КИБЕР
ПРОТЕКТ

Cyber Protego

Защита от утечки данных, где Zero Trust
не пустое слово

Почему происходят утечки данных?

Данные есть в любой организации и имеют ценность.

Технологические факторы

- Распределённость ИТ-процессов, распространение скоростных беспроводных сетей и ширпотребовских сервисов
- Распространённость моделей GYOD и BYOD
- Рост размеров памяти носителей и облачных хранилищ данных при снижении цены, сложности использования, габаритов
- Рост числа уязвимостей по мере усложнения корпоративной и личной ИТ инфраструктуры

Человеческий фактор

Все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный **пользователь** – который далеко не всегда является владельцем данных, будучи при этом сотрудником организации.

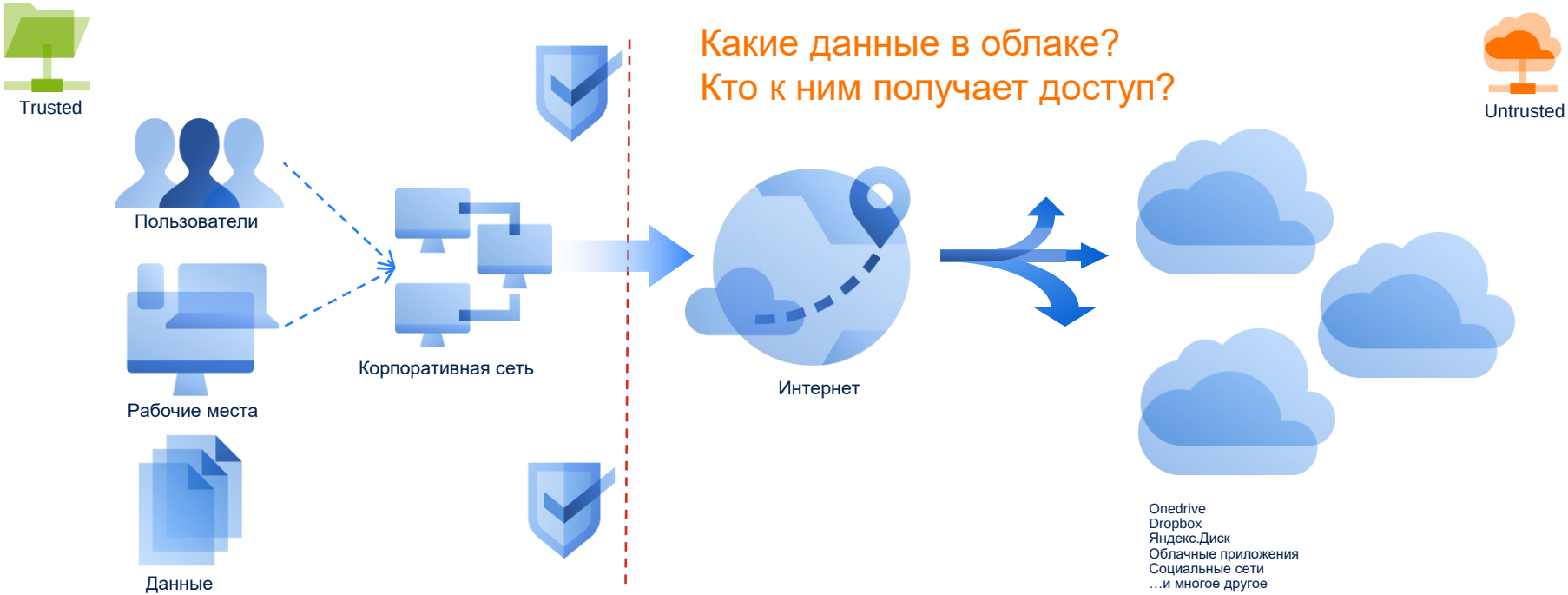
Чрезмерное доверие сотрудникам

- Непреднамеренные утечки: ошибки и халатность, чрезмерное усердие («доработка на дому»), превышение полномочий
- Направленные утечки: злоумышленники, промышленный и коммерческий шпионаж

Классика жанра – выстроить мощную систему противодействия внешним угрозам и атакам, игнорируя внутренние.

«Слепые зоны»

Облачные сетевые ресурсы не контролируются корпоративной ИБ



Немного объективной статистики

83%

of organizations studied have had more than one data breach.

60%

of organizations' breaches led to increases in prices passed on to customers.

79%

of critical infrastructure organizations didn't deploy a zero trust architecture.

19%

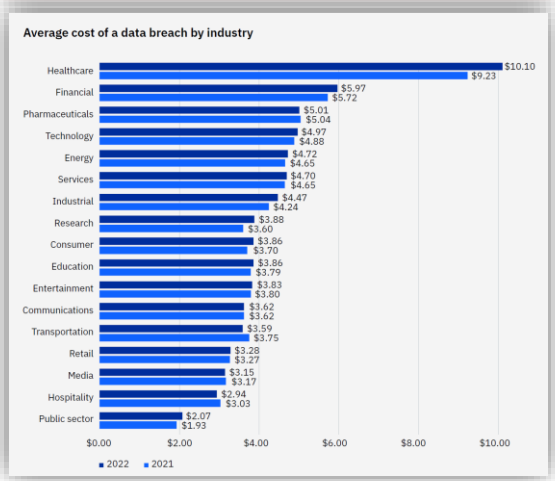
of breaches occurred because of a compromise at a business partner.

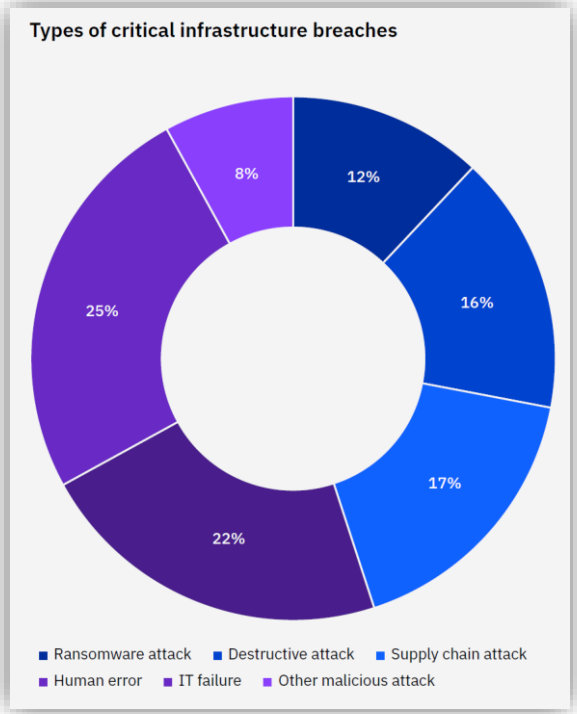
45%

of the breaches were cloud-based.

59%

Percentage of organizations that don't deploy zero trust





Ponemon: 3,600 separate interviews with individuals at 550 organizations that suffered a data breach between March 2021 and March 2022

Ponemon INSTITUTE

КИБЕРПРОТЕКТ

Источники: "Cost of a Data Breach", **Ponemon Institute & IBM Security, 2022** ; "Insider Threat Report", Cybersecurity Insiders, 2018; "Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017; CSO Online, 2017; "Insider Data Breach Survey", Opinion Matters, 2019; 2020 Cost of a Data Breach Report" Ponemon Institute LLC, July 2020; "2020 Cost of Insider Threats Global Report" Ponemon Institute LLC, February 2020; "Best Practices: Mitigating Insider Threats" Forrester Research, May 2019

Инсайдеры - основная причина утечки данных

90% организаций чувствуют себя уязвимыми перед лицом инсайдерских угроз - 53% сообщают, что подверглись атаке со стороны инсайдеров за последние 12 месяцев

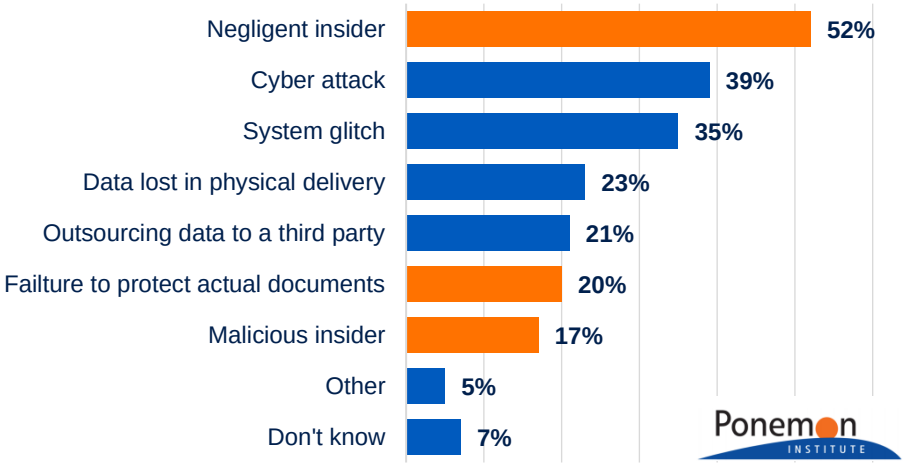
72% сотрудников делятся конфиденциальной или иной защищаемой информацией компании

35% сотрудников поделились информацией, **не подозревая,** что ей не следует делиться.

Годовой ущерб от утечек, связанных с инсайдерами (~ 45% всех нарушений)

- **31% увеличение** за последние 2 года
- Средний **по всему миру**: **$11,45 млн.**
- В среднем за **Малый и средний бизнес: $7,68**
- **89% от стоимости** связано с действиями после инцидента (реактивная защита)

Причины утечки данных



Традиционные антивирусы, брандмауэры, шифрование **и даже бэкапы** не защищают от внутренних утечек данных

КИБЕРПРОТЕКТ

Источники: “Global Cost of Insider Threats”, Ponemon Institute, 2020; “Insider Threat Report”, Cybersecurity Insiders, 2018; “Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017; CSO Online, 2017; “Insider Data Breach Survey”, Opinion Matters, 2019; 2020 Cost of a Data Breach Report” Ponemon Institute LLC, July 2020; “2020 Cost of Insider Threats Global Report” Ponemon Institute LLC, February 2020; “Best Practices: Mitigating Insider Threats” Forrester Research, May 2019

Что такое Zero Trust?

Zero Trust («нулевое доверие») – модель безопасности, предложенная Forrester в 2010 году, расширена в 2017 до ZTX.

Zero Trust eXtended означает полное отсутствие доверия кому-либо – даже пользователям внутри периметра.

- С моделью безопасности Zero Trust доверие больше не предоставляется по умолчанию никому, ни внутри корпоративной сети, ни за ее пределами. Вместо этого Zero Trust следует принципу «никогда не доверять, всегда проверять». Идентификация пользователя и конечная точка должны подтвердить, что они не скомпрометированы, и только тогда они получат доступ к корпоративным ресурсам и услугам.

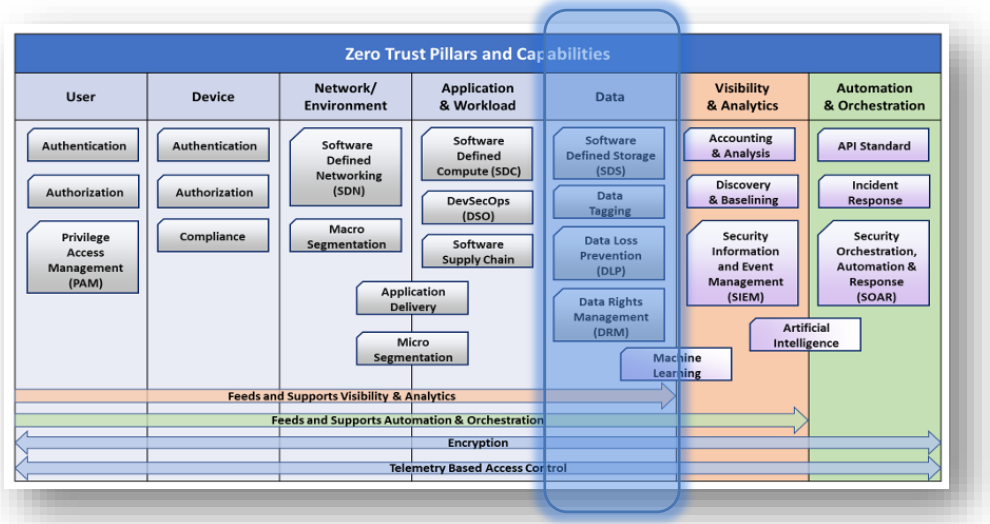
Концепция Zero Trust: угроза может исходить откуда угодно. Невозможно заранее описать и приоритизировать все угрозы.

- Данные Zero Trust: основа концепции «нулевого доверия» заключается в защите данных в первую очередь, а не последнюю. Это означает необходимость уметь анализировать, защищать, классифицировать, отслеживать и поддерживать безопасность своих корпоративных данных.
- Пользователи Zero Trust: Люди являются наиболее слабым звеном в стратегии безопасности. Ограничивайте, отслеживайте и строго контролируйте принципы получения пользователями доступа к ресурсам внутри сети и в интернете.

NIST 800-207
https://www.forrester.com/blogs/zero-trust-in-practice/
https://www.cisco.com/c/dam/global/uk_ua/training-events/zero-trust-1-dec.pdf

Zero Trust, ориентированный на данные

Zero Trust Reference Architecture



- ZeroTrust разбивается на семь столпов, каждый из которых является ключевой областью для реализации контроля Zero Trust.
- Первые пять столпов - это пользователи, устройства, сети, приложения и данные.
- Подход к Zero Trust, ориентированный на данные, интегрирует DLP в более широкую архитектуру с прицелом на непрерывную оценку угроз и возможность автоматического и быстрого реагирования на них.

Department of Defense (DOD)
Zero Trust Reference Architecture

Version 1.0
February 2021
Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

Ключевые принципы модели безопасности с нулевым доверием – примеряем к данным

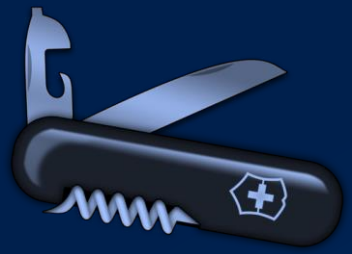
Требование безопасного и подтвержденного доступа ко всем ресурсам

Модель минимальных привилегий для контроля доступа

Отслеживание всей активности пользователей с помощью аналитики данных и журналов

Модель наименьших (минимальных) привилегий – парадигма безопасности, ограничивающая права доступа каждого пользователя до уровня, который необходим ему **для выполнения служебных обязанностей**. Ограничение доступа сотруднику – по сути равно созданию препятствий в получении злоумышленником доступа к большому числу данных через компрометацию одного аккаунта.

КИБЕРПРОТЕКТ



Cyber Protego

Универсальный инструмент для любой концепции безопасности

Принципы Zero Trust в Cyber Protego

Zero Trust – прежде всего модель «Доступ с наименьшими привилегиями»

Реализация сценария «минимальные привилегии»: расширенный гибкий контроль устройств, носителей и сетевых протоколов в зависимости от ряда параметров

Сначала ограничить до минимума перечень разрешенных каналов передачи данных – *оставить только необходимые для выполнения рабочих задач*

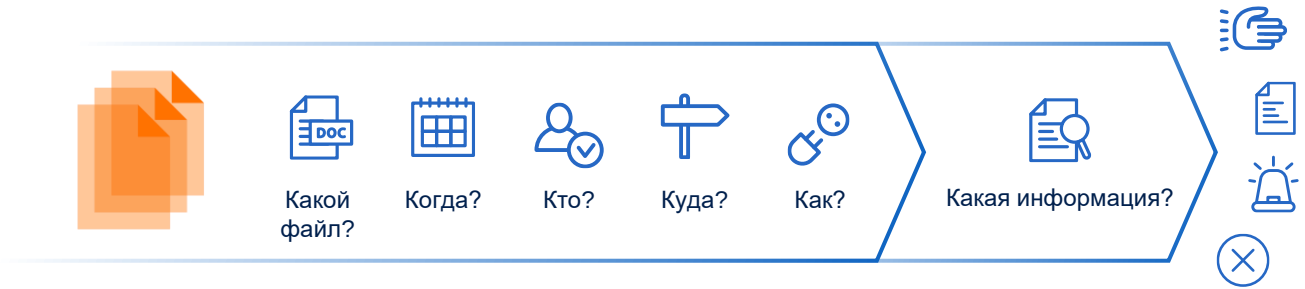
Расширять доступы по необходимости – принципы Белых списков и точечного доверия пользователю и его устройствам

Использовать инспекцию содержимого (контента) для избирательной блокировки попыток передачи данных, нерелевантных для бизнес-процессов, и приводящих к утечке

- Белый список USB-устройств
- Белый список Сетевых протоколов
- Временный Белый список USB-устройств
- Контентный анализ в режиме реального времени

Возможности Cyber Protego

Полнофункциональная DLP-система



Сценарии, когда DLP-агент – единственное решение

- Контроль рабочей станции вне офиса
- Контроль «закрытых» протоколов
- Анализ передаваемых данных в реальном времени (передача, сохранение, печать)
- Регулярное сканирование локальной файловой системы
- Запись экрана и клавиатуры

Ключевые возможности полноценного DLP-агента

- Защита данных при операциях с устройствами
- Защита данных в сетевых коммуникациях
- Контентный анализ в режиме реального времени
- Защита данных при операциях с системными функциями
- Сканирование хранимых данных на защищаемой рабочей станции
- Мониторинг активности пользователей

*Применимо к агенту для ОС Windows

Контроль устройств и интерфейсов

Контролируемые интерфейсы и устройства

USB	LPT	Оптический привод	Жёсткий диск
FireWire	COM	iPhone	Windows Mobile
Wi-Fi	IrDA	Blackberry	Palm
Bluetooth	Съёмные устройства	MTP	Буфер обмена
Гибкие диски	Ленточные накопители	Канал печати	ТС-устройства

Контроль каналов утечки

Распознавание **устройств**

HID, виртуальные принтеры, iPhone, модемы, зашифрованные, другие

Многоуровневый контроль

На уровнях интерфейса и типа устройств

Контроль множества **операций**

Чтения, записи, копирования, вставки, форматирования, извлечения, других

Расширенные настройки принтеров

Исключают заданные принтеры из общего контроля канала печати

Белые списки

Устройств USB, оптических носителей, временный белый список устройств USB

Базовые функции агента

Политики **для заданных пользователей и групп**

Независимые наборы политик внутри и вне корпоративной сети с автопереключением между ними

RBAC с защитой от действий локальных администраторов и антируткитов

Воспрепятствование деятельности **аппаратных кейлоггеров**

Интеграция с решениями по **шифрованию носителей**

Передача собираемых данных на *Серверы управления*

Контроль сетевых коммуникаций

Контролируемые каналы коммуникаций

SFTP (9.4.0)	HTTP(S)	FTP(S)	Telnet	SMTP(S)
IMAP (9.4.0)	MAPI	IBM Notes	Веб-почта	Соц. сети
Облачные хранилища		Веб-поиск	Поиск работы	Telegram
Viber	Zoom	Skype	WhatsApp	ICQ
Jabber	IRC	Mail.ru Агент	Торрент	SMB

Технологии контроля, в т.ч. VPN, P2P, прокси-трафика

Независимый от приложений контроль трафика

- Глубокая инспекция пакетов агентом **(DPI)**
- **MITM-контроль** SSL-трафика, в т.ч. своими сертификатами*
- Контроль **E2EE коммуникаций**

Встроенный **IP Firewall**

- Контроль **TCP и UDP** трафика вне списка поддерживаемых протоколов и сервисов
- **Независимо** от основных политик контроля **или в режиме наследования**

Выборочный контроль множества **операций**

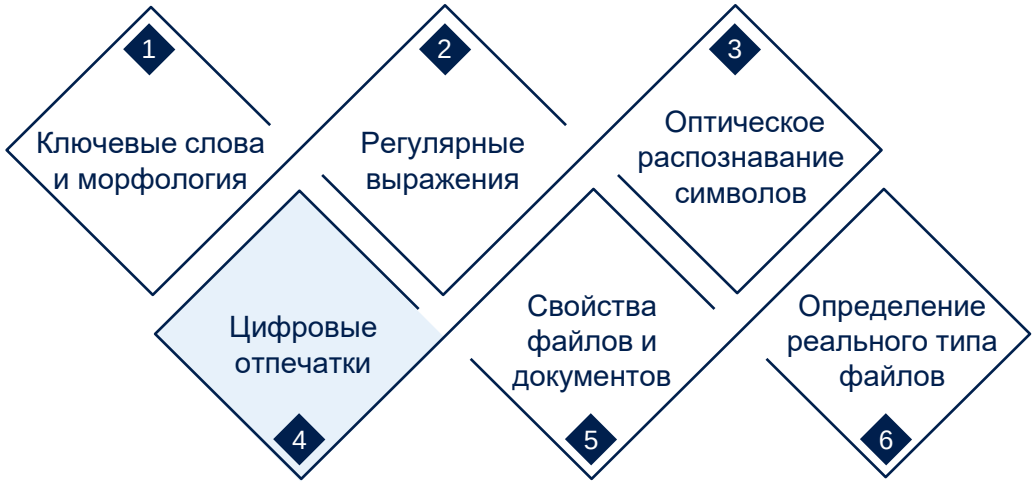
Подключения к серверам, отправки сообщений, вложений, POST- и поисковых запросов, публикации постов, других операций

Белые списки

Сетевых протоколов и веб-сервисов, SSL-коммуникаций, диапазонов IP адресов, портов, веб-ресурсов по URL, адресов и ID отправителя / получателя

Контроль содержимого

Автономные* технологии контентного анализа



Словари и шаблоны регулярных выражений **в комплекте поставки**

Составные правила, пороговые значения срабатывания

Типы правил

В разрыв

Блокировка, мониторинг, алерты

Пост-обработка

Мониторинг и алерты **без блокировки**

КИБЕРПРОТЕКТ

*За исключением правил поиска по цифровым отпечаткам

Контролируемый удаленный доступ к данным

Физические среды

Агент **на рабочей станции или сервере** контролирует каналы утечки и данные, передаваемые по ним

Виртуальные среды

Агент **внутри виртуальной машины** контролирует в т.ч. каналы связи между ВМ и хостом, данные, передаваемые по ним

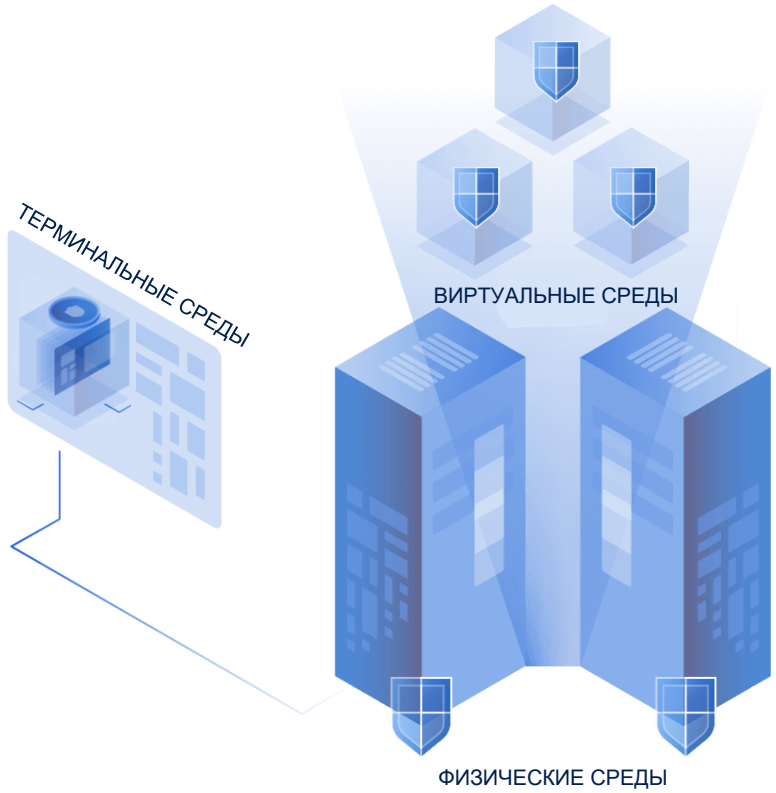
Терминальные среды

Агент **на терминальном сервере** контролирует в т.ч. каналы связи между терминальным клиентом и терминальным сервером, данные, передаваемые по ним

ТОТАЛЬНЫЙ КОНТРОЛЬ В ДВУХ НАПРАВЛЕНИЯХ

Все возможные каналы связи и данные, принимаемые и передаваемые по ним

Буфер обмена, проброшенные порты, устройства, диски



Мониторинг активности пользователей

Видеозапись экрана, запись сведений о запущенных процессах, кейлоггер

Запись **при реализации политики DLP** другими модулями агента

Напр., срабатывание **контентного правила**

Запись **при выполнении** заданных **системных условий**

Напр., **VPN** подключение, заданное **окно в фокусе**

Запись **до* или после** наступления заданного **события**

Видео может содержать **до 5** предшествующих событию **минут**

Глубокая **детализация условий** начала записи

Составные правила с условиями, объединёнными операторами **И/ИЛИ/НЕ**

Неотъемлемая часть контроля с прозрачной интеграцией в политики предотвращения утечек

Балансировка длительности и размера записей

- **Цветная или ч/б** запись
- Запись **в настраиваемом разрешении**
- **Запись** с настраиваемой **частотой кадров**
- **Остановка** записи **при отсутствии активности**

Особенности реализации и преимущества

Полноценный DLP-контроль в любых условиях – в офисе или вне его с автоматическим переключением DLP-политик

Контентная фильтрация **в режиме реального времени**

Централизованное управление, включая интеграцию в MS Active Directory

User Activity Monitor (UAM), интегрированный в DLP-политики, с записью до и после события

Защита данных в средах виртуализации **Cyber Protego TS**

Наибольшая широта охвата потенциальных каналов утечки данных

Высочайший уровень **самозащиты агентов**

Автоматические действия по устранению нарушений хранения данных (Discovery)

Независимый от приложений и портов контроль сетевых протоколов, встроенный **резидентный модуль DPI** (Deep Packet Inspection)

Почему без DLP не обойтись?

Единственно доступная сегодня технология, удовлетворяющая всем требованиям защиты от утечки данных

Защита стратегически важной информации

Непрерывный контроль всех возможных каналов информационного обмена и хранимых данных

Соответствие требованиям регуляторов

Обеспечение соответствия требованиям стандартов за счет полноценного контроля каналов передачи данных и устройств хранения информации, журналирования событий и инструментария расследования инцидентов

Выявление инцидентов

- Повышение эффективности ИБ - реагирование на события, связанные с вопросами защиты данных

- Аудит журналов DLP-системы

- Выявление инсайдеров-злоумышленников, нелояльных сотрудников.

Контроль исполнения политики хранения

Превентивная защита данных, размещенных в корпоративной ИТ-инфраструктуре

Отечественный производитель ПО

Полный цикл разработки, развития, поддержки

Примеры внедрений

КИБЕРПРОТЕКТ

ИТ-кластер Физтехпарк
Долгопрудный, Московская область

Технопарк Иннополис
Республика Татарстан

Экспертиза

ПРИОРИТЕТ 2020
НАЦИОНАЛЬНАЯ ПРЕМИЯ В ОБЛАСТИ ЭФФЕКТИВНОГО ПРИМЕНЕНИЯ ПЕРЕДОВЫХ ТЕХНОЛОГИЙ

1 место
Победитель Премии Цифровые Вершины 2020

Участие в проектах и ассоциациях, резидентный статус

АРПП Отечественный софт
Sk Сколково
ЦИФРОВАЯ ЭКОНОМИКА
RUS®SOFT
АПКИТ
INNOPOLIS UNIVERSITY

Продукты и решения

КИБЕР Бэкап

Резервное копирование
ИТ-систем любой сложности
с централизованным управлением
и оптимизацией хранения

КИБЕР Бэкап Облачный

Резервное копирование данных в физических, виртуальных и облачных средах **для поставщиков услуг**

Часть экосистемы
отечественного ПО с постоянно расширяющейся **сетью технологических партнёрств**

Единый реестр Минцифры

Сертификация ФСТЭК

КИБЕР Протего

Программный комплекс
предотвращения утечек используемых,
передаваемых и хранимых данных

КИБЕР Инфраструктура

Масштабируемое, экономичное и универсальное программно-определяемое решение: виртуализация, хранилище и сеть

КИБЕР Файлы

Корпоративное решение для синхронизации и безопасного обмена файлами

КИБЕРПРОТЕКТ

СПАСИБО!

Ильшат Латыпов

Менеджер продукта

Ilshat.Latypov@cyberprotect.ru

cyberprotect.ru