

The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing the continents. In the bottom-right corner, there are several overlapping, semi-transparent white geometric shapes, including a large circle and a smaller, more complex polygonal shape, creating a technical or digital aesthetic.

**Средства обнаружения  
атак компании  
*Internet Security Systems***

# RealSecure - система обнаружения атак в реальном времени

- ✓ *Устанавливается в сетевом сегменте или на отдельном узле*
- ✓ *Просматривает весь трафик сегмента или действия пользователя конкретного узла*
- ✓ *Анализирует трафик с целью обнаружения атак и других событий, связанных с безопасностью*
- ✓ *В случае обнаружения предпринимает ответные действия*



# Компоненты RealSecure

**Модуль слежения**

**Управляющая консоль**



**Сетевой модуль  
(Network Sensor)**



**Системный агент  
(OS Sensor)**

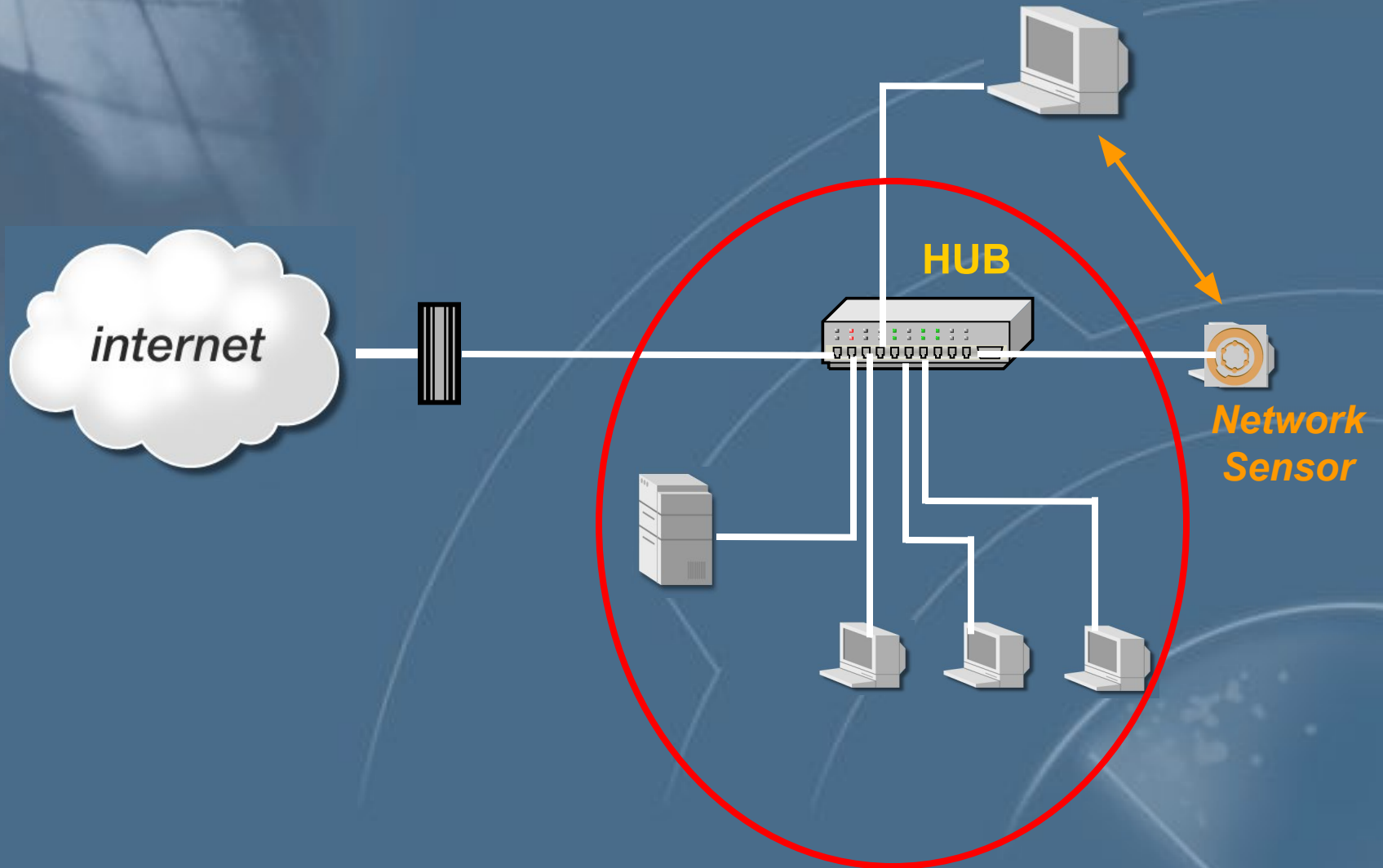


**Server Sensor**

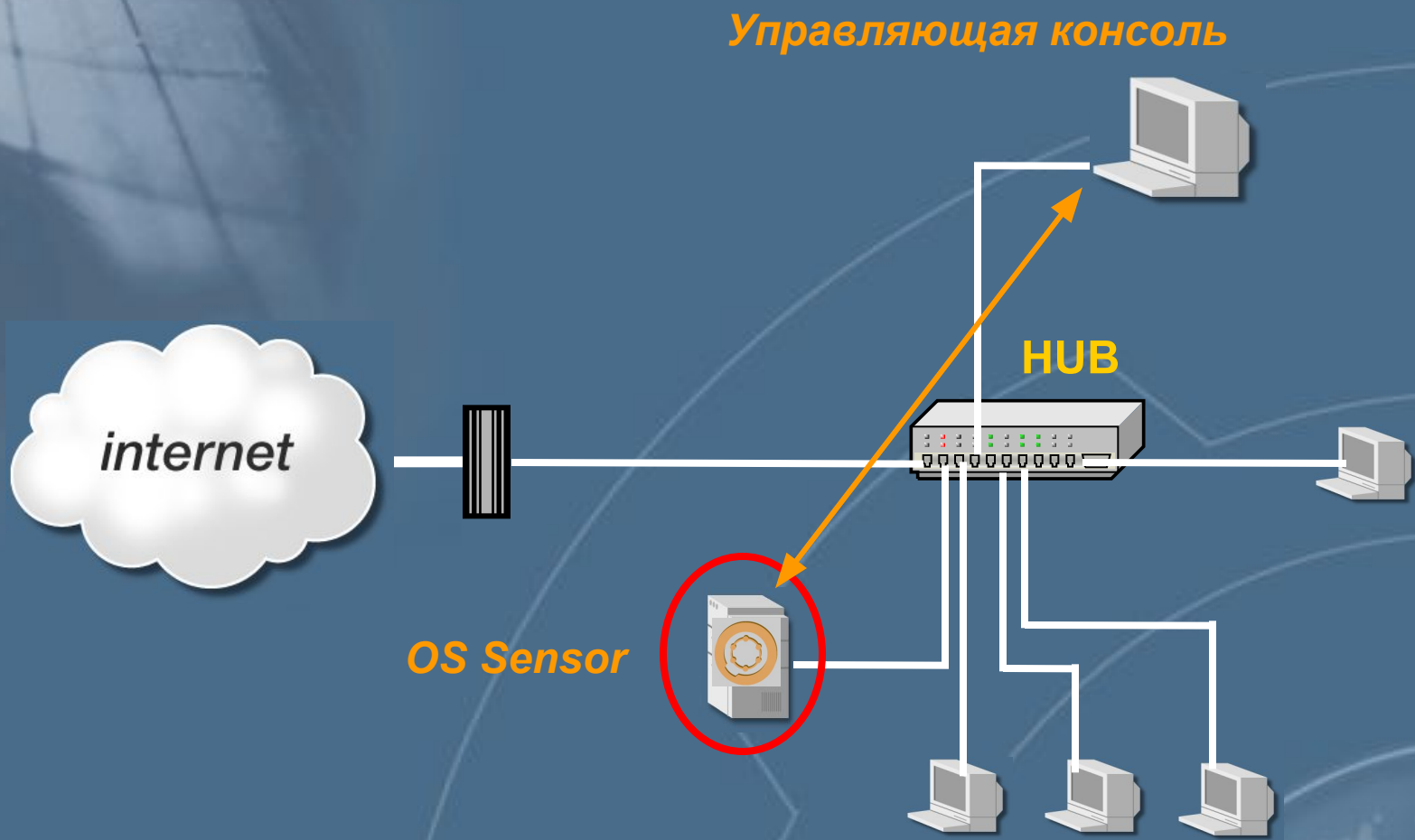


# Расположение сетевого модуля

*Управляющая консоль*

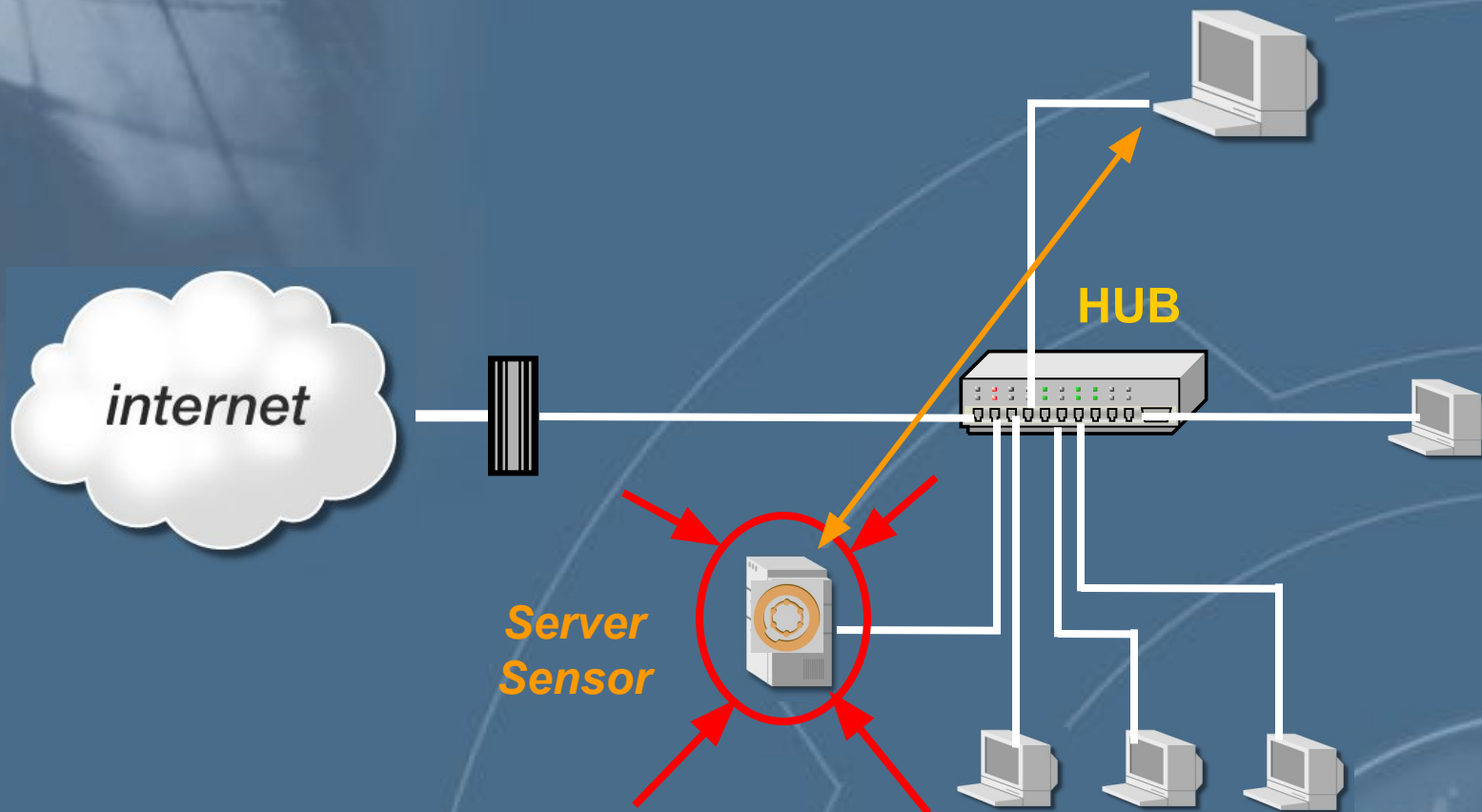


# Расположение системного агента

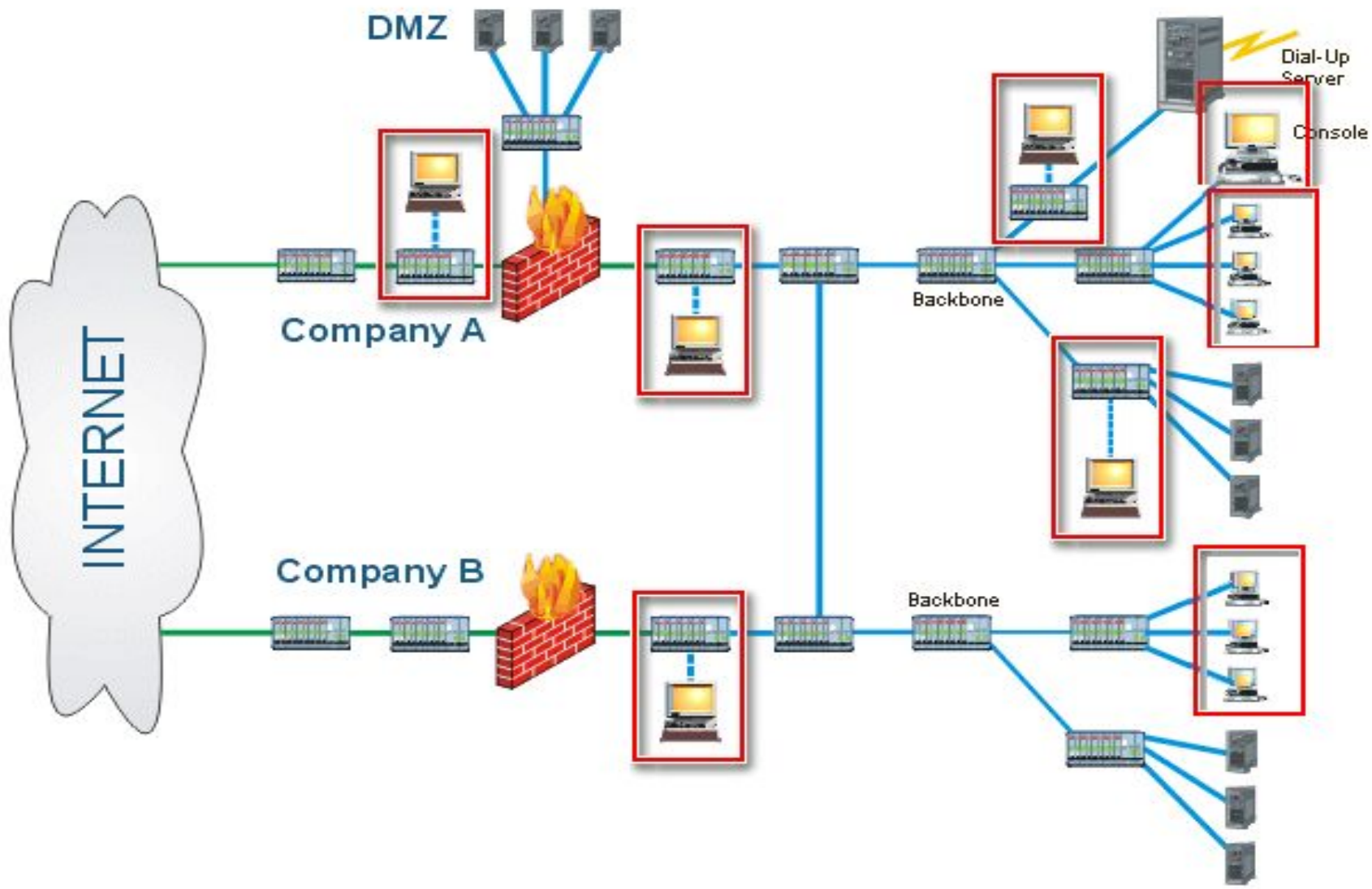


# Расположение микроагента (Server Sensor)

*Управляющая консоль*



# Примеры размещения RealSecure





# Категории обнаруживаемых атак

- *предварительные действия перед атакой*
  - Сканирование портов, SATAN
- *подозрительная активность*
  - Неизвестный протокол
- *«отказ в обслуживании»*
  - SYN Flood, Ping of Death, Teardrop, WinNuke
- *попытки неавторизованного доступа*
  - Back Orifice, Netbus, LOpht Crack for Windows
- *системные атаки*
  - Атаки на MS IIS, MS Exchange, MS SQL Server



# Механизмы реагирования RealSecure

*Разрыв соединения*

*Реконфигурация межсетевого экрана*

*Выполнение программы, определённой пользователем*

*Отправка сообщения*

*На консоль*

*По протоколу SNMP*

*По E-mail*

*Регистрация события в БД*

*Расширенная регистрация с возможностью последующего воспроизведения*

# Network Sensor

Проверка каждого пакета на:

- подозрительную активность
- враждебное содержание
- сетевые злоупотребления

Пользователь может:

- задавать свои контролируемые события
- задавать варианты реагирования на события
- настраивать сигнатуры атак
- игнорировать некоторые типы трафика

# Network Sensor

Поддержка Ethernet, Fast Ethernet, Token Ring и FDDI

Поддержка протоколов SMB/NetBIOS и стека протоколов TCP/IP (IP, TCP, UDP, ICMP и других на их основе)

Функционирование под управлением Windows NT и Solaris

**ИНФОРМЗАЩИТА**

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# Network Sensor

Достоинства:

- *низкая стоимость эксплуатации*
- *обнаружение сетевых атак*
- *хакеру трудно «замести следы»*
- *обнаружение в реальном режиме времени*
- *независимость от операционной системы*
- *обнаружение атак до достижения ею цели*
- *невозможность обнаружения (Stealth-режим)*

# RealSecure и межсетевые экраны

- Модемы
- Атаки через «туннели»
- Атаки со стороны авторизованных пользователей
- Атаки на межсетевые экраны

# Производительность

- Чем больше ОЗУ, тем эффективнее работает сетевой модуль слежения
- Чем больше в компьютере процессоров, тем эффективнее происходит анализ трафика
- В высокозагруженных сетях требуется использовать высокопроизводительные компьютеры
- Желательно запускать на выделенном компьютере

# OS Sensor

Чтение записей журнала регистрации

- сравнение записей с политикой аудита
- реагирование в случае нарушений

Пользователь может:

- задавать варианты реагирования на события
- определять новые события
- контролировать неиспользуемые порты



# Системный агент

Системный агент под управлением Windows NT

- Windows NT Security Log
- Windows NT Event Log
- Windows NT Application Log
- Unix Syslog
- Cisco Syslog

*Системный агент под управлением Unix  
(Solaris, HP UX, AIX)*

- *локальный Syslog*
- *удаленный Syslog*
- *Cisco Syslog*
- *BSM log*

# OS Sensor

Достоинства:

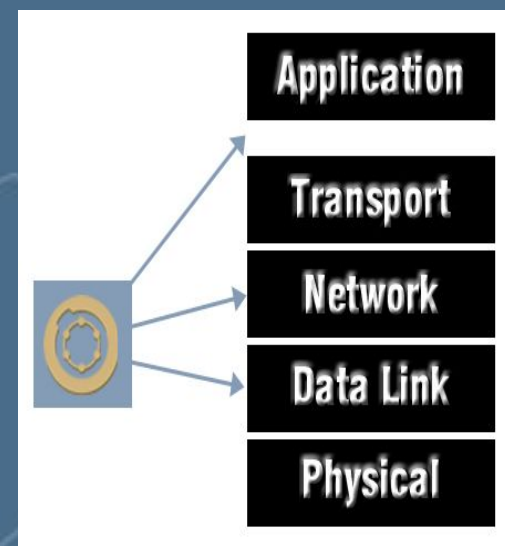
- *контроль конкретного компьютера*
- *обнаружение системных атак*
- *работают в коммутируемых сетях*
- *последующий анализ данных*

# Server Sensor

Обнаружение атак на всех уровнях на конкретный узел сети

Достоинства:

- *производительность*
- *обнаружение всех атак*
- *работа в коммутируемых сетях*
- *работают в сетях с шифрованием*



Функции персонального межсетевоего экрана

**ИНФОРМЗАЩИТА**

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# RealSecure Appliance

- *IPSO, защищенная ОС на базе BSD от NOKIA*
- *Несколько сетевых интерфейсов*
- *Высокая доступность и отказоустойчивость*
- *Повышение производительности*



**ИНФОРМЗАЩИТА**

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# Что делает управляющая консоль?



*Предоставляет интерфейс для конфигурирования модулей слежения*



*На консоль поступают сообщения от модулей слежения и данные, записанные модулями слежения*



*Позволяет формировать отчёты на основе собранных данных*

# RealSecure Manager

- Management Console
  - Windows NT
- RealSecure Manager for HP OpenView v1.3
  - Windows NT
  - Solaris SPARC
- RealSecure Manager for Tivoli v1.3
  - Windows NT
  - Solaris SPARC
- RealSecure Management SDK v1.1

# Концепция OPSec

- Использование OPSec SDK, предоставляющих необходимые API
- Применение открытых протоколов
  - CVP(Content Vectoring Protocol)
  - UFP (URL Filter Protocol)
  - SAMP (Suspicious Activity Monitoring Protocol)
  - LEA (Log Export API )
  - OMI (Object Management Interface)
- Использование языка INSPECT