Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Замена Kaspersky и ESET: Defender, Dr.Web ESS, UserGate NGFW

Схема миграции без окна незащищённости: Defender+GPO, Dr.Web ESS 13.0, UserGate UGOS 7.5 LTS

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У клиентов ESET не продлевается, Kaspersky контрагенты просят убрать. Антивирус с протухшими базами опаснее его отсутствия: парк выглядит защищённым, но новые шифровальщики он не ловит. Мы переводим станции и серверы на поддерживаемый стек — Defender+GPO, Dr.Web ESS 13.0, UserGate на периметре — с зачисткой старых агентов и переносом исключений 1С/КриптоПро без окна незащищённ…

Почему это важно бизнесу

- Антивирус без обновления баз — парк выглядит защищённым, но свежие шифровальщики уже проходят мимо него
- Просроченные лицензии СЗИ блокируют договоры: аудиторы и контрагенты требуют актуальную защиту
- Шифровальщик на сервере с базами 1С = дни простоя бухгалтерии и восстановление из устаревшего бэкапа
- Кривая миграция (хвосты старого AV) роняет скорость 1С и станций — скрытые потери времени всего офиса

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

13.0.1

Dr.Web Enterprise Security Suite: сервер + Центр управления + агенты Windows/Linux одной верси…

по докам Dr.Web ESS

7.5 LTS

UserGate UGOS: первая LTS-сборка с поддержкой 2 года; проверенные стабильные — 7.3.3/7.4.1

по докам docs.usergate.com

19

правил ASR Defender: включаем через GPO/Set-MpPreference — сначала Audit (2), затем Block (1)

по докам learn.microsoft.com

High

CloudBlockLevel Defender; CloudExtendedTimeout=50 — плюс 50 с к базовым 10 с на вердикт облака

наш стандарт

2193

TCP-порт агент↔сервер Dr.Web ESS: открываем на межсегментных фаерволах до раскатки агентов

по докам Dr.Web ESS

48 ч

порог свежести антивирусных баз в нашем Zabbix: старше — алерт дежурному в Telegram

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Defender + GPO вместо ESET на рабочих станциях

Что настраиваем

Офис 10–20 PM в домене AD: Windows 10/11 Pro, файловая 1С и клиенты, без подписок Microsoft 365

Как мы это делаем

1. Зачистка: kavremvr.exe / ESET Uninstaller в safe mode на каждом узле, контроль остаточных драйверов-фильтров командой fltmc filters
2. GPO ITF_Defender_Baseline (ADMX Microsoft Defender Antivirus): MAPS=Advanced, CloudBlockLevel=High, PUAProtection=Enabled, контроль AMRunningMode=Normal
3. ASR: две недели AuditMode, разбор Event ID 1121/1122 в журнале Defender/Operational, затем перевод боевых правил в Block
4. Исключения до запуска: Set-MpPreference -ExclusionPath на каталоги *.1CD, журналы 1Cv8Log, КриптоПро, папки обменов
5. Видимость: Get-MpComputerStatus по WinRM → Zabbix (AMRunningMode, AntivirusSignatureLastUpdated), алерт при базах старше 48 ч

РЕЗУЛЬТАТ

Парк без лицензионных платежей и продлений: облачная эвристика, защита от шифровальщиков через ASR и Controlled Folder Access, состояние каждого узла видно в мониторинге, а не «по жалобам пользователей».

КЛЮЧЕВОЙ НЮАНС

Пока сторонний антивирус числится в Security Center (WSC), real-time защита Defender не работает: после зачистки хвостов обязательно проверяем AMRunningMode=Normal на каждом узле — иначе парк фактически без за…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Dr.Web ESS 13.0: центральная консоль для парка с серверами

Что настраиваем

20–50 PM + файловый/1С-сервер Windows Server; сервер ESS — отдельная VM 2 vCPU / 4 ГБ

Как мы это делаем

1. Dr.Web Server на выделенной VM; на растущем парке — сразу внешняя БД PostgreSQL вместо встроенной, бэкап конфигурации сервера по расписанию
2. Центр управления по HTTPS (порт 9081), связь агент↔сервер TCP 2193; наружу за обновлениями ходит только сервер, станции берут базы с него
3. Группы «Серверы»/«Бухгалтерия»/«Офис» со своими политиками: на сервере 1С плановое сканирование — только ночью, с лимитом нагрузки
4. Исключения SpIDer Guard до боевого включения: каталоги баз *.1CD, 1Cv8Log, контейнеры КриптоПро, папки обмена с банк-клиентами
5. Раскатка агентов волнами по 5–10 машин с контролем запуска 1С и офисных приложений после каждой волны

РЕЗУЛЬТАТ

Одна веб-консоль на весь парк: политики, карантин, задачи сканирования, отчёты; лицензии в рублях без санкционных рисков, серверные роли закрыты серверными агентами, а не десктопными лицензиями.

КЛЮЧЕВОЙ НЮАНС

На машинах старше 5–7 лет Dr.Web заметнее Defender по нагрузке: спасают исключения на базы 1С и режим SpIDer Guard «Оптимальный» (проверка при записи) — закладываем в политику группы сразу, а не после жалоб на…

РЕАЛИЗАЦИЯ 3 ИЗ 3

UserGate NGFW: периметр и сегментация вместо «просто антивируса»

Что настраиваем

25–50 РМ с выделенным каналом: клиника с МИС и ПДн или производство с изолируемыми отделами; C150 или виртуальный UserGate

Как мы это делаем

1. Аппаратный C150 или UserGate VE; UGOS обновляем до 7.5.0 LTS (либо стабильной 7.3.3/7.4.1) из личного кабинета UserGate
2. Зоны Trusted/Untrusted/DMZ и межсегментные правила deny-all + явные разрешения: бухгалтерия, склад и гостевой Wi-Fi не видят друг друга
3. Включаем СОВ на профиле критичных сервисов, веб-фильтрацию по категориям и антивирусную проверку транзитного HTTP/SMTP
4. RDP из интернета закрываем полностью: доступ сотрудников — только через VPN-шлюз UserGate; брутфорс RDP — главный вектор шифровальщиков
5. Журналы — на syslog-коллектор/Log Analyzer; срабатывания СОВ и блокировки — алертами дежурному в Telegram

РЕЗУЛЬТАТ

Закрываем класс задач сетевой безопасности целиком: контроль периметра, сегментация, отчёты по трафику для аудиторов; решение из реестра Минцифры проходит требования по отечественным СЗИ.

КЛЮЧЕВОЙ НЮАНС

UTM не видит USB-носители и не заменяет агентов: конечные точки всё равно закрываем Defender или Dr.Web, а шифрованный трафик шлюз инспектирует только при включённой SSL-инспекции.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Хвосты старого антивируса**
  Удаление через «Программы и компоненты» оставляет драйверы-фильтры и службы; чистим только kavremvr/ESET Uninstaller и проверяем fltmc filters
- ✕ **Defender не вернулся в Normal**
  Пока сторонний AV зарегистрирован в Security Center, real-time защита Defender не работает; после миграции проверяем AMRunningMode скриптом на каждом…
- ✕ **ASR сразу в Block без аудита**
  Правила ломают макросы, обмены 1С и печатные формы; две недели AuditMode с разбором событий 1121/1122 — и только потом боевой режим
- ✕ **Исключения 1С/КриптоПро не перенесли**
  Сканер лезет в *.1CD и контейнеры ключей: тормоза и ложные блокировки в отчётный период; переносим список исключений до боевого запуска
- ✕ **Плановый скан в рабочие часы**
  Full scan на сервере 1С днём = «база тормозит»; расписание на ночь, лимит нагрузки сканера, на серверах — проверка при записи
- ✕ **Защиту можно снять локально**
  Пользователь или зловред выгружает агент; включаем Tamper Protection у Defender, у Dr.Web — самозащиту и запрет деинсталляции агента в правах станции…
- ✕ **Старый AV «поживёт» без лицензии**
  Продукт работает и после конца лицензии, но базы не обновляются — ложное чувство защиты; окно миграции планируем сразу, не откладываем
- ✕ **UTM вместо агентов на станциях**
  Шлюз фильтрует только транзитный трафик: вложения с USB и внутри VPN он не видит; периметр и конечные точки — два слоя, не один

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Defender активен везде: AMRunningMode=Normal, базы не старше 48 ч
- Хвосты Kaspersky/ESET сняты вендорскими утилитами на 100% парка
- Исключения 1С/КриптоПро перенесены; полный бэкап Veeam Agent до работ

НОРМАЛЬНО

- Dr.Web ESS 13.0: сервер, веб-консоль, группы политик, внешняя БД PostgreSQL
- ASR-правила в Block после двух недель аудита; Tamper Protection включён
- Статус защиты парка в Zabbix: базы, режим агента, алерты в Telegram
- Серверные роли под серверными агентами, сканирование по ночному расписанию

ХОРОШО

- UserGate NGFW: сегментация, COB, SSL-инспекция, VPN вместо открытого RDP
- Логи антивируса и шлюза в единый syslog/SIEM, регламент разбора инцидентов
- Ежеквартальный тест восстановления бэкапа и EICAR-проверка по парку
- Песочница для почтовых вложений на шлюзе при критичных данных

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли в парке машины, где антивирусные базы не обновлялись больше 7 дней?
- [ ] Удалены ли остатки Kaspersky/ESET вендорскими утилитами, а не через «Программы и компоненты»?
- [ ] Defender на станциях в режиме Normal, а не Passive/Disabled (Get-MpComputerStatus)?
- [ ] Перенесены ли исключения для баз 1С, КриптоПро и папок обмена в новое решение?
- [ ] Виден ли статус защиты всех машин в одной консоли или в мониторинге?
- [ ] Закрыт ли RDP из интернета — доступ только через VPN?
- [ ] Сделан ли полный бэкап и проверено ли восстановление перед миграцией?
- [ ] Включён ли Tamper Protection / самозащита агента, чтобы защиту нельзя было снять?
- [ ] Разнесены ли сегменты сети (бухгалтерия/склад/гости) правилами межсетевого экрана?

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 парка за 1–2 дня без остановки работы: что где стоит, состояние лицензий и баз, карта исключений
- Миграция под ключ: зачистка старого AV, раскатка Defender по GPO или Dr.Web ESS, перенос политик и исключений
- Внедрение UserGate NGFW: зонирование, COB, VPN, закрытие RDP — с планом отката
- Мониторинг защиты в нашем Zabbix: свежесть баз, статусы агентов, алерты в Telegram 24/7
- Регламент реагирования: карантин, изоляция узла, восстановление из бэкапа — прописываем и тренируем

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 Attack surface reduction rules reference / Configure Microsoft Defender An… (learn.microsoft.com — 2026)

02 Set-MpPreference, Get-MpComputerStatus — Defender PowerShell (learn.microsoft.com — 2026)

03 Руководство администратора Dr.Web Enterprise Security Suite (download.drweb.com — 13.0.1)

04 Портал документации UserGate NGFW (UGOS 7.5 LTS) (docs.usergate.com — 2026)

05 KB: kavremvr — полное удаление продуктов Kaspersky (support.kaspersky.ru — 2026)

06 KB: ESET Uninstaller (запуск в безопасном режиме) (support.eset.com — 2026)

07 Шаблон ITfresh: GPO ITF_Defender_Baseline + карта исключений 1С (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.