guardsix

Ваш надежный союзник в кибербезопасности

Разработано с учетом требований цифрового суверенитета Европы.
Развертывается на ваших условиях.
Полный операционный контроль.

Март 2026

Your closest ally in cybersecurity


Мы
обеспечиваем
безопасность общества
в цифровом мире

От Logpoint к guardsix

Новая, более сильная идентичность отражает нашу расширенную миссию: помогать MSSP защищать своих клиентов и уверенно расти. Мы объединяем передовые технологии кибербезопасности, европейскую надежность и настоящее партнерство, чтобы обеспечить защиту, которая масштабируется вместе с бизнесом. Потому что защита эффективнее, когда мы действуем вместе — как союзники.

Что меняется?

Название и бренд теперь лучше отражают компанию, которой мы стали.

Почему мы меняемся?

Прежний бренд больше не отражал нас такими, какие мы есть сегодня. Нам важна ясность — она помогает укреплять доверие и строить сильные партнерства.

Что это значит для вас?

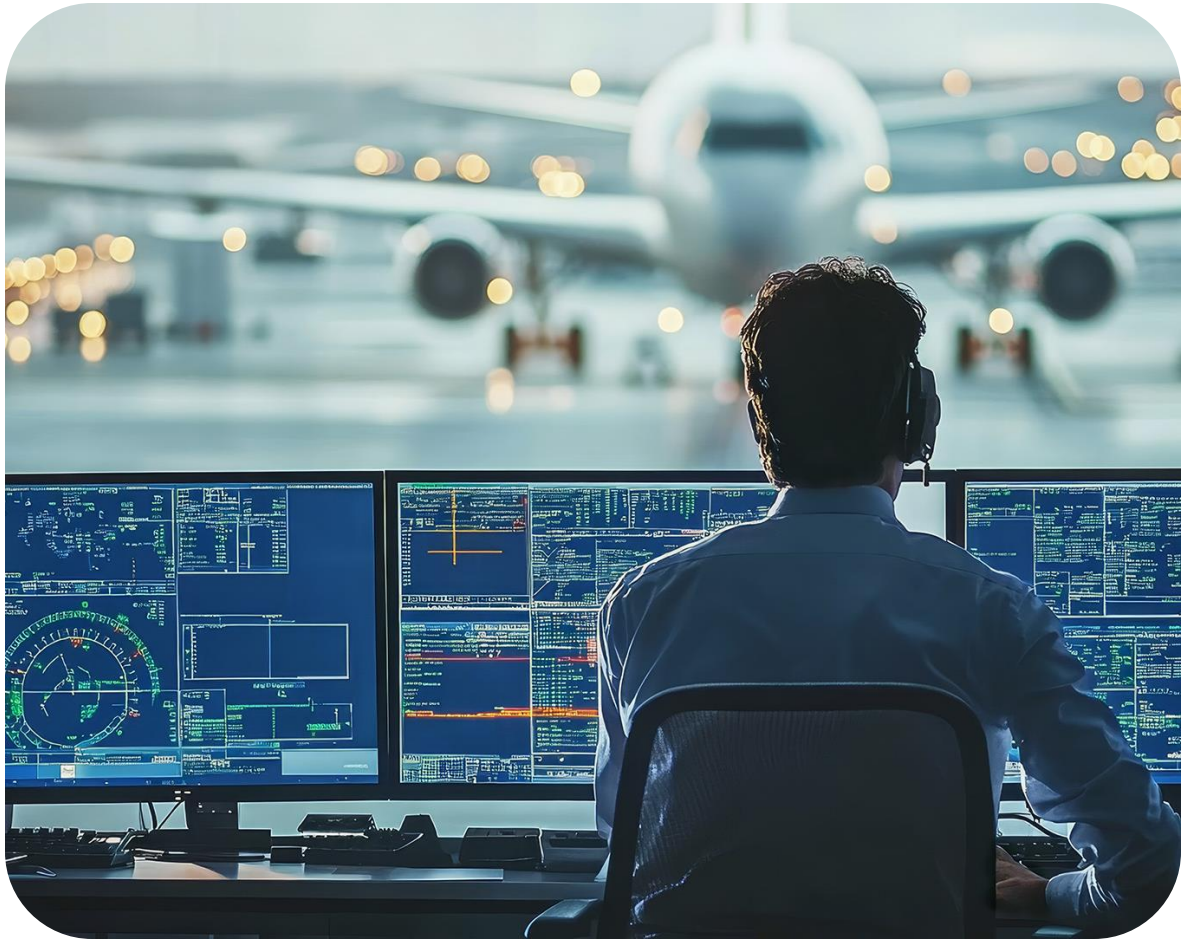
Вы по-прежнему получаете проверенные решения и надежную поддержку — теперь с более четким фокусом и еще большей приверженностью защите того, что действительно важно.

O guardsix

Ваш надежный союзник в кибербезопасности

- Штаб-квартира расположена в Копенгагене, Дания; присутствие — в странах Европы и Непале.
- Компания находится в частной собственности европейских инвесторов.
- Работает с организациями в критически важных отраслях по всей Европе.

Нагрузка на современные службы кибербезопасности



Команды на пределе

Команды кибербезопасности находятся под постоянным давлением, а аналитики перегружены. Их миссия слишком важна, чтобы оставлять специалистов по защите без поддержки.

Разрозненная экосистема безопасности

Инфраструктура безопасности часто опирается на множество несвязанных инструментов. Без единого контекста снижается видимость и растет информационный шум, мешая командам сосредоточиться на главном.

Перегрузка оповещениями

Аналитики получают в среднем 4 484 оповещения в день, 40% из которых — ложные срабатывания. Из-за такого объема критические угрозы неизбежно могут быть упущены.

1 https://swimlane.com/blog/top-soc-analyst-challenges/

Изменения в отрасли и новые требования регуляторов

Угрозы становятся сложнее и скоординированнее

Кибератаки развиваются: они становятся быстрее, сложнее и масштабнее. Разрозненный мониторинг уже не обеспечивает полной видимости. Современной защите нужен единый контекст, а не набор несвязанных инструментов.

Усиление регуляторного давления

После принятия директивы ЕС NIS2 кибербезопасность становится зоной ответственности руководства. Безопасность больше не только операционная функция — это часть стратегического управления.

Цифровой суверенитет важнее, чем когда-либо

В условиях геополитической неопределенности организации все тщательнее оценивают, где их данные хранятся, обрабатываются и защищаются.

Более сильная защита. Меньше операционной сложности.

Как понятные и эффективные процессы кибербезопасности повышают эффективность, соответствие требованиям, контроль рисков и суверенитет данных.

Эффективность

- Автоматизация и встроенные интеграции снижают усталость от оповещений, устраняют ручные задачи и помогают сосредоточиться на проактивной защите

Соответствие требованиям

- Упрощенное соблюдение требований фреймворков
- Готовые к аудиту отчеты и работа с данными в соответствии с регуляторными требованиями, такими как NIS2 и GDPR

Снижение рисков

- Обнаружение угроз в реальном времени
- Полная видимость во всех средах
- AI-аналитика для сокращения времени присутствия злоумышленника в системе и раннего предотвращения угроз.

Суверенитет данных

- Гарантированный доступ к данным
- Никто, кроме вас, не имеет доступа к вашим данным

Почему guardsix?

Улучшение обнаружения угроз и реагирования

- Полная видимость
- Снижение усталости от оповещений
- Автоматизация реагирования на инциденты
- Поиск угроз

Соответствие регуляторным требованиям

- Преднастроенные отчеты
- Подтверждение соответствия требованиям
- Соответствие NIS2 и GDPR

Суверенитет и конфиденциаль-ность данных

- Европейские облачные провайдеры
- Локальное развертывание
- Кибербезопасность, созданная в Европе

Эффективность и снижение затрат

- Мультитенантность
- Единая платформа
- Прогнозируемое лицензирование

Прозрачность, контроль и уверенность при любом масштабе

Помогаем сделать процессы кибербезопасности проще, быстрее и надежнее — с полным контролем над данными

Устраняйте пробелы в обнаружении угроз

Понимайте, когда отдельный инцидент является частью более крупной атаки. guardsix связывает события, инциденты и метаданные в единую картину, чтобы команда могла быстрее проследить действия злоумышленника и принять правильное решение.

Будьте готовы к требованиям регуляторов

Готовьтесь к аудитам, выполняйте требования по отчетности и управлению инцидентами. Отслеживайте соблюдение политик, формируйте и экспортируйте отчеты, контролируйте состояние инфраструктуры в режиме реального времени.

Сохраняйте контроль над данными

Размещайте и обрабатывайте данные так, как требует ваша политика безопасности, суверенитета и защиты информации. Выбирайте локальное развертывание для максимального контроля или используйте частное либо публичное облако.

Масштабируйтесь без лишней сложности

guardsix растет вместе с вашими объемами данных и подходит для сложной распределенной инфраструктуры. Платформа интегрируется с ведущими инструментами безопасности — как в облаке, так и в локальной среде.

Единая SecOps-платформа для современной киберзащиты

Создана для тех, кто каждый день обеспечивает устойчивость цифрового общества

guardsix command centre

SIEM

SOAR

NDR

Fleet

Governance

SIEM

Выявляйте угрозы на раннем этапе, соблюдайте требования регуляторов и сохраняйте полный контроль

Фокус на самом важном

- guardsix SIEM помогает компактным SecOps-командам видеть главное и опережать угрозы — даже в условиях высокой нагрузки.

Защита с первого дня

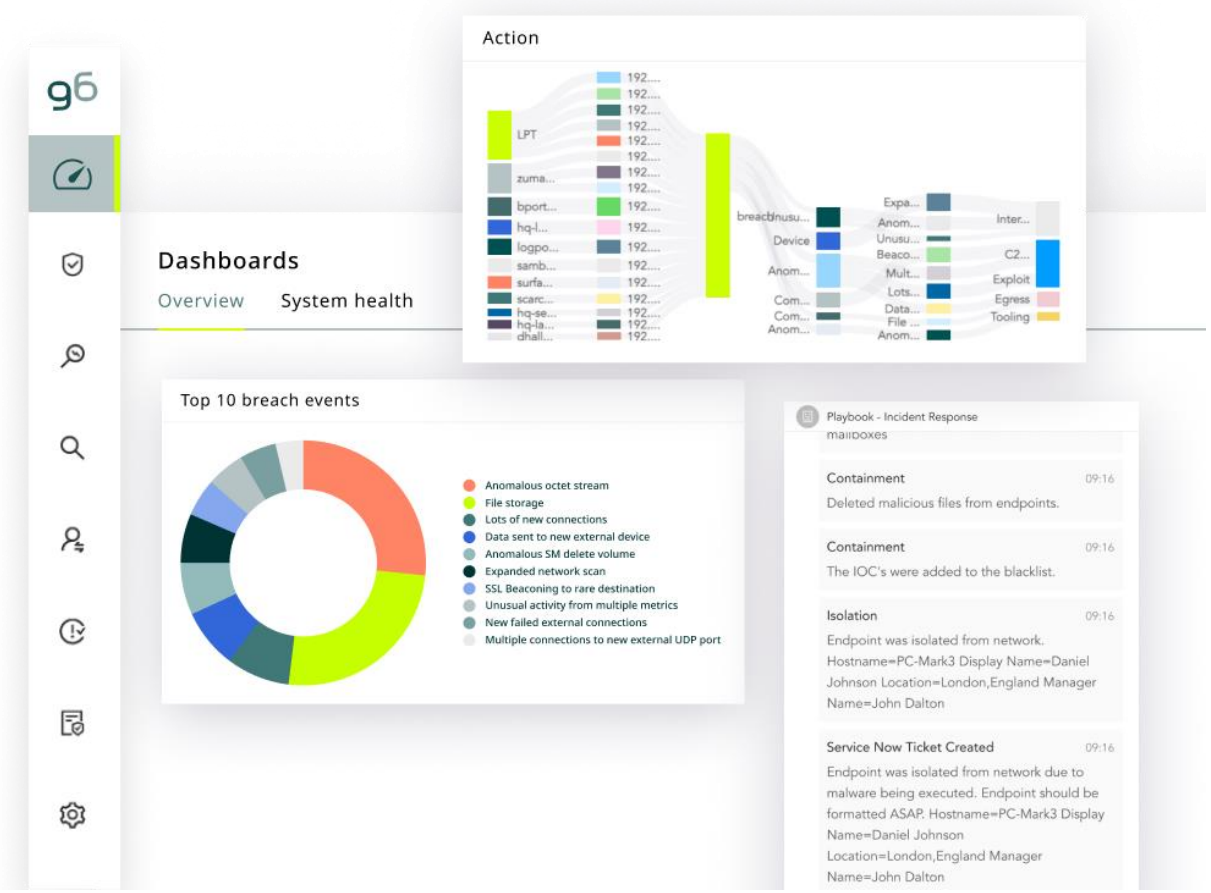
- Готовые наборы правил и сценариев обнаружения обеспечивают быструю защиту от программ-вымогателей, компрометации учетных данных, внутренних угроз и бокового перемещения — без сложной настройки.

Работайте на своих условиях

- Самостоятельное развертывание дает полный контроль над данными, управлением и доступом.

Соответствие требованиям без лишней нагрузки

- guardsix SIEM встраивает compliance в ежедневные процессы: помогает распределять ответственность, готовить данные к аудиту и соблюдать требования без нарушения операционной работы.



SOAR

От реактивного реагирования к управляемому процессу

Верните аналитикам время и фокус

- SOC-команды не должны тратить часы на рутинные проверки и низкоприоритетный шум. guardsix SOAR снимает нагрузку первичной triage-обработки, чтобы реальные угрозы становились видны сразу.

Реагируйте быстрее, чем атака успеет развиться

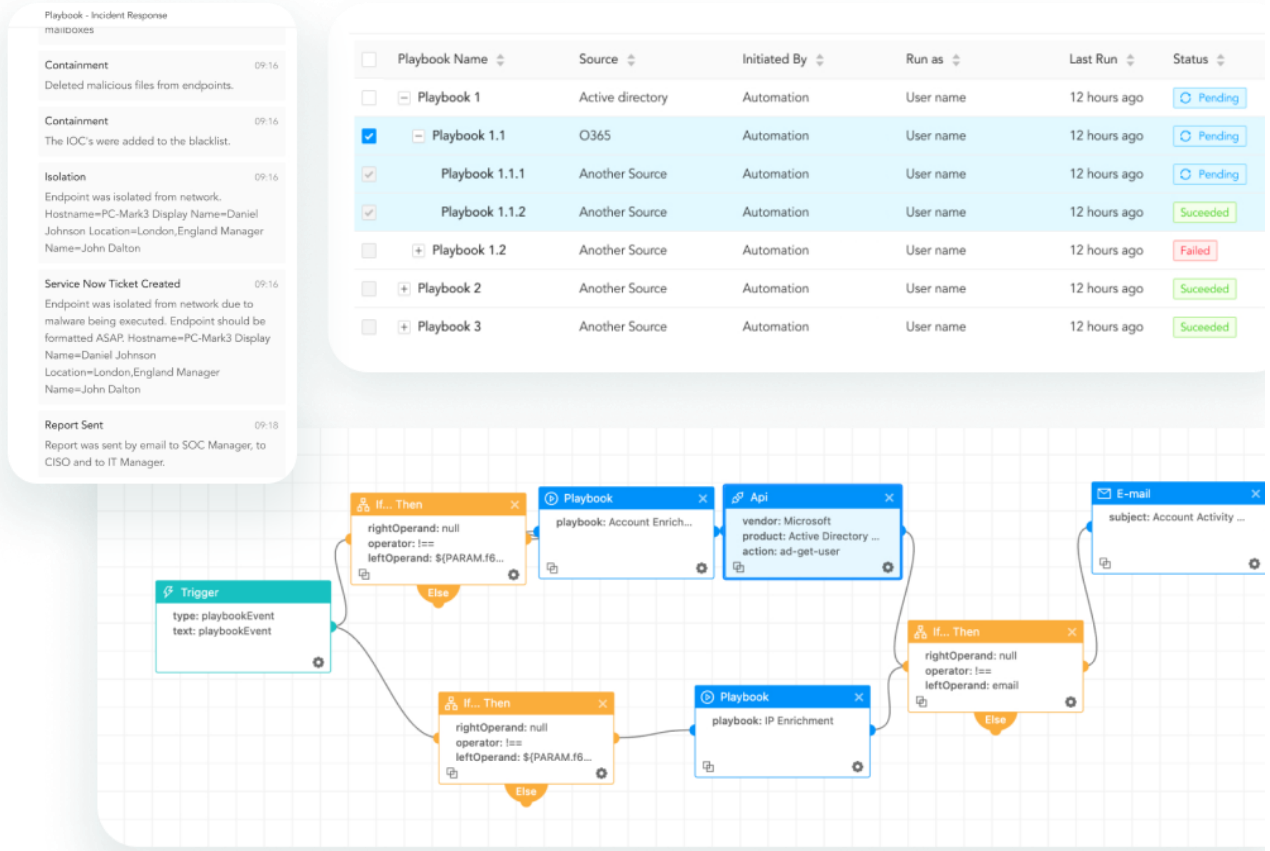
- Аналитики остаются в курсе происходящего и сохраняют контроль, пока повторяющиеся действия выполняются автоматически. Результат — меньше задержек, ниже impact и более спокойные, управляемые операции.

Расследуйте инциденты вместе и без хаоса

- Благодаря case management SOAR становится единым центром реагирования, где расследования структурированы, согласованы и движутся вперед.

Координируйте реагирование по всей экосистеме

- Инструменты безопасности должны работать вместе именно тогда, когда это важнее всего. guardsix SOAR связывает и координирует действия во всей инфраструктуре, чтобы реагирование было единым, а не фрагментированным.



NDR

Когда возможностей SIEM уже недостаточно

Видимость сети, которая раскрывает скрытые действия атакующих

- guardsix NDR дает специалистам по защите недостающую видимость сетевой активности — без лишней нагрузки на команду.

Останавливайте многоэтапные атаки до их развития

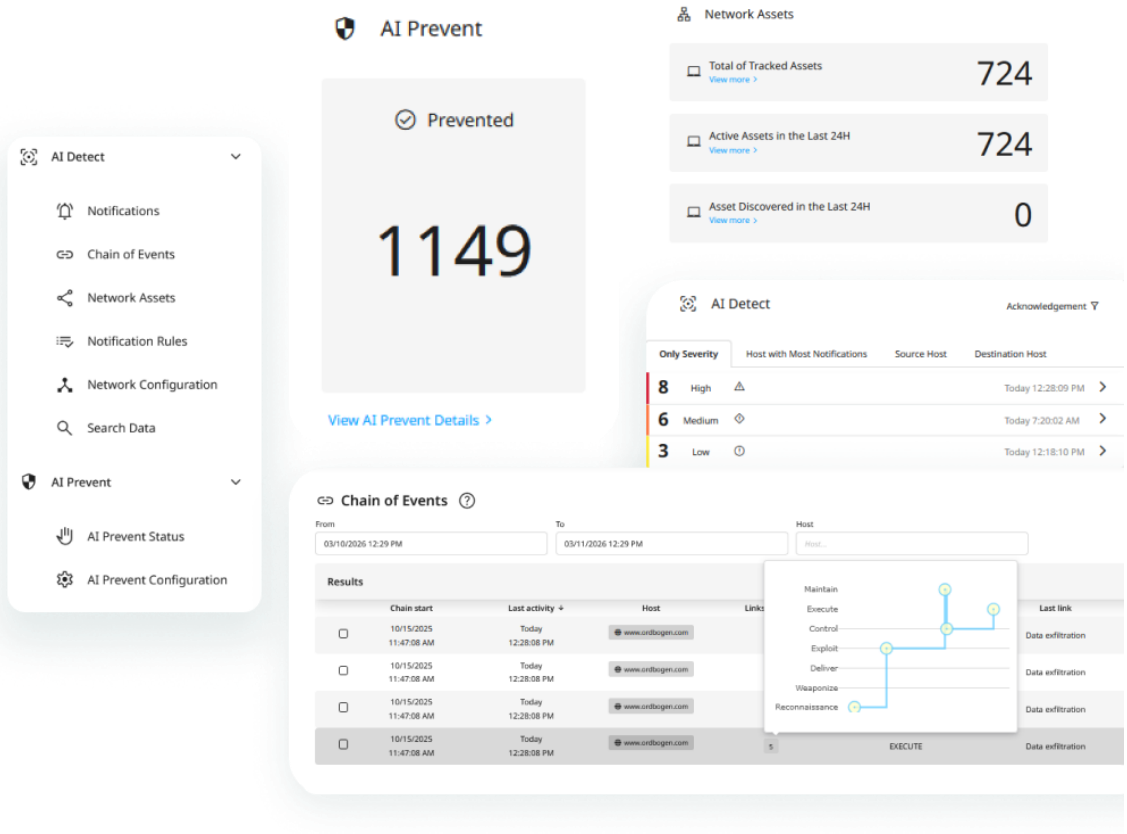
- Связывайте сетевые события во времени и выявляйте цепочки атаки еще на этапе формирования.

Наводите порядок в хаосе сигналов

- NDR превращает разрозненные сетевые события в понятные и объяснимые инсайты, чтобы аналитики могли быстро принимать решения без лишних сомнений.

Для компактных команд — без необходимости в узких специалистах

- Решение рассчитано на ежедневную работу аналитиков и не требует отдельной команды data science.



Fleet

Управление масштабной инфраструктурой для команд киберзащиты

Ускоряйте подключение клиентов

- Быстро добавляйте клиентов и новые среды без роста операционной нагрузки.

Сохраняйте единый подход при масштабировании

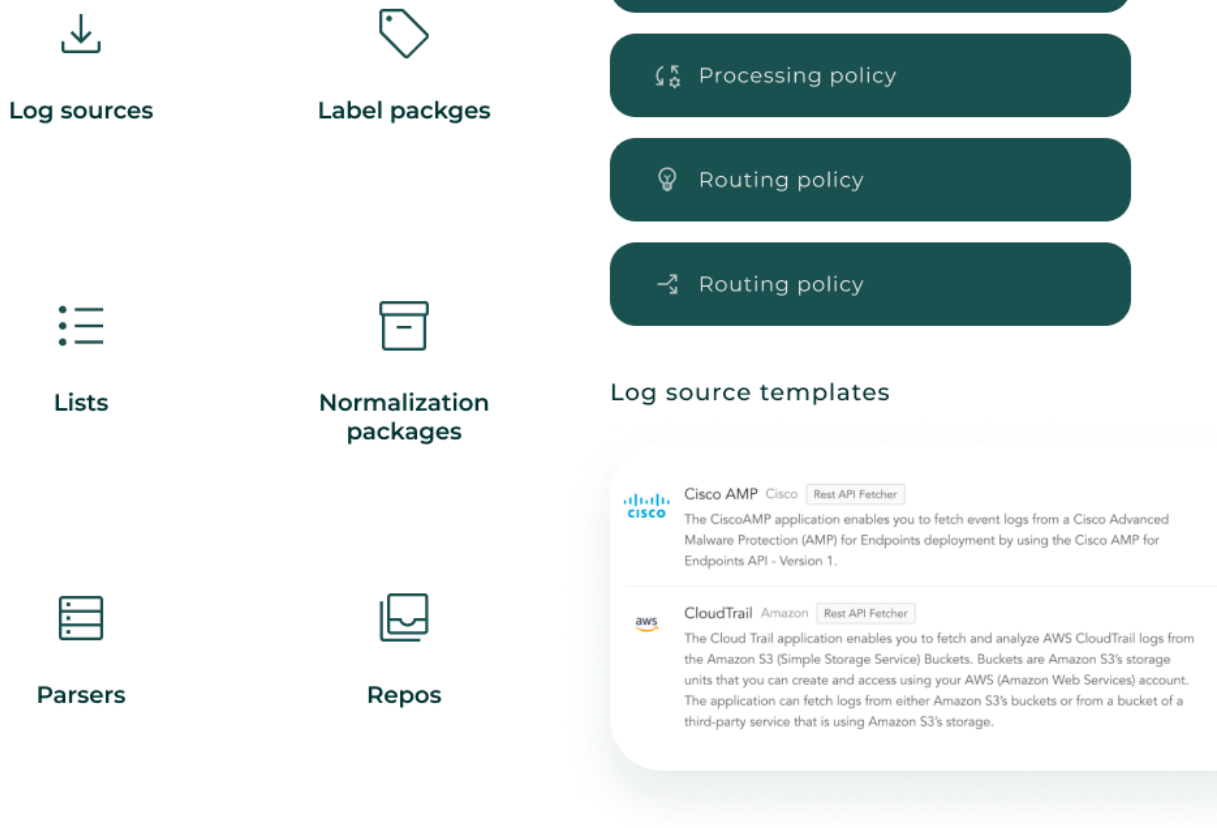
- Централизованно управляйте конфигурациями и контролируйте состояние систем во всех средах.

Обеспечивайте стабильный уровень защиты везде

- Единообразно разворачивайте возможности платформы и поддерживайте одинаковый уровень безопасности во всех средах.

Поддерживайте прибыльный рост

- Снижайте операционные затраты и масштабируйте сервисы без потери эффективности и маржинальности.



Контроль и соответствие требованиям для здравоохранения

Превратите регуляторную нагрузку в прозрачные и управляемые процессы

Контролируйте доступ к чувствительным данным

- Понимайте, кто обращался к чувствительным записям, когда это произошло и с какой целью — с надежным и понятным аудиторским следом.

Упростите compliance и подготовку к аудиту

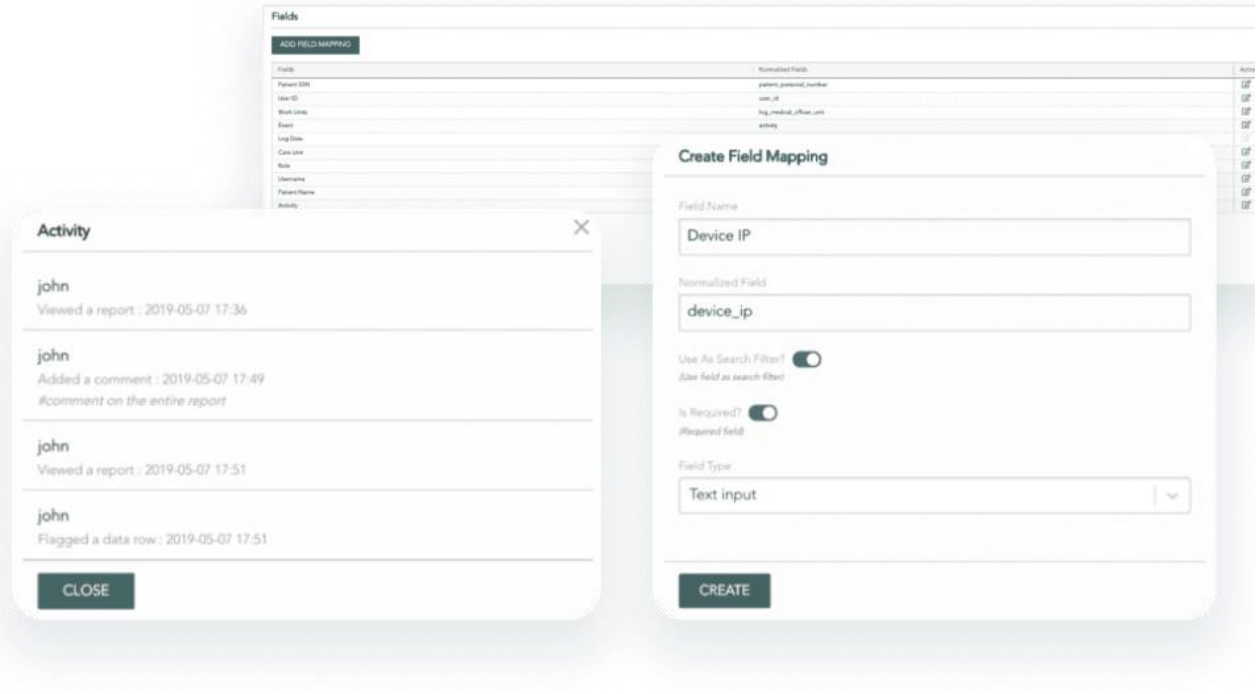
- Встроенные отчеты и дашборды помогают подтверждать соответствие требованиям без ручного сбора данных.

Помогайте нетехническим командам работать безопасно

- Простой интерфейс позволяет compliance-специалистам и аудиторам анализировать события доступа без глубокой технической экспертизы.

Укрепляйте доверие внутри организации

- Структурированные процессы помогают согласованно вести расследования и безопасно управлять ими между отделами.



Решения guardsix выбирают организации, отвечающие за защиту критической инфраструктуры Европы

MSSPs

8COM CYBER SECURITY

Telia Cygate

METCLOUD
GET CONNECTED • CYBER SAFE

NORDLO

KMD
An NEC Company

IT-TOTAL

CNI

SIEMENS

ENERGINET

CITY OF COPENHAGEN

NHS
Oxford Health
NHS Foundation Trust

Sachsen Energie

Göteborgs Stad

guardsix

Your closest ally in cybersecurity

headtechnology
it · security · distribution · services

Авторизированный дистрибутор

www.headtechnology.com
sales@headtechnology.com