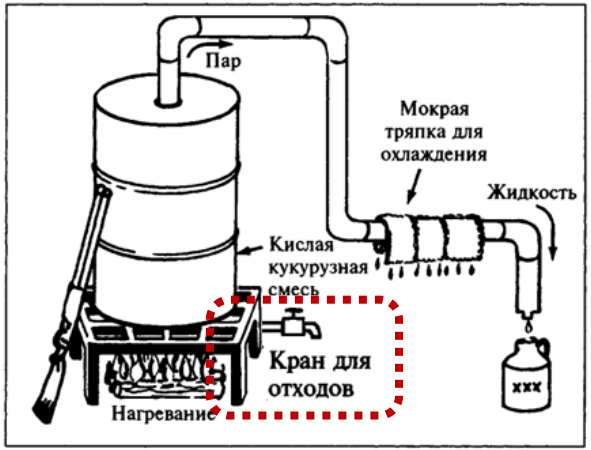
Как обеспечить понятные результаты от цифровизации и управлять новейшими киберрисками IIoT-проектов

Андрей Суворов, CEO
НПО «Адаптивные Промышленные Технологии» (АПРОТЕХ),
дочерняя компания «Лаборатории Касперского»

kaspersky

Вместо эпиграфа



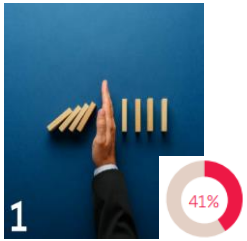
«В настоящее время 85% промышленных активов остаются неподключенными»

Источник: WEF – Technology and Innovation for the Future of Production: Accelerating Value Creation

Часть 1

Что наши начальники знают про киберриски, когда обсуждают цифровую трансформацию предприятия?

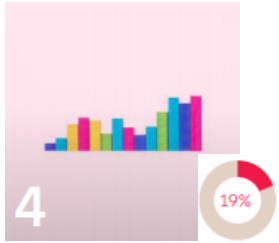
Топ-10 бизнес-рисков 2021: новые приоритеты



2020: 37,2% (2)
Нарушение непрерывности бизнеса

2020: 3% (17)
Вспышка пандемии

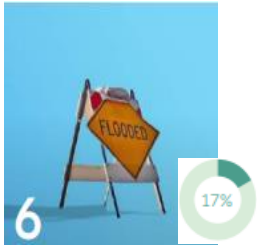
2020: 39% (1)
Киберинциденты



2020: 21 % (5)
Рыночные риски

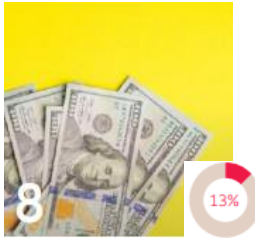
2020: 27% (3)
Изменения в законодательстве и регулировании

2013 - 13



2020: 21% (4)
Природные катаклизмы

2020: 20 % (6)
Пожары, взрывы



2020: 11% (10)
Изменения в макроэкономике

2020: 17 % (7)
Изменение климата/ возрастающая изменчивость погоды

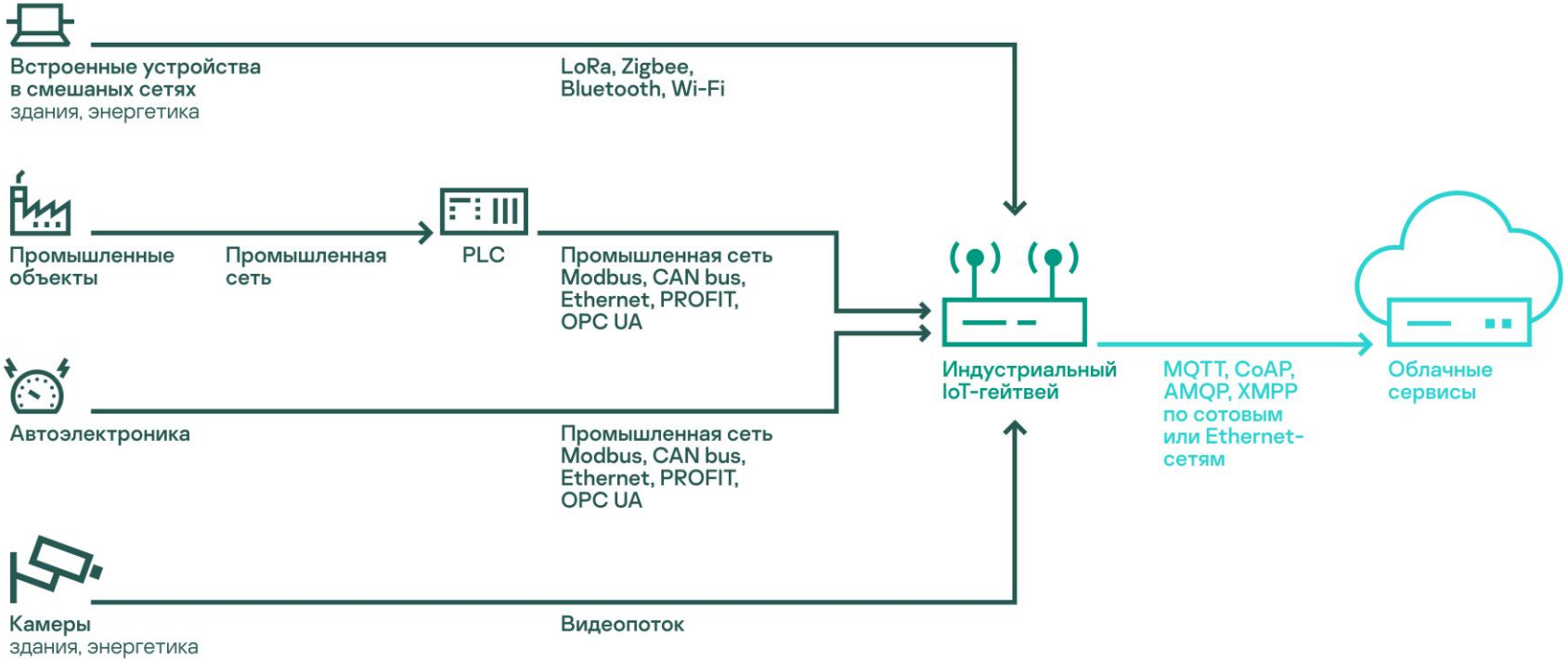
2020: 9% (11)
Политические риски и насилие

Источник: Allianz Risk Barometer | AGCS

Интернет вещей

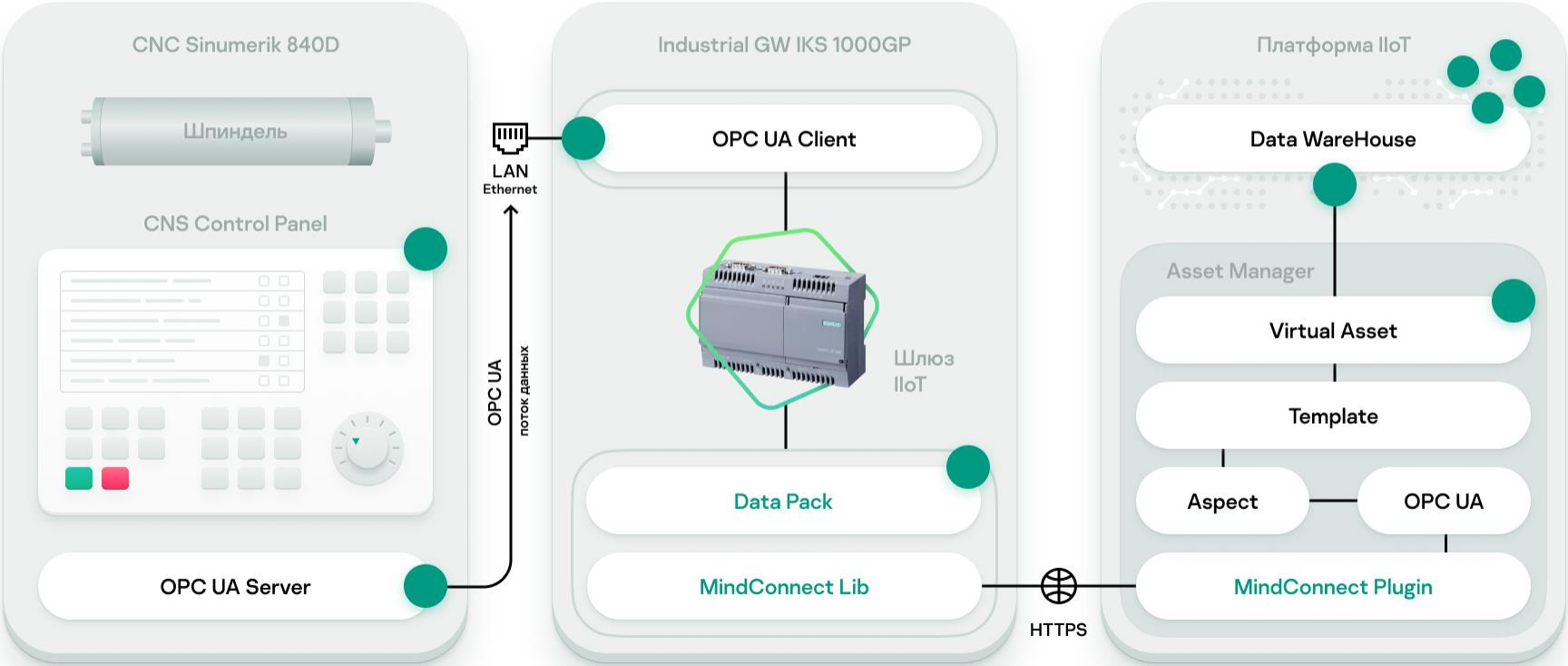
Архитектура усложняется по сравнению с традиционными системами

Что такое IoT-гейтвей?



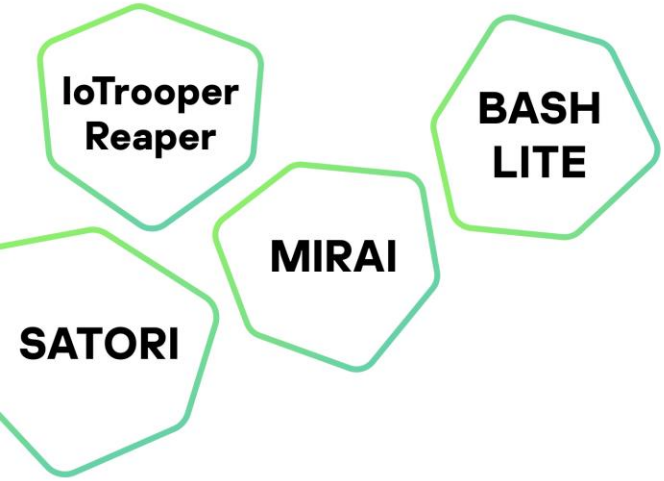
Как это выглядит в цеху

Ex. Конвертировать
«скорость шпинделя»
в финансовый показатель

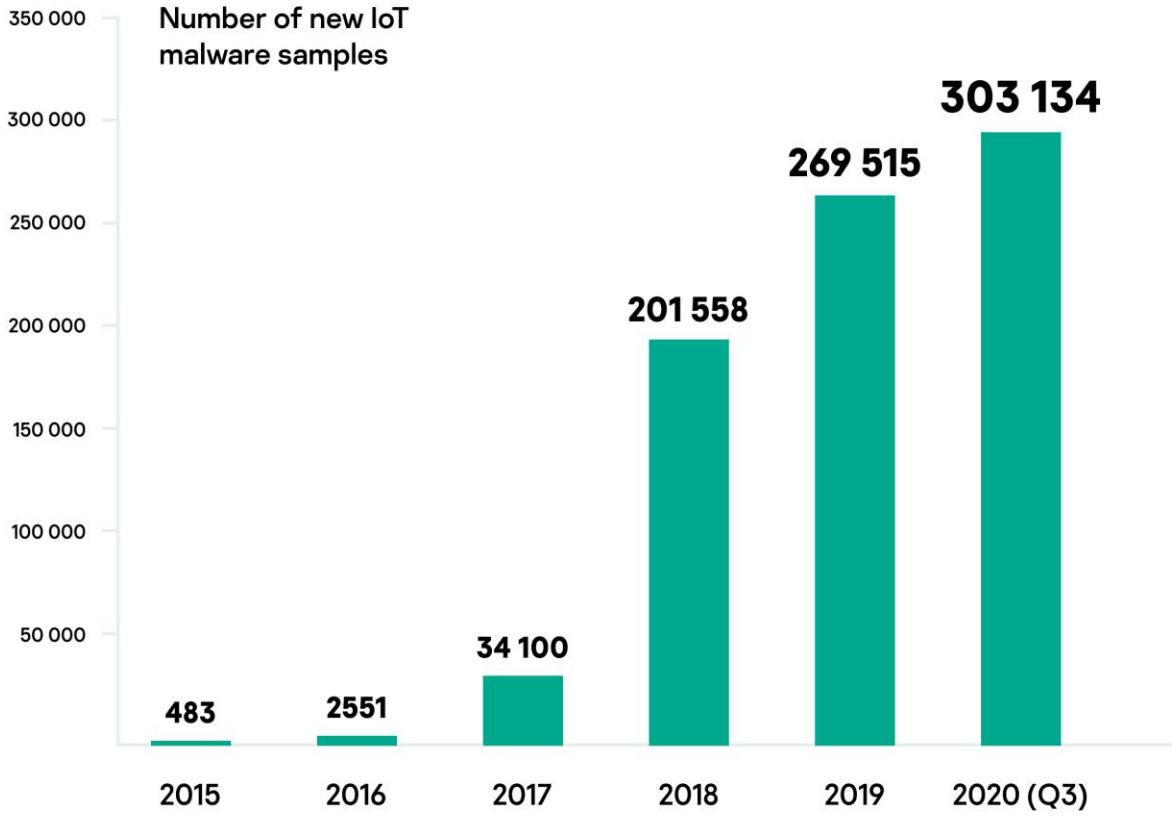


Интернет угроз

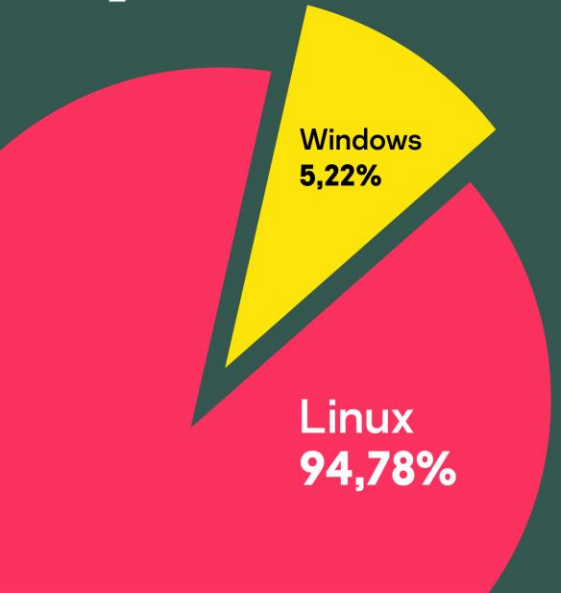
Статистика по урозам



Источник: «Лаборатория Касперского»



9 из 10 атак на устройства IoT эксплуатируют уязвимости в Linux



Соотношение атак устройств (ботнетов)

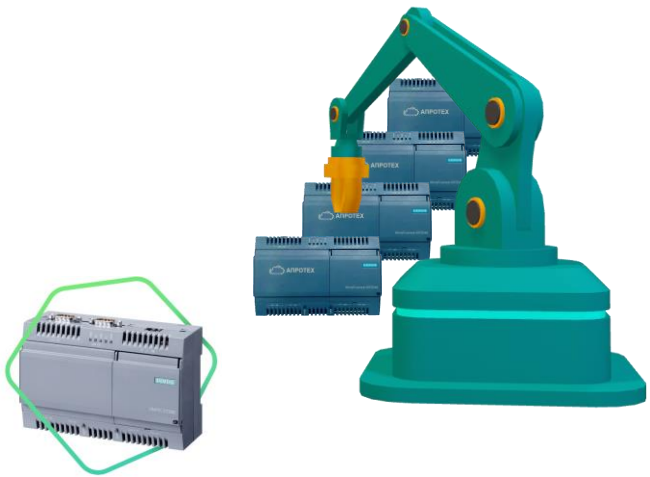
Топ-10 зловредов, загружаемых на зараженное IoT-устройство в результате успешной атаки

2020 (Q2)

	%	
1	37.78	Trojan-Downloader.Linux.NyaDrop.b
2	17,47	Backdoor.Linux.Mirai.b
3	12,72	HEUR:Backdoor.Linux.Mirai.b
4	9,76	HEUR:Backdoor.Linux.Gafgyt.a
5	7,99	Backdoor.Linux.Mirai.ba
6	4,49	HEUR:Backdoor.Linux.Mirai.ba
7	2,23	Backdoor.Linux.Gafgyt.bj
8	1,66	HEUR:Trojan-Downloader.Shell.Agent.p
9	1,26	Backdoor.Linux.Mirai.cn
10	0,73	HEUR:Backdoor.Linux.Mirai.c

Часть вторая. Кибериммунная

Как управлять возросшими киберрисками при трансформации бизнеса?



Традиционный подход не работает в IIoT

РЕАЛЬНОСТЬ

No patching
No antivirus
Уязвимости

Размеры
Количество
Связи

РИСКИ

Подмена данных

Доступ к активам

Неплановые остановки

СЕГОДНЯ

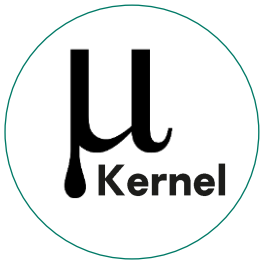
Форум: Технологии Безопасности

ЗАВТРА

Форум: Технологии Кибериммунитета

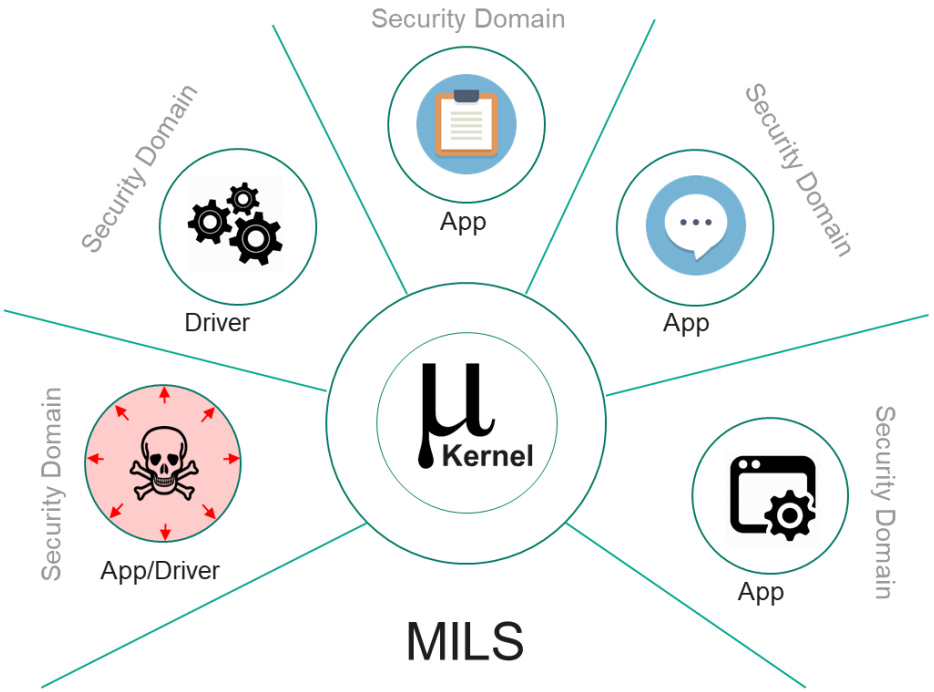
Microkernel

- Безопасная система должна **доверять** чему-то или кому-то
- В ИБ этот тезис был обоснован в терминах **TCB** (Trusted Computing Base)
  - John Rushby (Trusted Computing Base), “Design and Verification of Secure Systems”, 1981
- **TCB** должна быть простой и небольшой по размеру, насколько возможно



Microkernel (микроядро) как основа архитектуры ОС, удовлетворяющей этим требованиям

MILS (Multiple Independent Levels of Security)



Принципы MILS:

1. **Изоляция памяти и ресурсов CPU**
2. **Управление потоками данных между изолированными доменами**
3. **Свойства NEAT**

.

MILS обеспечивает достижение целей безопасности за счет изоляции доменов друг от друга, даже если:

- компоненты могут иметь уязвимости;
- компоненты могут иметь незадекларированные возможности;
- компоненты могут содержать вредоносный код.

FLASK (FLux Advanced Security Kernel)

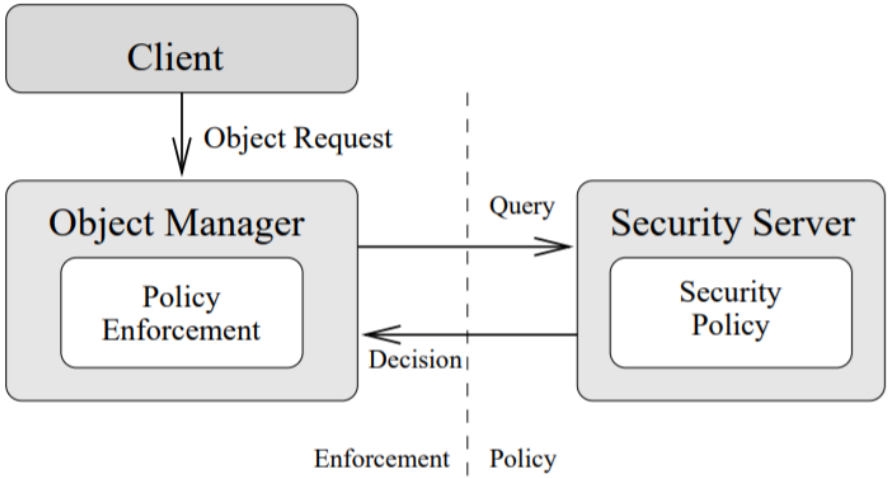
В современных системах присутствуют:

- политики безопасности, описанные разными языками и правилами;
- разрозненные точки принятия решений

«Security Policy Hell»

Никто не понимает, какая политика безопасности реально применяется к системе

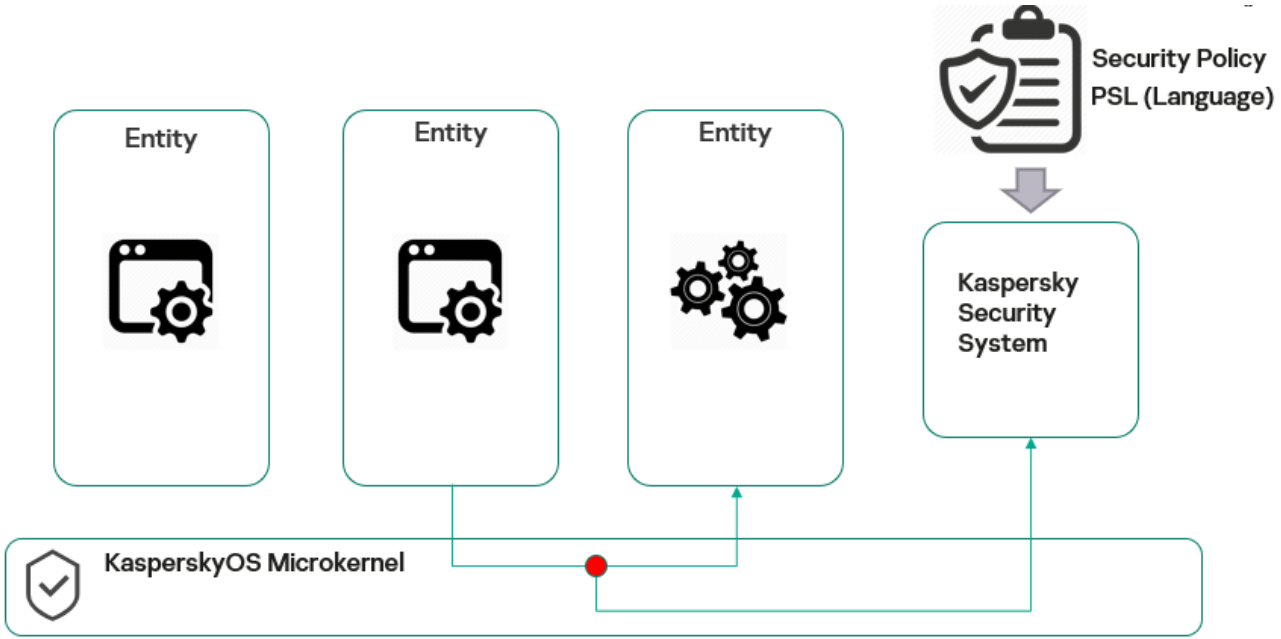
FLASK определяет подход с политиками безопасности



Принципы FLASK:

1. **Выделение** подсистемы формирования политик безопасности
2. **Единая точка** контроля политик безопасности для повышения эффективности и прозрачности всей системы

KasperskyOS: все три концепции в одной ОС



KaperskyOS : from cybersecurity to cyberimmunity

卡巴斯基操作系统：从网络安全到网络免疫

KasperskyOS

- Приоритетное направление развития компании
- Стратегия голубого океана – у нас нет конкурентов
- Многолетние разработки и многомиллионные инвестиции
- Прицел на глобальный рынок

Узнать больше: https://kas.pr/jgi8

Что такое кибериммунитет?

Кибериммунная система неуязвима для атак

KasperskyOS автоматически сделает мои решения неуязвимыми

Что такое кибериммунитет?

~~Кибериммунная система неуязвима для атак~~

~~KasperskyOS автоматически сделает мои решения неуязвимыми~~

Что такое кибериммунитет?

Подавляющее большинство типов кибератак на кибериммунную систему неэффективно

Потому что она разработана по определенной методологии

Встречайте первые решения

АПРОТЕХ
IKS 1000GP β*

Kaspersky IoT
Secure Gateway β*

Уже есть шлюзы с повышенной устойчивостью к киберинцидентам

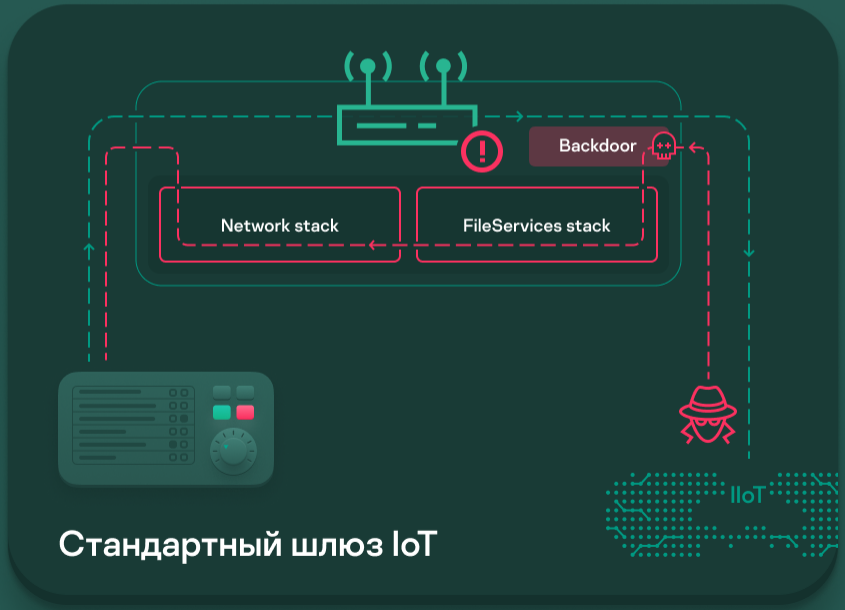
MindSphere

OPC UA

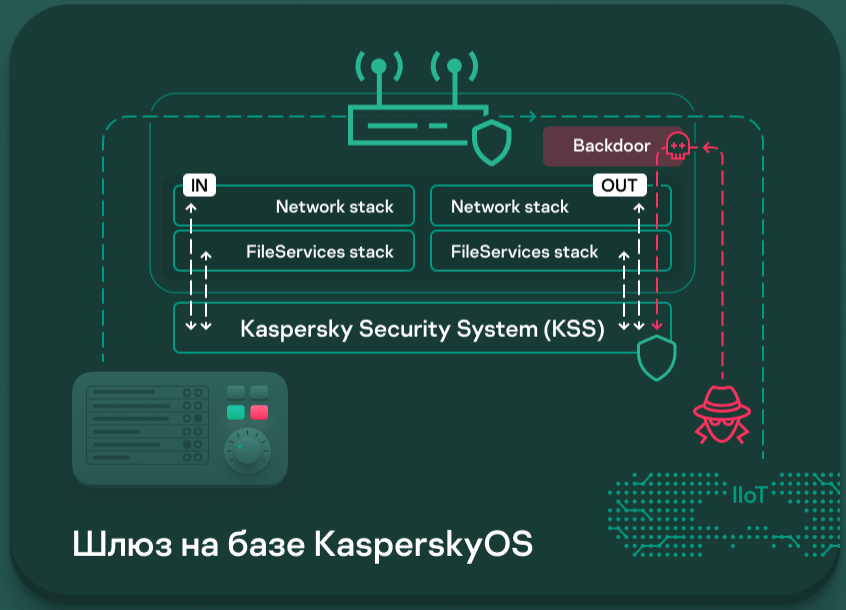
MQTT

Уникальные свойства в реальности*

* Сравнение проводится при схожих условиях заключительных стадий кибератаки цепочки KillChain



Стандартный шлюз IoT



Шлюз на базе KasperskyOS

Витрина технических решений

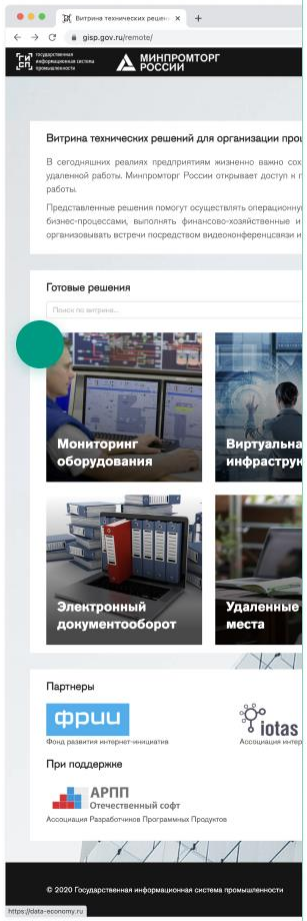
Наш программно-аппаратный комплекс размещён на gisp.gov.ru/remote в разделе «Мониторинг оборудования»

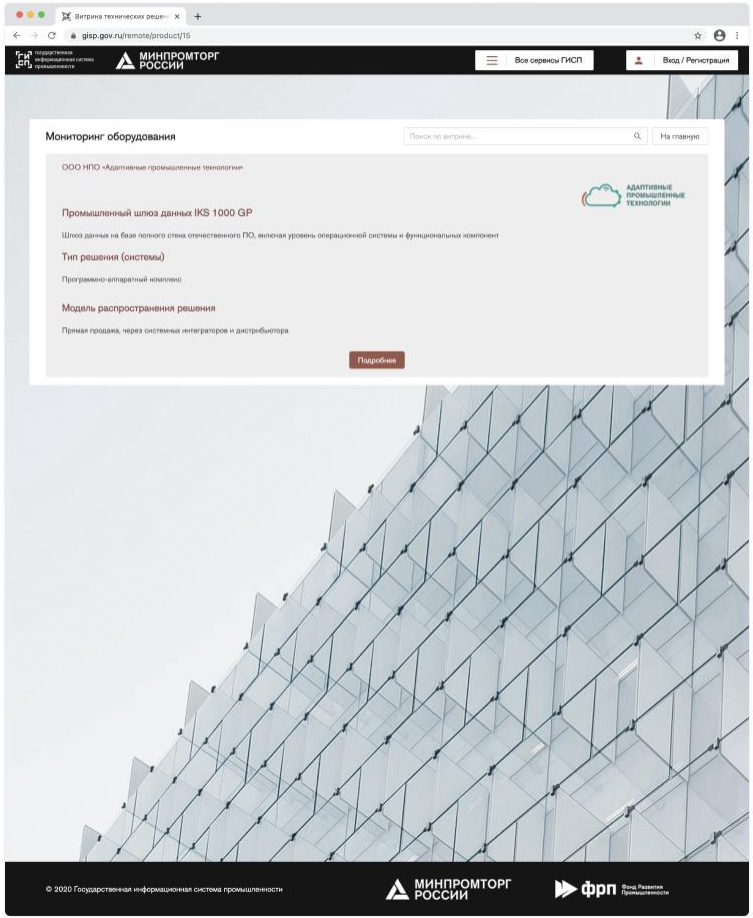
Наши партнёры

GAZPROM NEFT

CHELPIPE GROUP

НИИАС





KasperskyOS Gateway получил награду «World Leading Internet Scientific and Technological Achievement» в рамках крупнейшей китайской World Internet Conference (Wuzhen Summit)

23 ноября 2020

Вашим промышленным системам тоже нужна иммунизация

Андрей Суворов

A.Suvorov@aprotech.ru
Andrey.Suvorov@kaspersky.com

АДАПТИВНЫЕ ПРОМЫШЛЕННЫЕ ТЕХНОЛОГИИ

https://www.linkedin.com/in/andrey-suvorov-b8915513/