



iBatyr Monitor

Система для предотвращения утечек данных, комплексного расследования инцидентов внутренней информационной безопасности и мониторинга действий пользователей



Законодательные требования



Риски с зарубежным ПО

- Несоответствие 832 Постановлению Правительства РК
- Отсутствие в реестре доверенного ПО



Защищенность с iBaty Monitor

- Соответствие 832 Постановлению Правительства РК
- Входим в реестр доверенного ПО РК
- Наличие сертификата ОУД 4



Соответствие законодательству РК и сертификация

“Для защиты объектов информатизации ГО, МИО и критически важных объектов информационно-коммуникационной инфраструктуры применяются системы предотвращения утечки данных (DLP) “

Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»



iBaty Monitor
официально включен в
Реестр доверенного ПО РК



Имеет **сертификат соответствия**
требованиям информационной
безопасности ОУД 4

Система обеспечивает полное закрытие юридических рисков и соблюдение обязательных требований для государственного и квазигосударственного сектора

Скрытые угрозы внутри организации



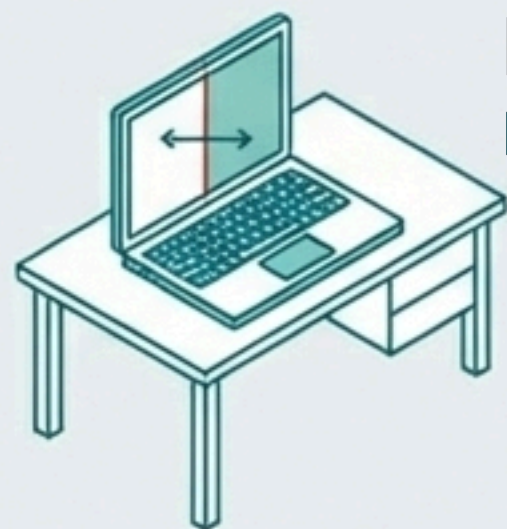
Утечки конфиденциальной информации

Несанкционированная передача документов, клиентских данных, коммерческой и служебной информации за пределы организации



Корпоративное мошенничество и коррупция

Соккрытие нарушений, использование служебного доступа в личных интересах и участие в сомнительных схемах



Нелояльность и работа на стороне

Использование рабочего времени и корпоративных ресурсов в интересах третьих лиц или для личной выгоды



Низкая продуктивность и саботаж

Снижение эффективности работы, умышленное затягивание задач и действия, наносящие ущерб бизнес-процессам

Гибридное решение: безопасность и эффективность



Инструмент управления для ключевых руководителей

Директора и Собственники



Выявление мошенничества
и коррупционных схем

Поиск нелояльных
сотрудников и выявление
групп риска

Выявление "узких" мест в
бизнес-процессах
организации

Службы ИБ и ИТ



Расследование инцидентов
внутренней информационной
безопасности

Своевременное оповещение
о нарушении политик ИБ

Расследование причин сбоев
на рабочих станциях

HR-директора



Повышение эффективности
труда

Учет рабочего времени
сотрудников

Контроль присутствия на
рабочем месте (включая
удаленных сотрудников)

Функционал iBaty Monitor



Мониторинг действий
сотрудников



Предотвращение утечек и
сливов



Оповещение о нарушении
политики ИБ



Выявление инсайдерской
деятельности



Блокировка
нежелательной
активности



Расследование
инцидентов



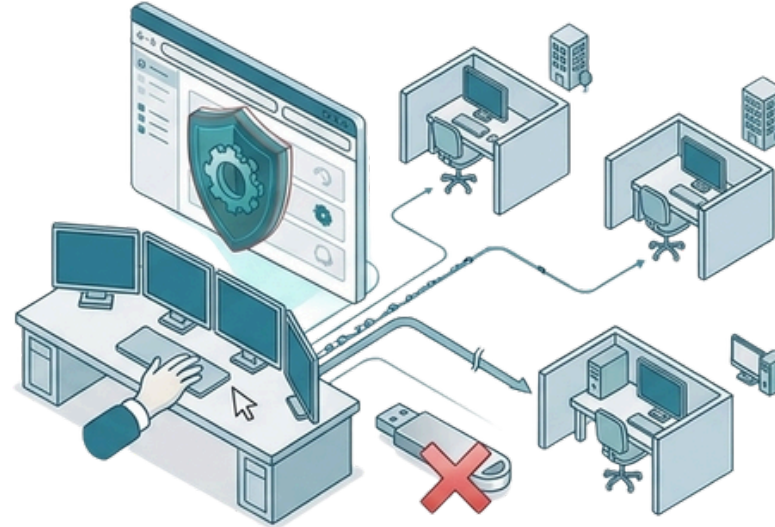
Выявление
мошенничества и
коррупции

Решаемые задачи



Расследование инцидентов внутренней информационной безопасности

- Выявление инсайдерской активности
- Предотвращение утечек чувствительной информации
- Оповещение о нарушениях политик безопасности



Удалённое администрирование

- Удаленное подключение к рабочим станциям
- Выявление использования несанкционированного ПО
- Защита ПК через контроль и блокировку программ, сайтов и USB-носителей



Повышение эффективности труда

- Аналитика продуктивности сотрудников и подразделений по ключевым показателям
- Выявление узких мест в бизнес процессах и отклонений в рабочей активности
- Контроль присутствия на рабочем месте

Возможности ПО



Расследование

Инцидентов внутренней информационной безопасности

Причин неэффективной работы



Выявление

Коррупционных схем и мошенничества внутри компании

Нелояльных сотрудников, работающих на конкурентов



Уведомление

Оповещение на почту или в Telegram по инцидентам



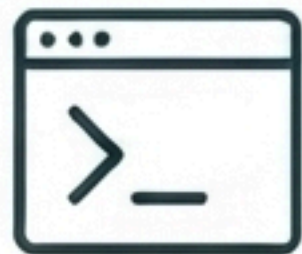
Блокировка

Копирования на съемные носители

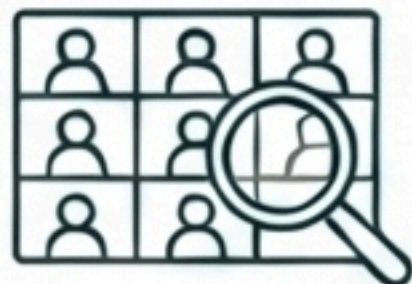
Пересылки конфиденциальной информации

Доступа к нерегламентированным ресурсам

Функциональные возможности



Перехват ввода
команд в терминалах



Контроль демонстрации
ВКС Zoom



Контроль
беспроводных сетей
Wi-Fi



Блокировка USB



Скриншоты
и запись
видео стола



Водяные
знаки поверх
экрана



Мониторинг
сайтов и
соцсетей



Контроль
почты и
мессенджеров



Перехват
с клавиатуры



Контроль
печати



Удаленное
управление



Инвентаризация
устройств и ПО

Текстовый перехват терминалов

```
dlp@172.16.115.9 pts/0 /usr/bin/bash 20260320180201
dlp@dlp: ~
dlp@dlp:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:61:50 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 10.0.194.165/26 brd 10.0.194.191 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:6150/64 scope link
        valid_lft forever preferred_lft forever
dlp@dlp:~$ sudo nano kdska
[sudo] password for dlp:
dlp@dlp:~$
dlp@dlp:~$
dlp@dlp:~$ sudo mkdir gelios
dlp@dlp:~$
```

18:03:00 sudo mkdir gelios<Enter>k

iBaty Monitor фиксирует все команды, вводимые сотрудниками в терминалах **Linux**, **CMD** и **PowerShell**. Это позволяет контролировать действия на серверах и полностью восстанавливать хронологию операций — от удаления файлов до изменения конфигураций и копирования данных.

Результат

Контроль действий привилегированных пользователей.

Снижение рисков саботажа и утечки данных со стороны системных администраторов и IT-специалистов

Контроль беспроводного подключения Wi-Fi



iBaty Monitor позволяет регламентировать подключения к беспроводным Wi-Fi сетям, создавая черные и белые списки доступных беспроводных сетей.

Результат

Защита от теневых сетевых подключений.

iBaty Monitor предотвращает обход корпоративной сетевой политики: сотрудники не смогут раздавать интернет со смартфона, подключаться к несанкционированным сетям или обходить корпоративный фаервол для передачи данных

Защита от массового копирования файлов



iBaty Monitor автоматически **блокирует** внешний носитель при обнаружении попытки массового копирования файлов. Система реагирует в момент начала передачи данных, предотвращая возможную утечку. Чувствительность срабатывания можно гибко настраивать, определяя пороговые значения для объёма, количества и периода копируемых файлов.

Результат

Предотвращение кражи данных злоумышленниками.

Система останавливает инцидент автоматически, не дожидаясь реакции офицера ИБ

Перейдите от догадок к контролю

Закажите бесплатную
демонстрацию продукта и
запустите **пилотный проект**
всего за **1 день**

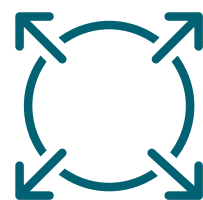


30
дней бесплатного
пробного периода



Быстро

Развертывание пилотного проекта
занимает не более одного дня



Комплексно

Вы сможете оценить сразу весь
комплекс решаемых задач и
принять правильное решение



Легко

Требуется минимум усилий и
ресурсов для запуска



info@msmax.kz



https://msmax.kz/dlp_ibatyr/