Panda Patch Management

Сократите риски и упростите управление уязвимостями в системах и сторонних приложениях

panda
a WatchGuard brand

Сегодня **99,96% активных уязвимостей** на корпоративных конечных устройствах вызваны **отсутствием обновлений**[1]. Если бы они были установлены, то они значительно сократили бы риски безопасности. На самом деле, по данным Ponemon Institute[2]**, 57% жертв** кибер-атак заявили, что **применение патчей предотвратило бы атаки** на них, а 34% заявили, что они знали об уязвимости еще до атаки.

Более того, **86% уязвимостей** вызваны такими **необновленными приложениями**, помимо прочих, как Java, Adobe, Firefox, Chrome, Flash и OpenOffice[1].

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.

Решение также **в реальном времени предоставляет централизованную видимость** статуса безопасности **программных уязвимостей**, недостающих патчей, обновлений и неподдерживаемого ПО (EOL[3]) 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.

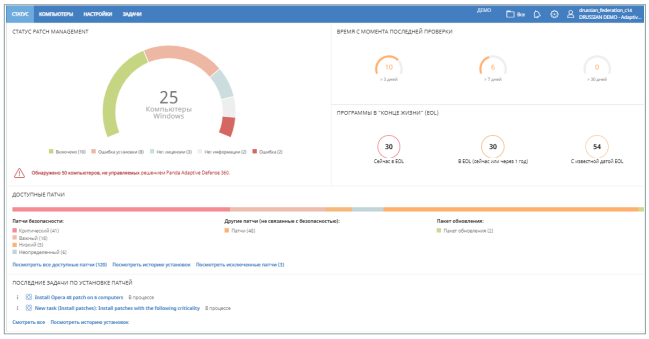

Рис. 1: Статус Patch Management - главная панель

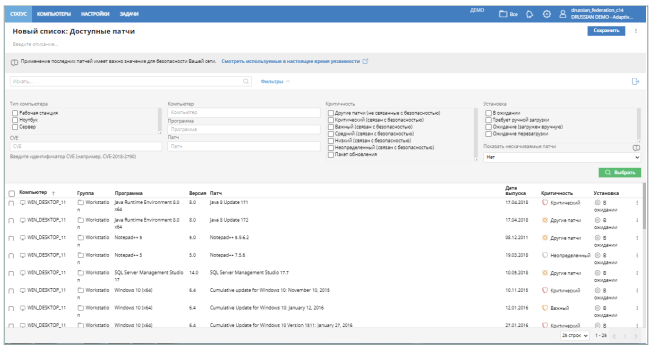

Рис. 2: Patch Management - доступные патчи

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.

Не менее **пяти общих операционных проблем мешают** программам управления уязвимостями (VM):

- **Процесс обнаружения уязвимостей занимает много времени**. Однако в случае инцидента ответ должен быть мгновенным.
- **Компании децентрализованы**, т.к. 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 уязвимостями** на конечных устройствах для ускорения процесса реагирования и смягчения последствий атаки.

Совместимые решения на ПЛАТФОРМЕ AETHER:

Panda Endpoint Protection | Panda Endpoint Protection Plus

Panda Adaptive Defense | Panda Adaptive Defense 360

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

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

[1] Gartner, Focus on the Biggest Security Threats, Not the most Publicized. Опубликована: 2 ноября 2017 г. Уязвимости "нулевого дня" составляют всего 0,4%, а для остальных 99,96% уязвимостей доступны патчи для их устранения. National Vulnerability Database. 86% уязвимостей найдены в сторонних приложениях.

[2] Cost and consequences of gaps in vulnerability response – Ponemon

[3] EOL (End-of-Life): Продукт, у которого закончился период "жизни", когда он был полезен (с точки зрения производителя), и для него не выпускаются обновления безопасности.

panda
a WatchGuard brand

ПРЕИМУЩЕСТВА

В рамках **единого решения**, Panda Patch Management позволяет Вам:

- **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 в ПО**. Управление патчами и обновлениями в реальном времени с помощью простых в использовании инструментов позволяет опережать атаки с использованием уязвимостей.
- **Сдерживать и устранять атаки, использующие уязвимости**, за счет мгновенных обновлений. Консоль управления Aether решений безопасности Panda в сочетании с Patch Management позволяет компаниям сопоставлять обнаруженные угрозы и эксплойты с обнаруженными уязвимостями. Сокращается время реакции, сдерживания и устранения атаки за счет немедленного внедрения патчей из веб-консоли. Кроме того, пострадавшие компьютеры могут быть изолированы от остальной сети, что предотвращает распространение атаки.
- **Сокращать операционные расходы:**
  - **Patch Management не требует внедрения или обновления любых новых или существующих агентов** на компьютерах, что упрощает управление и препятствует перегрузке 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]) с их статусом патчинга.
- Подробная информация о патчах и ожидаемых обновлениях со сведениями из соответствующего бюллетеня безопасности (CVE), информация по группе и компьютеру, и пр. Доступные действия:
  - Фильтрация и поиск патчей по критичности, компьютеру, группе, приложению, патчу, CVE и статусу.
  - Перезагрузка компьютеров, установка на них патчей сразу или по расписанию.
- Автоматическая незаметная проверка ожидаемых обновлений в реальном времени или каждые 3, 6, 12 или 24 часа.
- Уведомление об ожидаемых обновлениях при обнаружении эксплойтов. Возможность из консоли запускать установку патчей сразу же или по расписанию, изолируя при необходимости компьютер.

Планирование обновлений и задачи по установке:

- Настройки по критичности.
- Для определенных конечных устройств и групп.
- Мгновенно или по расписанию разово или с определенной периодичностью (дата/время).
- Возможность контролировать перезагрузки компьютеров и устанавливать исключения.
- Отмена установки патча, способного вызвать непредвиденный конфликт с существующей конфигурацией.

Мониторинг статуса устройств и обновлений через:

- Панель мониторинга и списки.
- 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 определенных патчей по версии/типу.
- Возможность исключения определенного ПО (например, Java).

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

WatchGuard

В МИРЕ +1 (206) 613-08-95 В РОССИИ И СНГ +7 (495) 105-94-51 watchguard.com | pandasecurity.com | cloudav.ru