SOFTPROM

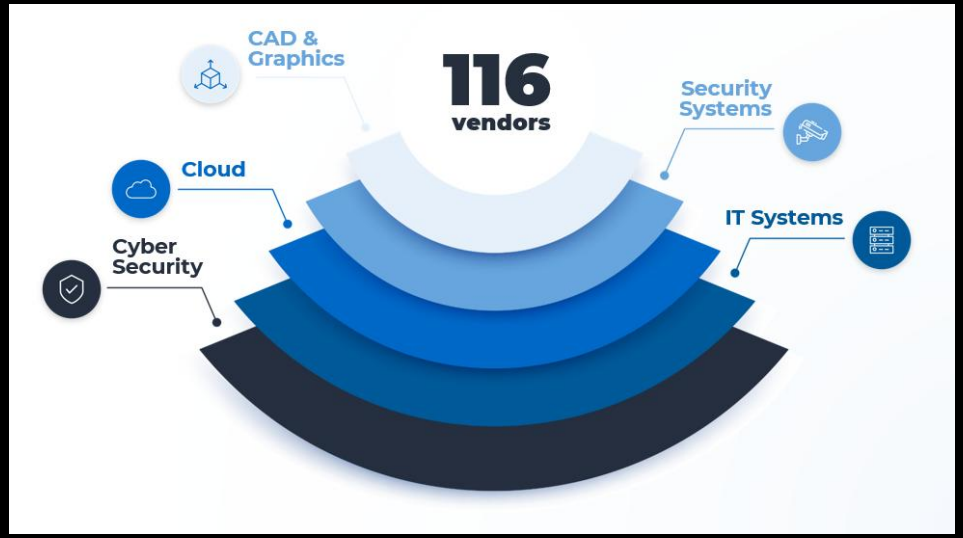
Что скрывается в нашем трафике?

Обнаружение скрытых атак в конвергентных сетях IT, OT и IoT

Barracuda GREYCORTEX CYBERARK Forcepoint

SOFTPROM

- **Value Added Distributor**
- **25** лет на рынке
- Центральная Азия, Кавказ, Восточная и Центральная Европа
- **15** офисов в странах региона
- Консалтинговый отдел (**30** инженеров)



Периметр — иллюзия безопасности

- Вопрос не в том, «**если**» взломают, а в «**когда**»...
- По данным **ГТС** рост кибератак в **Казахстане** — **в 2.6 раза** за последний год
- Стандартная **«входная дверь»** — веб-приложения и **API**; именно они становятся главной целью для проникновения
- Традиционных средств защиты уже недостаточно для такого потока

Насколько функционален наш **WAF**? Он видит атаки на **API**, **DDoS**, ботов?

Barracuda Networks — интеллектуальная защита веб-приложений (**WAF**)

Платформа BarracudaONE

- **Email Protection**
- **Data Protection**
- **Managed XDR**
- **Network Protection**
- **Application Protection**

Почему Barracuda WAF?

- Один из первых запустил **Bot Protection**: обнаружение ботов в спаме
- Простота развертывания и управления
- Готовые шаблоны для **Exchange**, **SharePoint**, **Oracle**, **SAML**, **PHP**
- Предотвращение захвата учетных данных (**account takeover**); оценка риска запросов и **fingerprinting** клиентов, вместо **IP**-адресов
- Разделение на уровне маршрутизации **production-** от **test-** среды – **Vsites**
- Предотвращение активного **DDoS**
- Встроенная балансировка веб-приложений
- Бесплатный **Barracuda Vulnerability Manager**: сканирование уязвимостей, конфигурация и профили **WAF**
- Интеграция со сканерами уязвимостей: **Rapid 7, HPE Security WebInspect, HPE Security Fortify, Barracuda Vulnerability Manager, IBM AppScan, Cenzic Hailstorm, ThreadFix, ImmuniWeb**
- Бесплатное обучение
- Цена ниже конкурентов

Слепые зоны сети

- Самая большая опасность — та, которую мы не видим
- Злоумышленник может быть уже внутри нашей сети
- И он не атакует **«в лоб»**, а незаметно перемещается по сети (**lateral movement**), исследуя наши **«слепые зоны»**, особенно в сетях **IT** и **OT**
- Решение – в сквозной аналитике сетевого траффика

GREYCORTEX

Как распознать активность, которая выглядит легитимной? Как безопасно контролировать сети **OT/SCADA**, не нарушая их работу?

GreyCortex (NDR/NTA) — это система **«thermal vision»** для всего трафика. **ИИ** анализирует не только сигнатуры, но поведение, выявляя аномалии, которые пропускают другие системы

GREYCORTEX Mendel

Вопросы...

GREYCORTEX

1. **Есть ли угрозы в трафике внутреннего периметра (за файрволом)?**
   - **Wi-Fi** зоны, **DMZ**, периметр дата-центров, офисная периферия, мультимедиа-оборудование, системы видеонаблюдение, **IoT**

2. **Кто, с кем, по каким протоколам комуницировал, какой объем данных передал?**
   - Какие пользователи, с какими **IP**, **MAC**, **VLAN**, через какие приложения или службы и с кем общаются?
   - Увидеть все соединения по всем отделениям по протоколу **FTP, SSH, RDP, SMB, etc.**
   - Мониторинг **DNS-**трафика

3. **Насколько типовой является та или иная коммуникация? Есть ли атипичный трафик в сети? Есть ли новые узлы, сетевые службы?**
   - Появление новых сетевых устройств, служб, протоколов, а также новых **MAC-**адресов в сети?
   - Пропажа служб, ранее стабильно работавших?
   - Отслеживание атипичного поведения оборудования

4. **Как защитить сетевые узлы, на которых не установлен EDR-агент?**

GREYCORTEX Mendel

GREYCORTEX

1. **Это система обнаружения сетевых атак и анализа сетевого трафика:**
   - Анализ всех сетевых данных для визуализации и мониторинга коммуникаций, поиска угроз и атак, выявления атипичных коммуникаций и реагирования на них

2. **Визуализация сетевых комуникаций:**
   - Какие пользователи, с какими **IP**, **MAC**, **VLAN**, через какие приложения или службы и с кем общаются?
   - Мониторинг трафика всей корпоративной инфраструктуры, датацентров, **Wi-Fi** зон, **DMZ**, трафика переферийной и **IoT**-инфраструктур

3. **Выявление киберугроз:**
   - Сигнатурный анализ и глубокая инспекция трафика для обнаружения атак по известным типам угроз
   - **ИИ** и **Machine Learning** для обнаружения атипичного, подозрительного трафика, который не соответствует типовому профилю трафика сетевых узлов и приложений
   - Репутационные и корреляционный анализ позволяет оценить безопасность коммуникаций

4. **Реагирование на угрозы:**
   - Интеграция с **NGFW**, **SIEM**, **AD**, **NAC** позволяют заблокировать атаку в ручном или автоматическом режиме
   - Быстрая локализация проблем за счет детализации сетевых комуникация
   - Запись трафика события для дальнейшего анализ и хранения доказательной базы
   - Управление инцидентами

Как это работает?

GREYCORTEX

КАК?

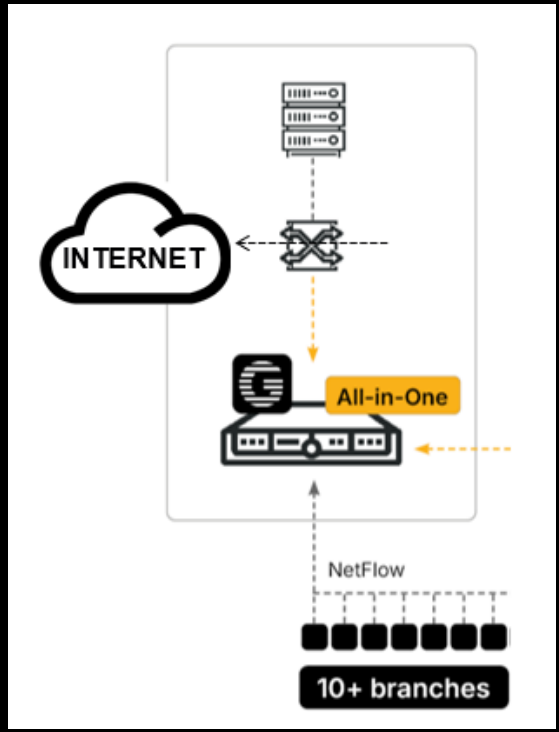
- **GreyCortex** разворачивается как виртуальный или физический сервер
- Выполнив настройки на коммутаторах ядра сети, на сервер **GreyCortex** направляется копия сетевого трафика
- Опционально, из удаленных локаций направляется **IPFIX, NetFlow, NSEL, NetStream**

ЗАЧЕМ?

- Все атаки распространяются и действуют в сети. Отслеживая сетевой трафик всегда можно найти характерные маркеры (сигнатуры) для известных атак, или атипичную для узла активность, в случае с неизвестными атаками
- Не на все утройства можно поставить **EDR**-агент. Некоторые типы атак распространяются через **IoT**-инфраструктуру, через незащищенные сегменты или через домашние устройства без **EDR**-агентов

ПРЕИМУЩЕСТВА?

- Обнаружение атак независимо от типа конечного устройства (**ПК**, сервер, принтер, видеонаблюдение, смартфоны и планшеты)....
- Независимо от наличия **EDR**-агента на конечном устройстве.
- Если зловред коммуницирует в сети – мы его зафиксируем тем или иными способом обнаружения



Привилегии под прицелом

- Одна из главных целей хакера — получить привилегированные учетные данные
- Аномальный трафик — это почти всегда скомпрометированные учетные данные
- Чтобы остановить его, нужно контролировать доступ к учётным данным

CYBERARK

Как управлять тысячами учетных записей (людей, сервисов, устройств) и гарантировать, что никто не превысит свои полномочия?

CyberArk (PAM) реализует **Zero Trust**, заменяя постоянные привилегии **Just-in-Time** доступом

CyberArk Identity Security Platform

Access Management	**Privileged Access**	**Endpoint Identity Security**
Secure Cloud Access	**Machine Identity Security**	

Что предоставляет CyberArk?

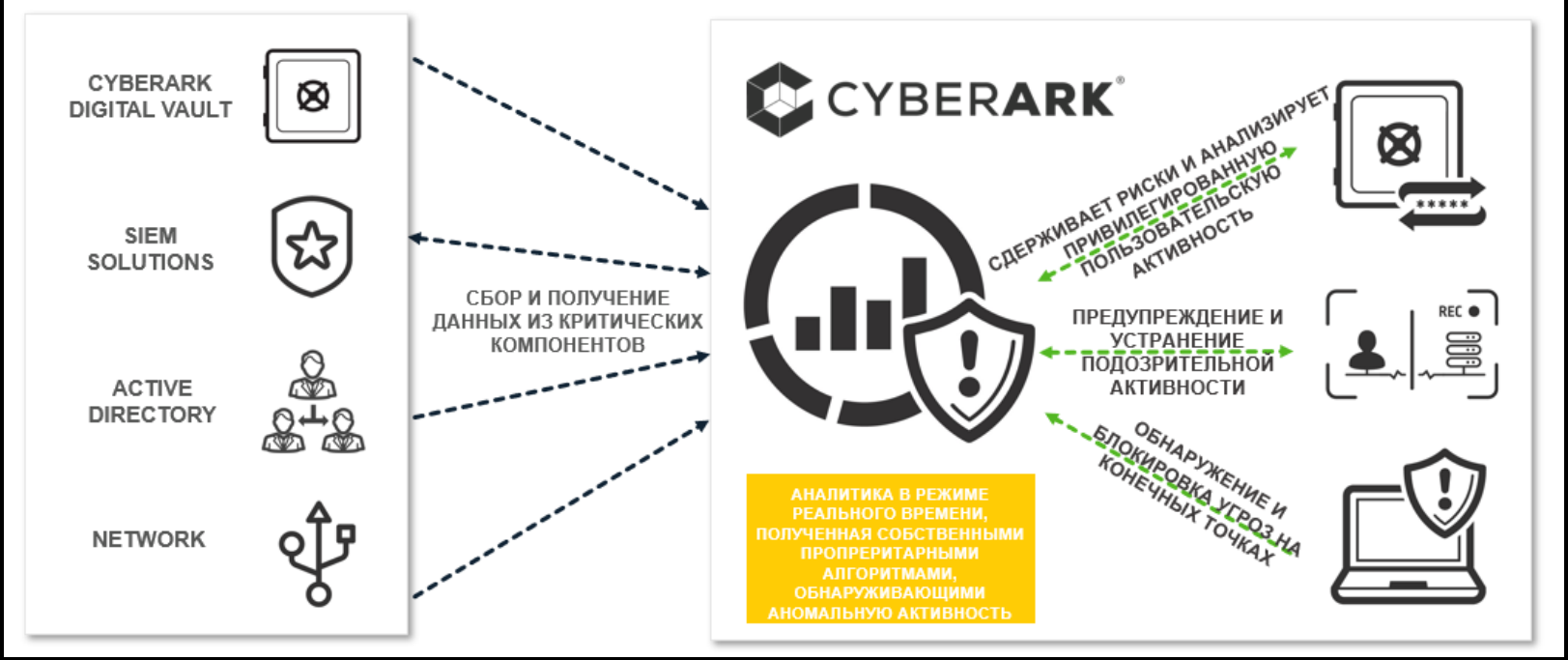
CYBERARK

1. Надежная аутентификация учетных записей всех типов
2. Высокий уровень безопасности привилегированного доступа
3. Полная видимость и анализ привилегированных сессий
4. Полный контроль персонала, обеспечение персональной ответственности
5. Надежное хранение паролей и независимость от человеческого фактора
6. Единая точка контроля привилегированного доступа к облачной среде, наземной, **SCADA**, сетевому оборудованию, бизнес-приложениям, среде разработки, доменной и не-доменной инфраструктуре
7. Надежная защита сервисных учеток с автоматической ротацией секретов
8. Полный контроль «третьих» лиц, подрядчиков и т.п. и уменьшение «площади атаки»
9. Удобная система лицензирования

Преимущества CyberArk?

1. **Комплексность:**
   - Возможность обеспечить безопасность всех типов привилегированных учетных данных решением от одного вендора
2. **Масштабируемость и надежность:**
   - Модульная архитектура решения позволяет внедрять **CyberArk** в крупных, распределенных инфраструктурах с обеспечением отказоустойчивости всех компонентов
3. **Удобство:**
   - Возможность автоматического обнаружения и контроля привилегированных учетных данных
4. **Универсальность:**
   - Наибольшее в отрасли число коннекторов к различным сторонним **ИТ/ИБ**-системам. Это дает возможность обеспечить безопасный и контролируемый доступ к любому приложению/сервису/устройству
5. **Полный контроль:**
   - Полноценная видеозапись и анализ всех сессий, независимо от используемых инструментов и протоколов
6. **Автоматизация:**
   - Возможность автоматического анализа сессий и их разрыва в случае обнаружения угроз

CyberArk – обнаружение угроз и аналитика



Угроза для цифровых активов

- Конечная цель любой атаки — это данные
- Утечка данных — это не просто инцидент...
- ... Это репутационный и финансовый удар...
- ... А также прямое нарушение **Закона РК «О персональных данных»**

Forcepoint

Как защитить то, что постоянно движется? Данные копируются, отправляются по почте, загружаются в облако....

Forcepoint (DLP) анализирует контекст и содержание данных, а не только тип файла. Он классифицирует, отслеживает и блокирует несанкционированную передачу по всем каналам — от почты до облаков

Forcepoint ONE

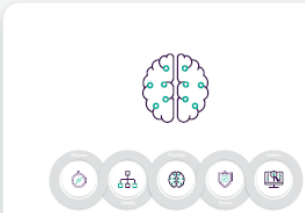
AI-Native DSPM	**Data Loss Prevention**	**Web Security**
Email Security	**NGFW**	**Data Detection & Response**

Forcepoint = Security.Simplified

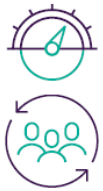
Forcepoint

Forcepoint

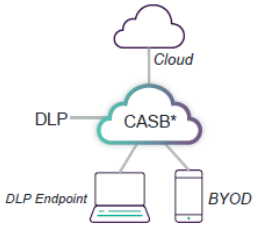
Security. Simplified.



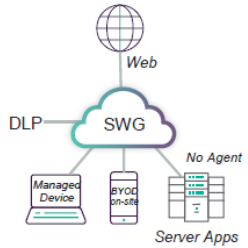
AI-powered discovery, classification, orchestration



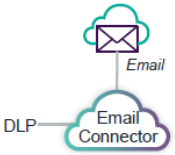
Risk-Adaptive Protection



Cloud Apps + Endpoint + BYOD



Web



Email

*Add ZTNA to replace VPNs for accessing private 'cloud' apps

Data Security Posture Management

Forcepoint

1. **DSPM (Data Security Posture Management):**

- Решение для **управления состоянием безопасности данных**, которое помогает организациям обнаруживать, классифицировать и приоритизировать меры по устранению рисков, связанных с конфиденциальными данными, по всей инфраструктуре

- **Обнаружение и классификация данных:** Решение автоматически идентифицирует и классифицирует конфиденциальную информацию, включая неструктурированные данные, с помощью технологий на базе искусственного интеллекта (**AI-powered Data Classification**)

- **Комплексный обзор: DSPM** обеспечивает полную видимость данных в различных хранилищах, как в локальных, так и в облачных средах, позволяя отслеживать, где хранятся данные, кто имеет к ним доступ и как они используются

- **Оценка и приоритизация рисков:** Инструмент непрерывно отслеживает политики безопасности, выявляет уязвимости и предоставляет оценку рисков в режиме реального времени, помогая сфокусироваться на наиболее критичных угрозах.

- **Автоматизация реагирования:** Оркестрация **Forcepoint DSPM** позволяет автоматизировать рабочие процессы реагирования на инциденты, связанные с управлением данными и соблюдением нормативных требований, минимизируя время простоя и повышая операционную эффективность

- **Соблюдение нормативных требований:** Решение помогает организациям обеспечивать соответствие нормативным требованиям безопасности данных, предоставляя необходимую информацию и контроль.

SOFTPROM

Мы предлагаем единую, эшелонированную архитектуру, где каждый элемент усиливает другой!

1

Barracuda Networks
Защищает **«входную дверь»** (веб-приложения и **API**)

2

GreyCortex
Обеспечивает сквозную видимость сети

3

CyberArk
Контролирует и управляет доступом

4

Forcepoint
Обеспечивает защиту информации

SOFTPROM

Рады будем продолжить на нашем стенде!

Softprom
Let’s talk!

kazakhstan@softprom.com
www.softprom.com