

Видима достъпност. Проследими доказателства.

Технически и стратегически white paper

Продуктова основа, мрежово разширяване и път към обясним анализ на инциденти.

БЪЛГАРСКО ИЗДАНИЕ | v1.2

04 октомври 2026 г.

Публично издание.

Реални браузъри + различни мрежови маршрути + история на доказателствата + обясним анализ

Как да четете документа

За клиенти, партньори и поддръжници на кампанията

Обозначения: ТЕКУЩО описва настоящия обхват; ПОТВЪРДЕНО ОТ СОБСТВЕНИКА - негови данни за разгръщания и тестове; ПРОВЕРЕНО В КОДА - ограничени проверки на реализацията; ПЛАНИРАНО и РЕФЕРЕНТЕН ДИЗАЙН не са внедрени гаранции. Изданията са със съпоставим обхват. Това не е независим одит, финансов проспект, обвързващ график или правно становище.

01 Резюме	3
02 Проблемът и пропуските в наблюдението	4
03 Защо ISP и мобилната видимост са важни	5
04 Как работи EyeballMonitor	6
05 Реални браузъри и визуални доказателства	7
06 Проследимост и произход на доказателствата	8
07 Модел на управлявана разпределена мрежа	9
08 Текуща мрежа срещу целево разширяване	10
09 Мрежова карта и операторски цели	11
10 Хронология на инцидента и живот на доказателствата	12
11 Клиентски сценарии и реалистична стойност	13
12 Контролирани браузърни сценарии	14
13 Third-Party Dependency Intelligence	15
14 Откриване на зависимости и обяснима корелация	16
15 Incident Agent и автономни доказателства	17
16 Сигурност, поверителност и клиентски граници	18
17 Ограничения, нетвърдения и валидиране	19
18 Пътна карта и условия за приемане	20
19 Търговски модел и контекст на кампанията	21
20 FalcoSoft ITS и отговорност за реализацията	22
21 Приложение: термини и оперативни мерки	23
Източници и основа на документа	24

01 / Резюме

От наличност на сървъра към наблюдаемо потребителско изживяване

EyeBallMonitor е платформа за мониторинг на сайтове, изградена около един основен въпрос: какво действително е наблюдавал браузърът през конкретен мрежов маршрут в конкретен момент? Тя съчетава проверки за достъпност, регионални наблюдения, визуализация в браузър и снимкови доказателства. Целта е оперативните екипи да имат обща фактологична основа, когато сайтът изглежда изправен централно, но не работи за част от аудиторията.

Публичният продукт вече представя работеща основа: uptime, време за отговор и HTTP резултати; снимки от браузър и профили на устройства; история на инцидентите; клиентски работни пространства; Full Website Check с технически анализ DAX. Това са възможности, описани в сайта и предоставените демонстрации, а не независима сертификация на всеки производствен процес. [1, 2]

Собственикът потвърждава четири действащи дейтацентърни локации и 28 по-рано тествани мобилни точки с мини-PC/SIM рутери, спрени поради липса на средства за експлоатация. Първият финансиран мобилен етап цели общо 80 агента, а не 80 допълнителни. Анализът на зависимости, обяснимата корелация и контролираният Incident Agent остават в пътната карта. Каталогът за 180 държави е дългосрочен план, а не разгърнато покритие. [2, 3]

Проектът е поетапно начинание за няколко години, а не обещание за завършване на глобална мрежа и сложен анализ на инциденти за няколко месеца. Първото мобилно разгръщане е една стъпка. Напредъкът следва проверени маршрути, надеждни доказателства, оперативен капацитет и устойчиви приходи.

Основна теза: успешният HTTP отговор е едно наблюдение, а не пълна картина на потребителското изживяване.

02 / Проблемът и пропуските в наблюдението

Един сайт може да има различна достъпност за различни потребители

Една централна проверка може полезно да потвърди, че услугата е отговорила от нейната собствена локация. Тя не установява, че всеки DNS резолвер, оператор, CDN възел, браузър или приложна зависимост е работил по същия начин. Мониторингът от център за данни остава полезен; EyeballMonitor цели да го допълни с други гледни точки, а не да го отхвърли.

Частични откази могат да възникнат преди HTTP заявката, при защитеното свързване, при получаването на отговора или след зареждането на документа. Страница може да върне 200 и все пак да показва приложна грешка, защитна проверка, неизползваем интерфейс или неработещо плащане. Затова всяка проверка трябва да определя както маршрута, така и критерия за успех.

Слой на отказа	Какво да се наблюдава
DNS / свързаност	Неуспешно разрешаване, timeout, грешка при свързване; липсата на данни не е доказан отказ на сайта.
TLS / HTTP	Валидиране на сертификата, редиректи, статус, време за отговор и клас на грешката.
Браузър / приложение	Визуализирано съдържание, очаквани елементи, защитни проверки и разрешени проверки без промяна на данни.
Зависимост / регион	Засегнати маршрути, външни компоненти и съпоставени по време доказателства; корелацията не доказва причина.

Доказателствата първо трябва да отговорят къде, кога и какво е отказало, а след това защо.

03 / Защо ISP и мобилната видимост са важни

Операторското разнообразие добавя повече от географията

Двама потребители в един град може да използват различни мрежи за достъп, резолвери, peering връзки, IP протоколи и CDN възли. Мобилната връзка добавя операторски NAT, вариации в радиосигнала и различни маршрутизационни политики. Това има значение при инциденти, засягащи част от аудиторията. Географията е едно измерение, а независимо използваният маршрут за достъп е друго.

Архитектурата цели наблюдения през действителен фиксиран ISP и мобилен достъп там, където връзката е осигурена и проверена. Браузър на хостван сървър в дадена държава дава хоствана перспектива, а не автоматично потребителска или мобилна. Продуктът трябва да пази тази разлика, дори когато и двата вида точки са оперативно полезни.

Разнообразието е ценно само когато е реално. Няколко агента може да споделят доставчик, изходен адрес или физическа линия. Затова целите по държави и оператори се оценяват по независимост, повторяемост и относимост към клиентския трафик, а не само по брой. Публична ASN справка е помощна информация, а не заместител на проверен инвентар.

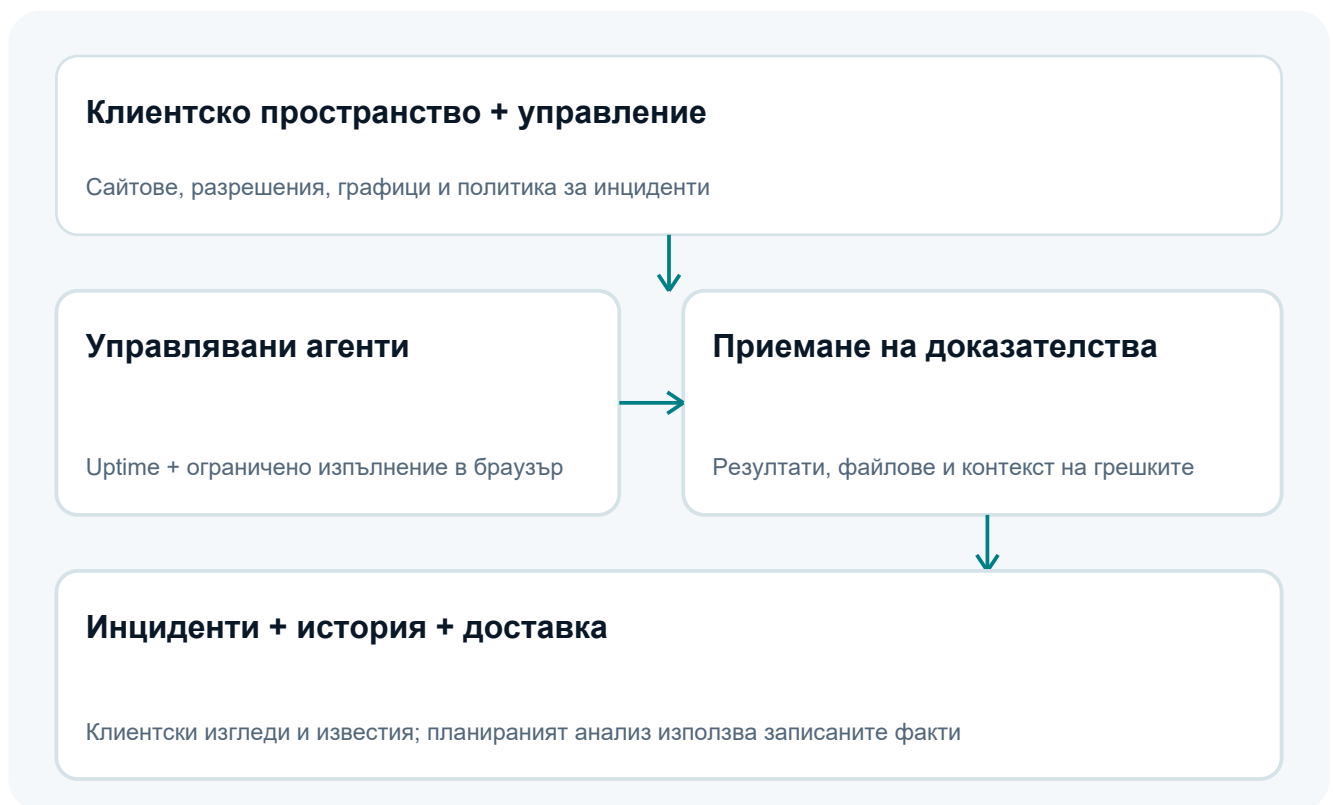
Търсеният резултат е по-точно твърдение: този сайт отказа при тези условия през този проверен маршрут, докато сравняваните маршрути се държаха различно. Това е по-силно оперативно доказателство от неподкрепено твърдение, че цяла държава или всички потребители са били без достъп.

04 / Как работи EyeballMonitor

Разделяне на организацията, наблюдението и интерпретацията

Клиентът добавя сайт, избира политика за мониторинг и преглежда резултати по маршрути. Леките uptime проверки откриват промени в достъпността; браузърните задачи добавят визуални доказателства. Full Website Check събира браузърните резултати с техническите диагностики DAX. Публичният продукт включва клиентски пространства, история и настройки за известия. [1, 2]

Диаграмата е логическа референтна архитектура, а не разкриване на производствената топология или твърдение за инсталирана конкретна опашка, база данни или система за съхранение. Управляващият слой определя клиентския обхват, политиките и задачите. Агентите изпълняват ограничени проверки и връщат структурирани наблюдения. Хранилището запазва доказателствата, а логиката за инциденти и работниците за доставка ги превръщат в видими за клиента събития.



Изискване към референтния дизайн: отказал работник за известия не трябва да изтрива инцидента или да блокира приемането на доказателства.

05 / Реални браузъри и визуални доказателства

Условията на всяко наблюдение трябва да са ясни

Всяка проверка трябва да пази целта, идентичността на маршрута, момента на изпълнение, версията на софтуера, профила на устройството, timeout и резултата. При редирект се запазват началният и крайният URL. Времето за отговор изисква определение: продължителност на заявката, навигацията и готовността за визуализация не са взаимозаменяеми. Timeout не трябва да се отчита като измерено време за успешен отговор.

Изгледите за desktop, Android, iPhone и tablet дават полезни перспективи за оформлението. Браузърната емуляция може да задава viewport, мащаб, user agent и поведение при докосване. Тя не превръща хоста във физически телефон и не проверява операционната система, модема, батерията, мобилното радио или конкретна версия на нативния браузър. [8]

Политиката за успех трябва да е явна: HTTP достъпност, видимо очаквано съдържание и разрешен потребителски сценарий са различни тестове. Защитни проверки, cookie диалози и екрани за съгласие се записват, а не се заобикалят скрито. Грешка при навигация може да попречи на нормална снимка на страницата; отказът остава полезно доказателство, когато точната грешка и контекстът са запазени.

Сравненията трябва да отчитат разминаване във времето, различни резолвери, кешове, персонализирано съдържание и натоварване на агента. Маршрутът може да е недостъпен при здрав агент; нездрав агент може да не дава надеждна информация за сайта. Липсващите данни трябва да останат с неизвестен статус.

06 / Проследимост и произход на доказателствата

Снимката е полезна, когато контекстът е запазен

Снимката записва визуално наблюдение, а не всеобща достъпност или доказана отговорност. Записът пази време, локация, заявен/краен URL, HTTP резултат, профил на устройство и контекст на проверката. Собственикът потвърждава събирането на тези данни. Неуспешната навигация или снимка трябва да остава различима от успешно заредена страница.

Ограниченият преглед на кода установи изчисляване на SHA-256 върху изображението в агентите в Полша, Милано и Лондон и хешово свързани записи в журнала на централната система. API за начално качване проверява формата на подадения хеш. Не е установен завършен процес за проверка на съхранения файл; полетата за подпис на агента и сървъра се създават празни. Турският агент не е проверен поради липса на SSH достъп.

Тези внедрени механизми подпомагат проследимостта, но не установяват цифрово удостоверен произход, неизменяемо съхранение или независимо одитирана верига на съхранение. Препоръчва се трайно пазене на хешове, проверка след качване/експорт, подписани описания, защитени одитни записи и отделяне на оригиналите от редактираните копия.

Група полета	Референтен запис
Идентичност	Идентификатори на клиент, сайт, монитор, инцидент, задача и агент; конкретен маршрут и профил.
Време и изпълнение	UTC моменти за планиране, начало, край и получаване; версии на runner и браузър; timeout.
Мрежов резултат и страница	Начален/краен URL, наличен HTTP статус, клас грешка, определение на продължителността и режим на снимката.
Файл и съхранение	Идентификатор, тип, достъп и съхранение; агентът изчислява SHA-256, а пълната трайна проверка и подписите изискват доразвитие.

Внедреното хеширане не е завършена система за цифрови подписи, гаранция за неизменяемост или автоматична юридическа допустимост.

07 / Модел на управлявана разпределена мрежа

Контролирано разгръщане, а не анонимен доброволен капацитет

Мобилният модел използва Linux мини-PC-та със SIM рутери на избрани мобилни оператори, разположени в наети колокационни места. Физическото място и изходният интернет маршрут са различни факти: за мобилен маршрут трафикът трябва да преминава през съответната SIM връзка, а не незабелязано през връзката на центъра. Архитектурата е описана от собственика, а не независимо одитирана точка по точка.

Нов маршрут следва да премине поетапно включване: допустимо местно разполагане, проверка на вида връзка, регистрация на агента, версия, синхронизация на часовника, ограничено браузърно изпълнение и успешно качване. Ключовете трябва да са отделни за агент и отменяеми. Замяната и извеждането от работа обновяват инвентара и обезсилват старите идентичности.

Управлението на здравето отделя деградацията на агент от отказ на сайт. Остарял heartbeat, отказал браузър, опашка, часово разминаване и проблеми при качване изискват явни причини. Автоматичното възстановяване е ограничено и ескалира повторните откази. Обновяването следва да има тест за съвместимост и връщане назад, а не едновременно да променя всички маршрути.

Собственикът потвърждава, че 28 мобилни точки са изпълнявали реални uptime проверки и браузърни снимки. Те са спрени, защото наемът за колокация, SIM интернетът и другите текущи разходи изискват финансиране. Софтуерът на четирите наети дейтацентърни сървъра остава полезен, но това са хоствани маршрути, а не активен мобилен достъп. Възстановяването изисква повторни проверки на свързаността и здравето.

Препоръчан критерий за включване: актуален heartbeat, проверен SIM маршрут, синхронизиран часовник, успешна браузърна снимка и качване; неубедителните наблюдения са UNKNOWN.

08 / Текуща мрежа срещу целево разширяване

Четири действащи хоствани точки; 28 мобилни точки за възстановяване

Статусът е уточнен от собственика на 4 октомври 2026 г. Работещите локации са Варшава, Милано, Истанбул и Лондон - наети сървъри в дейтацентрове. Другите 28 точки са мобилни разгръщания с Linux мини-PC/SIM рутери, тествани по-рано и спрени поради липса на средства за поддръжка. Следователно инвентарът от 32 точки не означава 32 активни точки.

Собственикът потвърждава исторически uptime проверки и браузърни снимки от 28-те мобилни точки. Изображенията са били в R2 с автоматично изтриване след 10 дни; тези исторически файлове вече не са налични за независим преглед. Предишното тестване е потвърдена от собственика история, а не запазено доказателство за текуща достъпност.

Група / брой	Статус и тълкуване
4 хоствани точки	Работят сега: Варшава, Милано, Истанбул и Лондон.
28 мобилни точки	Тествани по-рано; спрени до осигуряване на финансиране.
80 мобилни агента	Първа финансирана цел: възстановяване на 28 и добавяне на 52. Четирите хоствани точки са отделно.
180 целеви пазара	Каталожен план: 1 217 записа с 114 позиции за валидиране; не е активно покритие.

Старите каталожни обозначения, включително заглавният брой 32 активни и трите активни операторски карти, не са актуален опис на действащата мрежа.

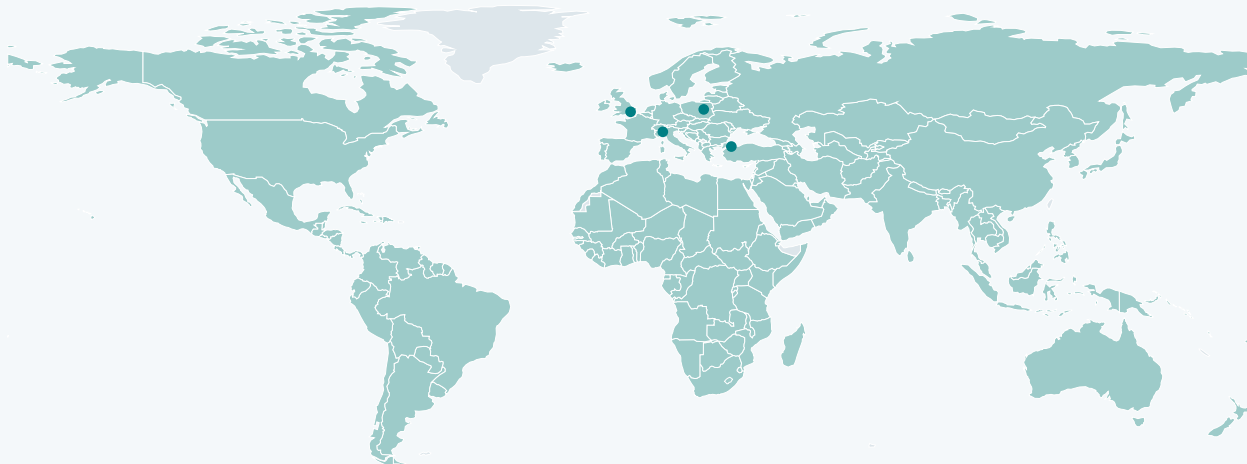
09 / Мрежова карта и операторски цели

Географски план, а не карта на действащо покритие

Картата откроява държави и пазари от целевия каталог, а не активно покритие. Малките пазари може да не се виждат в този мащаб. Основните локации са Лондон, Варшава, Милано и Истанбул; те не доказват пълно национално или мобилно покритие. Регионалните сборове следват каталога: Европа 40, Африка 54, Америка 31, Азия 47 и Океания 8. [3]

Операторските цели изискват поддържана идентичност, вид връзка, жизнен статус и дата на проверка. Четири целеви позиции са планова основа, а не твърдение за четири независими мобилни оператора във всяка държава. Подробната справка е в действащия каталог; картата е обобщена и не изразява позиция по спорни граници.

ЦЕЛЕВИ ПАЗАРИ - НЕ АКТИВНО ПОКРИТИЕ



Основни локации: Лондон / Варшава / Милано / Истанбул

Европа 40 | Африка 54 | Америка 31 | Азия 47 | Океания 8

ЦЕЛЕВИ КАТАЛОГ: 180 пазара | 1 217 записа, включително 114 позиции за валидиране.
Основа: Natural Earth, обобщена 1:110m.

10 / Хронология на инцидента и живот на доказателствата

Потвърден от собственика пълен тест; ясен обхват на отказа и възстановяването

На 4 октомври 2026 г. собственикът потвърди успешен тест след поправките на целия процес: втори DOWN, снимки на инцидента, получен DOWN имейл, възстановяване и получен RESOLVED имейл. Това е приеман резултат от собственика, а не гаранция за 100% надеждност, тест под натоварване или независимо измерен SLA за откриване.

Производствената политика трябва да различава последователни откази на един маршрут от едновременни резултати на различни маршрути. Записват се прагът, обхватът и условията за възстановяване. Референтният процес по-долу описва политиката с два DOWN; общият ефект по маршрути и закъснените резултати изискват отделни приемни тестове.

При втория подходящ отказ се отваря или обновява един инцидент, създават се задачи за снимки по засегнатите допустими маршрути и задача за DOWN известие. Качването на снимките не трябва да е условие за уведомяване на клиента. Грешката при заснемане принадлежи към записа за инцидента и не го заличава. Глобалният обхват изисква отделно настроена политика между маршрути.

01 Съмнение

Първи подходящ DOWN; запис по маршрут



02 Потвърждение

Втори DOWN; инцидент и задачи за снимки + известие



03 Възстановяване

Успешни проверки по политика; затваряне и RESOLVED

Потвърдено от собственика: DOWN -> снимки -> получен DOWN имейл -> възстановяване -> получен RESOLVED имейл. Остават нужни по-широки тестове за откази и повторни опити.

11 / Клиентски сценарии и реалистична стойност

Доказателствата подпомагат решенията, но не заменят разследването

Електронна търговия: сравнение на страницата и началото на checkout по маршрути, снимки при отказ и разследване дали проблемът е локален, регионален или свързан със зависимост. Проверката трябва да спира преди реална покупка, освен в отделно разрешена тестова среда. Успешна начална страница не доказва успешно плащане.

SaaS и корпоративни портали: достъпност на страницата за вход и одобрени сценарии без промяна на данни. Доказателствата помагат да се разграничи проблем с доставчика на идентичност от отказ при визуализация или маршрут. Нужни са специални тестови профили и лимити, за да не се блокират акаунти или разкрият данни.

Хостинг, CDN и WAF операции: сравнение на блокирани и незасегнати маршрути, заснемане на екрана и запазване на времеви и мрежовия контекст. Пакетът доказателства може да подобри ескалацията, но не определя автоматично отговорната страна и не гарантира приемане на договорна претенция.

Fintech, медии и публични услуги: сравнение на разрешени публични или тестови сценарии и регионални откази. Fintech проверките не трябва да извършват преводи, поръчки или да разкриват платежни данни. При медии може да се раздели достъпна основна страница от блокирани ресурси. Корпоративната употреба добавя клиентска изолация, контролиран експорт, съхранение и договорен обхват. Доказателствата подпомагат ескалацията, а не автоматичното приписване на отговорност.

Стойността се измерва чрез възпроизвеждане на инциденти, пълнота на използваемите доказателства, потвърдена доставка на известия и време до подкрепено обяснение. Ръстът на приходи, избегнатите загуби и намаленото време за реакция изискват клиентски измервания; документът не съдържа измислена възвръщаемост или сравнение с конкуренти.

12 / Контролирани браузърни сценарии

В разработка и тестове; не са внедрени за клиентите

Собственикът потвърждава, че login, cart и checkout сценарии са в разработка и тестове, но още не са внедрени като клиентски функции. Таблицата описва предвидени граници, а не налични производствени сценарии. По подразбиране наблюдението е ограничено и без промяна на данни; сценариите с вход изискват одобрени тестови профили, разрешени действия, обхват, почистване и правила за спиране.

Сценарий	Безопасна граница и тълкуване
Вход	Преглед на публична страница; вход само с одобрени тестови данни. Без достъп до несвързани клиентски записи.
Количка	Добавянето може да променя данни, резервира наличност или задейства аналитикс. Тестова среда или изрично разрешена временна количка с почистване.
Завършване на поръчка	Преглед на разрешения начален екран и ресурсите. Спиране преди поръчка или чувствителни данни, освен в изрично одобрен sandbox.
Плащане	Без реално таксуване, превод, извличане на токени или заобикаляне на защиты. Sandbox тест не доказва успешно реално плащане.

Предложени мерки: разрешени действия, максимални стъпки, лимити, скриване на тайни, аварийно спиране и одитна следа.

13 / Third-Party Dependency Intelligence

Следващ етап: сигнали от доставчици плюс наблюдавано въздействие

Предложеният модул позволява клиентът да свърже външни доставчици и техни компоненти със сайт. Категориите включват плащания, CDN/WAF, облак, DNS, имейл, SMS, идентичност, хостинг, SaaS, инструменти за разработка и AI API. Примерните доставчици илюстрират възможни адаптери, без да предполагат одобрение, партньорство или завършена интеграция.

Рамката за доставчици следва да предпочита официални status API, структурирани крайни точки и официални емисии. Всеки адаптер пази URL на източника, външни идентификатори на компонент и инцидент, време на обновяване, време на изтегляне, последен успех и грешки при обработката. Ограниченията на заявките, промените в емисиите и лицензионните условия са част от работата. Недостъпен източник става неизвестен или остарял, а не operational.

Клиентите трябва по възможност да избират относим компонент и регион, вместо да се абонират за всяко събитие при глобален доставчик. Откриването може да предлага зависимости от разрешени метаданни за заявки, но установен контакт не доказва критична зависимост. Потвърждение от клиента и ясен обхват ограничават шумните или подвеждащи заключения.

Модулът не трябва да използва прихванати пароли, платежни данни или неразрешен достъп за разследване на доставчик. Първата версия следва да се фокусира върху надеждно приемане на данни, съпоставяне на компоненти, клиентски избор, история и актуалност на известията, преди да въвежда причинни заключения. [2]

Планирана възможност. Status страницата на доставчик е сигнал, а не пълно описание на въздействието върху клиента.

14 / Откриване на зависимости и обяснима корелация

Планиран етап: вероятни причини без измислена сигурност

Корелацията съпоставя наблюденията за сайта, засегнатите маршрути, компонентните зависимости и събитията при доставчици в определен времеви прозорец. Хипотезата е по-полезна, когато сочи подкрепящи и противоречащи данни, актуалност и липсваща информация. Оценката за увереност трябва да обобщава документираните правила; тя не е калибрирана вероятност без отделно валидиране.

Илюстративен сценарий, а не измерен клиентски инцидент: документът на сайта се зарежда, разрешена проверка на checkout без промяна на данни отказва по два независими маршрута, а избраният платежен компонент съобщава инцидент в същия период. Платформата може да предложи вероятен проблем със зависимост. Тя трябва да покаже и незасегнатите маршрути, реалното използване на компонента и дали отказът предхожда съобщението на доставчика.

Полезните формулировки са вероятна причина, вероятна зависимост, корелиран инцидент и възможен проблем при доставчик. Категорично твърдение, че доставчик е причинил отказа, изисква преки доказателства и преглед. Глобален operational статус не отменя локален отказ; инцидент при доставчик не означава автоматично, че всеки клиент е засегнат.

Оценяването трябва да използва означени повторения на случаи, независим преглед и отрицателни примери: несвързани едновременни откази, остарели емисии, общи хоствани маршрути, преименувани компоненти и оскъдни доказателства. Версиите на правилата или моделите се пазят, за да може обяснението да се възстанови след обновяване.

Доказателствата се наблюдават. Причинността се извежда и трябва да остане ясно обозначена като заключение.

15 / Incident Agent и автономни доказателства

Дългосрочна посока с човешки контрол върху разрешенията

Дългосрочният Incident Agent би събирал наличните факти, заявявал допълнителни ограничени наблюдения и подготвял пакет доказателства за човешкия екип. Стойността му е дисциплинираното разследване, а не неограничен достъп до клиентската среда. Автономното събиране на доказателства и автономното отстраняване на повреди са различни функции; пътната карта не обещава самостоятелен ремонт на производствени системи. [2]

Референтният модел разделя нискорисковите проверки без промяна на данни, изрично одобрените тестови сценарии с вход и забранените действия, променящи продукцията. Покупки, преводи, унищожителни редакции, извличане на пароли, промени по акаунти и заобикаляне на защити са извън стандартния обхват. Одобрението трябва да определя цел, действие, продължителност и разрешени данни, а не да разрешава неограничен агент.

Уеб съдържание, логове и съобщения от доставчици са недоверени доказателства, а не инструкции за изпълнение. Разследващият механизъм изисква разрешен набор от инструменти, лимити, timeout, отмяна, изолация на тайните и одитна следа. Генерираните резюмета трябва да сочат първичните наблюдения и ясно да разделят факти, хипотези и препоръчани следващи стъпки.

Условията за пускане следва да включват възпроизвеждаеми следи, тестове със злонамерено съдържание, отказани разрешения, аварийно спиране и човешки преглед на неподкрепени твърдения. Началото трябва да е пакетиране на доказателства и помощ при разследване, преди по-широки автономни процеси.

16 / Сигурност, поверителност и клиентски граници

Изисквания към дизайна, а не сертификат за съответствие

Наблюдението на недоверени URL адреси носи риск за услугата и клиента. Браузърните работници трябва да са изолирани от управляващите услуги и другите клиенти, с ограничен изходящ достъп и ресурси. Валидирането на цели трябва да обхваща частни мрежи, локални адреси, metadata услуги и редиректи; първоначална проверка само на името не е достатъчна при промяна на дестинацията. Това са препоръчани мерки, а не проверен одит на текущото разгръщане. [9]

Собственикът посочва вход с Google акаунт и клиентски изглед само на собствените проверки и снимки. Прегледът на кода потвърди проверки за собственост в основните маршрути за резултати и изображения. Отделен маршрут за линк към снимка нямаше такава проверка; на 4 октомври 2026 г. тя е добавена чрез принадлежността на точния съхранен файл към проверка или инцидент, с отказ при неустановена собственост.

Промяната премина 21 теста за права, 11 изолирани HTTP теста и два отказа през публичния HTTPS адрес; проверени са и съществуващи записи за основни снимки, без извличане на клиентското съдържание. Това не е пълен тест за проникване. Временният R2 линк позволява достъп на притежателя до изтичането му, без нов Google вход. Подписаният линк за достъп не е цифров подпис на изображението. [12]

Снимките и URL адресите може да съдържат лични данни, токени или поверителна бизнес информация. Събирането по подразбиране трябва да ги минимизира; параметри, headers и bodies изискват внимателен подбор и скриване. Сценариите с вход трябва да използват специални тестови профили и изрично разрешение. Необработени тайни не трябва да попадат в публични пакети доказателства.

Сайтът публикува страници за сигурност и поверителност. Този документ не заявява ISO сертификация, завършен тест за проникване или юридически одобрено съответствие. Преди договорна употреба от предприятия трябва да се изяснят местоположение на данните, подизпълнители, изтриване, реакция при инцидент и необходимите условия за обработване с подходящ преглед. [4, 5]

17 / Ограничения, нетвърдения и валидиране

Напредъкът трябва да е измерим и проверим

Пускането трябва да се подкрепя от повторяеми тестове, а не само от визуално успешна демонстрация. Контролираните откази включват DNS грешка, невалиден TLS, HTTP грешки, timeout, защитни екрани, липсващо очаквано съдържание и частично възстановяване. Тестват се спрели агенти, закъснели резултати, дублирани задачи, отказало качване и проблеми с транспорта за известия.

Оперативните измервания включват актуалност на агенти, дял завършени задачи, пълнота на снимките, резултати от транспорта за известия, възраст на опашката, тестове за възстановяване и изяснен инвентар. Забавянето на откриването се отчита спрямо интервала и правилото за потвърждение; няма абсолютна гаранция за време. Тестовите за съхранение и изтрит домейн включват закъснели задачи и преглед на резервните копия.

Рисковете при физическо разгръщане включват доставки, местни договори, идентификация за SIM, промени в операторски политики, транспорт, електричество и замяна. Техническите рискове включват промени в браузъри, WAF, DNS кеширане, обща инфраструктура, погрешно приписване и растящо съхранение. Търговските рискове включват несигурно финансиране, постоянни разходи и задължения по награди.

Ограничаването на риска е поетапно разгръщане, валидиране на маршрути, ограничена автоматизация, документирани определения за доказателствата и прозрачно отчитане. Документът не гарантира непрекъсната услуга, пълно глобално покритие, винаги правилни автоматични причини или юридическа допустимост. White paper обяснява дизайн и посока; не заменя SLA, оценка за сигурност или клиентски договор.

18 / Пътна карта и условия за приемане

Поетапна програма за няколко години; приемни критерии преди обещани срокове

Собственикът определя цялата платформа и глобалната мрежа като програма за няколко години, а не изграждане за един до пет месеца. Първоначалната цел от 80 мобилни агента е ранен финансиран етап; по-широката операторска мрежа, анализът на зависимости, корелацията и контролираният Incident Agent се реализират и валидират постепенно. [2]

Фаза / статус	Обхват и предложен критерий за пускане
00 / текуща основа	Достъпност, снимки, история, работни пространства и DAX. Критерий: възпроизводими DOWN/снимка/възстановяване; проверени известия, изтриване и инвентар.
01 / следваща	Регистър на доставчици/компоненти и адаптери към официални източници. Критерий: остарели/неизвестни данни, лимити, клиентски абонаменти и произход.
02 / планирана	Откриване и обяснима корелация. Критерий: означени повторения, противоречиви данни, измерено погрешно приписване и обяснения с доказателства.
03 / дългосрочна	Контролиран Incident Agent и пакети доказателства. Критерий: ограничени инструменти, одобрения, злонамерени сценарии, отмяна и одитни следи.

Финансираните 12 месеца експлоатация не са краен срок за цялата система. Не са одобрени точен брой години, дати по фази или дата за разполагане на 80 агента; времето зависи от средства, проверки и експлоатация.

19 / Търговски модел и контекст на кампанията

Софтуерна услуга с постоянни разходи за мрежата

EyeBallMonitor се разработва и управлява от екип от двама души. Одобрената от собственика цел на черновата на кампанията е 75 000 EUR за 30 дни. Първоначалната мобилна цел е общо 80 агента: възстановяване на 28-те тествани точки и добавяне на 52 нови. Четирите действащи дейтацентърни точки са отделна основа, а не част от мобилния брой.

Собственикът посочва, че плановият бюджет покрива закупуване, инсталиране/разполагане и 12 месеца наем за колокация и SIM интернет за първоначалния мобилен етап. Не са предоставени потвърдени от доставчици цени за агент, разбивка по пера или график. Обхватът е одобрен финансов план, а не доказателство за получени средства или независимо оценена гаранция за изпълнение.

Следващото разширяване се планира чрез реинвестиране на приходи от платени клиентски акаунти/абонаменти. Поддържането на първите 80 маршрута също изисква текущи приходи след финансиранния период. Пълното изграждане зависи от реални продажби, оперативен марж, местна достъпност и капацитет; не се гарантират печалба или разгръщане на всички 180 пазара.

Преди старт се съпоставят оферти, удръжки по кампанията, логистика, резерви и задължения по наградите с посочения обхват. Датите, окончателните награди и видеото се одобряват отделно. Документът не предлага дялове, инвестиционна доходност, неограничена услуга или гарантирано място за конкретен поддръжник. [6, 7]

План за 75 000 EUR: общо 80 мобилни агента с възстановяване на 28 и 12 месеца колокация и SIM интернет. Клиентските цени остават крайни, с включен ДДС.

20 / FalcoSoft ITS и отговорност за реализацията

Фирмена идентичност и отговорности за растежа

EyeBallMonitor се разработва и управлява от екип от двама души във ФАЛКОСОФТ ИТС ЕООД, българско дружество с ЕИК 208644390 и регистрация по ДДС BG208644390. Публикуван адрес: бул. Александър Стамболийски 255, София, България. Поддръжка: support@eyeballmonitor.com. Числеността е потвърдена от собственика; не се подразбират непредоставени имена, биографии, инвестиции или акредитации.

Екипът трябва да покрива продуктови решения, експлоатация на агенти, браузърни проверки/доказателства, клиентска поддръжка, логистика и финансово планиране. Не е предоставено поименно разпределение. Физическа мрежа от 80 агента създава задължения за обслужване и поддръжка; растежът трябва да следва проверена експлоатация, а не само закупуване на хардуер.

Проектът следва да отчита напредъка чрез активирани проверени маршрути, приети софтуерни етапи, оперативни измервания и открито посочени ограничения. Пътната карта показва посоката; бележките за версии показват реалните промени. Обновяванията на кампанията разграничават закупуване, инсталиране, валидиране на връзката и клиентска достъпност.

Мрежовата история, екипът от двама души, приемният тест на инцидентите и бюджетният обхват в това издание са изрично потвърдени от собственика. Избрани механизми за хеширане и собственост са проверени в кода; това не е цялостен одит на сигурността или инфраструктурата. Бъдещите публични казуси следва да са от нови разрешени тестове, защото историческите мобилни снимки са изтрити.

21 / Приложение

Термини, архитектура и полета на доказателствата

Основни термини

Агент: управляван работник за проверки. Маршрут: наблюдаван мрежов път, а не цяла държава. Доказателство: файл плюс контекст на изпълнение. Инцидент: групирани откази и възстановяване. Зависимост: външна услуга, използвана от сайта. Корелация: свързани сигнали, а не доказана причинност. SLO/SLA: цел / договорен ангажимент с отделно определено измерване.

Архитектура и полета

Раздел 04 съдържа архитектурата управление / агенти / приемане; раздел 06 - групите полета и проследимостта; раздел 10 - хронологията потвърждение / заснемане / възстановяване. Това са логически референтни схеми и изисквания, а не конкретни производствени структури.

Известия и изтриване

DOWN и RESOLVED трябва да сочат един и същ инцидент и засегнат обхват. Възстановяване по един маршрут не трябва скрито да затваря останалите. Повторната доставка изисква ограничени интервали и ключ за недублиране по инцидент, канал, получател и версия на събитието. Неуспешните доставки трябва да са видими за операторите, а RESOLVED не бива да зависи от успешната доставка на предходния DOWN имейл.

Собственикът на продукта изисква домейните да могат да се изтриват и при активен мониторинг или налична история. Референтният процес спира планирането, отменя или обезсилва чакащите задачи, премахва свързаната история и доказателства и не допуска закъснели задачи да възстановяват изтрети данни. Преди унищожителни действия се проверява клиентската принадлежност.

Експлоатация и капацитет

Подновяването на сертификати е оперативен процес, а не само таймер: инвентар на сроковете, успешно подновяване, внедряване на конфигурацията, презареждане на услугата и външна TLS проверка. Нужни са и известия при отказ и тестови подновявания. Автоматизацията намалява риска, но не обосновава обещание, че сертификати или услуги никога няма да отказват.

Капацитетът трябва да моделира проверки в минута, едновременни браузъри, размер на снимките, съхранение, повторения и трафик. Само като илюстрация: 100 сайта x 4 маршрута през минута създават 400 леки проверки в минута. Снимки при всяка проверка са различно и много по-тежко натоварване. Заснемане при инцидент и ограничена паралелност контролират разходите; не се заявява измерен капацитет или SLA.

Источници и основа на документа

Версия 1.2 от 4 октомври 2026 г. включва уточненията на собственика: четири действащи хоствани точки, 28 спрени/тествани мобилни точки, историческо 10-дневно изтриване в R2, приемния тест на инцидентите, сценарии в разработка, екип от двама души и план за 80 агента / 12 месеца. Ограниченият преглед обхваща централната система и агентите в Полша/Милано/Лондон; поправката на правата за снимки премина 34 теста. Това не са независими инфраструктурни, финансови или одити по сигурността. Страниците/каталогът са проверени на 03-04 октомври; старите обозначения не отменят уточнения статус. Не са възпроизведени клиентски тайни или частни инфраструктурни идентификатори.

[1] EyeballMonitor product overview

<https://eyeballmonitor.com/>

[2] EyeballMonitor public roadmap

<https://eyeballmonitor.com/roadmap>

[3] EyeballMonitor network directory

<https://eyeballmonitor.com/network>

[4] EyeballMonitor security

<https://eyeballmonitor.com/security>

[5] EyeballMonitor privacy

<https://eyeballmonitor.com/privacy>

[6] EyeballMonitor service plans

<https://eyeballmonitor.com/pricing.php>

[7] EyeballMonitor terms

<https://eyeballmonitor.com/terms>

[8] Playwright documentation: emulation

<https://playwright.dev/docs/emulation>

[9] OWASP SSRF Prevention Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

[10] EyeballMonitor machine-readable network catalog

<https://eyeballmonitor.com/assets/data/monitoring-network.json>

[11] Natural Earth 1:110m countries basemap

https://github.com/nvkelso/natural-earth-vector/blob/master/geojson/ne_110m_admin_0_countries.geojson

[12] Cloudflare R2: presigned URLs and temporary access

<https://developers.cloudflare.com/r2/api/s3/presigned-urls/>