



PT Dephaze

Регулярная оценка уровня защищенности
через автопентест

Оценивать защищенность инфраструктуры все сложнее



Инфраструктура
постоянно меняется

**В 79%
компаний**

изменения в ИТ-среде
происходят чаще, чем раз в квартал

По данным исследования «Есть ли необходимость
в автоматизации тестирования на проникновение» ↗

Количество СЗИ
растет

**Только 20%
компаний**

используют
меньше 10 СЗИ

По данным исследования «Есть ли необходимость
в автоматизации тестирования на проникновение» ↗

Ландшафт киберугроз
становится более изощренным

На 35%

может вырасти количество
успешных кибератак на российские
компании в 2026 году***

ptsecurity.com ↗

Популярные методы оценки защищенности зачастую используются нерегулярно



Популярные методы оценки защищенности¹



Аудит безопасности



Сканеры безопасности



Тестирование на проникновение

- 1 Преимущественно **раз в год** компании проводят ИБ-аудит²
- 2 Только **14% компаний** проводят ручные пентесты ежемесячно³
- 3 Чаще всего компании проводят сканирование всей инфраструктуры **раз в квартал или реже**⁴

^{1,4} По данным исследования «Есть ли необходимость в автоматизации тестирования на проникновение»

^{2,3} По данным Positive Technologies



PT Dephaze превращает оценку защищенности
инфраструктуры в непрерывный процесс
и отвечает на главный вопрос

**Насколько ваша
инфраструктура готова
к отражению реальной
кибератаки?**



Что такое PT Dephaze



Автопентест для оценки уровня защищенности внутренней инфраструктуры



Атакуем контролируемо

Даем возможность управлять согласованием и интенсивностью атак, исключениями области тестирования и прозрачно показываем все атакующие действия

ВНЕДРЕНИЕ ЗА 1 ЧАС



Помогаем оценить и исправить

Говорим, какие атаки должны видеть ваши средства защиты, где были небезопасные пароли, как пропатчить системы и изменить небезопасные конфигурации. Для удобства оформляем это в отчет

FALSE POSITIVE = 0



Регулярно пополняем набор атак

Используем в продукте двадцатилетнюю экспертизу и опыт Positive Technologies в тестировании на проникновение, расследованиях и разведке техник

ПЕРВЫЕ РЕЗУЛЬТАТЫ ЗА 1 ЧАС

Популярные методы оценки защищенности vs PT Dephaze



Сканер уязвимостей

- ✓ Выявляет уязвимости и ошибки конфигурации
- ✗ Не показывает последствия их эксплуатации и не учитывает СЗИ

Ручной пентест

- ✓ Выявляет реальные векторы атак
- ✗ Проводится эпизодически и ограничен ресурсами

Симуляция атак (BAS)

- ✓ Оценивает эффективность средств защиты с помощью симуляции атак
- ✗ Ограничен предзаданными сценариями и не показывает полную картину защищенности



PT Dephaze

- ✓ Выстраивает реальные цепочки атак внутри инфраструктуры: анализирует взаимосвязи между узлами, переиспользует учетные данные на обнаруженных сервисах и показывает все возможные пути компрометации, а не отдельные уязвимости
- ✓ Не требует предварительного создания атакующих сценариев
- ✓ Самостоятельно принимает решения о развитии атаки при полном контроле со стороны пользователя
- ✓ Проверяет эффективность средств защиты, обнаружения и реагирования — оценивает способность СЗИ и процессов реагирования выявлять и останавливать атаки.

Какие задачи решает PT Dephaze



Регулярная оценка защищенности

После обновлений ПО, ввода новых систем или изменений в сети, PT Dephaze запускается для проверки появления новых уязвимостей или некорректных конфигураций



Проверка эффективности СЗИ

PT Dephaze запускается после изменения или обновления средств защиты, чтобы проверить, способны ли они обнаружить или предотвратить реальные атаки



Обучение и тестирование SOC*

PT Dephaze используется для тренировки аналитиков SOC и проверки готовности команды к реальным инцидентам

* Опыт заказчиков PT Dephaze

Как использовать PT Dephaze



Триггеры нового запуска

- Плановое тестирование
- Изменения в ИТ-инфраструктуре
- Обновление продукта
- Подготовка к регуляторным проверкам

Повторное тестирование с PT Dephaze и валидация устранения недостатков



Тестирование с PT Dephaze

Получение оценки защищенности и рекомендаций

Исправление, донастройка СЗИ

PT Dephaze — это...



Безопасно

Под капотом нет опасных эксплойтов, способных вывести из строя ПО или хост



Контролируемо

Все потенциально рискованные шаги выполняются детерминировано и под управлением пользователя

ВЫ МОЖЕТЕ

- > Ограничивать область тестирования
- > Исключать из проверки критичные бизнес-активы
- > Настраивать параметры отдельных атак
- > Согласовывать действия при продвижении внутри инфраструктуры



Как работает PT Dephaze

Не список уязвимостей, а полная цепочка атаки



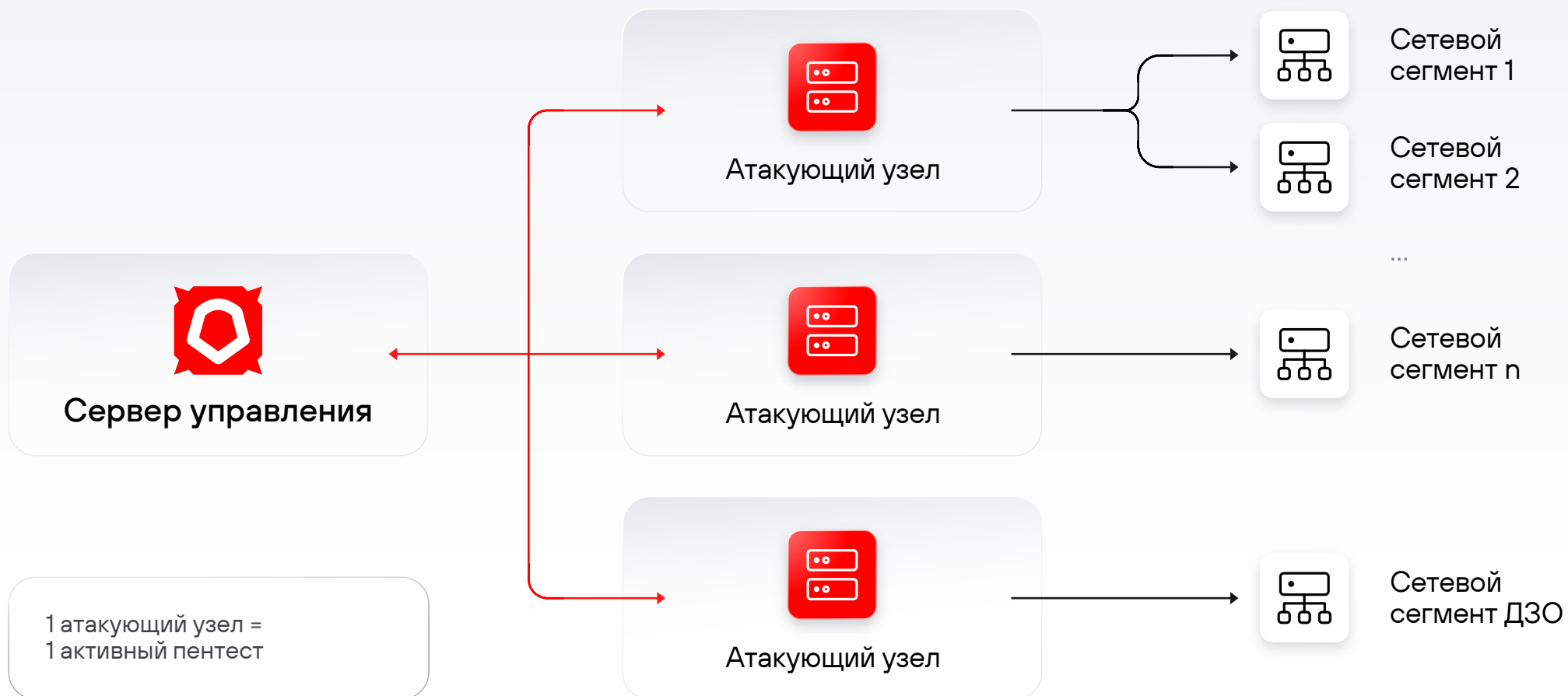




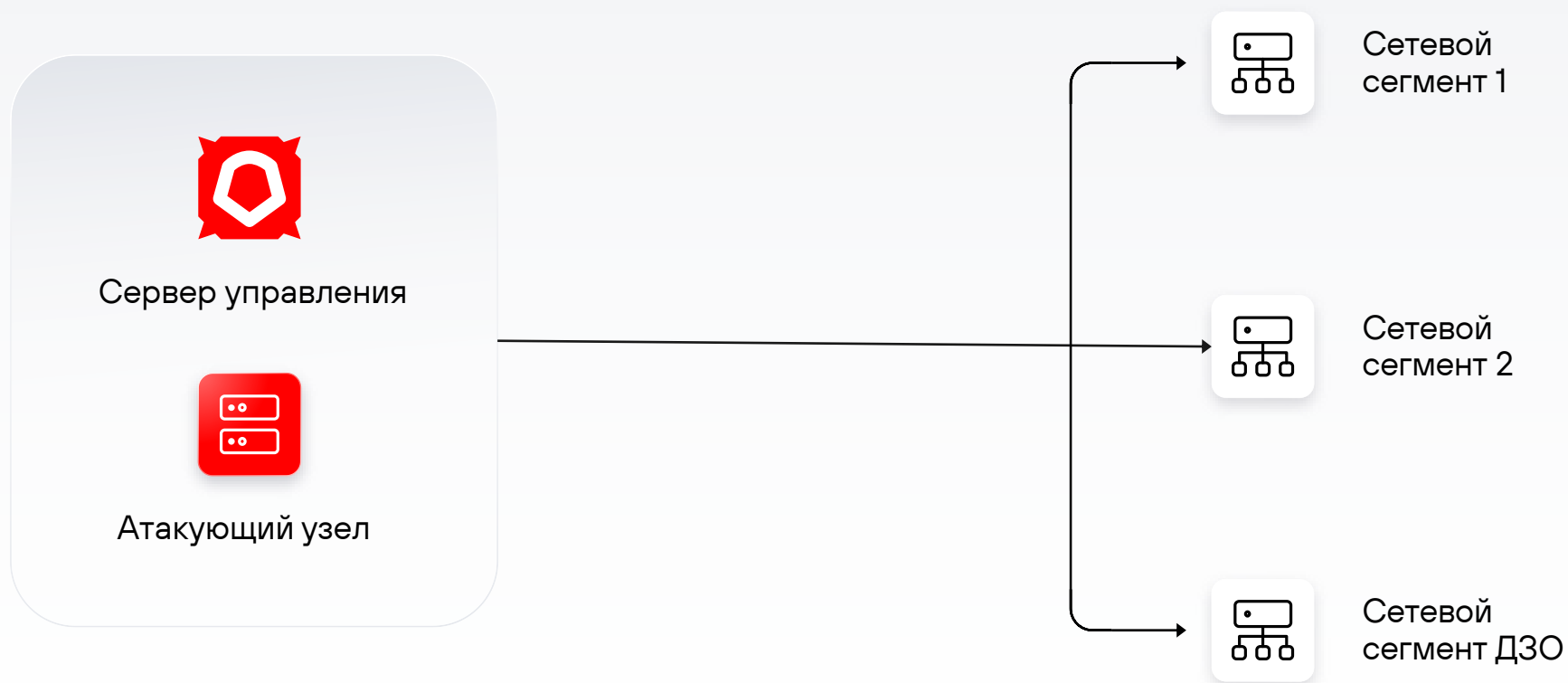
Как развернуть PT Dephaze



Серверная лицензия



Мобильная лицензия



Системные требования для серверной версии



Сервер управления
и атакующий узел — Linux
(включены в подготовленный
образ дистрибутива)

VMware ESXi, HyperV, KVM

Рекомендуемые требования	СЕРВЕР УПРАВЛЕНИЯ	АТАКУЮЩИЙ УЗЕЛ
Количество виртуальных ядер процессора	8 (или больше)	8
Память (ОЗУ)	32 ГБ	16 ГБ
Дисковое пространство	200 ГБ SSD	100 ГБ SSD

Варианты лицензирования PT Dephaze



ТИП ЛИЦЕНЗИИ

СЕРВЕРНАЯ (СТАЦИОНАРНАЯ)

МОБИЛЬНАЯ (ПЕРЕНОСНАЯ)

Масштабируемость

От 100 до безлимита IP

От 100 до 500

Бонус

10% от купленного объема IP,
раз в год (через 6 месяцев)
доступен полный сброс учтенных IP

—

Сценарий
использования

Идеально подходит
для регулярного внутреннего
тестирования

Оптимальный выбор
для выездных пентестов
и разовых аудитов небольших сегментов



PT Dephaze в 2026 году



H1 `26

Q3 `26

Q4 `26

2027

Продукт

- ☒ Управление областью тестирования
- ☒ Расширение словарей для атак методом перебора
- ☒ Поиск учетных данных в текстовых файлах с помощью ИИ

- Установка продукта и атакующего узла на Debian или Astra Linux
- Просмотр обнаруженных учетных данных
- Детализированная карта цепочек атак

- Ручное расширение области тестирования
- Умный поиск и автообнаружение новых узлов

- Ролевая модель
- Запуск по расписанию, уведомления
- Приоритизация для исправлений и проверки мониторинга
- Горизонтальное перемещение в другие сетевые сегменты («пивотинг»)
- Получение сертификата ФСТЭК РФ по 4-му уровню доверия
- Прототип использования ИИ для атакующих действий

Экспертиза

- ☒ Фокус на Windows и Linux-based инфраструктурах
- ☒ Расширение атак на службу каталогов Active Directory
- ☒ Добавление поддержки различных типовых ИТ-систем
- ☒ Расширение атак на службы каталогов (FreeIPA и аналоги)

- Расширение атак на службы каталогов (FreeIPA и аналоги, Active Directory)
- Расширение атак на ОС Linux и Windows
- Типовые системы для серверного сегмента
- Атаки через злоупотребление правами доступа в Active Directory
- Атаки на 1С



Узнать больше
о PT Dephaze



Канал PT Dephaze
в Telegram

