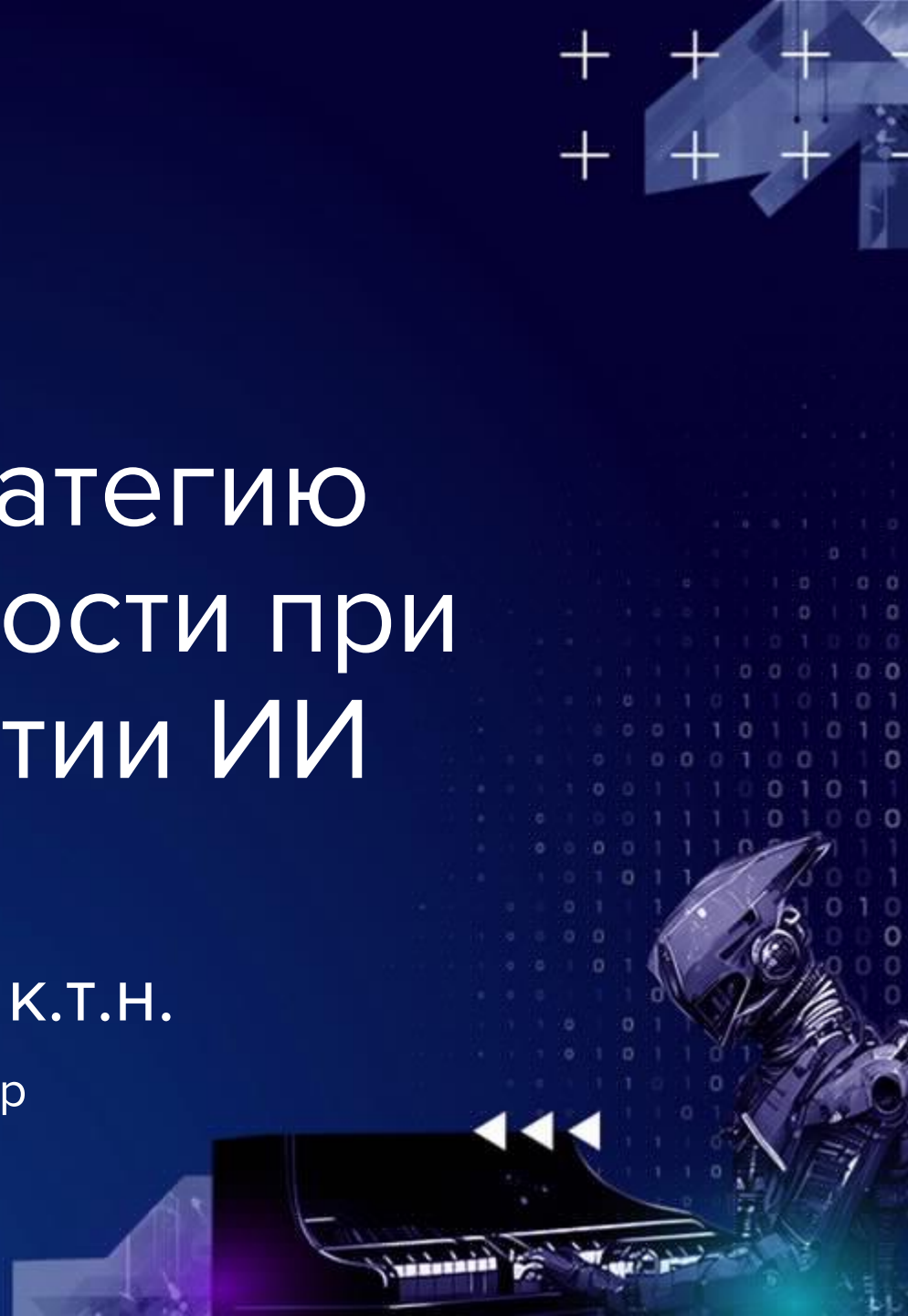
GIS DAYS

Взгляд на стратегию кибербезопасности при бурном развитии ИИ

Василий Широков, к.т.н.

Операционный директор

Check Point (Russia)



2023 СТАЛ ГОДОМ ИИ

Более половины жителей России (58%) готовы использовать технологии на основе искусственного интеллекта при управлении финансами (Газпромбанк).

Искусственный интеллект помог столичным терапевтам поставить более 10 миллионов диагнозов (Сергей Собянин).

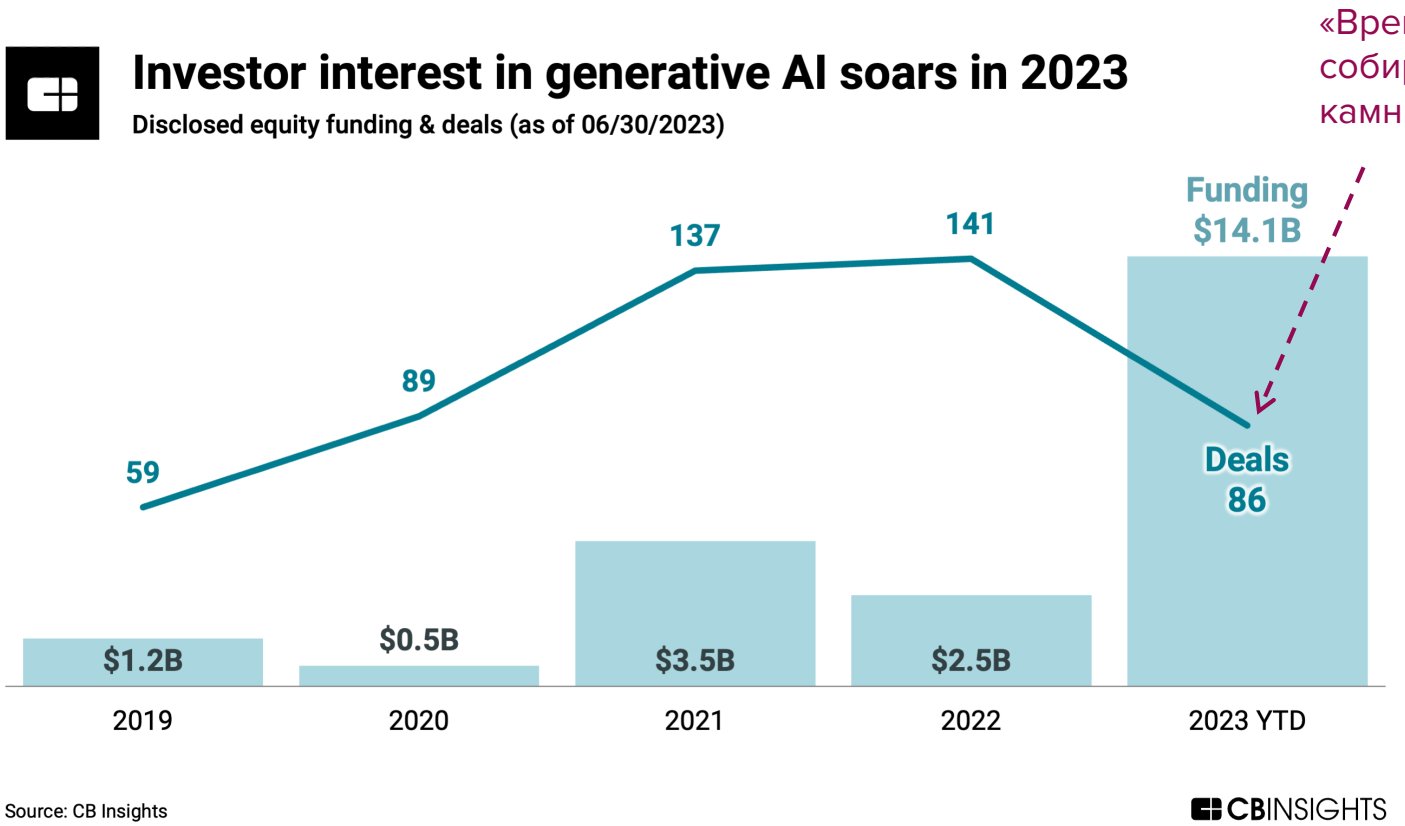
Уже сегодня порядка 40 сервисов искусственного интеллекта помогают рентгенологам по 17 направлениям исследований. (ТАСС)

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Быстрое появление генеративного ИИ

(технологий ИИ, которые генерируют новый контент от строк кода до изображений, музыки и человеческой речи)

вызвало неистовый ажиотаж среди стартапов и инвесторов.



*) Генеративный ИИ основан на моделях машинного обучения

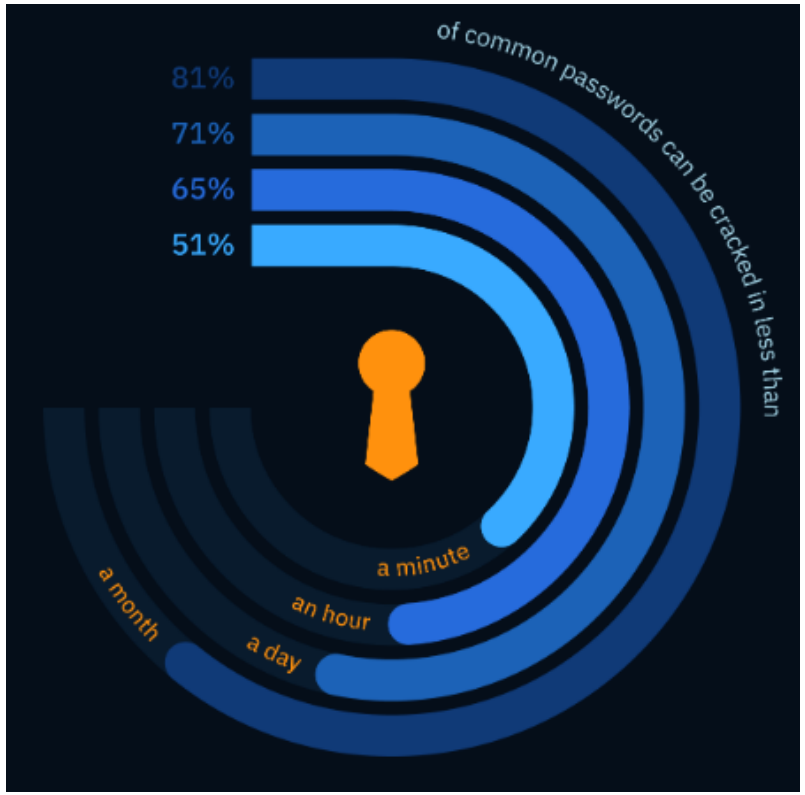
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Да, действительно, ИИ стал нашим помощником во многом.
А также стал новым занятным развлечением.

Но если вы думаете, что ИИ будет обыгрывать вас только в шахматы, вы глубоко ошибаетесь.

Все новые технологии рано или поздно приходят и на темную сторону.

ПОТЕНЦИАЛ ИИ

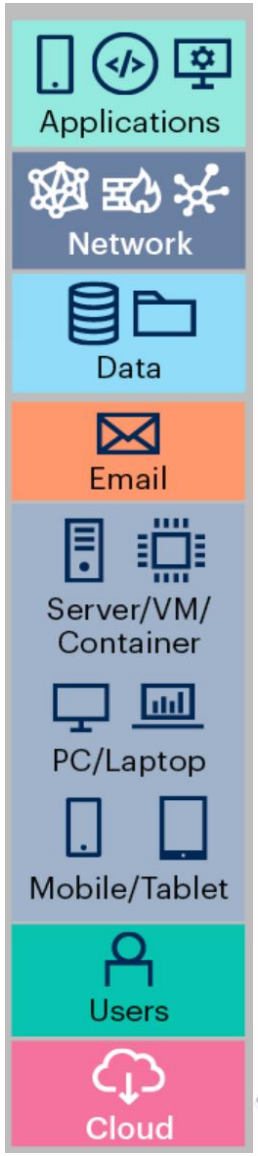


*) Исследование HSH

Time It Takes Using AI to Crack Your Password [2023]

# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ



... то мы поймем, что задача поиска лазеек и уязвимостей в вашей такой сложной и многоуровневой системе с размытыми и не всегда явными периматрами защиты как раз является большим преимуществом для ... ИИ на темной стороне.

И бороться с этим можно и нужно с использованием того, что пока еще непосильно ИИ.

Автономное мышление .....

А значит ... СТРАТЕГИЯ и СИСТЕМНОСТЬ.

СИСТЕМА – ЭТО ВАЖНО

Классическое определение системы звучит как:

Система представляет из себя набор функциональных элементов и взаимосвязей между ними.

При этом ключевой составляющей системы являются именно наличие взаимосвязей, которые придают системе уникальные свойства, отсутствующие у любого функционального элемента этой системы.

Нейронная система.

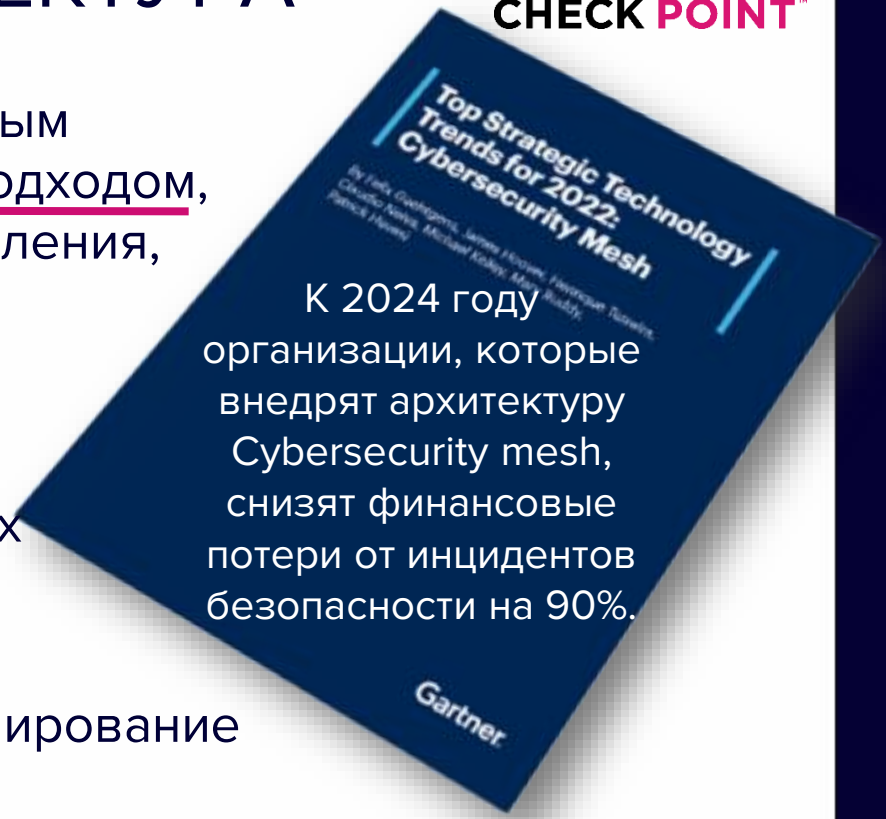
Электрический выключатель.

Таким образом, если вы используете многофункциональные МЭ, это всего лишь звенья в сложной и многогранной системе обеспечения ИБ.

И важным фактором эффективности этой системы является наличие связей с другими элементами системы.

CYBERSECURITY MESH АРХИТЕКТУРА

Cybersecurity mesh architecture(CSMA) является новым комплексным и масштабируемым архитектурным подходом, реализующим стратегию централизованного управления, контроля состояния и реагирования на инциденты безопасности в мире распределенных ИТ активов.



К 2024 году организации, которые внедрят архитектуру Cybersecurity mesh, снизят финансовые потери от инцидентов безопасности на 90%.

Архитектура CSMA является эволюционной и рассматривает в комплексе несколько целей, таких как ...

единое управление и обеспечение доверия распределенными цифровыми активам и функционирование в качестве единой системы кибербезопасности;

реализация архитектуры zero-trust;

построение решений, обеспечивающих превентивные действия против процессов, нарушающих безопасность;

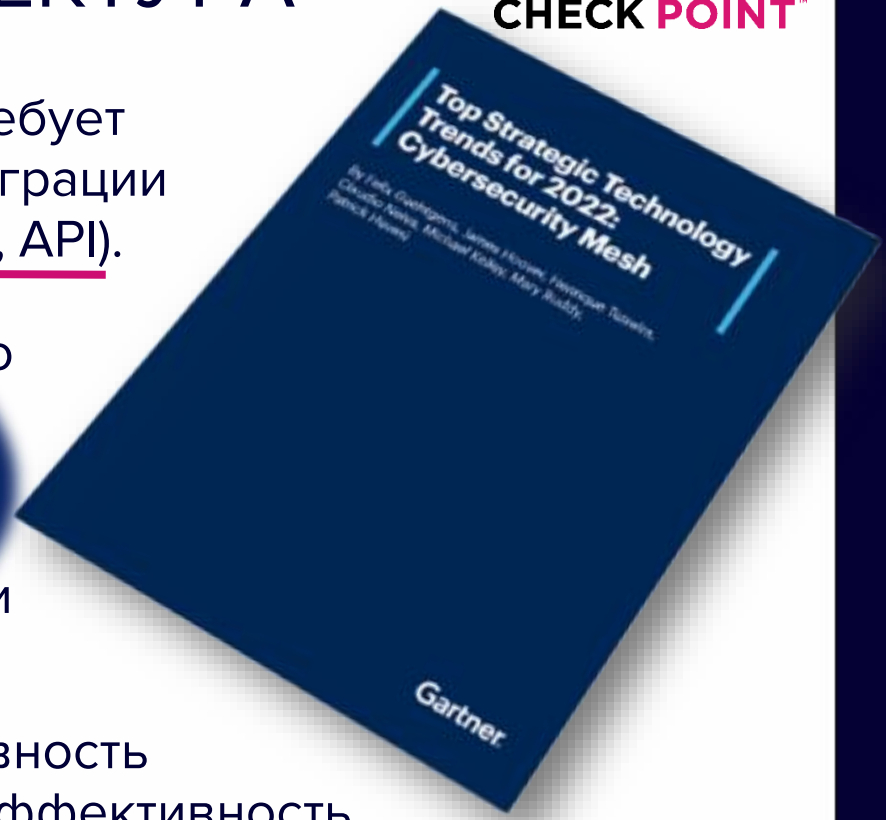
сокращение административных накладных расходов.

CYBERSECURITY MESH АРХИТЕКТУРА

Интеграция распределенных цифровых активов требует более глубокой и более стандартизированной интеграции между отдельными инструментами (стандартизация, API).

Ключевым аспе[illegible]что он не диктует[illegible] позволяет в[illegible] одного поста[illegible] набор груп ре[illegible]ими надстройками и вс[illegible]

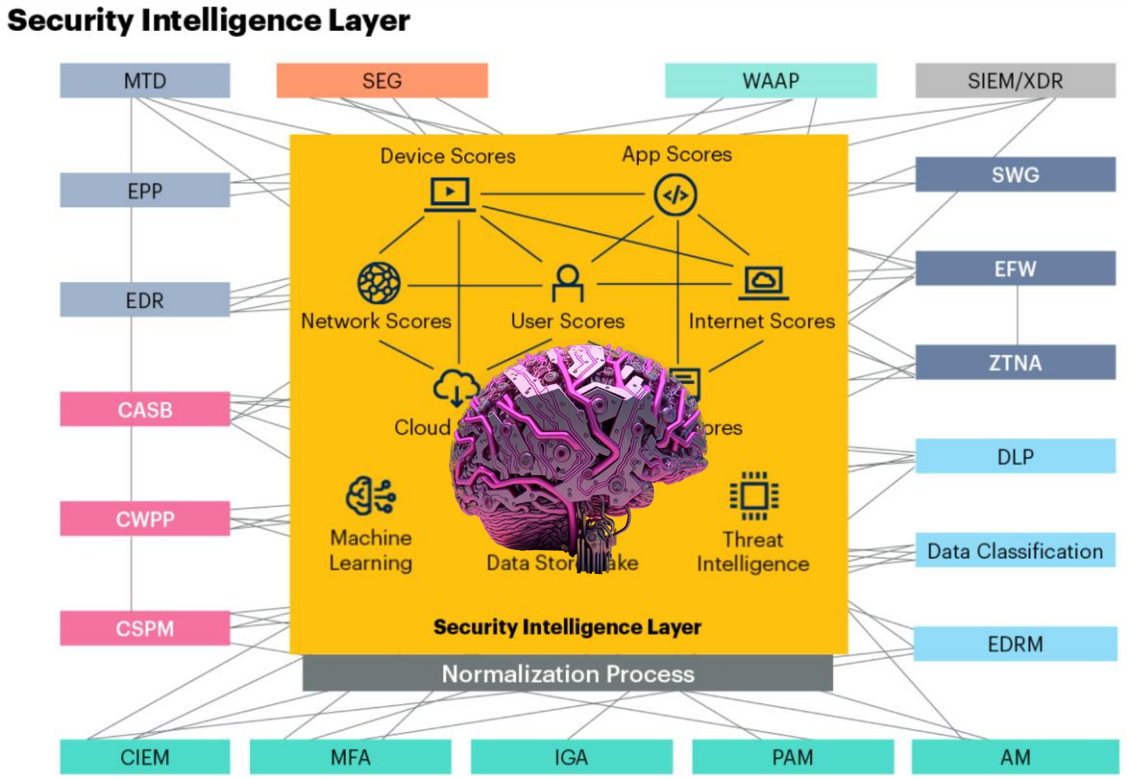
... и весь этот CyberJazz



Что будем иметь: радикально улучшенная оперативность развертывания систем защиты и идентификации, эффективность реагирования и глобальный контроль состояния безопасности.

Как это реализовать: Вместо того, чтобы каждый инструмент безопасности работал изолированно, CSMA предполагает взаимодействие этих инструментов через несколько объединяющих уровней.

АРХИТЕКТУРА CSMA - УРОВНИ УПРАВЛЕНИЯ



Source: Gartner
754315_C

Gartner

Аналитика и расследование

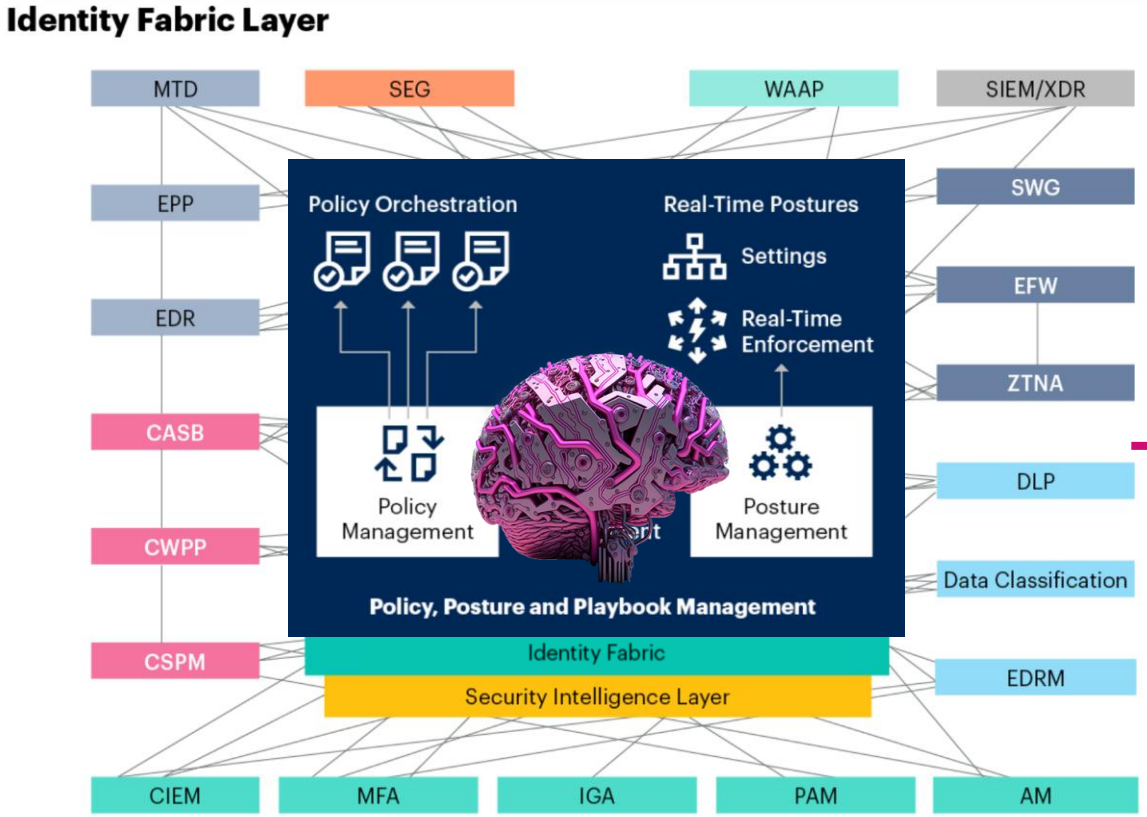
Этот слой является эволюцией того, что делают системы SIEM, SOAR, UEBA и XDR сегодня.

Архитектура CSMA требует реализации аналитики более высокого уровня, оценок рисков, контроля состояния безопасности, своевременного реагирования и превентивных действий .

Это предполагает унифицированные интерфейсы взаимодействия и оперативные реакций на события (желательно) без ручного вмешательства.

... Что с очевидностью приводит к требованию наличия ....

АРХИТЕКТУРА CSMA - УРОВНИ УПРАВЛЕНИЯ



Идентификационная фабрика

Концепция идентификационной фабрики — это распределенная платформа идентификации, которая поддерживает все общие функции управления идентификацией и доступом (IAM).

Управление политиками и настройками

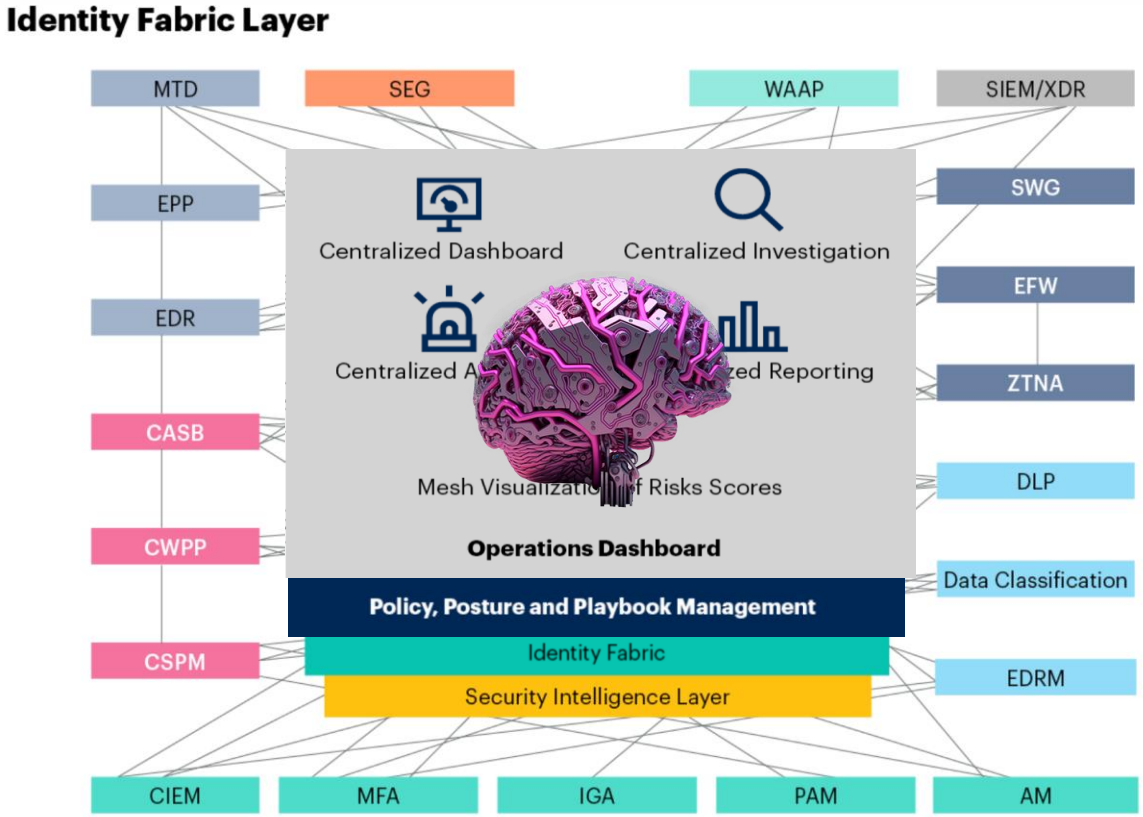
Одной из самых больших проблем в безопасности - многочисленные и сложные политики, настройки устройств и мониторинг соответствия требованиям безопасности и лучшим практикам. Этот уровень является ключевым для решения этих проблем.

SIEM (security information and event management)
SOAR (security orchestration, automation and response)
XDR (extended detection and response)

Gartner

CASB (cloud access security broker)
CSPM (cloud security posture management)
CIEM (cloud infrastructure entitlement management)

АРХИТЕКТУРА CSMA - УРОВНИ УПРАВЛЕНИЯ



Source: Gartner
754315_C

Единая операционная панель

Работает в режиме реального времени, основана на сетке динамической оценки рисков, должна быть основой для понимания существующих рисков безопасности и прогноза возможных предстоящих атак.

Имеет общие функции с текущими инструментами SIEM, SOAR и XDR.

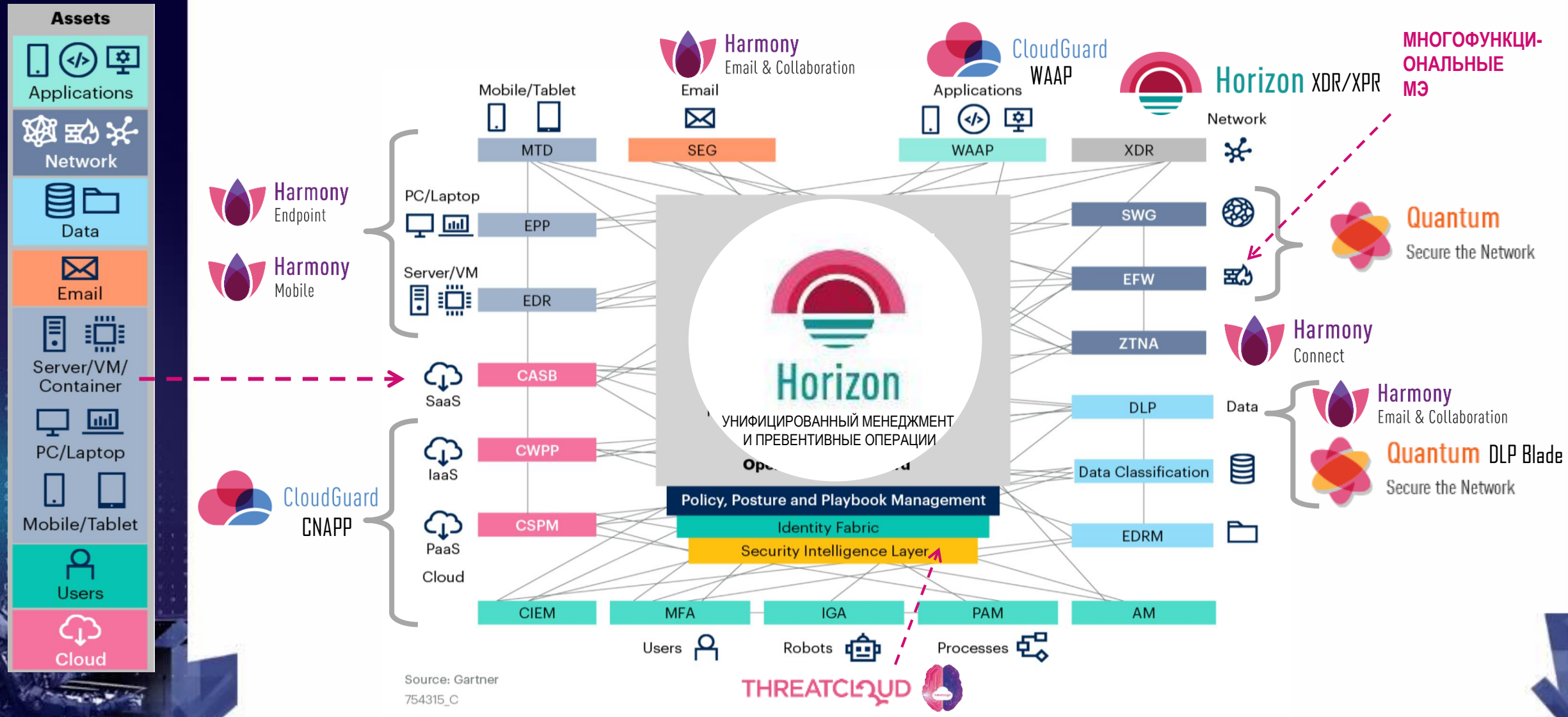
Но единая глобальная панель и динамическая визуализация сетки оценки рисков являются ключевыми функциями, которые отсутствуют в текущих продуктах безопасности.

Gartner

SIEM (security information and event management)
SOAR (security orchestration, automation and response)
XDR (extended detection and response)

CASB (cloud access security broker)
CSPM (cloud security posture management)
CIEM (cloud infrastructure entitlement management)

АРХИТЕКТУРА CSMA – КОНСОЛИДАЦИЯ ЭЛЕМЕНТОВ



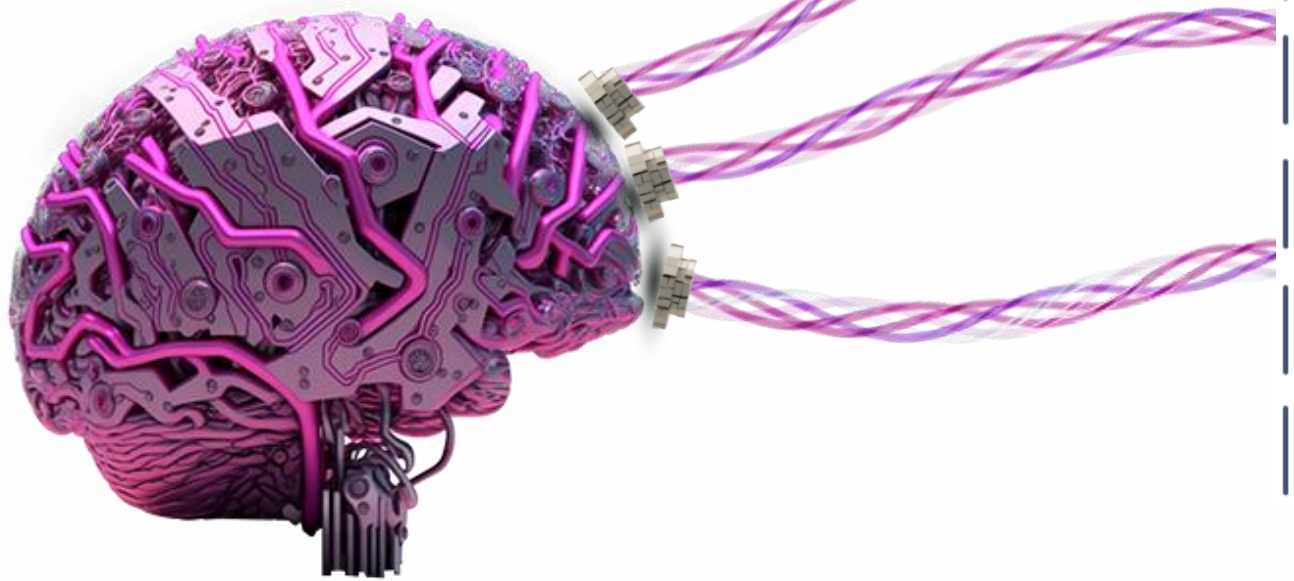
ПОЛНАЯ ЗАЩИТА

NEW

- Zero Phishing
- DNS Security
- Macros
- XPR-UEBA
- DGA

40 ИИ кибер-движков

+12 ИИ к концу 2023 года



Аналитика угроз с использованием ИИ:

2,000,000,000
Websites and files inspected

73,000,000
Full content emails

30,000,000
File emulations

20,000,000
Potential IoT devices

2,000,000
Malicious indicators

1,500,000
Newly installed mobile apps

1,000,000
Online web forms

Ежедневно!

30 ЛЕТ ВМЕСТЕ С ВАМИ

5 ИЮЛЯ 2023 ГОДА:

30 СЛОЁВ ОПЫТА В КИБЕРБЕЗОПАСНОСТИ
(Тель-Авив, штаб-квартира Check Point)

CHECK POINT SECURITY GATEWAYS: СЕРТИФИКАТ ФСТЭК (МЭ, СОВ) ПО УРОВНЮ ДОВЕРИЯ 4
СЕРТИФИКАТ ФСТЭК (МЭ, СОВ, САВЗ) ПО УРОВНЮ ДОВЕРИЯ 6

GIS DAYS

CHECK POINT™

А ПРИМЕНЯЕМЫЕ ВАМИ

МНОГОФУНКЦИОНАЛЬНЫЕ МЭ

ГОТОВЫ К ЦИФРОВЫМ ВЫЗОВАМ ВРЕМЕНИ?

GIS DAYS

СПАСИБО ЗА ВНИМАНИЕ!

Ваш В. Широков

www.checkpoint.com

CHECK POINT™