FORTINET

Фабрика промышленной безопасности

Гордеев Вячеслав

Операционные технологии

Промышленные системы управления (ICS)

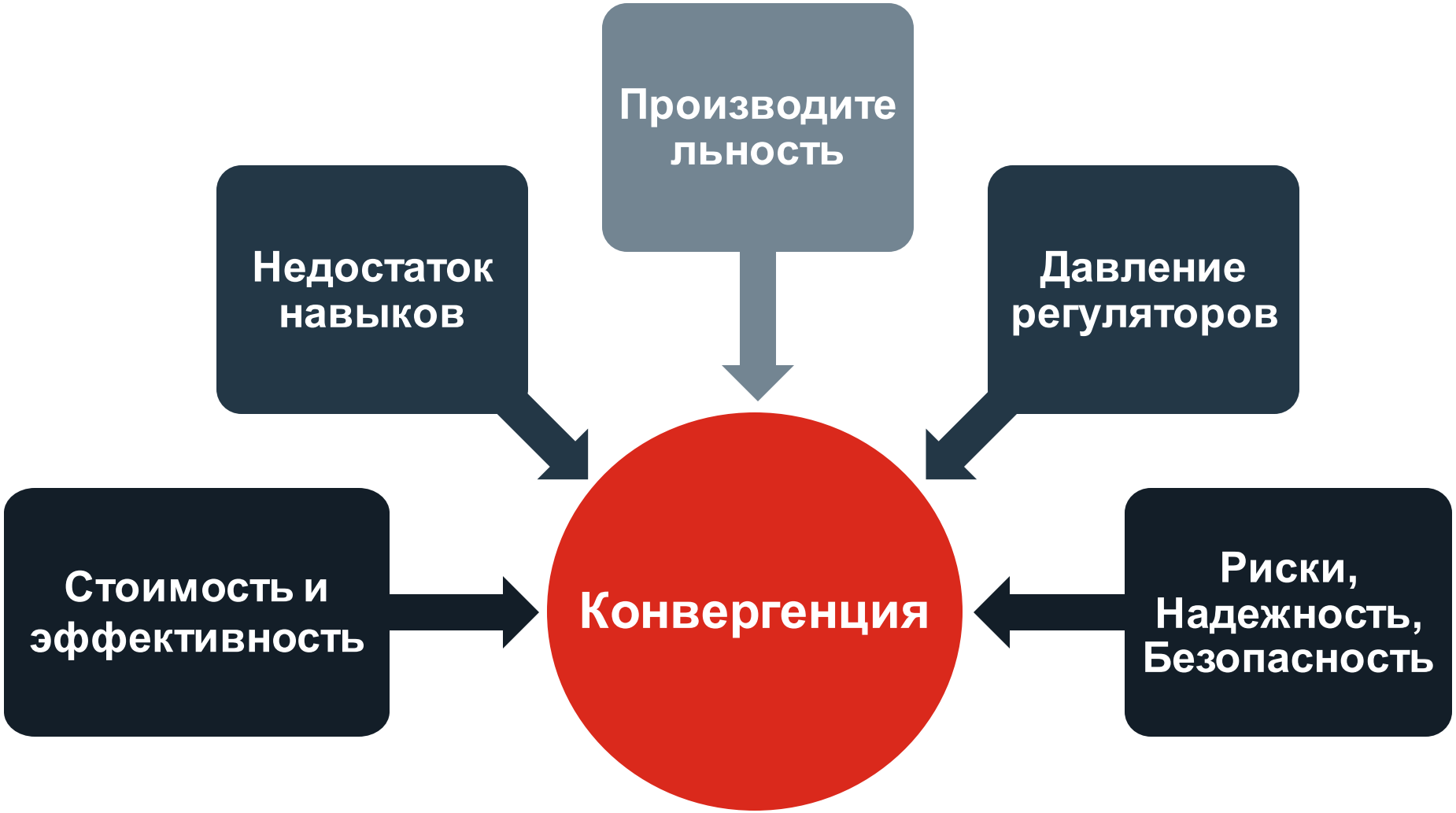
ВСЕ отрасли

Часто «критические» инфраструктуры

Все условия окружающей среды

Условия: (Жара, Влага, Вибрация); офис

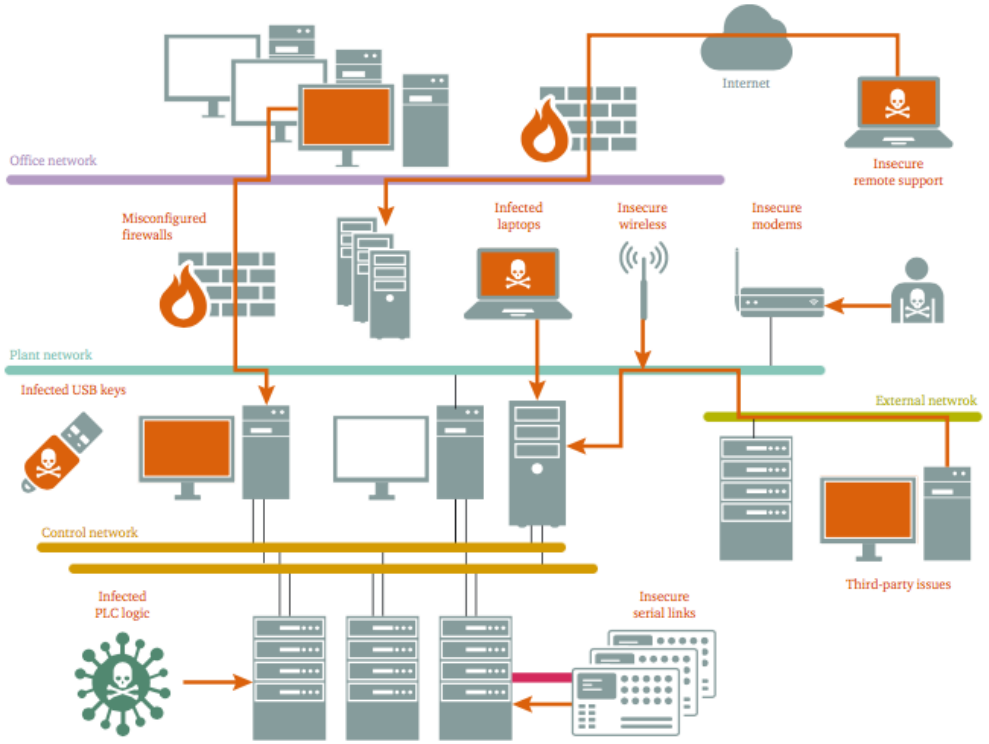
Силы, способствующие росту конвергенции ИТ / ОТ



Реальны ли кибер-урозы в OT-среде?

- Увеличение числа кибер-инцидентов АСУ ТП - преднамеренное или…
- Больше использования IoT и общих аппаратных платформ = общие уязвимости
- Industry 4.0, Big Data, Business Analytics; конвергенция IT & OT
- Длительные рабочие циклы = проблема применения исправлений
- Штрафы за нарушения и проблемы соответствия
- Передача на аутсорсинг по крайней мере части инфраструктуры и безопасности АСУ ТП/ICS

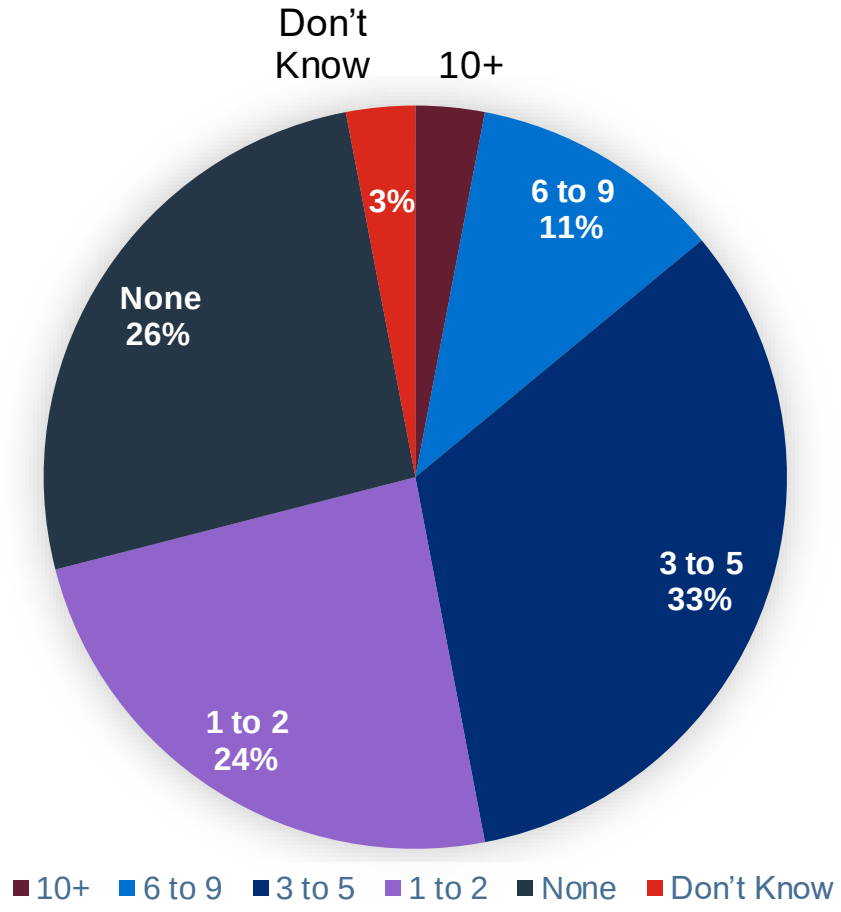
Figure 1: Potential control system vulnerabilities



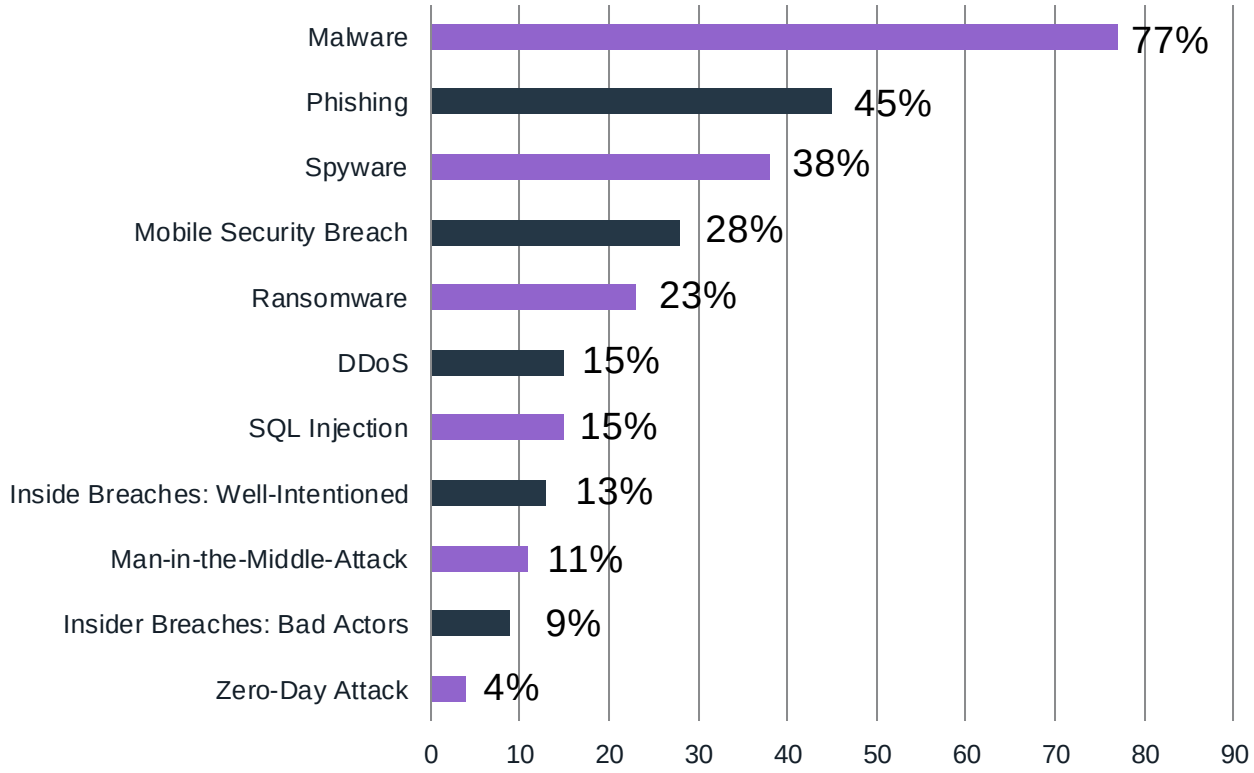
Опасения оправданы - 77% организаций сообщают, что в работе АСУ ТП/ICS возникли нарушения безопасности (и 51% в прошлом году). Серьезные последствия от этих нарушений повлияли на способность соответствовать требованиям стандартов с поддержанием функциональности и безопасности сотрудников.

OT угрозы

Обнаруженные угрозы в 2018



Типы обнаруженных угроз в 2018

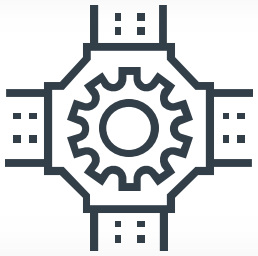


https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf

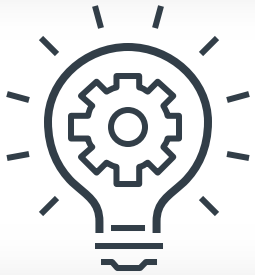
Fortinet Critical Infrastructure Perspective

Fortinet стремится улучшить национальную безопасность и экономическую конкурентоспособность стран предлагая решения для обеспечения безопасности критически важных инфраструктур



- Критические инфраструктуры стали местом холодной войны 21-го века
- Операционные технологии и ИТ-решения сходятся (конвергенция)

Различия в технологиях, архитектурах и культуре требуют специальных знаний и решений



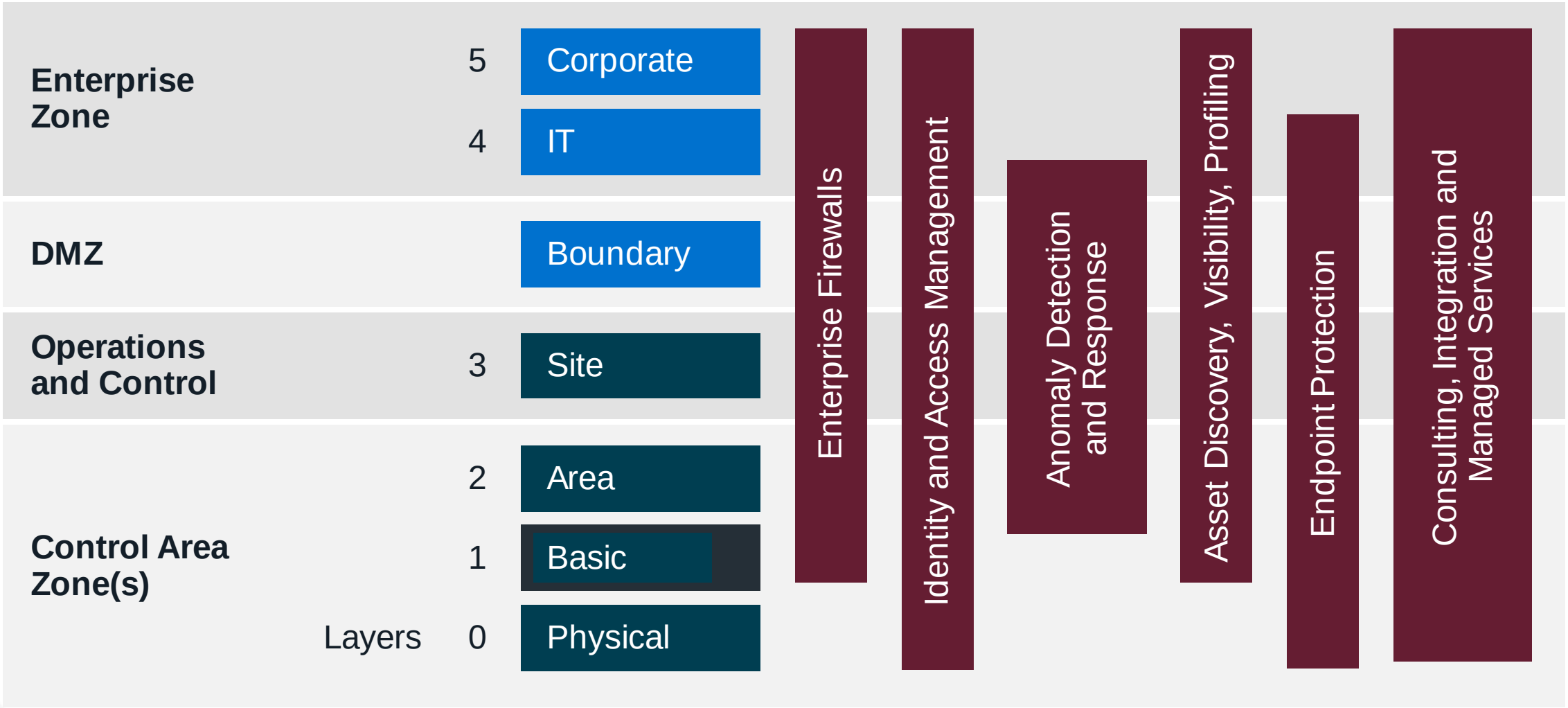
- У Fortinet есть новые решения соответствующие растущему спросу
- Техническая экспертиза Fortinet создана и интегрирована по всему миру

Мы стремимся к стратегическим альянсам с канальными партнерами и производителями ОТ, а также к тому, что необходимо обозначить нашу расширенную роль на рынке.

- Используйте существующие связи и создавайте новые
- Консалтинговые услуги и предпродажная поддержка доступны

FORTINET

Модель Purdue с наложенными защитными мерами



Fortinet Success in Cybersecurity

Инвестиции в инновации

Headquarters
Sunnyvale

$1.8B – 2017
(billings)

3.4M+ Shipments

Channel First

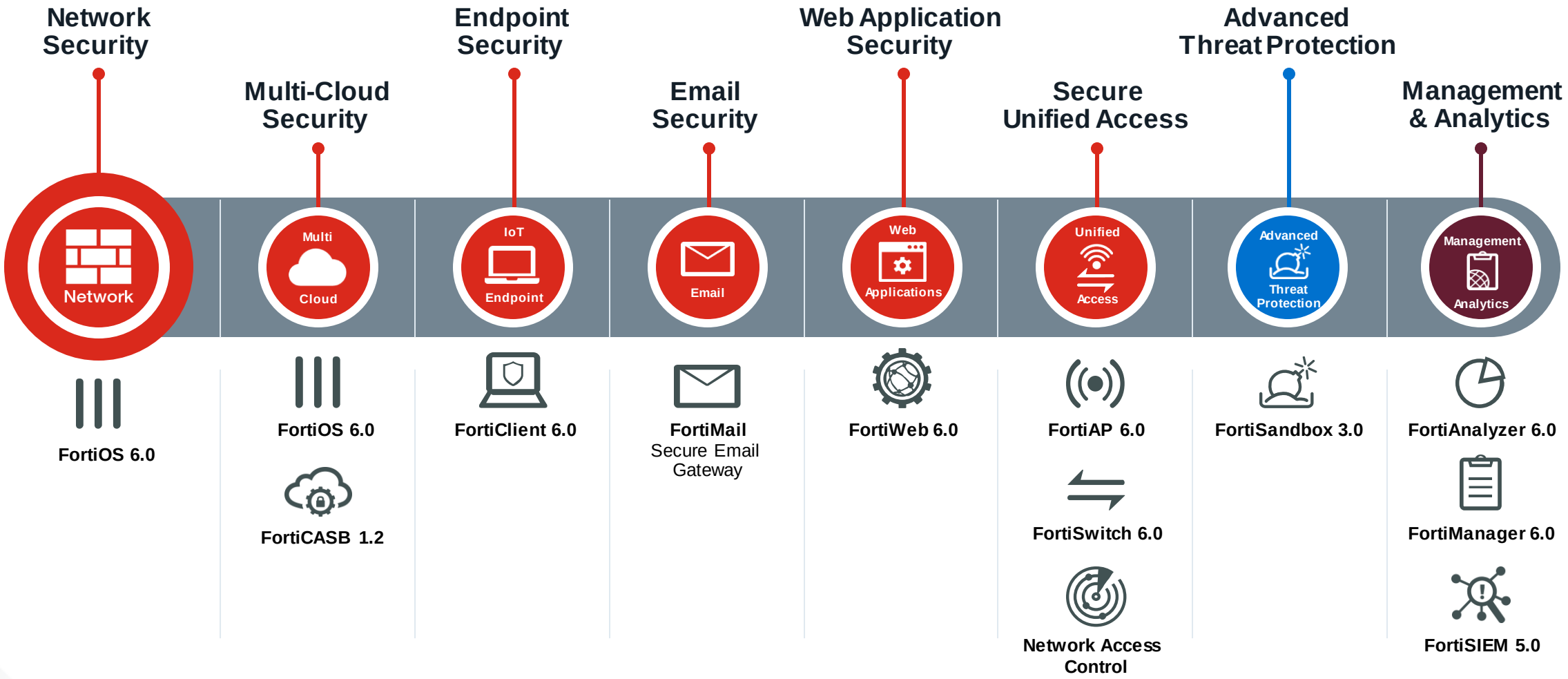
5,100 Employees

One of the Largest Public Cybersecurity companies

340,000 Customers

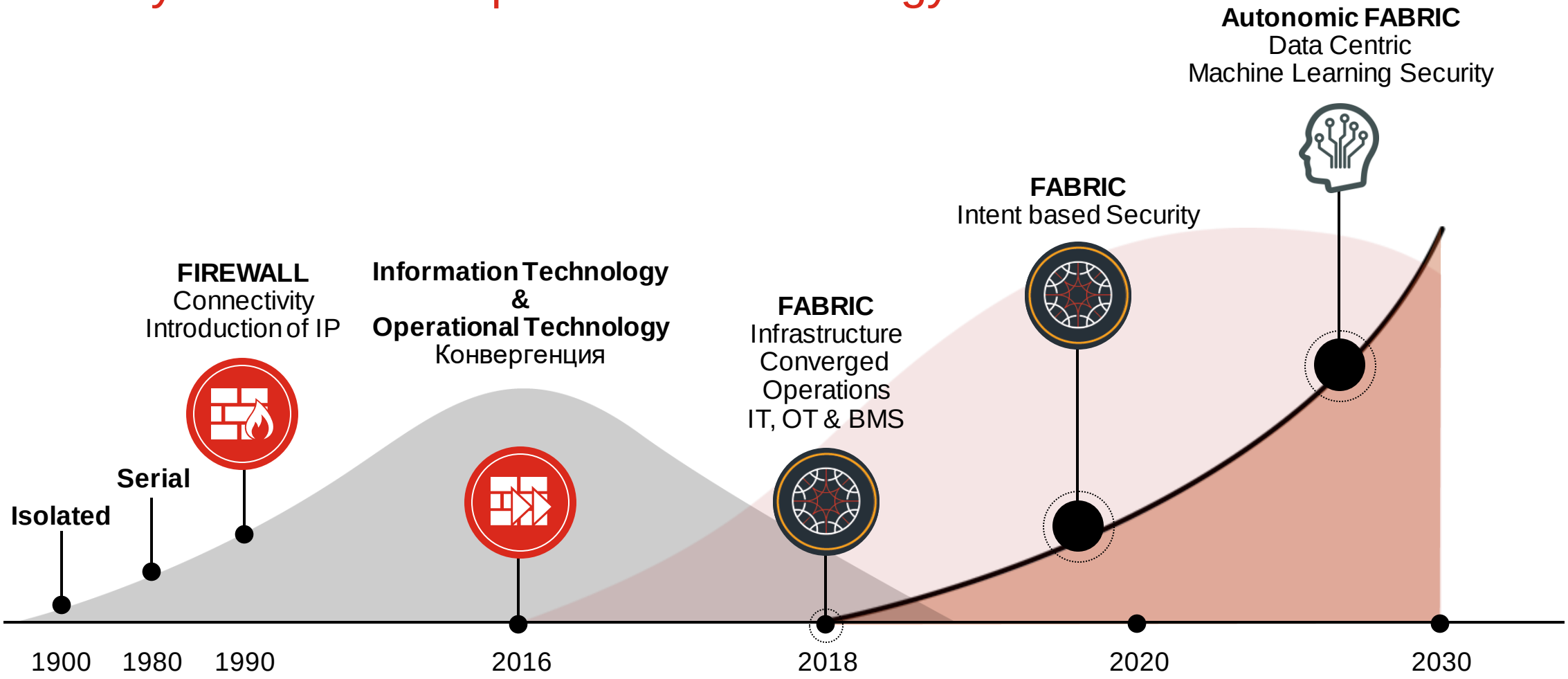
Patents 467

Лучший портфель решений в отрасли

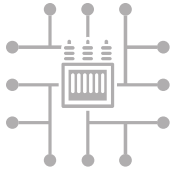


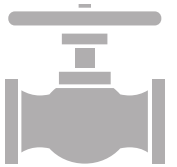
Physical to Digital Evolution of Operational Technology Environments

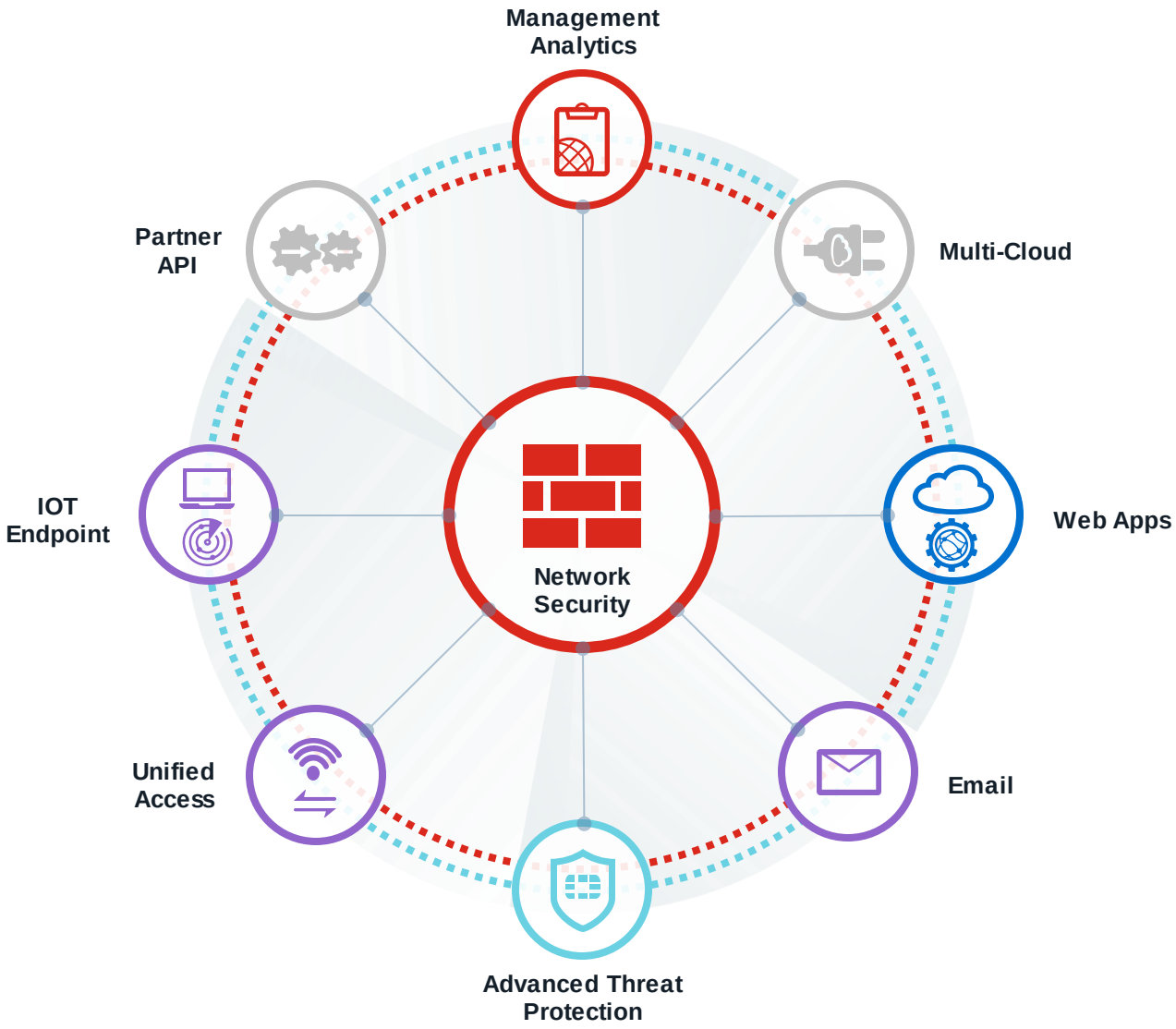
Security Evolution of Operational Technology



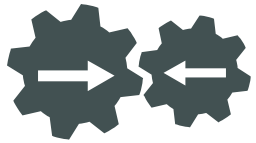
Fortinet Security Fabric для защиты OT







Открытая экосистема



FABRIC API

- Партнеры Fabric охватывают широкий спектр сетевых технологий от IoT до облаков
- Партнеры пишут код с использованием Fabric API для интеграции с продуктами Fortinet
- Fortinet официально подтверждает поддержку интеграции

DEVOPS

- Созданные в Fortinet скрипты DevOps, автоматизируют обеспечение безопасности через FortiManager
- Полная автоматизация функциональных возможностей FortiGate и управление конфигурацией
- Легко выполняются, доступны в FNDN & GitHub

FABRIC CONNECTORS

- Fabric Connectors обеспечивают глубокую интеграцию с компонентами экосистемы клиента, где критически важна автоматизация безопасности
- Существуют различные типы Fabric Connectors – список постоянно пополняется
- Активируются простым нажатием на GUI

OT специализированные решения

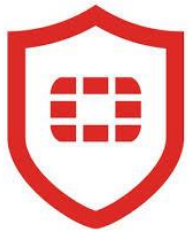
Железные решения

FortiGate Rugged 60D

FortiGate Rugged 90D

- Line of Rugged Firewalls
- Line of Rugged Switches
- Line of IPS-rated wireless access points

Информация об угрозах



- Industrial Control Services
- OT-specific protocols
- OT-specific vulnerabilities
- More signatures than any other cybersecurity vendor

Команда

- Experienced professionals
- Decades in Industry
- Decades of customers

FORTINET

IPS/ Application Control для OT

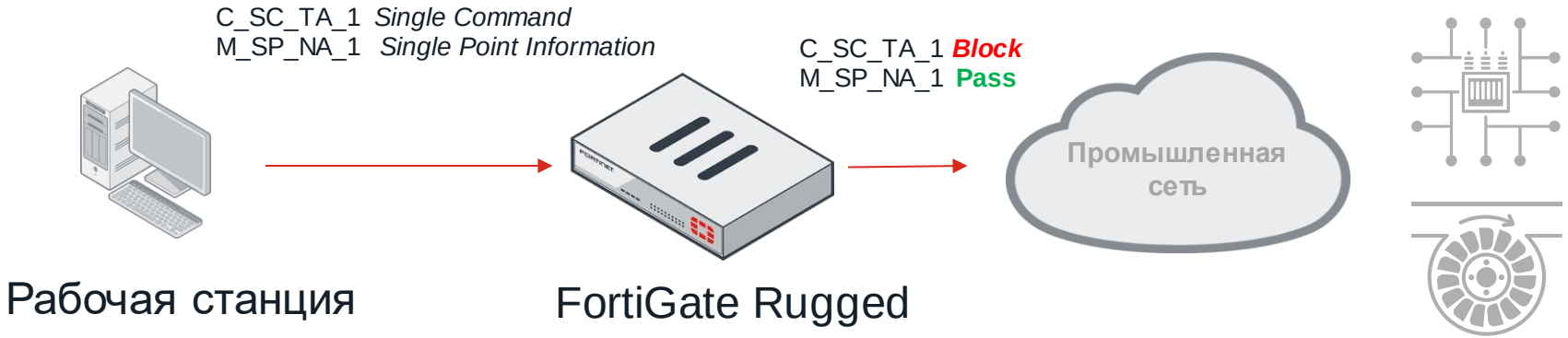
Некоторые из поддерживаемых

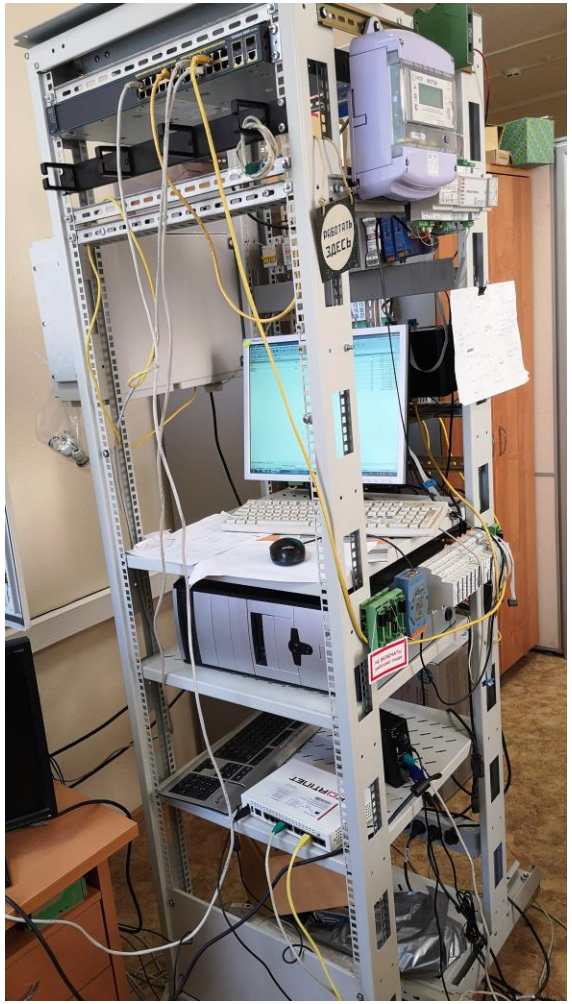
- BACnet
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- HART
- IEC 60870-6 (TASE 2) /ICCP
- IEC 60870-5-104
- IEC 61850
- LONTalk
- MMS
- Modbus
- OPC
- Profinet
- S7
- SafetyNET
- Synchrophasor

Поддерживаемые приложения и производители

- 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)
- Простая работы с кастомными сигнатурами (синтаксис похож на Snort)

Разработка сигнатур

Edit Application Signature

Name IEC104.1000-1500.Information.Transfer

Comments

Signature

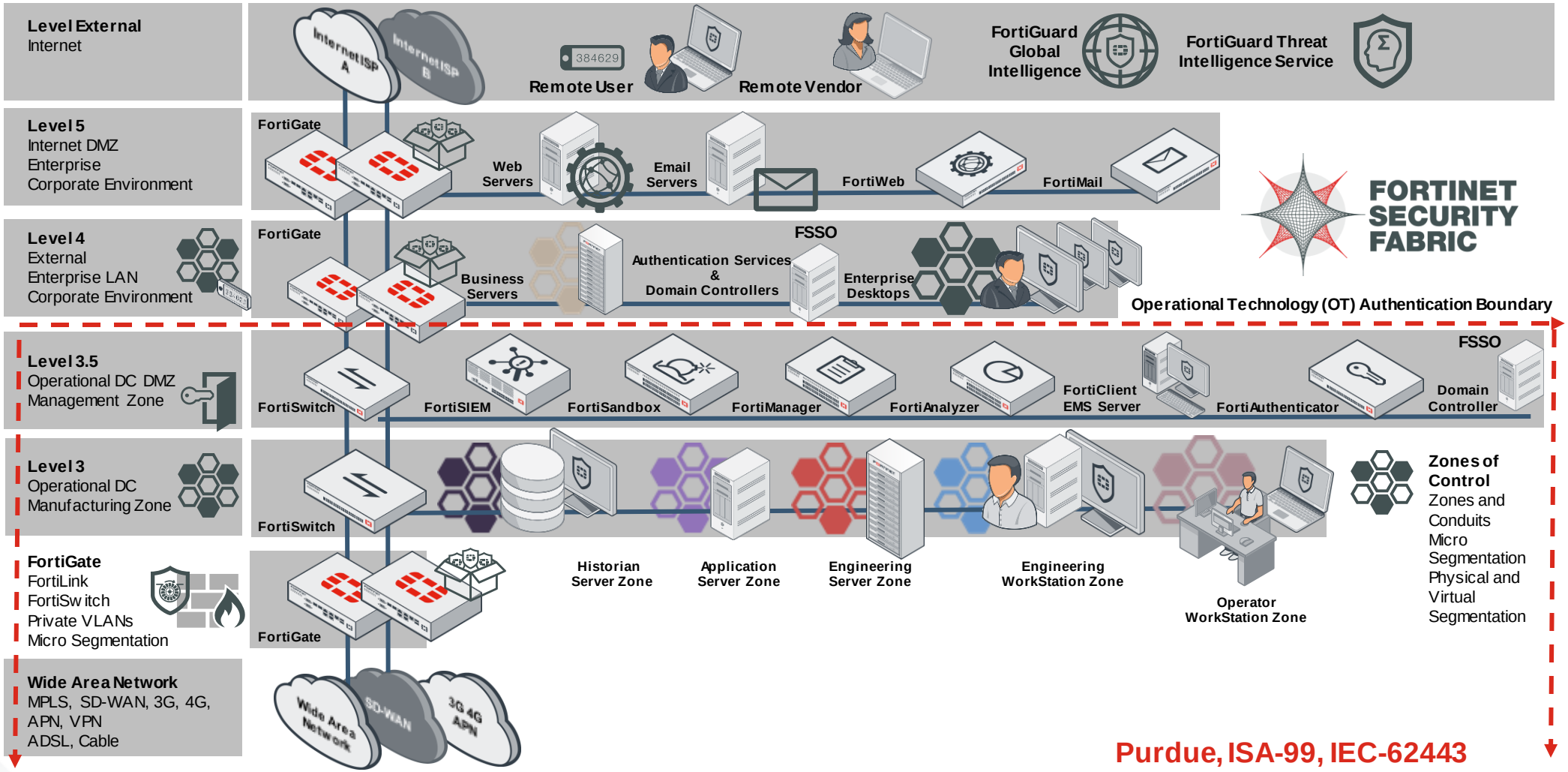
```
F-SBID( --attack_id 1002; --name "IEC104.1000-1500.Information.Transfer"; --protocol tcp; --app_cat
26; --default_action pass; --service iec104;  --dst_port 2404; --flow bi_direction; --pattern |68|;
--context body; --within 1,context; --byte_test 1,~,1,1,relative; --pcre "/(\x2d|\x2e|\x2f|\x30|\x31|
\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;)
```

Кастомные сигнатуры помогают детально декодировать промышленный протокол

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

Применение устройств Fortinet в модели Purdue




FORTINET

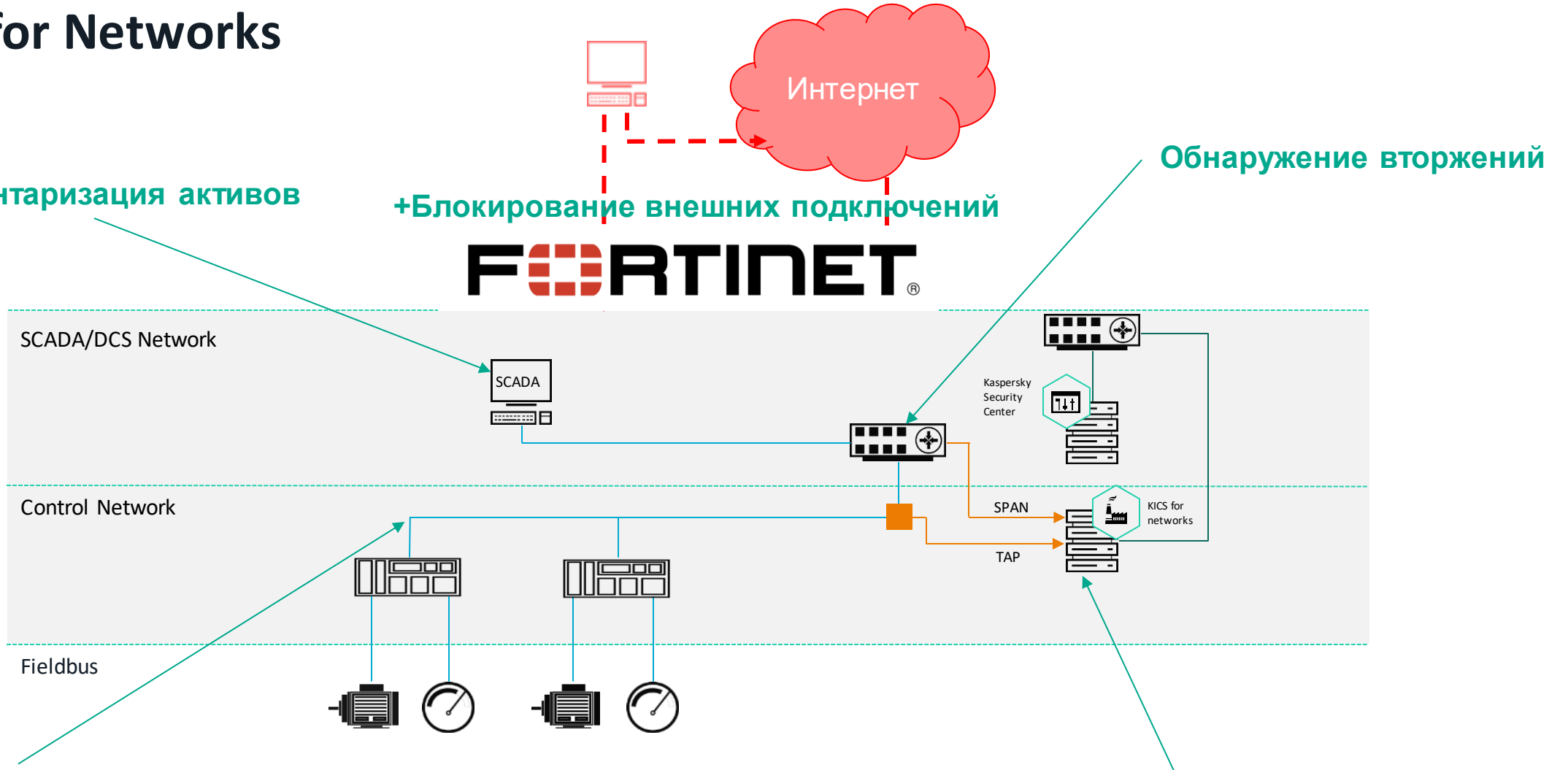
kaspersky

Kaspersky
Industrial
CyberSecurity

Кибербезопасность промышленных систем

Петухов Алексей
Руководитель направления защиты промышленных систем

+ KICS for Networks



kaspersky

Благодарю!

Петухов Алексей
Руководитель направления защиты промышленных систем
Alexey.Petukhov@Kaspersky.com
+7 963 686 07 83

Ics.kaspersky.com