Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Эшелонированная защита офиса до 50 РМ: наш стандартный стек

Периметр, SIEM на Wazuh, неизменяемые бэкапы Veeam и контроль доступов — как мы это внедряем

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Офису до 50 рабочих мест хватает одной успешной атаки: шифровальщик в ночь на понедельник, увод почтовой переписки или слив базы клиентов уволенным менеджером. Штатного ИБ-специалиста нет, защита сводится к антивирусу, а бэкап часто лежит в той же сети и шифруется вместе с данными. Мы закрываем это одним стандартизованным стеком: периметр, контроль доступов, SIEM и неизменяемы…

Почему это важно бизнесу

- Простой после шифровальщика — дни без 1С, почты и отгрузок; каждый день стоит выручки и штрафов по договорам
- Утечка клиентской базы — прямые потери продаж плюс риски по 152-ФЗ вплоть до оборотных штрафов
- Подделка писем от директора заканчивается оплатой фальшивых счетов — деньги возвращаются редко
- Восстановление без проверенных бэкапов непредсказуемо: RTO неизвестен, пока не случился инцидент

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

4.14.x

Ветка Wazuh, которую мы ставим: single-node manager+indexer закрывает офис до 50 агентов

Wazuh docs, Quickstart

14 дней

Immutability бэкапов на Linux Hardened Repository (минимум по докам — 7 дней)

Veeam B&R 13

p=reject

Целевая DMARC-политика домена: стартуем с p=none+rua, ужесточаем после 2–4 недель отчётов

наш стандарт

5 / 15 мин

Порог блокировки учётки: 5 неверных паролей — лок на 15 минут (Account Lockout Policy, GPO)

наш стандарт

0 портов

RDP/SMB, опубликованных наружу: ноль; доступ только через VPN (WireGuard/IPsec) или RD Gateway…

наш стандарт

3-2-1

Схема хранения копий: 3 копии, 2 носителя, 1 вне площадки — офсайт в S3 с Object Lock

Veeam B&R 13

РЕАЛИЗАЦИЯ 1 ИЗ 3

SIEM на Wazuh: видим взлом, а не узнаём постфактум

Что настраиваем

Все Windows/Linux-хосты офиса: контроллеры домена, серверы 1С, терминальники, рабочие станции — до 50 агентов на один узел

Как мы это делаем

1. Разворачиваем Wazuh 4.14 all-in-one (manager + indexer + dashboard) на отдельной VM 8 vCPU/8 ГБ/100 ГБ SSD: installation assistant (wazuh-install.sh -a), TLS между…
2. Агенты на Windows катим через GPO (MSI с параметром WAZUH_MANAGER), на Linux — из репозитория; группируем по ролям: dc, 1c, rdp, workstation
3. Включаем FIM (syscheck realtime на каталоги 1С и SYSVOL), SCA-профили CIS для Windows Server и Ubuntu, Vulnerability Detection по фидам
4. Маршрут алертов: level ≥ 10 уходит в Telegram-канал дежурного через integrations; брутфорс RDP (событие 4625) гасим active response

РЕЗУЛЬТАТ

Инцидент виден в первые минуты: подбор пароля, новый локальный админ, изменение GPO, отключение антивируса — всё поднимает алерт. SCA даёт измеримый процент соответствия CIS по каждому хосту, и харднинг превращается в план работ, а не в абстракцию.

КЛЮЧЕВОЙ НЮАНС

Single-node тянет офис до 50 агентов, но indexer требователен к диску: закладываем SSD и ротацию индексов (ISM ~90 дней), иначе dashboard деградирует раньше, чем кончится место.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Бэкапы, которые шифровальщик не достанет

Что настраиваем

Veeam B&R 13 + отдельный Linux-хост под Hardened Repository; охват — все VM и физические серверы клиента

Как мы это делаем

1. Ставим отдельный физический Linux-хост (Ubuntu LTS) под Hardened Repository: XFS с reflink=1 для fast clone, диск не публикуется по SMB/NFS
2. Подключаем в Veeam как Hardened Repository с single-use credentials: постоянного SSH-доступа с сервера бэкапов к репозиторию нет
3. Immutability 14 дней: Veeam ставит xattr user.immutable.until и .veeam.N.lock на файлы цепочки — изменить или удалить их с сервера Veeam нельзя
4. Офсайт-копия Backup Copy Job в S3-совместимое хранилище с Object Lock (compliance mode); health check и тестовое восстановление — ежемесячно

РЕЗУЛЬТАТ

Компрометация сервера Veeam или домена не уничтожает копии: последние 14 дней цепочки физически неизменяемы. Восстановление проверено заранее, поэтому RTO считается по фактам тестов, а не по надеждам.

КЛЮЧЕВОЙ НЮАНС

Отсчёт immutability идёт от последней точки активной цепочки — на длинных forever-incremental срок защиты плавает; мы фиксируем его синтетическими фуллами раз в неделю.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Закрываем удалённый доступ: RDP только через шлюз

Что настраиваем

Периметр офиса: pfSense 2.8 на границе, терминальные серверы, доступ сотрудников и подрядчиков

Как мы это делаем

1. Убираем все пробросы 3389/445 наружу; удалённый доступ — только WireGuard/IPsec на pfSense или RD Gateway на 443 с обязательной NLA
2. GPO: Account Lockout 5 попыток / 15 минут, запрет интерактивного входа доменных админов на рабочие станции
3. Подрядчикам — отдельные учётки со сроком действия (net user /expires) и доступом по IP-алиасам pfSense; отзыв — одним правилом
4. На Linux-периметре SSH только по ключам + CrowdSec 1.6 с firewall-bouncer; события 4624/4625 на Windows контролирует Wazuh

РЕЗУЛЬТАТ

Поверхность атаки снаружи — один VPN-порт и 443. Перебор паролей упирается в lockout и попадает в SIEM; после окончания проекта доступ подрядчика гаснет сам по expiration, а не «когда вспомним».

КЛЮЧЕВОЙ НЮАНС

Смена порта RDP — не защита: служба находится по отпечатку протокола за часы. Считаем закрытым только то, чего снаружи нет вообще, и проверяем внешним сканом портов после каждого изменения NAT.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Антивирус = вся защита**
  Эндпоинт-агент не видит подбор паролей, фишинг и кражу учёток; строим слои — периметр, MFA, SIEM, бэкапы, — чтобы пробой одного слоя не был фатален

- ✕ **Бэкап в той же сети по SMB**
  Шифровальщик находит доступную шару с копиями первой; храним цепочку на Hardened Repository с immutability и офсайт-копию в S3 с Object Lock

- ✕ **DMARC годами в p=none**
  Политика none только мониторит — подделку писем никто не блокирует; после разбора rua-отчётов переводим домен на quarantine, затем на reject

- ✕ **RDP наружу «на хитром порту»**
  Порт — не секрет: служба идентифицируется по отпечатку протокола; выносим RDP за VPN или RD Gateway и держим ноль публикаций наружу

- ✕ **SIEM поставили — никто не смотрит**
  Алерты без маршрута умирают в dashboard; настраиваем доставку level ≥ 10 в Telegram дежурному и еженедельный разбор ложных срабатываний

- ✕ **Общая админ-учётка на всех**
  Один пароль у троих — аудит бессмыслен, а увольнение требует смены везде; персональные учётки плюс Vaultwarden с шарингом по коллекциям

- ✕ **Шары с «Все — полный доступ»**
  Утечка и шифрование получают максимальный охват; режем NTFS-права по группам AD и раз в квартал снимаем срез эффективных прав

- ✕ **Уволенный с живыми доступами**
  Доступы разбросаны: VPN, почта, 1С, SaaS; ведём матрицу доступов на сотрудника и офбординг-чек-лист — полное отключение за один день

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Бэкап по 3-2-1 с immutable-копией и ежемесячным тестом восстановления
- Ноль RDP/SMB наружу: доступ только через VPN, лок-аут 5 попыток / 15 минут
- MFA на почту, VPN и админ-доступы; менеджер паролей вместо Excel
- SPF, DKIM 2048 бит и DMARC хотя бы p=quarantine на всех доменах

НОРМАЛЬНО

- Wazuh SIEM на все серверы: FIM, SCA по CIS, алерты в мессенджер дежурного
- Сегментация: серверы, пользователи, гостевой Wi-Fi и IoT в разных VLAN
- Блокировка USB-носителей через GPO, BitLocker на всех ноутбуках
- Матрица доступов и офбординг-чек-лист с отзывом за один день

ХОРОШО

- Hardened Repository + офсайт S3 Object Lock, SureBackup-проверки восстановимости
- EDR на рабочих станциях + active response Wazuh на брутфорс и новые службы
- Фишинговые учения дважды в год с разбором результатов с сотрудниками
- Ежегодный внешний скан периметра и аудит прав доступа к данным

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли копия бэкапа, которую нельзя удалить с сервера бэкапов (immutability/Object Lock)?
- [ ] Когда последний раз реально восстанавливали сервер из бэкапа и замеряли время?
- [ ] Открыт ли RDP или SMB из интернета хотя бы на один хост (проверено внешним сканом)?
- [ ] Включена ли MFA на почте, VPN и у всех административных учёток?
- [ ] Придёт ли алерт дежурному ночью при подборе пароля или создании нового админа?
- [ ] Заблокирует ли домен учётку после 5 неверных паролей подряд?
- [ ] Стоит ли DMARC-политика quarantine/reject на всех почтовых доменах компании?
- [ ] Отключаются ли все доступы уволенного (VPN, почта, 1С, SaaS) за один день по чек-листу?
- [ ] Зашифрованы ли диски ноутбуков BitLocker и хранятся ли ключи восстановления в AD?
- [ ] Разделены ли VLAN серверов, пользователей и гостевого Wi-Fi?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит периметра и доступов: внешний скан, срез прав на шарах, отчёт с приоритетами за неделю
- Wazuh SIEM под ключ: агенты через GPO, правила, алерты в Telegram, регламент реагирования
- Бэкап-контур на Veeam с Hardened Repository и офсайт-копией, тесты восстановления по календарю
- Порядок в доступах: Vaultwarden, MFA, матрица доступов, офбординг-процедура
- Дежурный мониторинг: реагирование на алерты SIEM и инциденты по SLA

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Wazuh documentation — Quickstart, Installation guide, Release notes 4.14 (documentation.wazuh.com — 4.14)

02 Veeam B&R User Guide — Hardened Repository, Immutability (helpcenter.veeam.com — v13)

03 Microsoft Learn — Account Lockout Policy, Remote Desktop Services (learn.microsoft.com — 2025)

04 pfSense Documentation — Firewall, VPN (WireGuard/IPsec) (docs.netgate.com — 2.8)

05 IETF RFC 7489 — DMARC: политика домена, отчёты rua (datatracker.ietf.org — 2015)

06 CrowdSec Docs — Security Engine и firewall bouncer (docs.crowdsec.net — 1.6)

07 Шаблон ITfresh — офбординг-чек-лист и матрица доступов (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.