kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Даниил Тамеев

Руководитель направления по работе с промышленными компаниями, Fortinet Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

В ногу со временем: современные решения на страже практической безопасности промышленного сегмента

Даниил Тамеев

Руководитель направления по работе
с промышленными компаниями

Fortinet Russia

О чем пойдет речь

DIGITAL

SECURITY

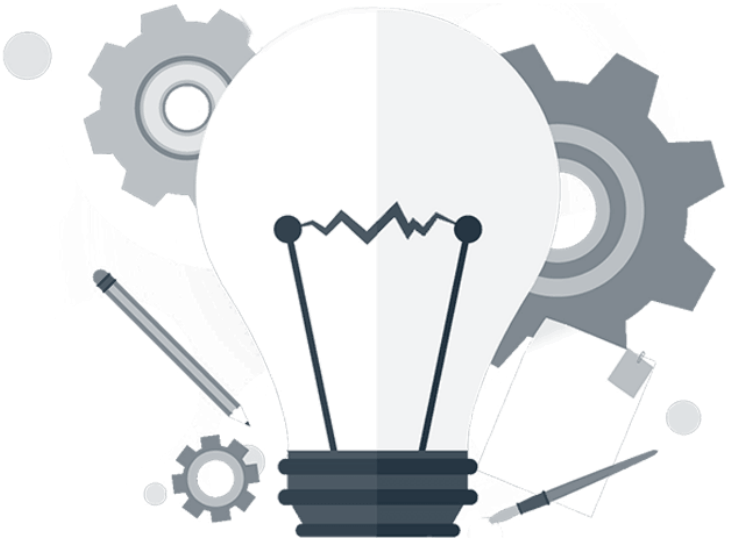
SOLUTIONS

О чем пойдет речь

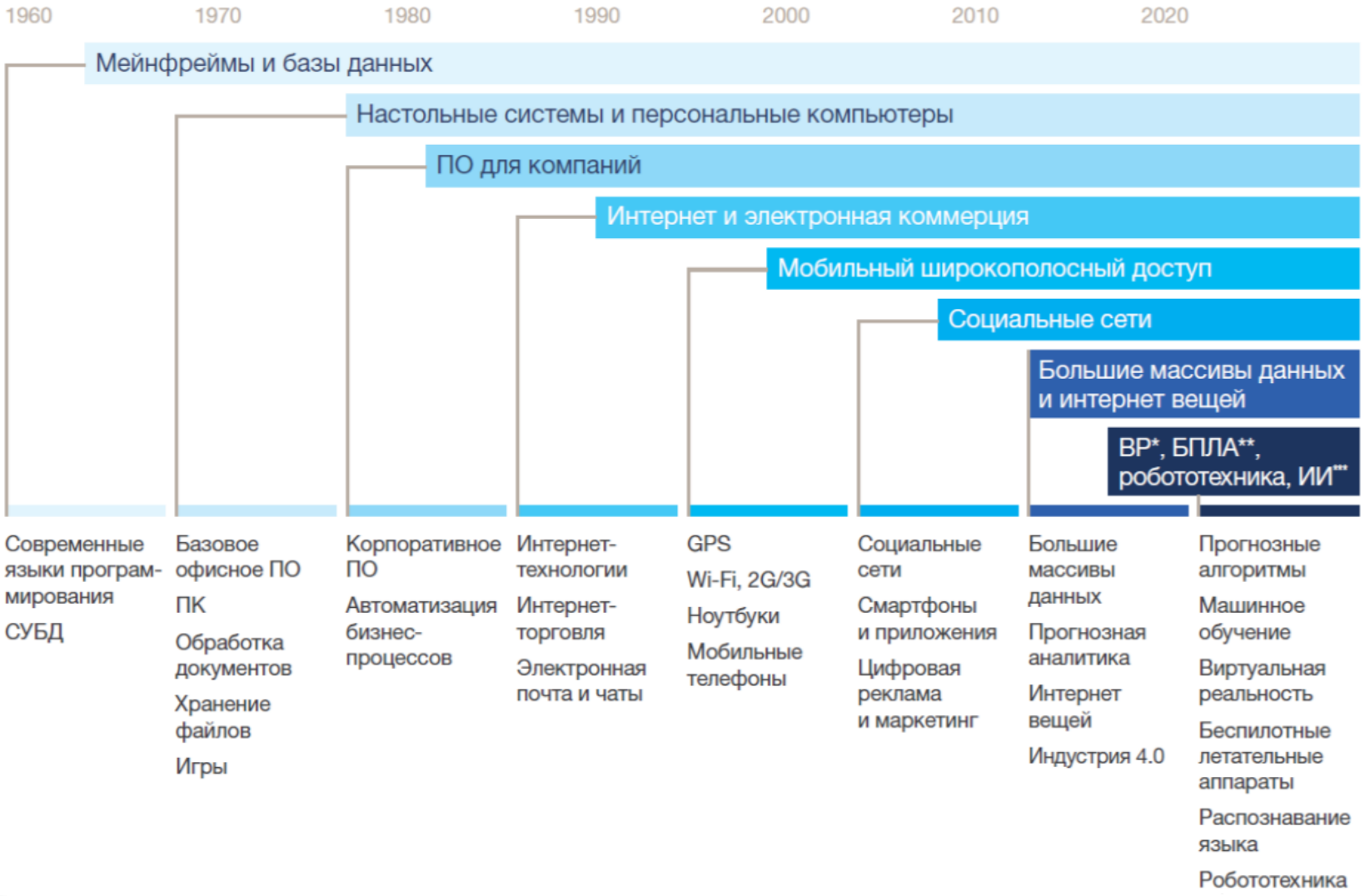
DIGITAL

SECURITY

SOLUTIONS

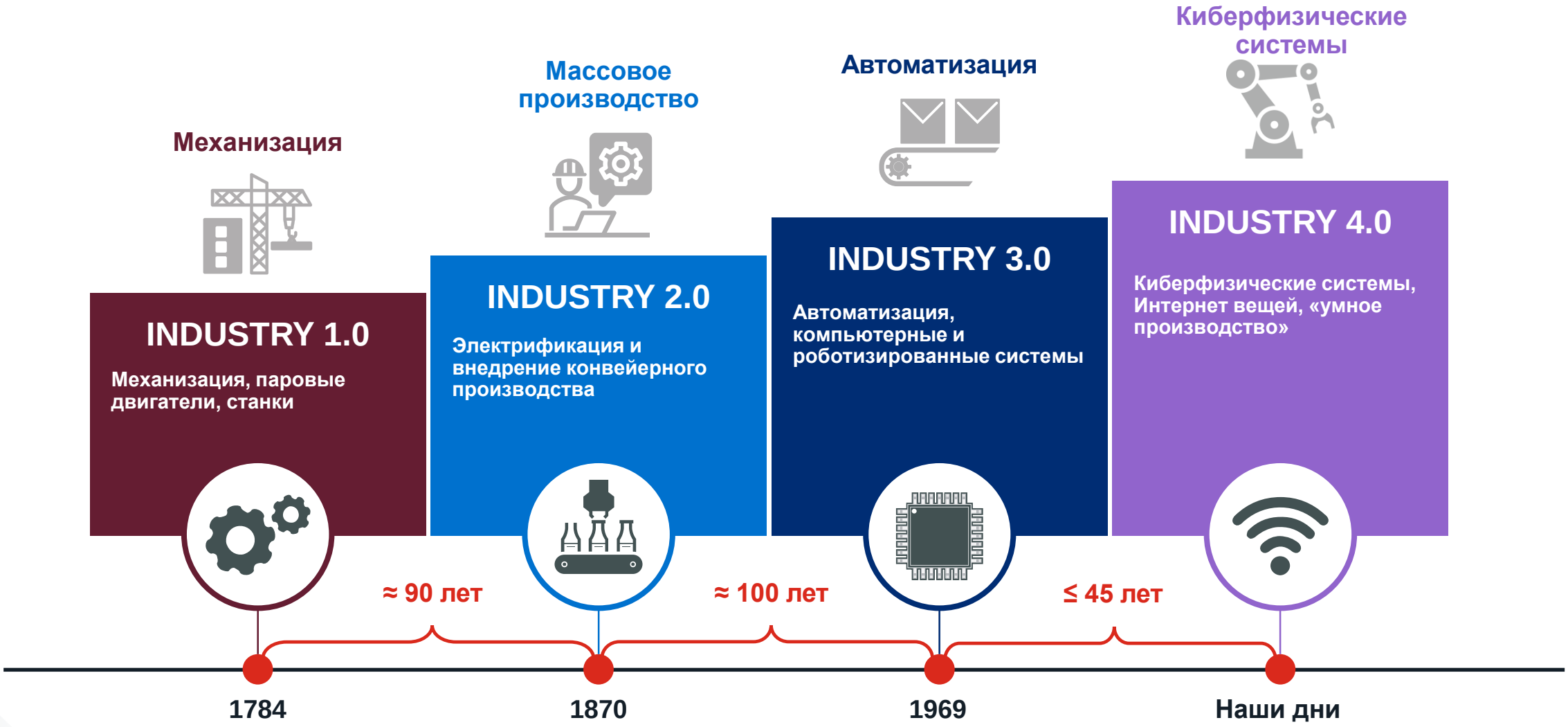


Цифровая экономика формируется под влиянием ускоряющихся волн инноваций



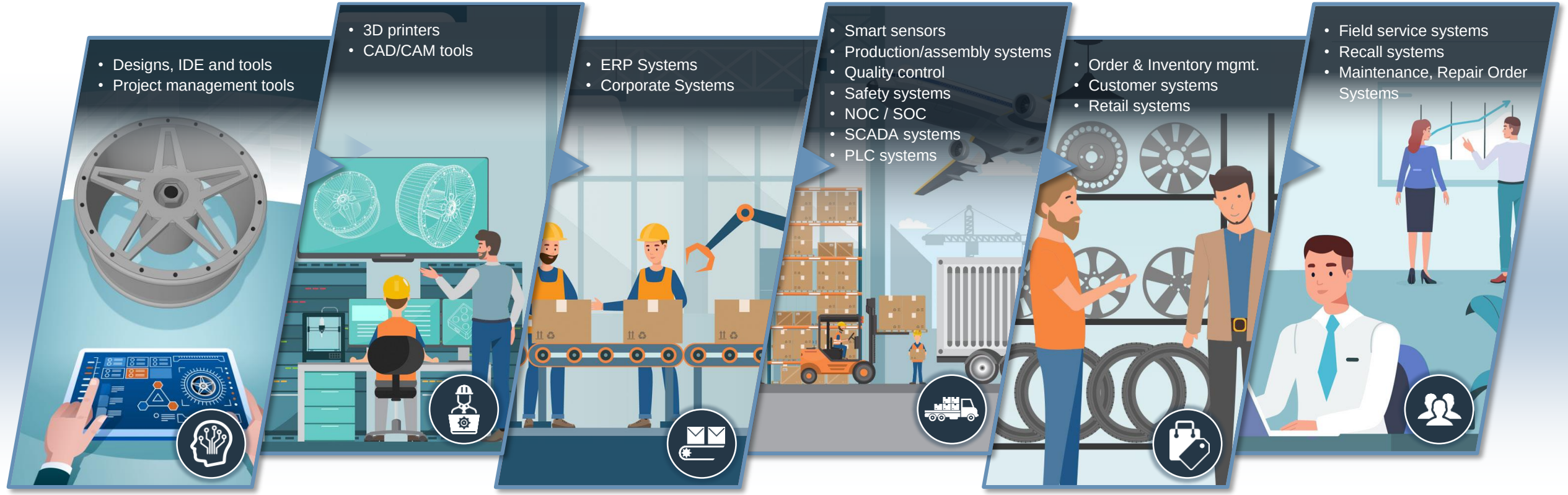
FORTINET

Индустрия 4.0 - инновационные технологии в промышленности и производстве



Цифровизация всей производственной цепи

Специфичные для сегмента ИТ и ОТ цели и решения



Разработка решений | **Инженерные прототипы** | **Линия производства** | **Хранение и распространение** | **Продажи** | **Корпоративные системы**

FORTINET

DX

интеграция цифровых технологий во все сферы бизнеса, приводящая к фундаментальным изменениям в том, как работают предприятия и как они приносят пользу клиентам

[Digital Transformation]

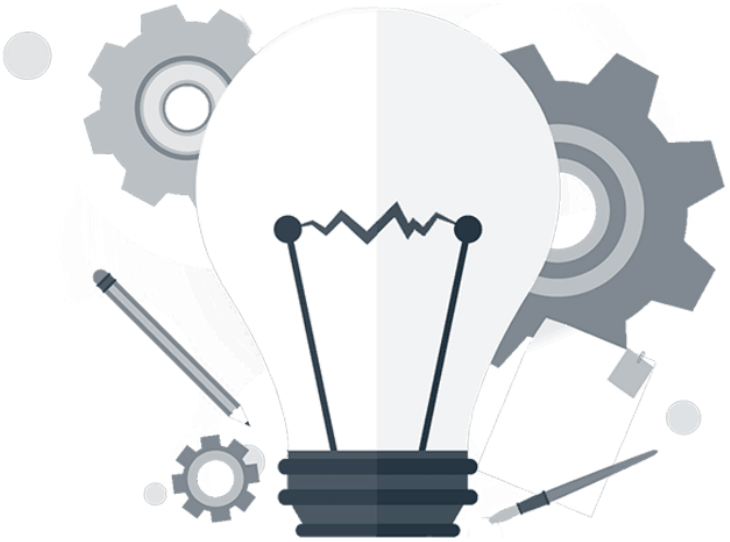
FORTINET

О чем пойдет речь

DIGITAL

SECURITY

SOLUTIONS



ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ УСПЕШНОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

ЗАЩИТА ДАННЫХ

Вне зависимости от местонахождения в сети, состояния и формата

БЕЗОПАСНОСТЬ ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Расширение защиты ИТ на промышленные сети

ГИБКИЕ ПРОЦЕССЫ БЕЗОПАСНОСТИ

Защита конвергентной, облачной и гибридной инфраструктуры

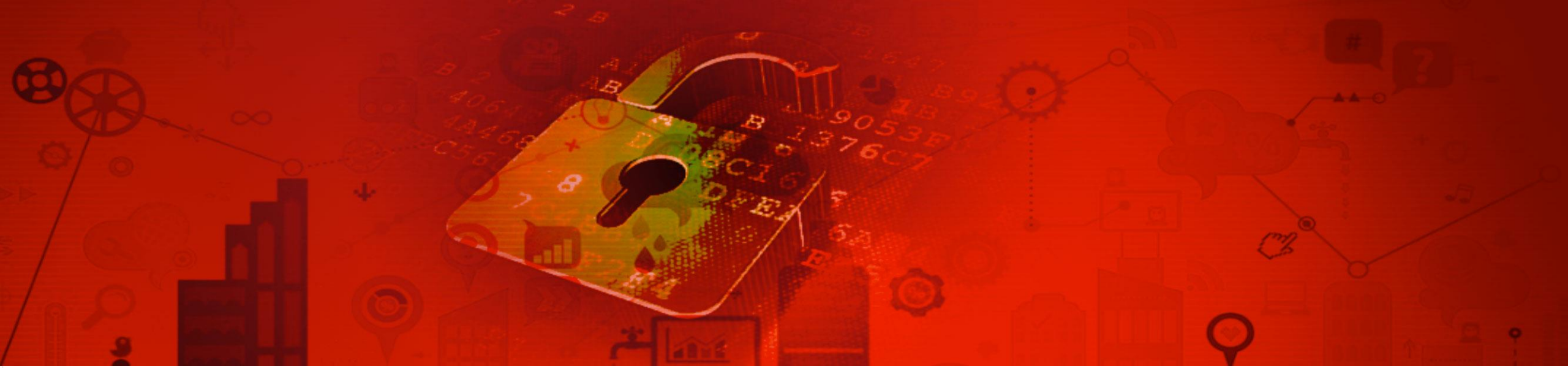
СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

В рамках стратегии управления рисками и отраслевых требований

РАСШИРЕНИЕ ВИДИМОГО ГОРИЗОНТА УГРОЗ

Требует инноваций и автоматизации

FORTINET



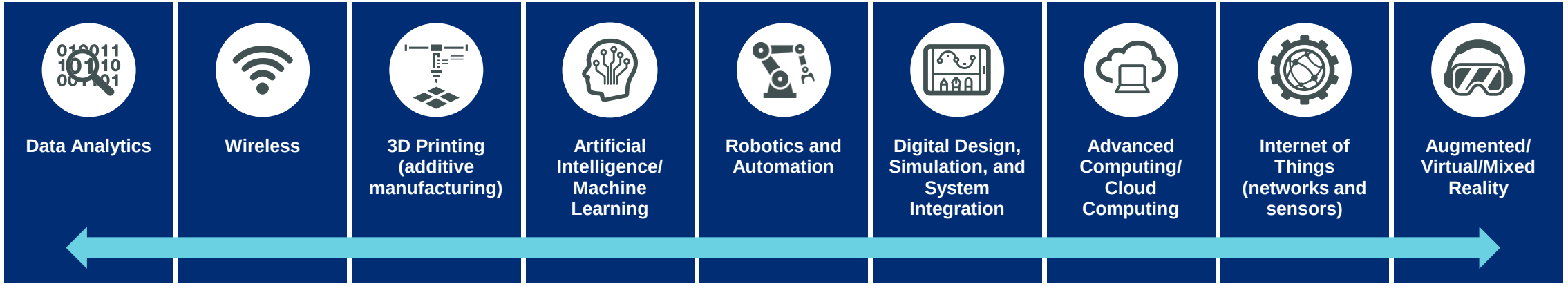
SX

это интеграция безопасности во все области цифровых технологий – архитектура безопасности, которая обеспечивает широту, погружение и автоматизацию защиты

[Security Transformation]

FORTINET

Технологии используемые для поддержки и продвижения Индустрии 4.0



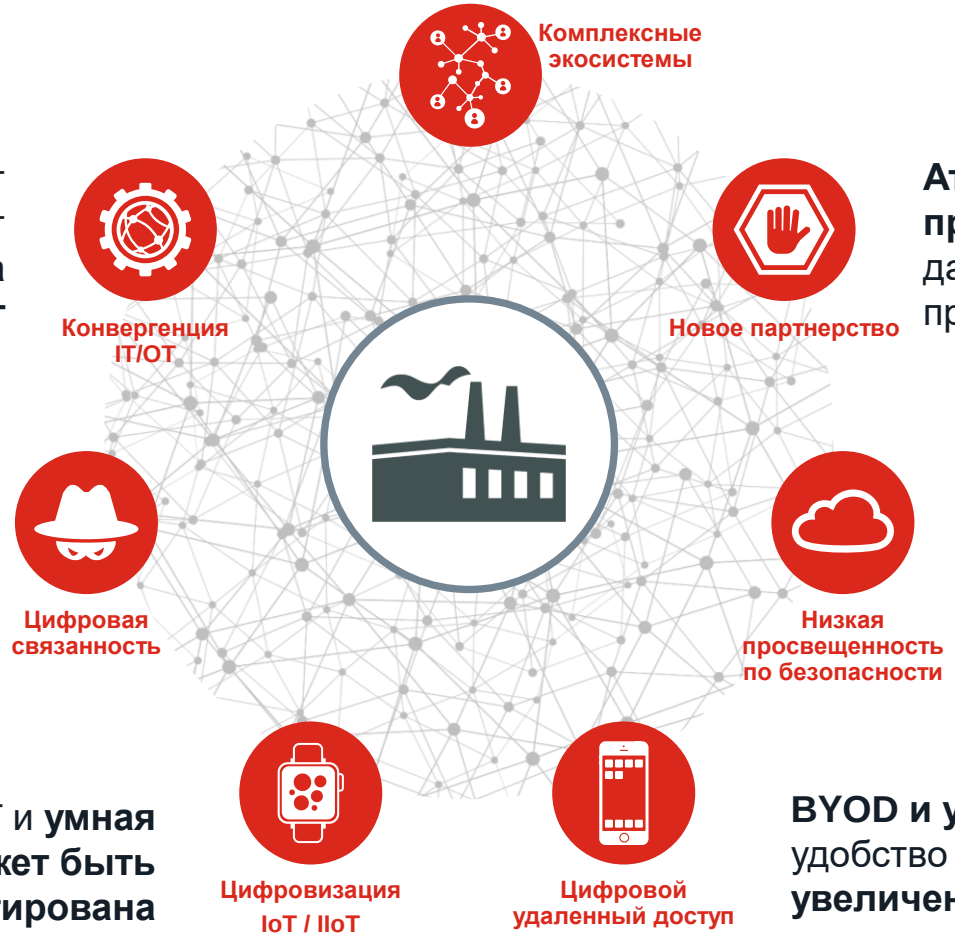
Безопасность имеет критическое значение при использования технологий

Преимущества использования инновационных технологий:

- Улучшает близость и знания клиентов, доступ к более релевантным данным
- Повышает маневренность при развитии, а также опережении и вытеснении конкурентов

Примеры увеличения кибер-риска для современной промышленной компании

Любые **пробелы в безопасности сетей контрагентов** могут служить точками доступа для хакеров



АСУ ТП обеспечивает автоматизацию, но открывают **дверь для хакерских атак на технологический сегмент**

Атаки типа «отказ в обслуживании» **могут привести к сбою в цепочке поставок**, даже если ваша организация не является прямой целью атаки.

Хакеры формируют из устройств подключенных к Интернету «армию» **IoT для подавления целевых серверов вредоносным трафиком**

Без адекватных мер безопасности и резервного копирования данных **информация в облаке может быть потеряна или украдена**

Ресурсы ИИ, устройства IoT и **умная инфраструктура может быть взломана и скомпрометирована**

BYOD и удаленный доступ повышает удобство работы, но **несет за собой увеличение количества векторов атаки**.

FORTINET

Как можно снизить кибер-риски?

Видимость горизонта цифровых атак

Новые технологии приводят к новым рискам.

Необходима **широкая видимость горизонта угроз** и проактивное обнаружение.

Защита от сложных и целевых угроз

Количество угроз и вредоносного ПО неуклонно растет.

Необходима **комплексная защита на всех уровнях** – устройств, сети, приложений.

Структурировать и утвердить архитектуру безопасности

Сложность - враг эффективности.

Необходимо **автоматически предотвращать, обнаруживать и реагировать** на угрозы.

Упростить соответствие требованиям

Международное, региональное, отраслевое и государственное регулирование.

Обеспечив полноценную **защиту** - станет **проще соответствие требованиям**.

FORTINET

О чем пойдет речь

DIGITAL

SECURITY

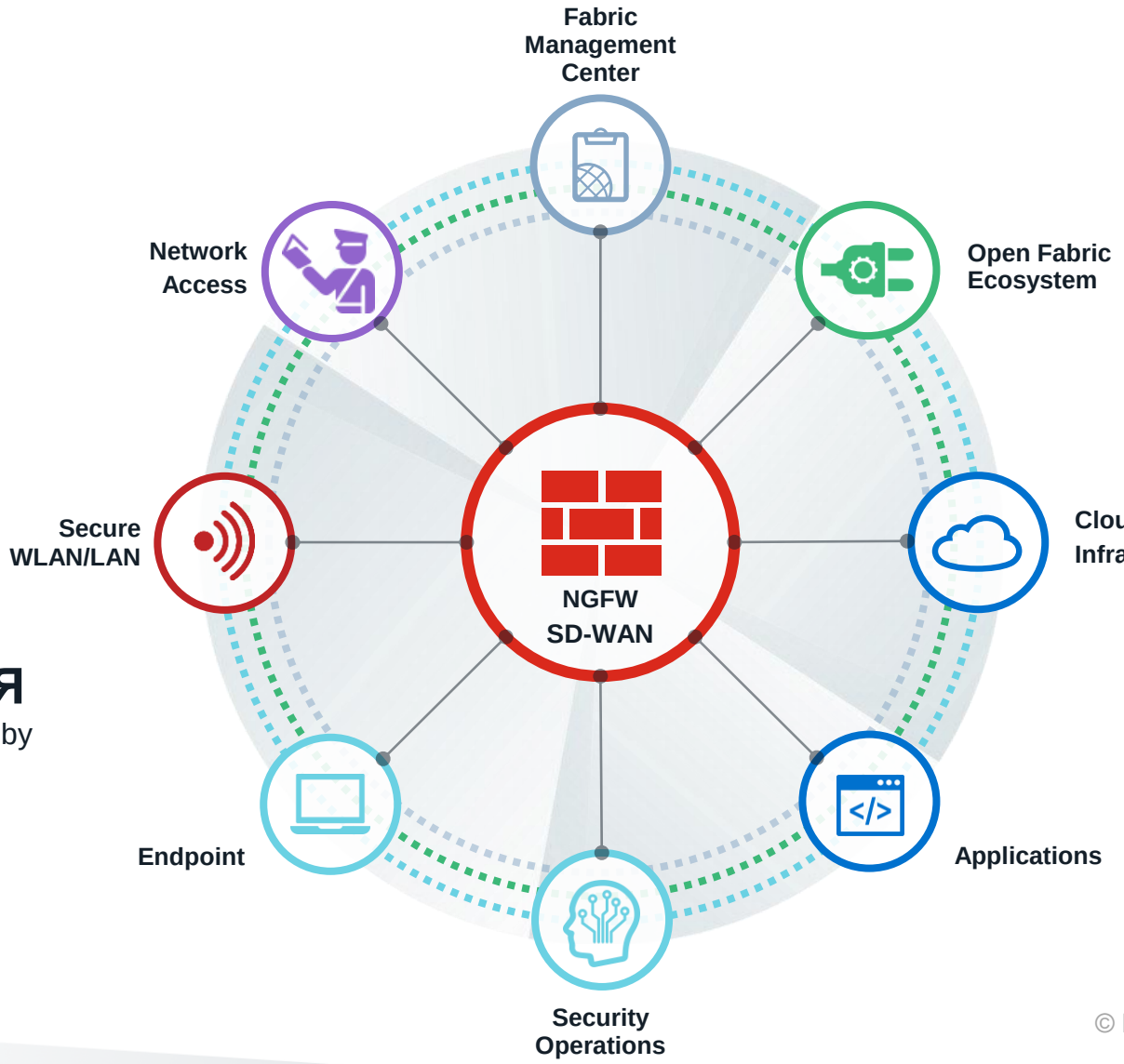
SOLUTIONS

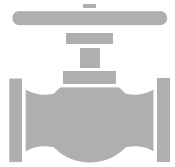
Fortinet Security Fabric для защиты OT

ШИРОТА
Visibility of the entire digital attack surface

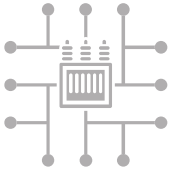
ИНТЕГРАЦИЯ
Protection across all devices, networks, and applications

АВТОМАТИЗАЦИЯ
Operations and response driven by Machine Learning










Особенности решений для OT

Аппаратная часть

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
- OT-specific sandbox, deception solutions

Профильная команда

- Experienced professionals
- Decades in Industry
- Decades of customers

FORTINET

Когда вендор рассказывает о своих решениях

Партнеры и интеграция решений

ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

ПАРТНЕРЫ ПО РЕШЕНИЯМ И ИНТЕГРАЦИИ

Fortinet OT Customers

Oil & Gas

bp
Shell
Exxon
TOTAL
Dominion Energy
ontras Gastransport GmbH
VEOLIA
HEDNO
energex
Verbundnetz Gas AG
CELG
BS NETZ
eog resources
EDF
وقود WOQOD

Electrical & Utilities

conEdison
PG&E
AVANGRID
КИЇВЕНЕРГО
NBU New Braunfels Utilities
Powercor AUSTRALIA
RWE The energy to lead
SAM HOUSTON ELECTRIC COOPERATIVE
Eidsiva
CONELECTRICAS R.L.
RED ELÉCTRICA DE ESPAÑA
AIK
SPgroup
DiCLE ELEKTRİK

Water

suez
Sydney WATER
هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority
Burbank Water and Power
Yarra Valley Water
City West Water
Barwon Water

Manufacturing

Mercedes-Benz
BMW
Volkswagen
BOSCH
GLENCORE
RHEINMETALL DEFENCE
AIR LIQUIDE
SANDVIK

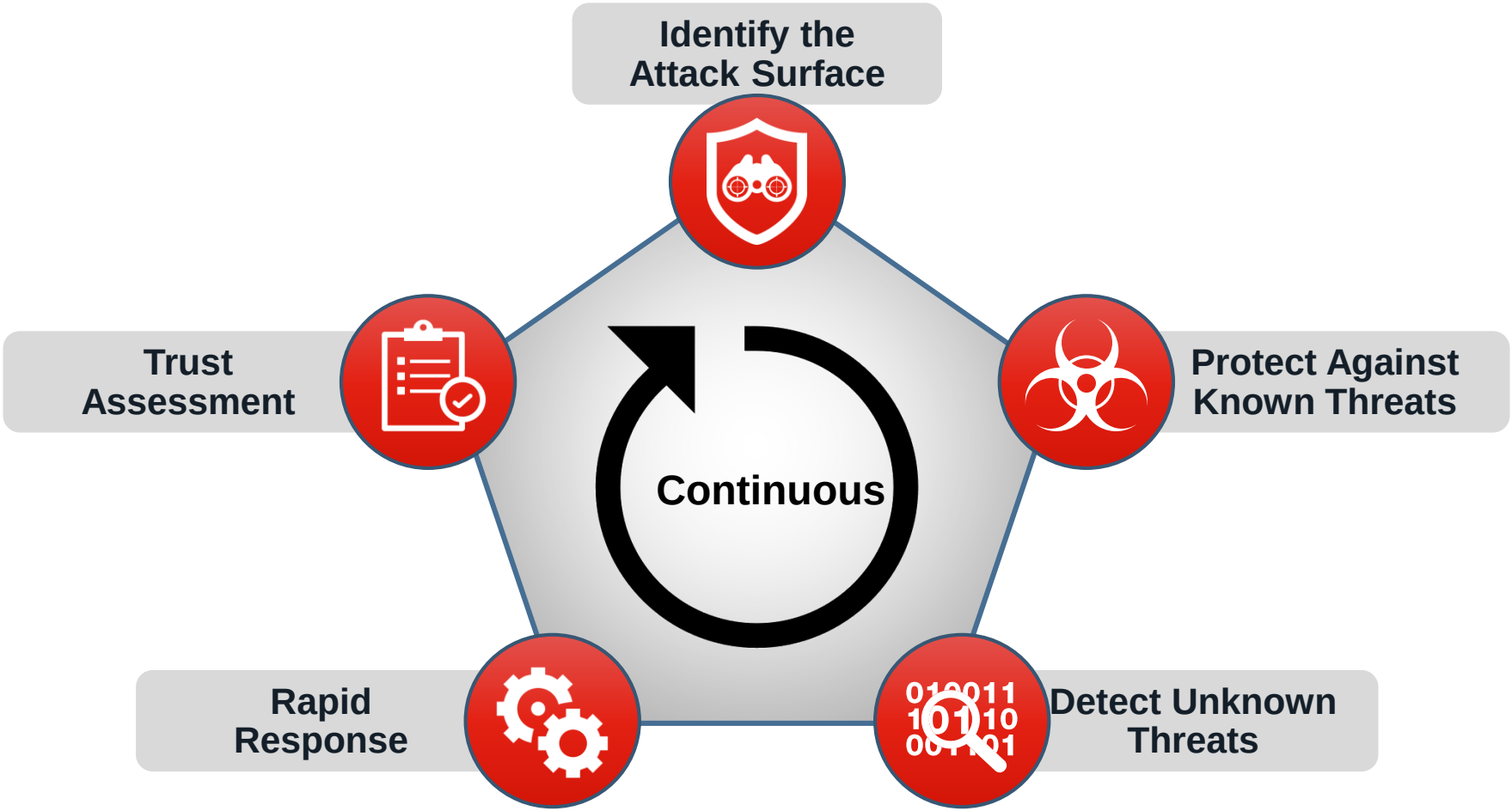
Transportation

DHL
FedEx
DB
CSX
AIRBUS
MAERSK
Hapag-Lloyd

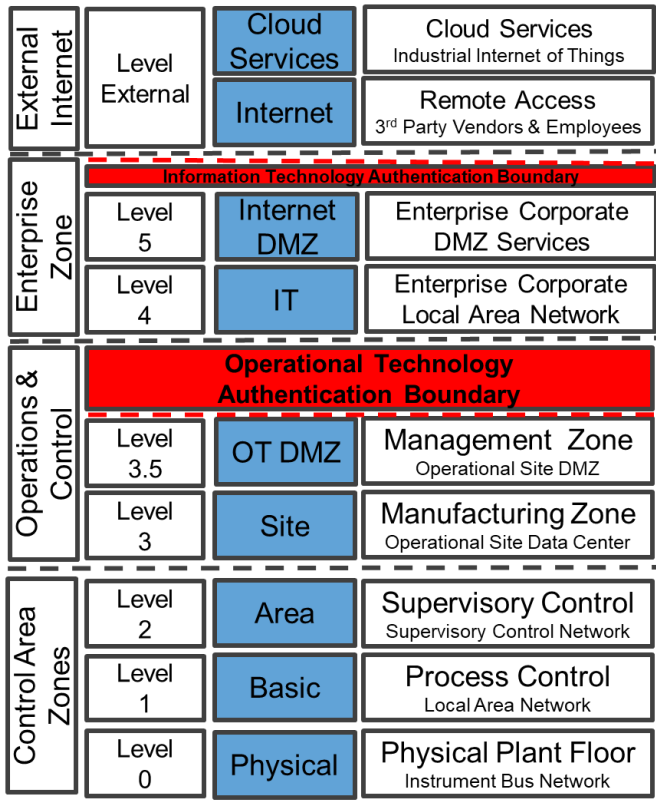
FORTINET

Классическая модель безопасности

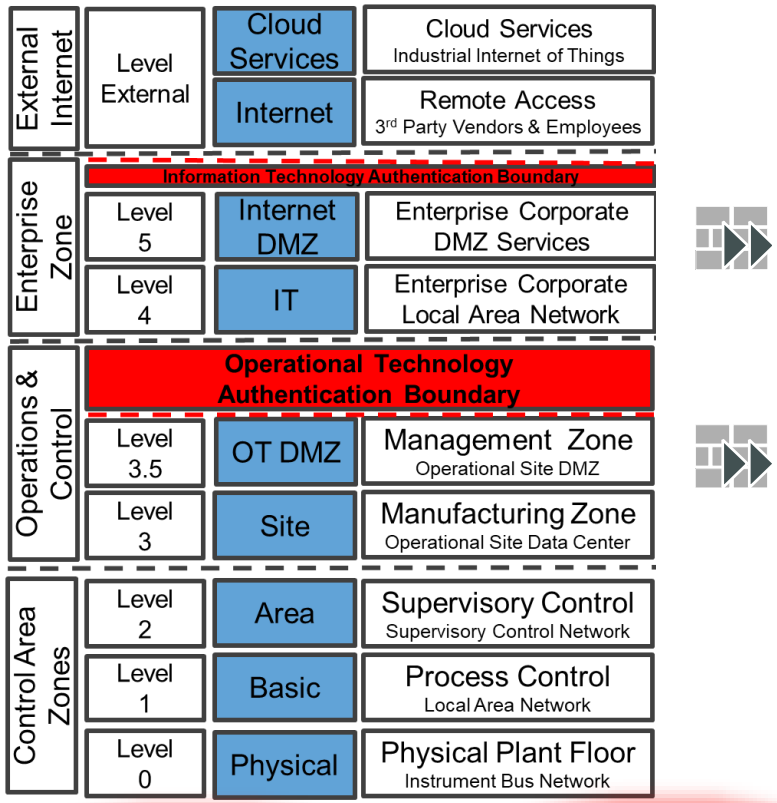
NIST Model



Путь к безопасности OT-инфраструктуры



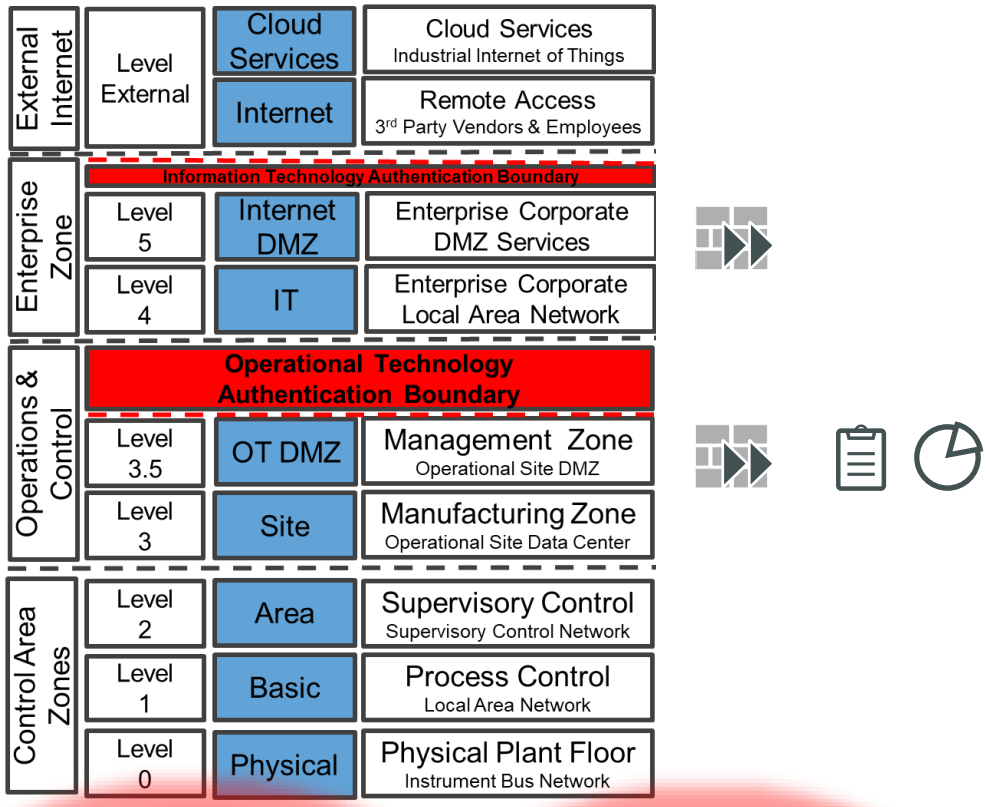
Путь к безопасности OT-инфраструктуры



Step 1. Basic Visibility & Control

- NGFW w/ OT protocol & vulnerability protection

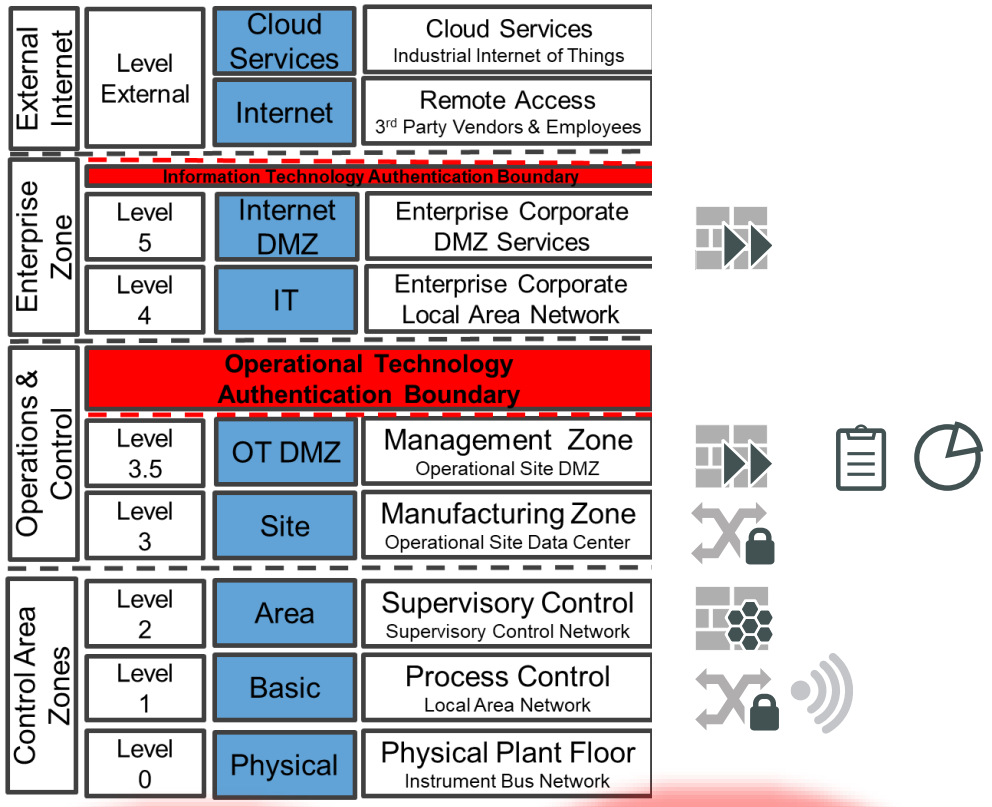
Путь к безопасности OT-инфраструктуры



Step 2. Visibility & Configuration

- Add Management & Analytics

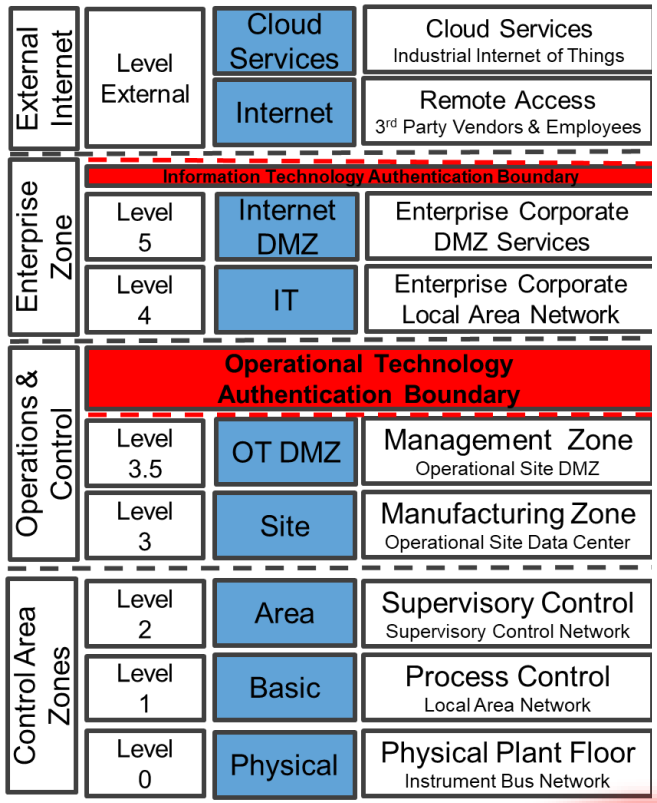
Путь к безопасности OT-инфраструктуры



Step 3. Internal segmentation

- OT Segmentation Firewall w/ OT-specific protections
- Industrial Switching & Wireless

Путь к безопасности OT-инфраструктуры

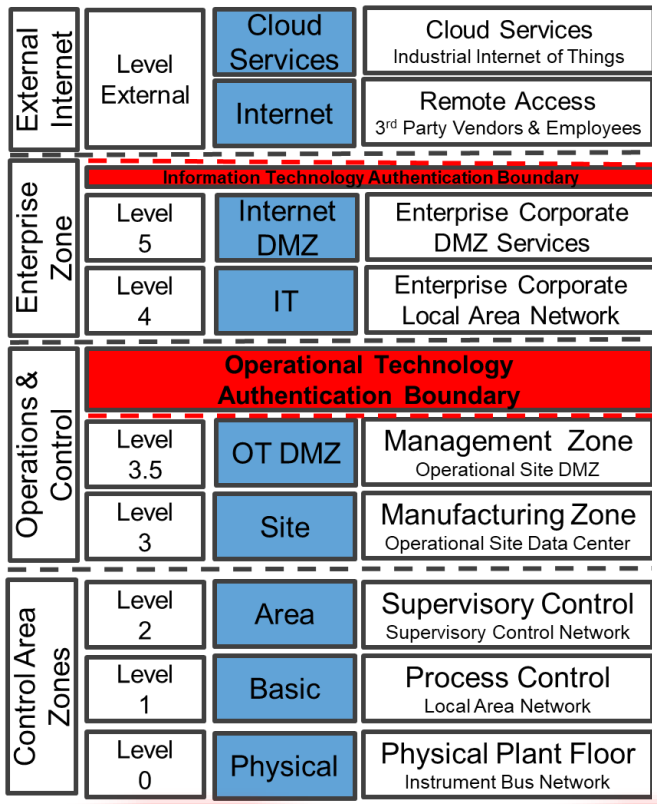


Step 4. Access Control Internal segmentation

- User Authentication (with MFA)
- Device Authentication with NAC
- Device Protection, Detection and Response (EDR)
- Insider Threat Detection (UEBA)

FORTINET

Путь к безопасности OT-инфраструктуры

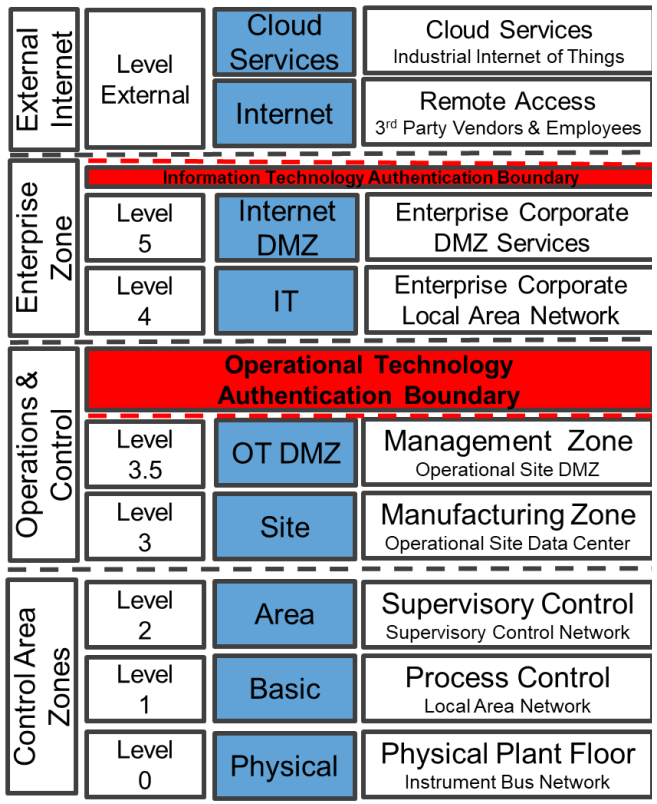


Step 5. Cloud Security

- Add Cloud WAF
- Secure Cloud-based Apps
- Secure remote access

FORTINET

Путь к безопасности OT-инфраструктуры

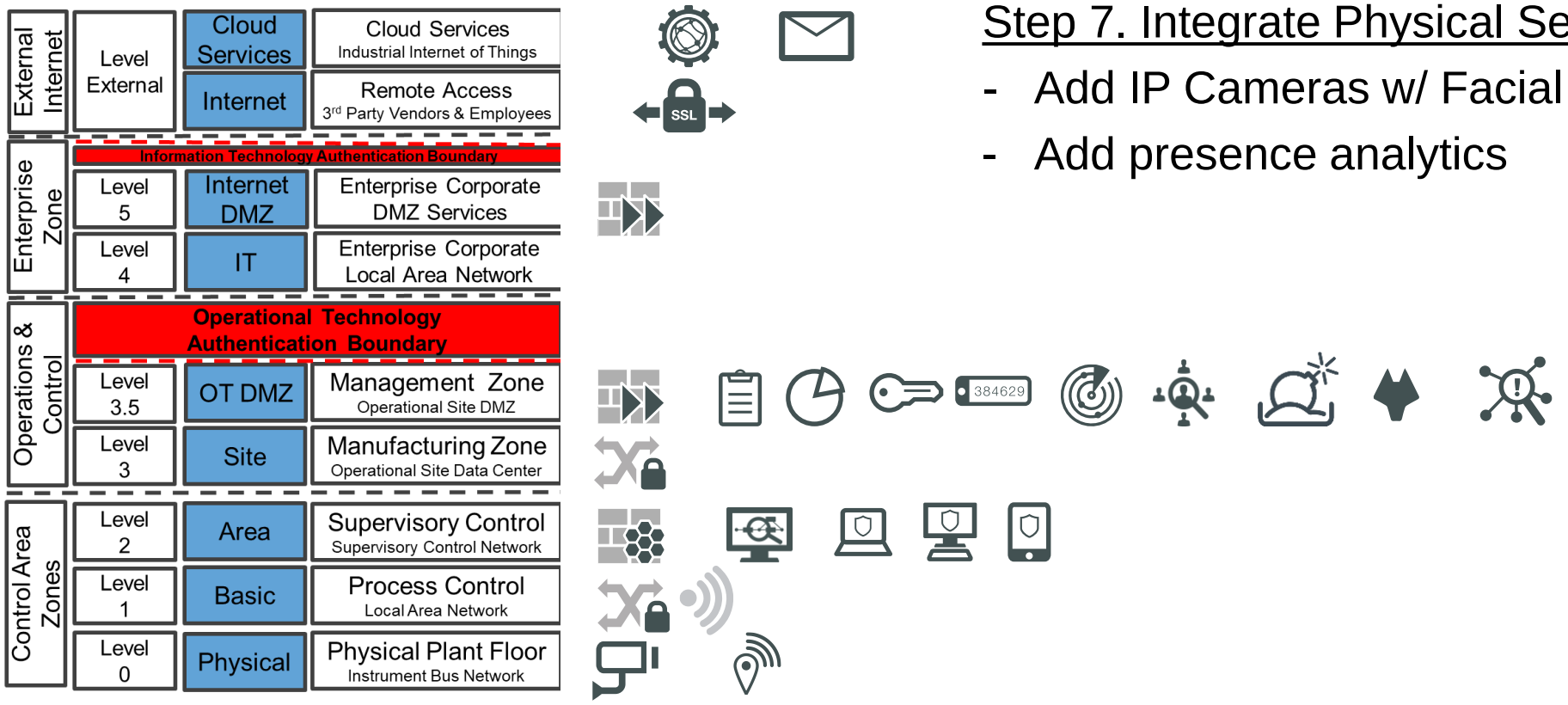


Step 6. Defend Against Unknowns

- Add Sandbox
- Add Deception Technologies
- Add SIEM

FORTINET

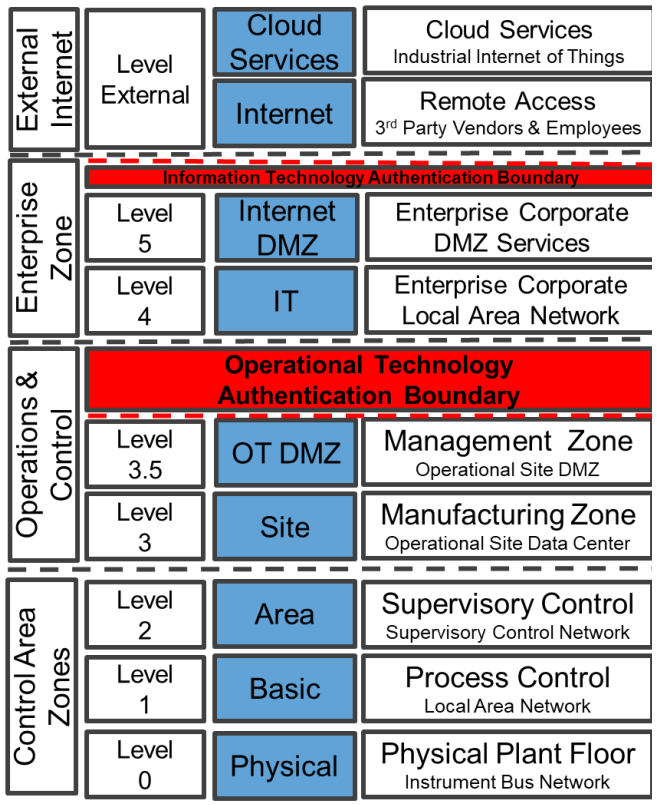
Путь к безопасности OT-инфраструктуры

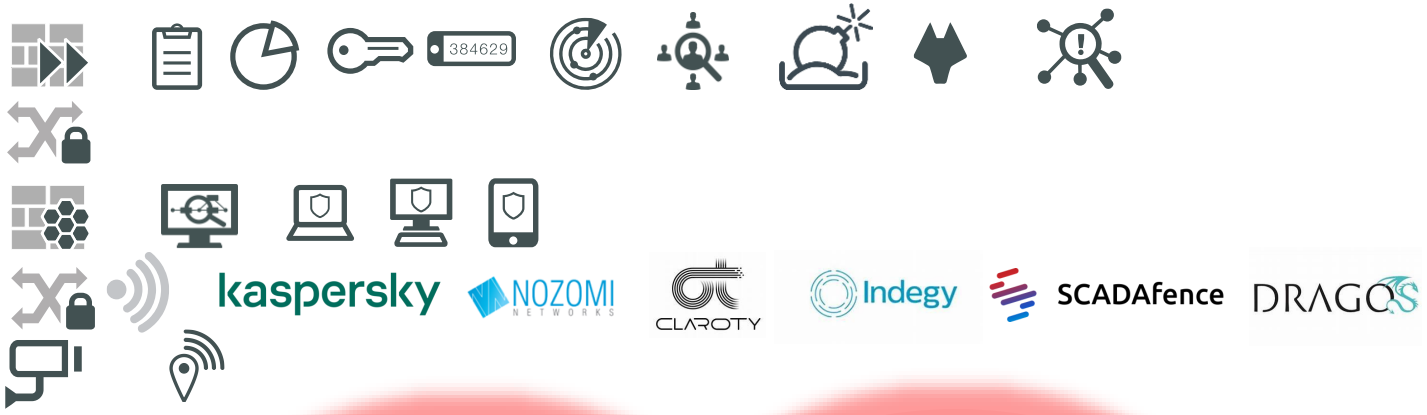


Step 7. Integrate Physical Security

- Add IP Cameras w/ Facial Recognition
- Add presence analytics

Путь к безопасности OT-инфраструктуры



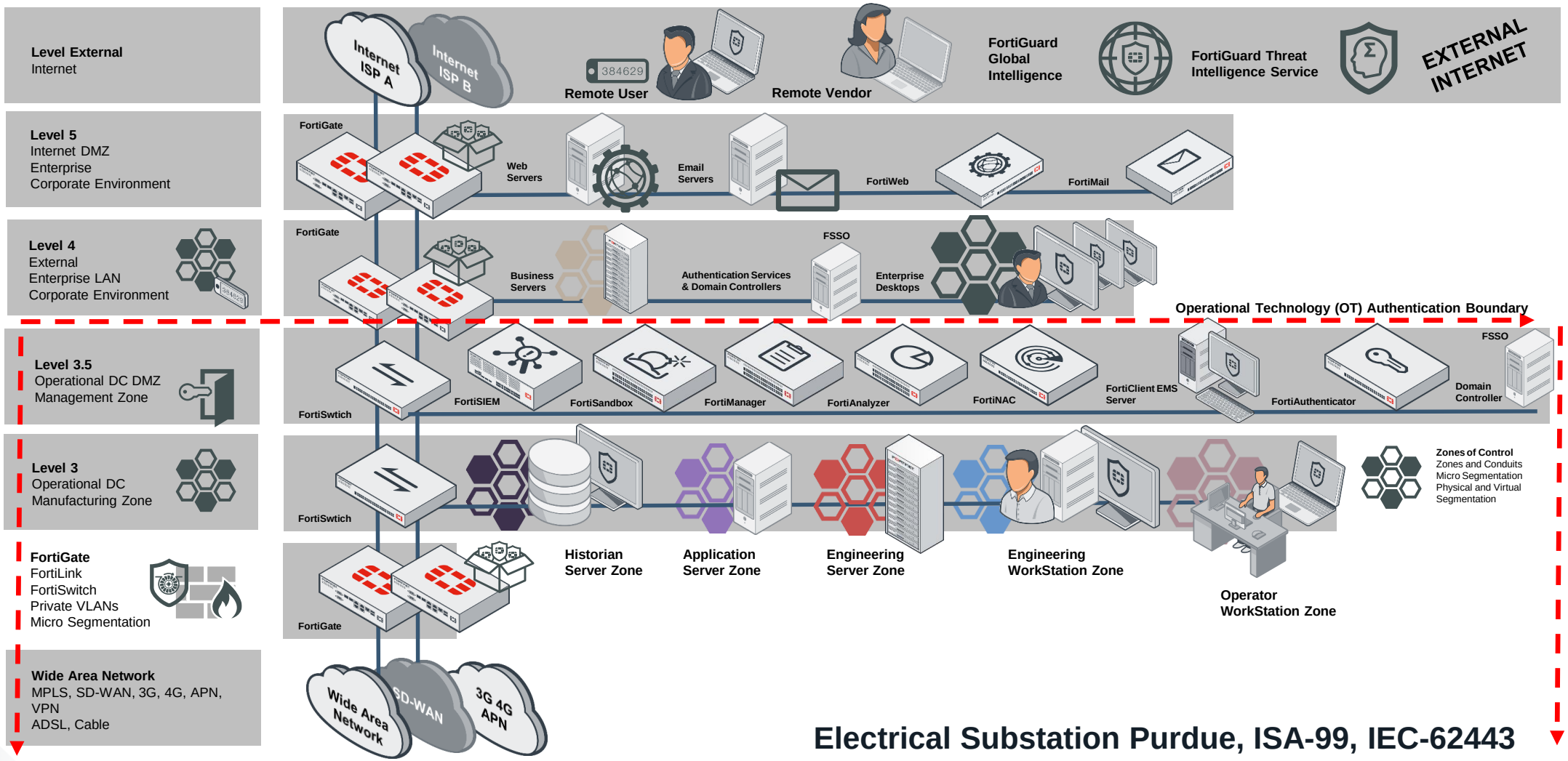


Step 8. Contextual Awareness

- Add DPI vendors with OT capabilities

FORTINET

Архитектура решений Fortinet на модели Purdue



Electrical Substation Purdue, ISA-99, IEC-62443

FORTINET

Как можно снизить кибер-риски?

Видимость горизонта цифровых атак

Новые технологии приводят к новым рискам.

Необходима **широкая видимость горизонта угроз** и проактивное обнаружение.

Защита от сложных и целевых угроз

Количество угроз и вредоносного ПО неуклонно растет.

Необходима **комплексная защита на всех уровнях** – устройств, сети, приложений.

Структурировать и утвердить архитектуру безопасности

Сложность - враг эффективности.

Необходимо **автоматически предотвращать, обнаруживать и реагировать** на угрозы.

Упростить соответствие требованиям

Международное, региональное, отраслевое и государственное регулирование.

Обеспечив полноценную **защиту** - станет **проще соответствие требованиям**.

FORTINET

Спасибо за внимание!

Даниил Тамеев

Руководитель направления по работе
с промышленными компаниями

dtameev@fortinet.com

BMW i Motorsport
Official Partner