Panda Patch Management

Сократите риски и упростите управление уязвимостями в системах и сторонних приложениях

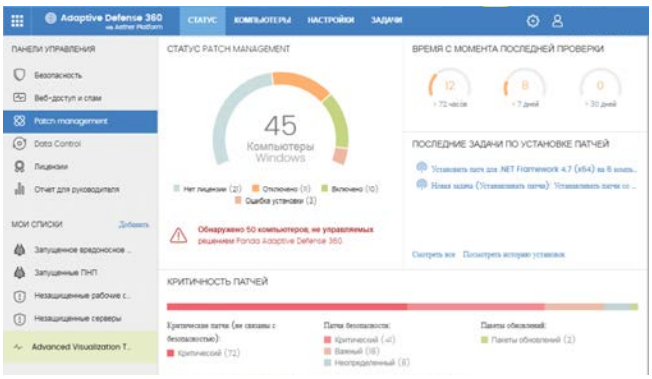
Сегодня 99,96% активных уязвимостей на корпоративных конечных устройствах связаны с отсутствием обновлений, которые, если бы были установлены, значительно сократили риски безопасности. Кроме того, 86% корпоративных устройств не имеют критических патчей для таких сторонних приложений как Java, Adobe, Mozilla, Firefox, Chrome, Flash и OpenOffice, помимо прочих[1].

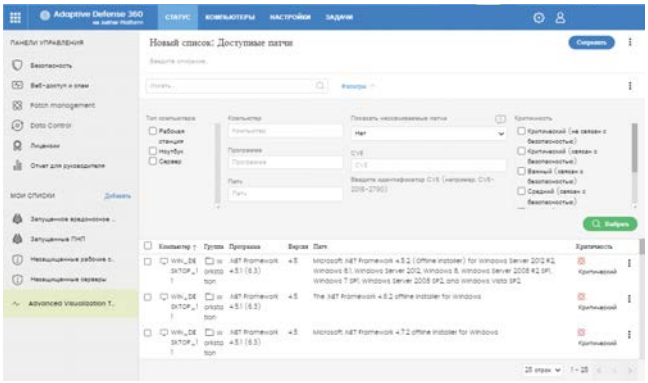
Если такая тенденция сохранится, то к 2020 году 99% уязвимостей, вызывающих инциденты безопасности, будут известными эксплойтами, которых можно было бы легко избежать за счет применения патчей до инцидента[2].

ПРИШЛО ВРЕМЯ ИЗМЕНИТЬ ЭТУ ТЕНДЕНЦИЮ: PANDA PATCH MANAGEMENT

Panda Patch Management - это удобное решение для управления уязвимостями операционных систем и сторонних приложений на рабочих станциях и серверах с Windows. Оно снижает риски при одновременном усилении возможностей Вашей организации по предотвращению, сдерживанию и сокращению поверхности атаки.

Решение не требует внедрения новых агентов на компьютерах или консоли управления, т.к. оно полностью интегрировано в решения Panda Security по защите конечных устройств. Плюс решение в реальном времени предоставляет централизованную видимость статуса безопасности программных уязвимостей, недостающих патчей, обновлений и неподдерживаемого (EOL˜) ПО внутри корпоративной сети и за ее пределами, а также легкие в использовании инструменты для всего цикла управления патчами в реальном времени: от обнаружения и планирования до установки и мониторинга.





УЯЗВИМОСТИ: СКРЫТЫЙ РИСК

Необновленные **операционные системы и сторонние приложения** обеспечивают идеальную среду для хакеров и эксплойтов, чтобы воспользоваться известными уязвимостями, для которых патчи стали доступны недели или даже месяцы до инцидента.

Массовое раскрытие информации об уязвимостях (например, раскрытых Shadow Brokers или WikiLeaks) с подробными инструкциями о том, как взломать системы и приложения, способствует значительному росту числа кибер-преступников, запускающих атаки.

Цифровая трансформация усложняет процесс сокращения поверхности атаки из-за растущего числа пользователей, устройств, систем и сторонних приложений, требующих обновлений.

Как минимум **пять общих операционных проблем мешают** программам управления уязвимостями (VM):

- **Процесс обнаружения уязвимостей занимает много времени**. Однако в случае инцидента ответ должен быть мгновенным.
- **Компании децентрализованы**, сотрудники не всегда подключены к корпоративной сети. **Локальные VM-инструменты** не охватывают такие сценарии.
- Для большинства VM-средств требуются **свои специальные агенты** на компьютерах, которые и так уже перегружены.
- VM-средства Microsoft не позволяют компаниям обновлять **сторонние приложения** централизованно и унифицированно.
- Другие решения безопасности, которые предлагают управление патчами, **не осуществляют корреляцию между обнаружениями и уязвимыми конечными устройствами** для ускорения реагирования и смягчения последствий атаки.

[1] National Vulnerability Database. Критические обновления сторонних приложений применяются только на 14% корпоративных конечных устройств и серверов
[2] Gartner: How to Respond to the 2018 Threat Landscape. Greg Young. Опубликовано 28 ноября 2017 г.
˜EOL (End-of-Life) - продукт, который находится в конце своего жизненного цикла (с точки зрения производителя), который в дальнейшем может уже не получать обновления безопасности

Panda Patch Management

ВЫГОДЫ

Panda Patch Management в рамках **единого удобного решения** позволяет:

- **Выполнять аудит, мониторинг и расставлять приоритеты обновлений операционных систем и приложений**. Решение обеспечивает оперативную и сводную информацию о статусе безопасности компании в отношении уязвимостей, патчей и ожидающих обновлений систем и сотен приложений.
- **Предотвращать инциденты, систематически сокращая поверхность атаки, создаваемой уязвимостями ПО.** Обработка патчей и обновлений с помощью простых в использовании инструментов управления в реальном времени, позволяющие опережать атаки с использованием уязвимостей.
- **Сдерживать и устранять атаки, использующие уязвимости,** за счет мгновенных обновлений. Консоль Panda Adaptive Defense 360 в сочетании с Patch Management позволяет компаниям сопоставлять обнаруженные угрозы и эксплойты с обнаруженными уязвимостями. Сокращается время реакции, сдерживая и устраняя атаки за счет немедленного внедрения патчей из веб-консоли. Кроме того, пострадавшие компьютеры могут быть изолированы от остальной сети, предотвращая распространение атаки.
- **Сокращать операционные расходы**
  - **Panda Patch Management не требует внедрения или обновления любых новых или существующих агентов на компьютерах**, упрощая управление и избегая перегрузки рабочих станций и серверов.
  - **Упрощает внедрение патчей, т.к. обновления запускаются удаленно** из облачной консоли. Оптимизирован процесс установки для сокращения ошибок.
  - **Предоставляет полную автоматическую видимость всех уязвимостей**, ожидаемых обновлений и приложений с EoL[3] сразу после активации.
- **Соблюдать принцип подотчетности,** предусмотренный во многих регламентах (GDPR, HIPAA и PCI). Заставляет компании предпринимать соответствующие технические и организационные меры для обеспечения надлежащей защиты конфиденциальных данных, находящихся под их контролем.

Panda Patch Management усиливает возможности решений Panda Security для конечных устройств по предотвращению, обнаружению и реагированию, обеспечивая надежное внедрение архитектуры адаптивной безопасности[4]

КЛЮЧЕВЫЕ ФУНКЦИИ

Panda Patch Management предоставляет все необходимые инструменты для управления безопасностью и обновлениями операционной системы и сторонних приложений из единой консоли.

Обнаружение:
Информация в реальном времени по всем уязвимым компьютерам, ожидаемым патчам и ПО без поддержки (EOL[3]) ПО с их статусом исправления.

- Подробная информация о патчах и ожидаемых обновлениях со сведениями из соответствующего бюллетеня безопасности, информация по группе и компьютеру и пр. Доступные действия:
  - Фильтрация и поиск патчей по критичности, компьютеру, группе, приложению, патчу, CVE ID и статусу.
  - Действия на самих компьютерах: перезагрузка, установка сразу или по расписанию.
- Настраиваемые оповещения при обнаружении уязвимых рабочих станций или серверов.
- Автоматическая проверка ожидаемых обновлений в реальном времени или каждые 3, 6, 12 или 24 часа.
- При обнаружении эксплойтов - уведомление об ожидаемых обновлениях. Возможность из консоли запускать установку сразу же или по расписанию, изолируя при необходимости компьютер.

Планирование обновлений и задачи по установке:

- Настройки по критичности и приложению.
- Можно выполнять для определенных ПК и групп.
- Выполнение немедленно или по расписанию (разово или многократно с определенной периодичностью по времени/датам).
- Возможность контролировать перезагрузки компьютеров и устанавливать исключения.
- Отмена установки патча, способного вызвать непредвиденный конфликт с текущей конфигурацией.

Мониторинг статуса устройств и обновлений через:

- Панель мониторинга и журналы действий.
- Высокоуровневые и подробные отчеты.
- Списки обновленных компьютеров, компьютеров с ожидаемыми обновлениями, с ошибками.

Гибкое управление на основе групп и ролей с различными правами:

- Видимость уязвимых компьютеров, патчей и сервис-паков в зависимости от роли пользователей.

Централизованный контроль обновлений, патчей и ПО:

- Возможность отключения Windows Update и централизованное управление обновлениями операционной системы.
- Возможность исключения патчей Windows Update и централизованное управление обновлениями операционной системы.
- Возможность исключить ПО (например, Java).

Совместимые решения на платформе Aether:

Panda Endpoint Protection | Panda Endpoint Protection Plus
Panda Adaptive Defense | Panda Adaptive Defense 360

Требования по установке Panda Patch Management
http://go.pandasecurity.com/patch-management/requirements

Поддерживаемые сторонние приложения
www.pandasecurity.com/business/PatchManagementApp

[4] Gartner: "Designing an Adaptive Security Architecture for Protection from Advanced Attacks", Neil MacDonald, Peter Firstbrook

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