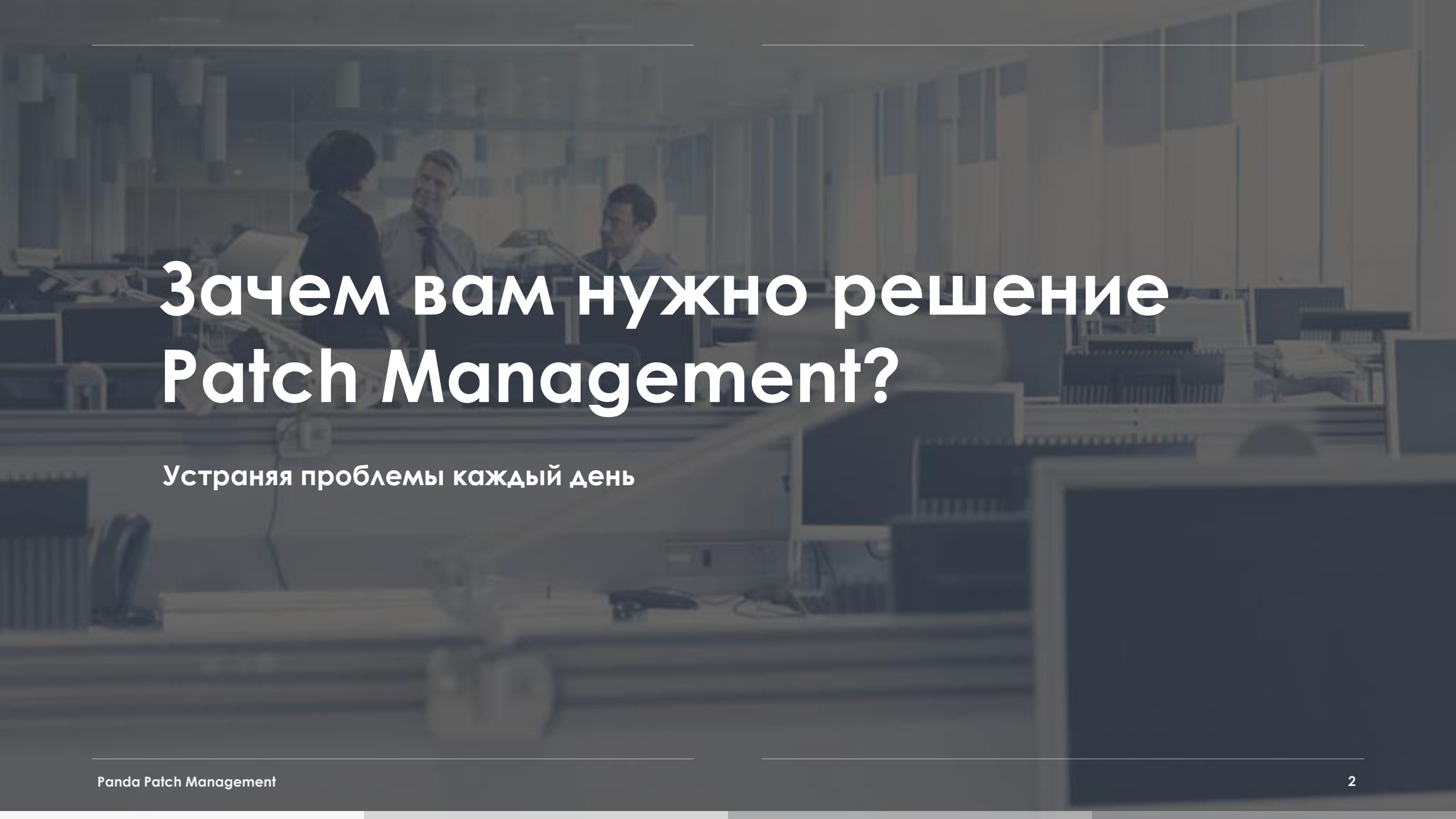
Panda Patch Management

Производительные ИТ-инфраструктуры без уязвимостей



Зачем вам нужно решение Patch Management?

Устраняя проблемы каждый день

РАСТУЩАЯ СЛОЖНОСТЬ

программных инструментов.

Разработка продуктов происходит все быстрее, каждый производитель предлагает все больше продуктов и разнообразных версий.

В 2017 году зарегистрировано **20 000 уязвимостей и дыр безопасности**, что на **38% больше, чем за предыдущие 5 лет**.

(Источник: **Vulnerability Review 2018)**

Уязвимое ПО – это не только проблема Microsoft:

86%

86% дыр безопасности найдены в **сторонних приложениях** (Adobe, Java, Chrome и т.д.).

(Источник: **National Vulnerability Database)**

16,6% уязвимостей классифицированы как **критические** и **0,3% - как чрезвычайно критические.**

(Источник: **Vulnerability Review 2018)**

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗ ОБНОВЛЕНИЙ
компрометирует безопасность компании.

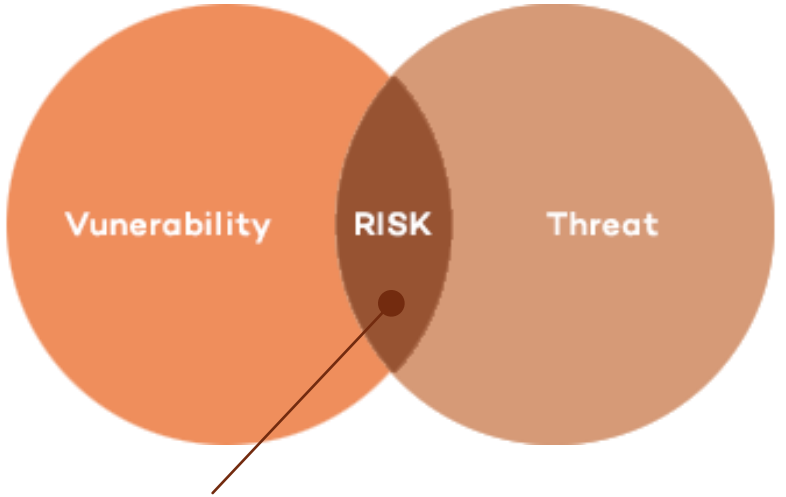
Хакеры эксплуатируют уязвимости в необновленных программах.

70%

70% Интернет-атак заражают компьютеры, эксплуатируя уязвимости в **установленном ПО**!

80%

Свыше 80% всех успешных кибер-атак эксплуатируют **известные уязвимости**, против которых не были применены существующие патчи.



РИСКИ – это сочетание уязвимости и соответствующей ей угрозы.

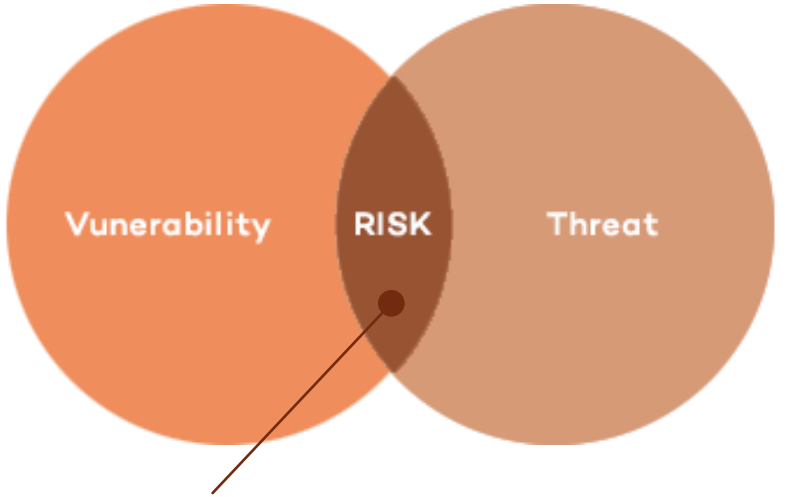
Сумма всех этих факторов УМНОЖАЕТ РИСКИ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗ ОБНОВЛЕНИЙ
компрометирует безопасность компании.

Хакеры эксплуатируют уязвимости в необновленных программах.

Пользователи не утруждают себя обновлением ПО. Их компьютеры **подвержены угрозам**.

Повышенная мобильность пользователей задерживает обновление устройств, делая их более **уязвимыми для вредоносного ПО**.



РИСКИ – это сочетание уязвимости и соответствующей ей угрозы.

Сумма всех этих факторов УМНОЖАЕТ РИСКИ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗ ОБНОВЛЕНИЙ
компрометирует безопасность компании.

Хакеры эксплуатируют уязвимости в необновленных программах.

50%

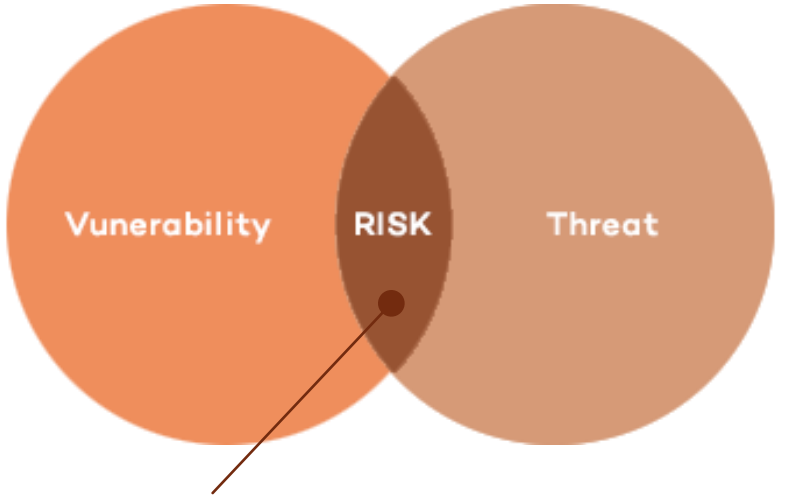
50% используемых уязвимостей появляются в течение 2-4 недель после выхода патча.

90%

90% используемых уязвимостей появляются через **40-60 дней после выхода приложения.**

120 days

Среднее время для внедрения компанией **критических патчей** от производителей составляет **120 дней**.



РИСКИ – это сочетание уязвимости и соответствующей ей угрозы.

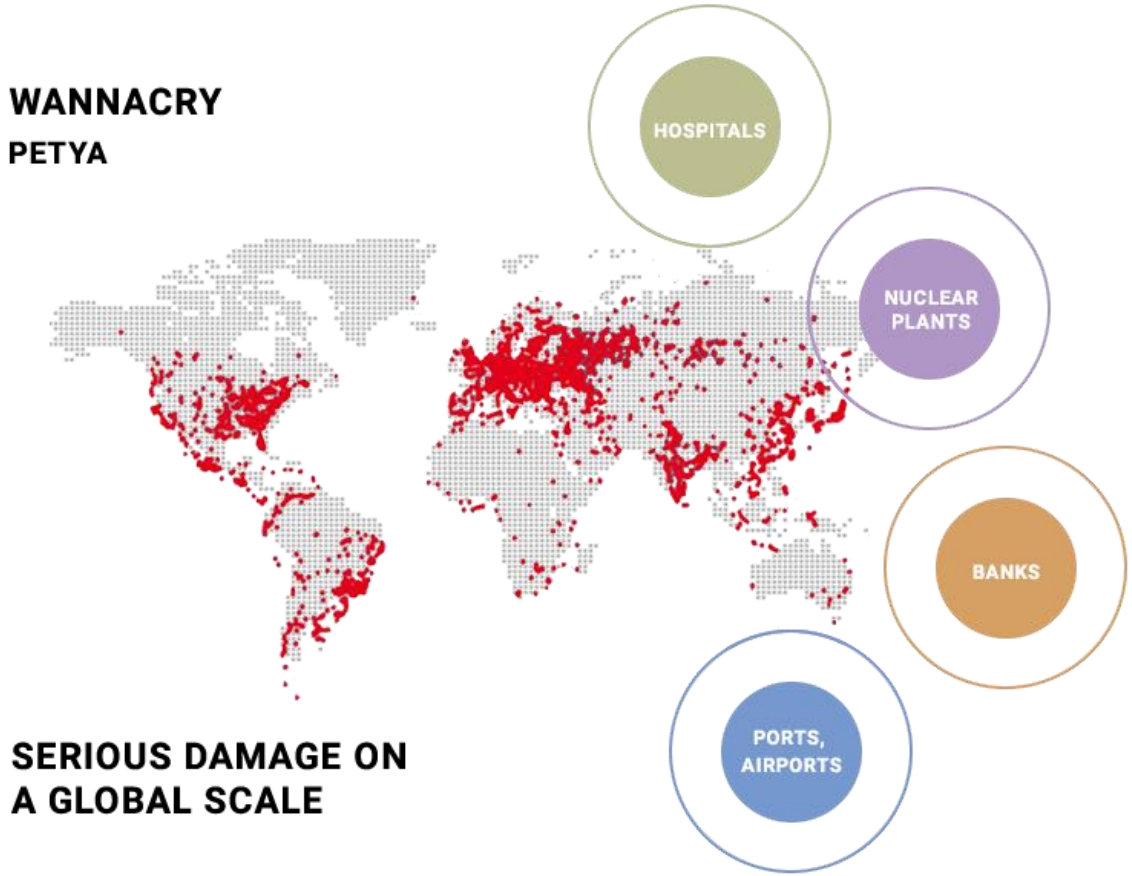
Сумма всех этих факторов УМНОЖАЕТ РИСКИ

WannaCry и Petya

использовали уязвимости, которые месяцами были известны

WannaCry парализовал больницы, банки и предприятия во всем мире. Больницы в Великобритании были вынуждены отменять прием пациентов.

Petya также поразил больницы (были отменены даже операции) и другие ключевые секторы экономики, включая авиакомпании, банки, даже Чернобыльскую АЭС.



ВЛИЯНИЕ НА ПРОИЗВОДИТЕЛЬНОСТЬ КОМПАНИИ

ПО без адекватных обновлений приводит к:

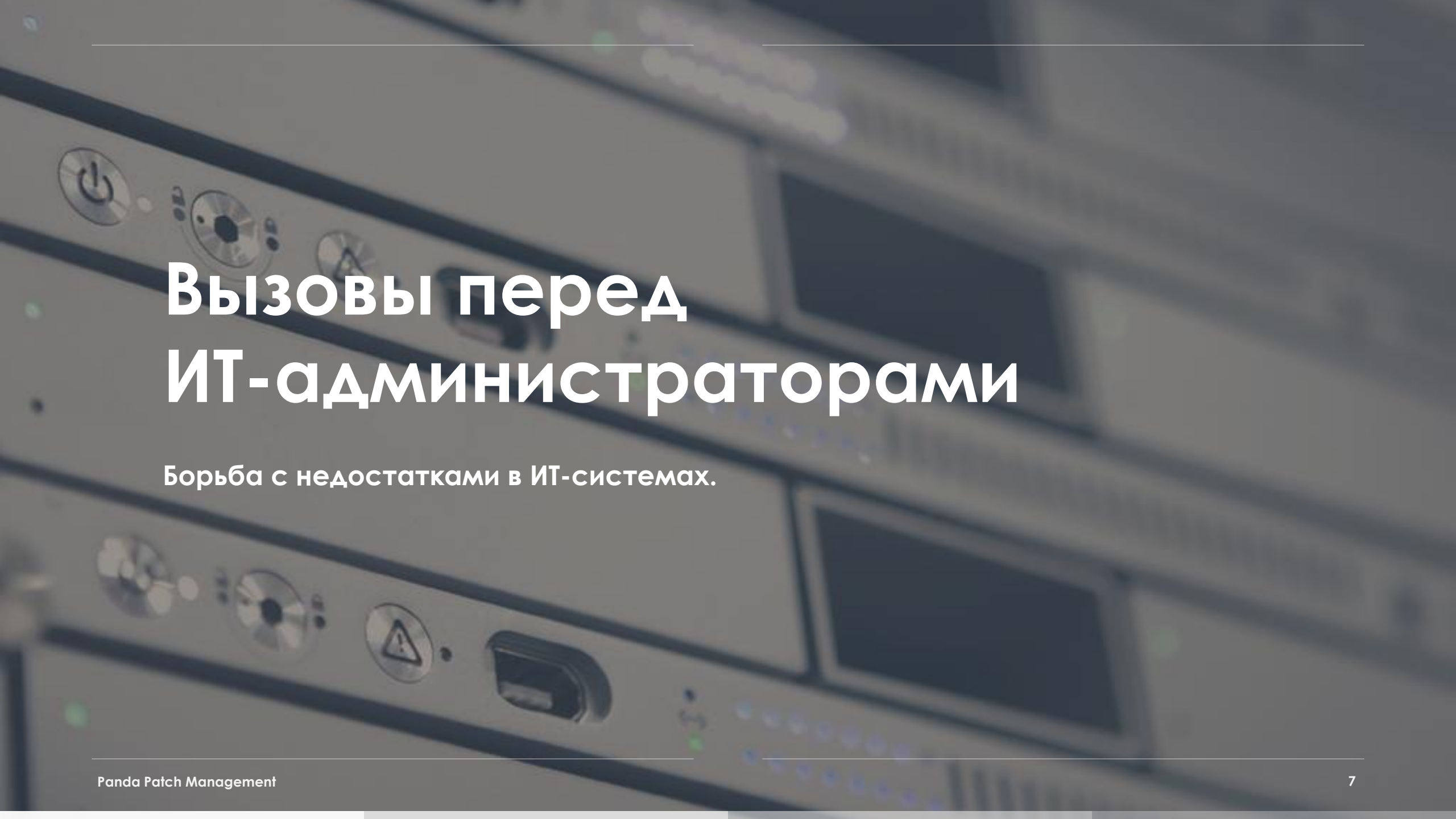
Перебоям в работе пользователей из-за ошибок ПО.

Потере данных и времени из-за внезапных и некорректных перезагрузок ПК, требуемых для обновления ПО.

Серьезным ошибкам на обновленных ПК из-за некорректного управления **совместимостью ПО**.

Низкой производительности приложений, т.к. они не обновлены до последней версии

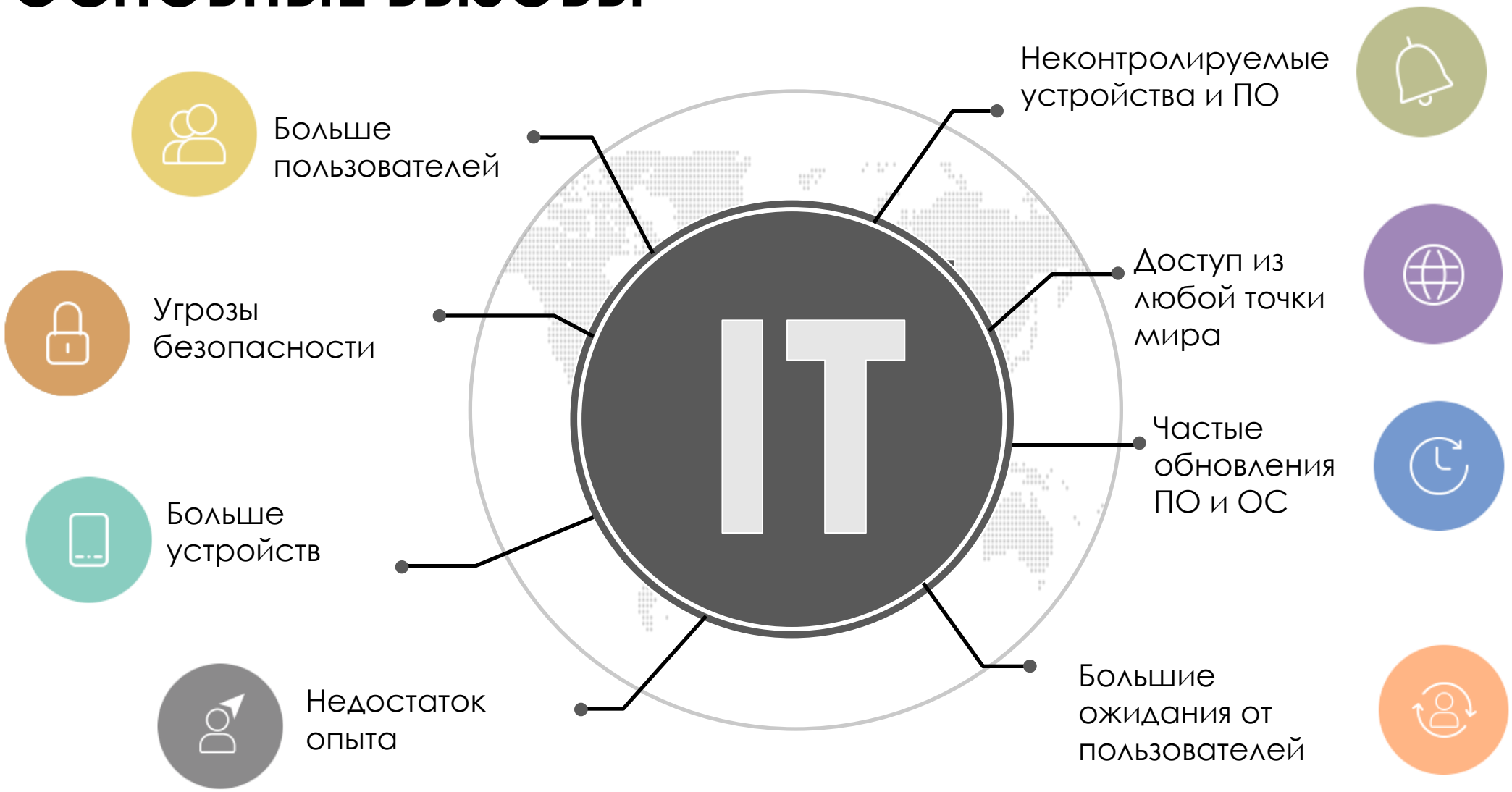
Высокому потреблению ресурсов (канал связи и процессор) на рабочих станциях и серверах из-за ПНП и ПО для майнинга криптовалют.



Вызовы перед ИТ-администраторами

Борьба с недостатками в ИТ-системах.

ОСНОВНЫЕ ВЫЗОВЫ



ОСНОВНЫЕ ВЫЗОВЫ
В ЕЖЕДНЕВНОЙ РАБОТЕ АДМИНИСТРАТОРОВ.

Сложно оценивать и знать общее состояние корпоративной сети. Недостаток видимости того, какие критические патчи не применены, и использование многочисленных инструментов

Многочисленные патчи. Сотни обновляемых приложений и совместимость между обновленным ПО.

Способность быстро реагировать на критические уязвимости.

Своевременное обновление всех ресурсов. Недостаток времени, нечеткие обязанности, не самый главный приоритет в списке задач ИТ-отдела

КЛЮЧЕВЫЕ ВОПРОСЫ

Кто отвечает за обновление ПО и его защиту от уязвимостей?

Сколько времени тратится на обновление компьютеров? Мне нужно, чтобы моя команда выполняла задачи по развитию бизнеса.

Насколько уязвимы компьютеры и серверы в моей организации?

Сколько времени требуется для применения патча после его выхода?

Как я могу обеспечить запланированный процесс обновления систем, не отвлекая сотрудников?

Что такое Panda Patch Management?

Системы без уязвимостей при минимальных затратах без отвлечения сотрудников от работы

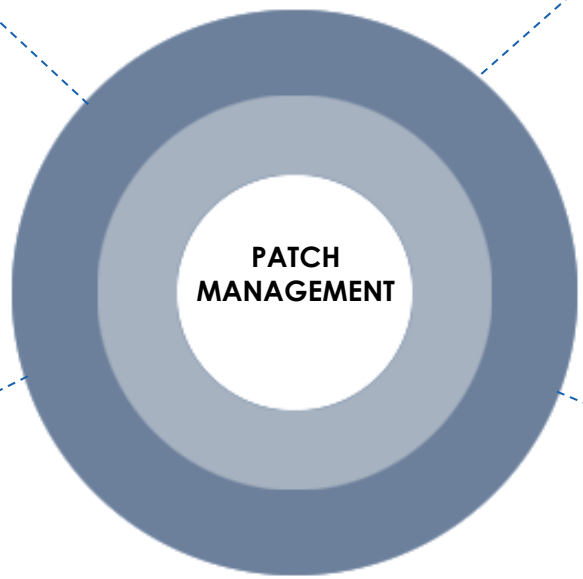
Panda Patch Management обеспечивает отсутствие уязвимостей в системах при минимальных затратах (инфраструктура, коммуникации, технический персонал), при этом не отвлекая сотрудников от работы.

СКАНИРОВАНИЕ

- **Проверка** всех компьютеров из любой точки в любое время.
- Не требуется дополнительное внедрение (**единый агент**).

ИНТЕЛЛЕКТ

- **Обновление всех версий** Windows…
- **…и сотен сторонних приложений**.
- **Исключение** патчей и ПО (при необходимости).



ОЦЕНКА И ПЛАНИРОВАНИЕ

- **Проверка** уязвимого ПО, критичности патчей и пр.
- **Применение** патчей на тестовых компьютерах до их внедрения во всей компании.
- **Создание** правил автоматического обновления с исключениями.

ВНЕДРЕНИЕ

- **Обновление** сотен тысяч ПК в реальном времени.
- **Автоматическое управление** совместимостью патчей.
- **Контроль** перезагрузок ПК.

Функции
Panda Patch Management

Windows и сторонние приложения | 100% интеграция в Aether

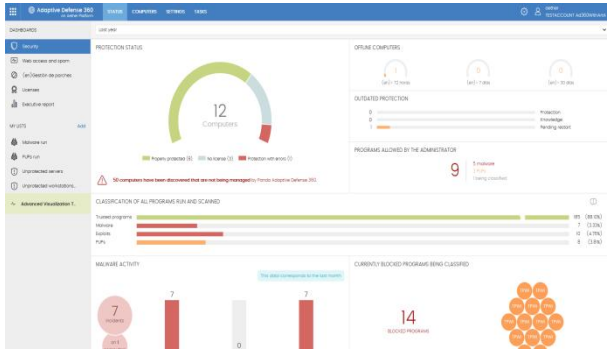
Windows и сторонние приложения 100% интеграция в Aether

ОБНОВЛЯЕМОЕ ПО

- Совместимость с сотнями сторонних приложений (Java, Adobe, Firefox, …).
- Совместимость со всеми операционными системами Windows.
- Исключение патчей или ПО (при необходимости).

ИНТЕГРАЦИЯ В AETHER

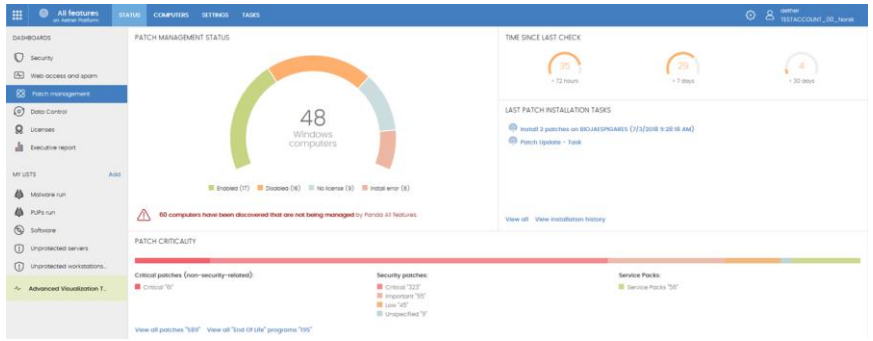
- Единое управление из веб-консоли Aether.
- Не требуется внедрять новый агент на рабочих станциях и серверах.
- Применение патчей в реальном времени.
- В сочетании с Adaptive Defense, возможность изолировать необновленные системы с критическими уязвимостями.



Панели мониторинга | Патчинг | Контроль

ПРОСМОТР СТАТУСА СЕТИ

• Графики показывают статус обновлений в сети (необновленные ПК, непримененные патчи и пр.).
• Настраиваемые списки и фильтры компьютеров без патчей.
• Отчеты.

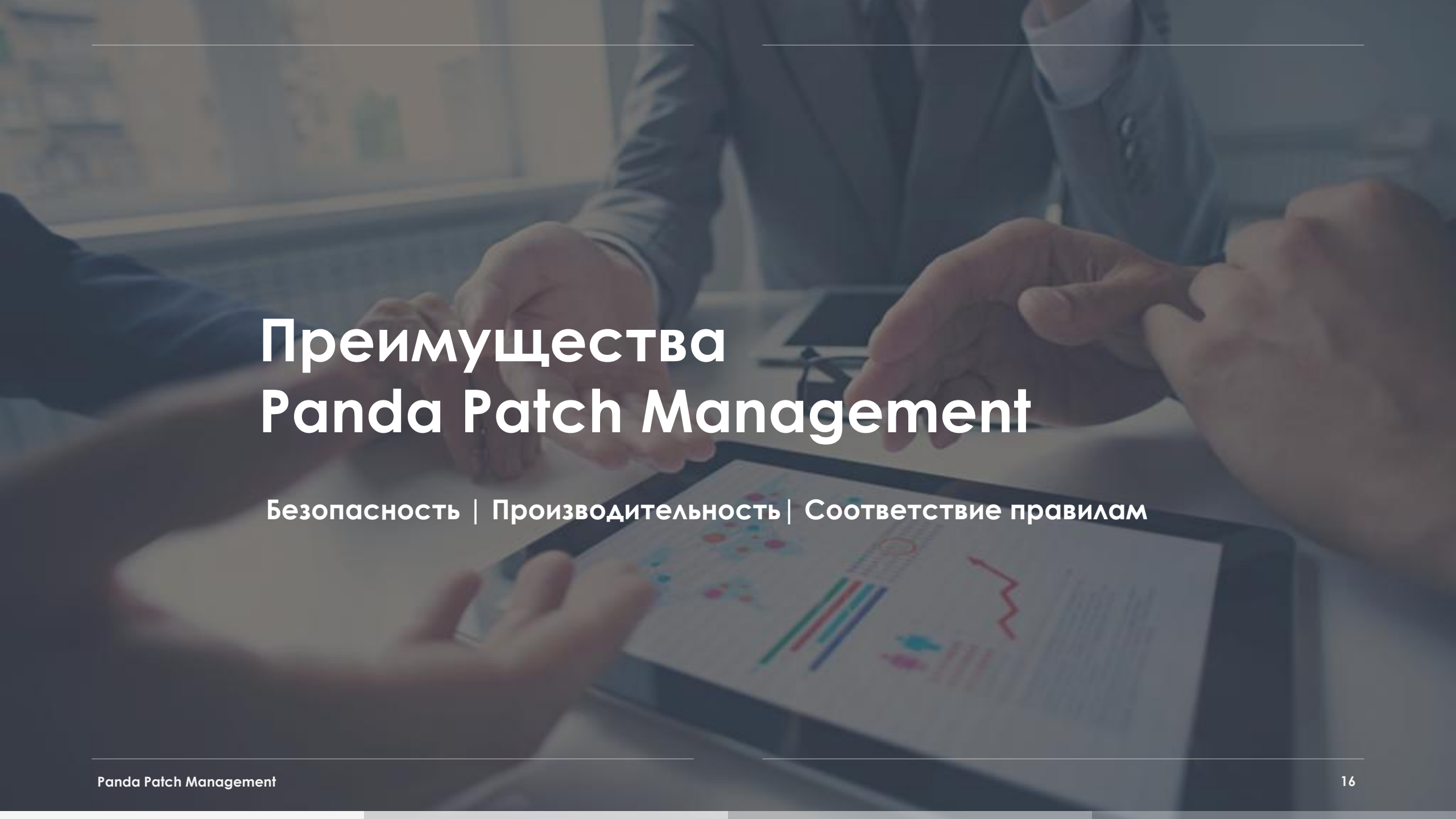


ВНЕДРЕНИЕ ПАТЧЕЙ

• Ручные или запланированные обновления в реальном времени.
• Возможность удалять патчи.
• Контроль времени перезагрузки системы.
• Автоматическое управление совместимостью патчей.
• Кеширование скаченных патчей.

КОНТРОЛЬ ДОСТУПА

• Роли с детализированными правами для управления доступом к функциям.
• Журнал выполнения задач по обновлениям.



Преимущества Panda Patch Management

Безопасность | Производительность | Соответствие правилам

ПРЕИМУЩЕСТВА

БЕЗОПАСНОСТЬ

- **Уменьшает поверхность атаки** (80% всех кибер-атак эксплуатируют известные уязвимости).
- **Обеспечивает защиту конфиденциальных данных** от кражи или взлома.
- **Защищает ИТ-ресурсы** от несанкционированного использования вредоносными программами для майнинга криптовалют.

ПРОИЗВОДИТЕЛЬНОСТЬ СОТРУДНИКОВ

- **Обеспечивает** использование сотрудниками **последних версий программ**. Предотвращает ошибки в работе ПО из-за использование старых версий с ошибками.
- **Обновляет ПО без простоя в работе сотрудников**.
- Предотвращает **потерю производительности, несовместимость** между программами и **чрезмерное использование канала связи** из-за ПНП.

ПРЕИМУЩЕСТВА

ПРОИЗВОДИТЕЛЬНОСТЬ ИТ-ДЕПАРТАМЕНТА

• **Сводит к минимуму усилия** по мониторингу статуса обновлений внутри сети.
• **Экономит время,** избегая ручных обновлений ПК (в среднем 4-8 часов на патч). Запланированное, автоматическое выполнение задач обновления. Простой запуск: без дополнительного внедрения.
• **Простое обучение**: модуль интегрирован в платформу Aether, единая веб-консоль.

СОБЛЮДЕНИЕ И ПЛАНИРОВАНИЕ

• Настройка **централизованного планирования** обновлений для соответствия требований к ИТ-инфраструктуре (PCI DSS, HIPAA, SOX и т.д.).

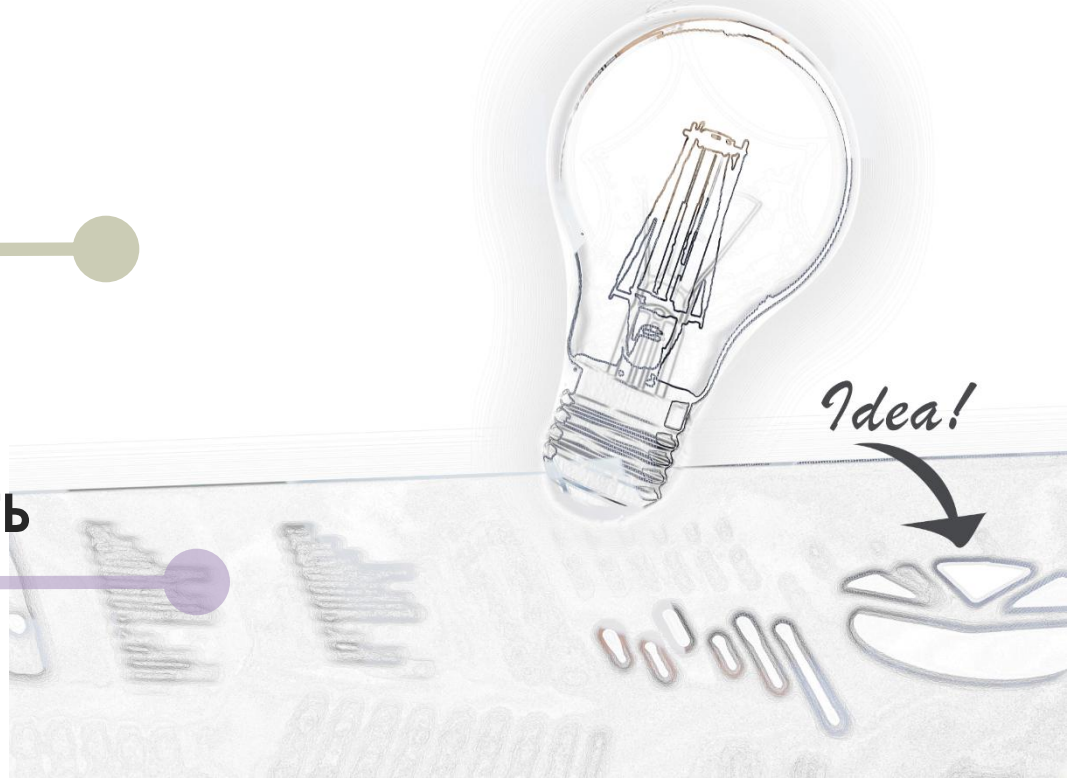
РЕЗЮМЕ

СМЯГЧАЕТ РИСКИ

СНИЖАЕТ РАСХОДЫ

ПОВЫШАЕТ ЭФФЕКТИВНОСТЬ

БОЛЬШЕ ВРЕМЕНИ ВЫДЕЛЯЕТСЯ НА СТРАТЕГИЧЕСКИЕ ПРОЕКТЫ



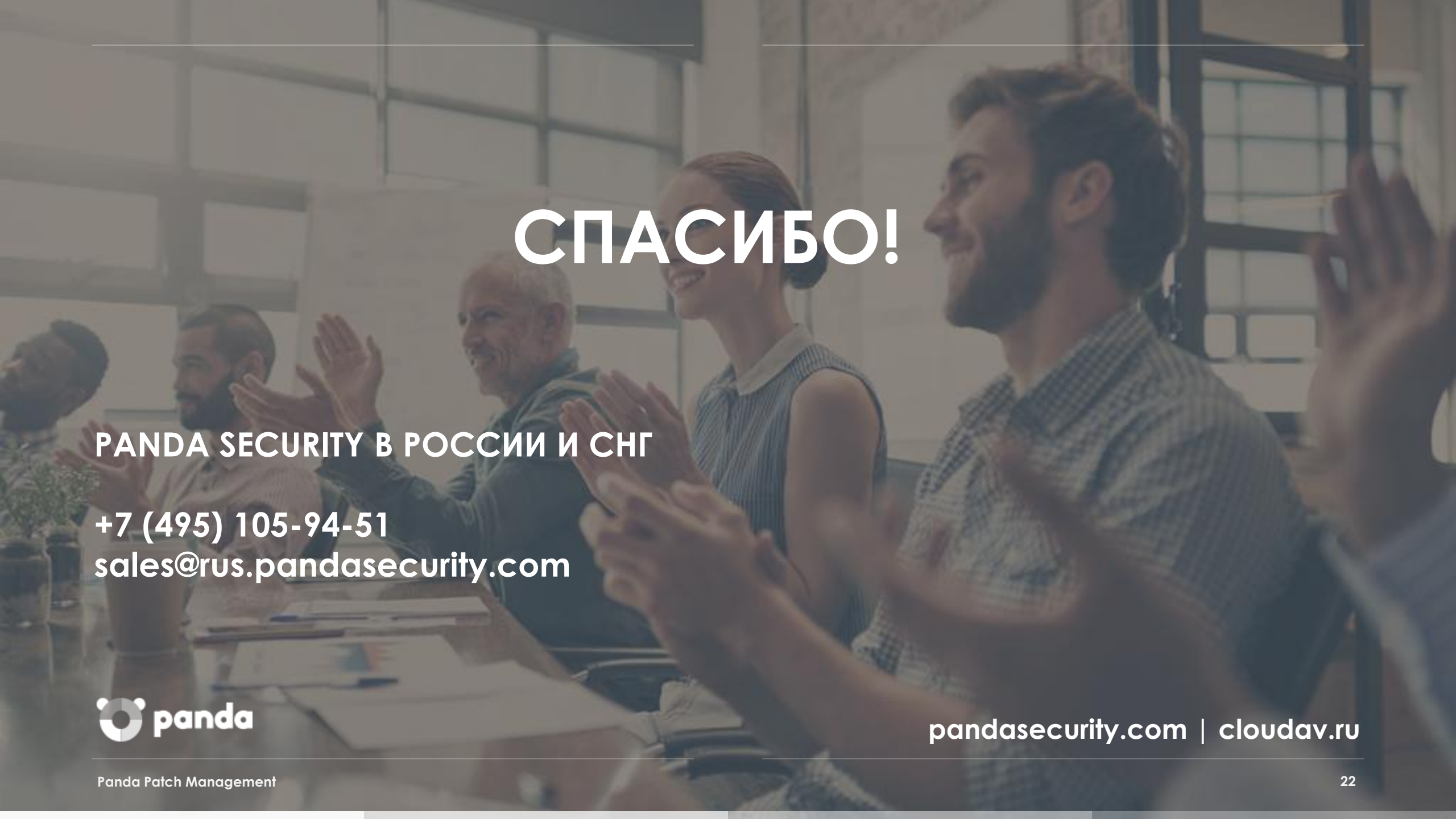
Доступность Panda Patch Management

С КАКИМИ ПРОДУКТАМИ ПОСТАВЛЯЕТСЯ?

- Panda Endpoint Protection на Aether.
- Panda Endpoint Protection Plus на Aether.
- Panda Adaptive Defense на Aether.
- Panda Adaptive Defense 360 на Aether.

В КАКОМ ВИДЕ ПРОДАЕТСЯ?

Как **дополнительный модуль.**



СПАСИБО!

PANDA SECURITY В РОССИИ И СНГ

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

panda

pandasecurity.com | cloudav.ru