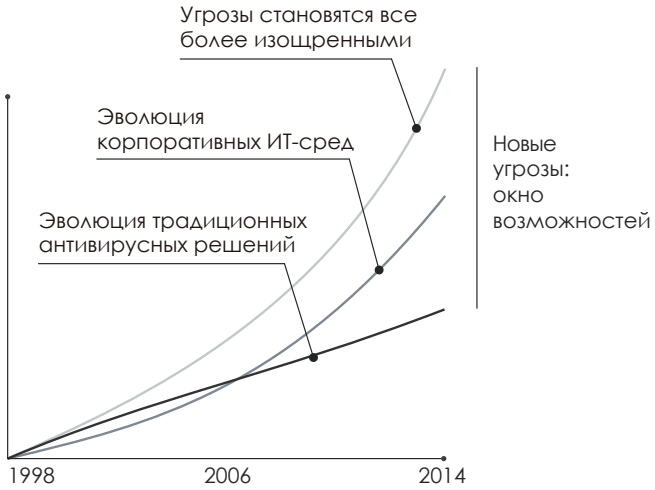
Panda Adaptive Defense

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 300 000 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 девять лет работаем 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