KSD 2022
Kaspersky Security Day

На пути реализации новой стратегии

Экосистема ИБ на принципах нулевого доверия

Дмитрий Кудревич
Региональный представитель
Kaspersky в Беларуси

kaspersky 25 лет

Актуальные проблемы

Мультивекторные атаки (APT) стали массовыми

Источники:

- Аналитические данные «Лаборатории Касперского»
- ENISA Threat Landscape 2021

Критическая нехватка квалифицированных кадров ИБ

- 3 млн специалистов требуется рынку
- 64% организаций сталкиваются с нехваткой квалифицированных кадров

Бюджеты ИБ оптимизируются и консолидируются вокруг крупных платформенных вендоров

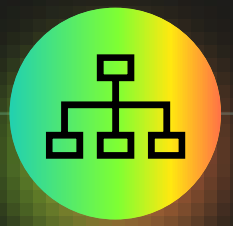
Gartner: к 2025 году 70% бюджетов организаций будет сконсолидировано вокруг крупнейших вендоров

Стратегические цели развития портфеля Kaspersky

Создать **экосистему безопасности** для всех целевых аудиторий

Обеспечить защиту от всех возможных **векторов кибератак**

Как мы достигаем стратегических целей



Полнота экосистемы

Покрывает все ИБ-сценарии поверх всей корпоративной инфраструктуры

Зрелая XDR-платформа

Открытость, обеспечение процесса реагирования (IRP workflow), ML, автоматизация

Zero Trust

Обеспечение подхода «нулевого доверия» для всей инфраструктуры, с управлением из единой XDR-платформы

● Работает ● В разработке планируется интеграция или M&A

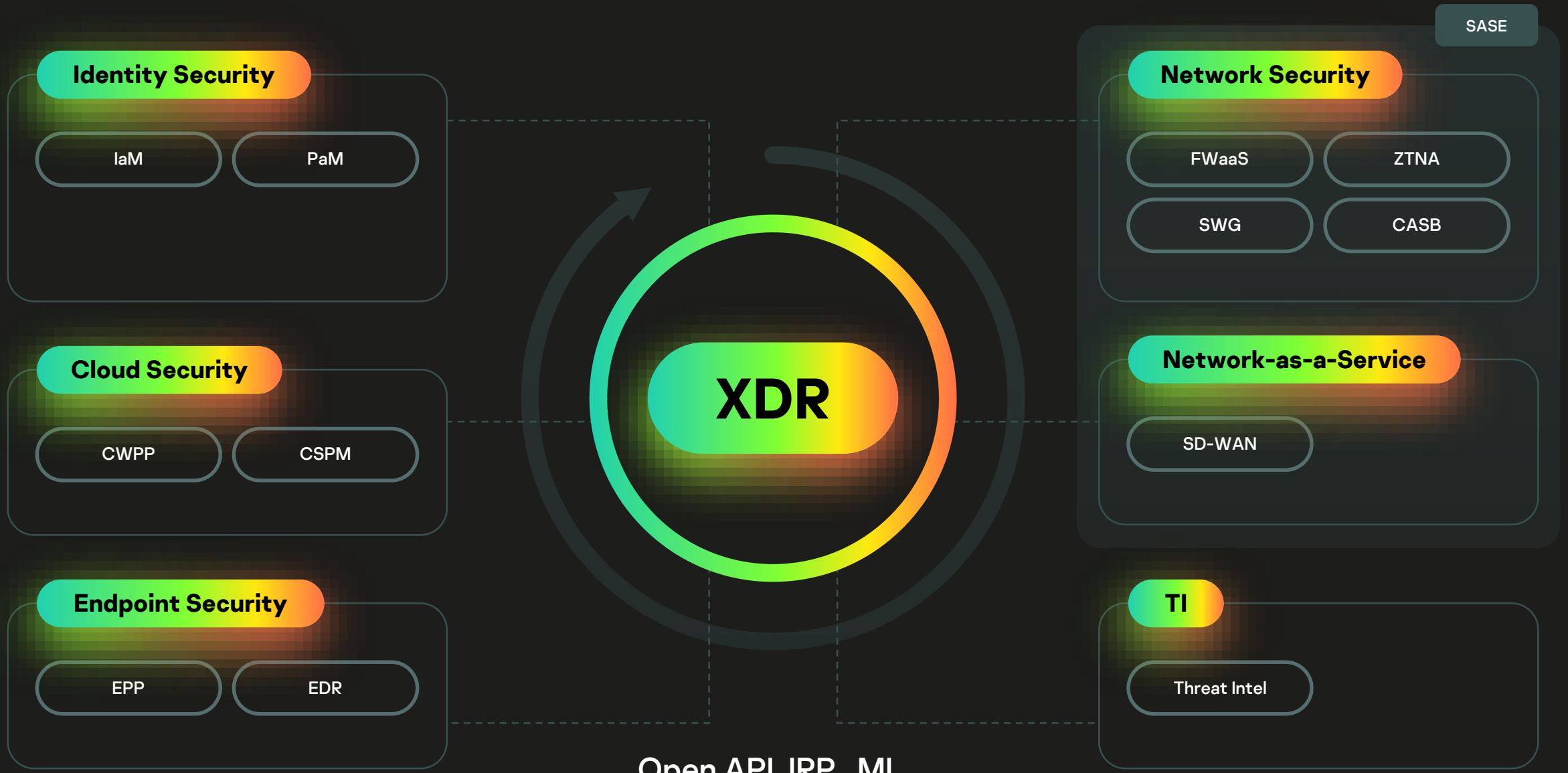
Сценарии безопасности

Ресурсы	Предотвращение	Детектирование	Расследование	Реагирование	Управление конфигурациями, hardening
Endpoints	KESB	KESB and KEDR	KEDR	KEDR	KESB and KSC
Servers	KESB and KHCS	KESB, KHCS, KEDR	KEDR	KEDR	KHCS, KESB, and KSC
AD / Identity	PaM / IaM	KEDR+ Identity scenarios	IaM	IaM	IaM
VMs	KHCS	KHCS and KEDR	KEDR	KEDR	CSPM
IaaS	KHCS	KHCS and KEDR	KEDR	KEDR	CSPM
Containers	KHCS	Container Security	Container Security	Container Security	CSPM
Mobile	KESB	KESB	Mobile EDR	Mobile EDR	KSC MDM
ICS	KICS4Nodes	KICS4Nodes	KICS4Nodes	KICS4Nodes + ICS EDR	
IoT	KESS	IoT EDR / NDR	IoT EDR / NDR	IoT EDR / NDR	IoT patch management
Network	NGFW	KATA Network	KATA Network	KATA Network	NCCM
SaaS / Business apps	KES and O365	CASB, WAF	CASB, WAF	CASB	CASB
Mail and Web	KLMS and KWTS	KLMS and KWTS	KATA Network	KLMS and KWTS	
Data	DLP in Kaspersky products	DAP	DAP		DAP

Наша стратегия — полное покрытие всех сценариев безопасности для всех устройств, пользователей, сетей и данных

Как обеспечиваем полноту: собственная продуктовая разработка, через интеграции с другими решениями, M&A

Зрелая XDR платформа



Zero Trust architecture

«Никогда не доверяй, всегда проверяй»: устройства и пользователи не являются доверенными по умолчанию, даже если они подключены к управляемой корпоративной сети

Доступ к каждому ресурсу в инфраструктуре клиента полностью контролируется и разрешается или запрещается в соответствии с политиками

Zero Trust это критически важная модель безопасности, которая приближает защищаемую организацию к киберимунности!

Злоумышленники жестко ограничены в передвижении внутри инфраструктуры, так как несанкционированные действия запрещены

Ключевые аспекты KasperskyOS

Собственное микроядро

Ключевой архитектурный компонент KasperskyOS, обеспечивающий надежность и прозрачность системы.

Kaspersky Security System

Гибкая конфигурация политик безопасности и бескомпромиссный контроль межпроцессных взаимодействий.

Поддержка MILS, FLASK

KSS основывается на классических концепциях информационной безопасности: архитектурах MILS (Multiple Independent Levels of Security) и FLASK (Flux Advanced Security Kernel).

Кибериммунитет – методология, позволяющая создавать ИТ-системы, которые могут исполнять свои функции в условиях агрессивной среды без дополнительных (наложенных) средств безопасности

Компоненты, необходимые для реализации подхода нулевого доверия

Identity management	Asset management	Data security management	Telemetry from all assets and users	Threat intelligence	Policy engine within XDR platform	Policy enforcement points
Инвентаризация и контроль пользовательских учёток и привилегий	Инвентаризация и контроль устройств	Мониторинг, анализ, защита корпоративных данных	Телеметрия со всех устройств и пользователей, скоррелированная с базами знаний об угрозах – позволяет определить уровень риска при операциях		Принимает решение по каждому запросу на авторизацию и на доступ к ресурсам	Исполняет решение о блокировке доступа или разрешении доступа

Based on Zero Trust architecture public researches, including NIST and Gartner

XDR-платформа с Zero Trust

Минимизирует количество инцидентов и позволяет снизить нагрузку на команды ИБ

- Identity Security
- Cloud Security
- Endpoint Security

SASE

- Network Security
- Network-as-a-Service
- Threat Intelligence

- Identity management
- Asset management
- Data security management
- Telemetry from all assets and users
- Threat intelligence
- Policy engine within XDR platform
- Policy enforcement points

Дорожная карта

Продукты 2022

- Kaspersky Symphony:
  - SIEM
  - EDR
  - KATA
  - Mail, Web GW
  - TI Platform
- KICS:
  - EDR
  - Oval
- Threat Intelligence:
  - DFI
  - Takedown
  - Ask the Analyst
- SD-WAN

Фокус в 2022-2023

- Полный портфель интеграций со сторонними решениями
- Полноценная экосистема управляемая из зрелой XDR-платформы: IRP-функционал, открытость, автоматизация

Возможности 2023-2025

- SASE (SD-WAN и функции безопасности)
- Cloud & Network products:
  - CASB
  - NGFW
  - ZTNA
- Экосистема на принципах нулевого доверия

Каждый имеет право чувствовать себя в безопасности.

Евгений Касперский

KSD 2022

Kaspersky Security Day

Спасибо!

kaspersky 25 лет