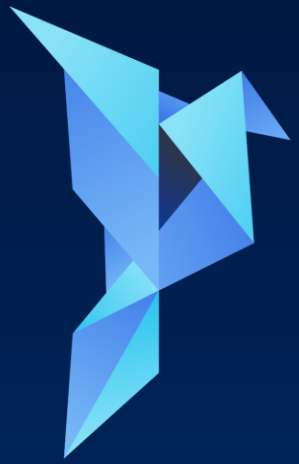


PACIFICA

A NOVENTIQ Company

Конечные точки как главные цели кибератак

Алан ИБРАГИМОВ – инженер по кибербезопасности

ЧТО ТАКОЕ КОНЕЧНАЯ ТОЧКА?

КОРПОРАТИВНЫЕ НОУТБУКИ

МОБИЛЬНЫЕ УСТРОЙСТВА

ВИРТУАЛЬНЫЕ СЕРВЕРА

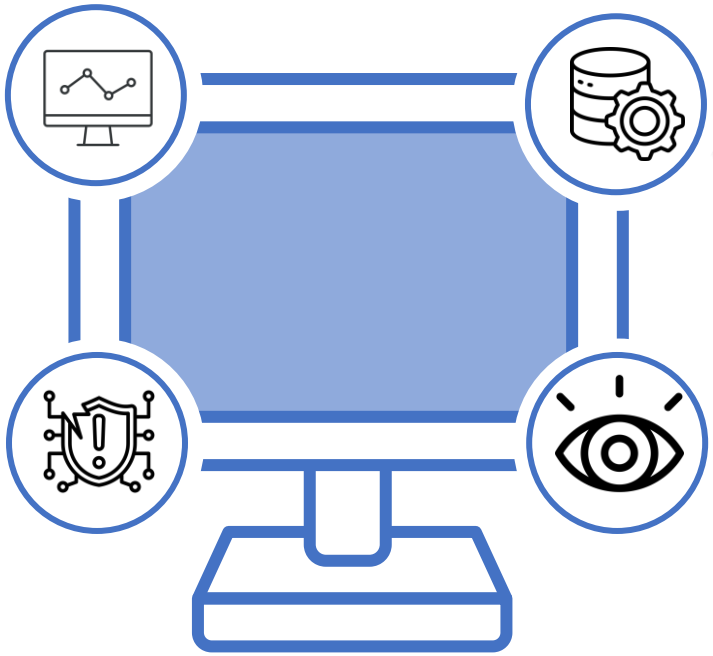
КОНЕЧНАЯ ТОЧКА КАК ГЛАВНАЯ ЦЕЛЬ КИБЕРАТАКИ

Возможность масштабирования атаки

- Одна скомпрометированная точка – доступ ко всей сети
- Перемещение и распространение атаки по внутренним системам с зараженного устройства

Слабые защита и контроль

- Работа вне корпоративного периметра (удалённо, в командировке)
- Редкие обновления и патчи
- Отсутствие постоянного мониторинга и централизованного управления



Неограниченный доступ к данным

- Хранение локальных копий документов и почты
- Доступ к корпоративным сервисам и базам данных
- Возможность кражи учетных данных и ключей доступа

Плохая осведомленность сотрудников

- Отсутствие базовых знаний о кибергигиене
- Неспособность распознать фишинговые письма и вредоносные вложения
- Игнорирование предупреждений систем безопасности

PACIFICA
A NOVENTIQ Company

Самые распространенные угрозы для конечных точек

Фишинг и его производные

E-mail

Звонки

Атаки нулевого дня (zero-day)

ПО, не присутствующее в базах сигнатур

Вредоносное ПО

Вирусы

Трояны

Кейлоггеры

Программы-вымогатели

Шифровальщики

Вымогатели

Внешние носители

Зараженные USB-накопители

Внешние диски

PACIFICA
A NOVENTIQ Company

Статистика за 2021-2024

Взрывной рост киберугроз

- Количество атак на корпоративные конечные точки выросло на **68%с 2021 по 2024** г. (Verizon DBIR 2024)
- **80%**успешных атак начинаются с **компрометации конечной точки** (IBM 2024)

Рекордные убытки от инцидентов

- Средняя мировая стоимость инцидента в крупной компании – **$4,88 млн** (IBM Cost of a Data Breach 2024)
- Восстановление после ransomware обходится в среднем в **$2,73 млн без учета стоимости выкупа** (Sophos 2024)
- Компании с удаленными сотрудниками **теряют на 20%больше** при атаках на конечные точки (IBM 2024)

Эволюция атакующих

- Среднее время до Lateral movement – **62 минуты** (CrowdStrike 2024)
- Рост числа атак с использованием **zero-day** уязвимостей **на 50%**за последние **2 года** (Mandiant 2024)

PACIFICA
A NOVENTIQ Company

КАК ЗАЩИТИТЬСЯ?

ТЕХНИЧЕСКАЯ ЗАЩИТА

- Использование **антивирусной системы** для обеспечения базовой защиты
- **Внедрение EDR** для **сбора телеметрии** и **реагирования** на сложные угрозы
- **Шифрование** дисков и данных на устройствах
- Обеспечение защиты **мобильных устройств**

ОРГАНИЗАЦИОННЫЕ МЕРЫ

- Политики безопасности для работы в **офисе и удаленно**
- Ограничение прав доступа по принципу «**минимально необходимого**»
- Постоянный **мониторинг состояния** всех конечных точек, подключающихся к корпоративной сети
- Регулярные **тесты на проникновение** и **аудит ИБ**

ОБУЧЕНИЕ И ОСВЕДОМЛЕННОСТЬ СОТРУДНИКОВ

- **Тренинги** по распознаванию фишинга и социальной инженерии
- Проведение **симуляций атак**
- Формирование **четких инструкций** по действиям при подозрительном инциденте

PACIFICA
A NOVENTIQ Company

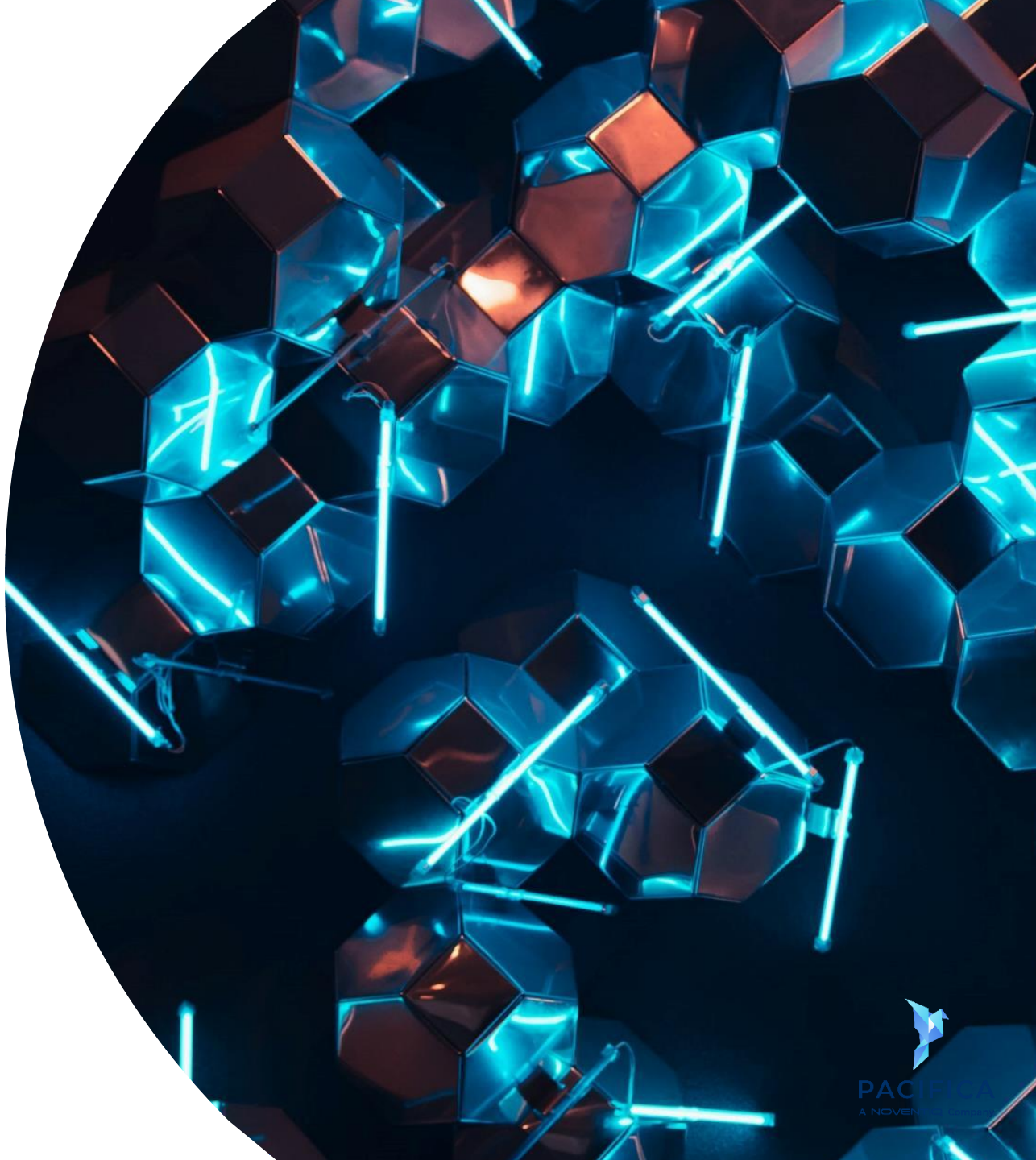
Антивирус – базовый щит для конечных точек

- **Обнаружение и блокировка известных угроз.** Сигнатурный анализ для вирусов, троянов, шпионских программ
- **Веб- и почтовая защита.** Фильтрация вредоносных сайтов, вложений и ссылок
- **Защита от программ-вымогателей.** Мониторинг изменений файлов и блокировка шифрования
- **Автоматическое обновление баз.** Постоянная актуализация данных об угрозах

PACIFICA
A NOVENTIQ Company

Endpoint Detection and Response (EDR)

- **Постоянный мониторинг конечных точек.** Круглосуточный сбор телеметрии и анализ активности на устройствах.
- **Обнаружение сложных и неизвестных ранее угроз.** Поведенческий анализ, поиск индикаторов компрометации (IOC), выявление и остановка zero-day атак
- **Автоматическое и ручное реагирование на инциденты.** Возможность изоляции зараженных устройств от сети, завершение вредоносных процессов и блокировка подключения к серверам
- **Расследование и анализ атак.** Подробная хронология событий на устройстве, сбор информации для улучшения защиты



AV + EDR = Комплексная защита

Выявление известных угроз

Сканирование и фильтрация

Сигнатуры и эвристика

Выявление сложных атак

Мгновенное реагирование

Расследование и форензика

PACIFICA
A NOVENTIQ Company

XDR – Единая консоль для управления безопасностью

Конечные точки

Облако

Сеть

Учетные записи

- Единый обзор всей инфраструктуры
- Выявление атак в сети и на конечных точках
- Полная хронология событий и расследование

Почта

Управление уязвимостями

PACIFICA
A NOVENTIQ Company

Цепочка атаки и ответ XDR

Подключение к незащищенной сети

Попытки входа в корпоративную почту

Вход под УЗ к облачным сервисам из другой страны

PACIFICA
A NOVENTIQ Company

Цепочка атаки и ответ XDR

Компрометация конечной точки → Попытка закрепиться в системе → Использование УЗ для доступа к облаку

Изоляция конечной точки → Блокировка учетной записи = Остановка атаки до того, как злоумышленник закрепится в сети

PACIFICA
A NOVENTIQ Company

MDM – Управление и защита мобильных устройств

Mobile Device Management – централизованное управление мобильными устройствами с контролем доступа, политиками безопасности и обеспечения compliance-статуса

Ключевые возможности

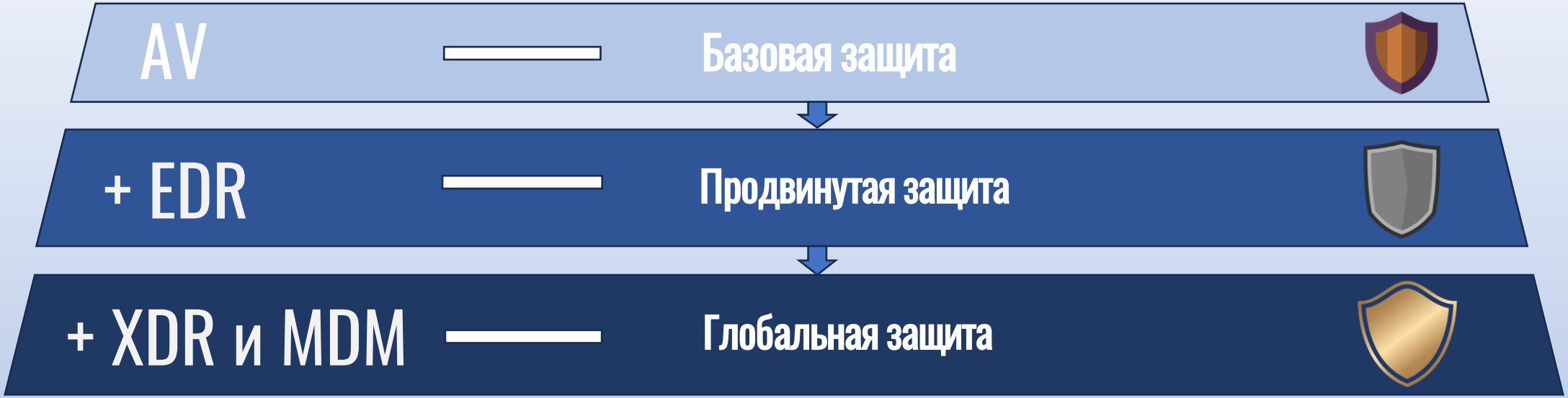
- Централизованное управление
- Защита данных
- Контроль доступа
- Обеспечение Compliance-статуса устройств

Зачем это нужно

- Снижение риска утечек при работе вне офиса
- Поддержка безопасного BYOD и удаленной работы
- Быстрое реагирование на инциденты с мобильными устройствами

PACIFICA
A NOVENTIQ Company

КТО НЕ ПЛАТИТ ЗА БЕЗОПАСНОСТЬ – ТОТ РАСПЛАЧИВАЕТСЯ



ЧТО МЫ ПОНЯЛИ СЕГОДНЯ?

- **Конечные точки** – главный вектор атак
- **Угрозы растут**, атаки становятся **сложнее**, а **цена** инцидентов – **выше**
- **Многоуровневая защита** снижает риск и стоимость инцидентов в разы
- **Инвестиции в безопасность** всегда дешевле **последствий**

PACIFICA
A NOVENTIQ Company

PACIFICA
A NOVENTIQ Company

Спасибо за внимание!

Алматы, проспект Достык 210, БЦ «Коктем Grand»
тел.: +7 (777) 812-03-31
e-mail: ai@pacifica.kz
www.pacifica.kz

PACIFICA – киберспокойствие Вашего бизнеса!


PACIFICA
A NOVENTIQ Company