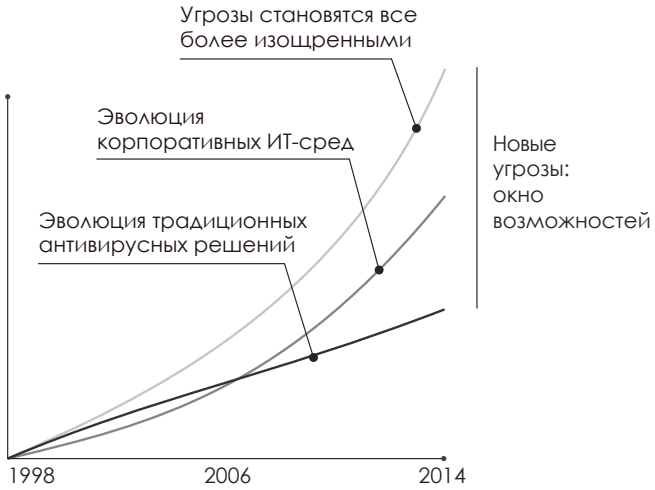
Panda Adaptive Defense

Закройте окно возможностей для сложных и неизвестных угроз

ВЫ ДУМАЕТЕ, ВАША КОМПАНИЯ ЗАЩИЩЕНА ОТ НАПРАВЛЕННЫХ АТАК И УГРОЗ НУЛЕВОГО ДНЯ?

Панорама вредоносного ПО и ИТ-безопасности претерпела серьезные изменения в плане количества и сложности угроз. Наблюдается экспоненциальный рост числа вирусов в обращении (свыше 200 000 новых вирусов появляется ежедневно), а новые техники преодоления защиты и маскировки вредоносных программ позволяют угрозам длительное время оставаться незамеченными в корпоративных сетях.



Одновременно с этим сложнее становятся и ИТ-среды, в результате чего управление становится более сложным, а системы - более уязвимыми.

Но традиционные антивирусы отстают от реальности. В силу своего линейного развития они все еще используют устаревшие методы обнаружения, основанные на сигнатурных файлах и эвристических алгоритмах. В итоге результаты являются неточными, т.е. угроза может оставаться необнаруженной или могут возникать ложные срабатывания.

Такое несоответствие привело к тому, что появилось "**окно возможностей для вредоносных программ**": промежуток времени между появлением нового вируса и выпуском противоядия от него. Увеличивающийся разрыв используется хакерами для заражения корпоративных сетей вирусами, троянами, шифровальщиками и другими типами вредоносных программ. Новые угрозы способны шифровать конфиденциальные документы и требовать выкуп за доступ к ним или просто собирать критически важную информацию в целях промышленного шпионажа.

Правительства, банки и другие крупные организации несут на себе всю тяжесть атак, которые не были вовремя обнаружены традиционными антивирусными решениями. Наш Аналитический департамент проанализировал миллионы вирусных образцов и лучшие антивирусы, представленные на рынке, и выяснил, что 18% угроз остаются необнаруженными в первые 24 часа после их появления, и даже через три месяца эти традиционные решения все еще не способны обнаруживать 2% угроз.

Решение для данной ситуации - это **Panda Adaptive Defense**, который способен точно классифицировать каждое приложение, запущенное в Вашей компании, разрешая запуск только легитимным приложениям.

Чтобы создать такой продукт, мы пять лет работали над **новой моделью безопасности**, основанной на трех принципах: непрерывный мониторинг приложений на компьютерах и серверах компании, автоматическая классификация с использованием техник машинного обучения на нашей облачной платформе Больших данных, и наши технические эксперты, анализирующие те приложения, которые не были классифицированы автоматически, чтобы точно знать поведение всех программ, запущенных на корпоративных системах.

ПРЕДОТВРАЩЕНИЕ
Блокировка приложений и изоляция систем для предотвращения будущих атак

ВИДИМОСТЬ
Отслеживаемость и видимость каждого действия со стороны запущенных приложений

РЕАГИРОВАНИЕ
Экспертная информация для тщательного анализа каждой попытки атаки

ОБНАРУЖЕНИЕ
Направленные атаки и угрозы "нулевого дня" блокируются в реальном времени без сигнатур

ЕДИНСТВЕННОЕ РЕШЕНИЕ, ГАРАНТИРУЮЩЕЕ БЕЗОПАСНОСТЬ ВСЕХ ЗАПУЩЕННЫХ ПРИЛОЖЕНИЙ

ГАРАНТИРОВАННАЯ ПОЛНАЯ И НАДЕЖНАЯ ЗАЩИТА

Panda Adaptive Defense предлагает два режима работы:

- **Стандартный режим** разрешает запуск всех приложений, классифицированных как goodware, а также приложений, которые еще не классифицированы Panda Security и автоматизированными системами.
- **Расширенный режим разрешает** запуск только goodware. Идеальная форма защиты для компаний, которым требуемся "нулевой риск" в плане безопасности.

ЭКСПЕРТНАЯ ИНФОРМАЦИЯ

- **Графики событий** дают четкое представление обо всех событиях, вызванных зловредами.
- Получите визуальную информацию с помощью **тепловых карт** о географии источника вредоносных подключений, созданных файлах и пр.
- Найдите программы с известными уязвимостями, установленные в Вашей сети.

СОВМЕСТИМОСТЬ С ТРАДИЦИОННЫМИ АНТИВИРУСНЫМИ РЕШЕНИЯМИ

Adaptive Defense может параллельно работать с традиционными антивирусными решениями и выполнять роль **корпоративного инструмента, способного блокировать все типы вредоносных программ, включая направленные атаки и угрозы "нулевого дня"**, которые традиционные решения обнаруживать не в состоянии.

ЗАЩИТА ДЛЯ УЯЗВИМЫХ ОПЕРАЦИОННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ

Такие системы как Windows XP, которая больше не поддерживается разработчиком, а потому не обновляется и уязвима, стали "легкой добычей" для угроз "нулевого дня" и атак нового поколения.

Более того, примерно 90% вредоносных программ используют уязвимости в таких приложениях, как Java, Adobe, Microsoft Office и браузерах.

Модуль защиты от уязвимостей в **Adaptive Defense** использует контекстные и поведенческие правила для того, чтобы компании могли работать в безопасной среде, даже если у них есть не обновляемые системы.

НЕПРЕРЫВНАЯ ИНФОРМАЦИЯ О СТАТУСЕ КОРПОРАТИВНОЙ СЕТИ

- Получайте оперативные оповещения в момент идентификации вредоносной программы в сети вместе с подробным отчетом о местоположении угрозы, зараженных компьютерах и действиях, предпринятых вредоносной программой.
- Получайте по электронной почте отчеты о ежедневной работе сервиса.

ДОСТУПНОСТЬ SIEM

Adaptive Defense интегрируется с SIEM-решениями для предоставления подробных данных об активности всех приложений, запущенных в Ваших системах.

Для клиентов без SIEM, **Adaptive Defense** может предложить свою собственную систему хранения и управления событиями безопасности для анализа всей собираемой информации в реальном времени.

100% УПРАВЛЯЕМЫЙ СЕРВИС

Забудьте о необходимости инвестировать в ИТ-персонал, чтобы справляться с карантином, подозрительными файлами или лечить и восстанавливать зараженные компьютеры. **Adaptive Defense** классифицирует все приложения автоматически благодаря машинному обучению в наших системах больших данных под постоянным наблюдением экспертов PandaLabs.

Совместимые решения на платформе Aether:

Panda Adaptive Defense Panda Adaptive Defense 360

Системные требования наших решений безопасности конечных устройств:

Серверы и рабочие станции Windows:
http://go.pandasecurity.com/endpoint-windows/requirements

Устройства с Mac OS:
http://go.pandasecurity.com/endpoint-macos/requirements

Серверы и рабочие станции Linux:
http://go.pandasecurity.com/endpoint-linux/requirements

Устройства с Android:
http://go.pandasecurity.com/endpoint-android/requirements

ОБЛАЧНАЯ ПЛАТФОРМА УПРАВЛЕНИЯ

Aether Platform

Облачная платформа и консоль управления Aether, общая для всех решений Panda для конечных устройств, предлагает оптимальное и улучшенное управление адаптивной безопасностью внутри и за пределами локальной сети. Простота, гибкость, детализация и масштабируемость.

Больше и быстрее. Простое внедрение

- Внедрение, установка и настройка за считанные минуты. Ценность с первого дня.
- Единый легкий агент для всех продуктов и платформ (Windows, Mac, Linux и Android).
- Автоматическое обнаружение незащищенных устройств. Удаленная установка.
- Собственные технологии прокси, репозитория/кэша. Оптимальные коммуникации даже с устройствами без подключения к Интернету.

Простота управления.
Адаптация к Вашей организации

- Интуитивно понятная веб-консоль. Гибкое и модульное управление, снижающее полную стоимость владения.
- Настройка пользователей с различными уровнями видимости и прав. Журнал событий.
- Политики на уровне групп и конечных устройств. Предустановленные и настраиваемые роли.
- Инвентаризация аппаратного и программного обеспечения. Журналы изменений.

Легкое масштабирование возможностей управления и безопасности

- Для внедрения новых модулей не требуется новая инфраструктура. Нет расходов на внедрение.
- Связь с конечными устройствами в реальном времени из единой веб-консоли.
- Панели контроля и индикаторы для каждого модуля.

СЕРТИФИКАТЫ И НАГРАДЫ

Panda Security регулярно принимает участие в тестированиях Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs, где получает награды за производительность и защиту.

Panda Adaptive Defense получил сертификацию EAL2+ при оценке по стандарту общих критериев (Common Criteria).

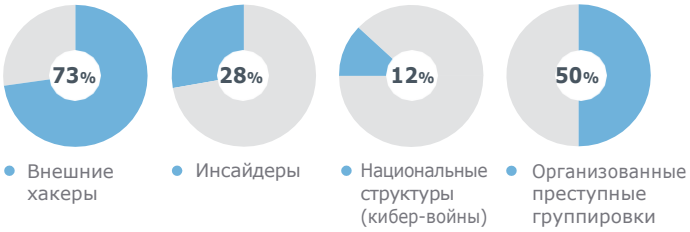
Panda Security получила статус "Visionary" в Магическом квадранте Gartner для платформ по защите конечных устройств (EPP) в 2018 году

Panda Adaptive Defense 360

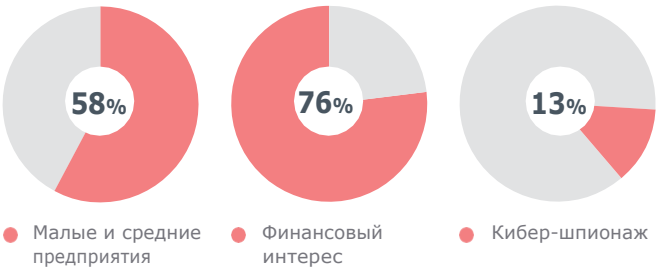
Автоматизированная и централизованная *Расширенная безопасность*
Положите конец кибер-угрозам

КОРПОРАТИВНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Кто стоит за кибер-угрозами?[1]



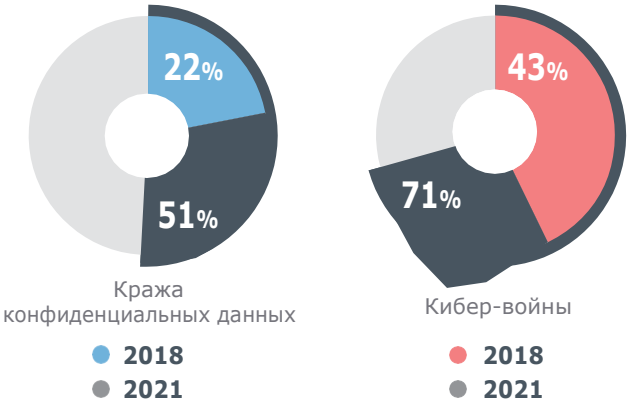
Кто жертвы? Каковы мотивы?[1]



Каков ущерб для компаний?

- **Глобальный ущерб:** 600 млрд. долларов[3]
- **Средний ущерб от нарушения данных:** 3,86 млн. долларов[4]

Компании и высокий риск[3]



В 60% случаев национальные атаки ведут к **кибер-войне**.

Конечные устройства - новый периметр

Мобильность, процессинг и облачные хранилища произвели революцию в корпоративной среде. **Конечные устройства - новый периметр**. Решения безопасности на конечных устройствах должны быть **передовыми, адаптивными и автоматическими**, с высочайшими уровнями предотвращения обнаружения злоумышленников, которым рано или поздно удастся избежать превентивных мер. Такие решения также должны предлагать гибкие инструменты для оперативного реагирования, минимизации ущерба и сокращения поверхности атаки.

Профессионализация хакеров

Враги становятся **изощреннее,** их **количество растет** в результате повышения уровня профессионализма, доступности технологий и постоянных утечек кибер-данных.

Кибер-угрозы следующего поколения разрабатываются так, чтобы оставаться полностью незамеченными для традиционных решений безопасности.

Кибер-оборона в организациях

Хакеры нацеливаются на компьютеры и серверы, где хранятся наиболее ценные активы организаций, и ИТ-службы испытывают большие трудности в их защите. EDR-приложения (Endpoint Detection and Response) сами по себе увеличивают нагрузку, т.к. у них нет полной автоматизации предотвращения, обнаружения, сдерживания и реагирования на угрозы. Повышение уровня безопасности вашей компании без увеличения операционных расходов неизбежно подразумевает автоматизацию безопасности на конечных устройствах.

РЕШЕНИЯ ПО ОБНАРУЖЕНИЮ АТАК НА КОНЕЧНЫЕ УСТРОЙСТВА И РЕАГИРОВАНИЮ НА НИХ (EDR)

EDR-решения отслеживают, регистрируют и сохраняют данные по активности конечных устройств (пользовательские события, процессы, изменения в реестре, использование памяти и сети). Такая видимость вскрывает угрозы, которые иначе остались бы незамеченными.

Какие бывают скрытые проблемы с EDR-решениями?

Для поиска аномалий безопасности в событиях и выдачи соответствующих предупреждений используются различные технологии. Все это требует вмешательства человека. EDR-решения требуют круглосуточного контроля и быстрой реакции высококвалифицированного персонала.

Однако такие ресурсы дороги и их трудно найти. Недостаточно укомплектованные организации с небольшими бюджетами не готовы самостоятельно использовать все преимущества EDR-решений. При внедрении и использовании этих решений сотрудники сталкиваются с высокими нагрузками, вместо того, чтобы получать от них поддержку в главном: повышение уровня безопасности их компаний.

1 "2018 Data Breach Investigation report". Verizon
2 "2018 Economic Impact of Cybercrime — No Slowing Down". CSIC/McAfee
3 "2018 Cost of Data Breach Study: Global Overview". Ponemon Institute/IBM Security
4 "2018 study on global megatrends in cybersecurity". Ponemon Institute

Panda Adaptive Defense 360

Panda Adaptive Defense 360 - это инновационное облачное решение информационной безопасности для ПК, ноутбуков и серверов. Оно **автоматизирует процессы предотвращения, обнаружения, сдерживания и реагирования** на любые существующие или потенциальные сложные атаки, неизвестные угрозы, шифровальщики, фишинг, эксплойты, работающие в памяти, и атаки, не использующие вредоносное ПО, как внутри, так и снаружи корпоративной сети.

Решение отличается от других решений тем, что сочетает в себе широкий спектр **традиционных технологий защиты конечных устройств (EPP) с автоматизированными EDR-возможностями**, благодаря двум сервисам **подуправлением экспертов Panda Security**, предоставляемым как функции решения:

- **Сервис 100% классификации.**
- **Сервис охоты за угрозами Threat Hunting и расследования атак и инцидентов (THIS).**

Благодаря облачной архитектуре **агент очень легок** и не влияет на скорость работы конечных устройств, которые управляются через **единую облачную консоль**, даже когда они не подключены к Интернету.

Panda Adaptive Defense 360 объединяет платформы **облачной защиты** и **управления (Aether)**, что позволяет достичь максимальных уровней предотвращения, обнаружения и автоматического реагирования при минимальных требуемых усилиях.

> AIRBUS
>
> "Предвидение - наш основной союзник при определении будущих потребностей и предотвращении рисков. Adaptive Defense 360 дает нам видимость, которая необходима для достижения этого предвидения".
>
> **Жан-Ив Андреолетти**
> Инженер по системной и сетевой интеграции, проверке и обслуживанию платформы

Panda Adaptive Defense 360 ПРЕИМУЩЕСТВА

Упрощает и минимизирует расходы на расширенную и адаптивную безопасность

- Его управляемые сервисы снижают расходы на экспертов. Нет ложных срабатываний, нет дополнительных обязанностей.
- Управляемые сервисы автоматически обучаются на угрозах. Не требуется время на ручные настройки.
- Максимальное предотвращение на конечных устройствах. Почти нулевые операционные расходы.
- Не требуется устанавливать, настраивать или обслуживать локальную инфраструктуру управления.
- Легкий агент и облачная архитектура - нет влияния на производительность конечных устройств.

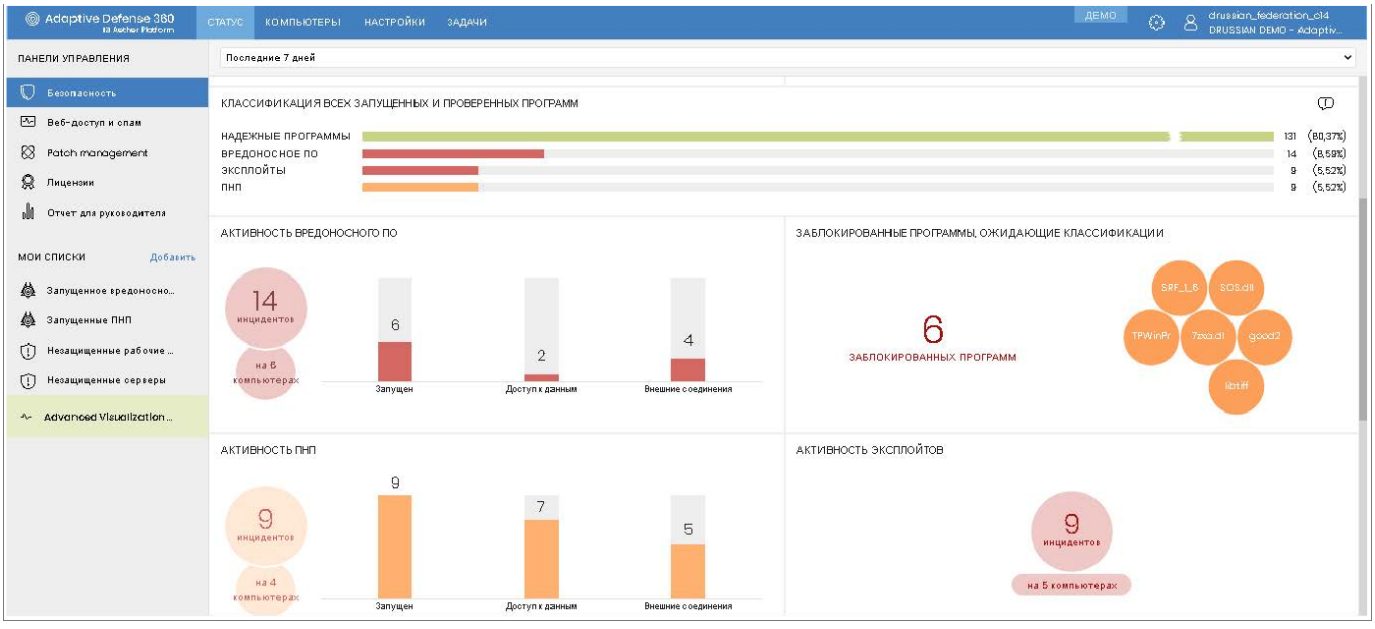
Автоматизирует и сокращает время обнаружения и выявления (Dwell Time)

- Предотвращает запуск угроз, неизестного вредоносного ПО, шифровальщиков и фишинга.
- Обнаруживает и блокирует вредоносную активность в памяти (эксплойты) до того как они могут причинить ущерб.
- Обнаруживает вредоносные процессы, которые невидимы для традиционных превентивных средств.
- Обнаруживает и блокирует хакерские техники и процедуры.

Автоматизирует и сокращает время для анализа и расследования

- Автоматическое и прозрачное восстановление.
- Оперативное восстановление нормальной работы конечного устройства.
- Видимость злоумышленников и понимание их действий, что ускоряет процесс расследования.
- Помогает сократить поверхность атаки. Повышает уровень безопасности.

Рис. 1: Единая панель предоставляет глобальную видимость и консолидированное управление с приоритетами для обнаруженных угроз



Облачная платформа защиты

Люди и машины: расширенная и адаптивная безопасность

Сервис 100% классификации отслеживает и предотвращает запуск вредоносных приложений и процессов на конечных устройствах. Для каждого запуска сервис в реальном времени осуществляет **классификацию (вредоносный или легитимный процесс) без неопределенности**, освобождая клиента от принятия решения. Все это возможно благодаря скорости, высокой производительности, гибкости и масштабируемости искусственного интеллекта и облачных вычислений.

Сервис сочетает **Большие данные** и многоуровневое **Машинное обучение**, включая **глубокое обучение** - результат непрерывного наблюдения и автоматизации **опыта, интеллекта и накопленных знаний экспертов** по безопасности и угрозам в центре расследований Panda Security.

Рис. 2: Рабочий процесс управляемого облачного сервиса классификации.

Управляемый сервис расследований и Threat Hunting управляется командой "охотников за угрозами" с помощью инструментов профилирования, анализа и корреляции событий в реальном времени и ретроспективе для проактивного обнаружения новых методов взлома и сокрытия.

"Охотники за угрозами" действуют исходя из того, что организации находятся в постоянном состоянии взлома.

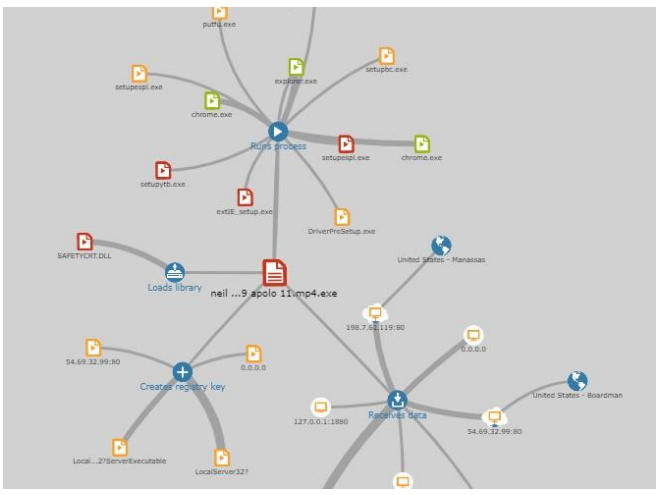


Рис. 3: Временная шкала инцидентов в консоли Panda Adaptive Defense 360 позволяет проводить экспертное расследование: дата первого обнаружения в сети, названия и количество пострадавших конечных устройств, изменения настроек, коммуникации.

Облачная платформа управления: Aether

Комплексная и масштабируемая безопасность следующего поколения, видимость и контроль из облака в режиме реального времени

Платформа Aether и ее облачная консоль, общие для всех корпоративных решений безопасности конечных устройств Panda Security, оптимизируют управление расширенной и адаптивной безопасностью внутри и за пределами сети.

Разработана так, чтобы сотрудники по ИБ могли сосредоточиться исключительно на управлении информационной безопасностью предприятия. Упрощает процессы управления и повышает гибкость, точность и масштабируемость.

ПРЕИМУЩЕСТВА AETHER В Panda Adaptive Defense 360

Делает больше за меньшее время. Простота внедрения - мгновенная видимость

- Внедрение, становка и настройка в считанные минуты. Получение результата с первого дня.
- Очень легкий мультипродуктовый и мультимодульный агент Panda. Поддержка Windows, Mac, Linux, Android.
- *Автоматическое обнаружение незащищенных конечных устройств. Удаленная установка.*
- *Собственная технология прокси, даже для компьютеров без Интернет-подключения.*
- *Оптимизация трафика с помощью собственной технологии репозиторий/кеш.*

Легко использовать, адаптация к Вашей организации

- *Интуитивно понятная веб-консоль. Гибкое и модульное управление.*
- *Предварительно настроенные и собственные роли.*
- *Подробный аудит действий в консоли.*
- *Пользователи с полными или ограниченными правами.*
- *Политики безопасности для групп и конечных устройств.*
- *Инвентаризация ПО и "железа", журнал изменений.*

Облегчает мониторинг. Ускоряет реагирование

- *Приоритетные ключевые индикаторы и панели мониторинга.*
- *Система уведомлений.*
- *Полная история инцидентов: процессы, источник, время обнаружения, распространение и пр.*
- *Действия с конечными устройствами одним кликом: перезагрузка, изоляция, патчи и проверка, ускорение реагирования.*

Рис. 4: Единая облачная платформа управления Aether

Panda Adaptive Defense 360

РАСШИРЕННАЯ АВТОМАТИЧЕСКАЯ ЗАЩИТА КОНЕЧНЫХ УСТРОЙСТВ

Традиционные технологии защиты (EPP), *сфокусированные на предотвращении, являются* недорогими *средствами, подходящими для борьбы с известными угрозами и вредоносным поведением, однако в наше время их уже недостаточно. Эффективная защита вашей организации и предотвращение существующих и будущих кибер-угроз подразумевает переход к технологиям предотвращения, обнаружения и непрерывного реагирования, предполагая, что ваша организация постоянно находится под угрозой, а конечным устройствам постоянно угрожают злоумышленники.*

Panda Adaptive Defense 360 *интегрирует в рамках единого решения традиционные технологии защиты с инновационными технологиями предотвращения, обнаружения и автоматического реагирования на сложные и неизвестные кибер-угрозы.*

Традиционные превентивные технологии

- *Персональный или управляемый файервол*. IDS.
- *Контроль устройств*.
- *Постоянная защита от вредоносного ПО и проверка по запросу.*
- *Управляемые белые/черные списки. Коллективный разум.*
- *Предварительная эвристика*.
- *Контроль веб-доступа*.
- *Антиспам и антифишинг*.
- *Антитамперинг*.
- *Почтовый контент-фильтр*.
- *Восстановление и откат*.

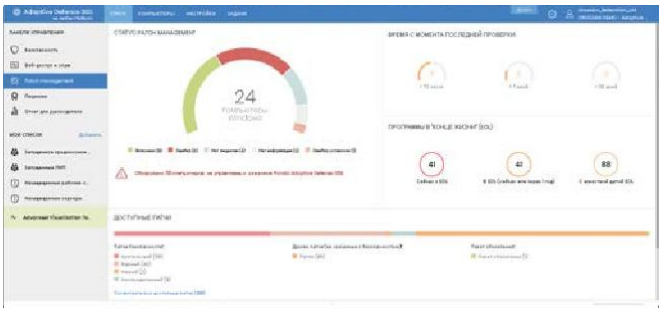
Технологии расширенной защиты

- EDR: *непрерывный мониторинг активности конечных устройств.*
- *Предотвращение выполнения неизвестных процессов.*
- *Облачное Машинное обучение поведения для классификации ВСЕХ неизвестных процессов* (APT, *шифровальщики, руткиты*...).
- *Облачная песочница в реальных окружениях*.
- *Поведенческий анализ и обнаружение* IoA (*скрипты, макросы*....).
- *Автоматическое обнаружение и реагирование на эксплойты в памяти.*
- *Управляемый* Threat Hunting *для атак, не использующих вредоносное ПО*.

ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ

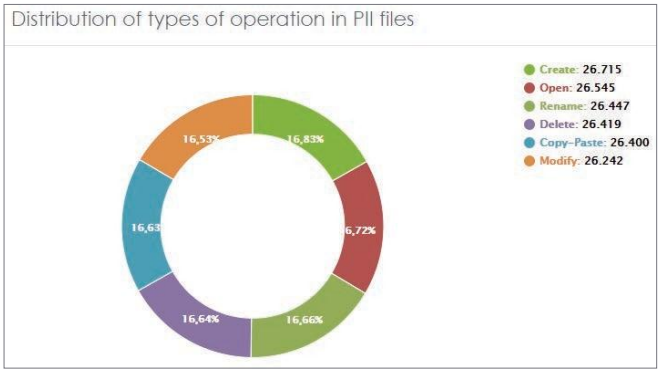
Panda Patch Management

Panda Patch Management - это интуитивно понятное решение для управления уязвимостями в операционных системах и сторонних приложениях на конечных устройствах и серверах с Windows. Результат: сокращение поверхности атаки, усиление превентивных возможностей и сдерживание инцидентов.



Panda Data Control

Panda Data Control обнаруживает, проверяет и отслеживает неструктурированные конфиденциальные или персональные данные на конечных устройствах: от неактивных данных до используемых и перемещаемых данных.



Panda Advanced Reporting Tool

Данный модуль автоматизирует процессы анализа информации, генерируемой при выполнении процессов и приложений на защищенных конечных устройствах и собираемой локальными агентами Panda Adaptive Defense 360, которая обрабатывается на облачной платформе защиты.

Panda Advanced Reporting Tool автоматически генерирует знания о деятельности организации и предоставляет возможности поиска, корреляции и настройки оповещений в зависимости от событий.

Panda SIEMFeeder

Модуль **SIEMFeeder** отправляет в реальном времени отправляет в компании данные по событиям, собранные с конечных устройств и обогащенные знаниями безопасности в Облачной платформе защиты для интеграции в корпоративную SIEM-систему.

Операционные системы на конечных устройствах
Рабочие станции Windows: XP SP3 и выше
Серверы Windows: Server 2003 (32/64-бит и R2) SP2 и выше
Рабочие станции и серверы MacOS: macOS 10.10 Yosemite и выше
Рабочие станции и серверы Linux: Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS и 16.10. Fedora 23, 24 и 25. Свяжитесь с Вашим поставщиком Panda для уточнения по другим поддерживаемым дистрибутивам.
Android: Версия 4 и выше
Сертификаты платформы: ISO27001, SAS 70

Награды и сертификаты

Panda Security регулярно участвует и получает награды за защиту и производительность от Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs.

Panda Adaptive Defense получил сертификацию EAL2+ при оценке на соответствие стандартам Common Criteria.

Panda Security назван "провидцем" в Магическом квадранте Gartner Magic для платформ защиты конечных устройств (EPP) 2018

AV-Comparatives высоко оценило Adaptive Defense 360, "т.к. данное решение классифицирует все исполняемые процессы, оно не может пропустить какое-либо вредоносное ПО".

Aether Platform

Инновационная и интегрированная платформа для всех решений Panda по защите конечных устройств.

Все из единой веб-консоли с помощью единого агента.

pandasecurity.com

panda

Преимущества платформы Aether

БОЛЕЕ ШИРОКИЕ ВОЗМОЖНОСТИ УПРАВЛЕНИЯ И МОНИТОРИНГА

Управляйте тысячами компьютеров с помощью детализированных настроек, фильтров и настраиваемых отчетов. Отслеживайте, кто что и когда делает с помощью контроля активности пользователей и прав на основе ролей.

ПОДРОБНЫЕ, НАСТРАИВАЕМЫЕ ОТЧЕТЫ

Отчеты с **подробной и настраиваемой информацией** с гибкими критериями выборки: фильтры, поиск, периоды времени, группы устройств и требуемый в отчете контент. Отчеты можно сохранить для последующего использования.

УПРАВЛЯЙТЕ БЕЗОПАСНОСТЬЮ С ЛЮБОГО УСТРОЙСТВА

Благодаря **адаптивному дизайну** консоли управления, Вы можете **использовать любое мобильное устройство** для управлению сетевой безопасностью из любого места в любое время.

ЭФФЕКТИВНЫЕ КОММУНИКАЦИИ

Защищайте и **управляйте всеми компьютерами в реальном времени, даже изолированными системами** *без доступа к Интернету благодаря функции прокси, которая включена в агента* Aether.

Экономьте пропускную способность канала связи и ускорьте внедрение агента и знаний безопасности, назначив сетевой компьютер в качестве кеша/репозитория.

В РЕАЛЬНОМ ВРЕМЕНИ

Мгновенно реагируйте *на любой критический инцидент безопасности. Применяйте настройки, устанавливайте исключения или запускайте сканирования на сотнях и тысячах компьютеров за несколько секунд*.

ДАННЫЕ ПО АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ НА КАЖДОМ КОМПЬЮТЕРЕ

Экономьте время и **оптимизируйте безопасность Вашей компании** с помощью информации об аппаратном и программном обеспечении, включенной во все продукты, управляемые на платформе Aether.

Вы уже используете продукт Panda для управления безопасностью Ваших компьютеров и серверов?

Вскоре Вы сможете спокойно перейти на платформу Aether.

Ваш поставщик решения Panda Security предоставит Вам всю необходимую для этого информацию.

Продукты под управлением платформы Aether

Следующие продукты **уже интегрированы** в Aether, новую платформу управления от компании Panda Security:

- Endpoint Protection
- Endpoint Protection Plus
- Adaptive Defense
- Adaptive Defense 360

Варианты покупки

Вам просто необходимо **купить один или несколько продуктов, управляемых** на платформе Aether, чтобы воспользоваться всеми преимуществами новой платформы управления Panda Security.

Технические требования

Интернет-браузер:

Все, что Вам необходимо, - это подключение к Интернету и современный браузер.

- Internet Explorer
- Edge
- Chrome
- Firefox
- Opera

Платформы, поддерживаемые продуктами под управлением Aether:

Операционная система	Поддерживаемые версии
Windows	XP SP3 и выше
Серверы Windows	Windows Server 2003 (32/64-бит и R2) SP2 и выше
Компьютеры и серверы MacOS	macOS 10.10 Yosemite и выше
Компьютеры и серверы Linux	Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS и 16.10 Fedora 23, 24 и 25 * Уточните и Вашего поставщика Panda поддержку других дистрибутивов
Android	Версия 4 и выше

Panda Adaptive Defense 360 на платформе Aether. Презентация продукта.

Содержание:

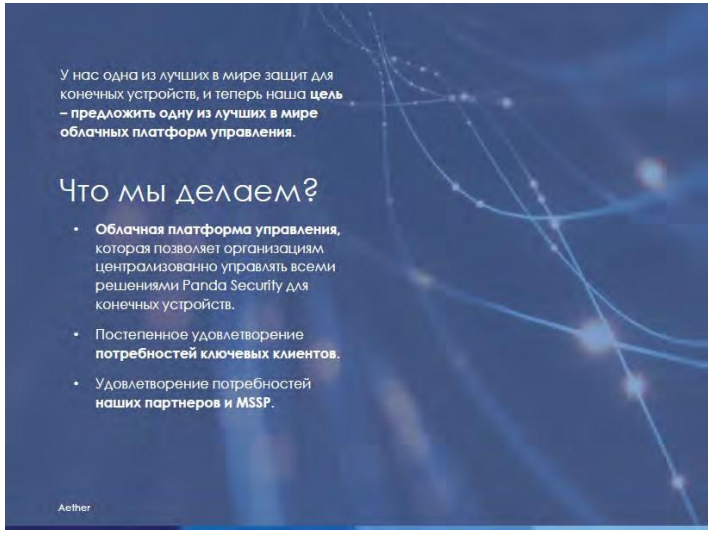
Цель настоящего документа - предоставить сценарий презентации продукта **Panda Adaptive Defense 360 на платформе Aether**.

Данный сценарий может использоваться для представления Panda Adaptive Defense 360 и улучшенных функций управления, включенных в новую платформу **Aether** для централизованного управления всех облачных решений Panda Security.

Документ также может служить в качестве основы для презентации других облачных корпоративных решений Panda, построенных на основе платформы Aether: Panda Endpoint Protection, Panda Endpoint Protection Plus и Panda Adaptive Defense.

Введение

Panda обладает лучшей защитой в мире для рабочих станций и серверов (Panda Adaptive Defense 360), а теперь мы решили предоставить лучшую облачную платформу управления.



ОБЗОР ПЛАТФОРМЫ AETHER
https://habrahabr.ru/company/panda/blog/351866/

ПРЕЗЕНТАЦИЯ PANDA ADAPTIVE DEFENSE 360

Уже некоторое время на рынке безопасности появляются новые модели защиты (**EDR**-решения), которые **дополняют антивирусные решения,** но они не способны их заменить. Но в отличие от своих конкурентов, **Panda Adaptive Defense 360** интегрирует в рамках единого решения защиты конечных устройств функции предотвращения, обнаружения, экспертного анализа и восстановления благодаря сочетанию **EPP-технологий** (платформа защиты конечных устройств) и **EDR-технологий** (обнаружение атак на конечные устройства и реагирование на них). Кроме того, продукт предоставляет два отличительных сервиса: 100% классификация всех приложений, программ и исполняемых файлов в качестве надежных или вредоносных программ, а также Threat Hunting Service, который обнаруживает аномальное поведение надежных приложений на конечных устройствах.

Решения **Panda Adaptive Defense** и **Panda Adaptive Defense 360** вновь и вновь продемонстрировали как в сетях клиентов, так и в рамках внешних сравнительных анализов (AV-Comparatives – Real World Protection Test – Июль-ноябрь 2017), свою эффективность в борьбе со всеми типами известных и неизвестных угроз, а также атак, использующих или неиспользующих вредоносные программы, эксплойтов и даже безфайловых атак, использующих административные инструменты.

ПРЕЗЕНТАЦИЯ ПЛАТФОРМЫ AETHER

Panda обладает лучшей защитой в мире для рабочих станций и серверов (**Panda Adaptive Defense 360**), а теперь мы решили предоставить лучшую облачную платформу управления. Именно по этой причине мы разработали Aether - новую инновационную платформу для централизованного управления решениями безопасности Panda Security.

Платформа Aether предоставляет еще больше **контроля**, **гибкости** и **детальности,** чтобы помочь администраторам управлять сетями из сотен или даже тысяч компьютеров. Она содержит **очень востребованные передовые функции** (обнаружение незащищенных компьютеров, фильтры, роли, отслеживание активности пользователей и пр.) и **дополнительную информацию о конечных устройствах (аппаратное и программное обеспечение, примененные патчи и т.д.**), что помогает компаниям экономить время и повышать эффективность корпоративной безопасности.

Все эти функции доступны компаниям в **единой веб-консоли с единым агентом** и **в реальном времени**, позволяя администраторам оперативно реагировать на любой критический инцидент безопасности в считанные секунды.

СТРАНИЦА СТАТУС

Безопасность

КЛАССИФИКАЦИЯ ВСЕХ ЗАПУЩЕННЫХ И ПРОВЕРЕННЫХ ПРОГРАММ

Глобальные данные
Активность вредоносного ПО
Активность ПНП
Активность эксплойтов
Заблокированные программы, ожидающие классификации

PANDA ADAPTIVE DEFENSE 360 НА ПЛАТФОРМЕ AETHER - ДЕМО-КОНСОЛЬ

ДЕЙСТВИЯ:

➔ Откройте демо-консоль для всех продуктов на базе Aether и авторизуйтесь:
- Страница: https://aetherdemo.pandasecurity.com/
- Логин: DRUSSIAN_FEDERATION_C14@panda.com
- Пароль: DRUSSIAN#123

СТАТУС ЗАЩИТЫ: При подключении к продукту Вы увидите панели, позволяющие Вам мгновенно оценивать основные проблемы безопасности в Вашей компании:

- Незащищенные компьютеры (с ошибками, в процессе установки защиты, без лицензии и пр.)
- Обнаруженные незащищенные компьютеры
- Компьютеры в оффлайне более 3, 7 или 30 дней
- Компьютеры с необновленной защитой

КЛАССИФИКАЦИЯ ВСЕХ ЗАПУЩЕННЫХ И ПРОВЕРЕННЫХ ПРОГРАММ: Эта диаграмма показывает результаты классификации всех программ и библиотек, запущенных в вашей компании. **Panda Adaptive Defense 360** не только классифицирует вредоносное ПО, но он также инспектирует все другие программы и процессы, минимизируя риск заражения.

В отличие от других EDR-решений, **Panda Adaptive Defense 360** предоставляет управляемый сервис, чтобы клиентам не приходилось самим беспокоиться о классификации приложений, программ или исполняемых файлов. Для этого продукт применяет алгоритмы Машинного обучения для всех событий и действий, происходящих на конечных устройствах, автоматически в реальном времени классифицируя 99,98% всех приложений в качестве вредоносных или надежных.

Даже если программа классифицирована как надежная, продукт все равно продолжит ее отслеживать, чтобы можно было в любой момент нейтрализовать казалось бы надежное приложение, которое позже может оказаться вредоносным ПО или ПНП.

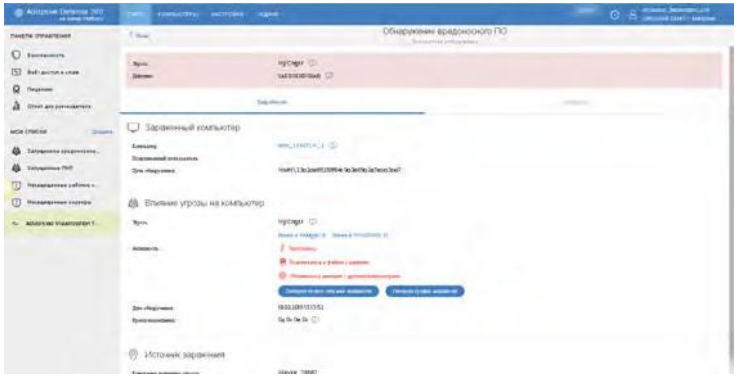
АКТИВНОСТЬ ВРЕДОНОСНОГО ПО: Этот виджет показывает информацию об угрозах (шифровальщики, направленные атаки, трояны и пр.) в реальном времени, обнаруженных защитой при попытке проникновения в систему или запуска в ней.

ДЕЙСТВИЯ:

➔ Нажмите на виджете на кол-во инцидентов
➔ нажмите на первую угрозу в списке (**Trj/CI.A)**.
- Покажите все **подробности** (угроза, пострадавший компьютер, источник заражения, появление на других компьютерах и пр.).

Экспертный анализ вредоносного ПО

Подробности



Подробная информация

График активности

- Покажите список всех действий на закладке **Активность**
- Покажите **график активности.** Покажите жизнь угрозы с начала
  - Нажмите кнопку **Первый узел** (в правом нижнем углу)
  - Нажмите **Запустить** (в левом нижнем углу)

Графическое представление жизненного цикла угроз позволяет Вам **увидеть действия, предпринятые хакером** в течение времени при попытке внедрения угрозы в систему. Вы можете детализировать и выбрать отображаемую информацию для:

- Выполнения экспертного анализа для оценки ущерба со стороны угрозы и обнаружения потенциальной утечки данных
- Принятия **превентивных мер** с целью предотвращения будущих атак: изменение прав пользователей, создание правил файервола для защиты периметра сети и пр.

На графике используются разные цвета для обозначения степени опасности каждого объекта: **ЗЕЛЕНЫЙ** для невредоносного ПО, **КРАСНЫЙ** для вредоносного ПО, **ОРАНЖЕВЫЙ** для объектов в процессе классификации и **СИНИЙ** для действий, осуществляемых отслеживаемыми процессами. В случае коммуникаций, установленных вредоносной программой, сервис определяет получателя соединения.

Этот пример показывает, как пользователь скачал якобы файл с видео, оказавшийся на самом деле программой, которая скачала некие компоненты, установила их и позже установила соединения с сервером в США. Риски:

- Предназначены ли эти действия для кражи данных?
- Является ли эта атака промышленным шпионажем?

Другие примеры:

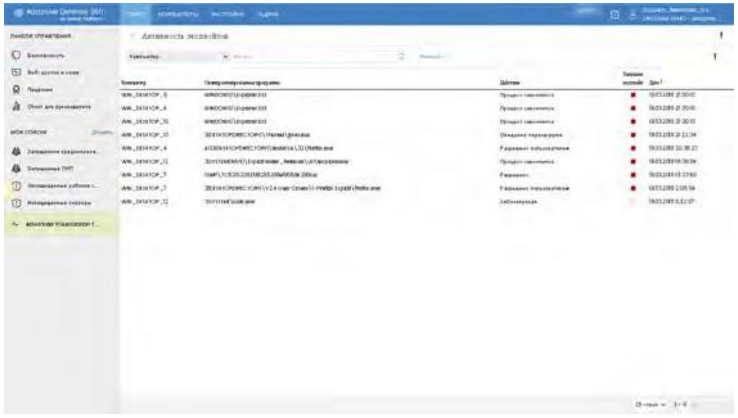
- **Trj/Generic.gen**: Вредоносное ПО, пытающееся выдать себя за "кряк" программы BeyondCompare, но в реальности оно подключается к различным IP-адресам, загружает данные и запускает разные приложения. После запуска выполняет действия с целью кражи данных и повреждения системы.
- **Trj/CryptoWall.A**: Вариант CryptoLocker, который проникает в систему через легитимные программы (Интернет-браузер, Powershell и т.д.). **Panda Adaptive Defense 360** предотвращает запуск этого шифровальщика за счет непрерывного мониторинга каждой программы, запущенной на конечных устройствах, включая даже надежные программы, которые могут стать точкой входа для вредоносного ПО.

Экспертный анализ ПНП

АКТИВНОСТЬ ПНП (Потенциально нежелательные программы): *Этот виджет в реальном времени показывает программы, обнаруженные защитой и классифицированные как ПНП (шпионы, хакерские утилиты, тулбары и пр.). ПНП имеют следующие вредоносные эффекты: снижение производительности компьютеров/серверов, вызывают несовместимость с определенными корпоративными программами и "пожирают" полосу пропускания канала связи.*

➔ Нажмите на кол-ве инцидентов и в списке выберите последний PUP/SoftwareUpdater: это ПНП, который взаимодействовал с различными IP-адресами в США в течение 5 дней.

Активность эксплойтов



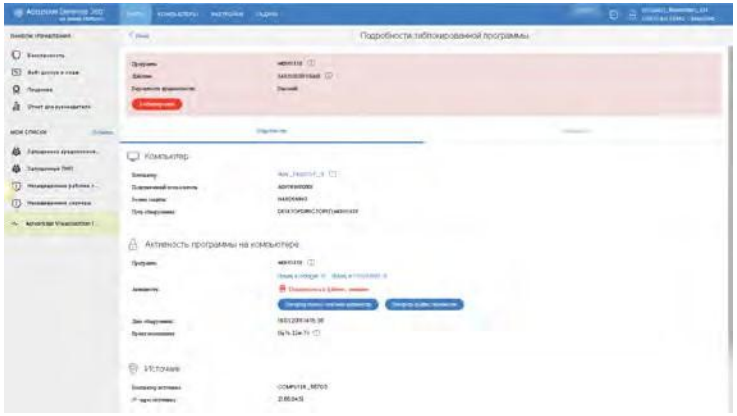
АКТИВНОСТЬ ЭКСПЛОЙТОВ: Данный виджет показывает эксплойты, обнаруженные в уязвимых процессах, запущенных пользователями.

Когда уязвимый процесс получает входные данные, злонамеренно созданные хакерами, то может возникнуть внутренняя неисправность, которая позволит хакеру встроить фрагменты вредоносного кода в области памяти, управляемые уязвимым процессом.

После этого процесс становится "скомпрометированным". Встроенный код может привести к тому, что скомпрометированный процесс начнет выполнять непредусмотренные действия, что может скомпрометировать безопасность самого компьютера. Антиэксплойтная защита в **Panda Adaptive Defense 360** обнаруживает все попытки внедрения вредоносного кода в уязвимые процессы, запущенные пользователями.

Чтобы защитить себя от атак эксплойтов, крайне важно закрывать уязвимости, найденные в скомпрометированных программах и обнаруженные антиэксплойтной технологией. Поэтому компаниям рекомендуется иметь инструмент, способный **обнаруживать и устаналивать патчи** как для операционной системы, так и для сторонних программ на компьютерах пользователей.

Заблокированные программы



ЗАБЛОКИРОВАННЫЕ ПРОГРАММЫ, ОЖИДАЮЩИЕ КЛАССИФИКАЦИИ: Показывает заблокированные в настоящий момент приложения, находящиеся в процессе классификации. Эти приложения анализируются в нашей аналитической платформе АНАЛИЗ БОЛЬШИХ ДАННЫХ, способной автоматически классифицировать 99,98% всех приложений. Остальное количество анализируется вручную экспертами по вредоносному ПО нашей антивирусной лаборатории PandaLabs.

Каждая заблокированная программа может быть разблокирована на странице с подробными данными при нажатии на кнопку **Разблокировать**.

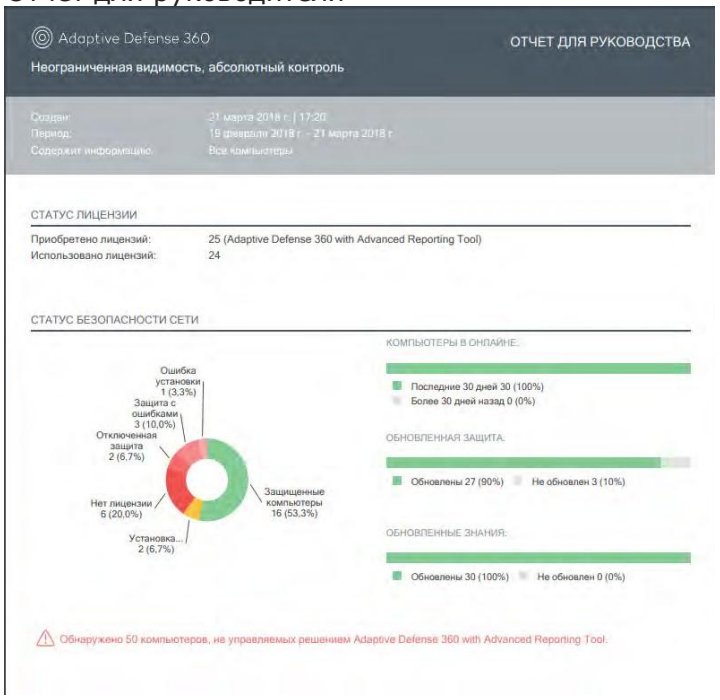
Если заблокированный объект является файлом EXE или COM, то его разблокировка разрешит выполнение программы и его библиотек на всех компьютерах (если они не являются известными угрозами). Следовательно, Вам необходимо создать только одно исключение, чтобы разрешить запуск программы и всех связанных с ней компонентов.

В любом случае, **Panda Adaptive Defense 360** продолжит мониторинг всех процессов, даже разблокированных, для того, чтобы ВСЕ обнаруженные программы были всегда корректно классифицированы.
Примечание: Рекомендуется разблокировать объекты только в том случае, если Вы на 100% уверены, что они являются надежными.

СТРАНИЦА СТАТУС

Безопасность
Веб-доступ и спам
Лицензии
Отчет для руководителя
Мои списки

Отчет для руководителя



ПРОГРАММЫ, РАЗРЕШЕННЫЕ АДМИНИСТРАТОРОМ: Данный виджет показывает все исключенные программы. Будьте осторожны, т.к. он может содержать объекты, классифицированные как вредоносное ПО или ПНП..

УГРОЗЫ, ОБНАРУЖЕННЫЕ АНТИВИРУСОМ: Показывает информацию о вредоносных программах, обнаруженных антивирусом и другими модулями защиты, включенными в **Panda Adaptive Defense 360** (Контроль устройств, Файервол и т.д.).

КОНТЕНТ-ФИЛЬТРАЦИЯ ДЛЯ СЕРВЕРОВ EXCHANGE: Показывает количество почтовых сообщений, заблокированных контент-фильтром для серверов Exchange.

РАЗДЕЛ ВЕБ-ДОСТУП И СПАМ: Показывает графики, отображающие категории веб-сайтов, к которым обращались с компьютеров вашей сети, а также спамовые сообщения, обнаруженные антиспамом для сервера Exchange.

РАЗДЕЛ ЛИЦЕНЗИИ: Показывает информацию о лицензиях всех приобретенных продуктов: использованные лицензии, компьютеры без лицензии, даты окончания лицензий и пр.

ОТЧЕТ ДЛЯ РУКОВОДИТЕЛЯ: Предоставляет ключевые данные для определения статуса безопасности предприятия. Можно настраивать содержание отчета, а сами отчеты могут формироваться по запросу или по расписанию с автоматической отправкой на указанные вами адреса электронной почты.

МОИ СПИСКИ: Показывает ряд настроенных **списков**. Эти списки очень полезны для технического персонала, которым требуется быстро получить список требуемых устройств для получения более подробной информации об инциденте. Они позволяют быстро получить важную информацию (кто что делал, как и когда).
Вы также можете создать и сохранить **собственные списки**.

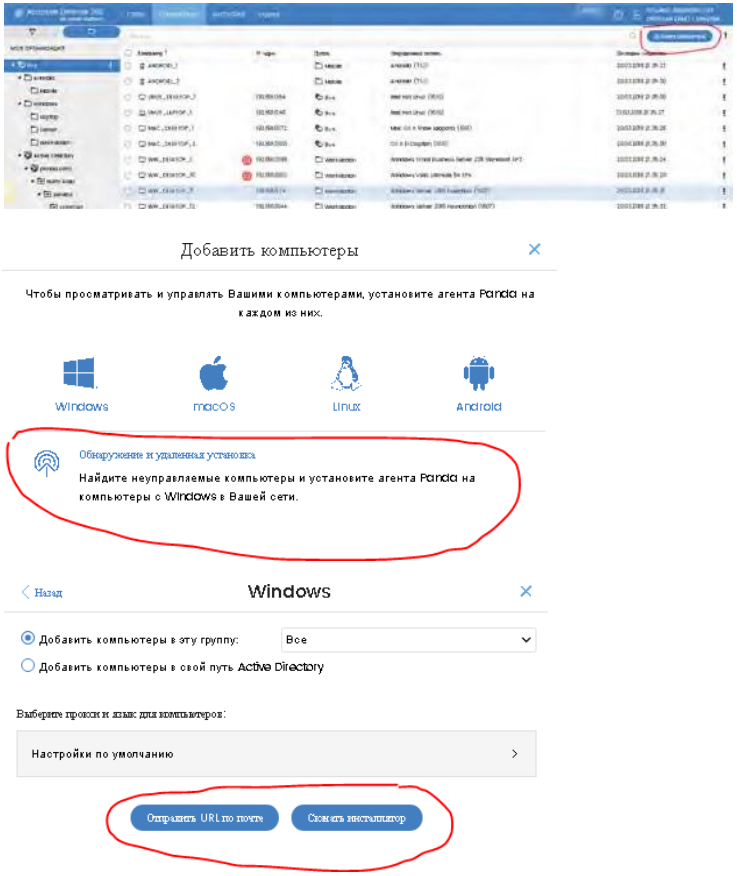
➔ Создайте новый список, содержащий обнаруженные неуправляемые компьютеры.

ДЕЙСТВИЯ:

➔ Показать каждую панель и вкратце объяснить ее функциональность
➔ Показать, что можно показывать данные за последние 24 часа, 7 дней, 1 месяц и 1 год

Установка

По электронной почте
Скачивание инсталлятора
Поиск незащищенных компьютеров и удаленная установка



УСТАНОВКА

Процесс установки агента Aether запускается при нажатии кнопки **Добавить компьютеры** на странице **КОМПЬЮТЕРЫ**. В появившемся окне выберите требуемую операционную систему (**Windows, macOS, Linux** и **Android**). Все версии защиты **полностью разработаны в Panda**, что позволяет нам предоставлять **максимальную безопасность** в реальном времени с помощью защиты, движка и сигнатур Panda для всех платформ.

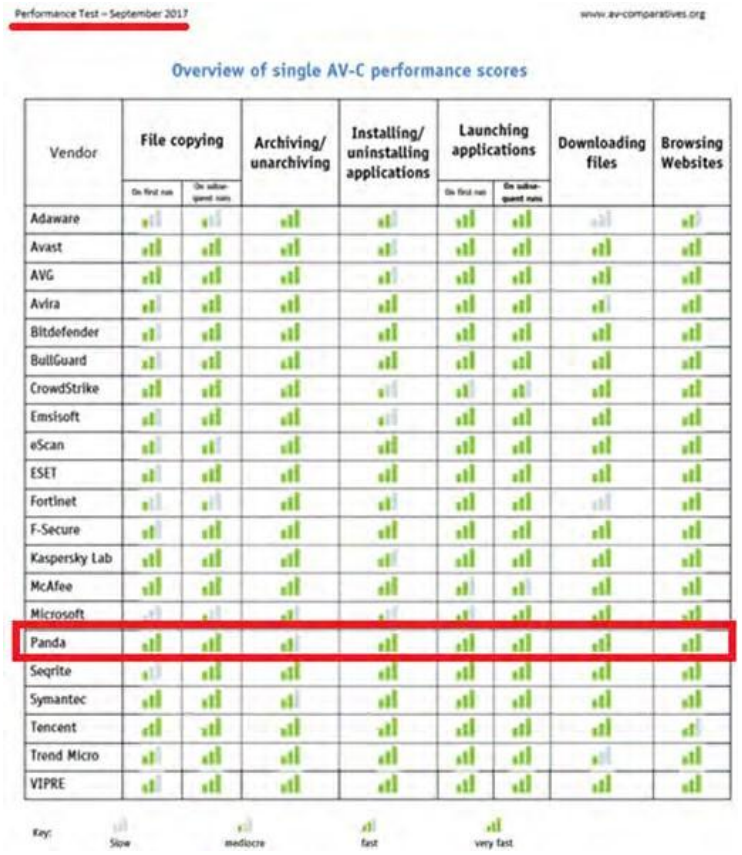
Существует **3 способа установки агента**:

1. Отправка инсталлятора **по почте** тем пользователям, которых Вы хотите защитить
2. **Скачивание инсталлятора** и его распространение с помощью утилиты распространения Panda или через Active Directory
3. С помощью опции **обнаружения компьютеров и удаленной установки**, для чего необходимо выполнить следующие шаги:
   a. Назначьте компьютер для обнаружения в **Настройки/Сетевые настройки/ Обнаружение**. Каждому компьютеру, который будет использоваться для поиска незащищенных устройств, Вы можете настроить опции автоматического запуска поиска незащищенных компьютеров или ограничения на зону поиска.
   b. Проверьте виджет **СТАТУС ЗАЩИТЫ** на главной странице, т.к. он будет показывать ссылку на список всех найденных незащищенных компьютеров.
   c. Удаленно установите защиту прямо из списка незащищенных компьютеров, указав соответствующие регистрационные данные администратора.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

1. Агенту Panda нежелательно параллельно сосуществовать с другими решениями безопасности (кроме продукта Panda Adaptive Defense), поэтому Вы можете сразу включить опцию автоматического удаления любой найденной сторонней защиты в разделе **Настройки/требуемый профиль/Основное**.
2. После первой установки объем потребления полосы составляет всего несколько КБ в день. Чтобы оптимизировать потребление полосы пропускания канала связи назначьте для каждого сегмента сети хотя бы один кеш-компьютер (**Настройки/Сетевые настройки/Кеш**).
3. Влияние агента и защиты **Panda Adaptive Defense 360** на производительность компьютера незначительно, поскольку потребление полосы пропускания оптимизировано благодаря использованию кеша, который хранит классификацию каждой программы/библиотеки, загруженной в системе.

В недавнем исследовании AV-Comparatives, Panda получила оценку **Очень быстро** во всех выполненных тестах производительности, за исключением одного, где мы получили оценку **Быстро**.



Performance Test – September 2017

www.av-comparatives.org

Overview of single AV-C performance scores

Vendor	File copying		Archiving/ unarchiving	Installing/ uninstalling applications	Launching applications		Downloading files	Browsing Websites
	On first run	On subsequent runs			On first run	On subsequent runs		
Adaware								
Avast								
AVG								
Avira								
Bitdefender								
BullGuard								
CrowdStrike								
Emsisoft								
eScan								
ESET								
Fortinet								
F-Secure								
Kaspersky Lab								
McAfee								
Microsoft								
Panda								
Seqrite								
Symantec								
Tencent								
Trend Micro								
VIPRE								

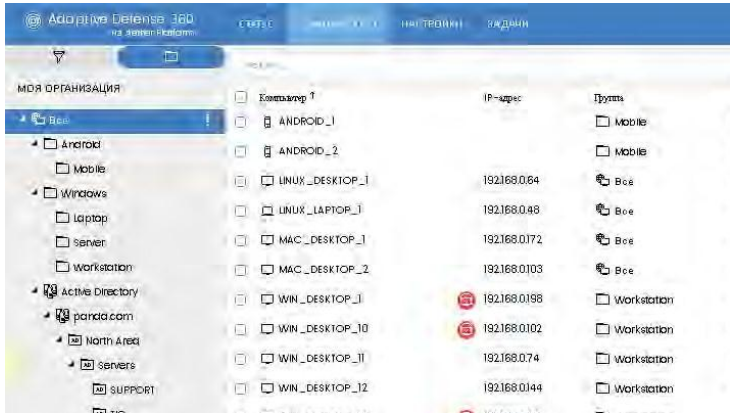
Key: Slow, mediocre, fast, very fast

В октябре 2017 года AV-Comparatives снова присудил нам наивысшую оценку за производительность.

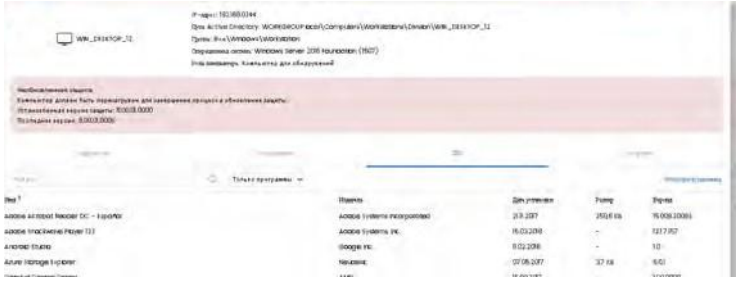
Управление компьютерами

Фильтры

Древо компьютеров (группы и Active Directory)



Сведения об аппаратном и программном обеспечении, журнал изменений



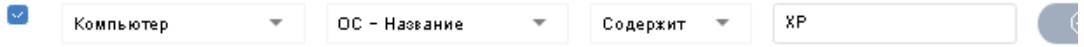
Примененные системные патчи

ФИЛЬТРЫ И ДРЕВО КОМПЬЮТЕРОВ

Существует **2 способа обзора компьютеров**:

1. **С помощью фильтров**: Этот способ позволяет вам организовать ваши компьютеры по операционной системе, ПО и прочим критериям, или создать собственный фильтр с определенными критериями, связанными с настройками, статусом защиты, оборудованием, ПО и пр.

   ➔ Создайте фильтр для выбора компьютеров с XP. Они являются уязвимыми и на них требуется обращать отдельное внимание.

   Фильтры дают **гибкость,** необходимую для управления сотнями или тысячами ПК.

2. **По организационному древу**: Это может быть пользовательское древо, древо Active Directory копании или их сочетание.

   ➔ Покажите, что необходимо установить агента для интеграции компьютера в пользовательскую группу или в свой путь Active Directory. Скажите, что компьютеры можно переносить из одной группы в другую.

СВЕДЕНИЯ ОБ АППАРАТНОМ ИЛИ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ, ЖУРНАЛ ИЗМЕНЕНИЙ

Нажмите на любом отображаемом компьютере, чтобы просмотреть о нем **подробную информацию**. Помимо информации о статусе, вы также можете видеть информацию об оборудовании и ПО на каждом компьютере. Эта информация позволяет администраторам экономить время и оптимизировать безопасность во всей компании.

➔ Покажите подробную информацию, сведения об аппаратном и программном обеспечении и журнал изменений (установки и удаления) о компьютере WIN_DESKTOP_1.

ПРИМЕНЕННЫЕ СИСТЕМНЫЕ ПАТЧИ

Информация на закладке **ПО** у каждого ПК показывает установленные **патчи Microsoft**. Эта информация очень полезна, если необходимо узнать статус безопасности ПК или требуется управлять несколькими ПК, т.к. вы можете создать фильтры, которые будут показывать те компьютеры, где применены определенные патчи или на которых они не имеются. Это очень полезно в критических ситуациях, которые могут быть вызваны, например, такими угрозами как WannaCry или Petya.

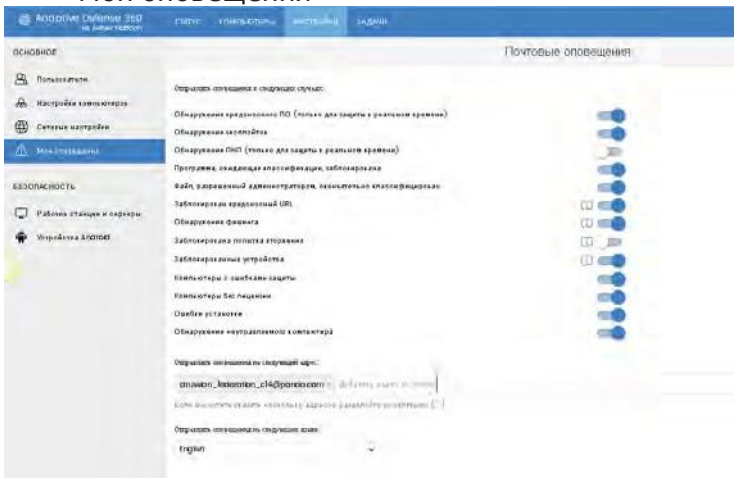
➔ Покажите информацию в разделе **ПО** у компьютера **WIN_DESKTOP_1**

➔ Покажите, как создать фильтр, который будет показывать компьютеры, где НЕ применен патч X.

Настройки

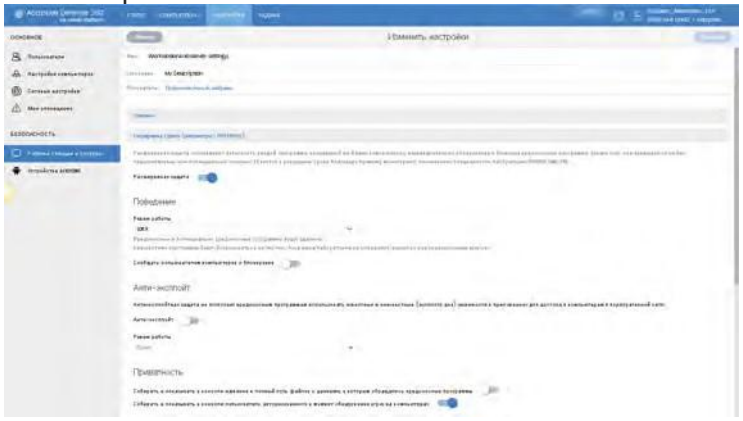
Основное

- Настройки компьютеров
- Сетевые настройки
- Мои оповещения



Безопасность

- Рабочие станции и серверы
- Устройства Android



ОСНОВНОЕ

Настройки - **гибкие и детальные**, их можно повторно использовать для подобных компьютеров

- **Настройки компьютеров:** Позволяют вам настраивать обновления и самозащиту
- **Сетевые настройки:**
  - **Прокси и язык**: Объясните, что **прокси Panda** позволяют вам подключать изолированные компьютеры к Интернету. Прокси Panda направляет все коммуникации **Adaptive Defense 360**, даже те, что направлены к облачной платформе Коллективный разум.
  - **Кеш** (показано ранее)
  - **Обнаружение** (показано ранее)

- **Мои оповещения**: Оповещения могут быть настроены по каждому пользователю. Вы можете настроить получателей почтовых оповещений о том, что обнаружено вредоносное ПО или обнаружен неуправляемый компьютер (у него отключена защита, нет лицензии или что-то другое). Почтовые оповещения держат вас в курсе наиболее критических событий, негативно влияющих на безопасность и производительность вашей компании без необходимости подключения к облачной консоли управления.

➔ Покажите все настраиваемые опции

БЕЗОПАСНОСТЬ

В зависимости от продукта, который вы приобрели, вы увидите различные функции безопасности:

- **Рабочие станции и серверы**: Позволяют вам настроить защиту для ваших серверов, настольных компьютеров и ноутбуков с Windows, Linux и macOS. Пользователи Linux и macOS могут использовать защиту в реальном времени и URL-фильтрацию.

➔ Покажите все опции и объясните различные режимы работы расширенной защиты.

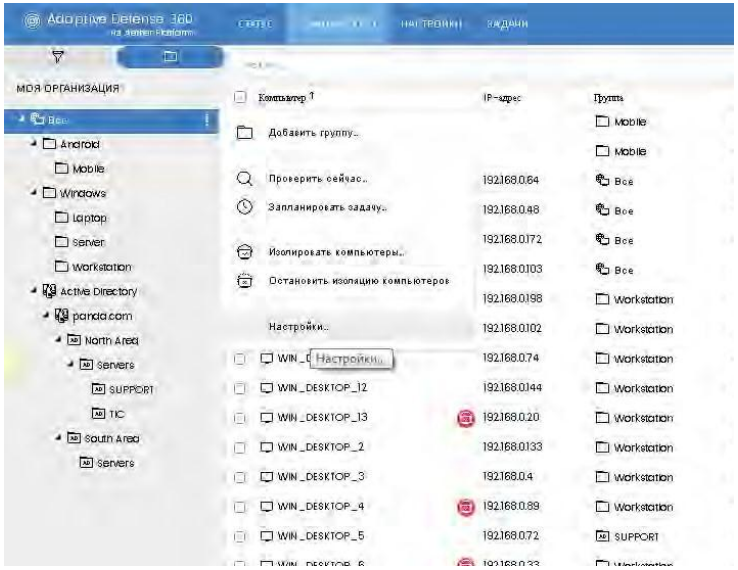
- **Устройства Android:** Позволяют вам настроить защиту ваших смартфонов и планшетов с Android 4.0 или позже. Пользователи Android имеют антивирусную защиту, а вскоре у них будет еще и защита Анти-вор (геолокация, удаленная очистка, удаленная блокировка и пр.).

В будущем мы встроим опции настройки для модуля Управления патчами и другие продукты Panda.

Настройки

Как назначать их

- Из профиля настроек
- Из древа компьютеров (наследование)
- Для отдельных компьютеров



КАК НАЗНАЧИТЬ НАСТРОЙКИ

Настройки во всех продуктах на платформе Aether наследуются, что ускоряет процесс назначения настроек. Настройки назначаются из организационного древа на странице **КОМПЬЮТЕРЫ**. Т.е. настройки, определенные в корневом узле, распространяются на каждый дочерний уровень через все организационное древо. Однако требуемым группам и компьютерам можно назначить отдельные настройки. отличающиеся от унаследованных.

➔ В качестве примера определите пару профилей настроек

Вы можете указать, к кому будет привязан профиль настроек, прямо в самом профиле.

Чтобы изменить настройки компьютера, нажмите на компьютер и измените его настройки безопасности на закладке **Настройки**.

➔ Покажите, как назначать профиль настроек определенному компьютеру.

Настройки применяются **в реальном времени.** Это позволяет администраторам изменять настройки, применяемые к сотням или тысячам компьютеров за считанные секунды, что может быть очень необходимо в критических ситуациях. Вы думаете, что это невозможно?

➔ Покажите в веб-консоли изменение настроек компьютеров. Для этого установите AD360 on Aether на компьютер, который вы используете для проведения демонстрационного показа. Удалите его лицензию или измените настройки защиты и покажите изменения в локальной консоли на этом компьютере.

Пользователи и роли

Пользователи и роли
Отслеживание активности

ПОЛЬЗОВАТЕЛИ И РОЛИ

Крупные партнеры и клиенты нуждаются в детализации прав, а также они хотят видеть, кто, что и когда делал в консоли управления.

В разделе **Настройки / Пользователи** на закладке **Роли** имеется две предварительно настроенные роли (**Полный контроль** и **Мониторинг**), но администраторы могут также создавать свои собственные роли. Например, вы можете создать роли, которые позволяют пользователям только устанавливать или изменять настройки и т.д. Кроме того, настройки роли позволяют вам указать, какие компьютеры будут видны каждому пользователю, т.к. не все администраторы должны иметь доступ ко всем компьютерам в компании.

- Создайте новую роль

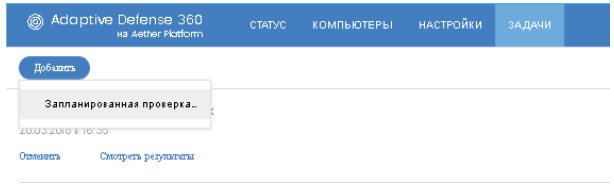
После создания новой роли вы можете назначить ее любому новому пользователю, которого вы можете создать, или существующим пользователям.

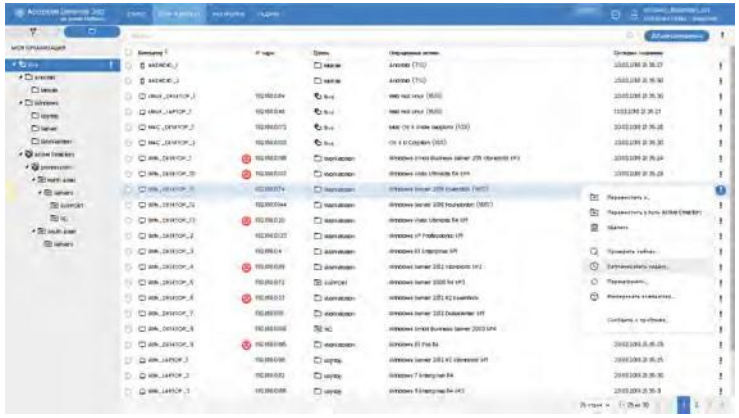
Закладка **Активность** позволяет вам видеть, кто и когда подключался к консоли (**СЕССИИ**), а также какие действия были выполнены каждым пользователем.

- Покажите закладку **Активность** и то, как можно просмотреть журнал активности.

Задачи и действия

Доступные виды задач
Откуда запускаются задачи





ЗАДАЧИ И ДЕЙСТВИЯ

В наших продуктах на платформе Aether **задачи независимы от настроек**. Т.е. они могут быть запущены без необходимости менять настройки.

Вы можете запустить проверку компьютеров по запросу и создать запланированные проверки с такими расширенными опциями как:

- Максимальное время выполнения
- Отложенное выполнение для отключенных компьютеров

➔ Покажите эти опции в разделе **ЗАДАЧИ**

Запланированные задачи показывают полную информацию о предыдущих запусках для каждого компьютера. Подобно настройкам, задачи запускаются в **реальном времени**. Т.е. срочные задачи могут быть запущены во всей сети в считанные секунды.

Решение также предоставляет ресурсы, которые облегчают управленческие задачи: вы можете **сообщать о проблемах** на ваших рабочих станциях и серверах в службу техподдержки Panda вместе с информацией и логами, собранными в вашей системе. Также вы можете удаленно **перезагружать** ваши управляемые компьютеры, если требуется обновить их защиту или если они некорректно работают.

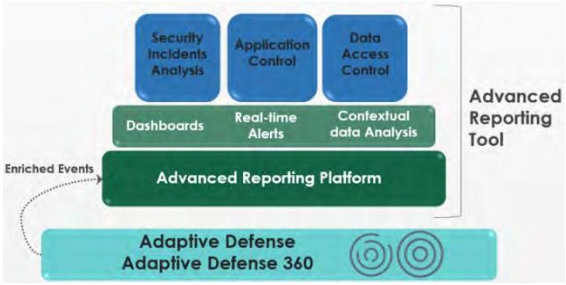
➔ Покажите эти опции со страницы **КОМПЬЮТЕРЫ**

Advanced Reporting Tool

Возможности

Advanced Reporting Tool использует файлы событий/журналов, собранные с компьютеров, которые защищены Adaptive Defense. Эти логи, обогащенные данными из платформы Adaptive Defense, хранятся в течение 1 года.

Advanced Reporting Tool предоставляет инструменты для облегчения управления и просмотра данных и событий, а также **глубокого анализа ситуации** - в противном случае **эти сложные задачи способны "пожирать" ресурсы ИТ-отделов**.



С помощью **Advanced Reporting Tool** вы можете:

1. Экономить средства:

   ➔ Покажите используемые лицензии (**Application Control / IT APPLICATIONS / Microsoft Office licenses in use)**

   ➔ Покажите потребление полосы пропускания канала связи (**Application Control / BANDWIDTH-CONSUMING APPLICATIONS + + Data Access Control / OUTBOUND NETWORK TRAFFIC + Data Access Control / BANDWIDTH CONSUMERS)**

2. Видеть, что происходит на ваших компьютерах:
   - Дважды нажмите Chrome для показа соответствующих компьютеров

   ➔ Обнаружьте несанкционированные программы и все запущенное ПО (**Application Control / IT APPLICATIONS / Executed Applications)**

   ➔ Покажите уязвимые приложения (**Application Control / VULNERABLE APPLICATIONS**)
   - Дважды нажмите Microsoft Corporation для показа всех уязвимых программ

   ➔ Покажите авторизованных пользователей (**Data Access Control / USER ACTIVITY**)
   ➔ Покажите файлы, открытые пользователями и другими компьютерами (**Data Access Control / DATA FILES ACCESSED)**

3. Осуществлять **глубокий экспертный анализ** безопасности:

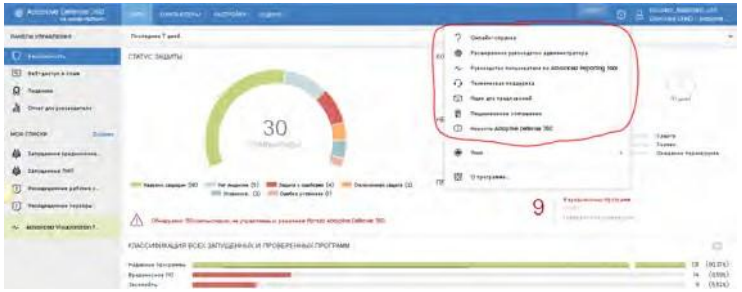
   ➔ Перейдите в панель **Security Incident**
   ➔ Перейдите к таблицам с первичными данными (таблицы с необработанными данными по всем событиям, происходящим в сети)

Кроме того, **Advanced Reporting Tool** предоставляет:

1. Настроенные оповещения и возможность создания собственных оповещений
2. Отчеты, связанные с графиками в панелях мониторинга
3. Возможность запуска своих запросов по всем собранным событиям (таблицы с первичными данными)

Руководства, справка и пр.

Расширенные руководства
Онлайн-справка
Техническая поддержка
Изменения в версиях



РУКОВОДСТВА, СПРАВКА И ПОДДЕРЖКА

Наши продукты на платформе Aether предоставляют доступ к различной документации:

- **Онлайн-справка**: Очень полезный источник информации. Функции:
  - Быстрый доступ к самым полезным статьям
  - Гибкий поиск для нахождения ответа на ваш вопрос
  - Содержание

- **Расширенные руководства**: PDF-документы с подробной информацией обо всех функциях продукта.

- **Техническая поддержка**: Доступ к нашему сайту технической поддержки с FAQ, инструментами для устранения неисправностей, хотфиксами и пр.

- **Новости Adaptive Defense 360:** Доступ к информации об изменениях в каждой новой версии. Содержит следующие сведения:
  - Версии агента и защиты
  - Основные новые функции
  - Исправленные ошибки

ЗАВЕРШЕНИЕ

У нас есть лучшая защита в мире для рабочих станций и серверов (**Panda Adaptive Defense 360**), а теперь мы хотим предоставить одну из лучших в мире облачную платформу управления.

Именно по этой причине мы разработали платформу Aether — это инновационная платформа для централизованного управления всеми облачными корпоративными решениями Panda Security. Aether предоставляет еще больше **контроля**, **гибкости и детализации**, что значительно облегчает решение вопросов по управлению безопасностью, хотя при этом наши продукты по-прежнему остаются легкими и простыми в использовании.

Новые модули, продукты и сервисы, которые в настоящее время разрабатываются в компании Panda Security (Data Control, Patch Management и пр.) , в ближайшее время будут интегрированы в Aether, что позволит нашим пользователям управлять несколькими продуктами **через единую веб-консоль с помощью единого агента** без необходимости во внедрении дополнительных решений. Кроме того, возможность выполнять действия в режиме **реального времени** позволяет компаниям за считанные секунды реагировать на любой критический инцидент.

Наше видение заключается в защите пользователей от кибер-преступлений и новых усовершенствованных угроз с помощью лучшей в мире защиты для конечных устройств под управлением Windows, Linux, macOS и Android.

С этой целью мы предоставляем лучшие в своем классе инструменты и максимальную безопасность без влияния на производительность системы или продуктивность пользователей, позволяя компаниям защищать свой самый ценный актив: информацию.

И все это - с помощью облачных решений с еще большим удобством и с меньшими расходами.

Adaptive Defense 360

pandasecurity.com/intelligence-platform/

panda

CryptoLocker

Можем ли мы его остановить?

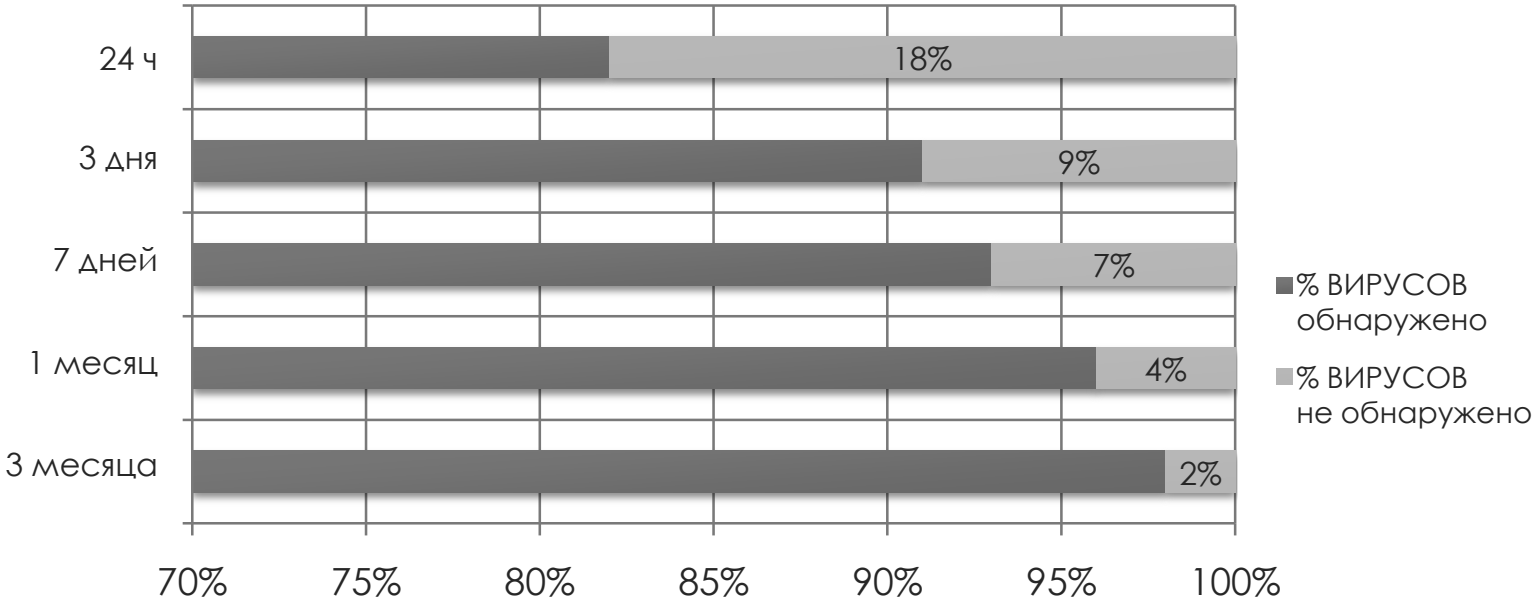
CryptoLocker

Могут ли антивирусные решения остановить CryptoLocker?

Достаточно ли иметь систему резервного копирования?

Могут ли антивирусы остановить такие атаки?

- **Антивирусные технологии** (сигнатуры, эвристика, контент-фильтрация, поведенческий анализ) являются **реактивными**.
- **Традиционные антивирусы неспособны обнаруживать 18% новых вредоносных программ** в течение первых 24 часов, а спустя три месяца все еще не обнаруживается порядка 2%.

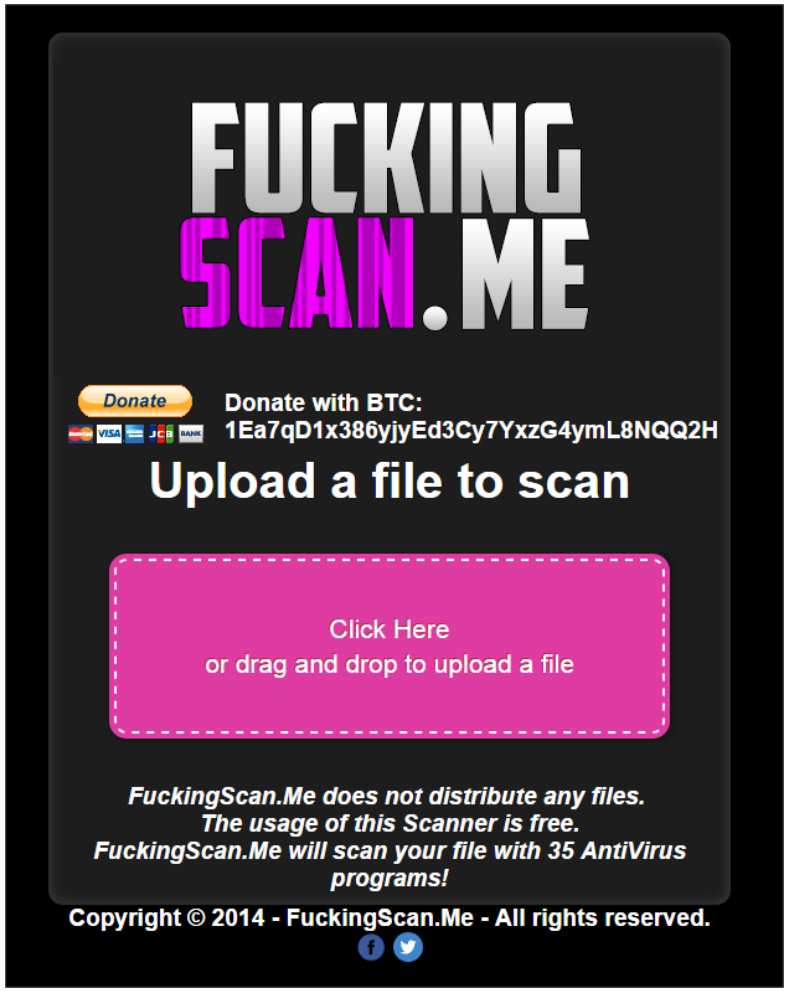


Исследование Panda Security об окне возможностей вредоносных программ

Могут ли антивирусы остановить такие атаки?

- Некоторые сайты позволяют Вам проверить, будет ли Ваш файл обнаружен антивирусными программами (и какими).
  - Они проверяют файл более чем 40 антивирусными программами
  - Бесплатно

-> Хакеры запускают свой вредоносной код, если они знают, что он **НЕ БУДЕТ обнаружен любым антивирусным решением.**



Могут ли контент-фильтр, антиспам и URL-фильтр остановить такие атаки?

- Иногда, но не всегда

- **Макровирусы снова используются** для преодоления контент-фильтров
  - Макро → Загрузчик → CryptoLocker
  - Макро → Загрузчик → CMD → CryptoLocker
  - Макро → VBS-код (встроенный) → Загрузчик → CryptoLocker
  - Макро → VBS-код (скачиваемый)→ Загрузчик → Cryptolocker

Антивирусный ответ для CryptoLocker

- Антивирусные технологии
  - Специальные сигнатуры
  - Общее и эвристическое обнаружение
  - Блокировка URL, связанных с ransomware
  - “Контекстное” обнаружение: останавливает процесс шифрования файла

ВЫВОД: НЕДОСТАТОЧНО

- Новые варианты продолжают заражать системы
- **Все, что антивирус не может обнаружить, РАЗРЕШЕНО ЗАПУСКАТЬ**


Cryptolocker: 10 steps to avoid the ransomware virus

Global cybercrime agencies say users already infected with the Cryptolocker ransomware have a two-week window to remove it

Cryptolocker virus network thwarted by global operation


The Windows Club

A THREE TIME GARTNER MAGIC QUADRANT LEADER

Home News Windows Downloads Security IE Office Phone General Deals Forum About

CryptoLocker Tripwire: Free Cryptolocker Prevention Tool

RECOMMENDED: Click here to fix Windows errors and optimize system performance

The **Cryptolocker Ransomware** has been morphing into more dangerous forms and even started targeting other operating systems like Android. While those affected are always looking out for ways to get rid of or remove Cryptolocker ransomware, the old proverb still stands – *Prevention is better than cure*!

*We have earlier seen how you can block or prevent Cryptolocker ransomware attacks using CryptoPrevent, Cryptolocker Prevention Kit and HitmanPro.Alert – and by following some steps to take to stay protected & secure, by **preventing Ransomware** from getting onto your Windows computer.*

Via this post, we would like to inform you about another Cryptolocker Prevention Tool called **CryptoLocker Tripwire**.

Достаточно ли иметь систему резервного копирования?

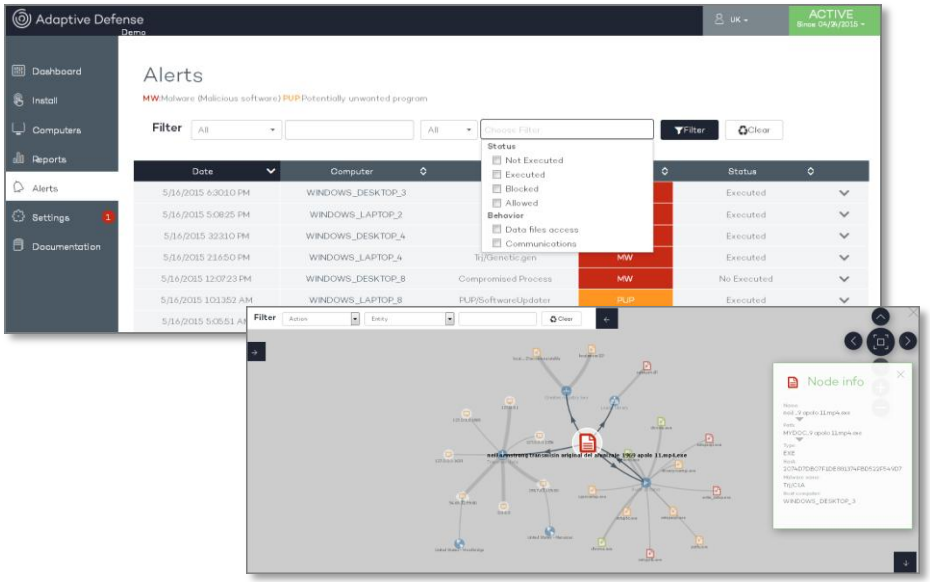
- Резервное копирование может очень негативно сказаться на производительности, но во многих случаях оно является эффективным инструментом

- Чтобы снизить эффективность систем резервного копирования, **хакеры угрожают раскрыть украденную информацию в Интернете** в том случае, если жертва не заплатит выкуп.

Panda Adaptive Defense

Решение проблем с CryptoLocker и другими усовершенствованными угрозами и угрозами «нулевого дня»

Модель Adaptive Defense

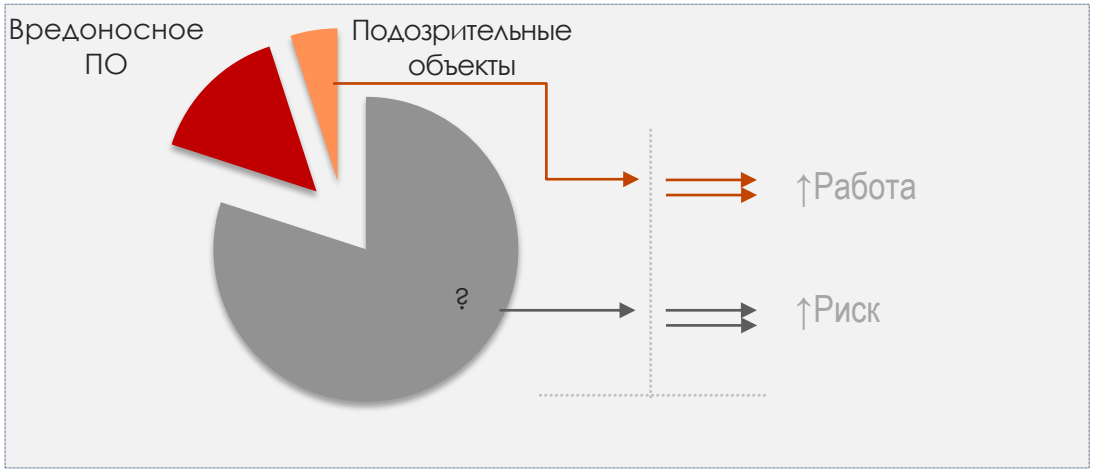


Модель основана на степени надежности, классификации файлов и контроле исполнения приложений.

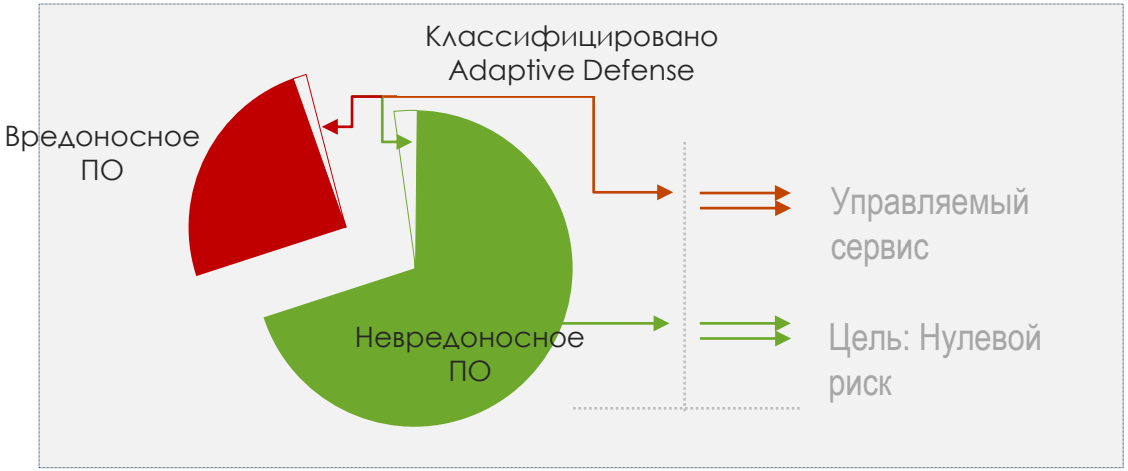
- **Аудит**
  - Только мониторинг, нет блокировки
  - Отчеты о найденных угрозах
- **Защита** (режим по умолчанию)
  - Блокирует вредоносные и неизвестные файлы из Интернета. Останавливает шифровальщики типа **CryptoLocker** и любые другие атаки нулевого дня
- **Блокировка**
  - Полная блокировка. Разрешено запускать только надежные приложения.

ВЫВОД: МЫ НИЧЕГО НЕ РАЗРЕШАЕМ ЗАПУСКАТЬ, ПОКА НЕ ЗНАЕМ ТОЧНО, ЧТО ЭТО ТАКОЕ

Традиционные антивирусы против Adaptive Defense



Традиционные антивирусные решения (могут идентифицировать вредоносные программы, но ничего более)



Adaptive Defense (мониторинг и классификация всех запущенных процессов)

CryptoLocker

Что мы видим у корпоративных клиентов?

Что мы видим у корпоративных клиентов?

Клиенты с традиционными антивирусами заражаются **CryptoLocker**

Что мы видим у клиентов с установленным Adaptive Defense?

Сервис Adaptive Defense	Текущий антивирус	Кол-во установок	**Нейтрализовано атак CryptoLocker**	Период
Куплен	Symantec Endpoint Protection	338	**62**	Последние 45 дней
Триал-версия	Panda Endpoint Protection	278	**3**	Последние 30 дней
Куплен	McAfee	2726	**49**	Последние 60 дней