



Угрозы в Интернете

Филипп Роггебанд, менеджер по развитию бизнеса

группа «Сети без границ», страны с развивающейся экономикой

Вопросы к обсуждению

- Отчет по безопасности Cisco за 2009 г.
- Угрозы в Интернете
- Защищенные сети без границ
- Вопросы и ответы

Насущные задачи

Противоборствующие силы



Глобализация



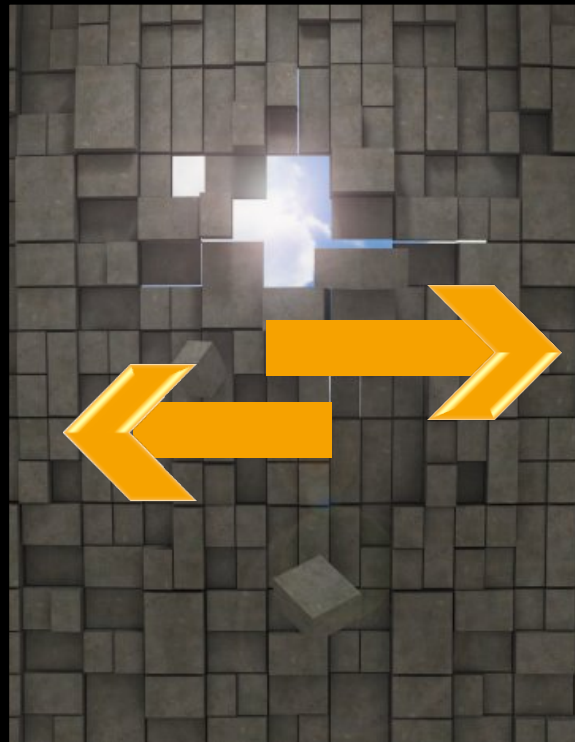
Мобильность



Совместная работа



Корпоративное
ПО как сервис



facebook



Допустимое
использование



Угрозы



Утрата
данных

Эволюция угроз безопасности

Специализация преступников как фактор усложнения атак

Веб-экосистемы как главное направление развития угроз

Преступники злоупотребляют доверием пользователей, что ставит под сомнение традиционные средства защиты

Творческий подход к привлечению жертв (бизнес-модели)



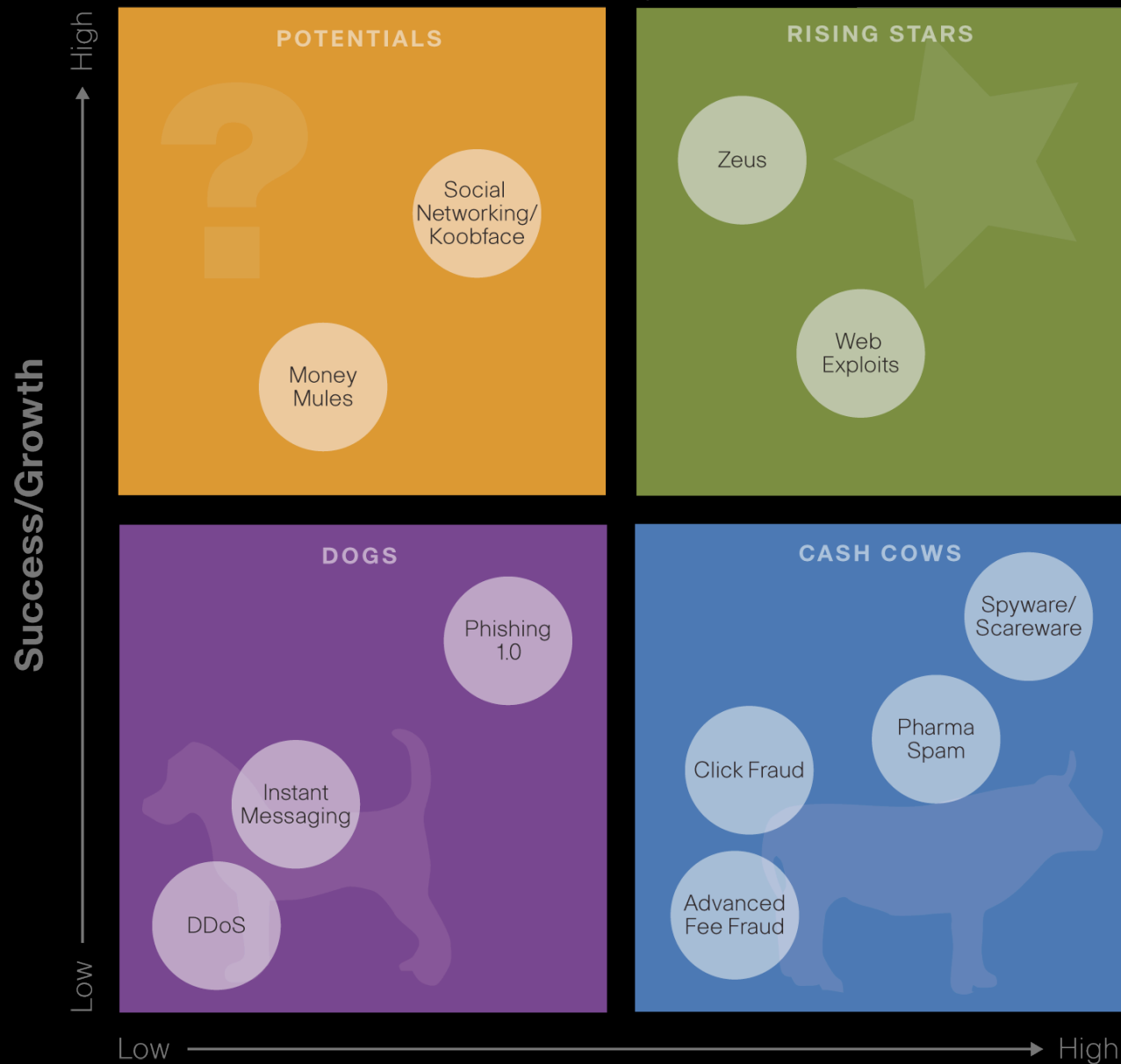
Отчет по безопасности Cisco за 2009 г.

Содержание

- Социальные сети
- Риски при работе в Интернете
- Монетизация киберпреступлений
- Указатель ресурсов киберпреступности
- Номинации "образцово-показательные киберпреступления"



Матрица : доход на капитал, вложенный в киберпреступление



"Изделие года" в области киберпреступности

The screenshot displays the Security Task Manager interface in the background, listing various Windows processes. In the foreground, the Antivirus XP 2008 application window is open, showing a scan result. A yellow callout box contains the text: "Антивирус XP нашел 2794 угрозы. Рекомендуется их устранить. Продолжить?". Below this, a dialog box titled "Antivirus XP 2008" asks for confirmation to proceed with removal of 2794 threats. A table of detected threats is visible, including items like Win32/IRCbot.AAH and Virus Win.CIH.

Severity	Status
High	Infected!
Medium	Infected!
High	Infected!
High	Infected!
High	Infected!
High	Infected!
High	Infected!
High	Infected!
Low	Infected!
Critical	Infected!

После сканирования – переход на узел, определяющий местонахождение и IP-адрес, удаление кнопки "Закреть" с экрана

Address <http://www.antivirusxp-08.net/buy/d6cd94f14c6a1b24ba0d27fb705a59a0>

Antivirus XP 2008

Buy

AUD 59.95 [Pay by credit card](#)

Antivirus XP 2008 Standard edition + 1 year free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE: AUD 59.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

AUD 126.95 [Pay by credit card](#)

Antivirus XP 2008 Standard edition + 3 years free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE: AUD 126.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

Instant Access, Discreet Billing, Secure Procedure by conveniently using our

Vakasoftware управляет криминальной сетью

- Партнеры Vakasoftware по продаже "шпионского" ПО для "устрашения"
- Партнеры загружают "ПО-устрашитель" в ботсети
- Партнеры выплачивают Vakasoftware комиссионные за покупки клиентов
- Доход партнера № 2 за 10 дней – 147 тыс. долларов, за год – 5 млн.

154 825 установок, 2772 покупки

	Loader	Сетапы	Покупки	Покупки
День 1	37943	19989	667	29853.86
День 2	39895	19722	74	5420.64
День 3	41687	18619	384	28148.96
День 4	38059	16038	249	13908.24
День 5	39160	15335	176	9726.17
День 6	29968	12076	207	11672.71
День 7	13293	6866	129	6920.81
День 8	18055	8915	157	7557.25
День 9	29642	14802	265	12852.29
День 10	50457	22463	464	21055.29
Итого	338159	154825	2772	147116.22
	Loads	Installs	Purchases	Total

Панель Vakasoftware с доходами за 10 дней ДФ № 2

Источник: <http://www.secureworks.com/research/threats/rogue-antivirus-part-2/?threat=rogue-antivirus-part-2>

Атака на Веб 2.0 – чат с "другом"

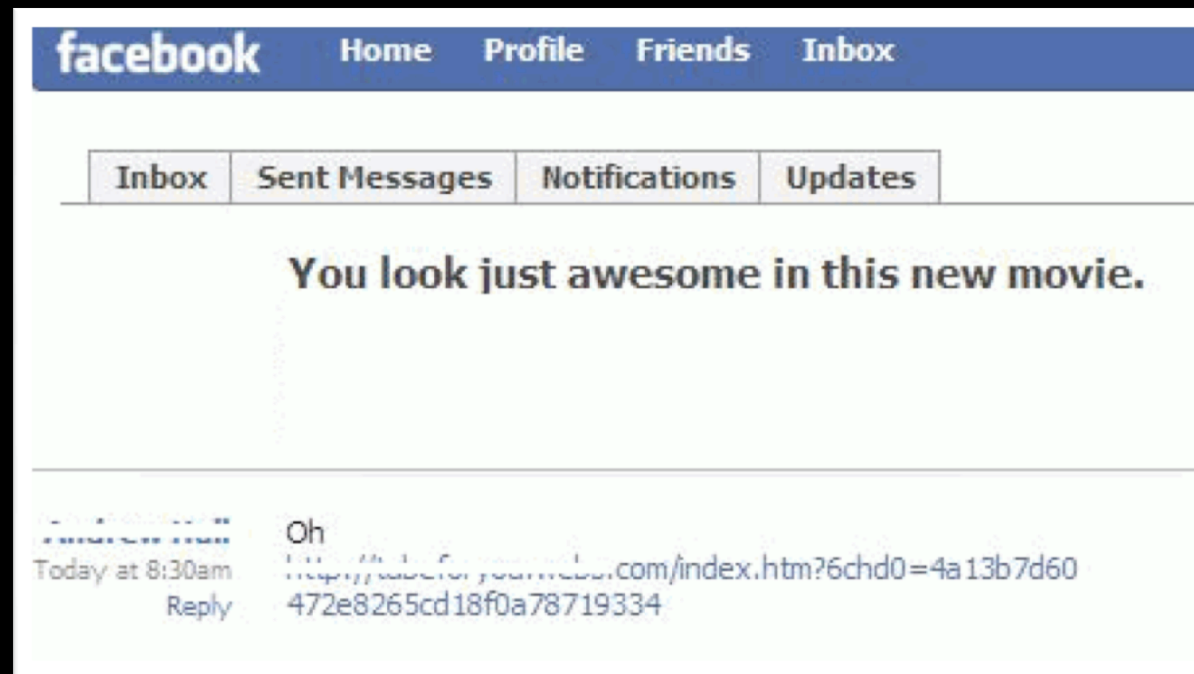
The screenshot shows a web chat interface with a navigation bar at the top containing 'Inbox', 'Sent Messages', 'Notifications', 'Updates', and '+ Compose Message'. The chat header indicates the conversation is 'Between Gilbert and You'. The chat history consists of the following messages:

- Gilbert:** Hey
- Tony:** hey gil what's up?
- Gilbert:** Not too good. I'm in some kind of deep mess right now
- Tony:** oh?
- Gilbert:** I'm stranded in London. I was mugged at gun point last night, all cash on me and my bank card was all stolen
- Tony:** dude that's horrible?
- Gilbert:** i have a plane back home in about 3 hours time but i need some money for the hotel bills
- Gilbert:** Can you please loan me some \$\$ for now i will def have the money refund when i get back home..?????????
- Tony:** uh... i'm not to sure how to do that. what's the easiest method?
- Gilbert:** You can have the money sent to me via westernunion money transfer

At the bottom of the chat window, there is a 'Reply:' label and a large empty text input box. The interface also features a status bar at the very bottom with icons for 'Applications', 'Online Friends (4)', and other system functions.

Всё вместе: червь Koobface

- Ссылки передаются на взломанные учетные записи социальных сетей (или приходят с них)



- Ссылка ведет к подложному узлу видео, где пользователю предлагают для просмотра установить новый проигрыватель Flash или кодек


Почему веб-эксплойт трудно обнаружить: BoingBoing.net: популярный блог



- URL в обозревателе: 1
- Запросов HTTP Get: 162
- Изображений: 66 из 18 доменов, в т.ч. 5 отдельных невидимых отслеживающих изображений 1x1 пиксель
- Скриптов: 87 из 7 доменов
- Куки-файлов: 118 из 15 доменов
- 8 Flash-объектов из 4 доменов

ПО как служба: все больше предложений от злоумышленников

Служба проверки вредоносного ПО на обнаружение с помощью антивирусов



Home Scan Exploit pack check Prices FAQ AV Versions Send money to account Регистрация

Account manager

Login

Password

Войти

Prices:

- **1 scan 1-26 AV engines (up to 5 files in archive file for one check) = 1\$**
- **1 scan exploit pack dumps 1-26 AV engines = 1\$**
- We introduce a policy of discounts, proportional to the number of performed scans:
For every 10 single scans you get 5 scans for free (10\$ -> 15 scans)
For every 15 single scans you get 10 scans for free (\$15 -> 25 scans)
For every 25 single scans you get 15 scans for free (\$25 -> 40 scans)

Почему Zeus?



Основа конфигурационного файла Zeus

- По умолчанию Zeus ворует все поля формы в обозревателе
- Каждый контроллер ботсети может адаптировать хищение персональных данных

Steal from these brands

```
banesnet.banesto  
*patagoniaebank.com  
*inetnkp.adelaidebank  
*login.commbank  
*sydneycu.com
```

- Может указать, что не похищать

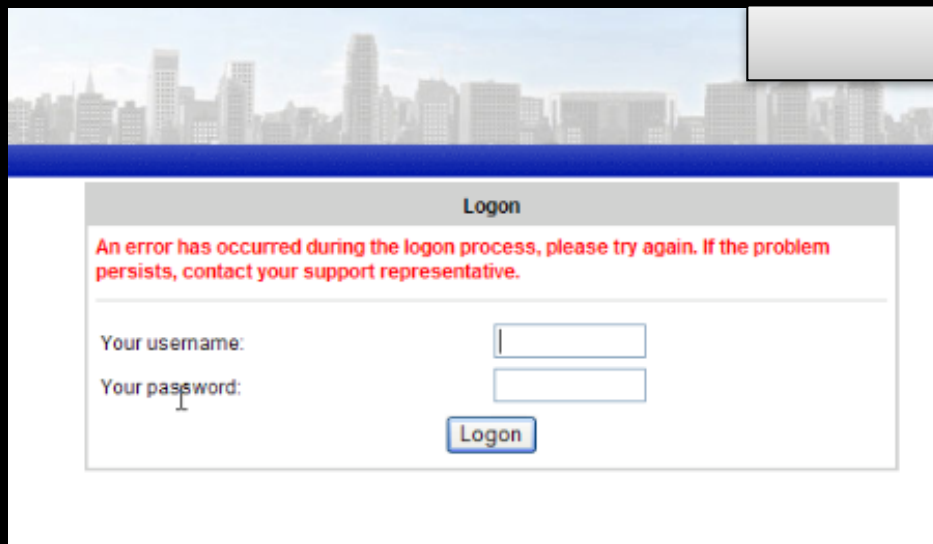
Don't steal from these brands

```
entry "WebFilters"  
!http://*.webkinz.com/*  
!http://*.myspace.com/*  
!http://*.microsoft.com/*  
!http://*.skyblueads.com/*
```

Материал предоставлен фирмой Silver Tail Systems

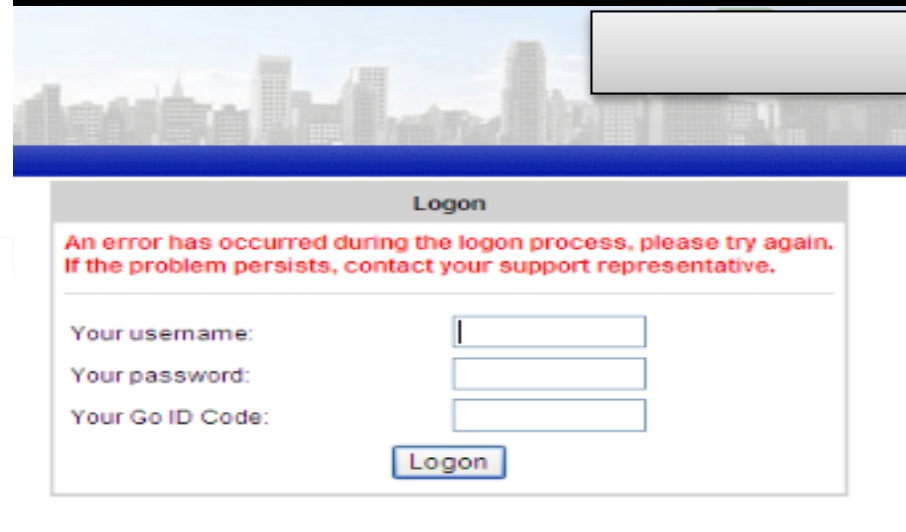
Внедрение элемента экрана

Обозреватель HE на узле Zeus:



The screenshot shows a web browser window with a city skyline background. The page title is "Logon". A red error message reads: "An error has occurred during the logon process, please try again. If the problem persists, contact your support representative." Below the message are two input fields: "Your username:" and "Your password:". A blue "Logon" button is positioned below the password field.

Обозреватель на узле Zeus:



The screenshot shows a web browser window with a city skyline background. The page title is "Logon". A red error message reads: "An error has occurred during the logon process, please try again. If the problem persists, contact your support representative." Below the message are three input fields: "Your username:", "Your password:", and "Your Go ID Code:". A blue "Logon" button is positioned below the "Your Go ID Code" field.

Материал предоставлен фирмой Silver Tail Systems

Статистика

- Трекер Zeus отслеживает 784 ботсети Zeus
- В ботсетях Zeus около 1,6 млн. ботов
- Атаки на 1130 брендов
- Около 960 – в финансовой сфере (85 %)
- **КАЖДЫЙ** из 5 крупнейших банков США атакуют свыше 500 ботсетей Zeus

Аналитический центр безопасности Cisco

Мощная поддержка средств безопасности Cisco

SensorBase

- В мире действует свыше 700 000 датчиков по четырем группам угроз
- Историческая библиотека 40 000 угроз
- 500 потоков информации от сторонних организаций, 100 потоков новостей, партнерства с разработчиками ПО с открытым кодом и коммерческого ПО

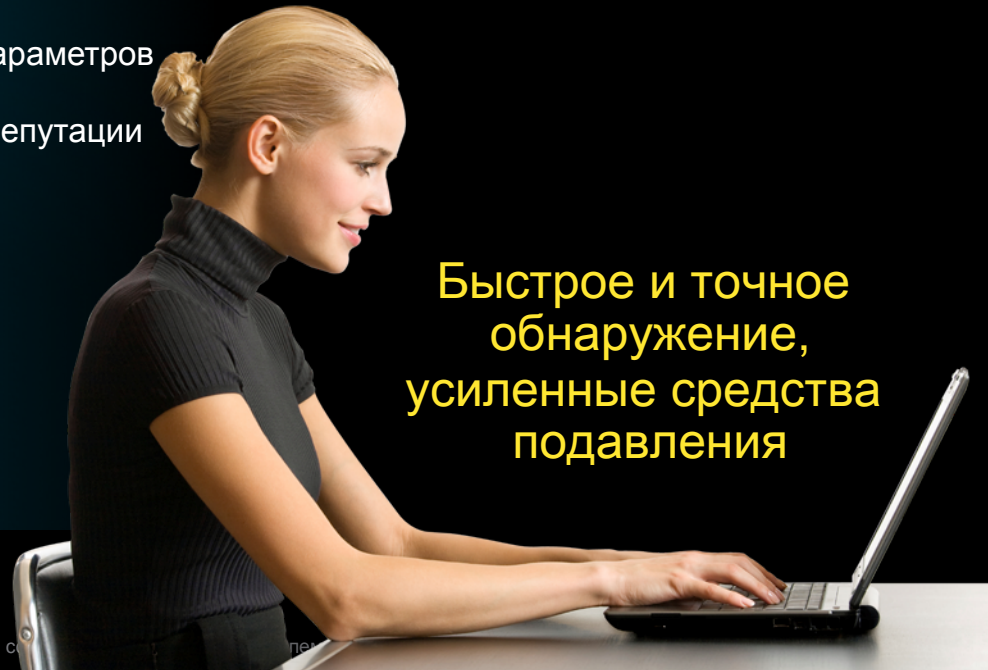
Центр оценки угроз

- Автоматическое отслеживание более чем 200 параметров
- SenderBase: классифицирует и строит рейтинг репутации
- Корреляция угроз в мировых масштабах

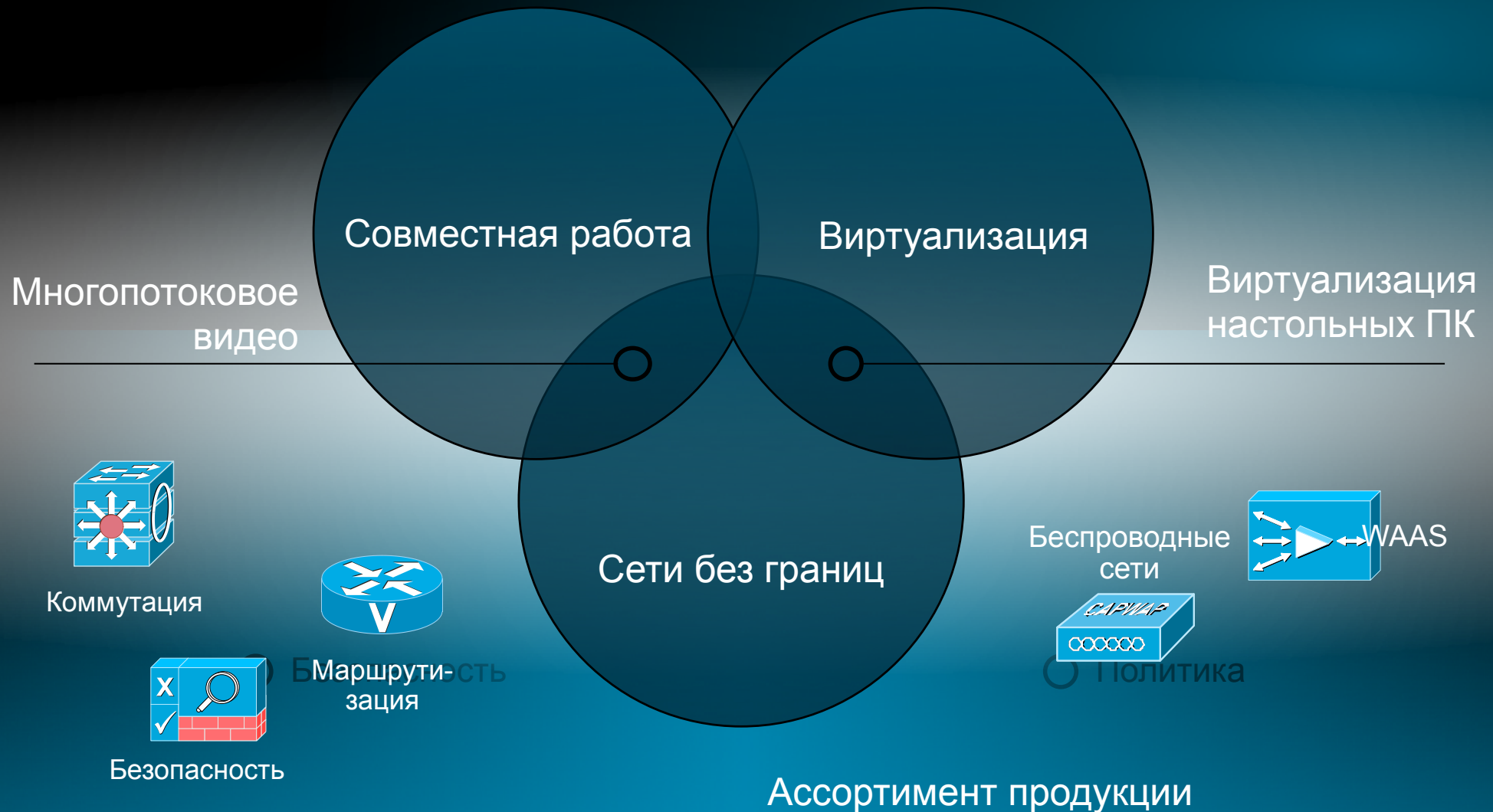
Усиленная защита

- Автоматическое создание правил и сигнатур
- Новейшие фильтры прорыва вируса

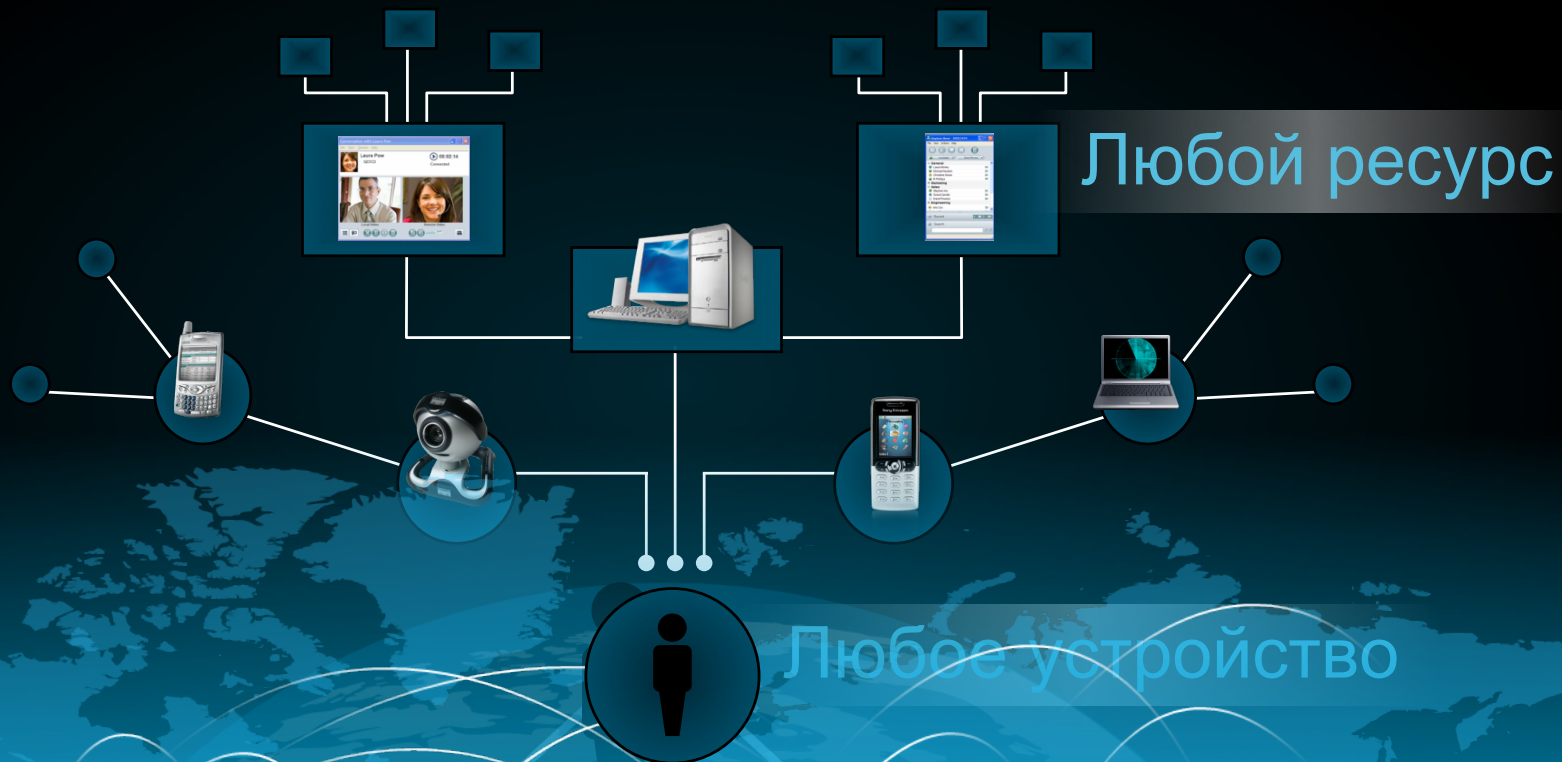
Быстрое и точное
обнаружение,
усиленные средства
подавления



Подход Cisco к архитектуре



Преобразование: Наше новое рабочее место – весь мир



СЕТИ БЕЗ ГРАНИЦ

Архитектура нового поколения как путь
реализации нового рабочего пространства



CISCO