлять единые масштабируемые решения Websense TRITON для развертывания на локальных устройствах или в облаке.

**Websense TRITON защищает от большего числа угроз, чем другие системы.**
**Доказательства вы найдете на странице** **www.websense.com/proveit**

---

**Дополнительные сведения: www.websense.com**

**+1 800-723-1166 | info@websense.com**

**TRITON БЛОКИРУЕТ БОЛЬШЕ УГРОЗ.**
**МЫ ГОТОВЫ ЭТО ДОКАЗАТЬ.**