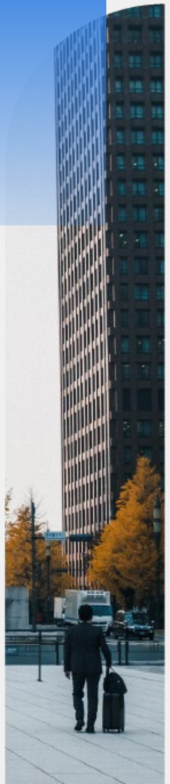


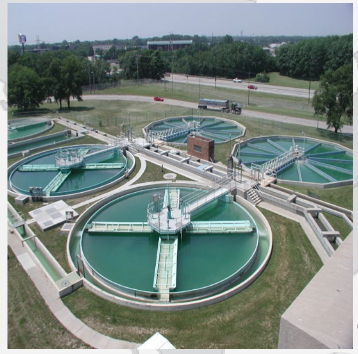
FORTINET

Защита критически важных объектов инфраструктуры

Вячеслав Гордеев

Операционные технологии

Промышленные системы управления (ICS)







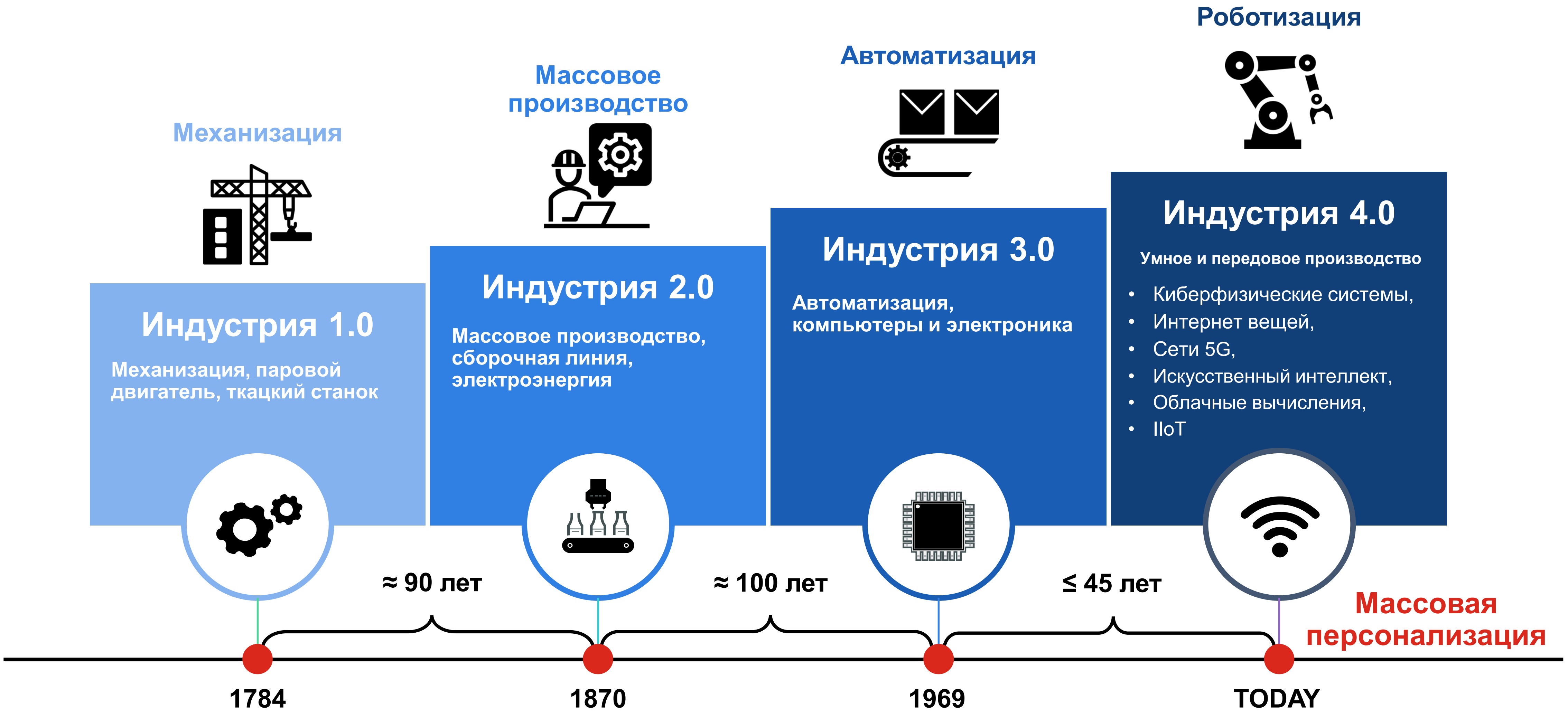
ВСЕ отрасли

Часто «критические» инфраструктуры

Все условия окружающей среды

Условия: (Жара, Влага, Вибрация); офис

Индустрия 4.0 — производители используют инновационные технологии



Эволюция промышленных систем управления

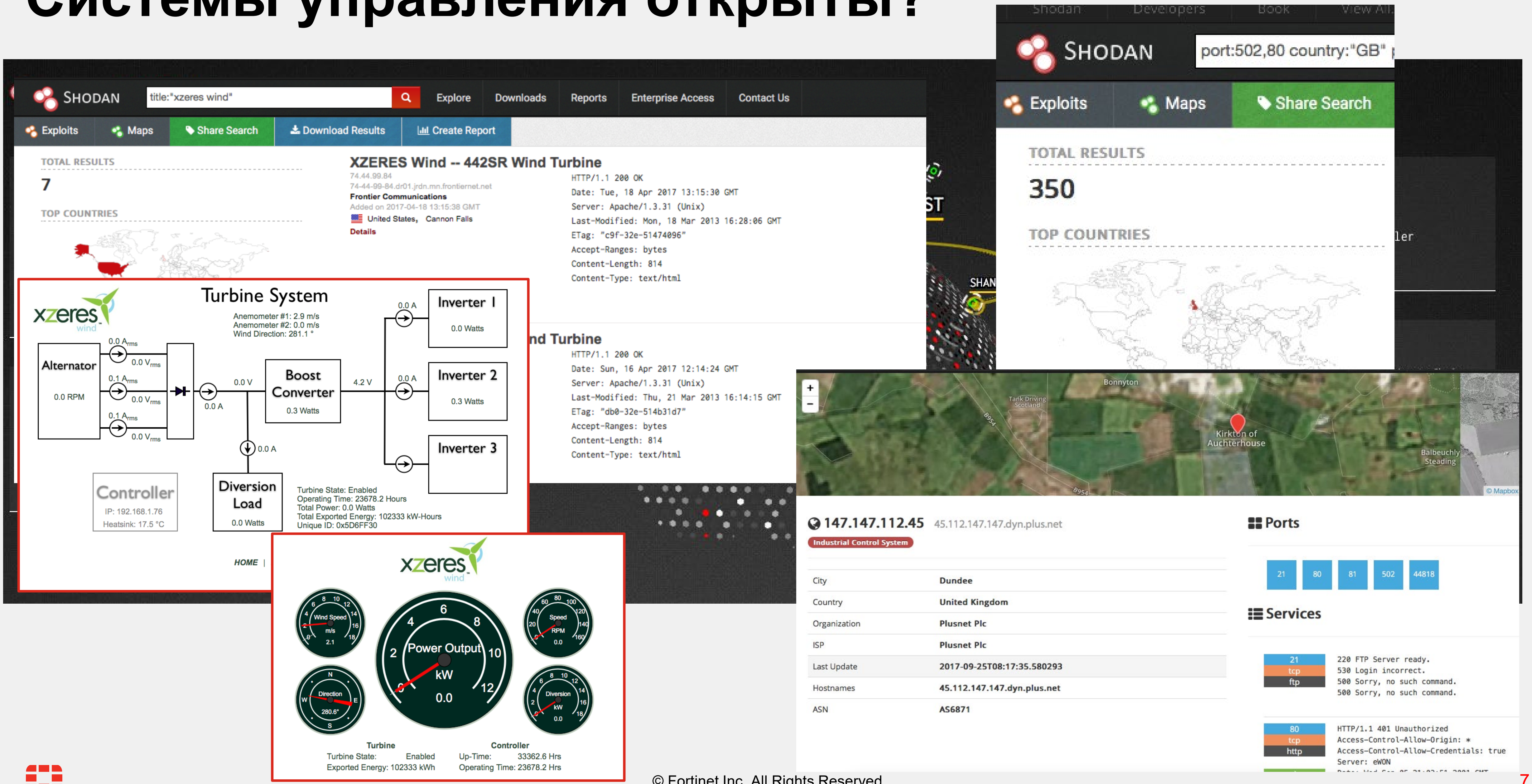
- Индустрия 4.0: Операционная эффективность = Кибер-Уязвимость
- Переход от проприетарных стандартов к IP-связности.
- Конвергенция ICS(АСУ ТП) / OT и ИТ-инфраструктуры
- Коммерческие готовые продукты (COTS), IOT и Cloud
- B2B-коммуникации, доступ для поставщиков / партнеров

Ключевые проблемы кибербезопасности в КИИ и Индустрии 4.0

Проблема №1: Расширение поверхности атаки

Периметр везде - бесконечные цифровые границы

Системы управления открыты?



References: Google Project Zero, The Register

Проблема № 2: рост продвинутых угроз

Проблемы, связанные с непрерывностью бизнеса и аварийным восстановлением

IT угрозы могут также повлиять на OT

Злоумышленники пользуются безумием из-за COVID-19 в СМИ

*many undisclosed | Record Stolen Reference—Breach Level Index | Ransomware stats—Statista

OT is proportional to OT Connectivity

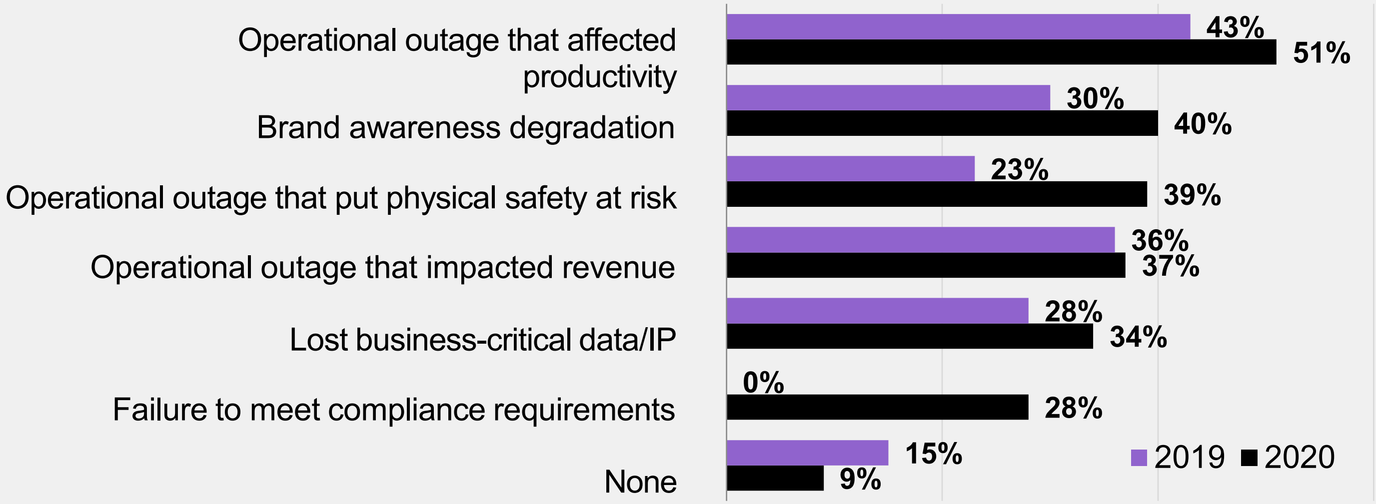
Yet inversely proportional to IT/OT security is integrated

9 out of 10

organizations **experienced at least 1 OT system intrusion** in the past year, up **19%** from 2019

65% had **3 or more intrusions**, up **18%** from 2019

Impact on organization



Top-tier organizations are:

4X

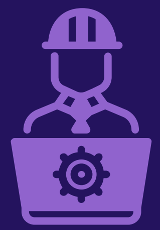
as likely to have centralized visibility in the SOC

133%

more likely to track and report vulnerabilities found and blocked

2X

as likely to currently have the CISO/CSO responsible for OT security



Source: The State of Operational Technology and Cybersecurity 2020

Крупнейшие атаки ransomware на производство

JBS SA
производитель говядины, свинины и курицы

Тип кибератаки: Ransomware (2020).
Расположение: Бразилия
Последствия: нарушение производства по всему миру
Стоимость: не разглашается

Ели бы он был закрыт хотя бы на один день, США потеряли бы почти четверть своих мощностей по переработке говядины, что эквивалентно 20.000 голов крупного рогатого скота.

Norsk Hydro
производитель алюминия

Тип кибератаки: Ransomware LockerGoga.
Расположение: Норвегия, Катар, Бразилия
Последствия: закрыл многие из своих заводов и был вынужден перевести другие на частичное ручное управление
Стоимость: $75 миллионов

Renault-Nissan

Тип кибератаки: Ransomware WannaCry
Расположение: Глобальная компания
Последствия: остановила производство на пяти заводах, расположенных в Англии, Франции, Словении, Румынии и Индии.
Стоимость: не разглашается

Не только о деньгах:
Глобальные атаки на производство часто спонсируются государством. У враждебных государств вполне могут быть причины для прекращения производства в рамках политической кампании.

Какие последствия от кибератак?

Влияние

- Безопасность оборудования и персонала
- Саботаж\Отключение заводов
- Повреждение оборудования
- Нарушение производства и поставки
- Саботаж на трубопроводах (разливы)
- Нарушение операционной деятельности
- Транспортировка и Доставка (эффективность и надежность отгрузки, кража)

Последствия

- Отрицательное влияние на национальный и глобальный ВВП
- Угроза безопасности экологии и человека
- Остановка управления компанией
- Угроза национальной безопасности
- Потеря бизнеса
- Нарушение предоставляемого сервиса
- Штрафы и взыскания
- Нарушение репутации
- Компрамис качества

Тяжелая промышленность сталкивается с уникальными проблемами кибербезопасности, учитывая их распределенные, децентрализованные структуры управления и большую оперативную технологическую среду (OT) - среду, которая не очень легко поддается традиционному контролю кибербезопасности.

McKinsey & Company

Critical infrastructure companies and the global cybersecurity, 2019

Проблема № 3: сложность управления инцидентами

Сложно найти баланс между людьми, процессами и технологиями

Слишком много Вендоров

Слишком много инцидентов

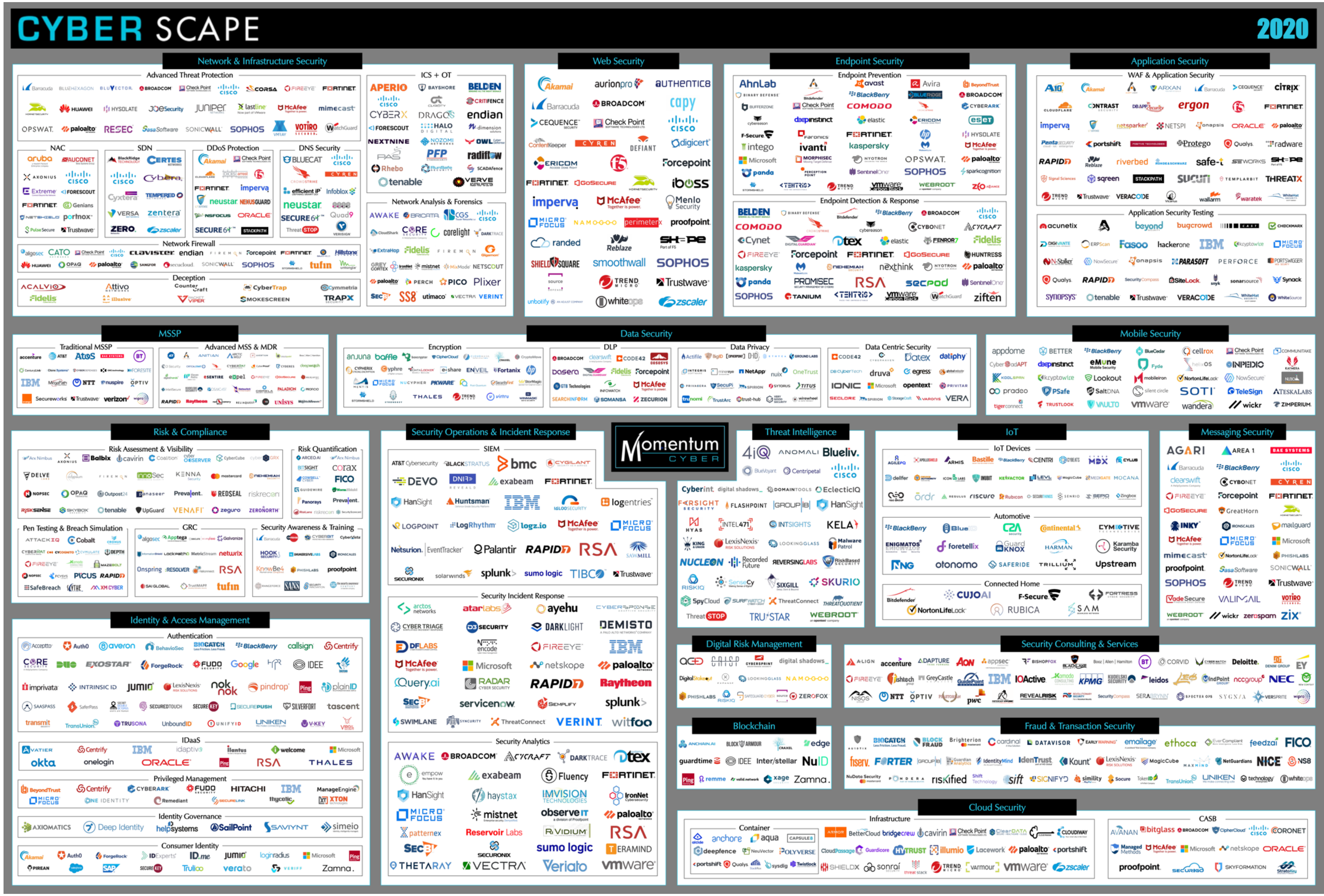
Ручные процессы

Скорость решения инцидентов

Проблема обученных специалистов

Множество решений по кибербезопасности: КУДА инвестировать?

При наличии в среднем 75 развернутых различных технологий и инструментов безопасности, как организация может рассчитывать на прозрачную и сквозную видимость инфраструктуры?



Source: *Momentum*

Как Fortinet обеспечивает защиту критически важных объектов инфраструктуры

Управление кибер-рисками по всей цепочки цифрового производства.

ЛИДЕР В ОБЛАСТИ ТЕХНОЛОГИЙ В ОБЛАСТИ КОРПОРАТИВНОГО УПРАВЛЕНИЯ

$30.1B+ Market Cap
Nasdaq: FTNT
S&P 500

$3.09B
FY2020 Billings
Fast Growing, Solid Profitability

770+
Patents
Top Innovator

#1 Компания по кибербезопасности в Мире

Возглавляет все этапы развития кибербезопасности

- ✓ *Наиболее устанавливаемый*
- ✓ *Самые проверенные*
- ✓ *Самый запатентованный*
- ✓ *Широчайшее портфолио*

30%
Global Firewall Shipments
Huge Scale

510,000+
Customers Worldwide
Massive Sensor Network

30+
Cybersecurity Product Lines
Broadest Attack Surface Coverage

Source: Company data, Figures as of March 31, 2021

Фабрика Информационной Безопасности

Прозрачность

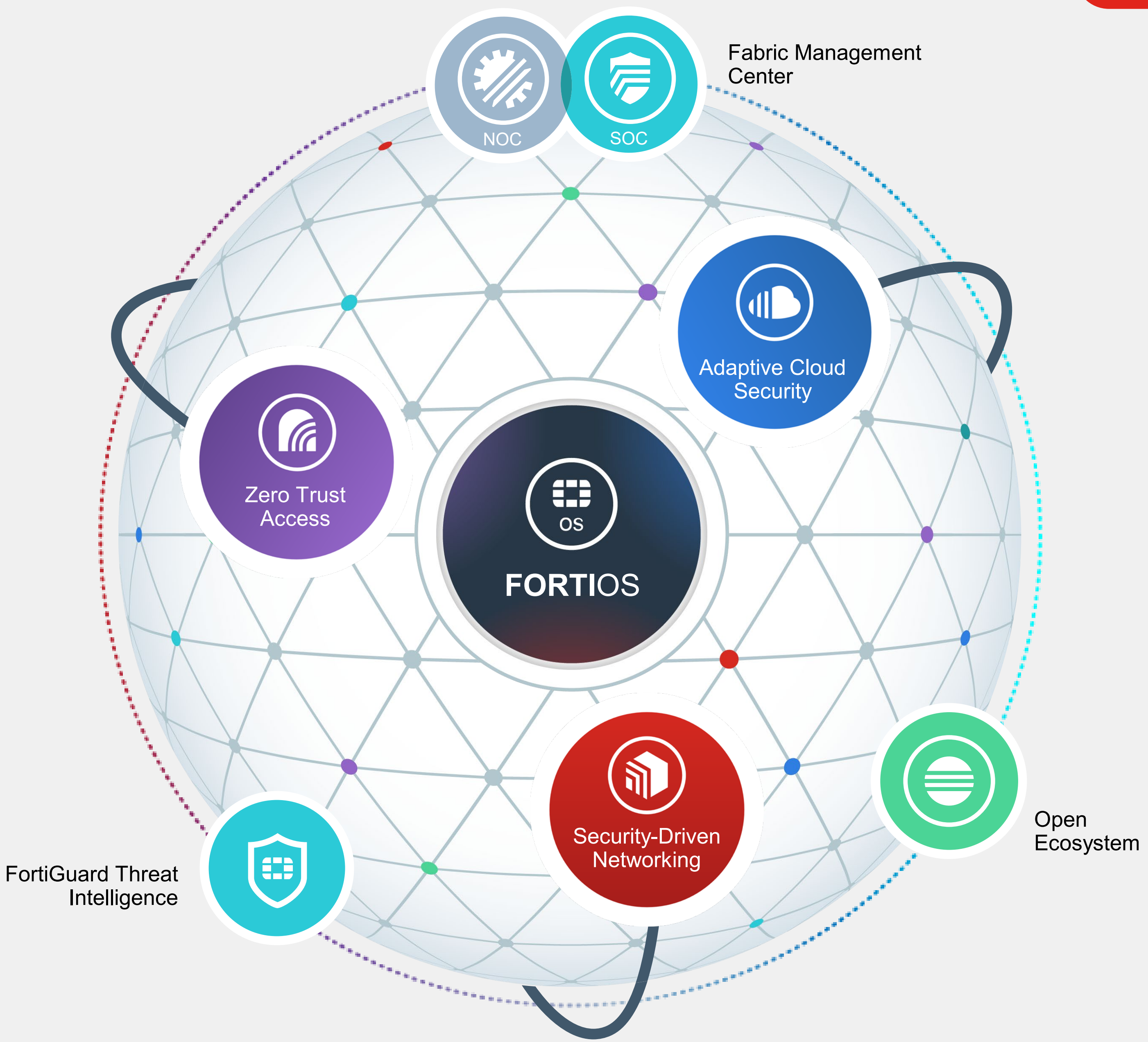
Полная видимость атакуемой поверхности для лучшего управления рисками ИБ

Комплексность

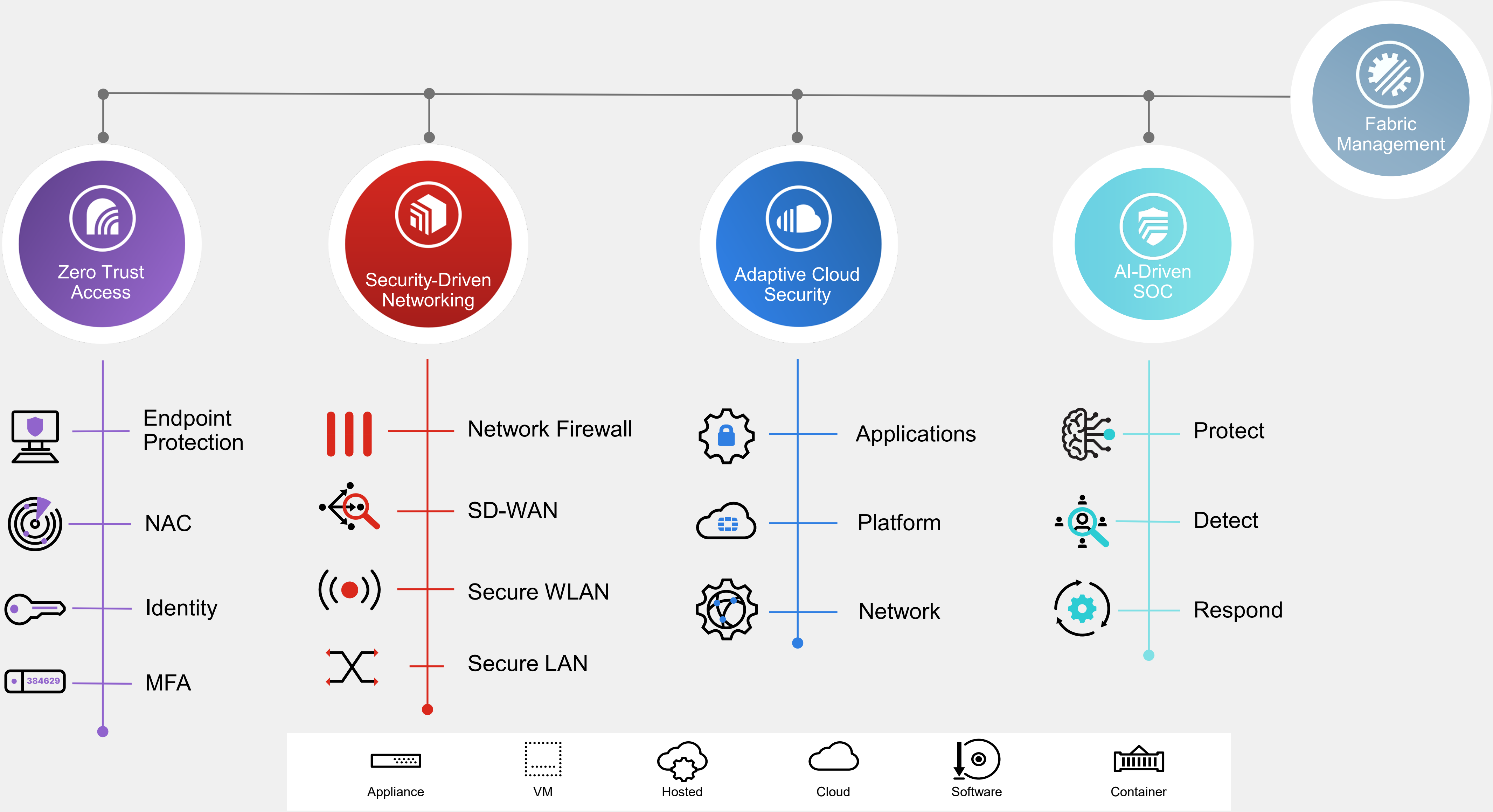
Снижение стоимости эксплуатации за счет объединения всех компонентов в рамках единой платформы

Автоматизация

Самостоятельная инфраструктура под управлением искусственного интеллекта



Fortinet платформа кибербезопасности



Открытая Экосистема

Более 400+ лучших в своем классе решений в составе платформы

Fortinet-developed deep integration automating security operations and policies

Fabric Connectors

aws, aruba, cisco, Google Cloud, IBM Cloud, Microsoft Azure, ORACLE, servicenow, Symantec

Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

Fabric APIs

EQUINIX, Guardicore, DELL, DRAGOS, ARISTA, SIEMENS Ingenuity for life, ordr, NVIDIA, tufin

Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration

Fabric DevOps

aws, Google Cloud, HashiCorp, Microsoft Azure, openstack, ORACLE, RED HAT ANSIBLE Automation, TIGERA, vmware

Integrations with threat sharing initiatives and other vendor technologies

Extended Ecosystem

CYBER THREAT ALLIANCE, MITRE, STIX, INTERPOL, OT CSA, Firewalls, Switching, Wireless, Endpoint Security

And many more…

Note: Logos are a representative subset of the Security Fabric Ecosystem

Преодоление разрыва между безопасностью IT и OT

Всесторонняя безопасность OT с использованием партнерских отношений

ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

ПОСТАВЩИКИ РЕШЕНИЙ И СИСТЕМНЫЕ ИНТЕГРАТОРЫ

Интеграция между SCADAGuardian и FortiGate

NOZOMI NETWORKS			FORTINET
Пассивный мониторинг в режиме реального времени гарантирует отсутствие негативного воздействия и полную видимость на всех уровнях.	**Пассивный мониторинг**	**In-line защита**	In-line разделение между IT и OT средами.
Глубокое понимание всех АСУ ТП протоколов, открытых и проприетарных	**Распознавание данных в трафике АСУТП**	**Контроль трафика по приложениям АСУТП**	Проактивная фильтрация вредоносного ПО и неавторизованного сетевого трафика.
Автоматически изучает поведение индустриальных систем и обнаруживает подозрительные действия.	**Поведенческий анализ**	**Применение политик безопасности**	Гибкость применения политик безопасности с различной степенью детализации.

Внутренний и внешний контроль

Тонкая настройка и мониторинг по наборам правил МЭ

Проактивная защита АСУ ТП

Примеры из жизни

Понимание трафика в сетях производства (OT)

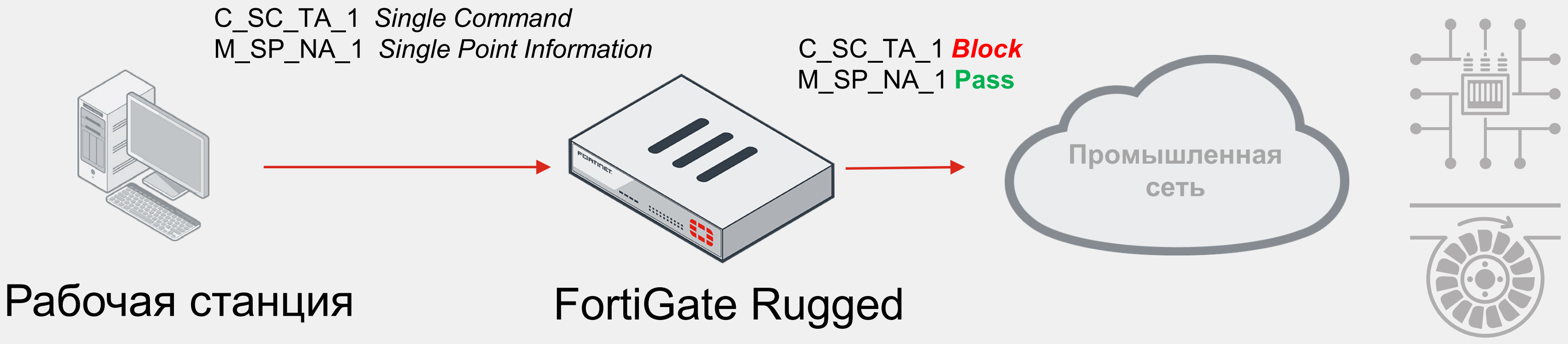
Протоколы

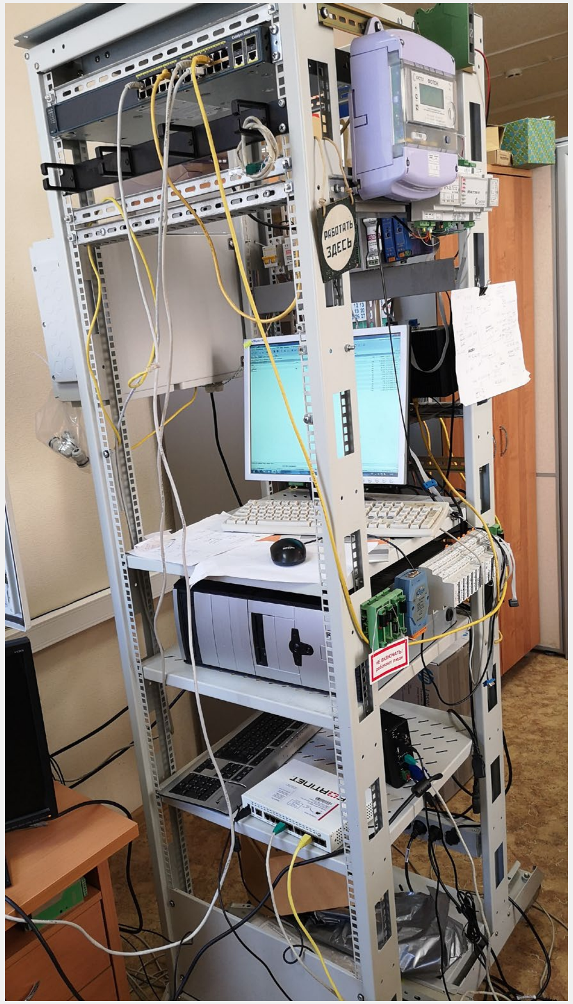
- BACnet
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- HART
- IEC 60870-6 (TASE 2) /ICCP
- IEC 60870-5-104
- IEC 61850
- LONTalk
- MMS
- Modbus
- OPC
- Profinet
- S7
- SafetyNET
- Synchrophasor

Приложения

- 7 Technologies/ Schneider Electric
- ABB
- Advantech
- Broadwin
- CitectSCADA
- CoDeSys
- Cogent
- DATAC
- Eaton
- GE
- Iconics
- InduSoft
- IntelliCom
- Measuresoft
- Microsys
- MOXA
- PcVue
- Progea
- QNX
- RealFlex
- Rockwell Automation
- RSLogix
- Siemens
- Sunway
- TeeChart
- VxWorks
- WellinTech
- Yokogawa

Тестирование FortiGate





- Глубокий анализ модифицированного протокола ГОСТ Р МЭК 104 (IEC-104)

- Конкуренты Hirschmann, UserGate и др.

23

Сценарий #1 | Контроль и мониторинг

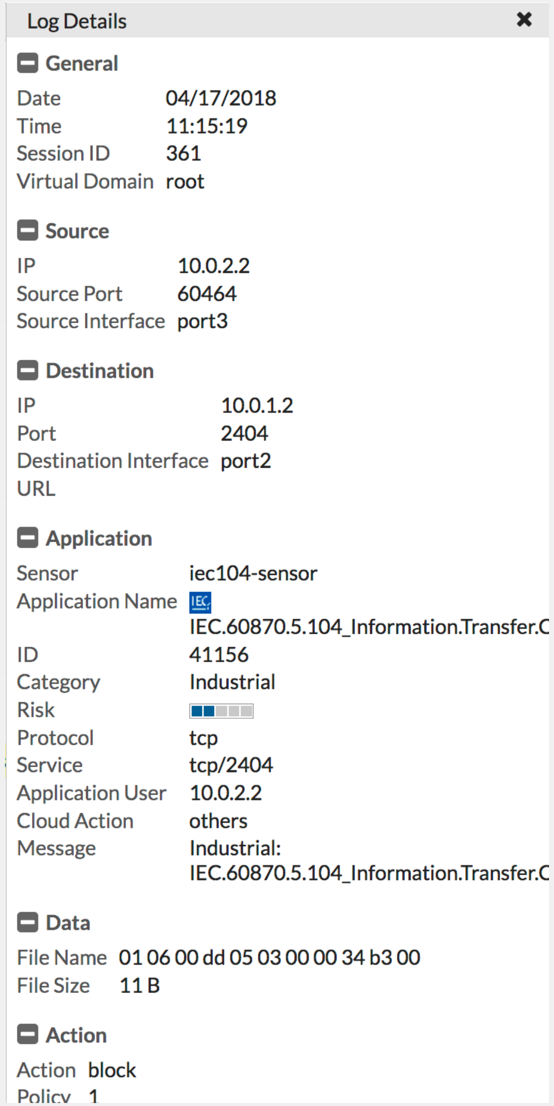
- Используется профиль Application Control
- IEC-104 отправляет команды в диапазон адресов СОА
- Регистрация всех выполняемых команд

Add Filter

#		Date/Time	Source	Destination	Application Name	Action	Application User
1		10:44:19	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NB.1	pass	10.0.1.2
2		10:44:19	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NB.1	pass	10.0.1.2
3		10:44:19	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NB.1	pass	10.0.2.2
4		10:44:19	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NA.1	pass	10.0.1.2
5		10:44:19	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NA.1	pass	10.0.1.2
6		10:44:19	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NA.1	pass	10.0.2.2
7		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.1.2
8		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.1.2
9		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.2.2
10		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.1.2
11		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.1.2
12		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.2.2
13		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.1.2
14		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.1.2
15		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.DC.NA.1	pass	10.0.2.2
16		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SC.NA.1	pass	10.0.1.2
17		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SC.NA.1	pass	10.0.1.2
18		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SC.NA.1	pass	10.0.2.2
19		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SC.NA.1	pass	10.0.1.2
20		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SC.NA.1	pass	10.0.1.2
21		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SC.NA.1	pass	10.0.2.2
22		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NA.1	pass	10.0.1.2
23		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NA.1	pass	10.0.1.2
24		10:44:18	10.0.2.2	10.0.1.2	IEC.60870.5.104_Information.Transfer.C.SE.NA.1	pass	10.0.2.2

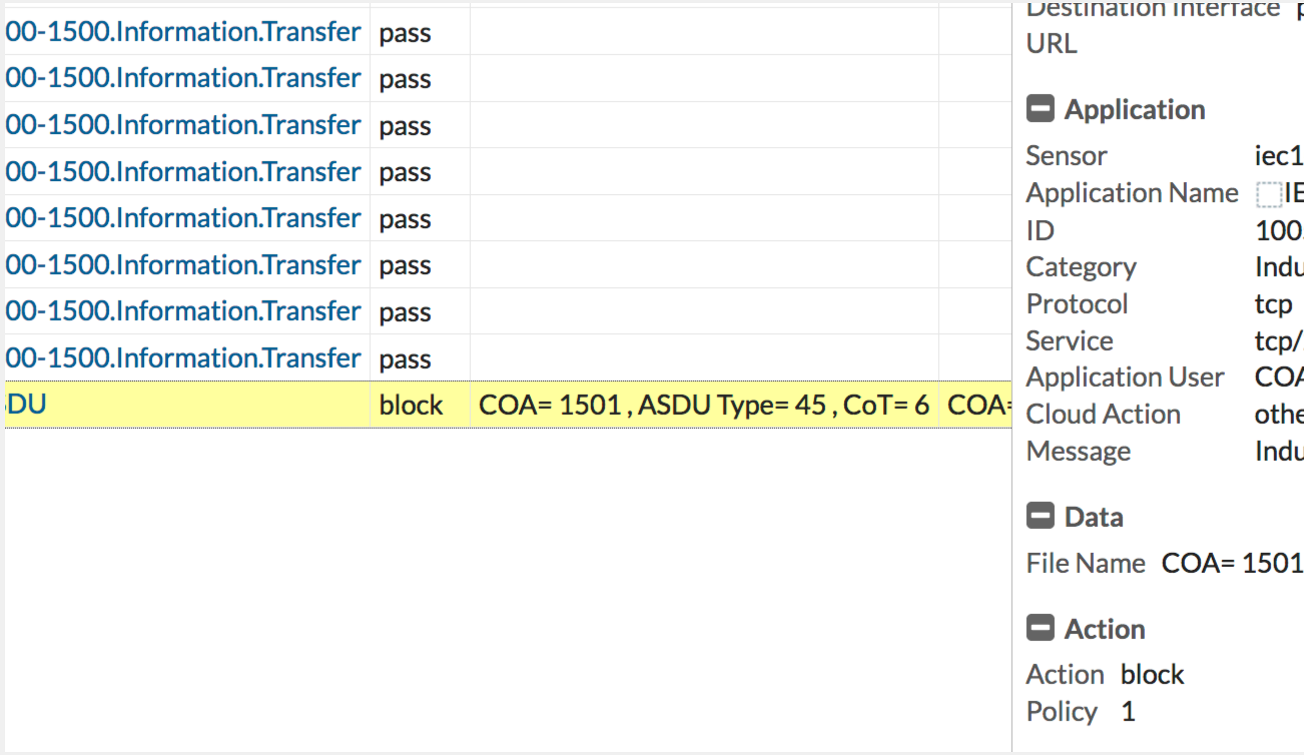
Сценарий #2 | Белый список

- Использование «кастом» сигнатур, разрешающих выполнения только определенных команд COA
- Остальное блокируется
- IEC-104 клиент отправляет трафик на неавторизированные COA
- Трафик записывается в журнал

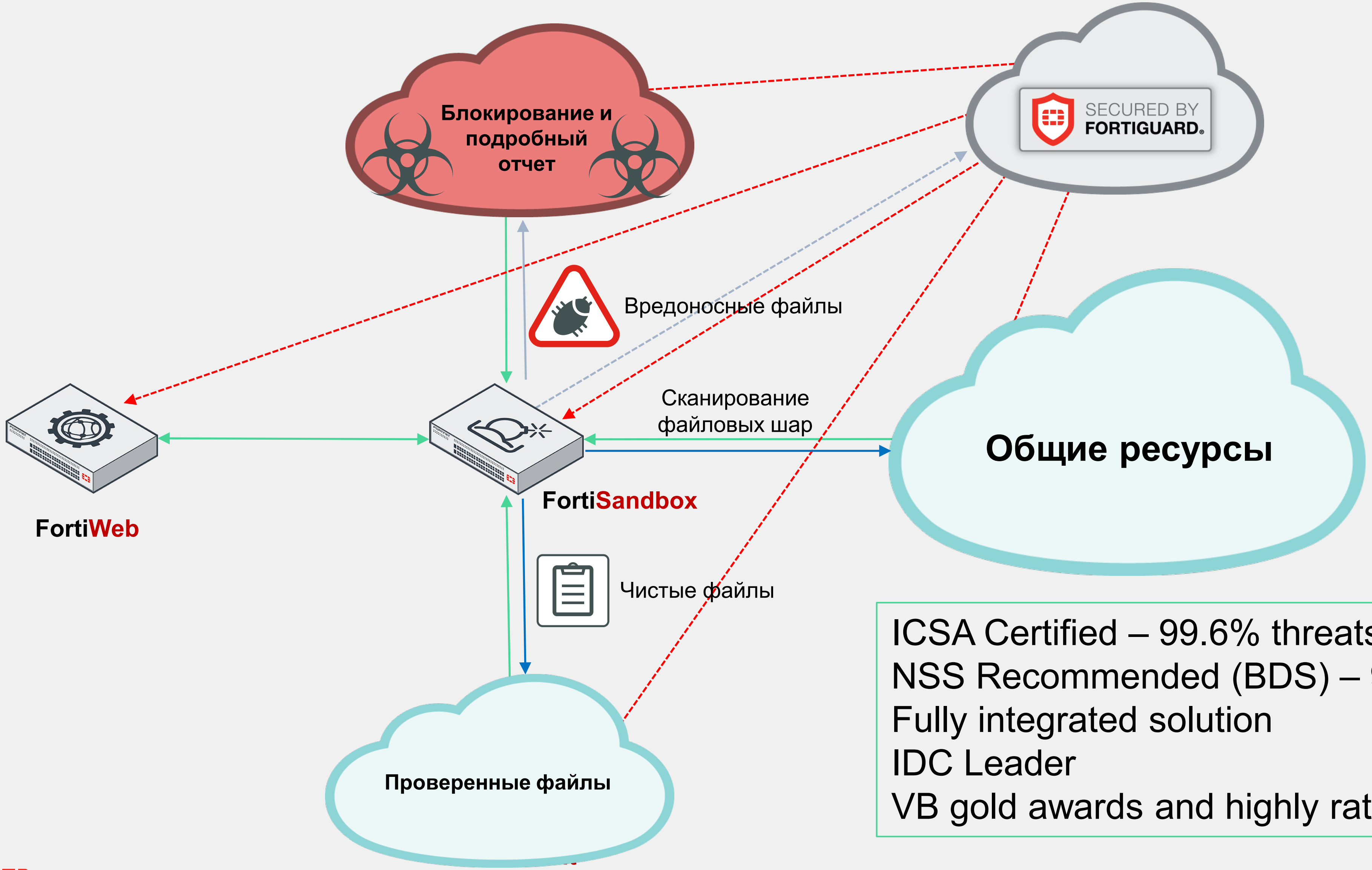


Сценарий #3 | Контекстная информация

- Разработка «кастом» сигнатуры, которая преобразует контекстную информацию в удобочитаемый формат
- IEC-104 клиент отправляет команды в не авторизованный COA
- Журнал с удобочитаемым форматом

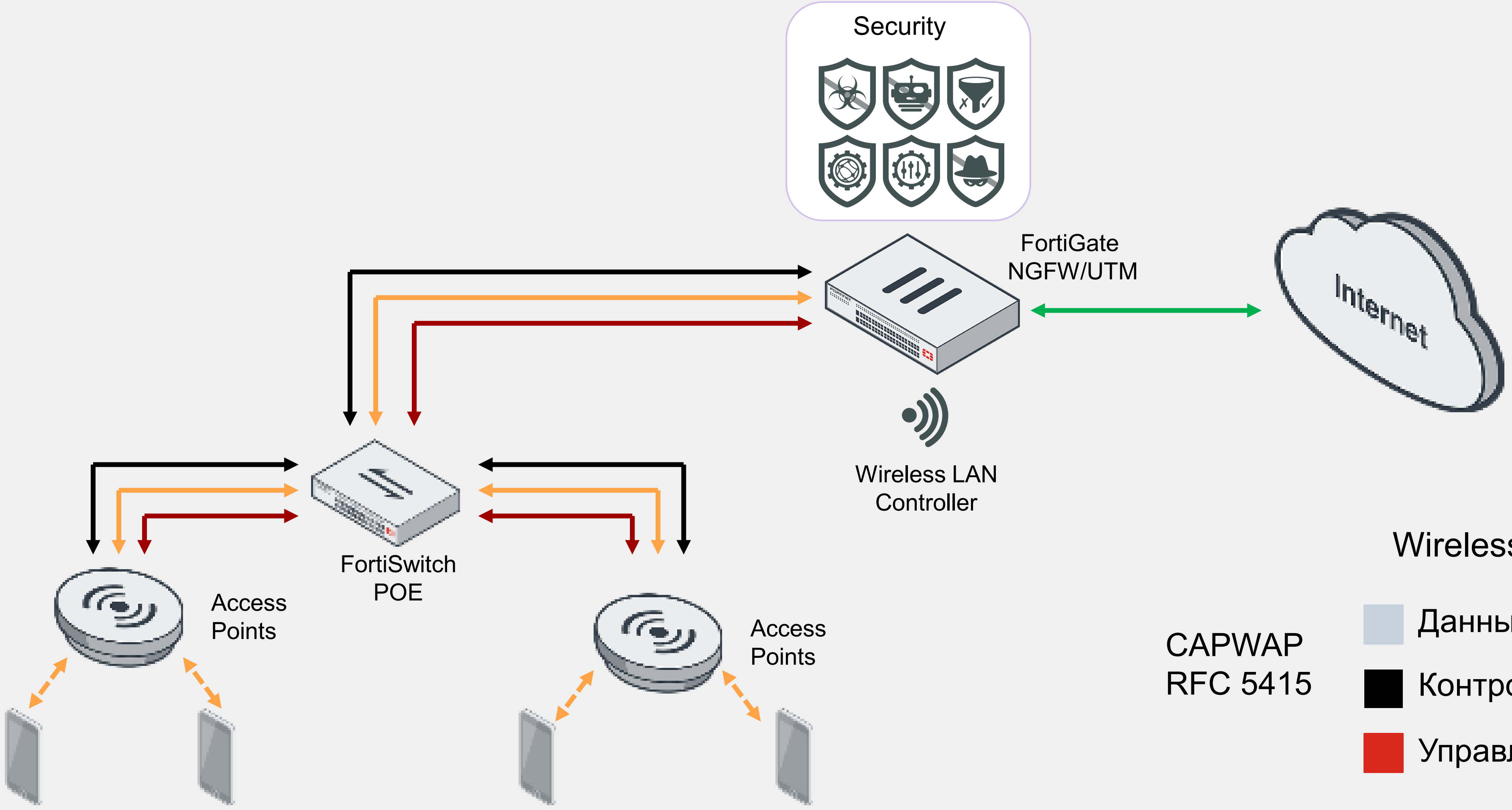


Сценарий #4 | Файловый контроль



ICSA Certified – 99.6% threats detected
NSS Recommended (BDS) – 99% breach detection rate
Fully integrated solution
IDC Leader
VB gold awards and highly rated for Spam & AV

Сценарий #5 | Безопасная беспроводная сеть



Wireless Plane

CAPWAP
RFC 5415

- Данные
- Контроль
- Управление

Сценарий #6 | Разработка «кастом» сигнатур

Кастомные сигнатуры помогают детально декодировать промышленный протокол

Edit Application Signature

Name: IEC104.1000-1500.Information.Transfer

Comments:

Signature

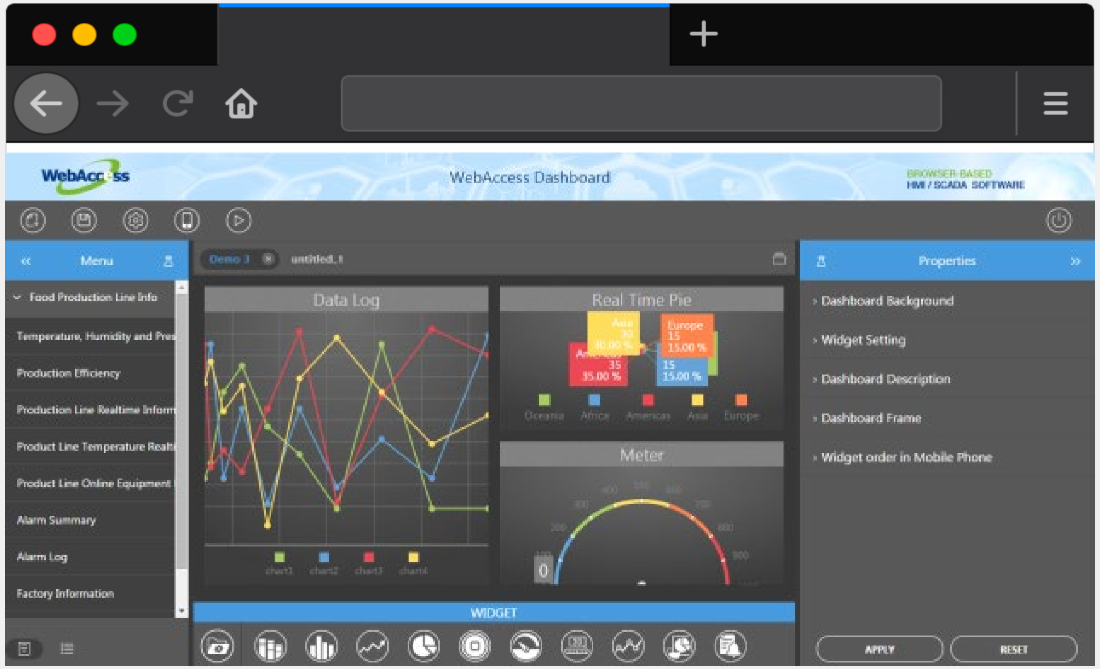
```
F-SBID( --attack_id 1002; --name "IEC104.1000-1500.Information.Transfer"; --protocol tcp; --app_cat
26; --default_action pass; --service iec104;  --dst_port 2404; --flow bi_direction; --pattern |68|;
--context body; --within 1,context; --byte_test 1,~,1,1,relative; --pcre "/(\x2d|\x2e|\x2f|\x30|\x31|
\x32|\x33)/"; --context body; --distance 5; --within 1; --pcre "/(\x06|\x07|\x08|\x09|\x0a|\x2c|\x2d|
\x2e|\x2f|\x46|\x47|\x48|\x49|\x4a|\x6c|\x6d|\x6e|\x6f|\x86|\x87|\x88|\x89|\x8a|\xac|\xad|
\xae|\xaf|\xc6|\xc7|\xc8|\xc9|\xca|\xec|\xed|\xee|\xef)/"; --context body; --distance 1; --within 1;
--byte_test 2,>,999,1,little,relative; --byte_test 2,<,1501,1,little,relative; --weight 20;  --skip-after 0;)
```

Детализация выполненных команд вплоть до адресов COA, ASDU и CoT

#		Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
1		16:11:48	10.0.2.2	10.0.1.2	IEC104.ASDU	block	COA= 1000 , ASDU Type= 49 , CoT= 7	COA= 1000 , ASDU Type= 49 , CoT= 7
2		16:11:48	10.0.2.2	10.0.1.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 49 , CoT= 6	COA= 1000 , ASDU Type= 49 , CoT= 6
3		16:11:47	10.0.2.2	10.0.1.2	IEC.60870.5.104_CF	pass		CF
4		16:11:47	10.0.2.2	10.0.1.2	IEC.60870.5.104_CF	pass		CF
5		16:11:00	10.0.2.2	10.0.1.2	IEC.60870.5.104_Supervisory.Functions	pass	10.0.2.2	Supervisory Functions
6		16:10:56	10.0.2.2	10.0.1.2	IEC104.ASDU	pass	COA= 1037 , ASDU Type= 46 , CoT= 10	COA= 1037 , ASDU Type= 46 , CoT= 10
7		16:10:56	10.0.2.2	10.0.1.2	IEC104.ASDU	pass	COA= 1037 , ASDU Type= 46 , CoT= 7	COA= 1037 , ASDU Type= 46 , CoT= 7
8		16:10:56	10.0.2.2	10.0.1.2	IEC104.ASDU	pass	COA= 1037 , ASDU Type= 46 , CoT= 6	COA= 1037 , ASDU Type= 46 , CoT= 6
9		16:10:56	10.0.2.2	10.0.1.2	IEC104.ASDU	pass	COA= 1036 , ASDU Type= 48 , CoT= 10	COA= 1036 , ASDU Type= 48 , CoT= 10
10		16:10:56	10.0.2.2	10.0.1.2	IEC104.ASDU	pass	COA= 1036 , ASDU Type= 48 , CoT= 7	COA= 1036 , ASDU Type= 48 , CoT= 7

29

Сценарий #7 | Публикация web-приложений



Публикация приложений мониторинга SCADA/HMI

Контроль управляющих воздействий для команд в обертке HTTP/HTTPS

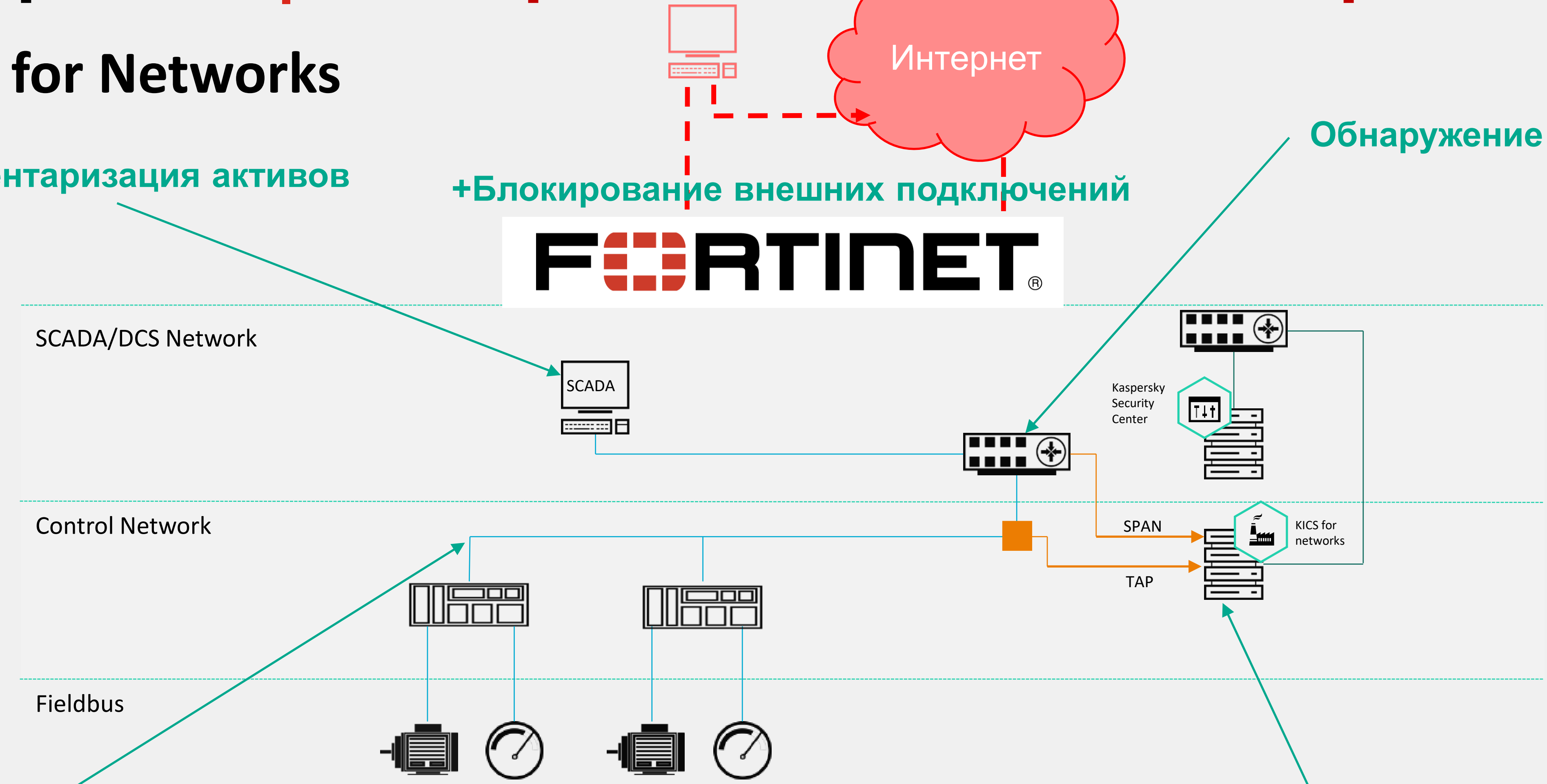
Сценарий #8 | Интеграция со сторонними решениями

+ KICS for Networks

Инвентаризация активов

+Блокирование внешних подключений

Обнаружение вторжений



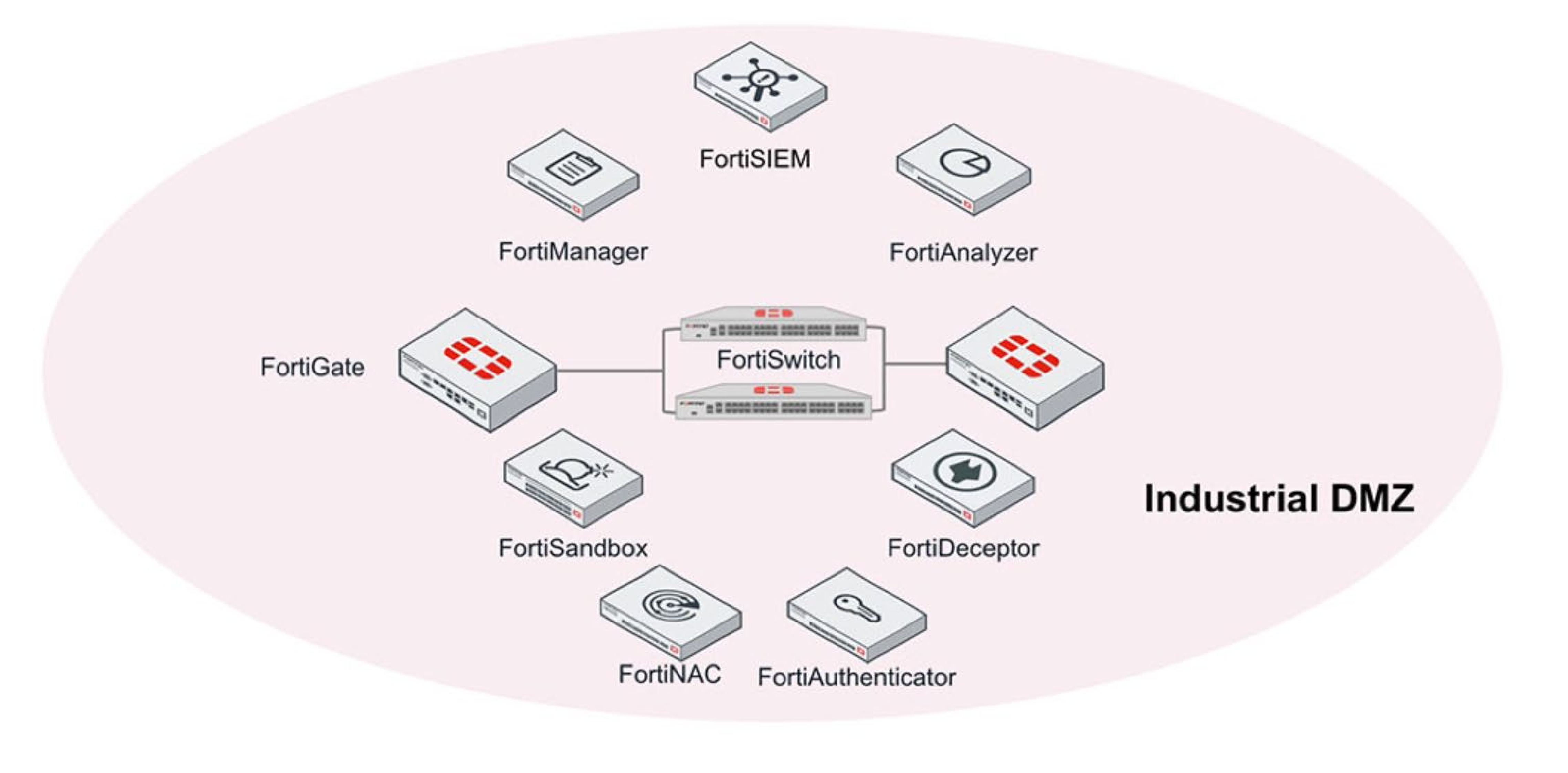
Глубокий анализ промышленного трафика

Сбор, корреляция и хранение событий

Контроль сетевой активности и правил работы системы

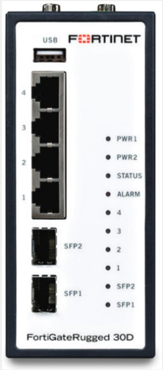
31

Сценарий #9-10 | Контроль сетевого доступа



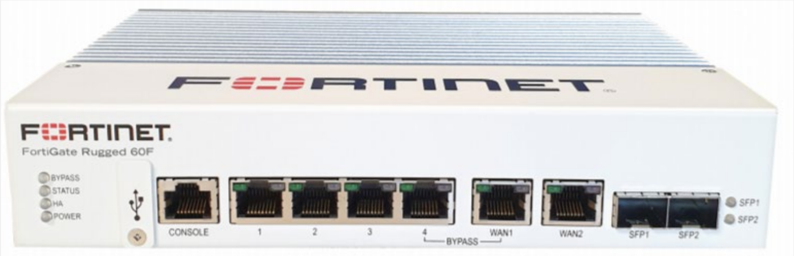
32

Устройства для индустриальной среды



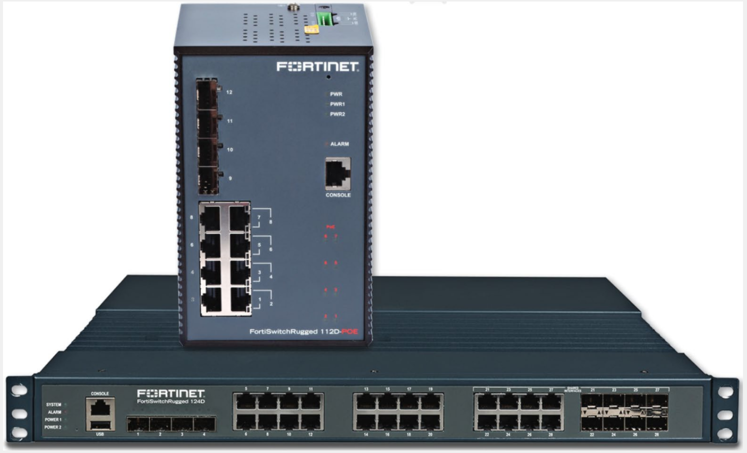
Универсальный шлюз безопасности (межсетевой экран) FortiGate Rugged 30D/35D/60D/90D

- Закрытый корпус без вентиляторов*
- Работа при экстремальных температурах (-40 до 75 С)
- Стандарты IEC 61850-3, IEEE 1613, Division1 Class 2 Compliant
- Опциональная поддержка Wi-Fi, поддержка 3G/4G модемов



Коммутаторы FortiSwitch Rugged 112D-PoE/124D

- Закрытый корпус без вентиляторов и движущихся частей, IP30
- Работа при экстремальных температурах (-40 до 60 С)
- Поддержка интеграции с FortiGate (расширение портовой емкости)



Точка доступа FortiAP 222C

- Поддержка стандартов IEEE 802.11a/b/g/n/ac и работа на частотах 2.4 GHz и 5 GHz
- Работа в экстремальных температурах (-40 до 60 С)
- FortiGate выступает в роли контроллера

Заключение

Мост безопасности между IT и OT

Переход от точечных решений к интеграционному решению

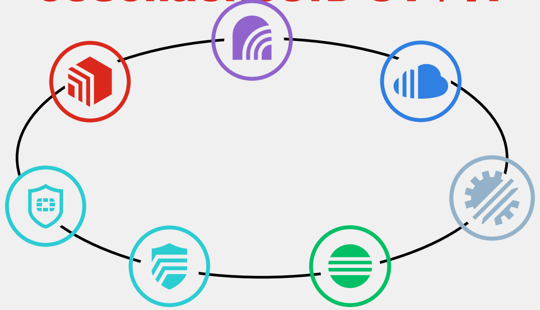
Точечные решения IT Security

- Трудное управление
- Добавляет сложности
- Вводит пробелы в безопасности

Точечные решения OT Security

Преодоление пробела с конвергентной и интегрированной безопасностью

Конвергентная безопасность OT / IT

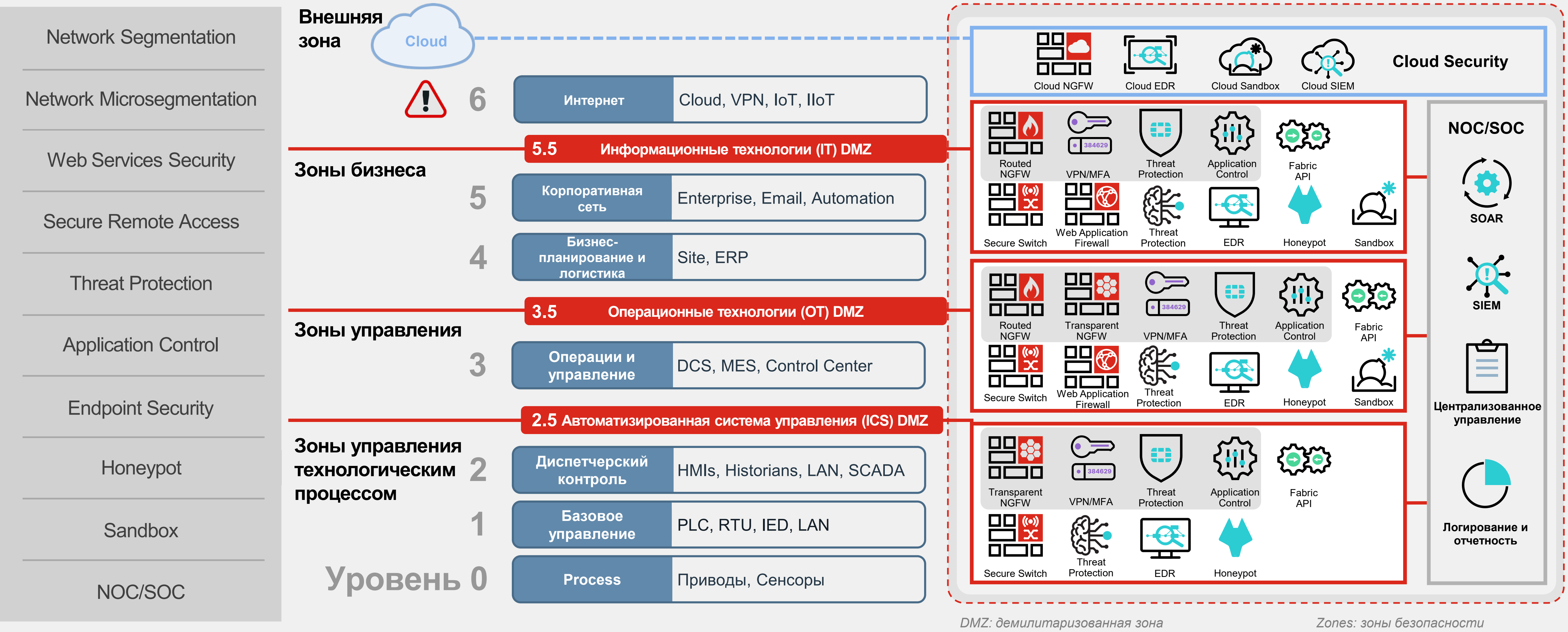


- Упрощенное управление
- Снижение сложности
- Единая безопасность

Обеспечение безопасности OT

с фабрикой безопасности Fortinet

Фабрика безопасности Fortinet



DMZ: демилитаризованная зона
EDR: Endpoint Detection & Response
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
Zones: зоны безопасности
MFA: Multi-factor Authentication
NGFW: Next-Generation Firewall
VPN: Virtual Private Network

Доверие и выполнение требований регуляторов Сертификация ФСТЭК России

ИТ.МЭ.А4.П3
ИТ.МЭ.Б4.П3
ИТ.СОВ.С4.П3

УД6
ИТ.МЭ.А6.П3, ИТ.МЭ.Б6.П3
ИТ.СОВ.С6.П3,
ИТ.САВЗ.Б6.П3

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4222

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
11 февраля 2020 г.

Выдан: 11 февраля 2020 г.
Действителен до: 11 февраля 2025 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS версии 6.X**, разработанный компанией Fortinet и производимый АО «НИЦ», является программно-аппаратным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений и межсетевого экрана, соответствует требованиям по безопасности информации, установленным в документах «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.П3» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.П3» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.П3» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре ЦТНВ-26.20.40.140-011 ФО.

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4362

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
15 января 2021 г.

Выдан: 15 января 2021 г.
Действителен до: 15 января 2026 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS версии 6.X**, разработанный компанией Fortinet и производимый АО «НИЦ», является системой обнаружения вторжений, межсетевым экраном и средством антивирусной защиты, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 6 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А шестого класса защиты. ИТ.МЭ.А6.П3» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б шестого класса защиты. ИТ.МЭ.Б6.П3» (ФСТЭК России, 2016), «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б шестого класса защиты. ИТ.САВЗ.Б6.П3» (ФСТЭК России, 2012), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети шестого класса защиты. ИТ.СОВ.С6.П3» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре ЦТНВ-26.20.40.140-020 ФО.

Безопасные и надежные решения ИТ и ОТ для цифрового производства от Fortinet

Вячеслав Гордеев

cis@fortinet.com – технические вопросы
russia@fortinet.com – общие вопросы