Адаптивная система информационной безопасности

Алексей Андрияшин

17.02.2017

Драйверы развития ИБ

Инфраструктура. Постоянные изменения.

Облака

82%

Рассматривают применение облачных решений

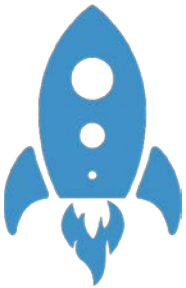
RIGHTSCALE

IoT

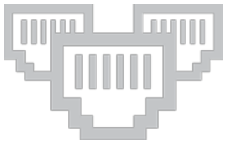
20 Млрд

IoT устройств к 2020

Gartner



Скорость



4X

100G порт

Secure https:// Infonetics RESEARCH

Безопасность ИЗМЕНИЛАСЬ

3.2 МИЛЛИАРДА ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ

1.3 МИЛЛИАРДА СМАРТФОНОВ В МИРЕ

3 МИЛЛИАРДА УСТРОЙСТВ ЕЖЕГОДНО ДО 2020

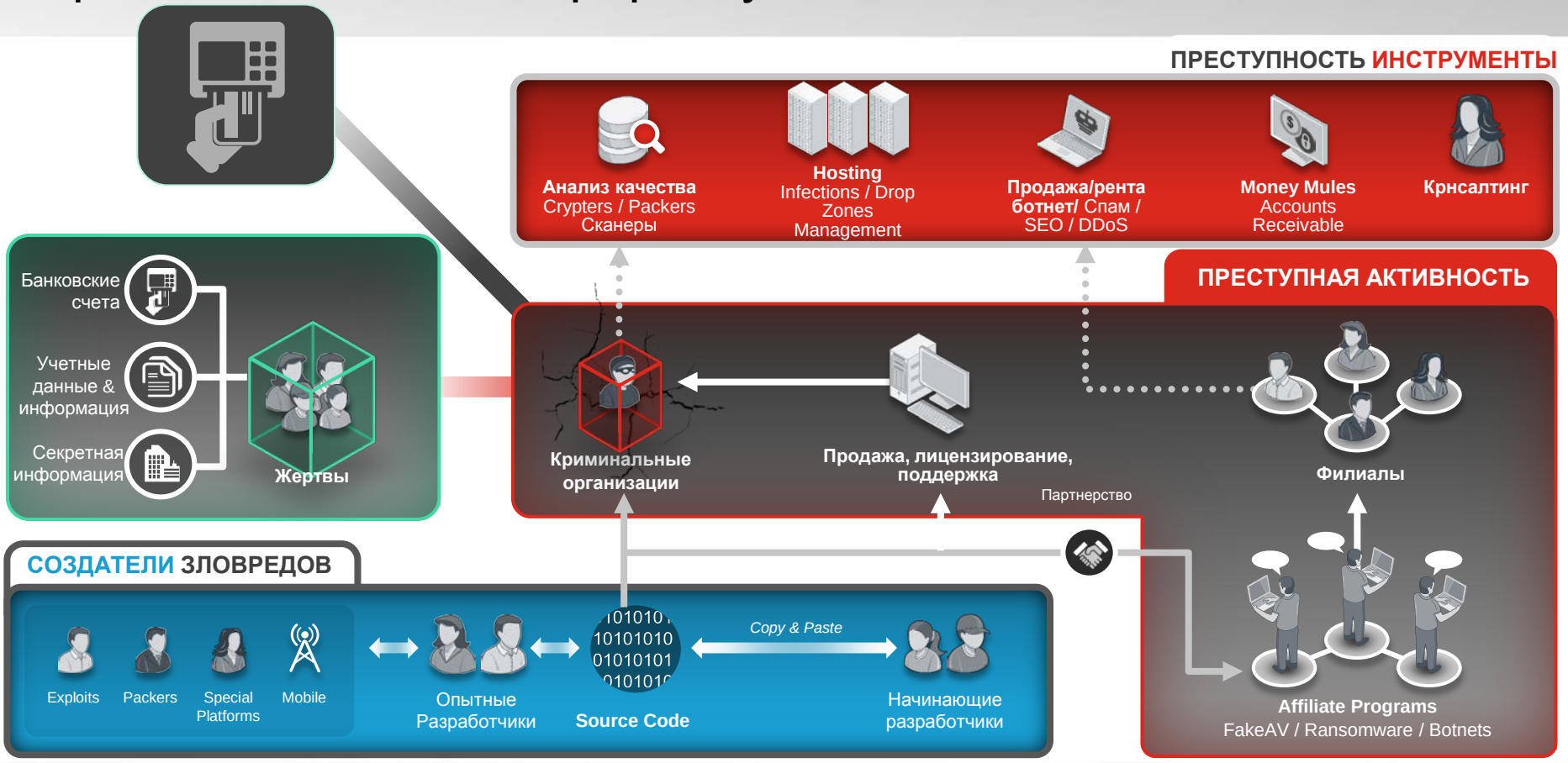
10,000x

РОСТ КИБЕР УГРОЗ

РЫНОК ОБЛАЧНЫХ УСЛУГ ДОСТИГНЕТ

$191 МИЛЛИАРДА

Организованная киберпреступность



Анатомия атаки

	Подготовка	Внедрение	Активные действия
Cyber Kill Chain	1 Разведка: Сбор адресов электронной почты, звонках, контактах 2 Вооружение: Использование эксплойтов и бекдоров	3 Доставка: Доставка зловредного кода по почте, Интернет, USB 4 Эксплуатация: Использование уязвимости для выполнения кода в системе жертвы 5 Установка: Установка зловредного/ шпионского ПО	6 Управление (C2): Каналы управления для удаленных манипуляций в IT структуре жертвы 7 Работа по целям: Повышение привилегий, получение управления, достижение цели
Время	Часы - Месяцы	Секунды	Месяцы

Основано на Lockheed Martin's Cyber Kill Chain

Безопасность. Изменение ландшафта.

ОБЪЕМ

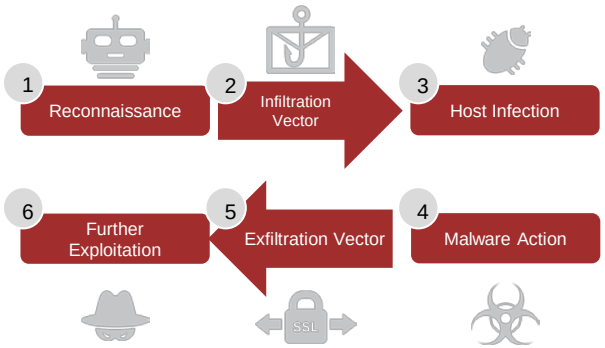
500,000

IPS
Угроз в минуту

http://threatmap.fortiguard.com

СЛОЖНОСТЬ

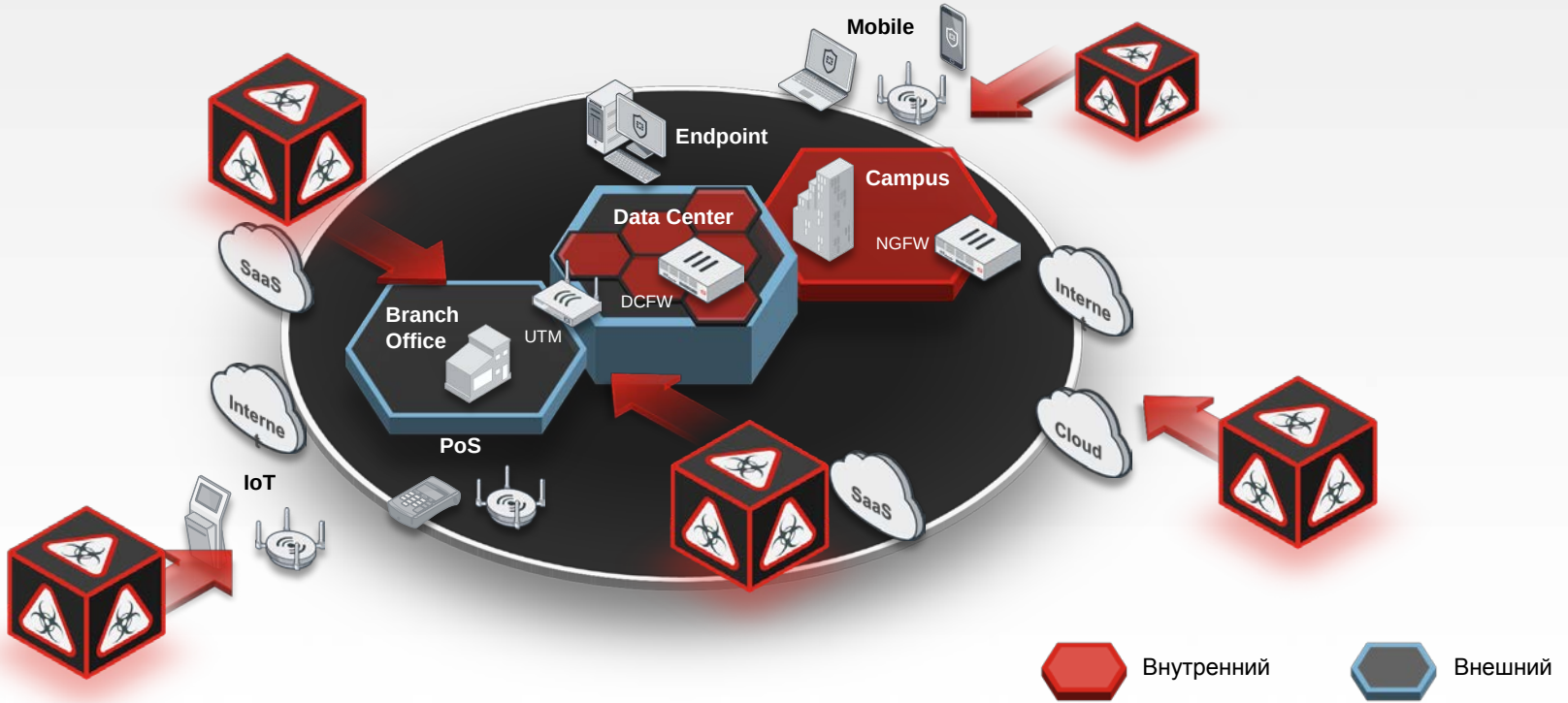
Kill Chain



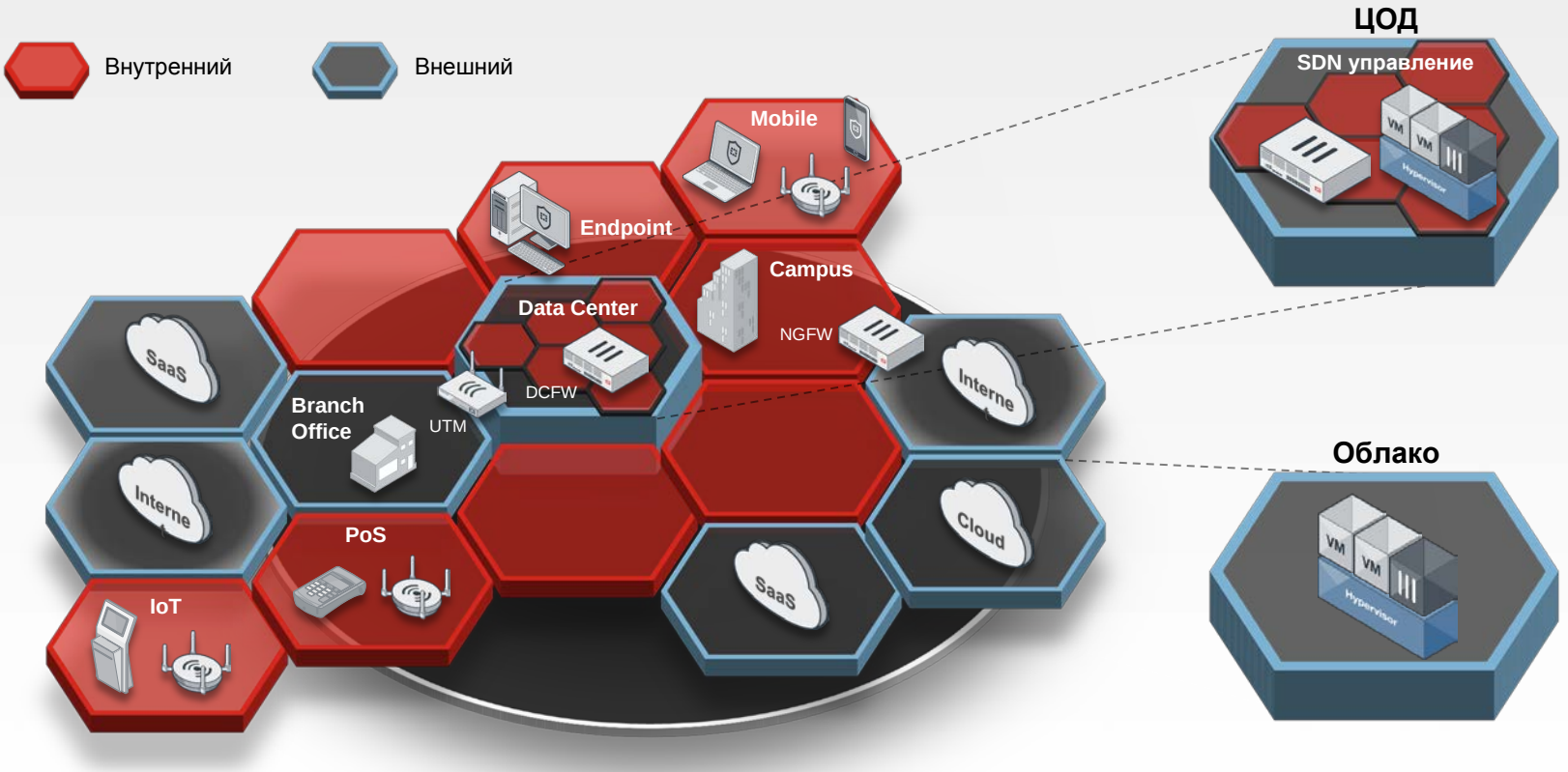
МОТИВАЦИЯ

Тип атаки	Стоимость
Zero Day	$5K - $50K
Exploit Kit	$1K - $20K
Botnet Rental	10 центов
Spam 100,000	$120

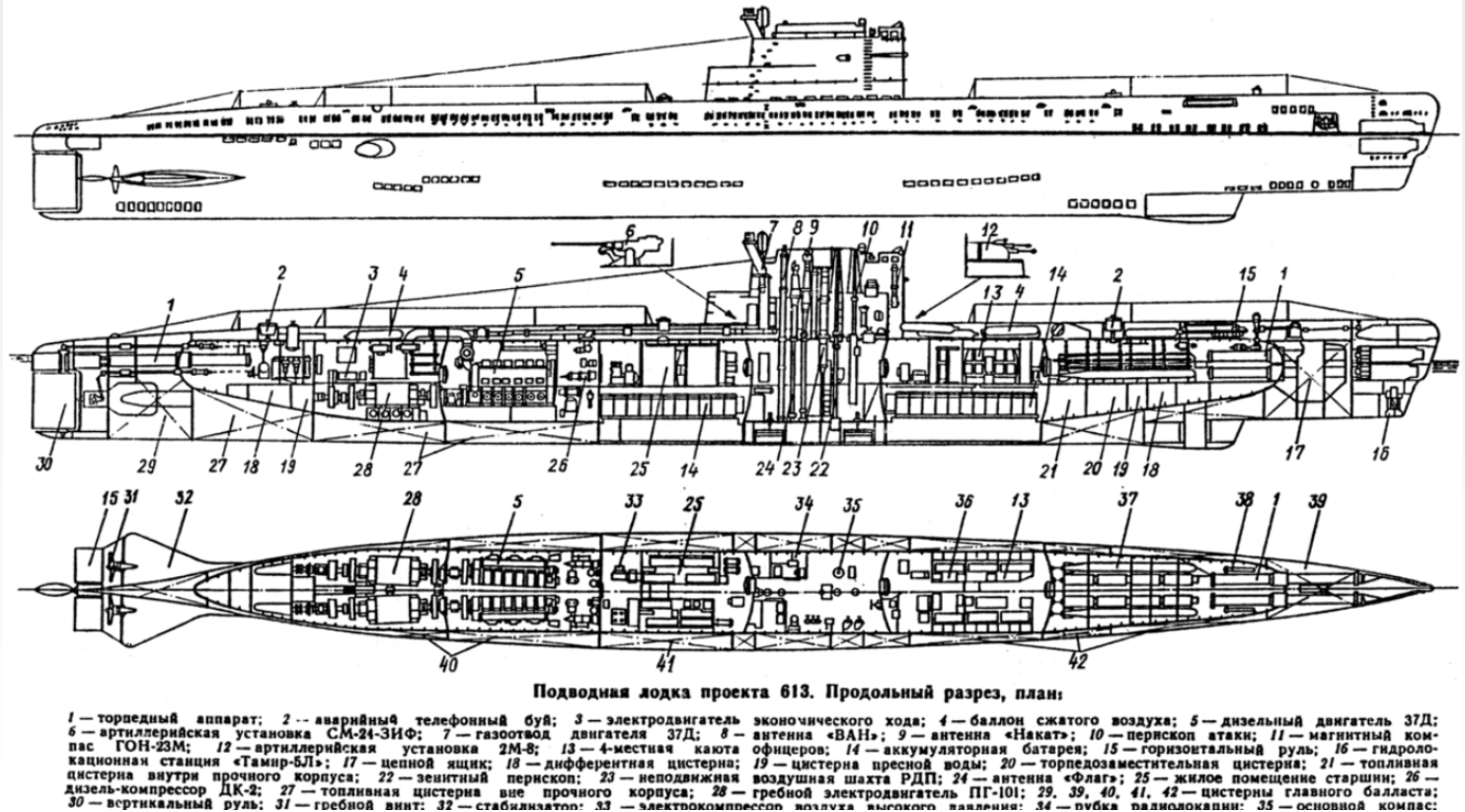
Площадь атак стремительно растет с высокой динамикой



Высокий уровень Сегментации



Слушать в отсеках!



Подводная лодка проекта 613. Продольный разрез, план:

1 — торпедный аппарат; *2* — аварийный телефонный буй; *3* — электродвигатель экономического хода; *4* — баллон сжатого воздуха; *5* — дизельный двигатель 37Д; *6* — артиллерийская установка СМ-24-3ИФ; *7* — газоотвод двигателя 37Д; *8* — антенна «ВАН»; *9* — антенна «Накат»; *10* — перископ атаки; *11* — магнитный компас ГОН-23М; *12* — артиллерийская установка 2М-8; *13* — 4-местная каюта офицеров; *14* — аккумуляторная батарея; *15* — горизонтальный руль; *16* — гидроакустическая станция «Тамир-5Л»; *17* — цепной ящик; *18* — дифферентная цистерна; *19* — цистерна пресной воды; *20* — торпедозаместительная цистерна; *21* — топливная цистерна внутри прочного корпуса; *22* — зенитный перископ; *23* — неподвижная воздушная шахта РДП; *24* — антенна «Флаг»; *25* — жилое помещение старшин; *26* — дизель-компрессор ДК-2; *27* — топливная цистерна вне прочного корпуса; *28* — гребной электродвигатель ПГ-101; *29, 39, 40, 41, 42* — цистерны главного балласта; *30* — вертикальный руль; *31* — гребной винт; *32* — стабилизатор; *33* — электрокомпрессор воздуха высокого давления; *34* — рубка радиолокации; *35* — основной компас;

Регуляторы. Выполнение требований.

РЕГУЛЯТОРЫ

PCI DSS COMPLIANT

Банк России

ISO 27001

HIPAA COMPLIANT

ГОСУДАРСТВО

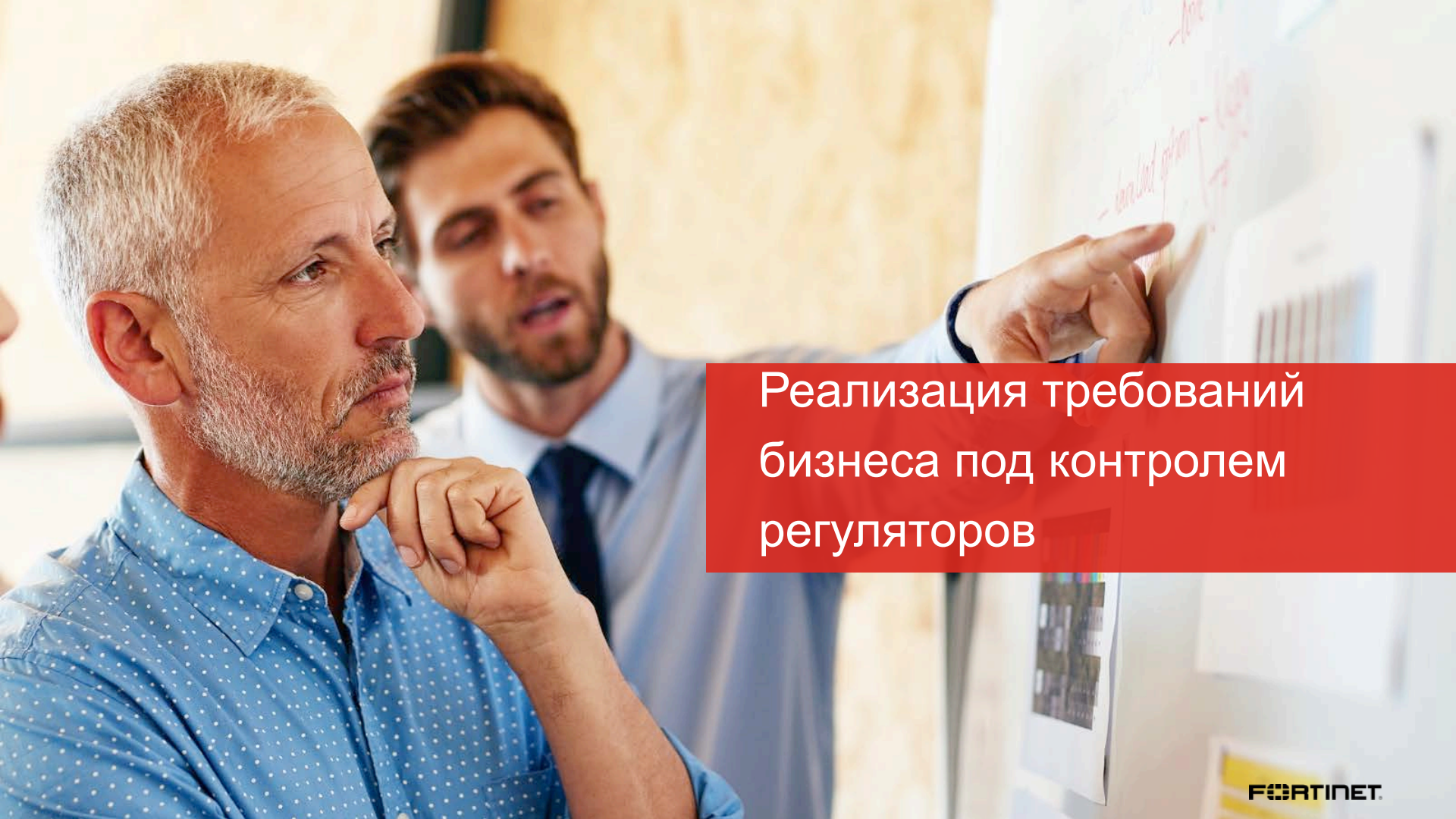
СЕРТИФИКАЦИЯ

NIST

EAC

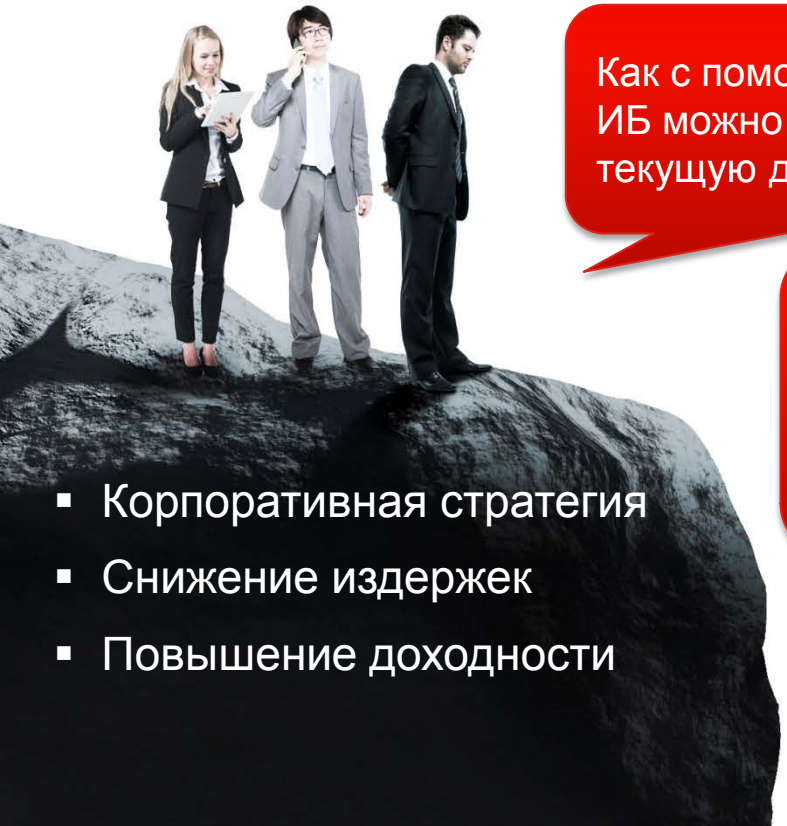
NSS LABS

ICSA labs CERTIFIED ANTI-VIRUS


Реализация требований
бизнеса под контролем
регуляторов

Понимание потребностей бизнеса

Правление / Топ-менеджмент

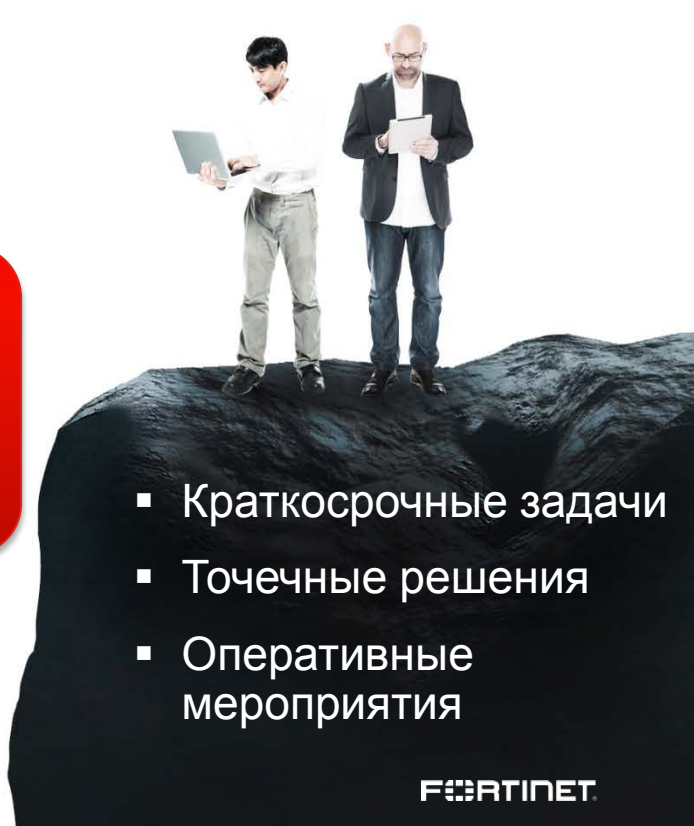


- Корпоративная стратегия
- Снижение издержек
- Повышение доходности

Как с помощью решений ИБ можно повысить текущую доходность

Как можно продемонстрировать соответствие требованиям, пройти аудит?

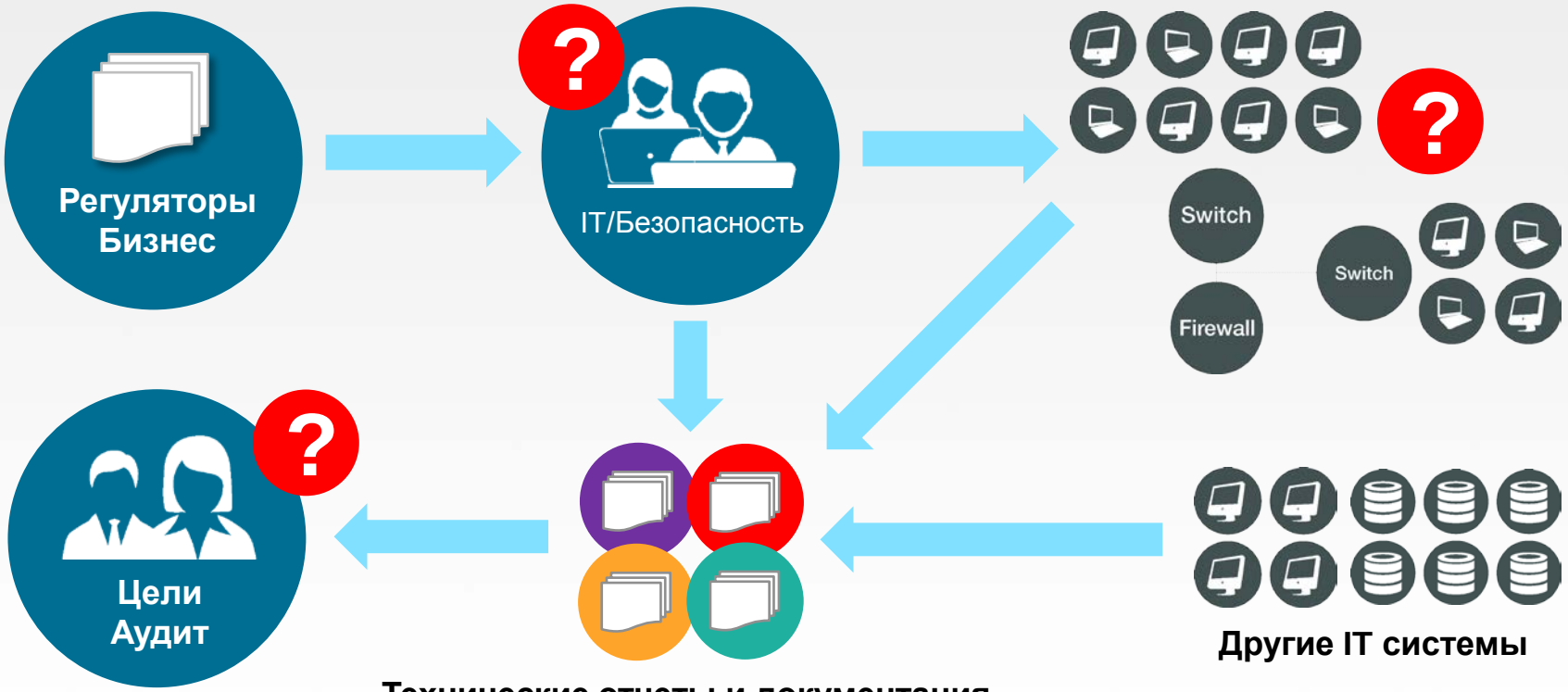
Безопасность / IT



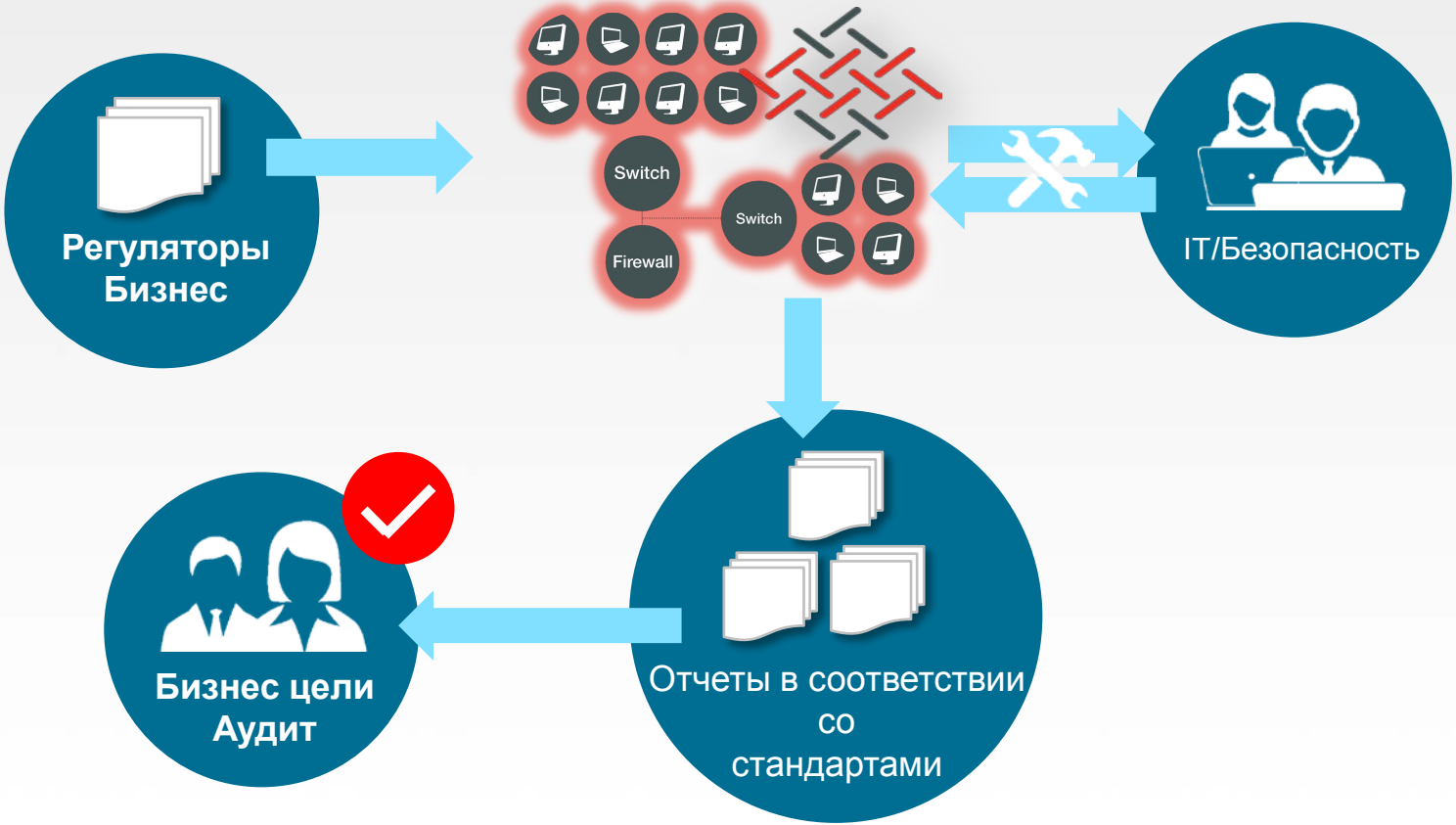
- Краткосрочные задачи
- Точечные решения
- Оперативные мероприятия

FORTINET

Задача


Регуляторы
Бизнес
IT/Безопасность
Switch
Switch
Firewall
Цели
Аудит
Технические отчеты и документация
Другие IT системы

Решение задачи



Ликвидировать разрыв. Установить доверие

Правление / Топ-менеджмент

Безопасность / IT

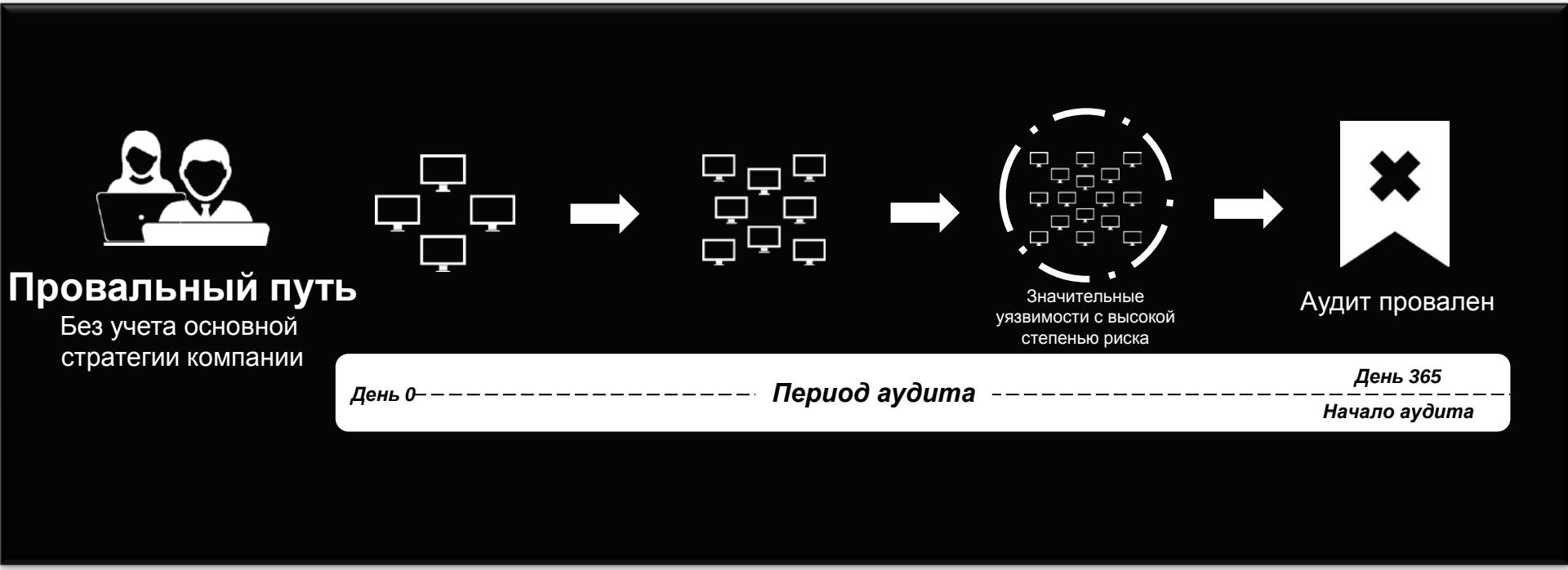
Понимание требований и методов соответствия

Раскрытие проблем и установка приоритетов

Эффективность коммуникаций

Установка доверия

Безопасность и соответствие задним числом



Безопасность “под-ключ”

Верный путь

В соответствии с бизнес стратегией

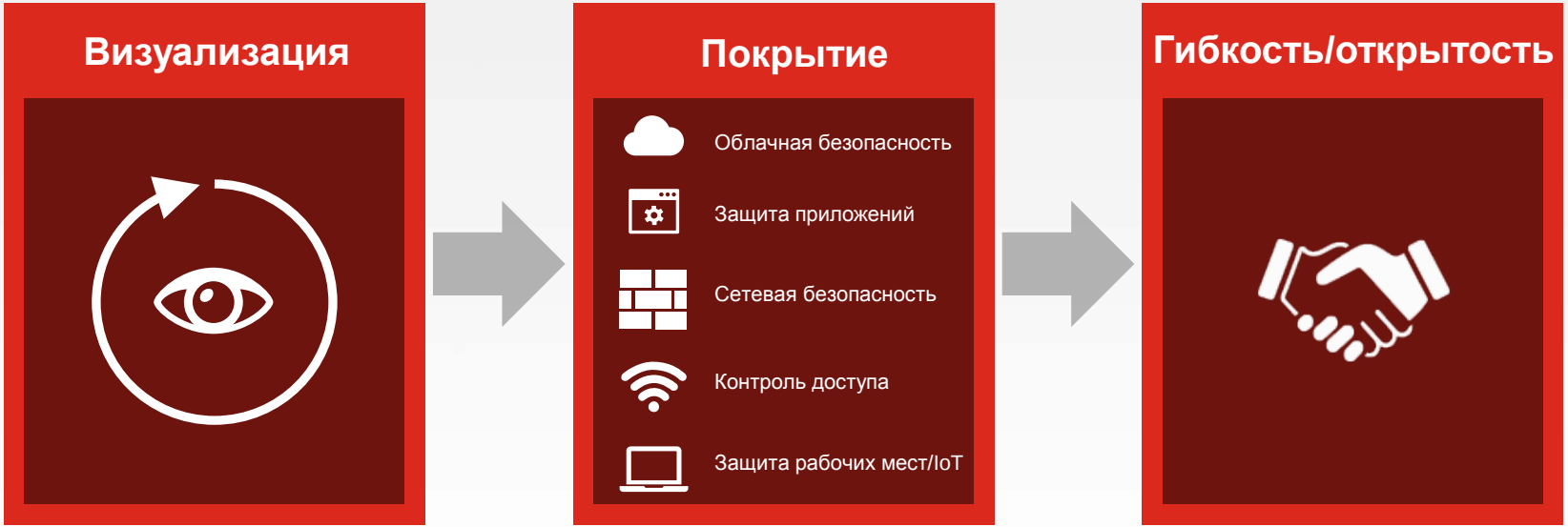
Безопасность / IT

Фабрика безопасности

FORTINET SECURITY FABRIC

- **ШИРОТА**
- **МОЩНОСТЬ**
- **ИНТЕЛЛЕКТ**

ШИРОТА – Фабрика предоставляет ВИЗУАЛИЗАЦИЮ, ПОКРЫТИЕ и ГИБКОСТЬ по всему спектру возможных УГРОЗ



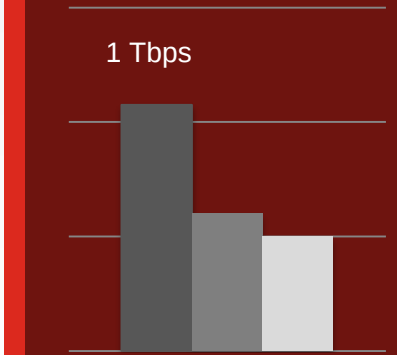
ШИРОТА – возможность интеграции с технологическими партнёрами

МОЩНОСТЬ – Повышение производительности и снижение нагрузки на инфраструктуру

Процессоры безопасности (SPUs)

- **NP6** — Ускорение обработки сетевого трафика
- **CP9** — Ускорение контентного анализа
- **SoC3** — Оптимизация процессов на всех уровнях

Распараллеливание процессов



Разнообразие

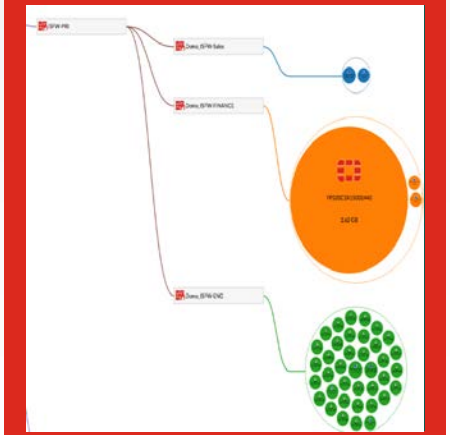
ИНТЕЛЛЕКТ
Быстрая, скоординированная реакция на угрозы

Глобально и локально

Известные угрозы
FortiGuard

Неизвестные угрозы
FortiSandbox

Аудит и рекомендации



Координация

Решения Fortinet

Корпорации

- ENTERPRISE FIREWALL
- CLOUD SECURITY
- ADVANCED THREAT PROTECTION
- APPLICATION SECURITY
- SECURE ACCESS
- SECURITY OPERATIONS

Малый бизнес

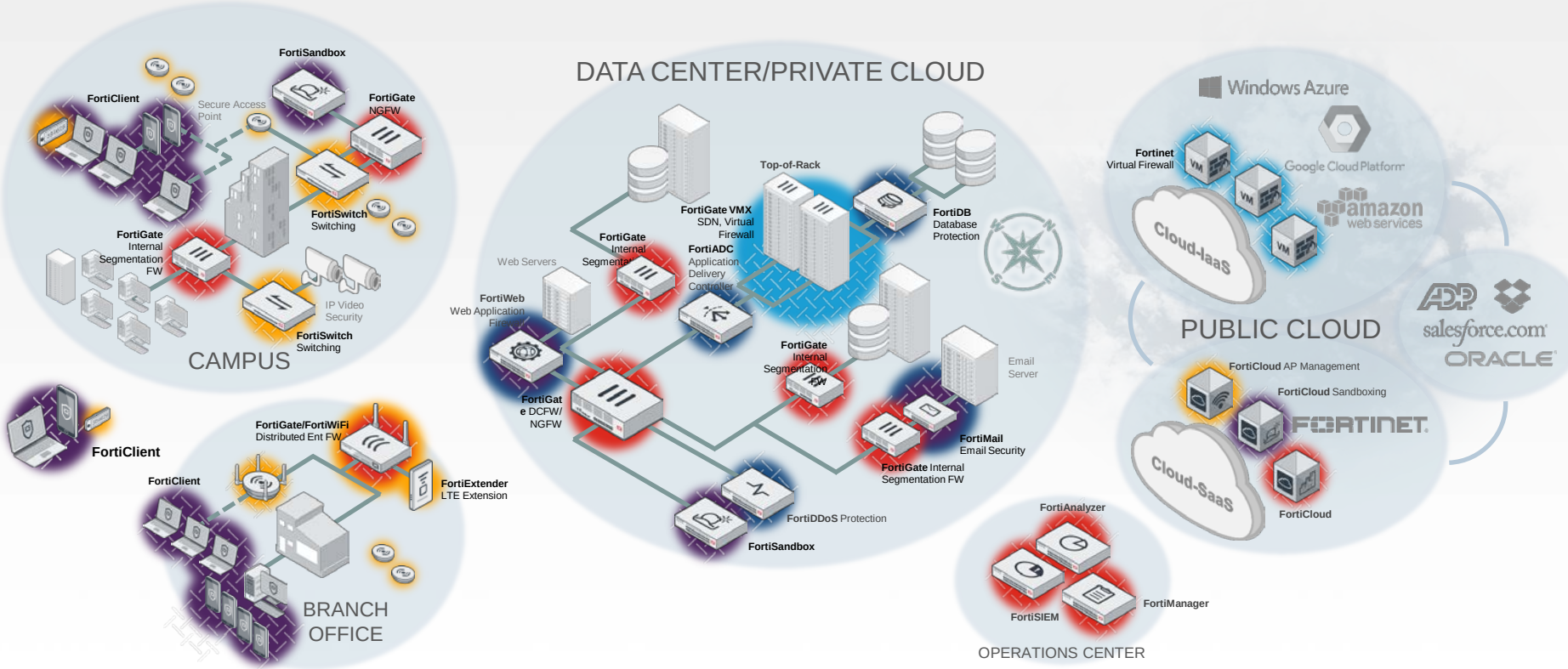
- CONNECTED UTM

Сервис провайдеры

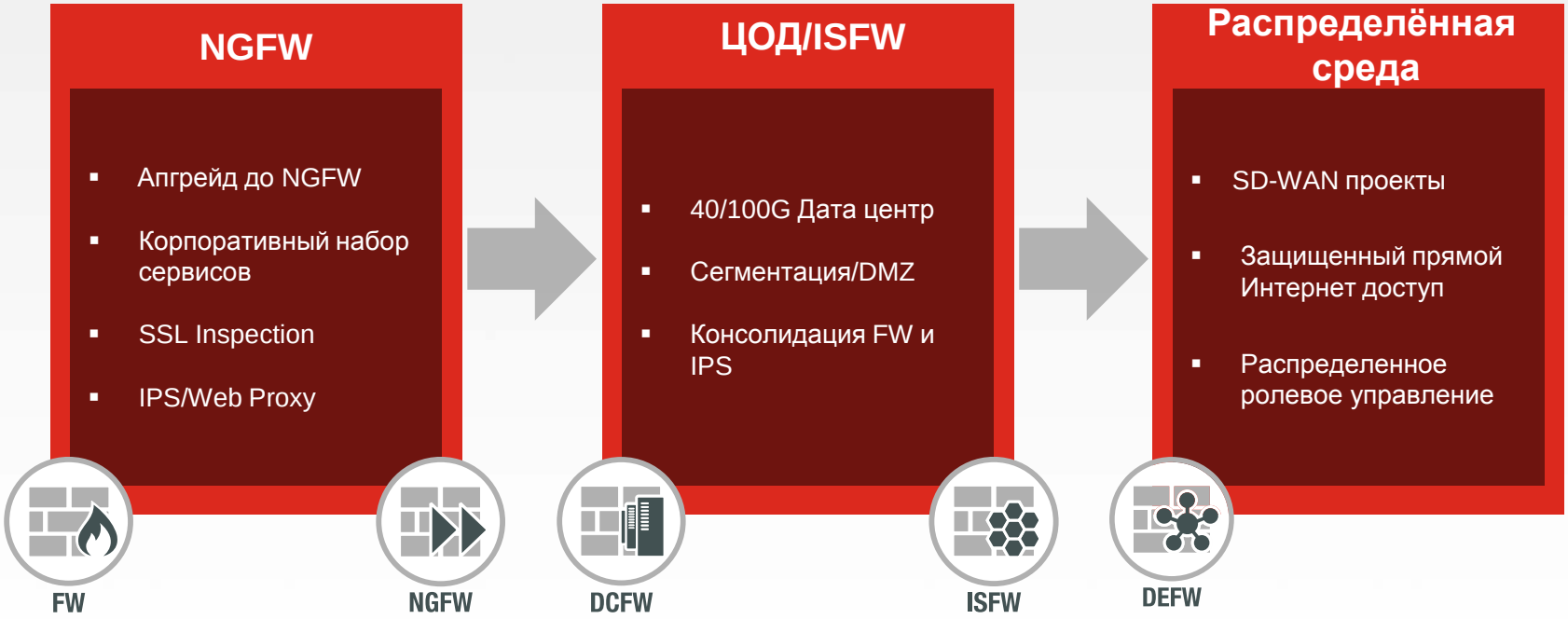
- CARRIER-GRADE SECURITY

FORTINET SECURITY FABRIC

SECURITY OPERATIONS | SECURE ACCESS | APPLICATION SECURITY | ADVANCED THREAT PROTECTION | CLOUD SECURITY | ENTERPRISE FIREWALL



Межсетевые экраны корпоративного уровня



Межсетевые экраны корпоративного уровня

КОРПОРАТИВНЫЙ МСЭ

ASIC — SPU

FortiGuard

5.6 — FortiOS

Enterprise Bundle Services

FortiManager

FortiAnalyzer

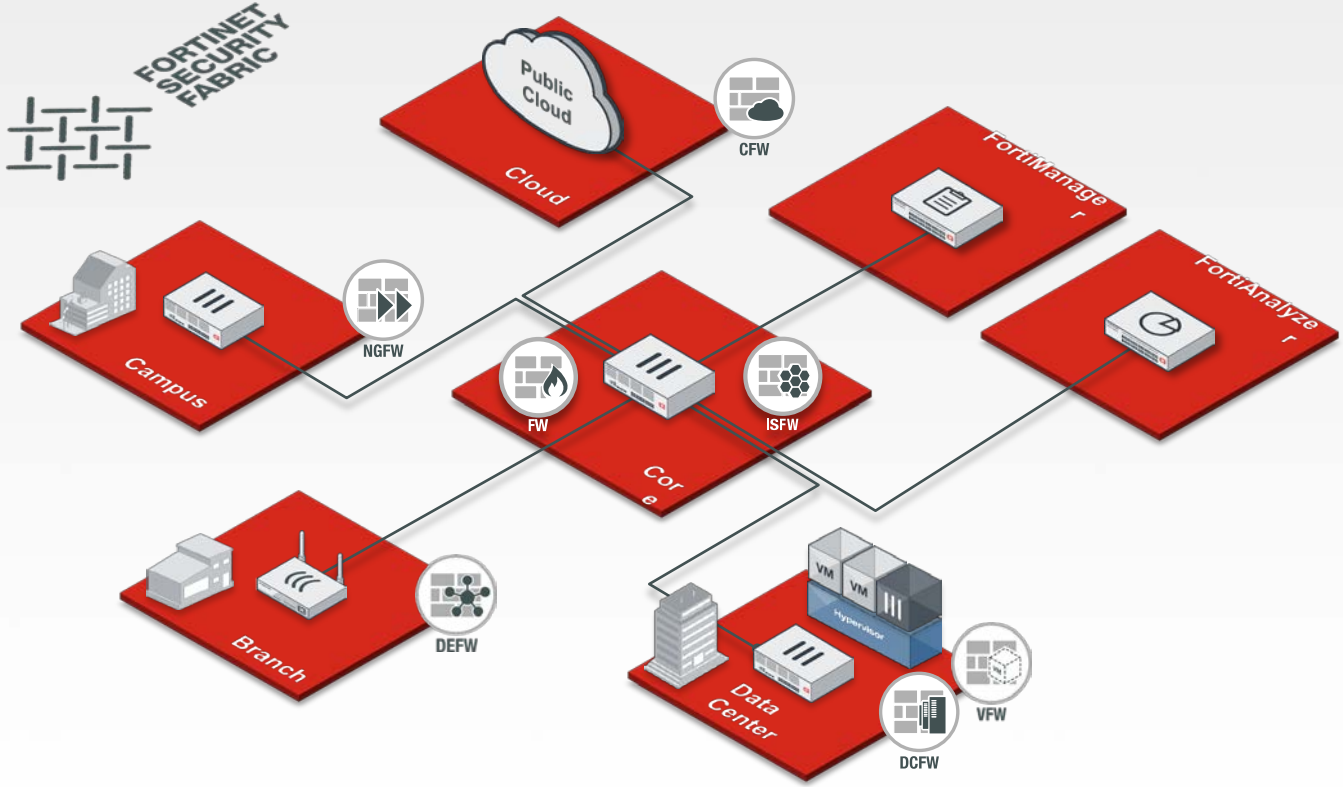
Physical

Virtual

Cloud

Rugged

FortiGate

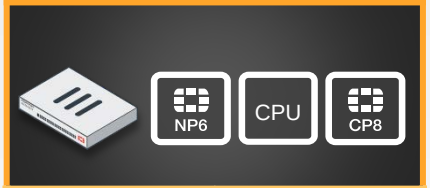


Продуктовая линейка Fortigate

Начальный уровень

Model	FW
FGT 30E*	950 Mbps
FGT 50E	2.5 Gbps
FGT 60E	3 Gbps
FGT 80D	1.3 Gbps
FGT 90E	4 Gbps

Средний уровень



Модель	FW
FGT 100D	2.5 Gbps
FGT 200D	4 Gbps
FGT 300D	8 Gbps
FGT 400D	16 Gbps
FGT 500D	16 Gbps
FGT 600D (10G)	36 Gbps
FGT 800D	36 Gbps
FGT 900D	52 Gbps

Верхний уровень

Модель	FW
FGT 1000D	52 Gbps
FGT 1200D	72 Gbps
FGT 1500D	80 Gbps
FGT 2000E	90 Gbps
FGT 2500E	150 Gbps
FGT 3000D	80 Gbps
FGT 3700D (40G)	160 Gbps
FGT 3800D (100/40G)	320 Gbps
FGT 3960/ 3980E (100/10G)	640 Gbps/ 1 Tbps

Операторский класс

Модель	FW
FGT 5144C	1 Tbps
FGT 5903	40G
FGT 5913	100G

Корпоративные шасси

Модель	FW
FGT 7040E (100/40/10G)	315 Gbps
FGT 7060 (100/40/10G)	2X 7040E

FortiGate – комплекс сетевой безопасности

НАЧАЛЬНЫЙ УРОВЕНЬ
30-90 СЕРИЯ

- **Распределенные**
- **Начального уровня**
  - SOC Based
  - FW Throughput ~ 4 Gbits/s
  - NGFW Throughput ~ 400 Mbits/s
  - Ports 1Ge

СРЕДНИЙ УРОВЕНЬ
100-900 СЕРИЯ

- **NGFW**
- **Филиалы**
  - NP + CP Based
  - FW Throughput ~ 50 Gbits/s
  - NGFW Throughput ~ 5 Gbits/s
  - Ports 1Ge 10Ge

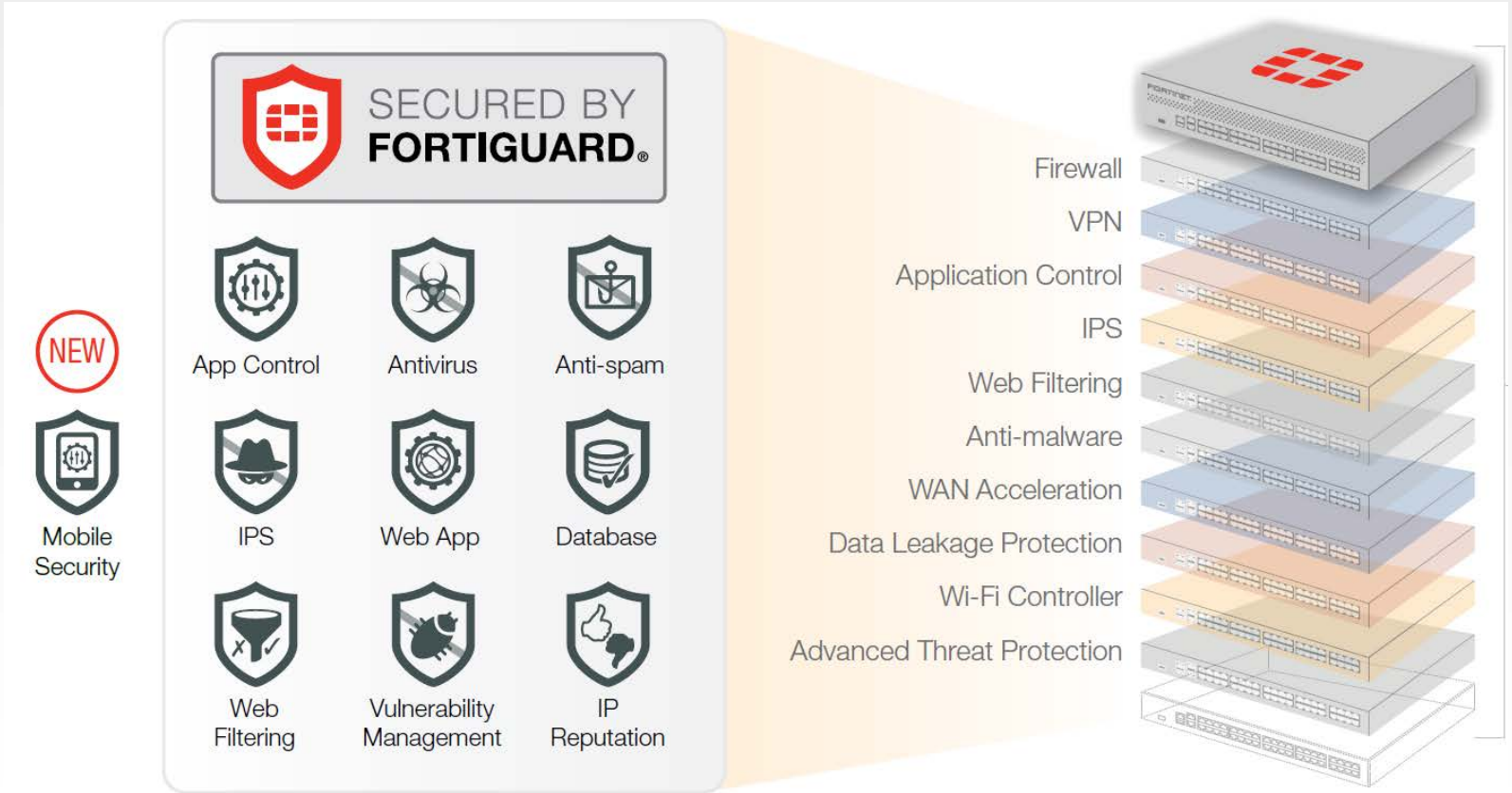
ТОПОВЫЙ УРОВЕНЬ
1000-3000 СЕРИЯ

- **ЦОД**
- **NGFW**
  - Multiple NP + CP Based
  - FW Throughput ~ 300 Gbits/s
  - NGFW Throughput ~ 30 Gbits/s
  - Ports 10Ge, 40Ge & 100Ge

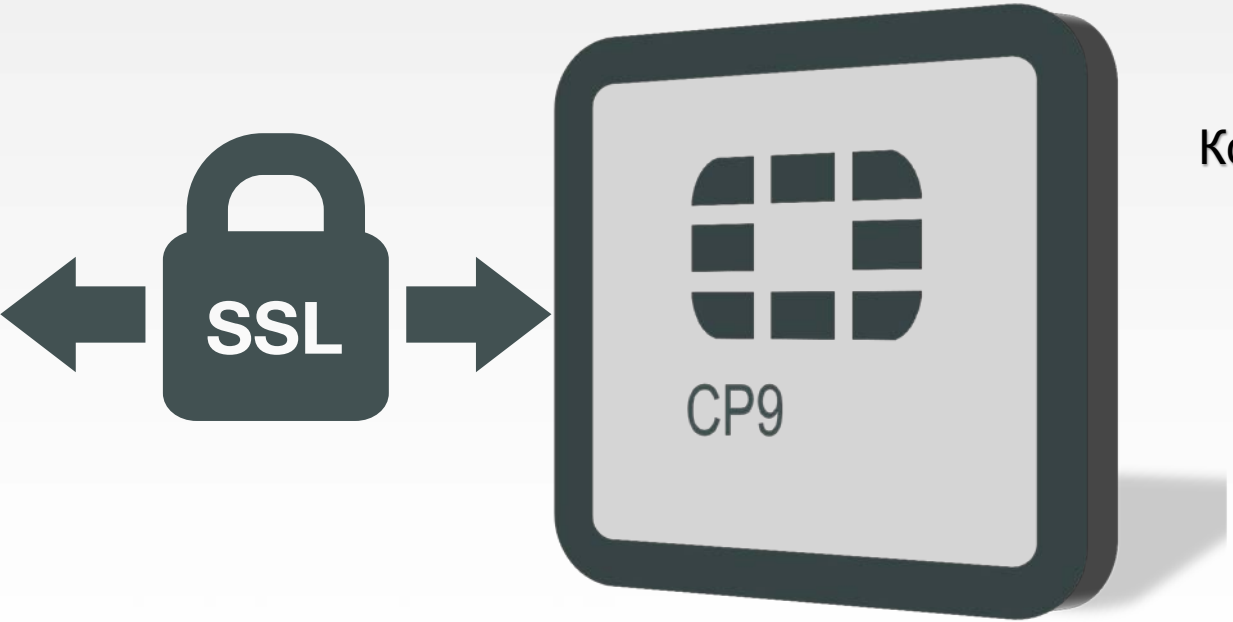
ОПЕРАТОРСКИЙ КЛАСС
5000/7000 СЕРИЯ

- **Операторы**
- **ЦОД**
  - Blade NP + CP Based
  - FW Throughput ~ 1 Tbps
  - NGFW Throughput ~ 100 Gbits/s
  - Ports 10, 40 & 100G

Сервисы безопасности и технологии



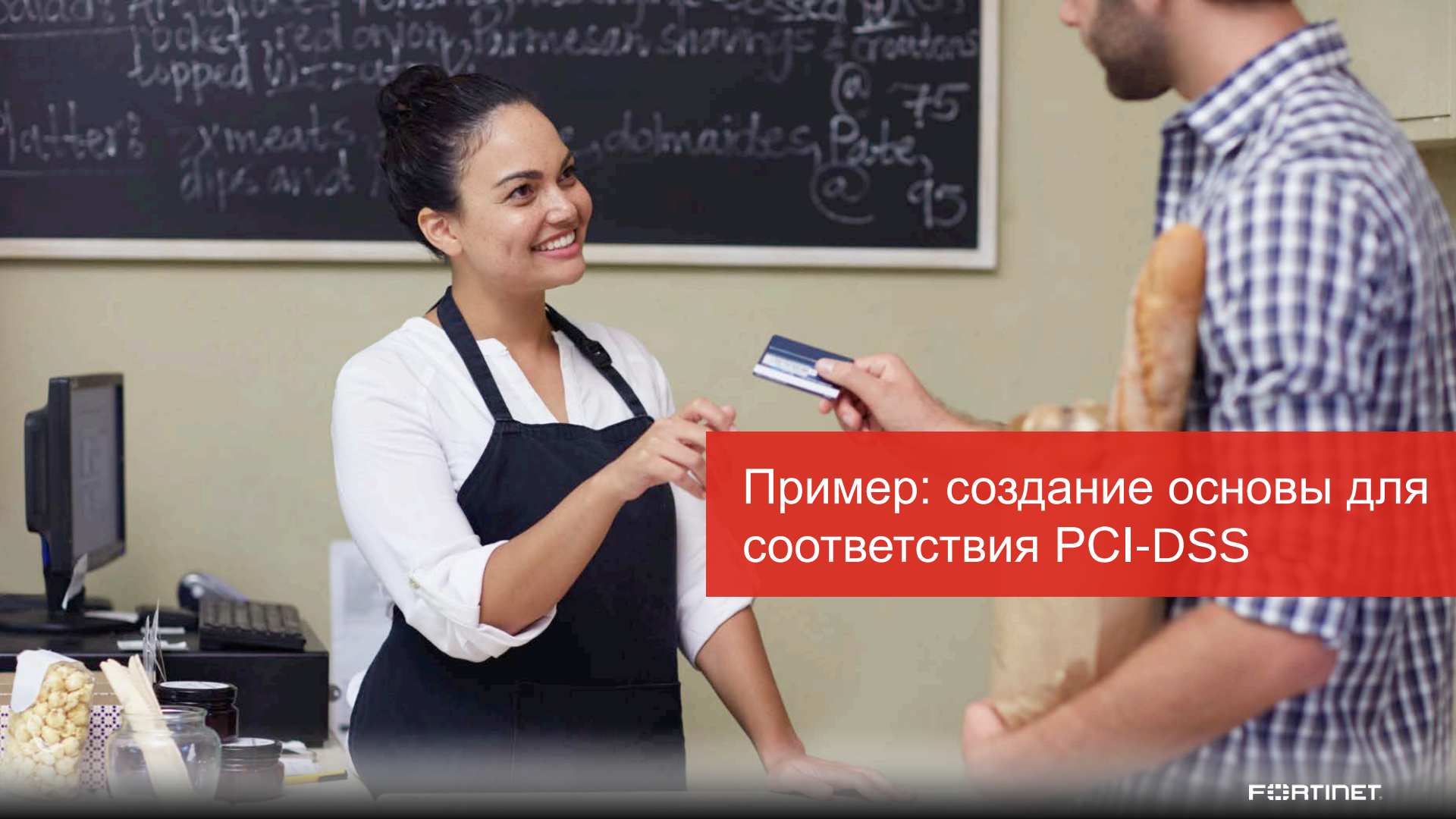
Инспекция SSL



Корпоративный трафик

50%

SSL/2017

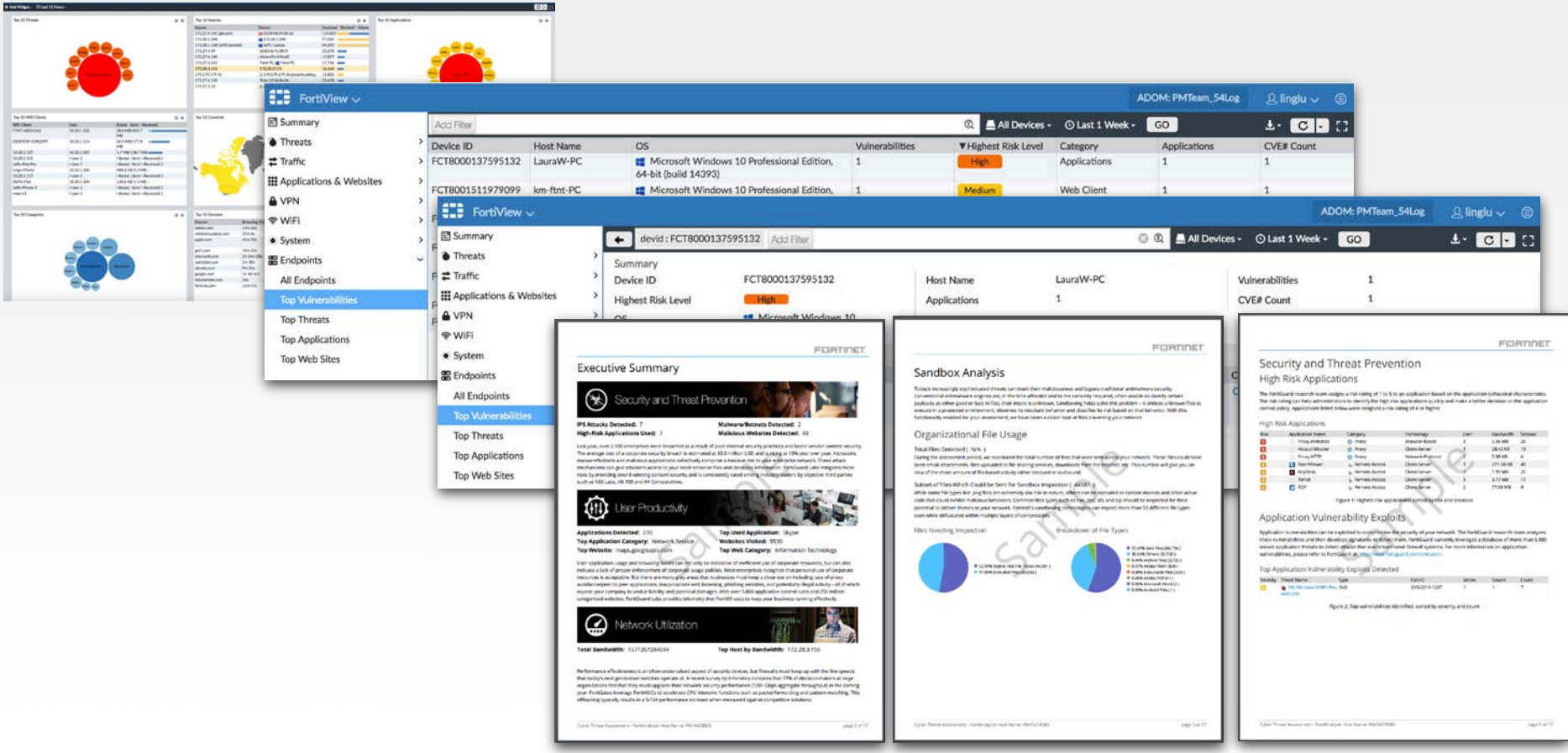


Пример: создание основы для соответствия PCI-DSS

Соответствие требованиям PCI I Функционал

PCI DSS Требования	FortiGate, FortiAP, FortiAnalyzer, FortiManager	FortiClient
Построение и обслуживание защищенной сети (Требования 1 и 2)	▪ Защита сети и сегментация ▪ Анализ соответствия (FGT) ▪ Защита беспроводных сетей ▪ Многоуровневая фабрика безопасности	▪ Защита рабочих станций (FW)
Защита данных о держателях карт (Требования 3 и 4)	▪ Шифрованные туннели ▪ Шифрованные пароли	
Управление уязвимостями (Требования 5 и 6)	▪ Обнаружение зловредного ПО ▪ Автоматические обновления, ▪ Контроль трафика приложений	▪ Обнаружение зловредного ПО ▪ Соответствие требованиям ▪ Обнаружение конечных точек
Внедрение строгих мер контроля доступа (Требования 7,8 и 9)	▪ Контроль и управление доступом ▪ Политика паролей ▪ Управление пользователями и устройствами ▪ Защищенный удаленный доступ ▪ Многофакторная аутентификация	
Регулярный мониторинг и тестирование сети (Требования 10 и 11)	▪ Отчеты об инцидентах ▪ Обнаружение беспроводных точек доступа ▪ Подавление “вражеских” точек доступа	▪ Сканер уязвимостей
Поддержка политики информационной безопасности (Требование 12)	**Корпоративная политика ИБ и процессы**	

Отчетность – FortiAnalyzer



Отчеты соответствия – подготовка к аудиту

PCI-DSS Compliance Review

Report Date: May 17, 2016 09:29
Data Range: 2015-08-06 00:00 2015-08-12 00:00 PDT (FAZ local)

PCI-DSS Compliance Review

This report is designed to help meet PCI-DSS requirements by providing a view of compliant and non-compliant security systems and processes that are regularly tested under Fortinet Best Practice controls. The validations in this report are in accordance with the requirements for PCI-DSS version 3.1.

About PCI DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of policies and procedures, mandated by the four major credit-card companies: Visa, MasterCard, Discover and American Express, with the intention of improving the security of credit and debit card transactions and protect cardholders against theft and misuse of their personal information. Any company that is involved in the transmission, processing or storage of credit card data, must be compliant with PCI-DSS.

PCI is divided into 12 main requirements, and further broken down into approximately 200 control areas.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measure	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

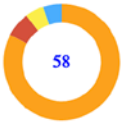
PCI DSS COMPLIANT 78.38 % Compliant

Non-Compliant	58
Compliant	16

Non-Compliant Requirements by Severity

The following provides a summary of the number of PCI requirements that are non-compliant, by Fortinet Security Best Practice Severities.

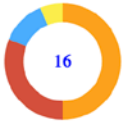
High	48
Critical	4
Medium	3
Low	3



Compliant Requirements by Severity

The following provides a summary of the number of PCI requirements that are compliant, by Fortinet Security Best Practice Severities.

High	8
Critical	5
Low	2
Medium	1



Отчетность – Фабрика безопасности

Детальная визуализация сети с использованием телеметрии

Изучение топологии

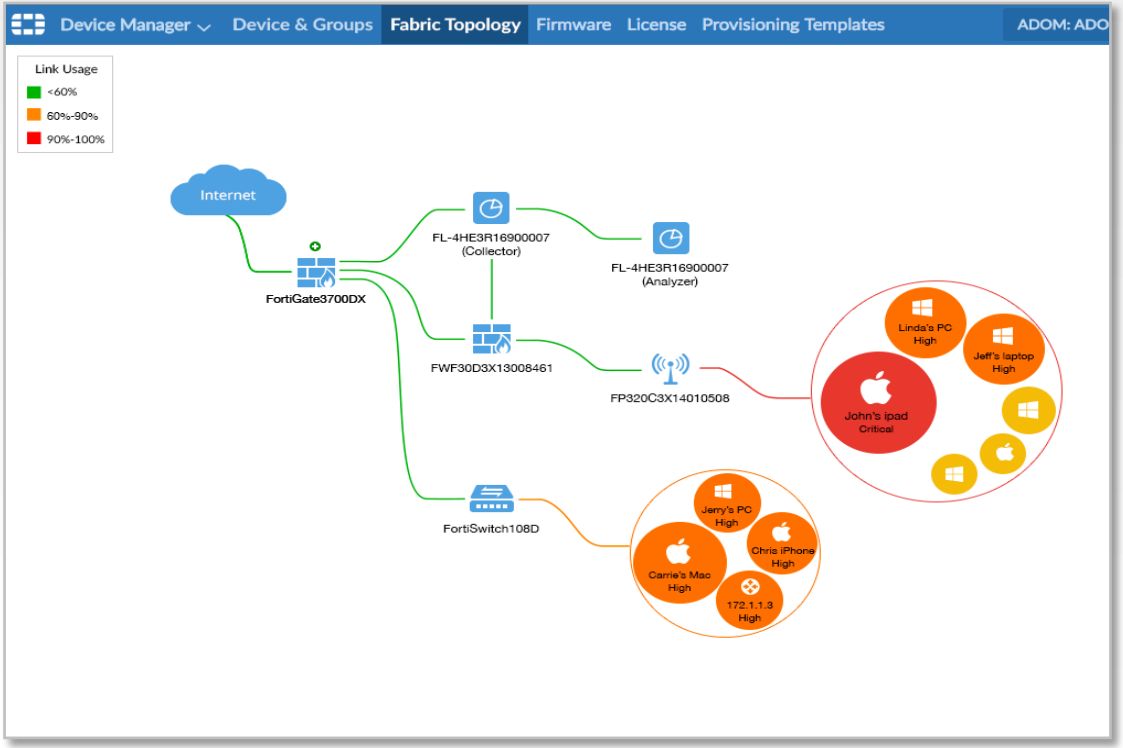
- » Синхронизация со средствами контроля
- » Анализ поведения

Коллекторы / Анализаторы

- » Обновление топологии

FortiManager – система упарления

- » Построение отчетов с учетом текущей топологии сети



Отченость – FortiAnalyzer

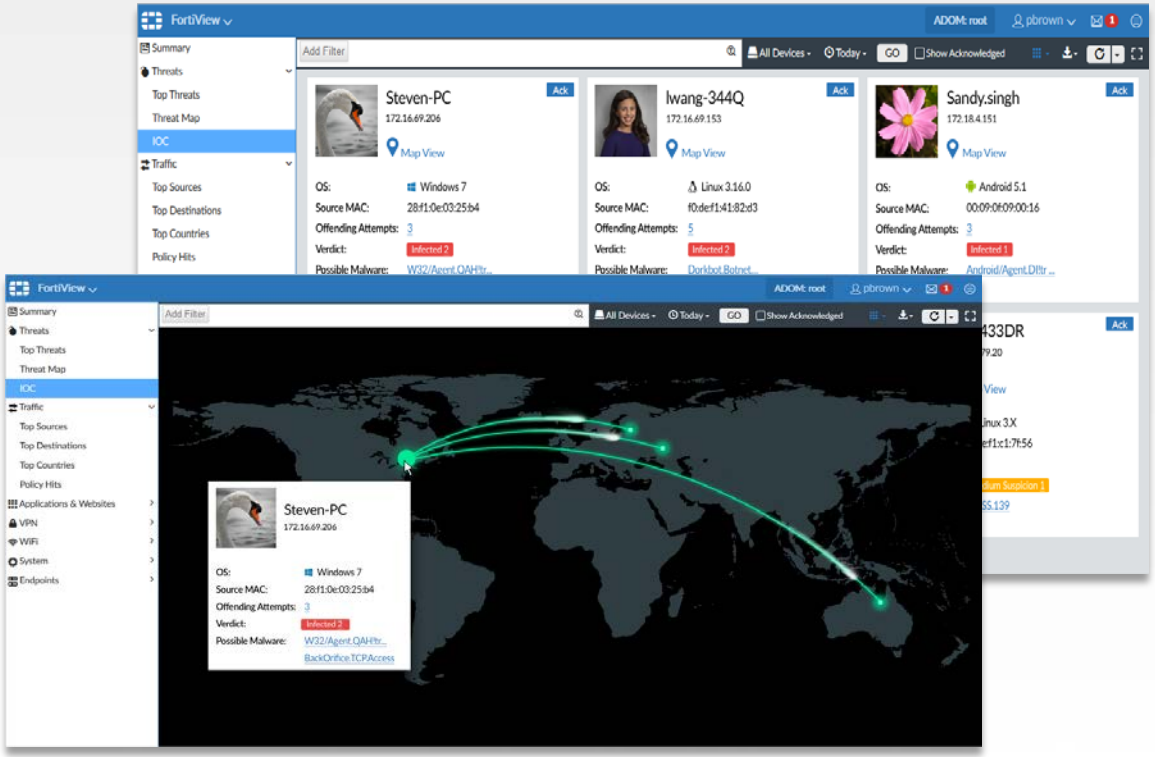
Детальная визуализация – телеметрия

Сенсоры безопасности

- » Журналирование событий на уровне рабочих мест
- » События
- » Уязвимости

Расширенные отчеты

- » Детальная отчетность на основании телеметрических данных



Отчетность – FortiAnalyzer
Детальная визуализация

Еженедельная/ежедневная отчетность

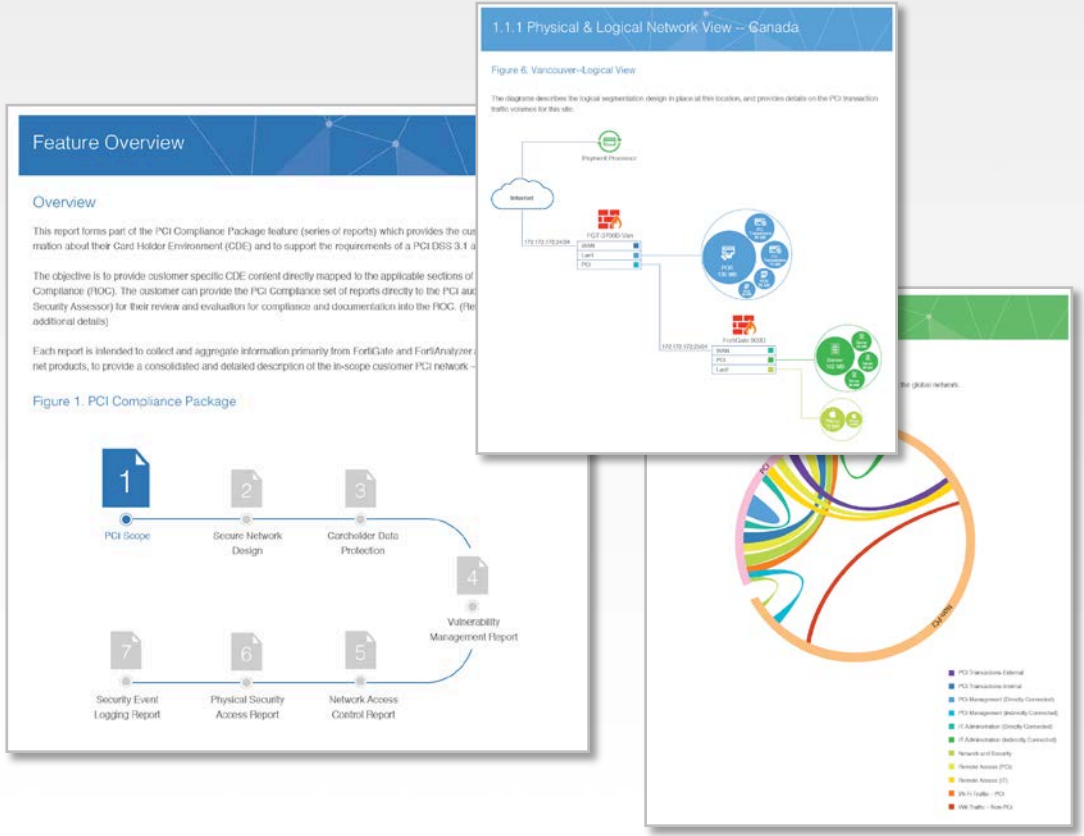
- » Новые пользователи
- » Новые устройства
- » Новое ПО
- » Новые уязвимости
- » Новые угрозы
- » Сигналы тревоги

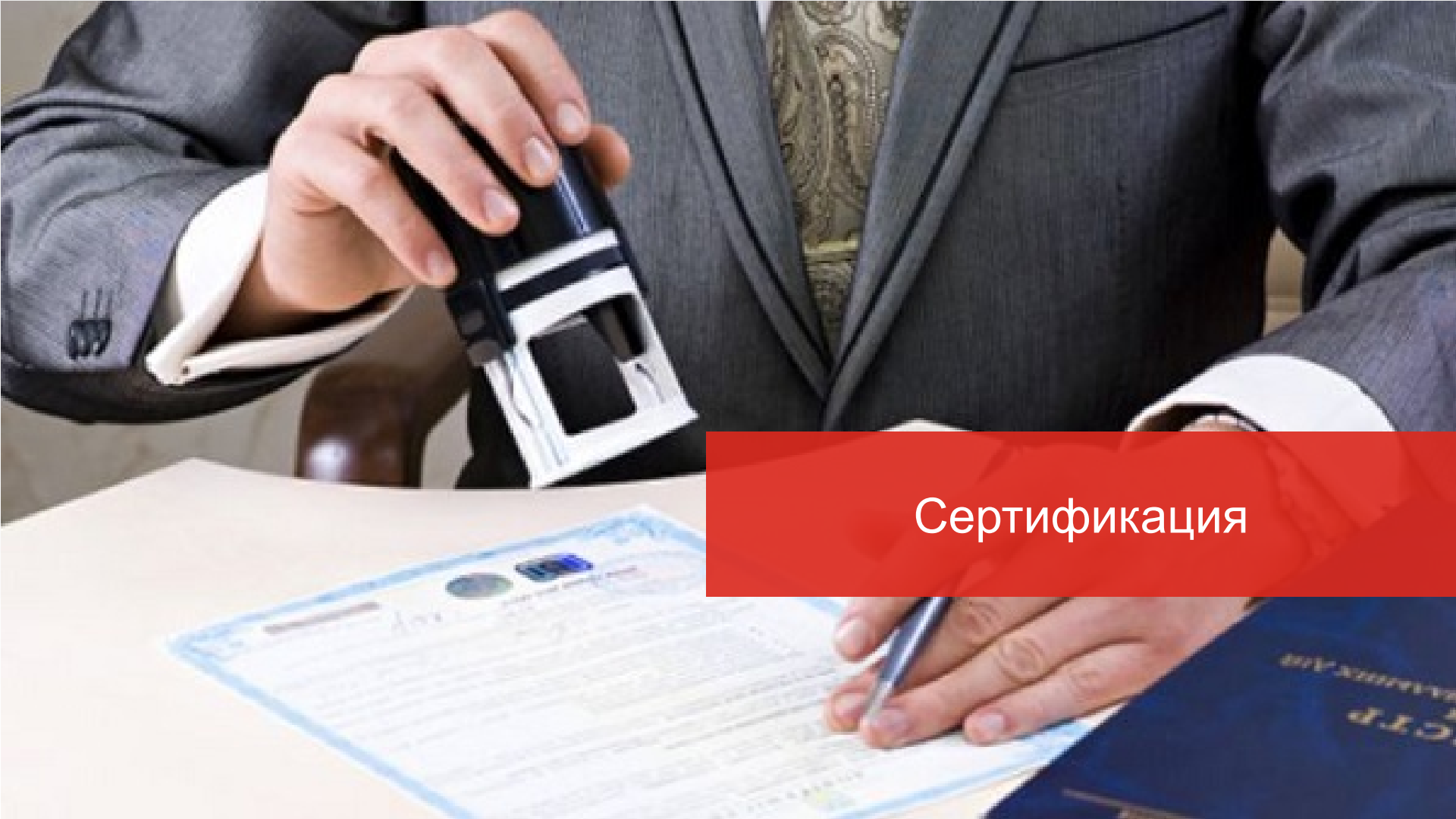
Ситуационные отчеты

Отчеты для руководства и аудита
Детальная визуализация – отчеты соответствия

Отчеты соответствия

- PCI
- Защищенный сетевой дизайн
- Защита данных держателей карт
- Анализ уязвимостей
- Контроль доступа в сеть (NAC)
- Контроль доступа
- Журнал инцидентов





Сертификация

Пару слов о сертификации

Сертификация – это проверка механизмов безопасности, реализованных в продукте, на соответствие требованиям регулирующих органов

ФСТЭК – Федеральная служба по техническому и экспортному контролю

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3171

Выдан 30 июня 2014 г.
Действителен до 30 июня 2017 г.

Настоящий сертификат удостоверяет, что межсетевой экран FortiGate с установленным программным обеспечением 5.0 (версия исполнения: FortiGate-40C-LENC/FortiGate-80C-LENC/FortiGate-100D-LENC/FortiGate-300C-LENC/FortiGate-600C-LENC/FortiGate-1000C-LENC/FortiGate-3040B-LENC/FortiGate-3950B-LENC/FortiGate-5101C-LENC), разработанный компанией Fortinet Singapore Private Limited и произведенный ЗАО «Профессиональные Системы и Проекты. Профи-СП» в соответствии с техническими условиями ТУ 4040-010-98945270-14, является программно-техническим средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели зашищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 3 классу зашищенности и «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля при выполнении ограничений по эксплуатации, указанных в формулярах 4040-40C-98945270-14 30, 4040-80C-98945270-14 30, 4040-100D-98945270-14 30, 4040-300C-98945270-14 30, 4040-600C-98945270-14 30, 4040-1000C-98945270-14 30, 4040-3040B-98945270-14 30, 4040-3950B-98945270-14 30 и 4040-5101C-98945270-14 30.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 13.05.2003 № СЗИ RU.1190.5032.056) – техническое заключение от 15.01.2014, и экспертного заключения от 30.04.2014 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.A92.007).

Заявитель: ЗАО «Профессиональные Системы и Проекты. Профи-СП»
Адрес: 121471, г. Москва, Можайское шоссе, д. 29
Телефон: (495)995-9819

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 30 июня 2014 г.

ФЗ 149 «Об информации, информационных технологиях и о защите информации» ст.14 п.8: «…технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, **должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании**».

Пару слов о сертификации

Использование сертифицированных по требованиям безопасности средств защиты информации является необходимым для:

Государственных организаций, обрабатывающих информацию ограниченного доступа

Коммерческих организаций, работающие со «служебной информацией государственных органов»

Любых организаций, обрабатывающих персональные данные (ПДн)

Сертификация решений Фортинет

1. По результатам экспертизы материалов сертификационных испытаний комиссия отмечает, что программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS 5.4.1, разработанный компанией Fortinet и производимый ЗАО «Национальный Инновационный Центр» в соответствии с техническими условиями ТУ 5015-003-95561296-15, является межсетевым экраном и системой обнаружения вторжений, соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты.

Формуляр

Заверенная копия сертификата

Технические условия

Специальный защитный знак

Дистрибутив с сертифицированным эталоном


FORTINET