Panda Adaptive Defense 360 на платформе Aether. План просмотра демо-консоли

Декабрь 2017

Содержание:

Цель настоящего документа - предоставить план просмотра демо-консоли **Aether** для управления корпоративными решениями информационной безопасности **Panda**.

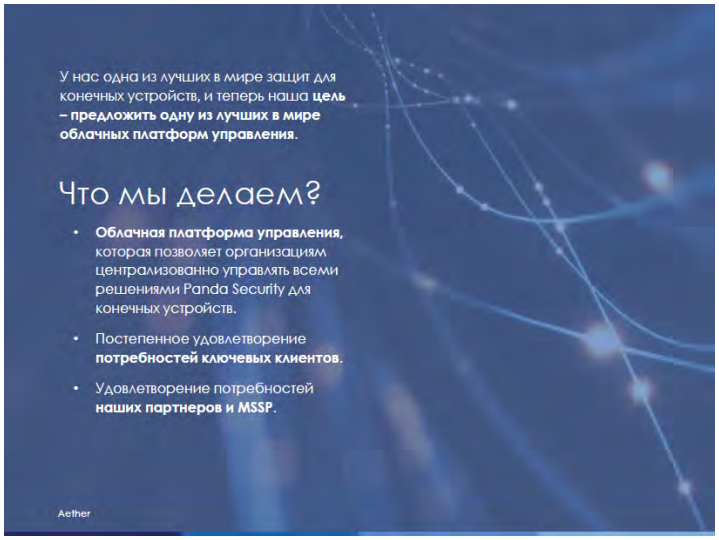
Данный план позволяет посмотреть демо-консоль в режиме работы для следующих решений безопасности Panda:
- Panda Adaptive Defense 360 with Advanced Reporting Tool and Patch Management
- Panda Adaptive Defense with Advanced Reporting Tool and Patch Management
- Panda Endpoint Protection Plus with Patch Management
- Panda Endpoint Protection with Patch Management

Если Вы точно знаете, какой продукт Вас интересует, то выберите соответствующий продукт. Если Вы еще не определились с продуктом, то рекомендуем Вам посмотреть демо-консоль в максимальном режиме работы. Для этого при подключении к демо-консоли выберите верхний продукт:
Panda Adaptive Defense 360 with Advanced Reporting Tool and Patch Management

Данный документ представлен для просмотра демо-консоли именно в максимальном режиме.

Введение

Panda обладает лучшей защитой 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 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.

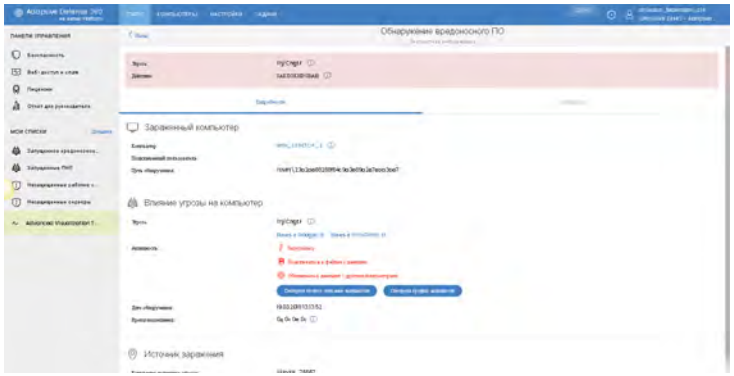
АКТИВНОСТЬ ВРЕДОНОСНОГО ПО: Этот виджет показывает информацию об угрозах (шифровальщики, направленные атаки, трояны и пр.) в реальном времени, обнаруженных защитой при попытке проникновения в систему или запуска в ней.

ДЕЙСТВИЯ:

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

Экспертный анализ вредоносного ПО

Подробности



Подробная информация

График активности

- Посмотрите список всех действий на закладке **Активность**
- Посмотрите **график активности.** Вы увидите жизненный цикл атаки 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:

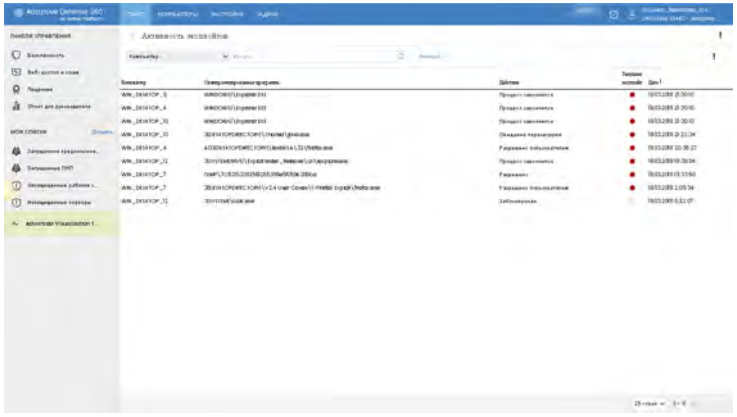
- **Trj/Generic.gen**: Вредоносное ПО, пытающееся выдать себя за "кряк" программы BeyondCompare, но в реальности оно подключается к различным IP-адресам, загружает данные и запускает разные приложения. После запуска выполняет действия с целью кражи данных и повреждения системы.
- **Trj/CryptoWall.A**: 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



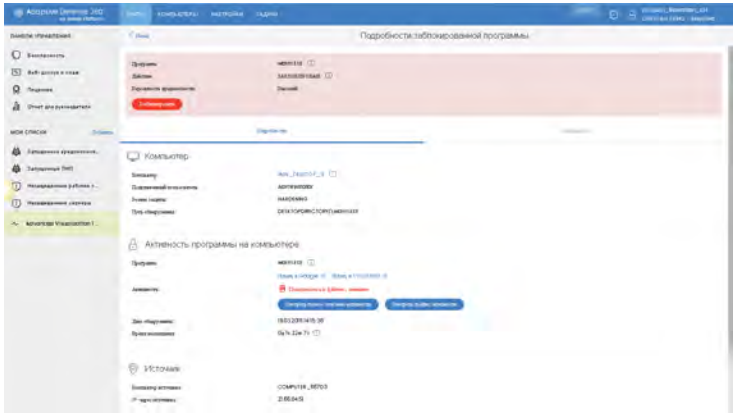
АКТИВНОСТЬ ЭКСПЛОЙТОВ: Данный виджет показывает эксплойты, обнаруженные в уязвимых процессах, запущенных пользователями.

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.

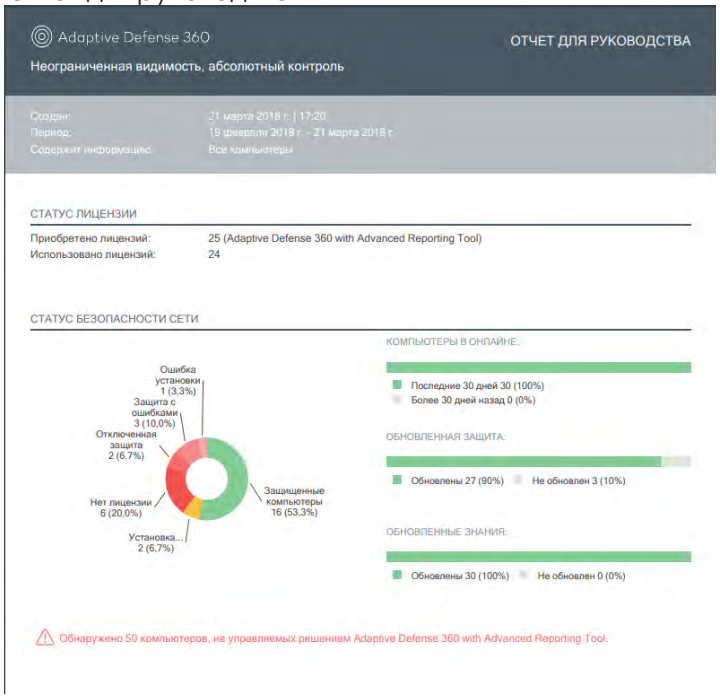
В любом случае, **Panda Adaptive Defense 360** продолжит мониторинг всех процессов, даже разблокированных, для того, чтобы ВСЕ обнаруженные программы были всегда корректно классифицированы.

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**.

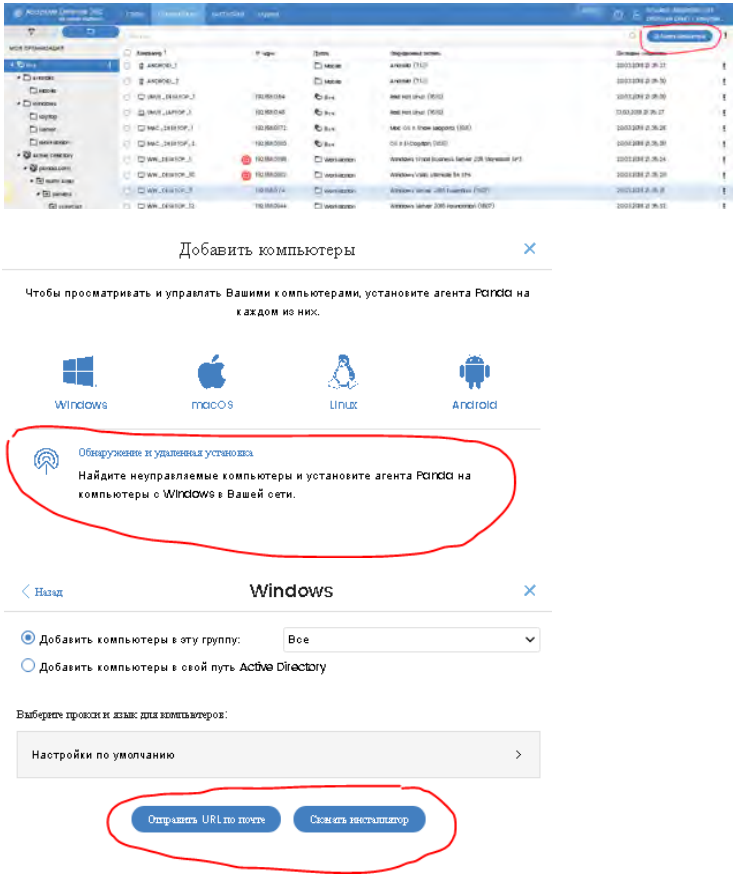
➔ Создайте новый список, содержащий обнаруженные неуправляемые компьютеры.

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**.

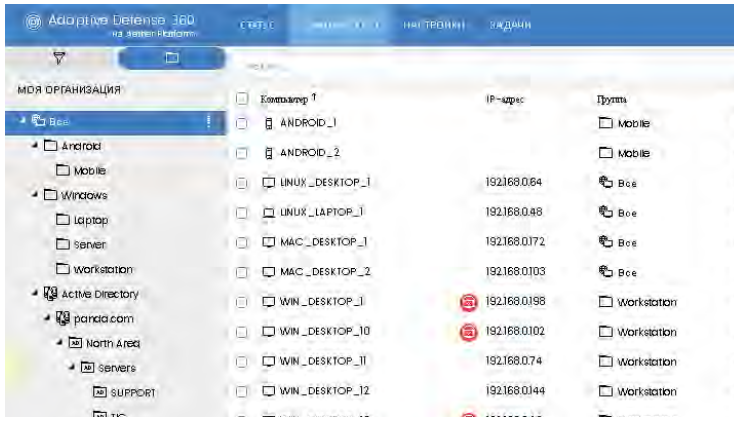
2. После первой установки объем потребления полосы составляет всего несколько КБ в день. Чтобы оптимизировать потребление полосы пропускания канала связи назначьте для каждого сегмента сети хотя бы один кеш-компьютер (**Настройки/Сетевые настройки/Кеш**).

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.

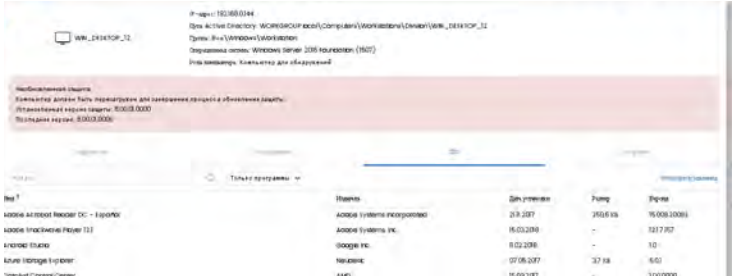
Управление компьютерами

Фильтры

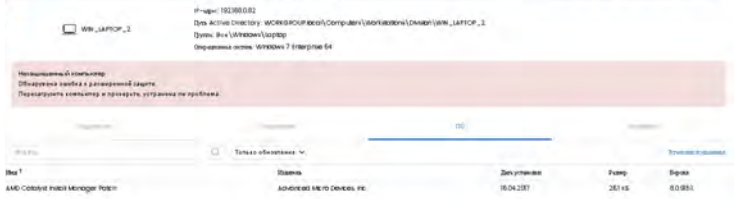
Древо компьютеров (группы и Active Directory)



Сведения об аппаратном и программном обеспечении, журнал изменений



Примененные системные патчи

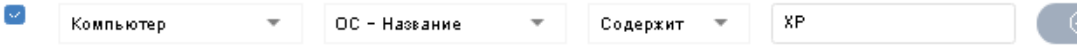


ФИЛЬТРЫ И ДРЕВО КОМПЬЮТЕРОВ

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.

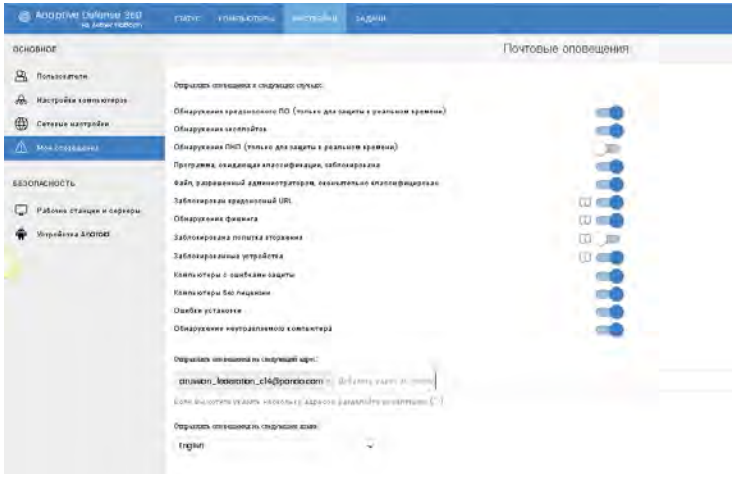
➔ Покажите информацию в разделе **ПО** у компьютера **WIN_DESKTOP_1**

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

Настройки

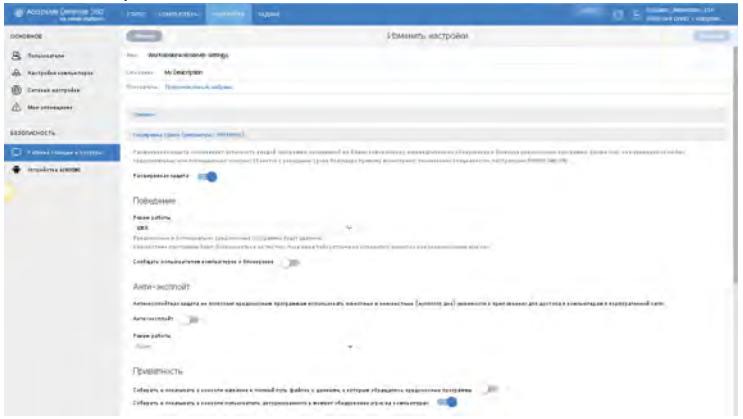
Основное

- 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.

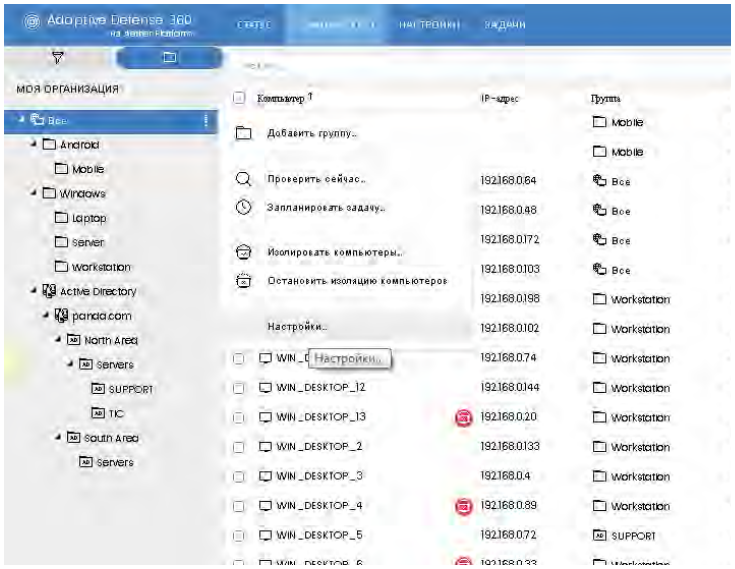
- **Устройства Android:** Позволяют вам настроить защиту ваших смартфонов и планшетов с Android 4.0 или позже. Пользователи Android имеют антивирусную защиту, а вскоре у них будет еще и защита Анти-вор (геолокация, удаленная очистка, удаленная блокировка и пр.).

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**.

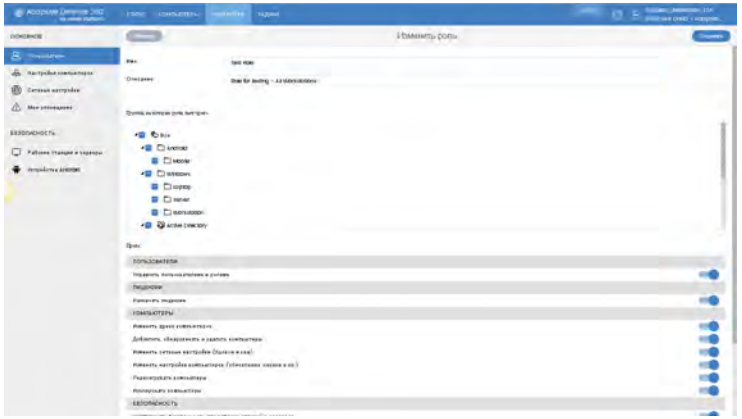
➔ Покажите, как назначать профиль настроек определенному компьютеру.

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

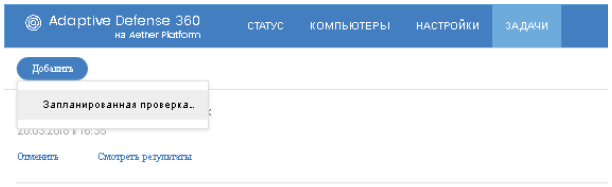
После создания новой роли вы можете назначить ее любому новому пользователю, которого вы можете создать, или существующим пользователям.

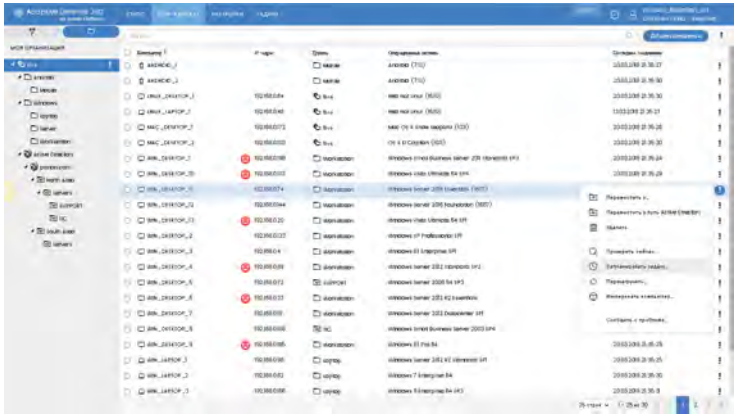
Закладка **Активность** позволяет вам видеть, кто и когда подключался к консоли (**СЕССИИ**), а также какие действия были выполнены каждым пользователем.

- 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**

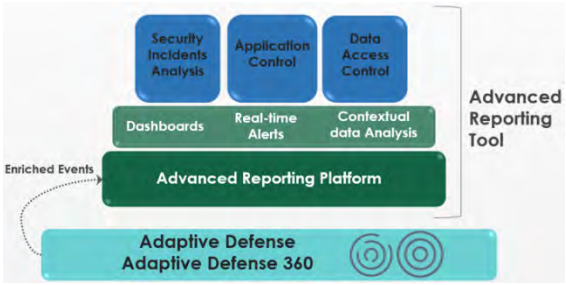
Advanced Reporting Tool

Возможности

ОБЗОР ADVANCED REPORTING TOOL
https://habr.com/company/panda/blog/312544/

КАК ДОБАВЛЯТЬ СПРАВОЧНЫЕ ТАБЛИЦЫ В ADVANCED REPORTING TOOL
https://habrahabr.ru/company/panda/blog/323850/

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:

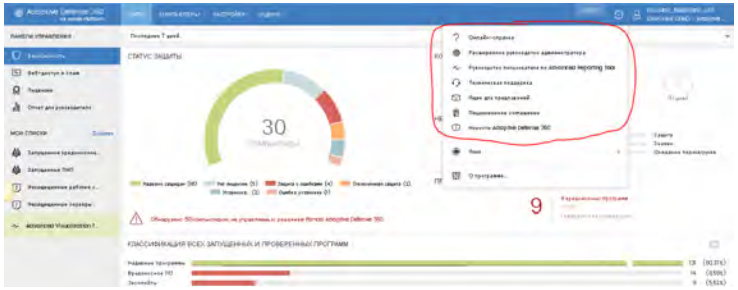
1. Экономить средства:
   - ➔ Покажите используемые лицензии (**Application Control / IT APPLICATIONS / Microsoft Office licenses in use)**
   - ➔ Покажите потребление полосы пропускания канала связи (**Application Control / BANDWIDTH-CONSUMING APPLICATIONS + + Data Access Control / OUTBOUND NETWORK TRAFFIC + Data Access Control / BANDWIDTH CONSUMERS)**
2. Видеть, что происходит на ваших компьютерах:
   - o 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**)
   - o 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

Вы посмотрели одну из лучших в мире облачных платформ Aether для удаленного и централизованного управления безопасностью конечных устройств на предприятии.

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.

В консоли Aether могут быть интегрированы дополнительные модули (например, Data Control, Patch Management и пр.), которые уже доступны пользователям или будут доступны в будущем. Все это позволяет 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 защиты для конечных устройств под управлением Windows, Linux, macOS и Android.

С этой целью мы предоставляем лучшие 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.

СПАСИБО!

PANDA SECURITY В РОССИИ И СНГ

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

www.cloudav.ru
www.pandasecurity.com