



15 ЛЕТ ЗАЩИЩАЕМ
ВАШИ ДАННЫЕ

ГК InfoWatch, о продуктах и технологиях

Зайнулла Жумаев
Старший менеджер по
техническому сопровождению продаж

Москва, 2019

Ответим на 2 вопроса:

1. Как защитить данные в условиях удаленной работы?
2. На сколько активно сотрудники работают из дома?

Некоторые клиенты



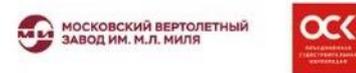
НЕФТЕГАЗОВЫЙ СЕКТОР



ЭНЕРГЕТИКА



ПРОМЫШЛЕННОСТЬ



ТЕЛЕКОММУНИКАЦИИ



БАНКИ



СТРАХОВЫЕ КОМПАНИИ



ГОСУДАРСТВЕННЫЙ СЕКТОР



HOME CREDIT BANK

ТРАНСПОРТ И ЛОГИСТИКА



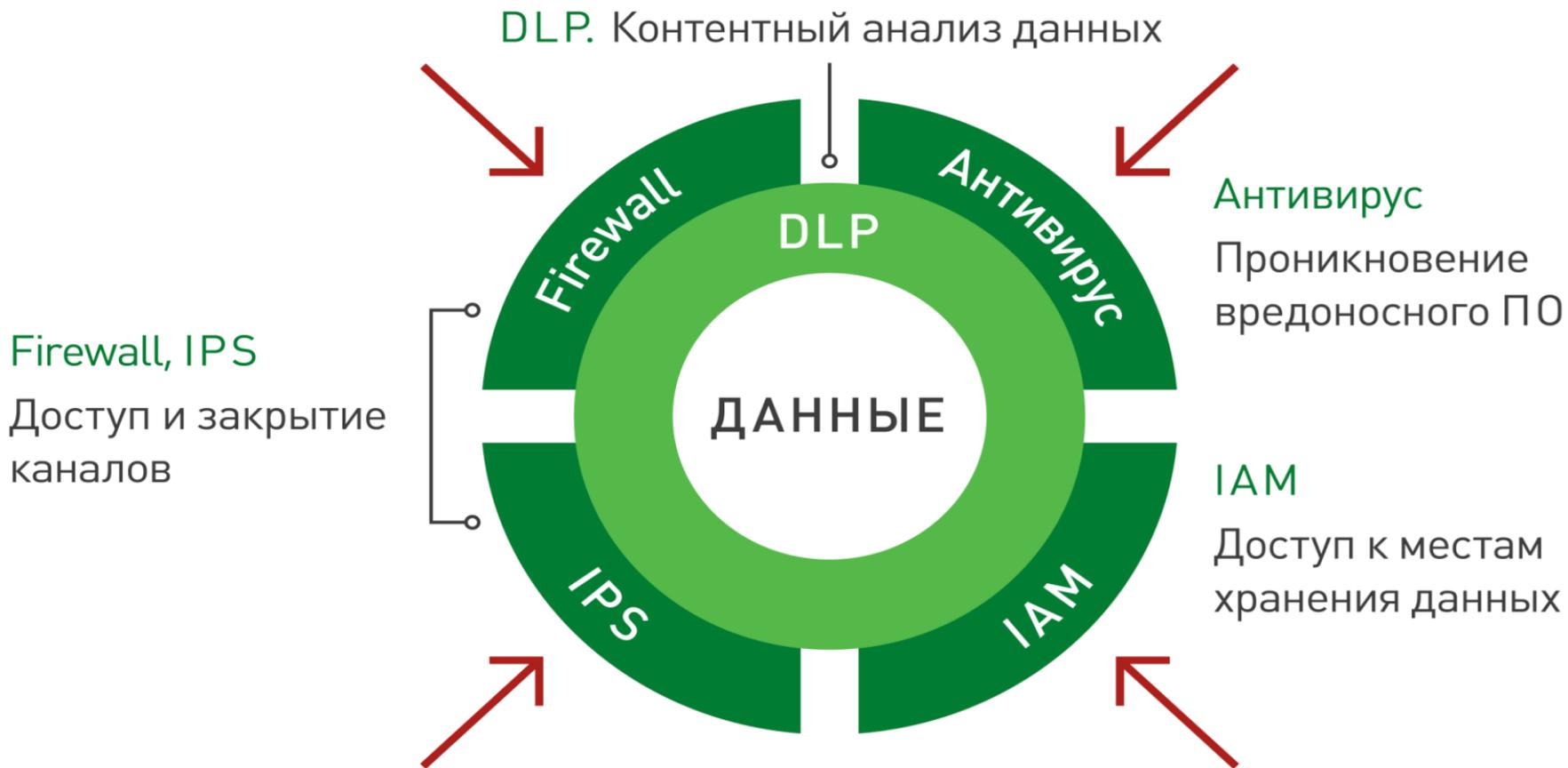
МЕДИЦИНА И ФАРМАЦЕВТИКА



ТОРГОВЛЯ



DLP расширяет инструментарий ИБ





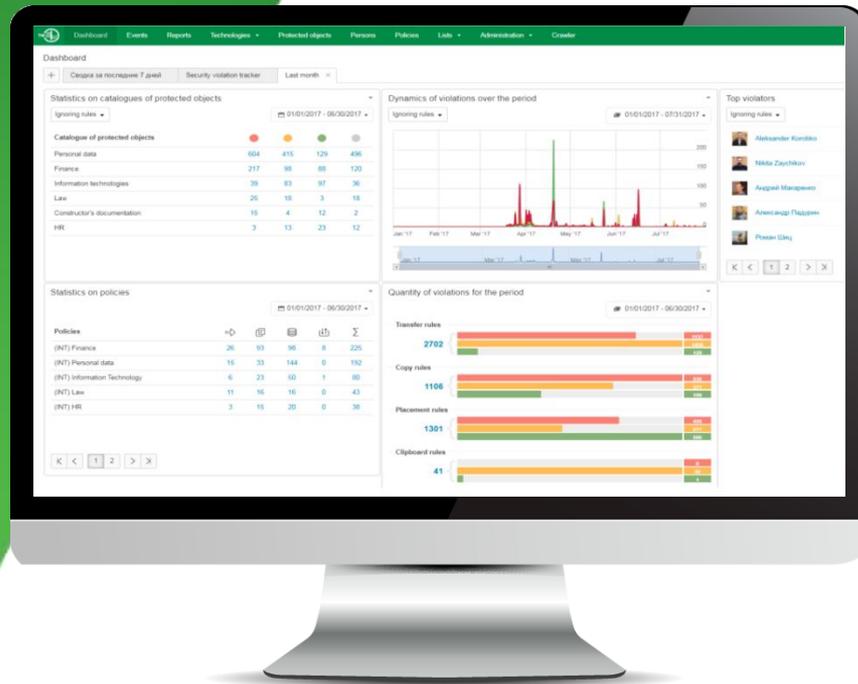
Определяет
содержимое файлов



Использует
комбинации технологий



Выявляет сговоры и
мошеннические схемы



Логика работы Traffic Monitor



Перехват

Анализ

Решение

Хранение

ПЕРЕХВАТ



Контроль почты и сети интернет



контроль
на шлюзе

MAPI

SMTP(S)

IMAP4(S)

POP3(S)

HTTP(S)

контроль
на агенте

Контроль устройств и подключений



CD/DVD

FTP

MTP

SMB

PTP

Flash

УСТРОЙСТВА

Bluetooth

FireWire

и др.

ПЕЧАТЬ

локальные

сетевые

терминальные

Контроль приложений



буфер обмена

печать

черные и белые
списки

Контроль в
терминальных
сессиях

МЕССЕНДЖЕРЫ

Jabber (XMPP)
Telegram
Vk&Facebook
Lync
...

ПРИЛОЖЕНИЯ

**Терминальные
СЕРВЕРА**

Microsoft RDP
Citrix ICA

Контроль хранилищ



Контроль вставки

Контроль в приложениях

Контроль в терминальных сессиях

БУФЕР ОБМЕНА

ОБЛАЧНЫЕ хранилища

Dropbox
GoogleDrive
Evernote
OneDrive
SugarSync
Яндекс.Диск



Локальные папки

Сетевые папки

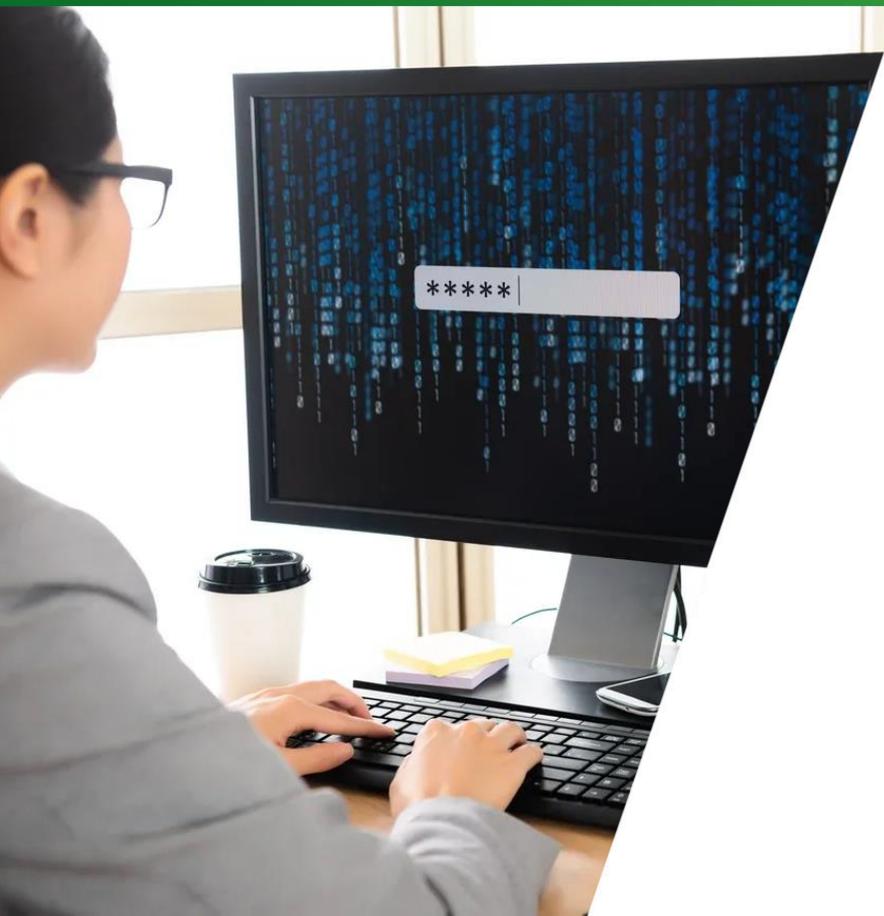
Сетевое хранилище
SharePoint

ЛОКАЛЬНЫЕ И СЕТЕВЫЕ хранилища



InfoWatch
Crawler
Контроль хранилищ

Keyboard Monitor



- Перехватывает набор с клавиатуры для конкретных приложений
- Фиксирует скриншоты окна, в котором вводился текст

АНАЛИЗ



INFOWATCH®
ИСТОРИЯ
КОМПАНИИ

2002

2004

2006

2010 2009 2008 2007 2006 2005 2004 2003 2002 2001

2003

2001

INFOWATCH

Объекты защиты

- Договора
- Специфика компании
- Строго конфиденциальная информация
- Финансовые анкеты и заявления

Содержимое

- Внешнее устройство
 - Гриф ограничения доступа.docx
 - Гриф ограничения доступа.docx
 - Текст

Название вложения

Внешнее устройство

[Развернуть текст без совпадений](#)

пометы типа: «Лично», «Только в руки», «Только адресату», «Лично в руки» и др. При регистрации **конфиденциальных** документов к его номеру грифа конфиденциальности, например: № 37к, 89ск, 97дсп.

Документы и информация, **конфиденциальные** в целом (например, документация службы персонала, службы безопасности, документы, отн. т.д.), как правило, не маркируются, потому что в полном объеме обладают строгим ограничением доступа к ним персонала.

На ценных, но неконфиденциальных документах может проставляться помета (отметка, надпись, штамп), привлекающая особое внимание и. Например: «Собственная информация фирмы», «Информация особого внимания», «Копии не снимать», «Хранить в сейфе» и др. Может ставит согласия фирмы не может быть

[Развернуть текст без совпадений](#)

или штамп обязательно проставляются при направлении **конфиденциальной** для фирмы информации в государственные учреждения, котор. Гриф конфиденциальности присваивается документу:

- исполнителем при подготовке к составлению проекта документа;
 - руководителем структурного подразделения (направления деятельности) или руководителем фирмы при согласовании или подписании до
 - работником службы КД при первичной обработке поступающих документов, если **конфиденциальный** для фирмы документ не имеет грифа
- Изменение или снятие грифа конфиденциальности документа производится при изменении степени конфиденциальности и ценности содер. для этих действий являются: соответствующая корректировка перечней **конфиденциальных** сведений или документов фирмы; истечение

[Развернуть текст без совпадений](#)

службы КД должен регулярно просматривать учетные карточки или инвентарные описи **конфиденциальных** документов и выявлять те доку. характеристики ограничения доступа. При изменении или снятии грифа полномочное должностное зачеркивания грифа или написания нового, указания основания для выполнения этого действия и г. необходимые записи в учетной форме документа. После снятия грифа документ передается в служ. снятия грифа конфиденциальности с документа сообщается заинтересованным фирмам и предпри.

Tsvileva Anna
Tsvileva Anna
1
2013-02-06T09:42:00Z
2013-02-06T09:43:00Z

Категория
Объекты защиты:
- Строго конфиденциальная информация

Категории:
- Грифы секретности

Категория
Объекты защиты:
- Строго конфиденциальная информация

..

Анализ изображений



Паспорта



Банковские карты



Печати и факсимиле



Другие графические объекты, обучение

Анализ выгрузок из баз данных

Обнаружение фрагментов даже одной записи из базы данных

О СДЕЛКЕ изменить

Сумма и валюта
4 453 000 руб.

Стадия
Финальный счёт

Дата завершения
4 Апреля 2019

Клиент

Контакт

Петр Иванов

+7 964 123-45-67 petr.ivanov@yandex.ru

[Выбрать поле](#) [Создать поле](#) [Удалить раздел](#)

Simona	Morasca	3 502 283	Chapman, Ross E Esq	419-503-2484	simona
Mitsue	Tollner	3 749 169	Morlong Associates	773-573-6914	mitsue
Leota	Dilliard	2 414 155	Commercial Press	408-752-3500	leota@
Sage	Wieser	3 562 765	Truhlar And Truhlar Attys	605-414-2147	sage_w
Kris	Marrier	3 045 284	King, Christopher A Esq	410-655-8723	kris@g
Minna	Amigon	3 676 339	Dorl, James J Esq	215-874-1229	minna
Abel	Maclead	3 841 612	Rangoni Of Florence	631-335-3414	amacle
Kiley	Caldarera	3 593 615	Feiner Bros	310-498-5651	kiley.ca
Петр	Иванов	4 453 000	физ лицо	+7 964 123-45-67	petr.fa
Graciela	Ruta	4 808 288	Buckley Miller & Wright	440-780-8425	gruta@
Cammy	Albares	2 004 544	Mousseaux, Michael Esq	956-537-6195	calbare
Mattie	Loquette	3 138 495	Century Communications	602-277-4385	mattie
Meaghan	Garufi	3 596 378	Bolton, Wilbur Esq	931-313-9635	meagha
Gladys	Rim	3 934 820	T M Bxbee Company Pc	414-661-9598	gladys.i
Yuki	Whobrey	4 895 322	Farmers Insurance Group	313-288-7937	yuki_w
Fletcher	Flosi	4 037 080	Post Box Services Plus	815-828-2147	fletche
Bette	Nicka	2 244 373	Sport En Art	610-545-3615	bette_r
Veronika	Inouye	4 549 666	C 4 Network Inc	408-540-1785	vinouye
Willard	Kolmetz	4 534 372	Ingallo, Donald R Esq	972-303-0107	willard

Клиентские базы, финансовая информация, персональные данные

Комбинирование технологий анализа

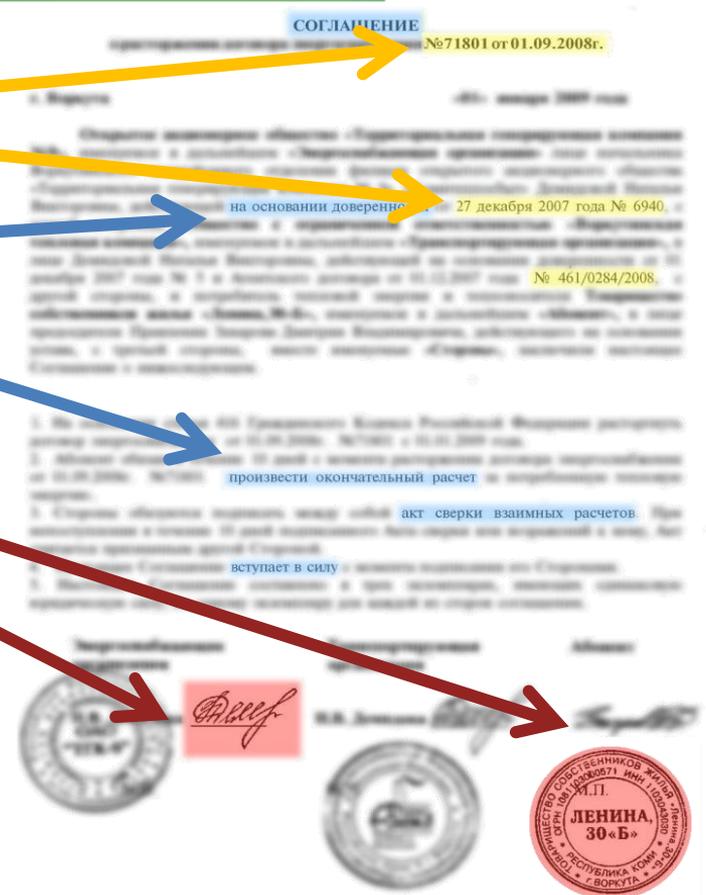
Текстовые
объекты

Термины и
фразы

Печати и
факсимиле



Tesseract
ABBYY[®]
Fine Reader Engine



PersonMonitor -
Точечное
расследование
ИНЦИДЕНТОВ



INFOWATCH®
ИСТОРИЯ
КОМПАНИИ

2002

2004

2006
2007
2008
2009
2010

2003

2002

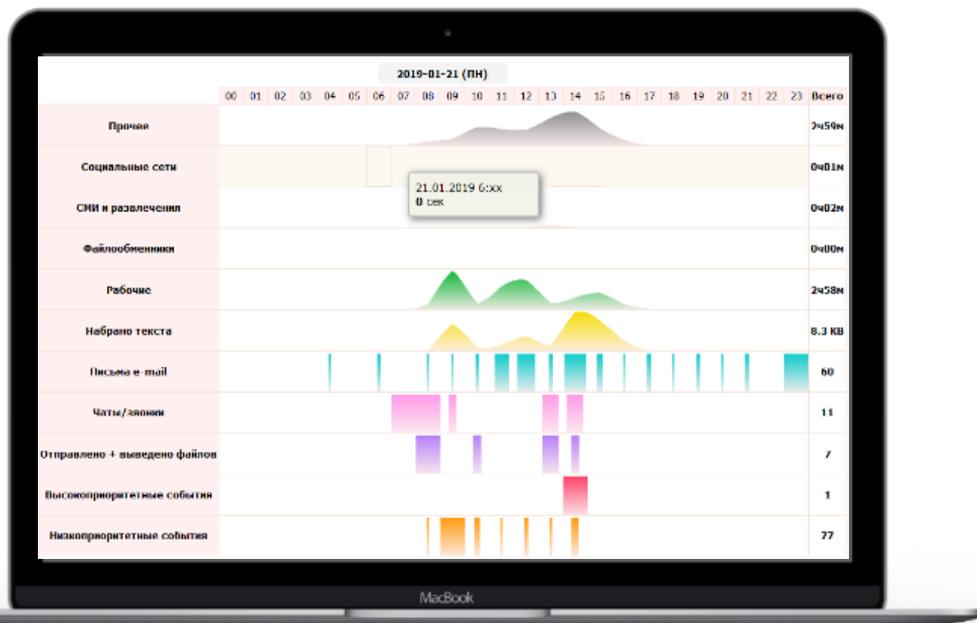
2001

2003

2001

INFOWATCH

Лента активности



Визуализирует и поминутно отражает рабочий день сотрудника.

Каждое (не)эффективное решение, каждая минута, потраченная впустую, любая рискованная ситуация наглядно показаны в ленте.

Мониторинг в режиме реального времени



- ✓ Удаленное подключение к рабочему столу сотрудника
- ✓ Мониторинг действий привилегированных пользователей

Веб-камера, скриншоты, микрофон



- ✓ Запись звука и видео с веб-камеры на рабочем месте
- ✓ Снятие скриншотов с рабочего стола сотрудника

Мобильная защита



INFOWATCH®
ИСТОРИЯ
КОМПАНИИ

2002

2004

2007

2010

2010

2009

2008

2007

2006

2005

2004

2003

2002

2001

2003

2001

INFOWATCH



Расширение защищаемого периметра



Использование приложений и сайтов



Контроль звонков, СМС и клавиатуры



7.0 +

Можно начать с пилотного проекта



ПИЛОТ



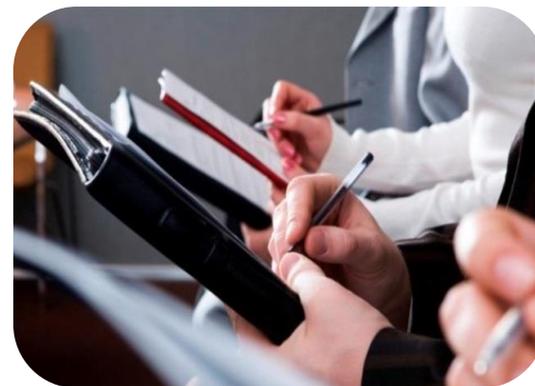
АУДИТ

ВНЕДРЕНИЕ



ОБУЧЕНИЕ

ТЕХПОДДЕРЖКА





15 ЛЕТ ЗАЩИЩАЕМ
ВАШИ ДАННЫЕ

ГК InfoWatch, о продуктах и технологиях

Зайнулла Жумаев

+7 (964) 620-39-46

Zaynulla.Zhumaev@InfoWatch.com

Москва, 2019