Check Point
SOFTWARE TECHNOLOGIES LTD.

РЕШЕНИЯ CHECK POINT ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

Дмитрий Кудра | Консультант по безопасности

Индустриальный сектор

ИНДУСТРИАЛЬНЫЙ СЕКТОР

Энергетика

- Энергетика
- Водоснаб.
- Газ
- НПЗ
- Химия

Транспорт

- Управление
- Диспетчерские
- Порты
- Морской транспорт

Производство

- Производство
- Переработка
- Сборка

Оборона

- ВПК

Индустриальные системы под угрозой!

Критичные и индустриальные системы формируют наш современный мир

Как и любые другие IT-системы, они подвержены атакам

Последствия таких атак значительно серьезнее:

Сбои электроэнергии

Наводнения и заргязнения воды

Сбои в транспортных системах

Неисправности производственных процессов

АСУ ТП Факты и реальность

Check Point
SOFTWARE TECHNOLOGIES LTD.

Декабрь 2014	Металлургический завод в Германии был атакован (атака Spear Phishing) – были причинены серьезные повреждения
Декабрь 2015	В Украине зафиксирована первая в истории государства успешная хакерская атака на сеть АСУ ТП Цель хакеров - «Прикарпатьеоблэнерго». Результат -Блэкаут на территории западной Украине (атака BlackEnergy malware) И повторная атака 19 января 2016
2015год	Американский центр реагирования на инциденты ICS-CERT, специализирующийся на угрозах для промышленных систем, за 2015 год получил от владельцев АСУ ТП и отраслевых партнеров сведения о **295 инцидентах** нарушения безопасности

Декабрь 2014:
Металлургический завод в Германии

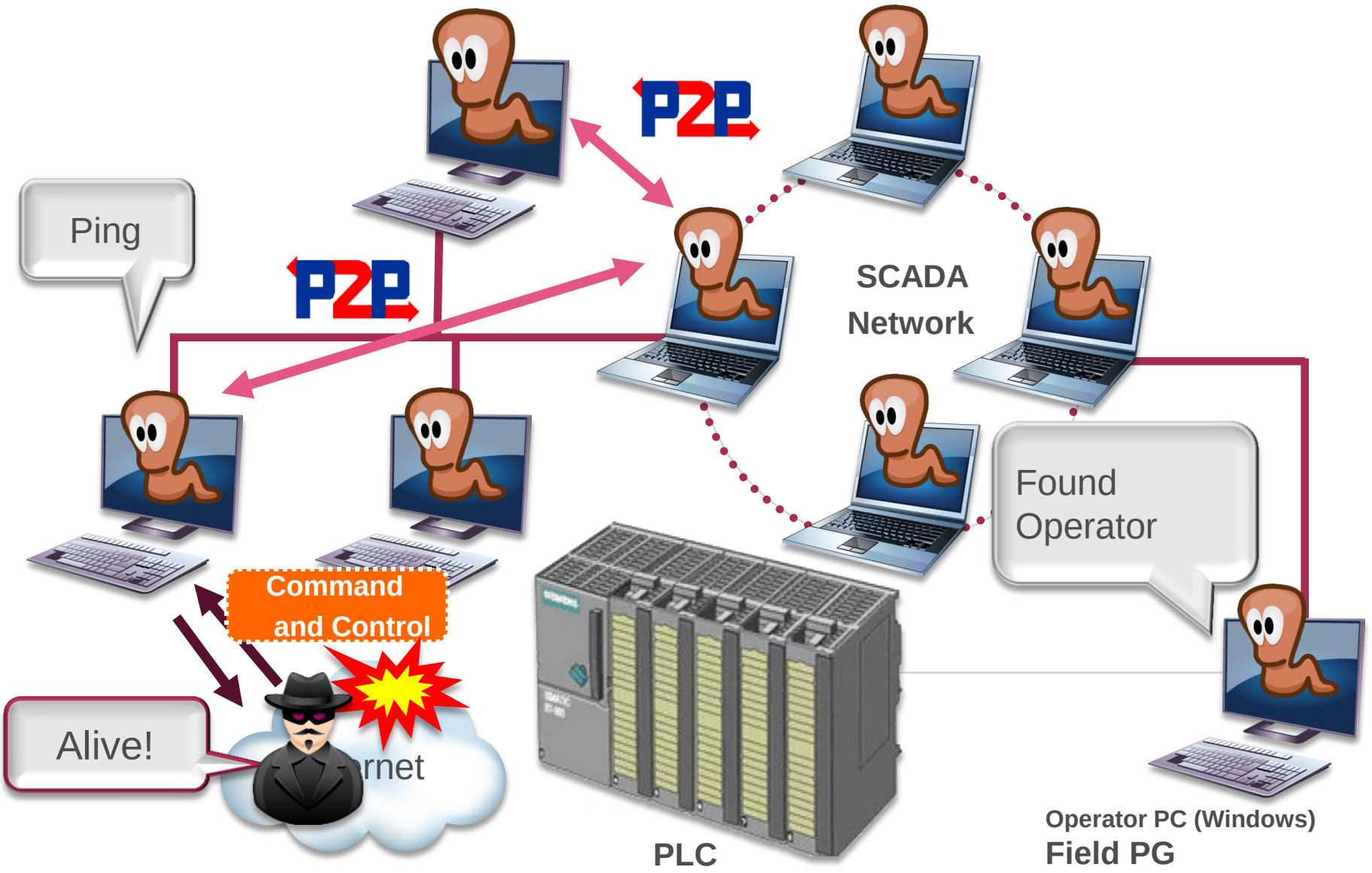
Check Point
SOFTWARE TECHNOLOGIES LTD.

https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Декабрь 2015: Энергетическая компания Украины «Прикарпатьеоблэнерго»

Check Point
SOFTWARE TECHNOLOGIES LTD.

Заражение и контроль



Расположение PLC (Цель)

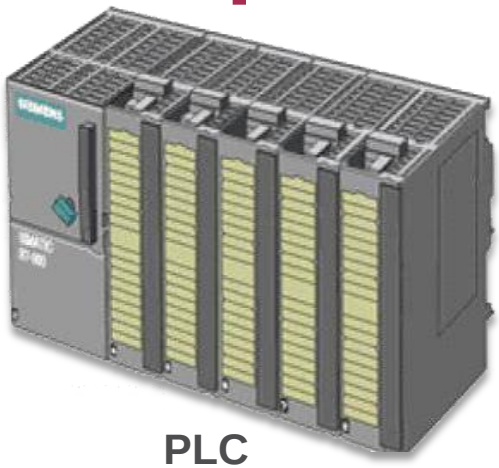
Check Point
SOFTWARE TECHNOLOGIES LTD.

Водопровод

Трубопровод

Станция очистки воды

Internal Network



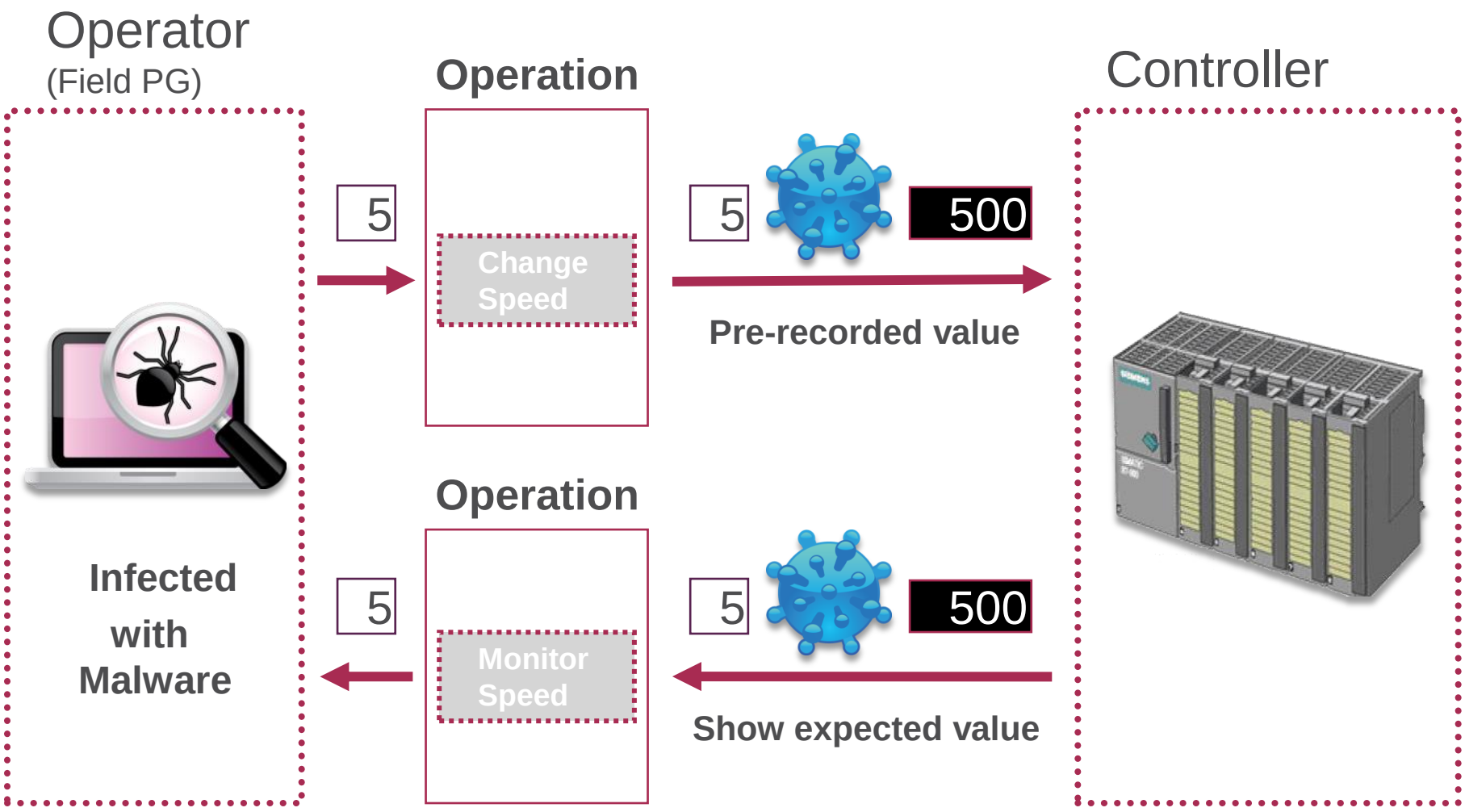
PLC

Write

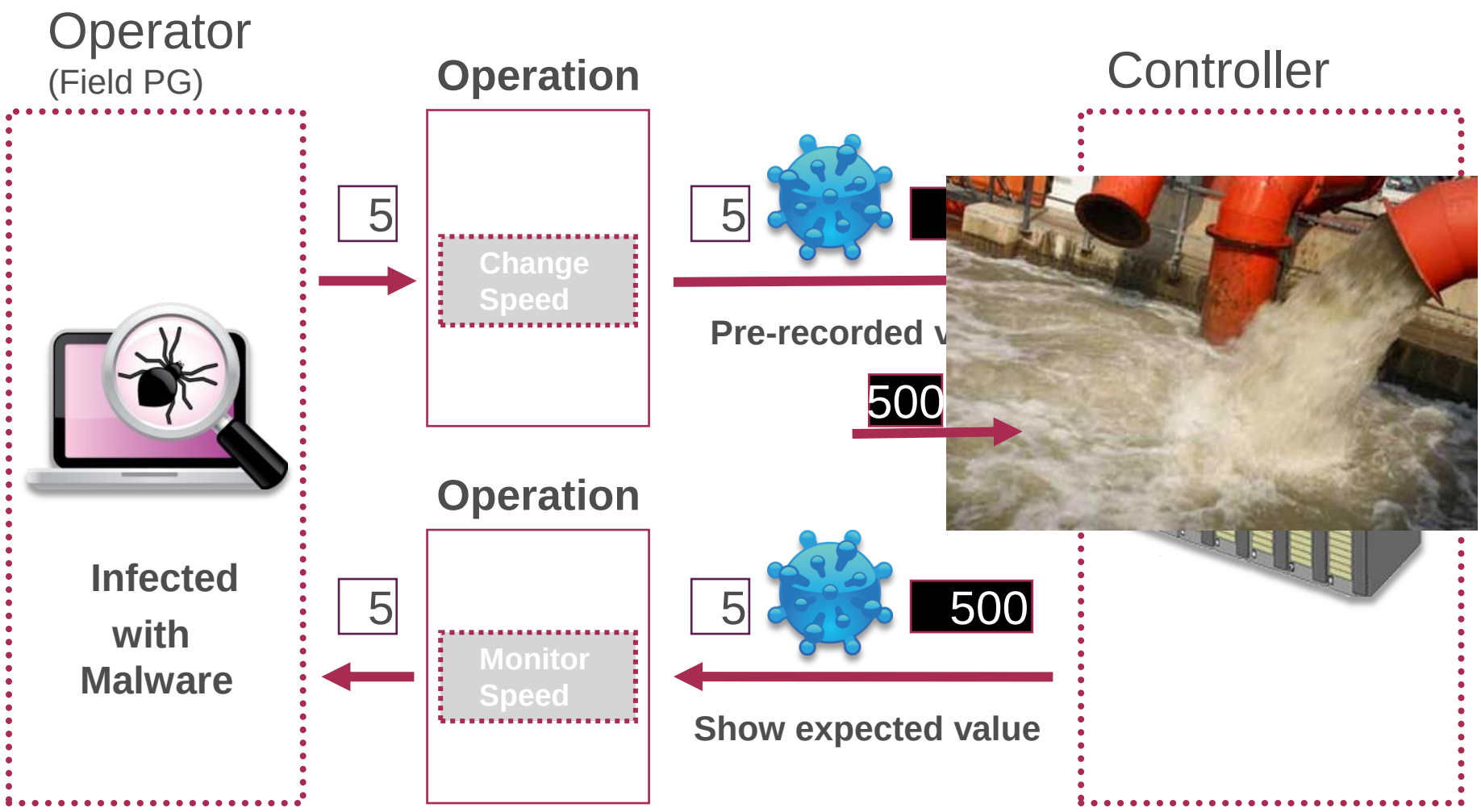
Read

Operator PC (Windows)
Field PG

Компрометация PLC Пример (READ/WRITE)



Компрометация PLC Пример (READ/WRITE)



Почему эти атаки возможны?

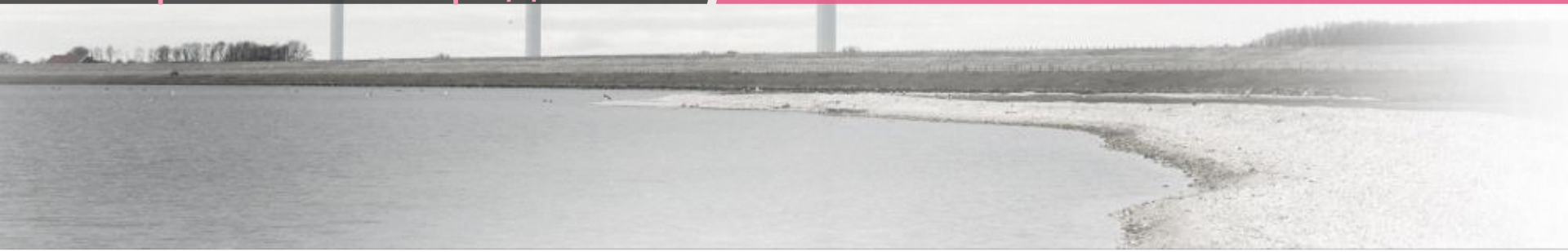
Устаревшие и необновленные системы

Ошибки в сегментации, подключение технологических сетей к Интернету

Задержки в обслуживании критических систем препятствуют адекватной защите

Требуется специализация на промышленных процессах

УСЛОВИЯ ОКРУЖЕНИЯ	ТРЕБОВАНИЯ БЕЗОПАСНОСТИ
Специализированные протоколы АСУ ТП между машинами операторов и контроллерами	Детализация АСУ ТП трафика до уровня команд
Специализированные системы в условиях непрерывности производства и агрессивной среды	Надежная платформа для обеспечения безопасности в тяжелых условиях



Представляем:

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

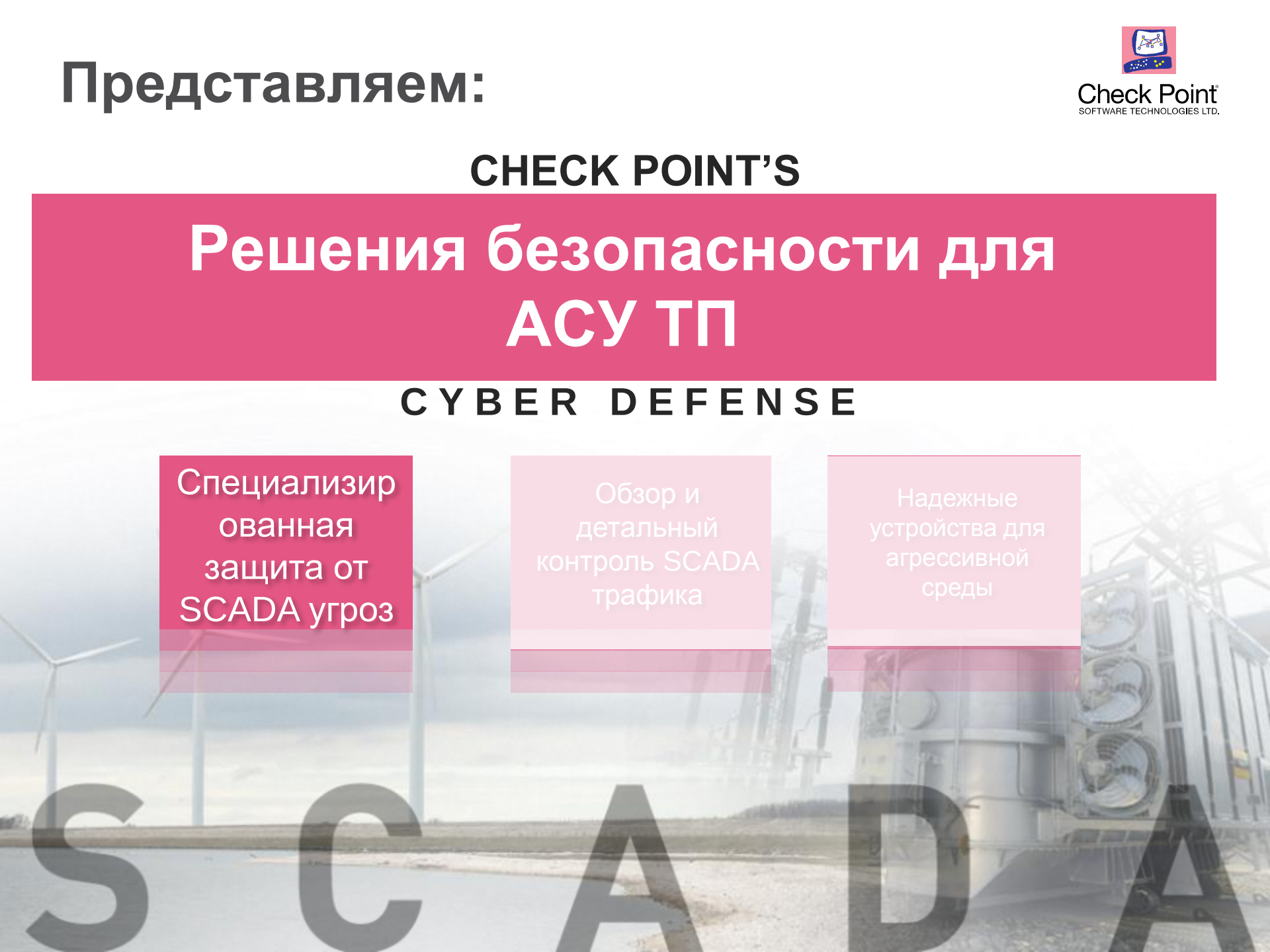
Решения безопасности для АСУ ТП

CYBER DEFENSE

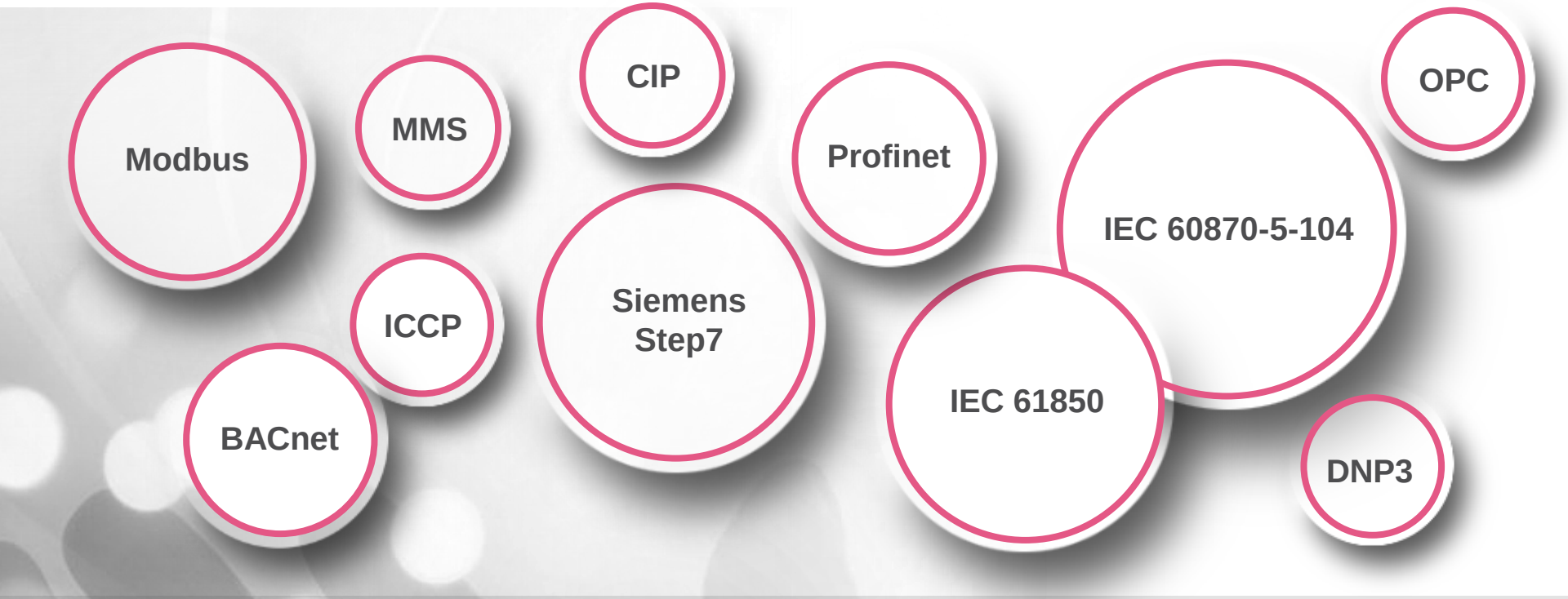
Специализированная защита от SCADA угроз

Обзор и детальный контроль SCADA трафика

Надежные устройства для агрессивной среды

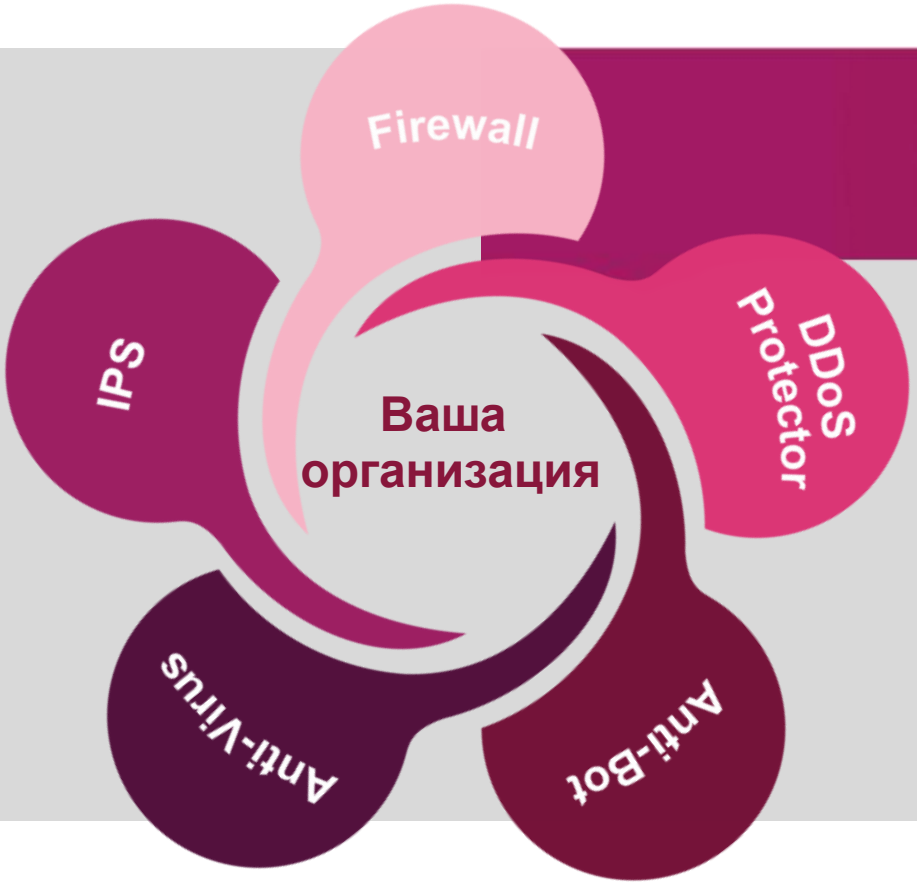


Обширная поддержка SCADA/ICS-специализированных протоколов



Свыше 720 АСУ ТП команд в Check Point Application Control

Комплексная защита от угроз



IPS

Блокирует запусков эксплойтов и известных уязвимостей

NSS Labs
Highest Rating

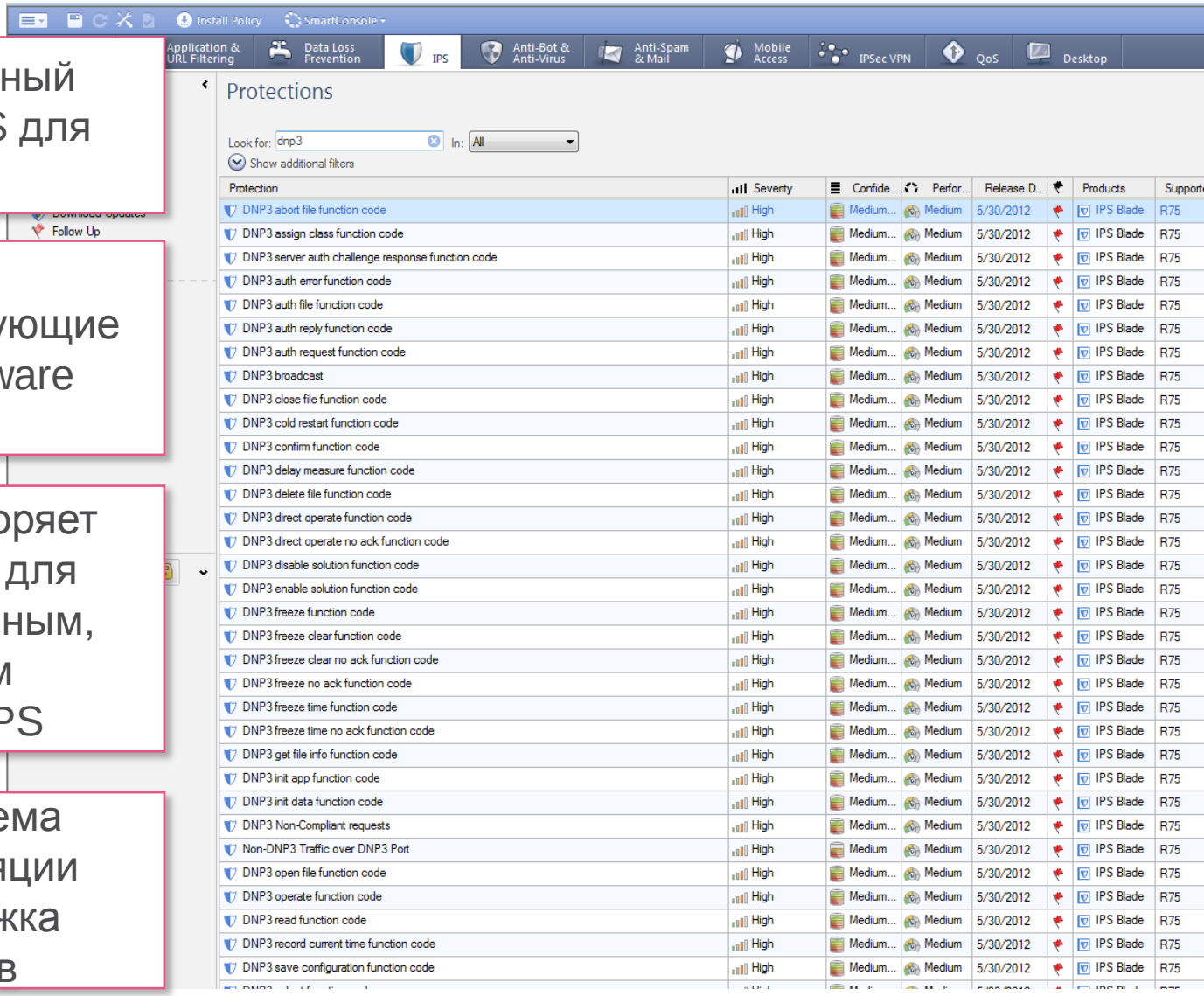
Защита от SCADA эксплойтов в IPS

Специализированный набор сигнатур IPS для SCADA

Используется занимающий лидирующие позиции IPS Software Blade

Решение удовлетворяет как специфичным для SCADA, так и обычным, корпоративным требованиям к IPS

Встроенная система анализа и корреляции событий, поддержка захвата пакетов



Устаревшие системы не обновлены

Виртуальный патчинг с около 200 специализированными IDS/IPS сигнатурами

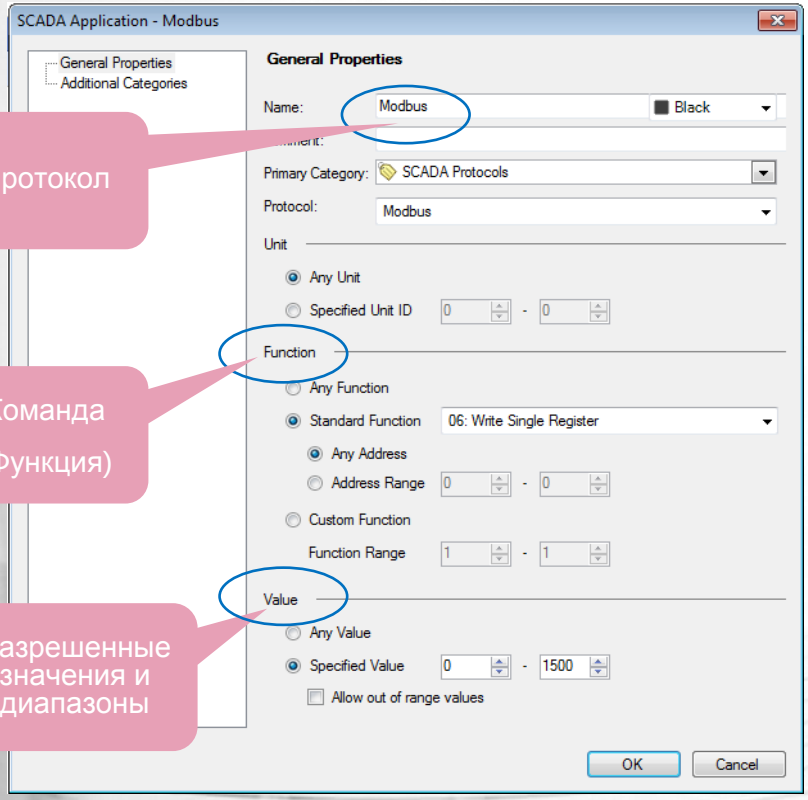
Check Point

Защищено Check Point IPS

Protection	Sever...
Citect SCADA ODBC Overflow Attempt	Medium
Rockwell RSLogix Denial of Service Vulnerability	Critical
SCADA Engine OPC Client Buffer Overflow Vulnerability	High
Schneider Electric UnitelWay Windows Device Driver Buffer Overflow	Critical
Siemens Tecnomatix FactoryLink Stack Overflow Vulnerability	Critical
Siemens Automation License Manager Multiple Vulnerabilities	Critical
ScadaTEC SCADAPhone and ModbusTagServer Buffer Overflow	High
RealWin HMI Service Buffer Overflow 2	High
Automated Solutions Modbus/TCP Master OPC server Modbus TCP Header	High
RealWin INFOTAG/SET_CONTROL Packet Processing Buffer Overflow	High
Unauthorized Miscellaneous Request to a PLC	Critical
Broadcast Request from an Authorized Client	Critical
IGSS SCADA RMS Report Template WriteFile Command Buffer Overflow	Critical
IGSS SCADA STDREP Request Buffer Overflow	High
Iconics Genesis SCADA Freeing of Unitialized Memory Trigger	High
Rockwell RNA Message Negative Header Length	Critical
Intellicom NetBiter Config HICP Hostname Buffer Overflow	Medium
WonderWare SuiteLink DOS Attempt	High

Политики/Правила на основе Функций и Значений в SCADA командах

- Специализированные Политики и Правила для защиты АСУ ТП
- Правила для АСУ ТП протоколов с учетом направления коммуникации
- Настройка политики до уровня конкретных команд: например, read/write/get



Name	Source	Destination	Applications/Sites	Action
Block High Risk apps	Any	Any	High Risk	Block Blocked
Control servers	Control_servers	PLCs	Modbus Protocol-write single register Modbus Protocol-write multiple coils Modbus Protocol-write file record Modbus Protocol-write single coil	Allow
Monitor servers	Monitor_servers	PLCs	Modbus Protocol-read input register Modbus Protocol-read coils Modbus Protocol-read file record	Allow
Block SCADA traffic	Any	Internal PLCs	SCADA Protocols	Block

Name	Source	Destination	Applications/Sites	Action
Single Point ASDUs	Master	RTU	IEC 60870-5-104 - Single Point Information IEC 60870-5-104 - Single Point Information With Time Tag CP56Time2a	Allow
Double Point ASDUs	Master	RTU	IEC 60870-5-104 - Double Point Information IEC 60870-5-104 - Double Point Information With Time Tag CP56Time2a	Allow
Step Point ASDU	Master	RTU	IEC 60870-5-104 - Step Position Information	Allow
Measured Value ASDU	Master	RTU	IEC 60870-5-104 - Measured Value, Normalized Value	Allow
Any other communication between master and RTU	Master	RTU	Any Recognized	Allow

Firewall

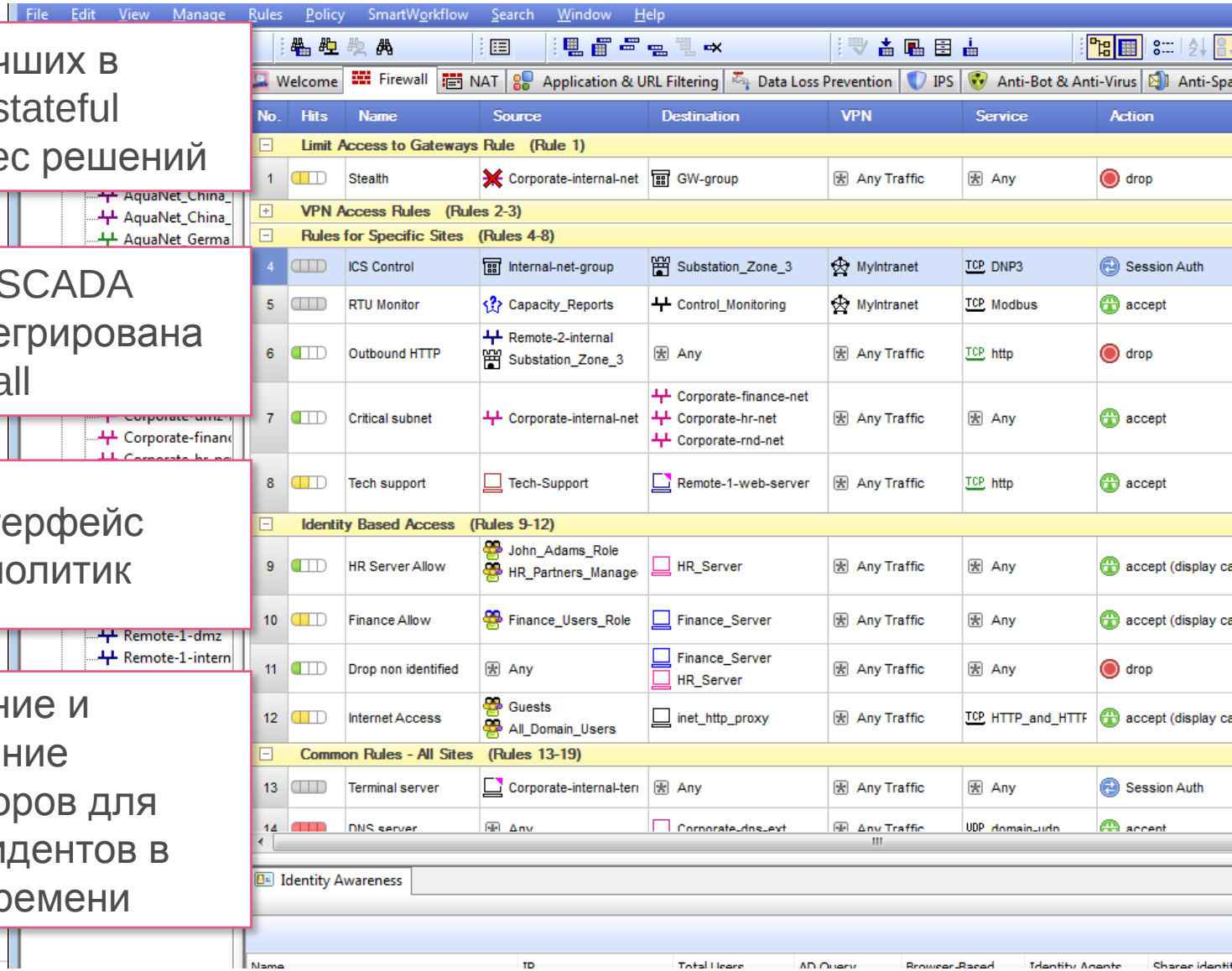
Check Point
SOFTWARE TECHNOLOGIES LTD.

Одно из лучших в индустрии stateful inspection и IPSec решений

Поддержка SCADA протоколов интегрирована в firewall

Удобный интерфейс написания политик

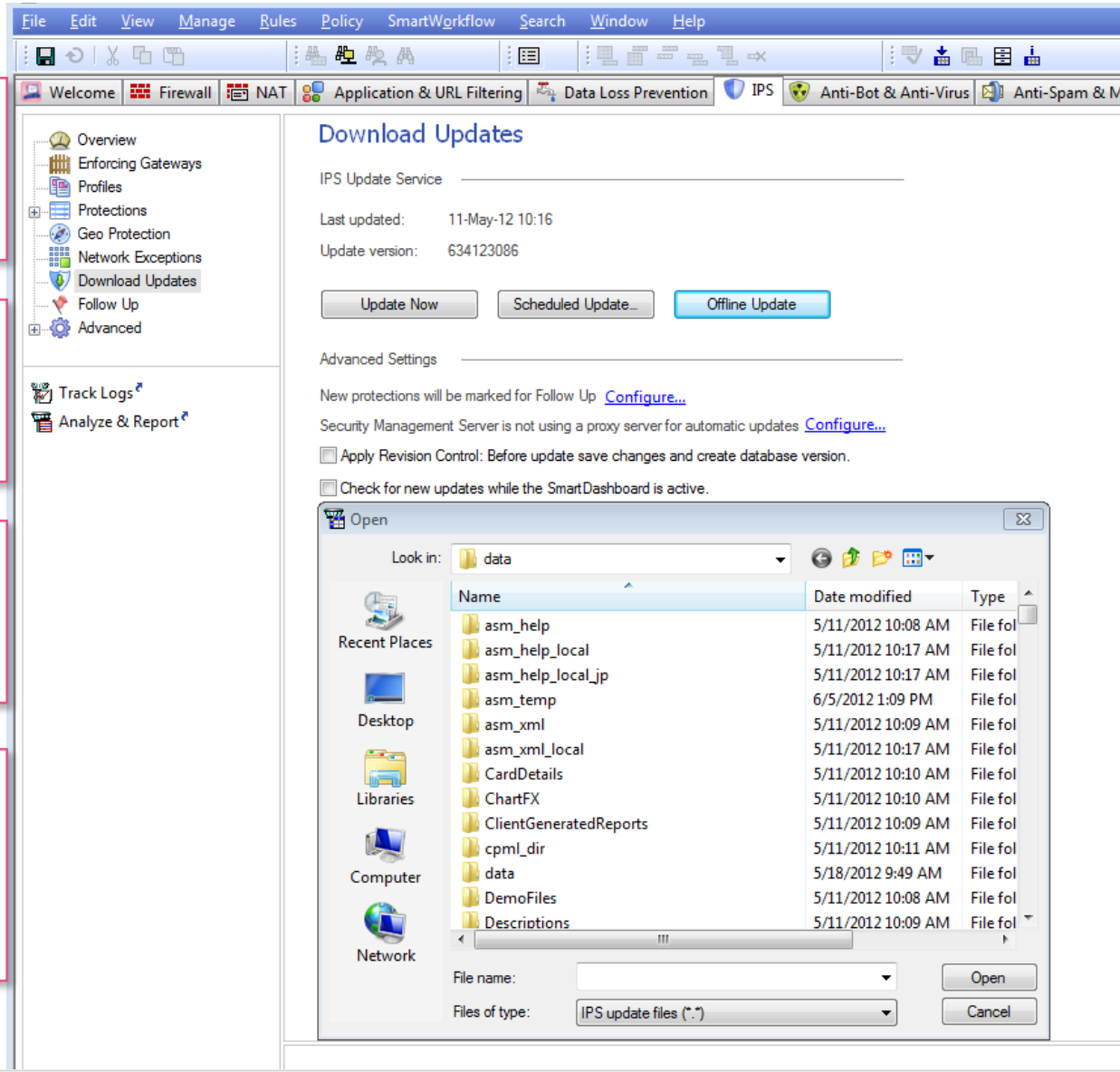
Логирование и оповещение администраторов для контроля инцидентов в реальном времени



Обновление сигнатур – Online и Offline

Check Point

- Постоянное совершенствование сигнатур
- Централизованное обновление
- Распространение в режиме online и offline
- Механизм Workflow для аудита, отслеживания изменения конфигураций



Противодействие угрозам

Check Point
SOFTWARE TECHNOLOGIES LTD.

Многоуровневая система противодействия современным угрозам

Предотвращает атаки на приложения

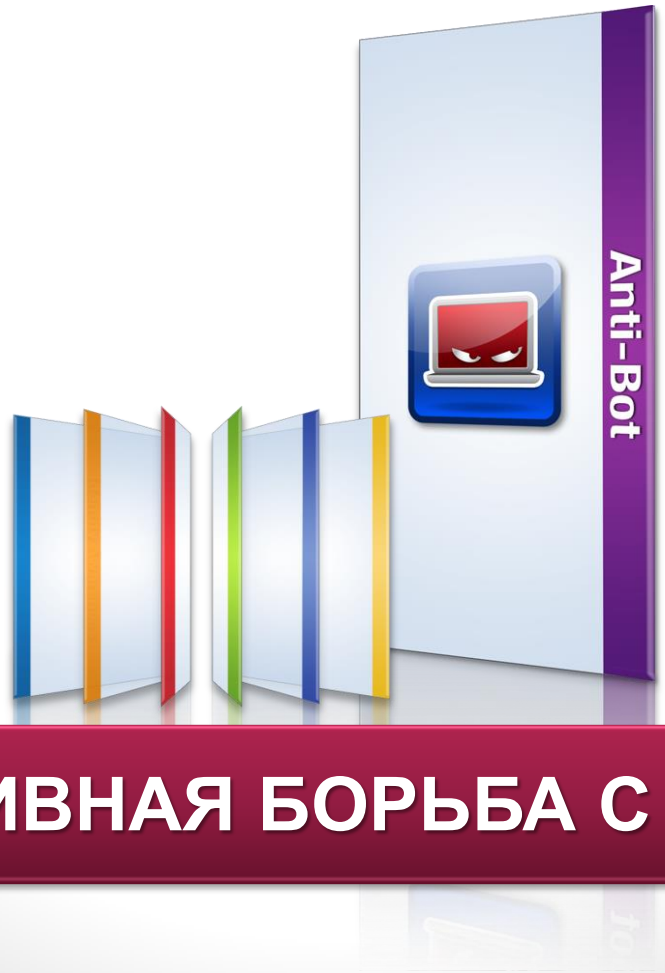
Борется с вирусами

Обезвреживает ботов

Противодействие ботнетам

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point
Anti-Bot Software Blade



ЭФФЕКТИВНАЯ БОРЬБА С БОТАМИ!

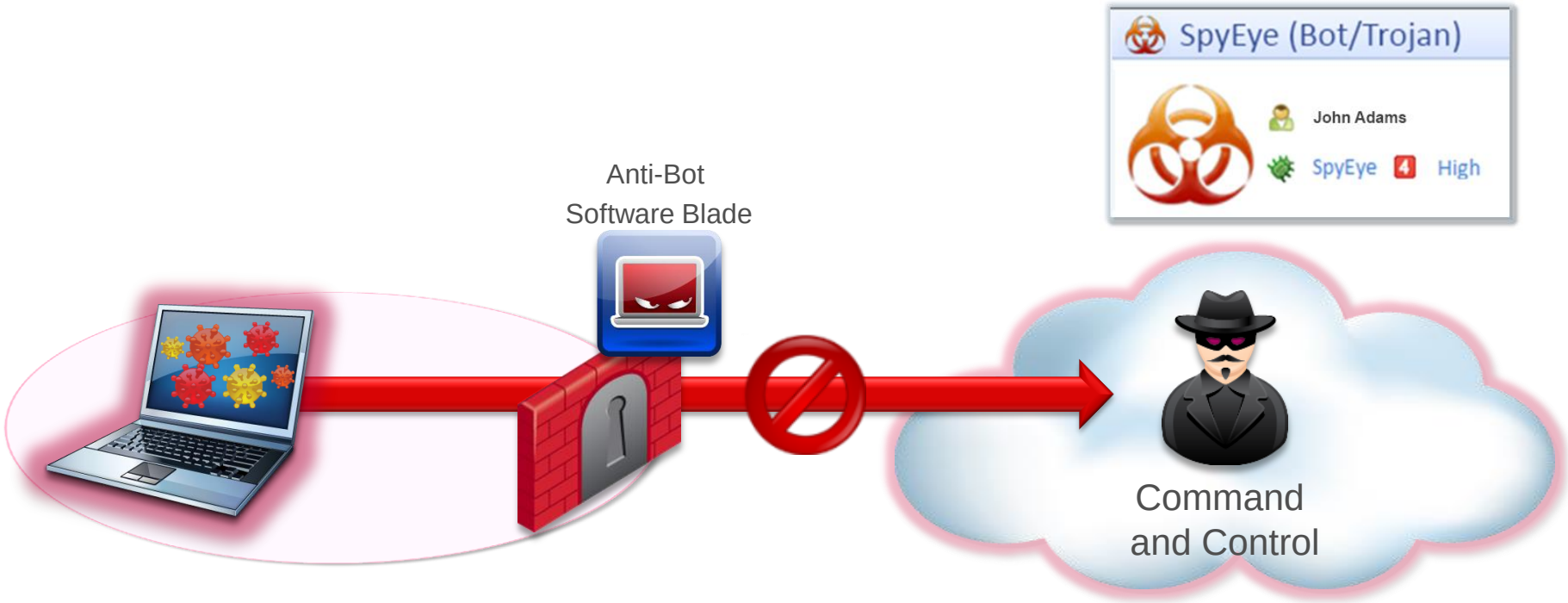
Check Point Anti-Bot Software Blade

Check Point
SOFTWARE TECHNOLOGIES LTD.

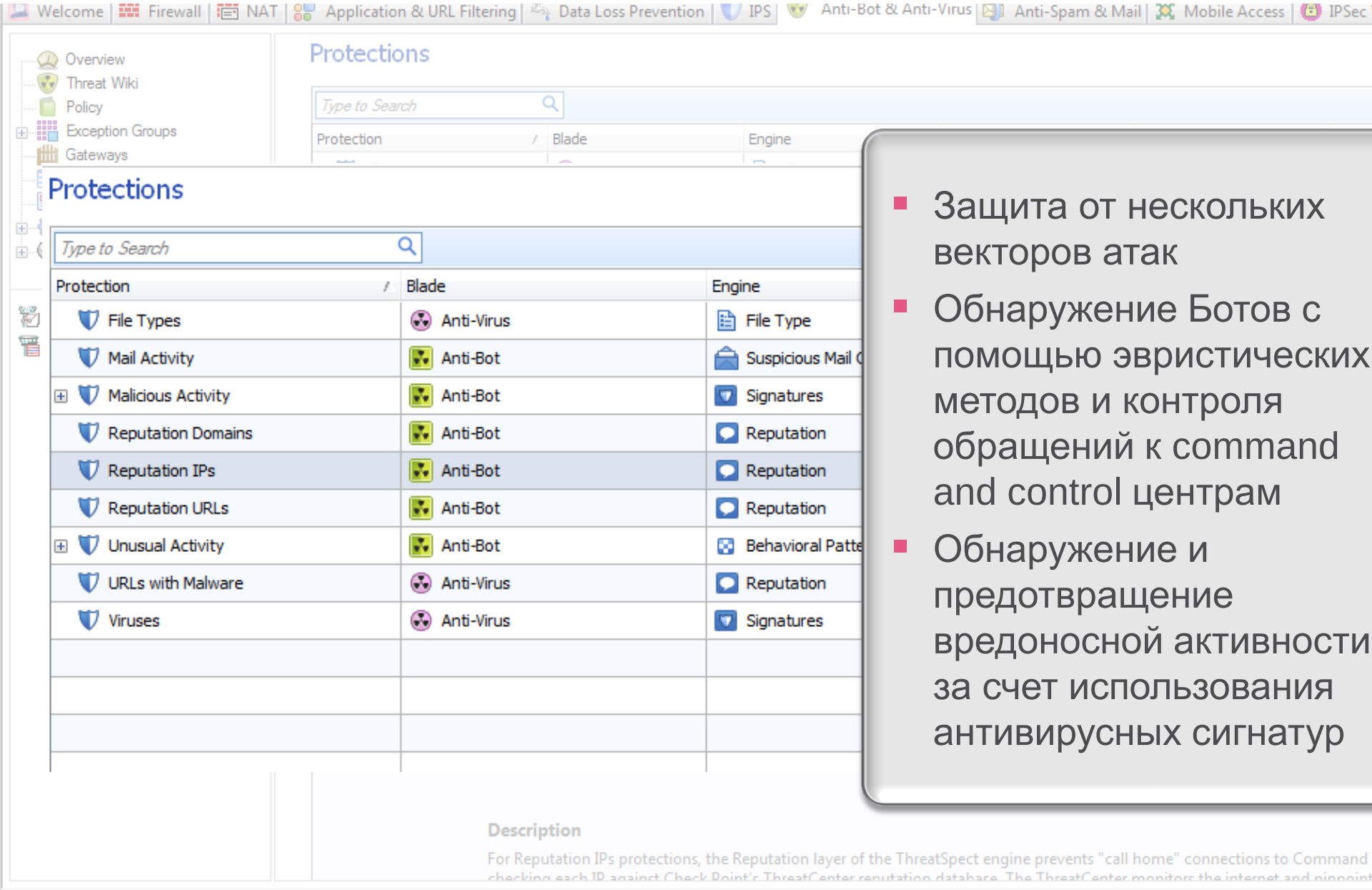
Находит зараженные машины

Обезвреживает зараженные машины

Интегрированная система



Защита от ботнетов и вредоносного ПО



- Защита от нескольких векторов атак
- Обнаружение Ботов с помощью эвристических методов и контроля обращений к command and control центрам
- Обнаружение и предотвращение вредоносной активности за счет использования антивирусных сигнатур

Представляем:

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

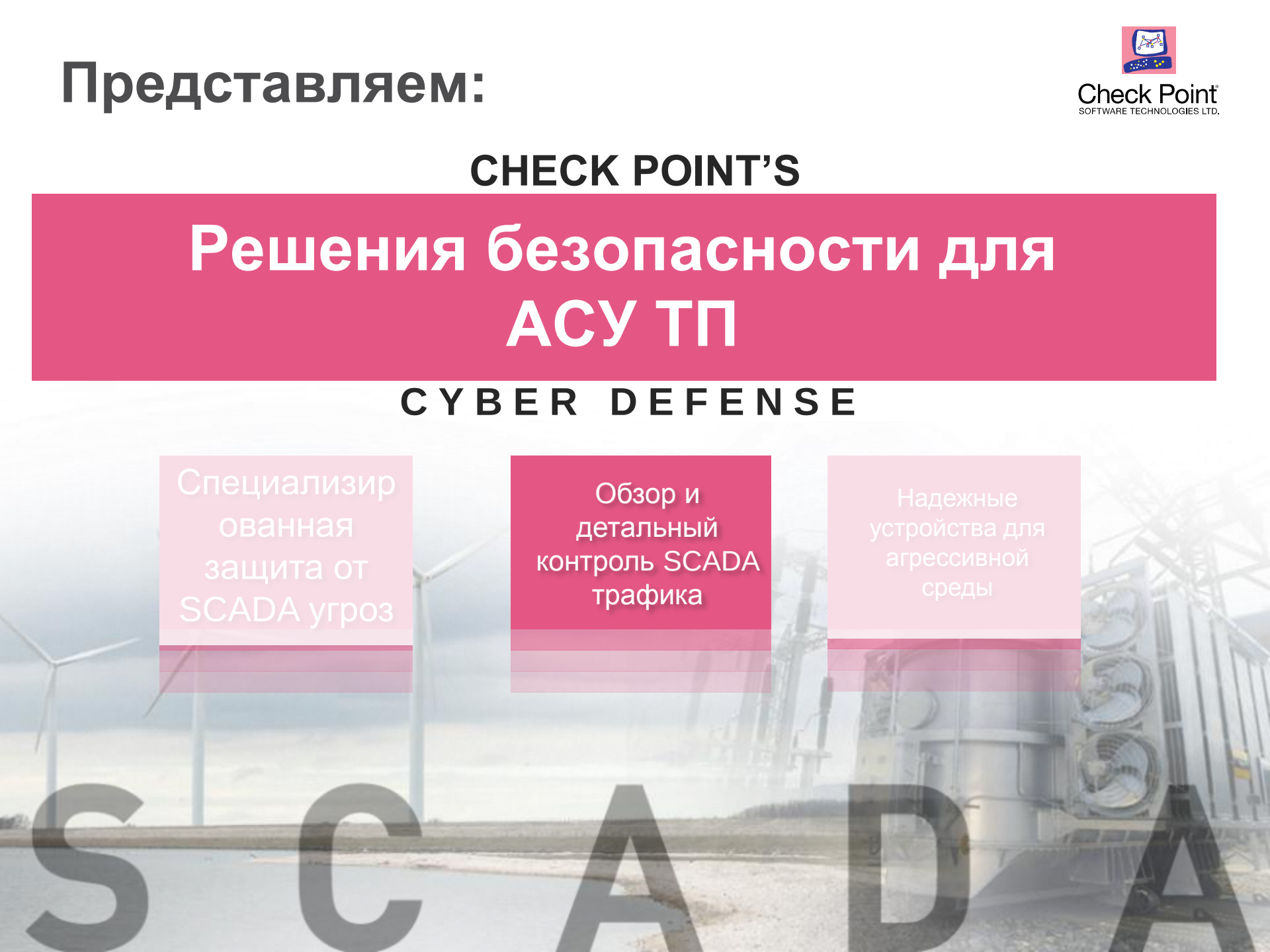
Решения безопасности для АСУ ТП

CYBER DEFENSE

Специализированная защита от SCADA угроз

Обзор и детальный контроль SCADA трафика

Надежные устройства для агрессивной среды



Гранулярное логирование АСУ ТП трафика до уровня команд

Check Point
SOFTWARE TECHNOLOGIES LTD.

Может использоваться для расследования инцидентов

Проанализировано
Check Point
SMARTLOG и SMARTEVENT

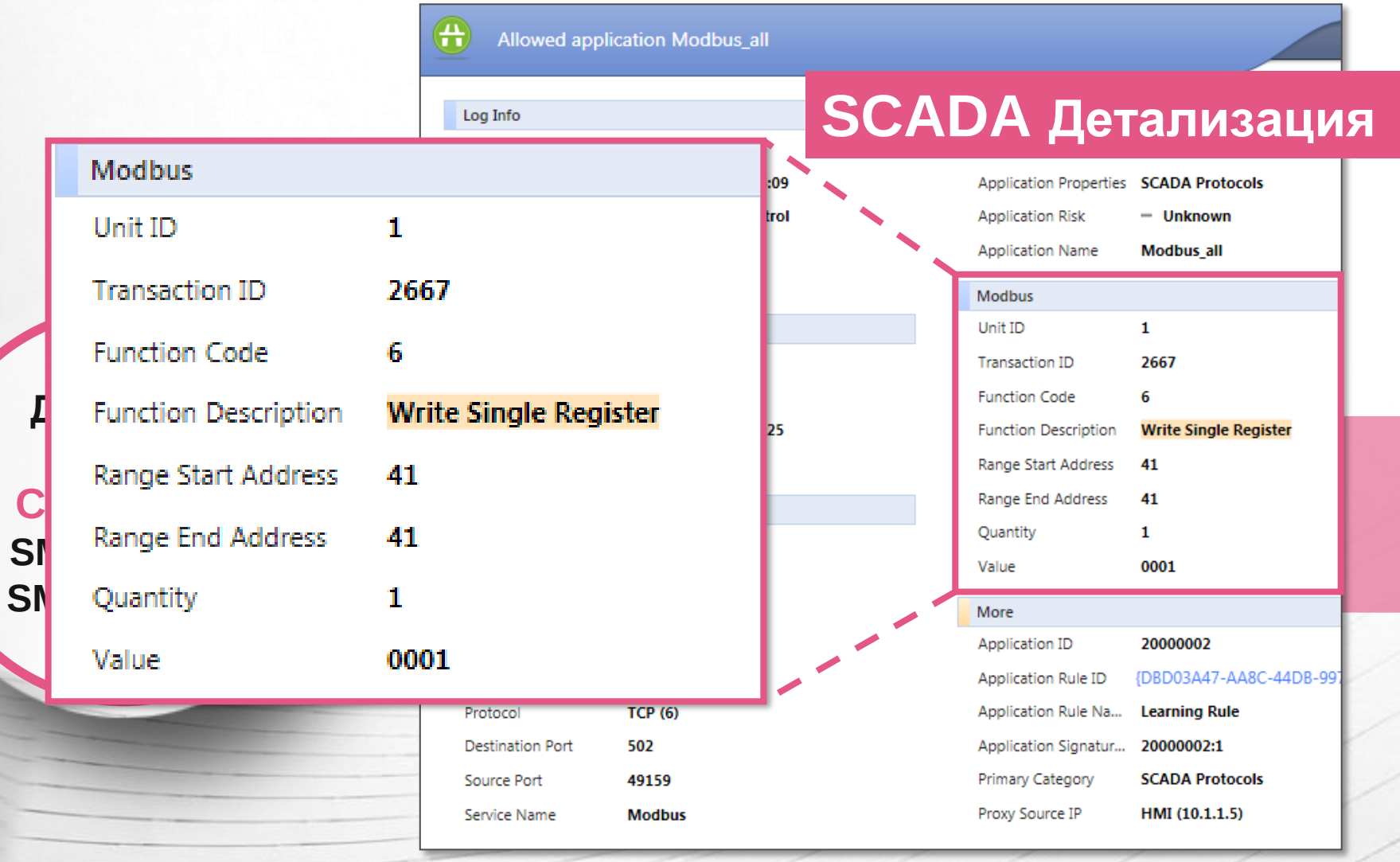
Подробно

Time		B...	A...	T...	Origin	Application...	Transa...	Fu...	Function Description	Source	Desti...	...	Matched Ca
Today	10:45:35				gw-71ec22	ModbusAll	33394	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33490	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33490	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33489	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33489	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33488	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33488	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33487	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33487	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33486	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33486	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33485	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33485	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33484	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33484	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33483	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33483	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33482	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33482	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33481	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33481	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33480	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot

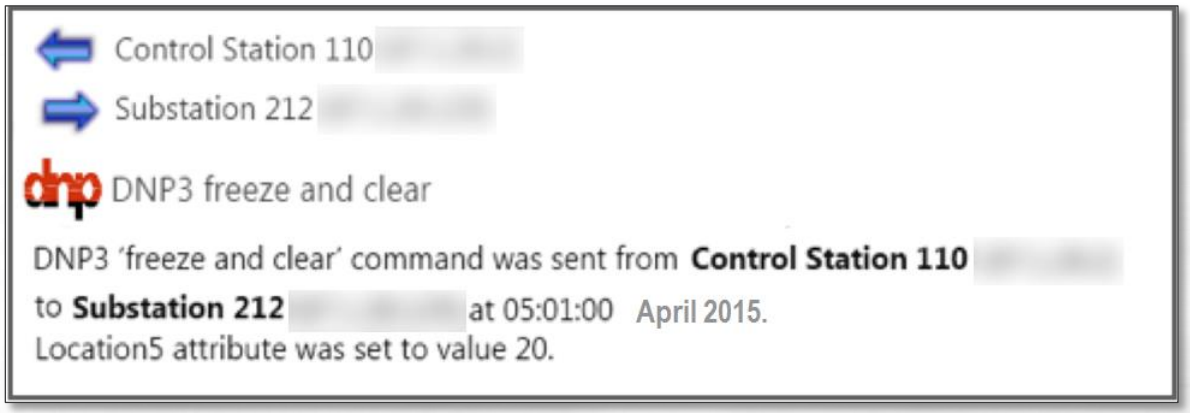
Сгруппировано

Count	Source	Destination	Unit ID	Function Description	Transaction ID	Start Address
500	**HMI (10.1.1.5)**	**PLC (20.1.1.5)**	**1**	**Read Holding Registers**		
100	**HMI (10.1.1.5)**	**PLC (20.1.1.5)**	**1**	**Read Input Registers**		**10**
1	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Write Single Register	19	50

Детальные отчеты по трафику АСУ ТП



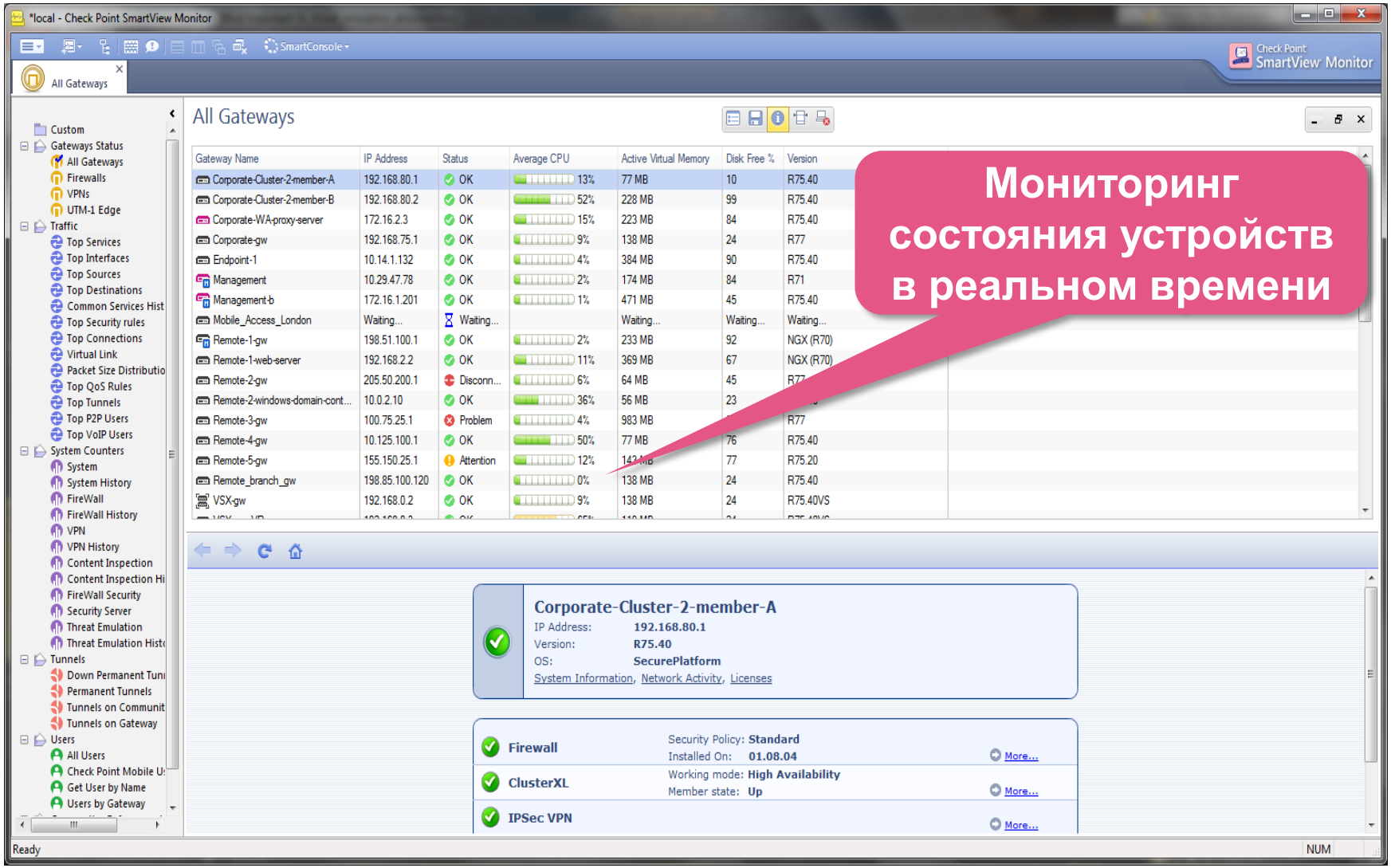
Мгновенный анализ подозрительного трафика между контроллерами



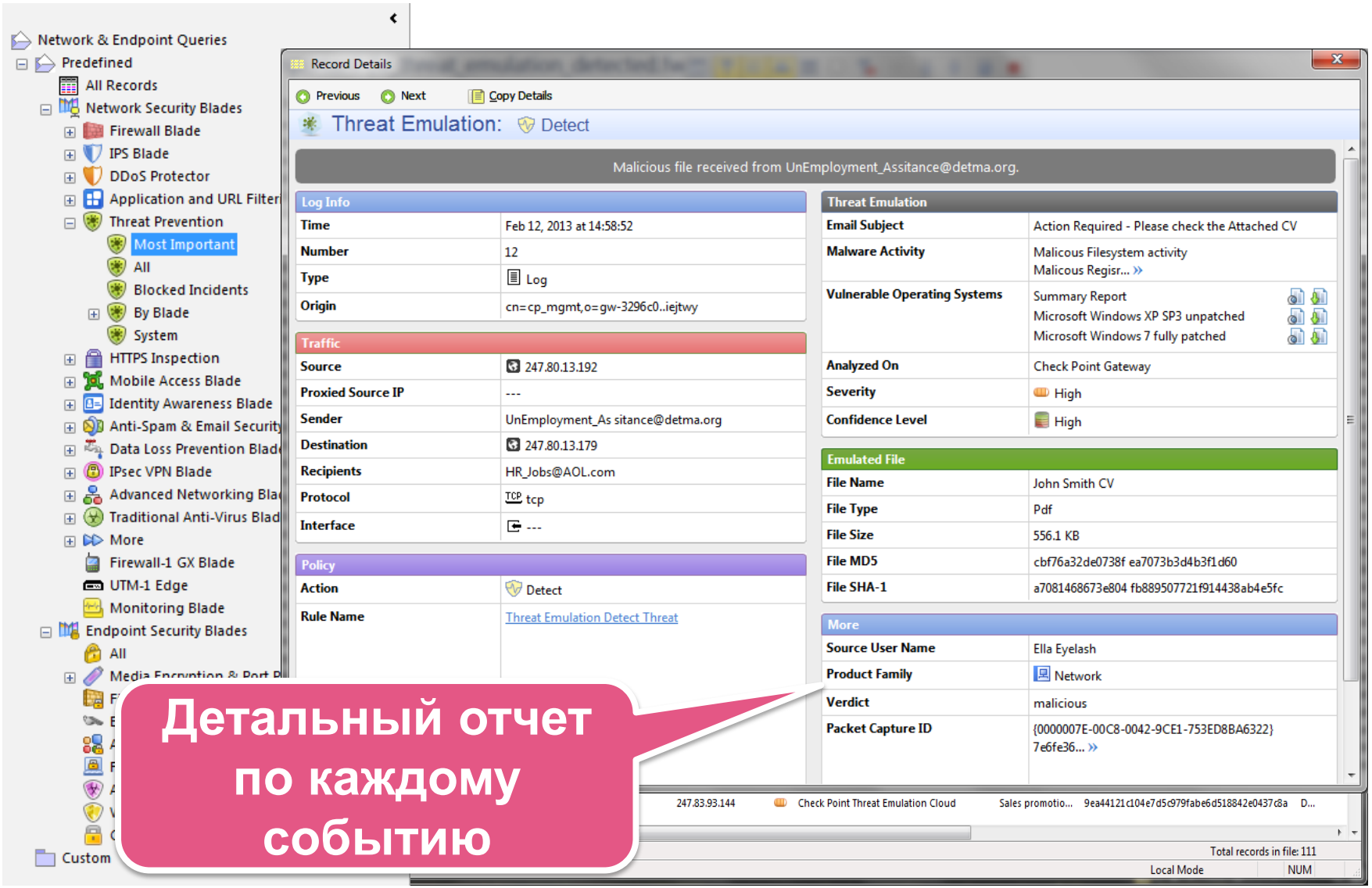
Проанализировано
Check Point
SMARTEVENT

- Анализ рисков с помощью специализированных отчетов по угрозам
- Отслеживание попыток отправки подозрительного количества комманд
- Отслеживание попыток разведки сети

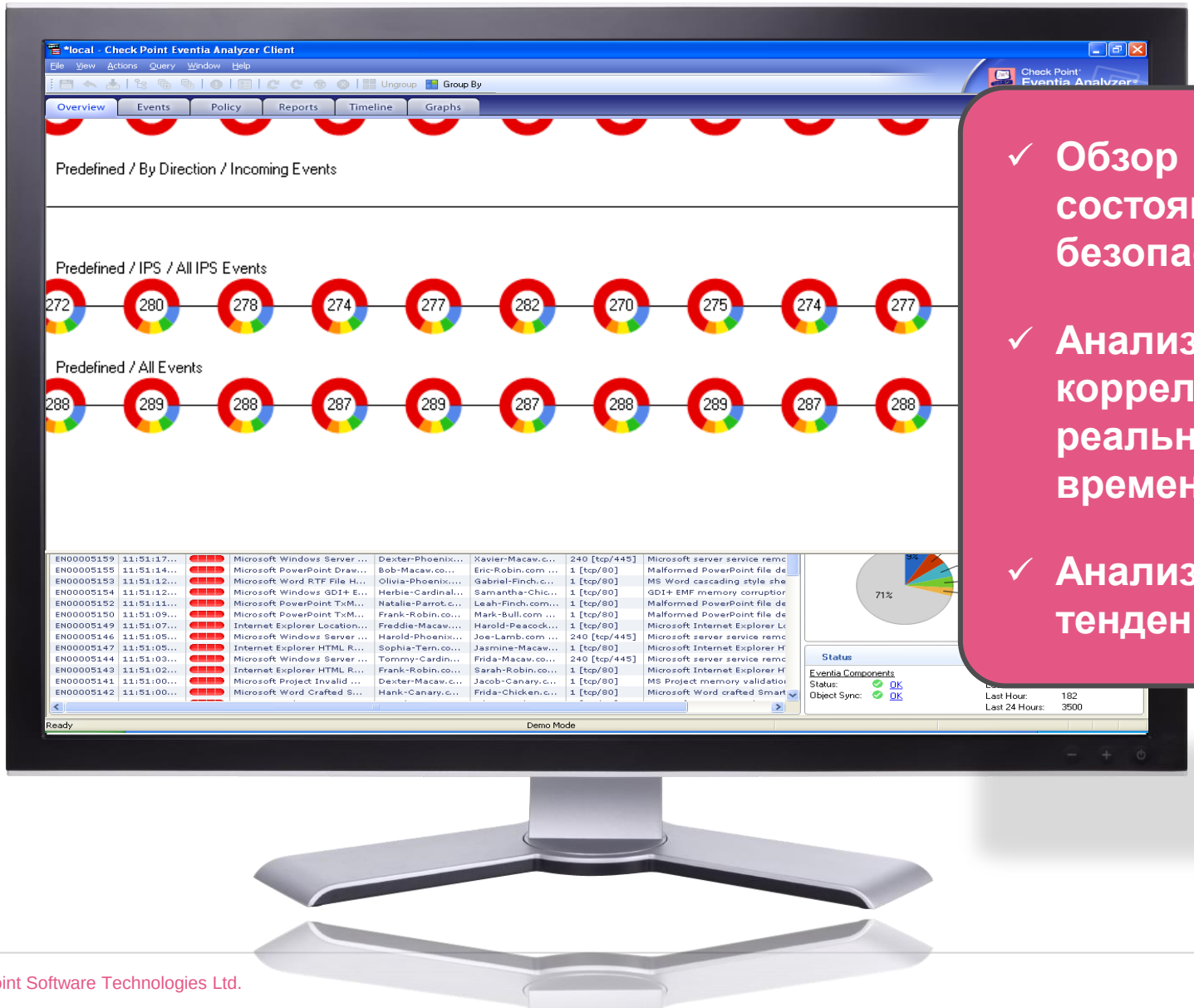
SmartView Monitor



SmartView Tracker



SmartEvent



- ✓ **Обзор состояния безопасности**
- ✓ **Анализ и корреляция в реальном времени**
- ✓ **Анализ тенденций**

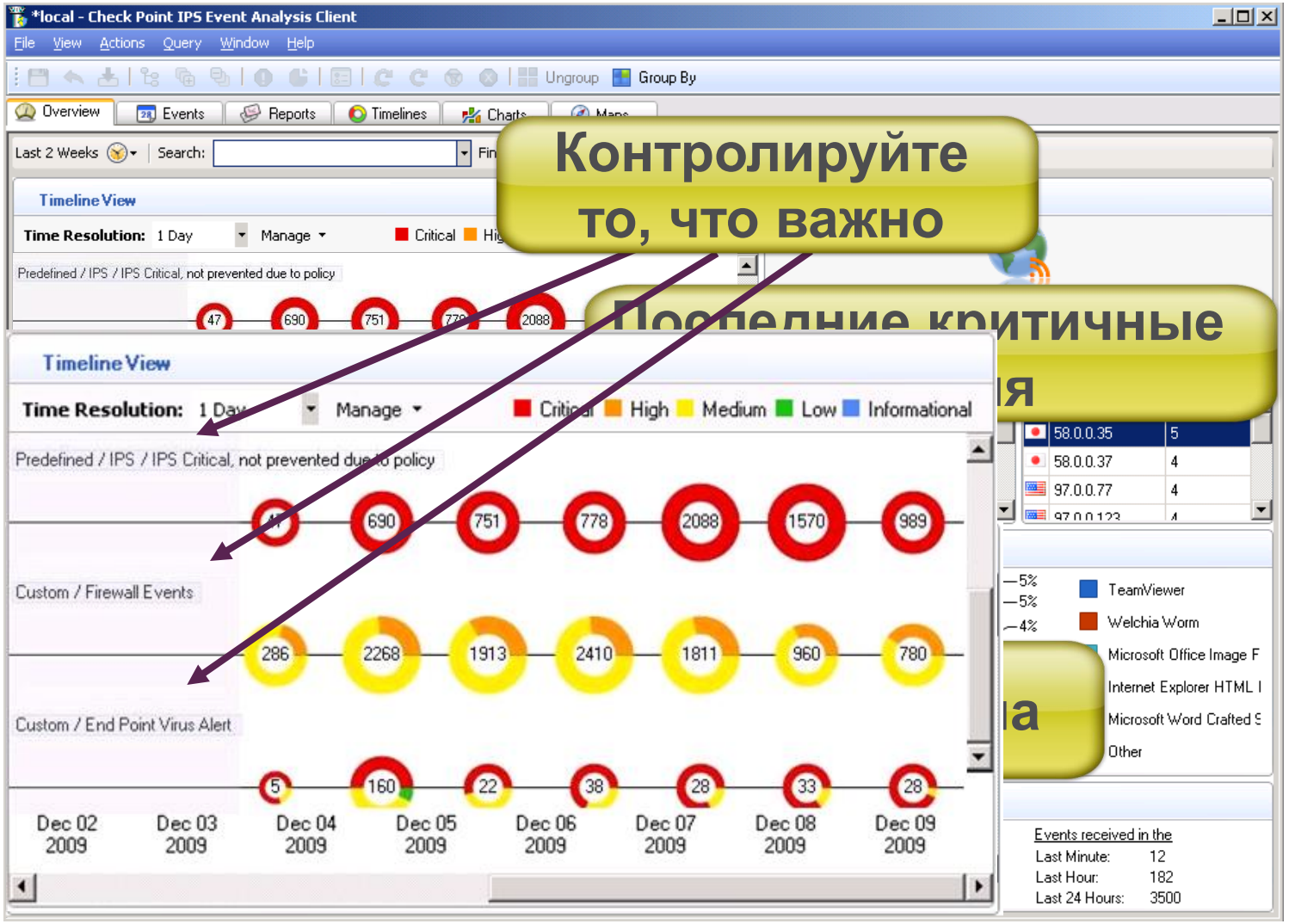
Контроль за событиями

Временная шкала

- Количество и важность атак
- Просто кликните мышкой для дальнейшего анализа
- Кастомизация – добавление своих временных шкал

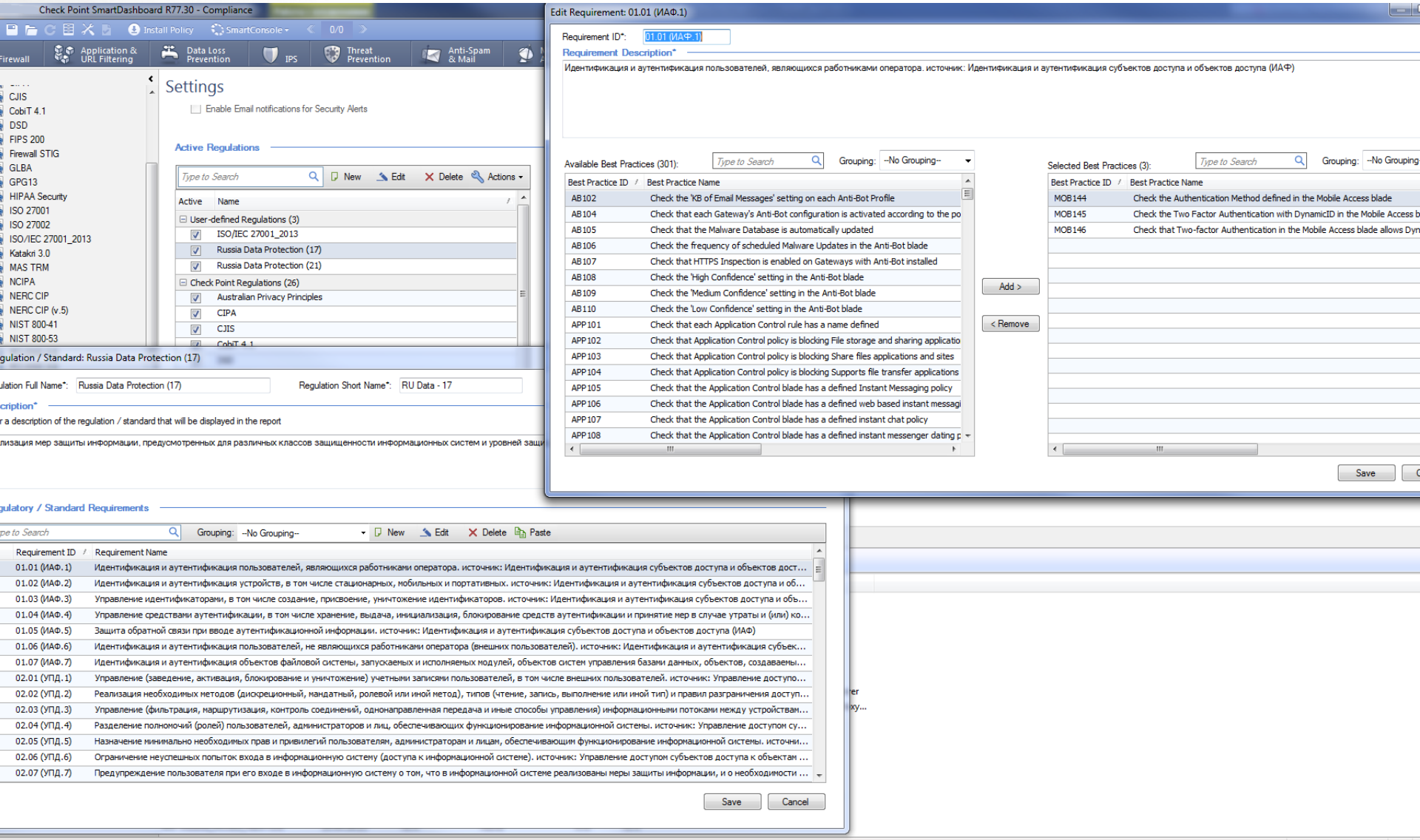
Последние критичные события

- Обзор последних критичных событий
- Просто кликните мышкой для дальнейшего анализа



Мониторинг соответствия специализированным стандартам и правилам

Check Point
SOFTWARE TECHNOLOGIES LTD.



Представляем:

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

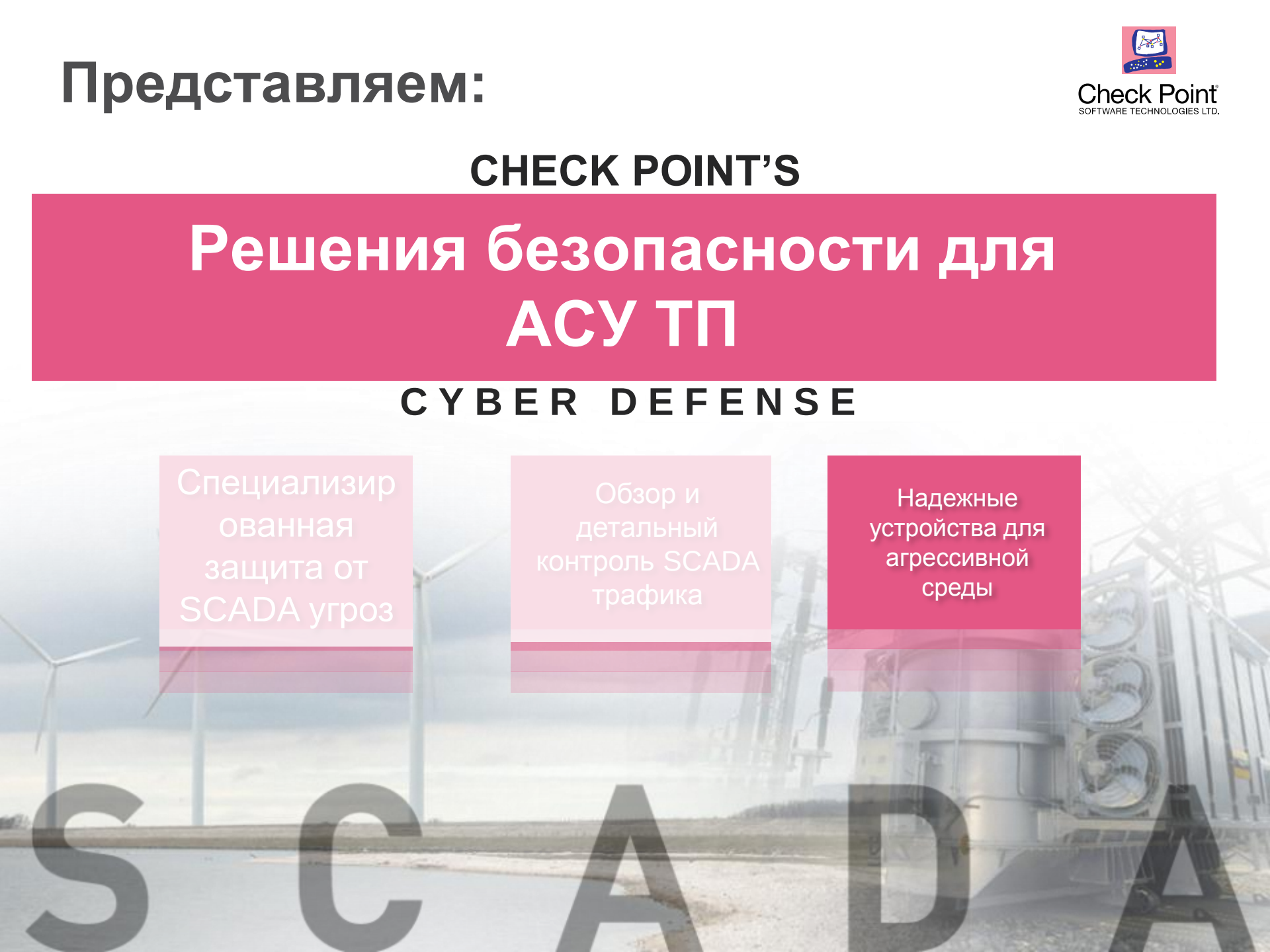
Решения безопасности для АСУ ТП

CYBER DEFENSE

Специализированная защита от SCADA угроз

Обзор и детальный контроль SCADA трафика

Надежные устройства для агрессивной среды



Спецификация устройств

Индустриальные решения Check Point

Универсальность

Функциональность

- 1200R
- IAS U1
- 3200 (2016 Appliances + SSD + DC)
- Integrated Security Module for Siemens / RuggedCom 1500 Switch

Защита АСУ ТП с помощью Check Point

Линейка устройств в индустриальном исполнении

- Работа в широком диапазоне температур, влажности
- Отсутствие движущихся частей
- Соответствие международным стандартам IEC 61850-3 и IEEE 1613

IAS U1

IAS T1

RuggedCom/Siemens

1200R

Монтаж на Din-рейку

Средняя производительность

Монтаж в стойку

Высокая производительность

Монтаж в стойку

Линейка устройств Check Point

Для защиты предприятий любых масштабов

41000 и **61000**
23000 линейка
(3 модели)

15000 Appliances
(2 модели)

Крупный офис

Защита ЦОД

Защита сервис провайдеров

3200 Appliance
1400 Appliances
(4 модели)

Малый офис

5000 Appliances
(4 модели)

Средний офис

CHECK POINT 1200R

Check Point
SOFTWARE TECHNOLOGIES LTD.

Специализированное решение для применения в промышленных и SCADA сетях

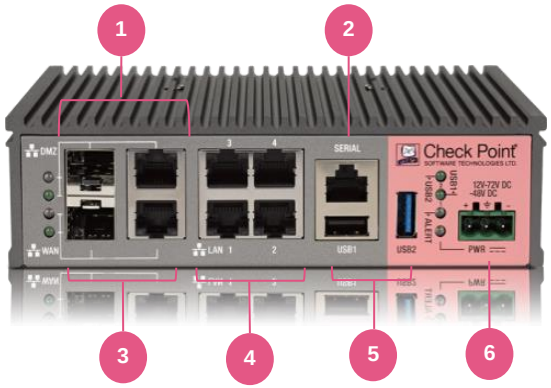
CHECK POINT 1200R

- **Надежное решение**
  - Специализированное решение
  - Прочная конструкция – высокий уровень MTBF около 300,000 часов
  - Различные варианты монтажа и питания AC/DC
- **Функциональность**
  - Firewall,
  - IPS,
  - Application Control & URL Filtering,
  - Antivirus & AntiBot
  - IPSec VPN
- **Различные варианты управления**
  - SMART архитектура
  - Локальное управление
  - Out-of-the-box развертывание
- **Промышленное применение**
  - SCADA + Modbus, BACNet, DNP3, MMS, Profinet, S7 (Siemens) и прочие
  - IPS

Платформа

Check Point 1200R

1. DMZ порт (медный или оптический)
2. Консольный порт RJ-45
3. WAN-порт **(медный или оптический)**
4. LAN-порты (4 x 10/100/1000BaseT)
5. USB-порты (2.0/3.0)
6. DC питание
7. AC питание
8. SD card слот (для хранения логов)
9. Крепления для установки DIN рейки



DIN rail

Check Point 1200R- Спецификация

Производительность:

- 49 SecurityPower[1] Units
- Пропускная способность МСЭ 2 Гбит/с, 1518 байт UDP
- 700 Мбит/с МСЭ, смешанный трафик
- 60 Мбит/с МСЭ и IPS, смешанный трафик
- Пропускная способность VPN 450 Мбит/с
- 400,000 одновременных соединений

Соответствие требованиям:

- IEEE 1613 , IEC 61850-3
- CE, EN 55024, EN 55022
- EN 61000-3, EN 61000-4
- CB, IEC 60950, UL 60950

- Температура и влажность:
  - от -40 до 75°C,
  - 20%-90%
- Соответствует промышленным стандартам по температуре, вибрациям, влажности и ЭМИ
- Отсутствие движущихся частей
- Гибкие варианты монтажа устройства
- Различные опции по питанию:
  - AC: 100-240V, 50 – 60 Hz
  - DC: 12V-72V, -48V DC

IAS U1 Appliance

Check Point
SOFTWARE TECHNOLOGIES LTD.

Специализированное устройство Check Point для защиты критичных систем (Smart Grid)

IAS U1

IEC 61850-3 and IEEE 1613 compliant Designed for critical network security

IAS U1 - Описание

- Богатый функционал Software Blades – R7X/R77
- Централизованное управление Smart Center/Multi Domain
- Удовлетворяет требованиям Smart Grid
  - IEC-61850-3 И IEEE 1613
- Работает в экстремальных условиях
- Нет движущихся компонентов
- Возможны 48v DC блоки питания
- Высокая плотность портов – поддержка Fiber

IAS U1 - Спецификация

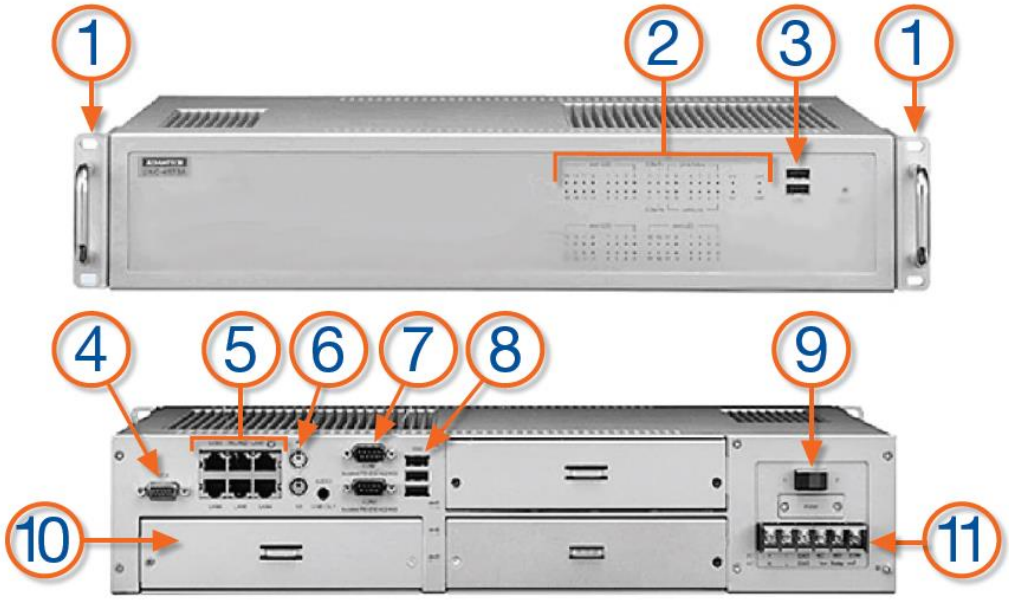
- Software Blades – R7X/R75
- Based on Secure Platform
  - SSD/HDD
  - 2 G ram
  - Rear wiring & I/O LED status indicators
  - 2 - USB 2.0
- IEC-61850-3 and IEEE 1613
- System Design: Fan less
- Power – 48v DC
- Interfaces – 3 x expansion slots
  - 2 x 1000 Base T, 4 x 1/100 Base T
  - Optional - 4 Fiber – mm 100 base FX
    - Serial 2x DB6 RS232, 8 screw terminal RS232/422/485

- **Environmental**
  - Power Consumption 5V ±5% @
  - Operating Temperature -20° ~ 70° C)
  - Operating humidity 20 ~ 95% RH non-condensing (refer to IEC 68-2-3)
  - Shock and vibration protection

IAS U1 - Спецификация

IAS U1

1. Rack mount
2. Network interface LEDs
3. Two USB ports
4. DB-15 VGA monitor connector
5. 2 x 10/100/1000 Base-T and 4 x 10/100 Base-T
6. PS-2 keyboard connector
7. DB-9 serial console connectors
8. Three USB ports
9. Power switch
10. Three I/O expansion slots
11. DC/AC power supply



- Производительность до 3 Гб/с в режиме межсетевого экрана
- Производительность до 2 Гб/с в режиме IPS (Default IPS profile)
- Соответствие требованиям IEC 61850-3 и IEEE 1613

- Температура и влажность: от -20 до 70° C, 20%-95%
- Отсутствие движущихся частей— безвентиляторный дизайн с использованием SSD накопителей и отсутствием внутренних кабельных соединений
- Различные опции по питанию

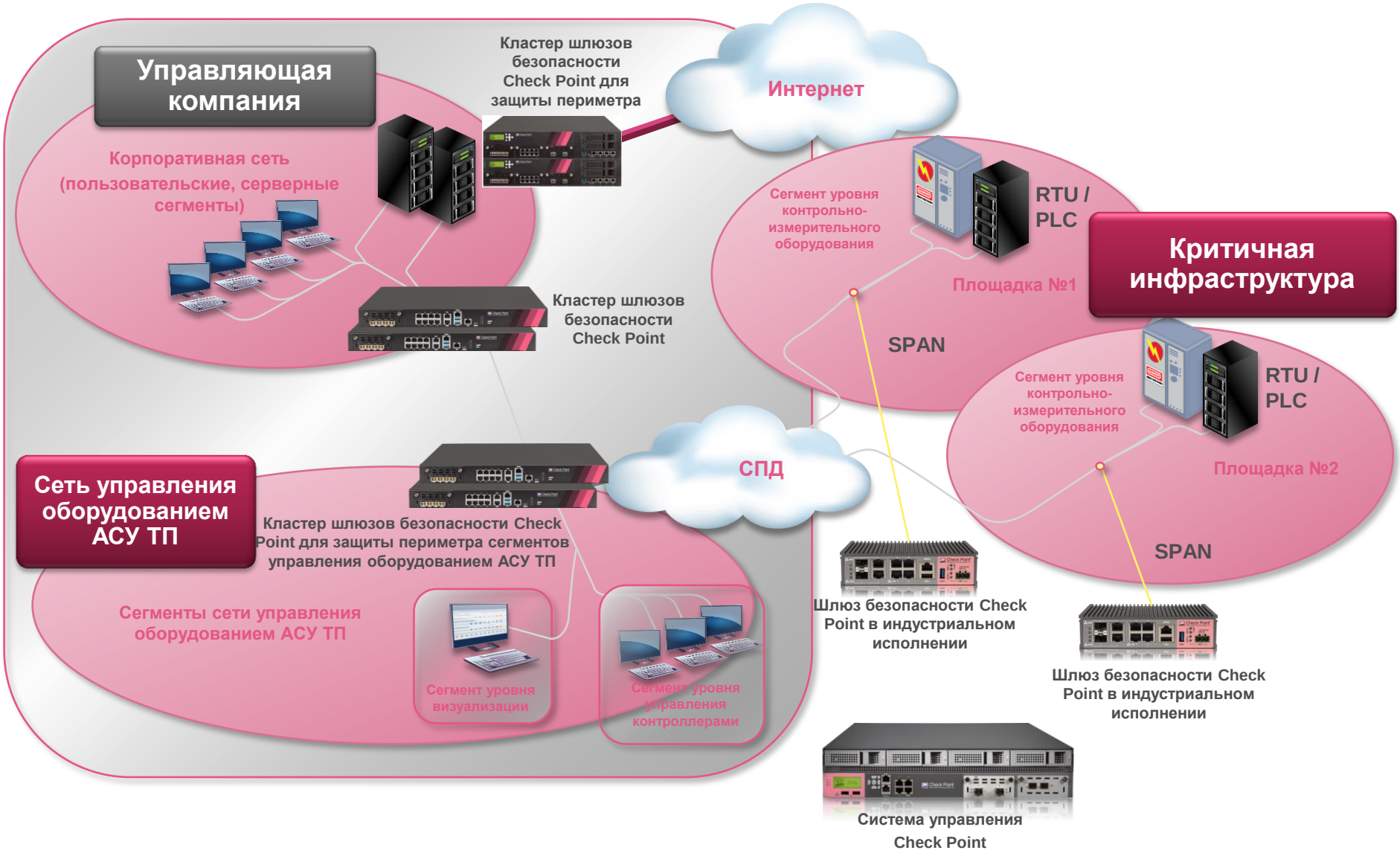
Integrated Security Module for Siemens / RuggedCom 1500 Switch

- ПО Check Point R77.10 интегрировано в модуль RuggedApe
- Прямой доступ к внутренней шине (не нужны лишние кабели)
- Соответствует требованиям IEC 61800-3 и IEC 61000-6-2

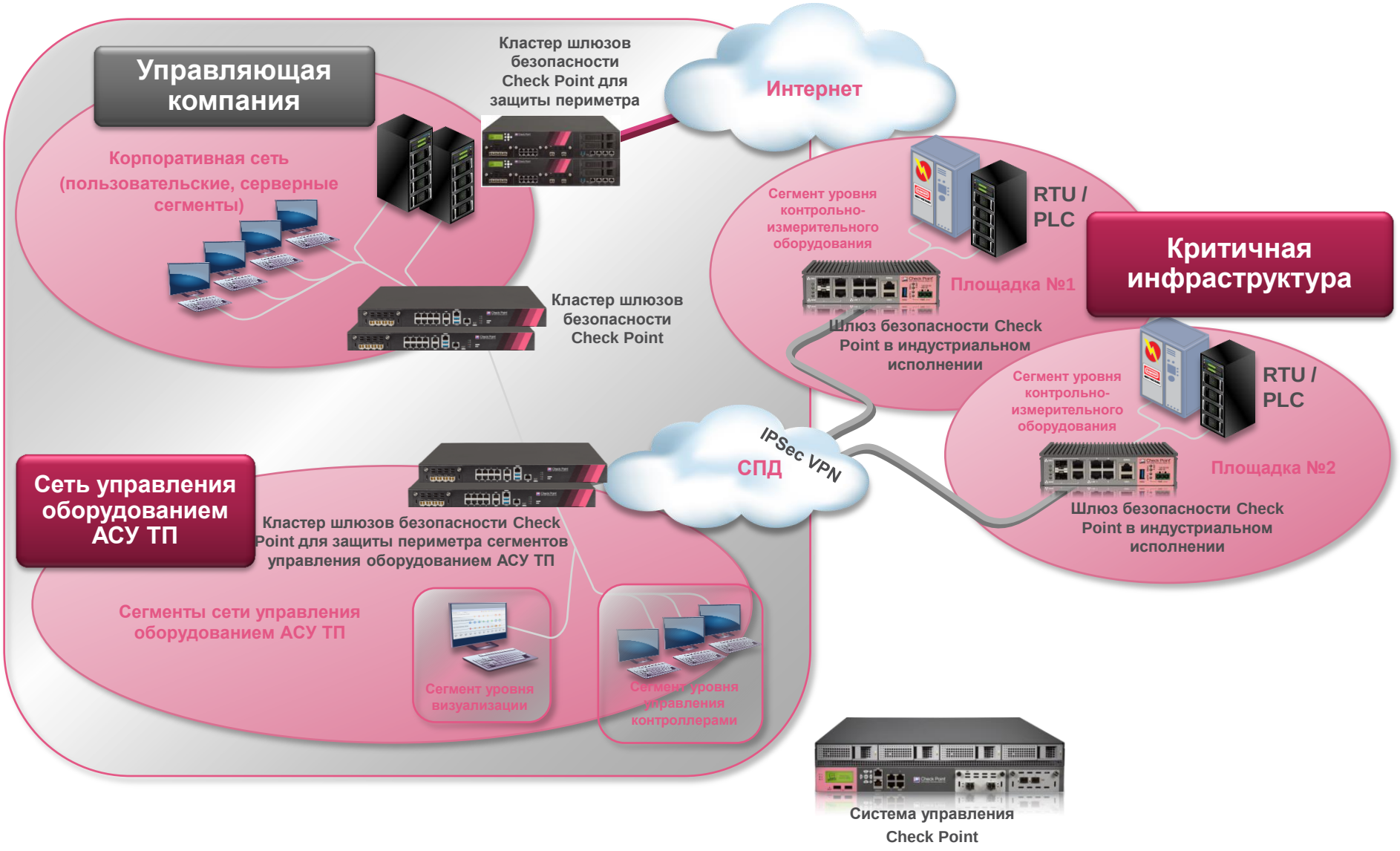
- Температура и влажность: от -40 до 70°C, 50%-95%
- Rack mount and DIN rail form factors
- 1x GigE и 2 x USB интерфейса на лицевой панели
- 1x GigE on backplane

Варианты развертывания

Индустриальные сети



Индустриальные сети



Требования к сетевой безопасности

Check Point
SOFTWARE TECHNOLOGIES LTD.

Корпоративный периметр

- Application Control
- Firewall – Сегментация сети
  - в Internet
  - к индустриальной сети
- IPS
- Защищенный удаленный доступ
- Anti-Malware и Anti-Bot

Индустриальная сеть

- Firewall – контроль доступа
- IPS
- Защищенный удаленный доступ
- Неблагоприятное окружение
- Анализ протоколов SCADA
- Anti-Bot
- Управление
- Аудит

Консолидация и централизованное управление

Требования защиты информации в РФ

Защита информации при межсетевом взаимодействии

ФСТЭК России. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».

МЭ не ниже 4 класса

5.7.4. Подключение ЛВС и автоматизированной системы (локальной или вычислительной сети) должно осуществляться с использованием МЭ, требования к которым определяются РД Гостехкомиссии России. Например, для защиты АС при ее взаимодействии с другой АС по каналам связи необходимо использовать: **в АС класса 1Г – МЭ не ниже класса 4**

МЭ Check Point R65, R71, R75, R77 сертифицированы как МЭ**3**

Сертифицированное СКЗИ

5.7.5. Для защиты конфиденциальной информации, передаваемой по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи, а **при использовании открытых каналов связи - сертифицированные ФАПСИ криптографические средства защиты информации**

Используются сертифицированные ФСБ КриптоПроCSP 3.6, 3.9

Сертификация Check Point во ФСТЭК

Сертификация Check Point Security Gateway R75.30 на соответствие МЭ3

СИС СЕРТИФИЦИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3018

Выдан 19 ноября 2013 г.
Действителен до 19 ноября 2016 г.

Настоящий сертификат удостоверяет, что **шлюз безопасности «Check Point Security Gateway версии R75»**, разработанный компанией Check Point Software Technologies Ltd. и производимый ООО «Сертифицированные информационные системы» в соответствии с техническими условиями ТУ 5015-008-82487552-2012, функционирующий на аппаратных платформах с версиями программного обеспечения, указанными в формуляре 5015-008-82487552-2012 ФО, является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, обрабатываемой в локальных вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей и соответствует требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по **3** классу защищённости при выполнении ограничений по эксплуатации, приведённых в формуляре.

Сертификат ФСТЭК России на шлюз безопасности «Check Point Security Gateway версии R75» на соответствие требованиям РД Средства вычислительной техники. Межсетевые экраны. 3 класс защищенности.

Сертификация производства
Power-1,
UTM-1,
2012 series,
SG на универсальных платформах
Для АС до 1Г и ИСПДн до К2 включительно

Сертификация Check Point во ФСТЭК

Сертификация Check Point Security Gateway R75.40VS на соответствие МЭ3

СИС СЕРТИФИЦИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3297

Выдан 12 декабря 2014 г.
Действителен до 12 декабря 2017 г.

Настоящий сертификат удостоверяет, что **шлюз безопасности «Check Point Security Gateway версии R75.40VS»**, разработанный компанией Check Point Software Technologies Ltd. и производимый ООО «Сертифицированные информационные системы» в соответствии с техническими условиями ТУ 5015-009-82487552-2013, функционирующий на аппаратных и программных платформах, указанных в формуляре 501540-009-82487552-2013 01 30, является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, обрабатываемой в локальных вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей и соответствует требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 3 классу защищённости при выполнении ограничений по эксплуатации, указанных в

Сертификат ФСТЭК России на шлюз безопасности «Check Point Security Gateway версии R75.40VS» на соответствие требованиям РД Средства вычислительной техники. Межсетевые экраны. 3 класс защищенности.

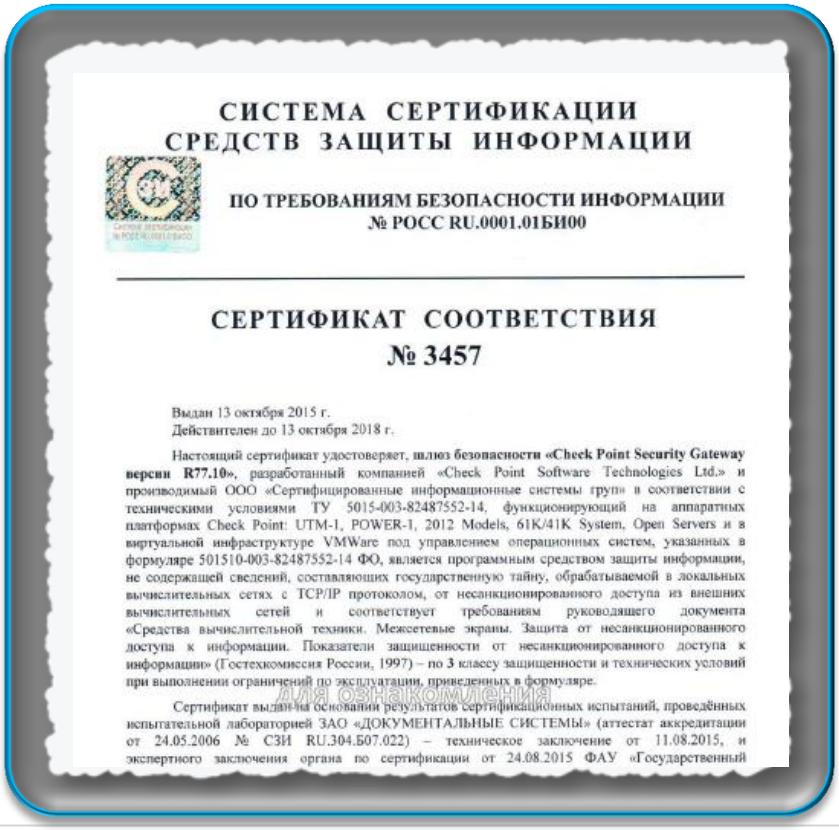
Сертификация производства
Power-1, UTM-1,
2012 series,
61000,
SG на универсальных платформах

Для АС до 1Г и ИСПДн до К2 включительно

Сертификация Check Point во ФСТЭК

Сертификация Check Point Security Gateway R77.10 на соответствие МЭ3+СОВ4+НДВ4

СИС СЕРТИФИЦИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3457

Выдан 13 октября 2015 г.
Действителен до 13 октября 2018 г.

Настоящий сертификат удостоверяет, **шлюз безопасности «Check Point Security Gateway версии R77.10»**, разработанный компанией «Check Point Software Technologies Ltd.» и производимый ООО «Сертифицированные информационные системы груп» в соответствии с техническими условиями ТУ 5015-003-82487552-14, функционирующий на аппаратных платформах Check Point: UTM-1, POWER-1, 2012 Models, 61K/41K System, Open Servers и в виртуальной инфраструктуре VMWare под управлением операционных систем, указанных в формуляре 501510-003-82487552-14 ФО, является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, обрабатываемой в локальных вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей и соответствует требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 3 классу защищенности и технических условий при выполнении ограничений по эксплуатации, приведенных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведённых испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 24.05.2006 № СЗИ RU.304.507.022) – техническое заключение от 11.08.2015, и экспертного заключения органа по сертификации от 24.08.2015 ФАУ «Государственный

Сертификат ФСТЭК России на шлюз безопасности «Check Point Security Gateway версии R77.10» на соответствие требованиям РД Средства вычислительной техники. Межсетевые экраны. 3 класс защищенности.

Сертификация производства Power-1, UTM-1, 2012 series, 41000, 61000, SG на универсальных платформах, и в виртуальной инфраструктуре VMWare

Для АС до 1Г и ИСПДн до К2 включительно

Защита АСУ ТП с помощью Check Point

Check Point
SOFTWARE TECHNOLOGIES LTD.

Анализ протоколов АСУ ТП
с точностью до команды

Предотвращение атак на АСУ ТП

Логирование всех команд АСУ ТП

Оповещение администраторов в
реальном времени

Итоги:

Решения Check Point для обеспечения безопасности АСУ ТП

Специализированные аппаратные платформы	Защита от специфичных угроз, за счет анализа SCADA протоколов	Централизованный менеджмент

Check Point
SOFTWARE TECHNOLOGIES LTD.

СПАСИБО!