Nevel

БЕЗОПАСНОСТЬ

Корпоративная среда и российские средства ИБ

Как включить Nevel в корпоративный контур с SIEM, DLP, сетевым шлюзом и IdP; точки контроля, соединения и программа проверки.

Облако / В контуре

https://docs.nevel.sh/security/corporate-environment/

Nevel включается в существующую среду компании через отдельные соединения для входа, модельных запросов, контроля содержания и доставки событий. Для каждого соединения определяются инициатор, получатель, видимые данные, аутентификация и поведение при недоступности. Это позволяет использовать корпоративные средства ИБ, сохраняя понятную границу ответственности между платформой и инфраструктурой заказчика.

Ниже приведены российские продукты с документированными производителем интерфейсами и варианты их места в архитектуре. Это **основа проектирования интеграции**, а не перечень испытанной совместимости Nevel. Подтверждённая интеграция относится к конкретным версиям, настройкам и протоколу испытаний. Ссылка на документацию производителя не подтверждает наличие у Nevel сертификата, готового коннектора или совместного внедрения.

Какие средства за что отвечают

Задача	Примеры продуктов	Документированный механизм	Место в проекте Nevel
Собирать и разбирать события	Kaspersky KUMA	Нормализаторы JSON, CEF и Syslog, сопоставление полей	Получатель событий платформы и инфраструктуры
Централизовать события и правила их обработки	MaxPatrol SIEM	Сбор событий и правила нормализации	Разбор отдельного источника Nevel по подготовленному профилю
Принимать Syslog	UserGate SIEM	TCP/UDP, TLS для TCP, ограничения отправителей	Корпоративный приёмник либо следующий узел после relay
Контролировать сетевой путь и передавать содержание на проверку	UserGate NGFW	Инспектирование TLS и подключения к ICAP-серверам	Сетевой шлюз и клиент DLP, если этот путь выбран в проекте
Проверять содержание средствами корпоративной DLP	InfoWatch Traffic Monitor	Интеграционные API; опубликованные примеры ICAP/ICAPS	Отдельная точка анализа в разрешённой схеме
Выполнять корпоративную аутентификацию	Avanpost FAM	SAML, OpenID Connect и другие механизмы интеграции	IdP для корпоративного входа в согласованном профиле SSO

Основания таблицы: KUMA — парсинг событий, MaxPatrol SIEM — нормализация, UserGate SIEM — Syslog, UserGate NGFW — ICAP, интеграции InfoWatch Traffic Monitor, Avanpost FAM. ICAP/ICAPS у InfoWatch также описаны на примере интеграции с DION; этот пример относится к указанным производителем продуктам и не является свидетельством интеграции с Nevel.

Обычный сетевой экран, DLP и специализированный AI firewall решают разные задачи. Сетевой экран управляет соединениями. DLP анализирует доступное ему содержание. AI firewall или модельный шлюз может быть включён в прикладную цепочку, если его интерфейс поддерживает нужные форматы модельного API. Поддержку streaming, инструментов, изображений и форматов ошибок проверяют отдельно; она не следует из наличия HTTPS или ICAP. Принцип подключения собственного AI firewall описан в сетевой защите.

Где средство видит исходный текст

Выбор точки контроля определяет область раскрытия. TLS защищает данные между точками завершения соединения; средство, которое анализирует тело запроса, получает доступ к расшифрованному содержимому соответствующего участка.

Точка контроля	Что доступно средству	Что проверить
До Guardrail и маскирования	Исходный запрос или извлечённый текст; оригинал файла — только если он передан этой стадии	Разрешение на обработку оригинала, дополнительные копии, журналы и временные файлы
После маскирования, перед моделью	Подготовленный модельный контекст с масками и оставшимся содержанием	Сохранение масок, роли сообщений, вложений и параметров; отсутствие обходного вызова
На ответе до восстановления	Ответ модели с маркерами	Сохранение структуры ответа, streaming и возврат результата контроля
После восстановления	Результат с восстановленными значениями	Отдельная чувствительная граница; не пересылать сюда ответ автоматически ради дополнительной проверки
Копия трафика или экспорт событий	Только реально переданный экземпляр или метаданные	Копирование не является синхронным разрешением на отправку исходного запроса

Если браузер отправил файл в Platform, а Platform позже извлекла текст и добавила фрагменты RAG, перехват только браузерного соединения не показывает итоговый контекст модели. И наоборот, контроль модельного запроса после маскирования не даёт DLP оригинальных значений. Для цели «проверить весь фактически отправляемый контекст» точка контроля связывается со сборкой контекста, а не только с пользовательским интерфейсом.

СХЕМА 1

Две возможные точки контроля

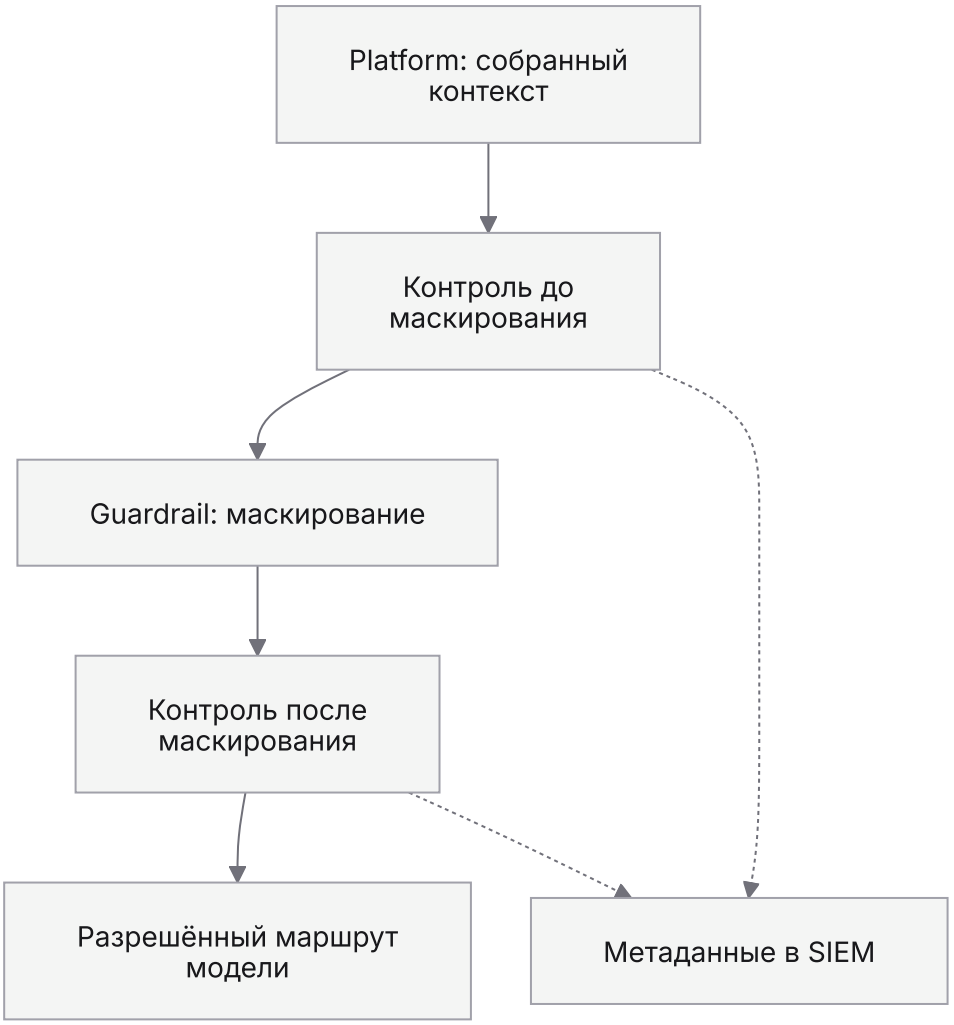


Схема показывает места включения, а не необходимость последовательно устанавливать два одинаковых продукта. Если выбрана одна точка, другая не добавляется автоматически. Обратный путь ответа и точку восстановления фиксируют в паспорте подключения отдельно.

Выбор адреса и способа подключения

Есть три разных способа включить контроль. **Модельный reverse proxy** становится адресом, на который настроен модельный клиент; он сохраняет контракт запросов и ответов. **Сетевой proxy с DLP по ICAP** принимает сетевой трафик и отправляет доступное содержание DLP; ICAP-адрес не является OpenAI-compatible endpoint. **Адаптер анализа** вызывает отдельный API проверки в выбранной стадии приложения; для него нужны спецификация вердикта и согласованная реализация подключения.

Не подставляйте ICAP-адрес вместо базового URL модели. Не используйте адрес веб-консоли DLP как API анализа. Получите адрес именно принимающего сервиса, его протокол, требования к сертификатам и поддерживаемые операции. Точные URL и секреты принадлежат конфигурации установки; в публичных примерах используются только зарезервированные демонстрационные домены.

Соединение	Параметры конфигурации	Контроль результата
Platform → модельный шлюз	Базовый URL, разрешённые пути, авторизация, CA, тайм-ауты	Сохраняются модель, сообщения, tools и события окончания потока

Соединение	Параметры конфигурации	Контроль результата
Сетевой шлюз → DLP	Адрес/порт ICAP или другой подтверждённый интерфейс, направление проверки, предел сообщения	Проверка действительно получает нужное тело, а не только заголовок
Platform → IdP	Metadata/discovery, идентификатор приложения, адрес возврата и доверие	Ответ предназначен этому приложению; корпоративные атрибуты правильно связаны с учётной записью
Экспортер → relay/SIEM	Адрес приёмника, формат события, транспорт, сертификаты, область организаций	Событие принято, разобрано и находится по исходному ID

В UserGate NGFW документация ICAP перечисляет адрес, порт, предел сообщения, проверку доступности, направления REQMOD/RESPMOD и параметр `bypass`. Последний допускает работу без передачи в недоступный ICAP-сервер. Поэтому для обязательного контроля проверяются и настройка bypass, и действия соответствующих правил; итог подтверждается тестом отказа. Параметры ICAP, работа с внешними ICAP-серверами.

Облако, on-prem и размещение промежуточных узлов

On-prem определяет место Platform, а не расположение каждой модели. Платформа заказчика может обращаться к локальной модели, разрешённому российскому провайдеру, self-hosted модели Nevel в РФ или глобальному провайдеру. Корпоративный шлюз проверяет именно выбранные маршруты. Матрица размещения отделяет их от изолированного профиля.

Для облачной Platform корпоративное средство заказчика должно быть доступно по явно подготовленному защищённому соединению, если его включают в обязательный рабочий путь. Наличие средства во внутренней сети не даёт облаку такой доступ автоматически. Маршрут включает сеть, DNS, сертификаты, ограничения источников и обратный ответ; исходные хранилища и административные консоли для этого не публикуются.

Relay для событий можно разместить у заказчика или на выделенной разрешённой площадке в РФ. Он завершает входящее соединение, при необходимости преобразует формат и доставляет события в SIEM. Это отдельный обработчик метаданных: его дисковая очередь, диагностика и резервирование входят в схему хранения. Размещение relay в РФ не определяет географию модельного запроса; модельный путь и путь аудита рассматриваются независимо.

В изолированном профиле модели, средства анализа, IdP, relay и SIEM рабочего процесса находятся внутри заданной границы. В обычном on-prem допустимы разрешённые внешние соединения. Ни один профиль не должен скрыто переключаться на другого модельного получателя из-за недоступности средства контроля.

Корпоративный вход

Avanpost FAM предоставляет механизмы SAML и OpenID Connect для подключения приложений, а также способы интеграции с каталогами учётных записей. Это подтверждённые возможности IdP, а не готовый профиль Nevel. Описание FAM, документация FAM 1.17.

При проектировании определяются стабильный идентификатор пользователя, допустимые атрибуты, группы и процедура изменения членства. Успешный ответ IdP создаёт проверенную идентичность, но не должен автоматически превращать каждую группу каталога в административную роль Platform. Для входа, сервисного API-ключа и чтения событий SIEM действуют отдельные полномочия. Подробности — идентификация и права.

Как принять интеграцию

ИТ фиксирует версии Nevel и подключаемого продукта, размещение узлов и конфигурацию соединений; ИБ определяет видимое содержание и обязательность контроля; владелец SIEM проверяет разбор событий. На стенде выполняются текстовый запрос, streaming, файл, разрешённый инструмент, отмена, ошибка провайдера, недоступность контрольного узла и приём события.

Для каждого результата должны быть исходный ID операции, запись на контрольном компоненте и запись у получателя аудита. Проверяются сохранность структуры сообщения и невозможность обойти обязательный шлюз альтернативным адресом. Одна успешная проверка соединения подтверждает лишь доступность адреса, а не корректность всего сценария.

Итоговый комплект: схема фактических соединений, таблица видимых данных, профиль настроек без секретов, reference mapping событий и протокол проверенных сценариев с ограничениями. Пошаговое подключение и проверка доставки раскрыты в SIEM-процессе; структура событий — в профиле аудита.

Версии и совместимость

Параметры подключения относятся к KUMA 3.0.1, MaxPatrol SIEM 8.1, UserGate 7.x и Avanpost FAM 1.17. Перед настройкой сверяйте интерфейсы с установленным выпуском и лицензией. Описанный интерфейс продукта не подтверждает совместимость с Nevel: для выбранной конфигурации нужен протокол испытаний.