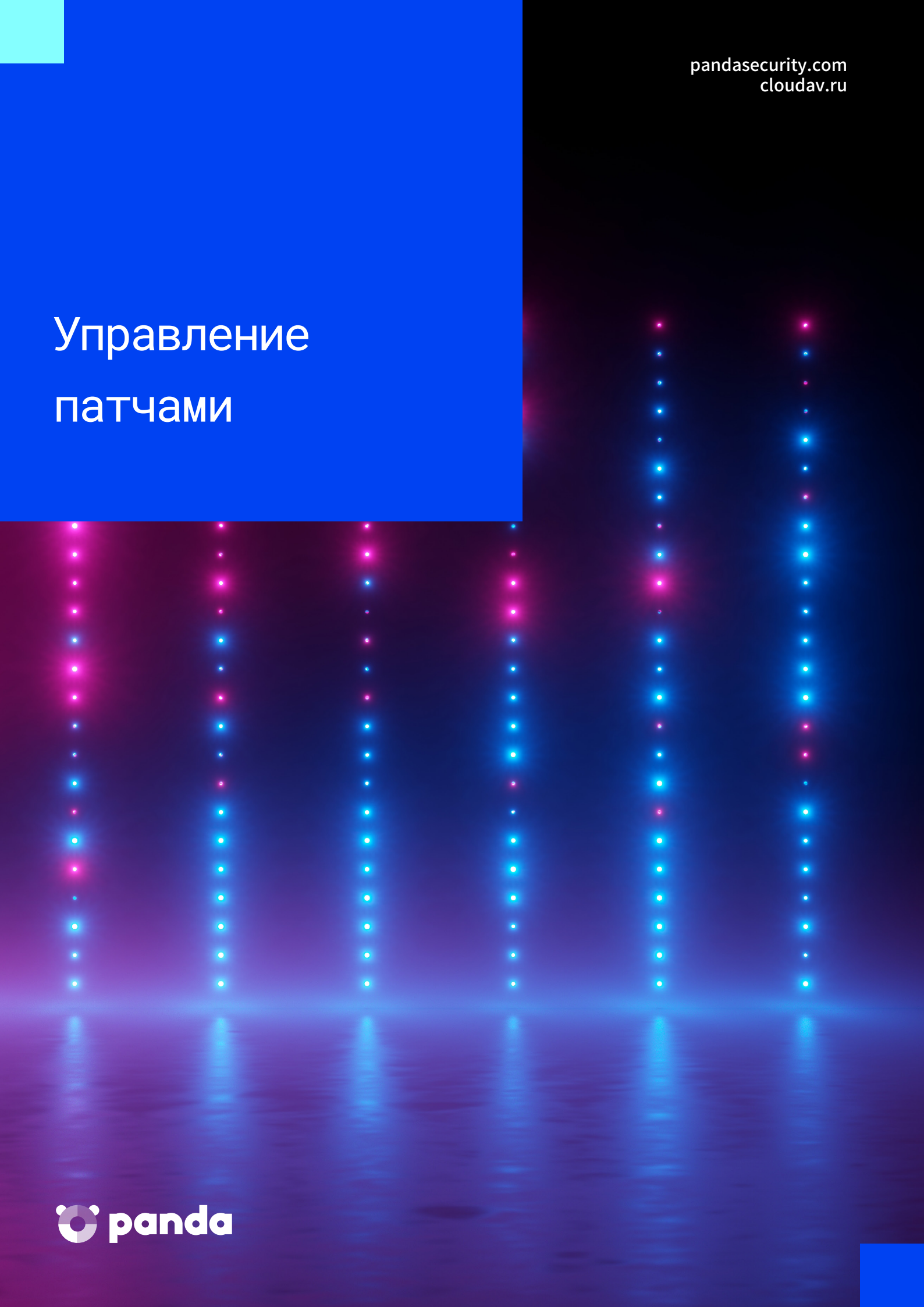
pandasecurity.com
cloudav.ru

Управление патчами

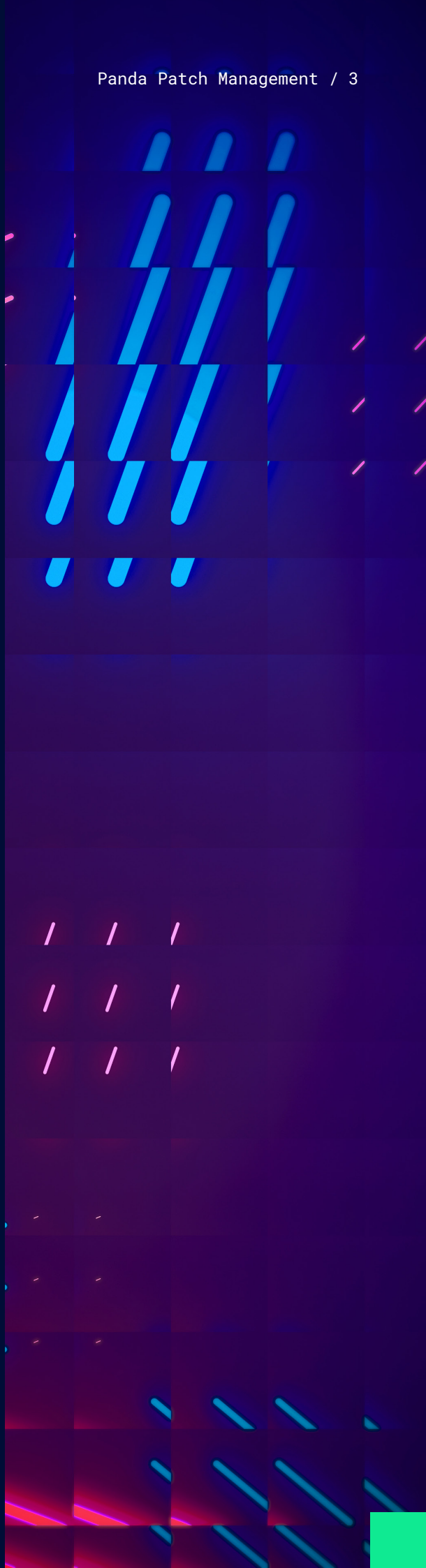


Содержание :

|Необходимость управления патчами в компаниях

Обновление ПО, как правило, представляет проблему для ИТ-администраторов. Определение приоритетов и их внедрение - это трудоемкая задача, причем не только для них, но и для пользователей тоже: необходимо перезагружать компьютеры и серверы, что приводит к остановкам в работе. Очень часто по этой причине установка обновлений откладывается, а рекомендуемые патчи игнорируются. Впрочем, то, что может показаться невинным действием, фактически может иметь очень серьезные последствия для организаций.

Кроме того, ИТ-администраторы могут испытывать серьезные трудности с обеспечением того, чтобы на всех системах в их сети были установлены все требуемые патчи и обновления. Однако они имеют решающее значение в том случае, если требуется обеспечить надежную защиту организации от ИТ-угроз, поскольку своевременное обновление установленного ПО сводят к минимуму уязвимость ПО и систем перед угрозами безопасности.



|Статистика по уязвимостям

В 2019 году количество зарегистрированных уязвимостей безопасности составил **12174**. Учитывая эту статистику, неудивительно, что организациям с ограниченными ИТ-ресурсами крайне трудно поддерживать и защищать свою инфраструктуру.

Управление патчами - это задача, которая может потребовать достаточно много времени и ресурсов, и часто бывает трудно получить актуальный список Ваших ИТ-активов и приложений, определить приоритеты среди патчей, и даже быстро обновить критические программы и системы. Компании должны уметь управлять патчами максимально эффективно, иначе они могут столкнуться с серьезными проблемами производительности и информационной безопасности.

24.1%[1] уязвимостей приходятся на решения всего пяти компаний: Software in the Public Interest (SPI), SUSE, Oracle, IBM и Microsoft.

Наиболее широко используемые сторонние приложения являются основной мишенью для хакеров. Согласно индексу общеизвестных уязвимостей и рисков (Common Vulnerabilities and Exposures, CVE[2]), наибольшее число уязвимостей имеют такие приложения как Java, Adobe, Google Chrome, Mozilla Firefox и OpenOffice. Поэтому уже недостаточно обновлять только операционную систему.

Еще один фактор, который следует учитывать, - это рост числа хакеров, обладающих необходимыми для быстрого обнаружения уязвимостей навыками. После их обнаружения они внедряют программы, которые автоматизируют использование этих новых уязвимостей - причем все это делается быстро и с максимально возможным охватом. Результат такого сочетания угроз, уязвимостей и последствий от них представляет серьезный риск для компаний. Однако именно нераскрытые уязвимости несут наибольшую опасность.

panda

Источники:
1. Cybersecurity alert – TechRepublic
2. attack.mitre.org – MITRE

Известные уязвимости, уязвимости с высоким риском

В настоящее время использование уязвимостей по-прежнему является главной причиной большинства нарушений безопасности. Все еще свежи в памяти печально известные случаи с **WannaCry, Petya** и **BlueKeep**, которые посеяли хаос во всем мире. Лишь небольшое число атак происходит в результате действительно неизвестных уязвимостей (атаки нулевого дня), но большинство из них вызваны известными уязвимостями.

По данным Gartner[3], в нынешнем 2020 году 99% уязвимостей на момент возникновения инцидента будут известны для специалистов по безопасности и ИТ-администраторов. А вот на долю уязвимостей нулевого дня приходится порядка 0,4% от числа уязвимостей за последнее десятилетие.

Важно помнить, что хакеры также имеют доступ к известным эксплойтам для осуществления своих атак, и они несомненно будут их использовать, т.к. знают, что большинство компаний не обновляют свои системы своевременно. Фактически, 80% успешных атак использовали уязвимости, для закрытия которых уже были доступны патчи, но они не были применены.

В свете этих фактов становится ясно, что компании должны сосредоточить свои усилия на контроле и смягчении риска известных уязвимостей, которые снова и снова могут эксплуатироваться. Как видим, они представляют собой большую опасность, чем другие виды угроз.

Время между обнаружением уязвимости и ее использованием также существенно сократилось, что вынуждает компании внедрять патчи и обновления быстрее, чем кибер-преступники смогут скомпрометировать их системы, используя различные векторы атак.

> 57% жертв кибер-атак говорят, что применение патча могло предотвратить атаку. 34% сказали, что они знали об уязвимости еще до атаки[4].

Источники:
3. Focus on the Biggest Security Threats, Not the most Publicized – Gartner
4. Cost and consequences of gaps in vulnerability response – Ponemon

| Управление патчами

a) Что подразумевает управление патчами

Это процесс, с помощью которого ИТ-отделы организаций скачивают и устанавливают патчи и обновления (изменения в коде или данных), предназначенные для обновления, оптимизации или защиты ПО, компьютеров, серверов и ИТ-систем. Это необходимо для обеспечения корректности работы этих компонентов и закрытия имеющихся в них уязвимостей. Хотя это может показаться простой задачей, большинство компаний затрудняются определить, какие критические патчи и обновления им необходимо устанавливать в первую очередь. Таким образом, приоритеты среди патчей является ключевым вопросом для администраторов. Фактически, согласно данным от Ponemon, среднее время, необходимое компаниям для обновления приложений и систем, составляет 102 дня[5]. Но среднее время, в течение которого появляются атаки, использующие критически уязвимости безопасности, составляет всего 43 дня[6], а это означает, что в среднем **"окно риска"** составляет **59 дней.**

Источники:
5. State of Endpoint security risk 2018 – Ponemon
6. Cost and consequences of gaps in vulnerability response – Ponemon

б) Какие существуют типы патчей?

Существуют различные виды патчей, и каждый из них разработан с определенной целью: исправить ошибку или закрыть определенную уязвимость. Вот лишь некоторые примеры: хотфиксы, сервис-патчи, версии продуктов, Monkey-патчи и пр.

В данном документе мы рассмотрим два типа, которые считаем наиболее важными, т.к. их цель - закрыть критические уязвимости безопасности, которые обычно используются злоумышленниками и поэтому являются наиболее актуальными для компаний и экспертов по безопасности.

- **Патчи безопасности - влияют как на операционные системы, так и на сторонние программы.** Патч безопасности - это изменение, внесенное в приложение или программу для исправления ошибок или недостатков, которые вызывают уязвимости. Применение таких патчей предотвращает или сокращает возможности угроз использовать уязвимости в ПО. Управление патчами - это часть управления уязвимостями, т.е. постоянной работы по идентификации, классификации, устранения и смягчения уязвимостей (рисков безопасности).
- **Сервис-пак (Service Pack, SP)** или **Пакет функций (Feature Pack, FP)**. Это важные обновления, которые включают в себя набор обновлений, исправлений ошибок или улучшений функций программы. Как правило, они решают множество задач, и обычно они содержат патчи, хотфиксы, исправления и патчи безопасности, которые были выпущены ранее.

в) Для какой цели служат патчи

Патчи предназначены для устранения уязвимостей или ошибок/брешей в системе безопасности, выявленных после выхода программы.

Необновленное программное обеспечение может подвергать все конечные устройства риску со стороны эксплойтов, что предоставляет хакерам прекрасную возможность для успешного проведения своих атак. Программные патчи являются важным компонентом в работе ИТ-администраторов и специалистов по безопасности.

В технологическом секторе, а точнее - в секторе программного обеспечения, часто бывает так, что после выхода приложения требуется исправить в нем ошибки, доработать или даже изменить. В связи с этим рекомендуется разработать процесс, аналогичный жизненному циклу ПО, когда устанавливаются различные этапы для проведения анализа, оценки и регулярного применения патчей для устранения любых возникающих проблем.

|Жизненный цикл управления патчами

При грамотном внедрении управление патчами может быть наиболее эффективным инструментом для защиты Вашей компании от уязвимостей и наименее затратным в обслуживании. В этом разделе мы объясним, как создать процедуру управления патчами для ее интеграции в стандартные операции Вашей компании. В этом цикле (процедуре) выделим шесть этапов[7]:

Идентификация устройств и базового ПО:

Идентификация устройств и установленного на них базового ПО, а также их уровень обновления, - это сложная задача, но ее решение повышает безопасность и производительность. Это позволяет Вам вносить изменения в систему без рисков и делает возможным возврат к предыдущему известному функциональному состоянию, если при установке обновления или патча возникнет проблема.

Доступность:

Текущий список патчей должен быть проверен с учетом инвентаризации устройств и ПО, чтобы определить, какие патчи на какие устройства требуется устанавливать.

Применимость:

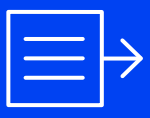
Опубликованные патчи не всегда действительны для всех устройств. Это означает, что важно проверить, подходит ли конкретное обновление для устройств в Вашем процессе.

Получение:

Не всегда легко получить файл обновления из официального источника, как и проверить его легитимность. Использование хэшей не является обычной практикой для патчей, связанных с системами управления.

Валидация:

Цель валидации - проверить, что обновление не окажет негативного влияния на процесс. Чтобы проверить патч или обновление, требуется использовать тестовое устройство до этапа внедрения. Валидация позволяет оценить, какие последствия может иметь обновление, какие могут потребоваться изменения в политики файервола, изменения настроек и пр.



Внедрение:

В процессе валидации необходимо создать пакет для внедрения. Он должен содержать файлы обновления и инструкции по установке, а также список устройств, где необходимо внедрить этот пакет обновлений.

Источник:
7. Patch management in control systems – INCIBE-CERT

|Panda Patch Management: защита от известных уязвимостей в Вашей ИТ-инфраструктуре

Panda Patch Management - это решение, которое устраняет сложности в жизненном цикле управления патчами для операционных систем и стороннего ПО. В результате этого значительно сокращается поверхность атаки и усиливается способность предотвращать и сдерживать инциденты, которые вызваны уязвимостями в системе.

Это решение интегрировано в решения компании Panda Security для обеспечения безопасности конечных устройств, и значит, что не требуются дополнительные агенты или консоли управления. Решение в реальном времени предоставляет централизованную видимость статуса уязвимостей, патчей, ожидаемых обновлений и неподдерживаемого ПО (EoL) на компьютерах и серверах внутри и за пределами корпоративной сети. Его инструменты управления позволяют Вам автоматизировать процессы обнаружения, планирования, установки и мониторинга критических патчей и обновлений, требуемых в Вашей организации - все это в реальном времени в простом и интуитивно понятном формате.

Основные преимущества и функции Panda Patch Management:

- Возможность **аудита, мониторинга** и **определения приоритетов обновлений** для операционных систем и приложений. Позволяет Вам видеть статус ожидаемых патчей и обновлений для системы и сотен сторонних приложений, а также иметь возможность отменить применение патчей.
- **Предотвращение инцидентов** за счет систематического сокращения поверхности атак, вызванных уязвимостями. Управление патчами и обновлениями позволяет Вам опережать эксплойты уязвимостей.
- **Сдерживание и смягчение атак, которые используют уязвимости** за счет оперативного применения критических обновлений из облачной консоли. Консоль сопоставляет обнаружения с уязвимостями, сводя к минимуму время реагирования, сдерживания и восстановления, применяя по мере необходимости из консоли управления соответствующие патчи. Более того, консоль позволяет Вам изолировать от сети требуемые компьютеры, сдерживая реальные и потенциальные атаки.
- **Снижение операционных расходов**, т.к. решение не требует внедрения новых агентов или обновлений на конечных устройствах, **упрощая управление** без дополнительной нагрузки на компьютеры и серверы. **Сведите к минимуму Ваши усилия по удаленному внедрению обновлений** из облачной консоли. **Оперативная и автоматическая видимость** уязвимостей, обновлений, патчей и неподдерживаемого ПО.

Управление патчами - это процесс, который должен выполняться регулярно, и он должен быть максимально комплексным для достижения высокой эффективности. Но это не означает, что ко всем системам следует относиться одинаково - каждая компания должна расставить свои приоритеты и обеспечить защиту наиболее важных и критических устройств в первую очередь.

Тем не менее, важно обеспечить внедрение патчей на всех машинах, а не только на наиболее ценных и важных для предприятия. Более того, патчи требуют действий не только со стороны системных администраторов, но и поддержку руководства для согласования времени и графика их внедрения.

Защита от атаки

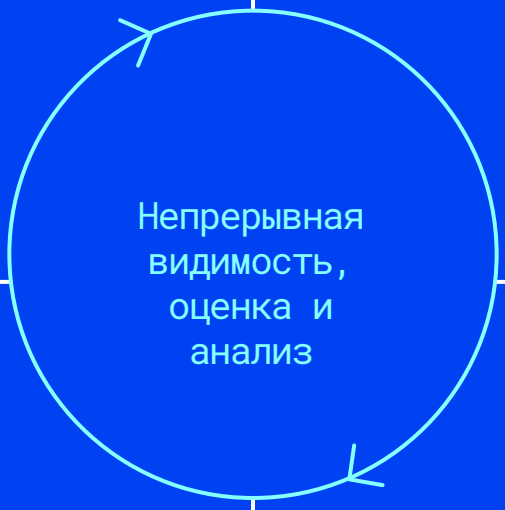
Адаптивная архитектура безопасности

Прогноз/ Предвосхищение

Обнаруживайте уязвимости, ожидаемые патчи и обновления, EoL-приложения.

Предотвращение

Автоматизируйте график внедрения патчей. Меняйте EoL-приложения.



Реагирование

Патчинг всех уязвимых конечных устройств.

Обнаружение и сдерживание

Сдерживание атак за счет патчинга в реальном времени.

Узнайте, как Panda Patch Management может помочь Вам упростить управление уязвимостями с помощью управления обновлениями и патчами безопасности.

Подробнее о Panda Patch Management