Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

AppLocker в офисе: белые списки запуска программ

Как мы строим whitelist-контроль запуска через GPO: правила, режим аудита, перевод в enforce

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Пользователи ставят на рабочие станции неучтённый софт — от торрент-клиентов до «активаторов», а фишинговые вложения запускают PowerShell-нагрузку. Итог: шифровальщики, простои, юридические риски нелицензионного ПО. Мы закрываем класс проблемы целиком: переводим парк на модель «запрещено всё, что явно не разрешено» штатным AppLocker — без агентов и покупки стороннего софта.

Почему это важно бизнесу

- Шифровальщик из фишингового вложения — это простой всего офиса на дни; AppLocker режет запуск полезной нагрузки ещё на старте процесса
- Нелицензионный софт на рабочих машинах — прямой юридический риск для компании при любой проверке
- «Левый» софт — постоянный источник фоновых сбоев и обращений в поддержку; чистый парк заметно дешевле в сопровождении
- Механизм штатный: входит в Windows, лицензий и агентов не требует — компания платит только за внедрение и сопровождение

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2004+

версия Windows 10, с которой enforcement работает на любой редакции, включая Pro (KB5024351);…

по докам Microsoft Learn

4+1

коллекции правил: EXE, MSI, скрипты, packaged apps + отдельно DLL для строгого профиля

AppLocker, learn.microsoft.com

10 раб. дн

держим политику в Audit only и собираем события 8003/8006 перед включением блокировок

наш стандарт

8004/8007

события enforce-блокировок EXE/DLL и MSI/скриптов — на них строим алертинг и разбор обращений

журнал AppLocker

3

типа условий в правиле: издатель (подпись), путь, хэш файла — приоритет всегда отдаём издателю

по докам Microsoft Learn

Automatic

автозапуск службы Application Identity (AppIDSvc) фиксируем через GPO — без неё правила не при…

по докам Microsoft Learn

РЕАЛИЗАЦИЯ 1 ИЗ 3

Инвентаризация ПО и проектирование правил

Что настраиваем

Все рабочие станции домена AD; фактуру собираем с эталонных машин каждой роли: бухгалтерия, менеджеры, производство

Как мы это делаем

1. Снимаем срез ПО: Get-AppLockerFileInformation -Directory 'C:\Program Files' -Recurse плюс выгрузка установленных пакетов с каждой машины в общий CSV
2. Делим найденное на три корзины: рабочее, допустимое личное, запрещённое; итоговый список утверждает руководитель заказчика
3. Строим правила от издателя (publisher) для подписанного софта: Microsoft, 1С, Kaspersky; хэш-правила — только для неподписанных exe
4. Path-правила ограничиваем C:\Windows и C:\Program Files, а подкаталоги внутри них с правом записи пользователя закрываем явными deny
5. Черновик собираем New-AppLockerPolicy и прогоняем Test-AppLockerPolicy по срезу файлов ещё до публикации в GPO

РЕЗУЛЬТАТ

Ещё до включения политики получаем полную карту софта парка и вычищаем неучтённое ПО. Правил в итоге 30–60 вместо сотен хэшей — политика остаётся читаемой и сопровождаемой любым инженером смены.

КЛЮЧЕВОЙ НЮАНС

Правило от издателя переживает обновления версий, хэш — нет: после апдейта неподписанной программы хэш-правило перестаёт совпадать. Поэтому долю хэшей минимизируем и каждый помечаем в комментарии.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Развёртывание через GPO и режим Audit only

Что настраиваем

Отдельная OU рабочих станций, GPO AppLocker-Workstations; контроллеры домена и серверы 1С из области действия исключаем

Как мы это делаем

1. Создаём GPO: Computer Configuration → Windows Settings → Security Settings → Application Control Policies → AppLocker, импортируем XML политики
2. Тем же GPO фиксируем службу Application Identity (AppIDSvc) в Automatic через System Services — из оснастки services.msc тип не сменить, служба защищённая; резерв —…
3. Все коллекции ставим в Enforcement: Audit only; на пилотную группу из 3–5 машин применяем полный набор правил сразу
4. Ежедневно собираем события 8003/8006 из журналов Microsoft-Windows-AppLocker (EXE and DLL, MSI and Script) скриптом на Get-WinEvent в общий CSV
5. По итогам 10 рабочих дней дописываем исключения на легитимный софт из нестандартных путей — обычно выходит 10–20 правил

РЕЗУЛЬТАТ

Пользователи весь период аудита работают без единой блокировки, а мы получаем реальную статистику запусков по каждой машине. К моменту включения enforce политика уже отлажена — шквала обращений в поддержку в первый день не бывает.

КЛЮЧЕВОЙ НЮАНС

Событие 8003 «would have been blocked» — главный рабочий инструмент: если за период аудита по файлу нет 8003, правило под него не нужно. Исключения пишем только по фактам журнала, не «на всякий случай».

РЕАЛИЗАЦИЯ 3 ИЗ 3

Перевод в Enforce и регламент эксплуатации

Что настраиваем

Весь парк станций; включение вне рабочих часов, план отката — переключение GPO обратно в Audit only за один gpupdate

Как мы это делаем

1. Переключаем коллекции в Enforce rules, форсируем gpupdate /force и сверяем применение через Get-AppLockerPolicy -Effective на контрольных машинах
2. Настраиваем алертинг на события 8004/8007: выгрузка в мониторинг, каждая блокировка разбирается в день обращения
3. Новый софт вводим по регламенту: заявка → установка в Program Files из проверенного дистрибутива → publisher-правило в GPO → gpupdate
4. Раз в квартал ревизия: выгружаем политику Get-AppLockerPolicy -Xml, сверяем с документацией, удаляем мёртвые хэш-правила

РЕЗУЛЬТАТ

Политика живёт годами без деградации: новый софт попадает в белый список за одну заявку, попытки запуска постороннего видны в мониторинге, а фишинговая нагрузка умирает на событии 8004 ещё до старта процесса — до повышения привилегий дело не доходит.

КЛЮЧЕВОЙ НЮАНС

Get-AppLockerPolicy -Effective показывает реально применённый набор с учётом наследования GPO — сверяем именно его, а не содержимое оснастки; проверку повторяем после каждого изменения политики.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Enforce без этапа аудита**
  Блокирует легитимный софт из нестандартных путей в первый же день; мы держим Audit only 10 рабочих дней и разбираем события 8003/8006

- ✕ **Правила по умолчанию «как есть»**
  Default rules разрешают всё из Program Files и Windows, включая подкаталоги с правом записи пользователя; закрываем их явными deny-правилами

- ✕ **AppIDSvc не переведена в Automatic**
  Служба защищённая, из оснастки Services тип запуска не меняется; задаём автозапуск через GPO System Services или sc.exe config appidsvc start=auto, п…

- ✕ **Path-правила на пользовательские папки**
  Разрешение на %USERPROFILE% или %TEMP% обнуляет весь whitelist — туда пишет сам пользователь; разрешаем только пути, требующие прав администратора

- ✕ **Хэш-правила на обновляемый софт**
  После каждого апдейта хэш меняется и запуск ломается; для подписанного ПО используем условия издателя, хэш оставляем как последний резерв

- ✕ **AppLocker на контроллерах домена**
  Блокировка системного компонента на DC — риск потерять управление доменом; DC и серверные роли выносим в OU вне области действия GPO

- ✕ **DLL-коллекция игнорируется**
  Без правил для DLL контроль обходится подгрузкой посторонних библиотек; включаем коллекцию после обкатки EXE-правил, начиная с Audit only

- ✕ **Нет документации по исключениям**
  Через год никто не помнит, зачем правило существует; каждое исключение документируем в поле Description с датой, причиной и номером заявки

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Инвентаризация ПО парка и белый список, согласованный с руководителем
- AppLocker в Audit only: коллекции EXE, MSI, Script через GPO на OU станций
- AppIDSvc = Automatic через GPO, разбор журналов аудита раз в неделю

НОРМАЛЬНО

- Enforce rules для EXE/MSI/Script + deny на записываемые подкаталоги Windows
- Publisher-правила для основного софта, регламент ввода нового ПО
- Центральный сбор событий 8003–8007 и разбор блокировок в день обращения
- Комментарий в каждом правиле + квартальная ревизия политики

ХОРОШО

- DLL-коллекция в Enforce после обкатки, packaged apps под контролем
- Алертинг 8004/8007 в мониторинг (Zabbix/почта), SLA на добавление исключений
- Отдельные наборы правил по ролям OU: бухгалтерия, менеджеры, инженеры
- Для критичных узлов — App Control for Business (WDAC) поверх AppLocker

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Редакции и версии парка проверены: до Windows 10 2004 enforcement через GPO работает только на Enterprise/Serve…
- [ ] Служба Application Identity закреплена в Automatic групповой политикой, а не вручную на машинах?
- [ ] Политика прожила в Audit only не меньше 10 рабочих дней до включения блокировок?
- [ ] Подкаталоги Windows и Program Files с правом записи пользователя закрыты явными deny-правилами?
- [ ] Доля хэш-правил минимальна, а обновляемый подписанный софт покрыт правилами издателя?
- [ ] Контроллеры домена и серверы исключены из области действия GPO с AppLocker?
- [ ] События 8003/8004/8006/8007 собираются централизованно и регулярно разбираются?
- [ ] Есть регламент ввода нового ПО: кто одобряет, кто пишет правило, в какой срок?
- [ ] Каждое правило снабжено комментарием: дата, причина, номер заявки?
- [ ] Откат проверен: переключение GPO обратно в Audit only возвращает работу за один gpupdate?

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 установленного ПО всего парка и согласование белого списка с руководством
- Проектирование и развёртывание политик AppLocker через GPO: EXE, MSI, Script, DLL
- Этап Audit only с разбором журналов и доводкой исключений до включения блокировок
- Перевод в Enforce, алертинг на блокировки и регламент ввода нового софта
- Сопровождение: квартальная ревизия правил, документация, обучение вашего админа

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 AppLocker overview (learn.microsoft.com — 2025)

02 Requirements to use AppLocker (KB5024351) (learn.microsoft.com — 2025)

03 Configure the Application Identity service (learn.microsoft.com — 2025)

04 Using Event Viewer with AppLocker (learn.microsoft.com — 2025)

05 AppLocker deployment guide (learn.microsoft.com — 2025)

06 AppLocker PowerShell cmdlets (Get-/New-/Set-/Test-AppLockerPolicy) (learn.microsoft.com — 2025)

07 Шаблон ITfresh: GPO AppLocker-Workstations + скрипт сбора событий (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.