Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Тормозит, а антивирус молчит: наш регламент диагностики

Телеметрия Windows 10/11, Sysinternals и счётчики вместо переустановки

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сотрудник теряет по часу в день на «подождать, пока откроется», а антивирус рапортует «угроз нет». Для бизнеса это два риска сразу: оплаченное, но не отработанное время и скрытая компрометация, которую сигнатурная проверка не видит по определению. Мы не гадаем и не переустанавливаем наугад: снимаем телеметрию и доказываем причину цифрами.

Почему это важно бизнесу

- Тормоза на 15 PM — это фонд оплаты труда, который уходит в ожидание, а не в работу.
- Вердикт «чисто» — не доказательство: fileless-техника не оставляет файла, по которому сверяют хеш.
- Скрытый майнер или adware месяцами живёт на машине бухгалтера, у которой открыт клиент-банк.
- Изношенный SSD и «тяжёлый» агент защиты дают те же симптомы, но лечатся по-разному и стоят разных денег.
- Без телеметрии решение принимается вслепую: переустановка ОС на 20 машин вместо замены двух дисков.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

17.12 / 14.3

Process Explorer и Autoruns: наши рабочие версии Sysinternals; PE v17.12 требует Windows 11+

learn.microsoft.com/sysinternals, 2026

v15.21

Sysmon: ID 1/3/8/19/20/21/22/25 в журнале Microsoft-Windows-Sysmon/Operational

learn.microsoft.com/sysinternals, 2026

4688 + 4104

Аудит создания процессов с командной строкой и PowerShell Script Block Logging

learn.microsoft.com, about_Logging_Windows

1121 / 1122

События ASR: блокировка и аудит в Microsoft-Windows-Windows Defender/Operational

learn.microsoft.com/defender-endpoint, 2026

≤ 10 мс

Наш порог PhysicalDisk\Avg. Disk sec/Read на SSD; устойчиво выше 20 мс — разбор носителя

стандарт ITfresh + Perfmon disk counters

≤ 2 / ядро

System\Processor Queue Length: устойчивое превышение на ядро — очередь к процессору

learn.microsoft.com, Performance Monitor

РЕАЛИЗАЦИЯ 1 ИЗ 3

Экспресс-триаж рабочей станции: 40 минут до вердикта

Что настраиваем

Бухгалтерия, 25 PM, Windows 11 24H2, домен; жалоба «всё тормозит, антивирус чист»

Как мы это делаем

1. Снимаем базу: Get-Counter '\Processor(_Total)\% Processor Time','\System\Processor Queue Length','\PhysicalDisk(_Total)\Avg. Disk sec/Read' -MaxSamples 60
2. Process Explorer v17.12: колонки CPU, Private Bytes, Company Name; включаем Verify Image Signatures и смотрим дерево «родитель → потомок»
3. Autoruns v14.3: Hide Signed Microsoft Entries и Verify code signatures; для парка — autorunsc -a * -h -s -c и сверка CSV с эталоном клиента
4. Журнал Microsoft-Windows-Diagnostics-Performance/Operational: ID 100 (загрузка), 101 (приложение), 102 (драйвер), 103 (служба)
5. Диск: Get-PhysicalDisk | Get-StorageReliabilityCounter — Wear, PowerOnHours, Temperature, ReadErrorsUncorrected

РЕЗУЛЬТАТ

Из 25 машин 4 оказались с износом SSD (Wear > 85%), ещё 3 — с надстройкой в автозагрузке, дававшей 30–40% CPU в фоне. Ни одна не была «заражением». Замена дисков и чистка автозапуска сняли жалобы, на остальных 18 PM мы получили baseline для будущих сравнений.

КЛЮЧЕВОЙ НЮАНС

Пока нет цифр, «тормозит» — не диагноз. Мы всегда начинаем с четырёх измерений: CPU, очередь к CPU, латентность диска и износ носителя, и только потом идём в тему безопасности.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Почему AV «молчит»: разбор персистентности и LOLBins

Что настраиваем

Юрфирма, 18 PM, домен; на двух машинах активность по ночам без открытых окон

Как мы это делаем

1. Включаем GPO «Audit Process Creation» и «Include command line in process creation events» — событие 4688 получает полную командную строку
2. PowerShell: Script Block Logging (4104) и Module Logging (4103) в журнал Microsoft-Windows-PowerShell/Operational
3. Инвентаризация WMI: Get-CimInstance -Namespace root/subscription -ClassName __FilterToConsumerBinding плюс событие 5861 в WMI-Activity/Operational
4. Ставим Sysmon v15.21 с конфигом: ProcessCreate(1), NetworkConnect(3), CreateRemoteThread(8), WmiEvent(19/20/21), DnsQuery(22), ProcessTampering(25)
5. ASR в режиме Audit: 5beb7efe (обфускация), d1e49aac (PsExec/WMI), e6db77e5 (WMI-персистентность); неделю читаем 1122, затем Block

РЕЗУЛЬТАТ

Ночная активность оказалась PUA-загрузчиком, приехавшим с «бесплатным конвертером PDF»: сигнатуры на него не было, а поведение видно в 4688 и Sysmon ID 1/22. Включение PUAProtection и ASR закрыло вектор на всём парке, а не на двух машинах.

КЛЮЧЕВОЙ НЮАНС

Отсутствие детекта — это не «чисто», а отсутствие файла для сверки. Мы закрываем разрыв журналами процессов и сетевых запросов, а не сменой антивируса на «более сильный».

РЕАЛИЗАЦИЯ 3 ИЗ 3

Когда тормозит не вирус, а сам агент защиты

Что настраиваем

Производство, 40 PM и сервер 1С; после смены AV открытие форм 1С выросло вдвое

Как мы это делаем

1. New-MpPerformanceRecording -RecordTo C:\Temp\scan.etl — 10–15 минут под реальной работой пользователя, а не «на холостом ходу»
2. Get-MpPerformanceReport -Path C:\Temp\scan.etl -TopFiles 10 -TopExtensions 10 -TopProcesses 10 -TopScans 10
3. Сверяем Get-MpPreference: ExclusionPath, ExclusionProcess, ScanAvgCPULoadFactor, DisableRealtimeMonitoring — что реально включено
4. Если картина шире антивируса: wpr -start CPU -start DiskIO, затем wpr -stop trace.etl и разбор в WPA из Windows ADK
5. Исключения оформляем точечно: каталоги баз 1С и файлы .1CD/.mdf/.ldf, а не диск целиком; фиксируем в паспорте клиента

РЕЗУЛЬТАТ

Отчёт показал, что большая часть времени сканирования уходила на временные файлы 1С и журналы обмена. Четыре точечных исключения по путям и процессам вернули прежнюю скорость форм, при этом реальная защита осталась включённой — ни одного исключения уровня диска.

КЛЮЧЕВОЙ НЮАНС

Тяжёлый агент защиты — такая же законная причина тормозов, как майнер. Разница в том, что доказывается она отчётом Performance Analyzer, а не отключением защиты «на попробовать».

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Диагноз по Диспетчеру задач**
  Task Manager не показывает родителя процесса, издателя и полный путь. Дерево «кто кого запустил» и подписи даёт только Process Explorer.

- ✕ **Исключения антивируса «на весь диск»**
  Широкий ExclusionPath вида C:\ выключает защиту тома целиком. Исключения задаём по конкретным каталогам и процессам, с записью в паспорт.

- ✕ **Autoruns без проверки подписей**
  Без Verify code signatures и Hide Signed Microsoft Entries список автозапуска нечитаем: сотни строк, в которых аномалию не найти.

- ✕ **4688 без командной строки**
  Без политики «Include command line in process creation events» событие 4688 показывает только имя процесса — доказать ничего нельзя.

- ✕ **Журналы, которые перекрываются за часы**
  Штатные размеры Security и PowerShell/Operational перекрываются за часы. Увеличиваем объём и настраиваем пересылку через WEF.

- ✕ **ASR сразу в режим Block**
  Правила PsExec/WMI и WMI-персистентности ломают агенты управления. Всегда сначала Audit, разбор событий 1122, только потом Block.

- ✕ **«Healthy» вместо счётчиков диска**
  HealthStatus «Healthy» не отменяет Wear 90% и растущих ReadErrorsUncorrected. Решение принимаем по счётчикам надёжности.

- ✕ **Переустановка вместо разбора**
  Reimage без ответа «как зашло» возвращает проблему через недели. Сначала артефакты и вектор входа, потом чистая ОС.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Sysinternals Suite у инженера: Process Explorer, Autoruns, Procmon, Sigcheck
- Defender: облачная защита включена, PUAProtection = Enabled через Set-MpPreference
- Аудит создания процессов 4688 с командной строкой на всех рабочих станциях
- Квартальная выгрузка autorunsc и сверка с эталоном по каждой машине

НОРМАЛЬНО

- Script Block Logging 4104, увеличенные журналы и сбор через Windows Event Forwarding
- Стандартный набор ASR-правил: неделя в Audit, разбор 1122, затем Block
- Baseline Perfmon: CPU, Processor Queue Length, Avg. Disk sec/Read, память
- Ежемесячный опрос root\subscription по всему парку скриптом

ХОРОШО

- Sysmon v15.21 с типовым конфигом на всех PM и централизованный сбор событий
- EDR с поведенческим анализом и изоляцией хоста в один клик
- AppLocker или App Control (WDAC): запрет запуска из %APPDATA% и %TEMP%
- S.M.A.R.T./Wear дисков в Zabbix с порогами и авто-заявкой на замену

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знаем ли мы, какой процесс держал CPU в момент жалобы, или судим по словам пользователя?
- [ ] Включён ли аудит 4688 с командной строкой и Script Block Logging 4104 на всех станциях?
- [ ] Есть ли эталонная выгрузка автозапуска (autorunsc CSV), с которой можно сравнить «сейчас»?
- [ ] Проверялись ли WMI-подписки root\subscription за последние 30 дней хотя бы выборочно?
- [ ] Нет ли в антивирусе исключений уровня диска, спрятанных «чтобы 1С не тормозила»?
- [ ] Сняты ли Wear и ReadErrorsUncorrected по всем SSD старше трёх лет?
- [ ] Есть ли baseline счётчиков, с которым сравнивается заявление «стало медленно»?
- [ ] Прогонялись ли ASR-правила в режиме Audit до включения блокировки?
- [ ] Собираются ли журналы централизованно, или они умирают вместе с машиной?
- [ ] Известен ли вектор входа по последнему инциденту, или машину просто переустановили?

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).

- Экспресс-триаж станции: телеметрия, Process Explorer/Autoruns, S.M.A.R.T. — заключение за 2–4 часа
- Разворачиваем аудит 4688/4104, Sysmon и централизованный сбор журналов на парк до 50 PM
- Настраиваем ASR и PUA-защиту Defender: Audit → разбор 1122 → Block без простоя бизнеса
- Разбираем тормоза от самого агента защиты через Defender Performance Analyzer и WPR
- Ведём паспорт парка: baseline счётчиков, эталон автозапуска, состояние носителей

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 Sysinternals: Process Explorer v17.12, Autoruns v14.3, Sysmon v15.21 (learn.microsoft.com — 2026)

02 Attack surface reduction rules reference (GUID, Audit/Block) (learn.microsoft.com — 2026)

03 Block potentially unwanted applications with Defender Antivirus (learn.microsoft.com — 2026)

04 Performance analyzer for Microsoft Defender Antivirus (learn.microsoft.com — 2026)

05 Command line process auditing (4688) + about_Logging_Windows (4104) (learn.microsoft.com — 2026)

06 Get-StorageReliabilityCounter, Get-PhysicalDisk (модуль Storage) (learn.microsoft.com — 2026)

07 Windows Performance Recorder / Analyzer (Windows ADK) (learn.microsoft.com — 2026)

08 Регламент триажа рабочих станций ITfresh (itfresh.ru (внутр.) — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.