

Обзор рынка решений для защиты сетей

Павел Иванов
Директор, шеф-редактор
Агентство корпоративных
коммуникаций OSP-Con
psi@osp.ru

Угрозы в области ИБ в 2009 г.: прогноз MessageLabs Intelligence

- ◆ Web 2.0 – среда для контекстного вредоносного ПО
 - консолидация нескольких динамических потоков данных из несвязанных источников
 - появление MaaS (Malware As A Service)
 - большая гибкость и скорость модификации вредоносного кода
- ◆ Социальные сети
 - более профессиональный phishing → более адресный и персонализированный спам
- ◆ Особенности спама
 - персональное обращение
 - сегментация по рынкам и демографии
 - лаконичность (меньше контента для фильтрации)
 - большее сходство с запрошенными рассылками и спецпредложениями
- ◆ Фундаментальные недостатки протокола DNS (середина 2008)
 - phishing-атаки на базе уязвимостей DNS-доменов и Web-сайтов вместо традиционных «подделок»
 - Выход: более широкое применение DNS Security Extensions (DNSSEC)

Защита корпоративных сетей:

10 ноября
2009 г.

минимизация рисков и повышение гибкости
бизнеса

Угрозы в области ИБ в 2009 г.: прогноз MessageLabs Intelligence

- ◆ Scam в стиле Nigerian 419
 - подобные виды мошенничества станет труднее распознать (сообщения из 1-2 предложений, «новые возможности для бизнеса», использование присоединенных файлов)
 - ◆ Глобализация спама
 - развитие ШПД в странах BRIC
 - спам на локальных языках на развивающихся рынках
 - ◆ Атаки на смартфоны и другие мобильные устройства
 - 2008: любительские атаки через бесплатную загрузку игр и приложений
 - 2009: криминальные атаки с явной финансовой составляющей
 - 300 вирусов для мобильных терминалов, 400К – для ПК
 - SMS на номера «premium»
 - ◆ Воскрешение botnet
 - подавление крупных сетей в конце 2008 (Intercage, McColo)
 - возможное воскрешение с хостингом в странах BRIC
 - киберпреступники усовершенствуют технологии botnet
 - технологии супервизора (использование слоя виртуализации поверх HW)
 - прямой перехват важных вызовов ОС
 - ОС не будет догадываться о существовании вредоносного ПО
- 10 ноября 2009 г. Защита корпоративных сетей:
минимизация рисков и повышение гибкости
бизнеса

Угрозы в области ИБ в 2009 г.:

5 тенденций от WatchGuard

◆ Тенденция 5:

- усиление законодательства в области защиты данных, в том числе персональных
- новые уголовные дела и прецедентное право

◆ Тенденция 4:

- botnets станут более качественными и ... прибыльными

◆ Тенденция 3:

- наиболее популярные социальные сети – платформа для сетевых атак, инициации несанкционированных scam-рассылок, phishing'a и т.п.

◆ Тенденция 2:

- рост числа атак через SSL и HTTPS

◆ Тенденция 1:

- угрозы из доверенных сайтов и доменов
- автоматические атаки, распространяющиеся через Web

Защита корпоративных сетей:

минимизация рисков и повышение гибкости

бизнеса

10 ноября
2009 г.

Тенденции в области ИБ в 2009-?? годах

- ◆ Тот же уровень защиты при меньших бюджетах
- ◆ Исчезновение поставщиков и слияния/поглощения
- ◆ Модель SaaS в области ИБ (Qualys, WhiteHat Security)
- ◆ Дистанционный сетевой мониторинг поставщиками устройств защиты
- ◆ От соответствия регулирующим актам – обратно к операциям

Защита корпоративных сетей:

минимизация рисков и повышение гибкости
бизнеса

10 ноября
2009 г.

MQ: брандмауэры для предприятий



As of November 2008

10 ноября 2008
2009 г.

минимизация рисков и повышение эффективности
бизнеса

MQ: средства контроля доступа



As of March 2009

10 March 2009
2009 г.

минимизация рисков и повышение эффективности
бизнеса

Средства сетевого доступа: ForresterWave

◆ Лидеры

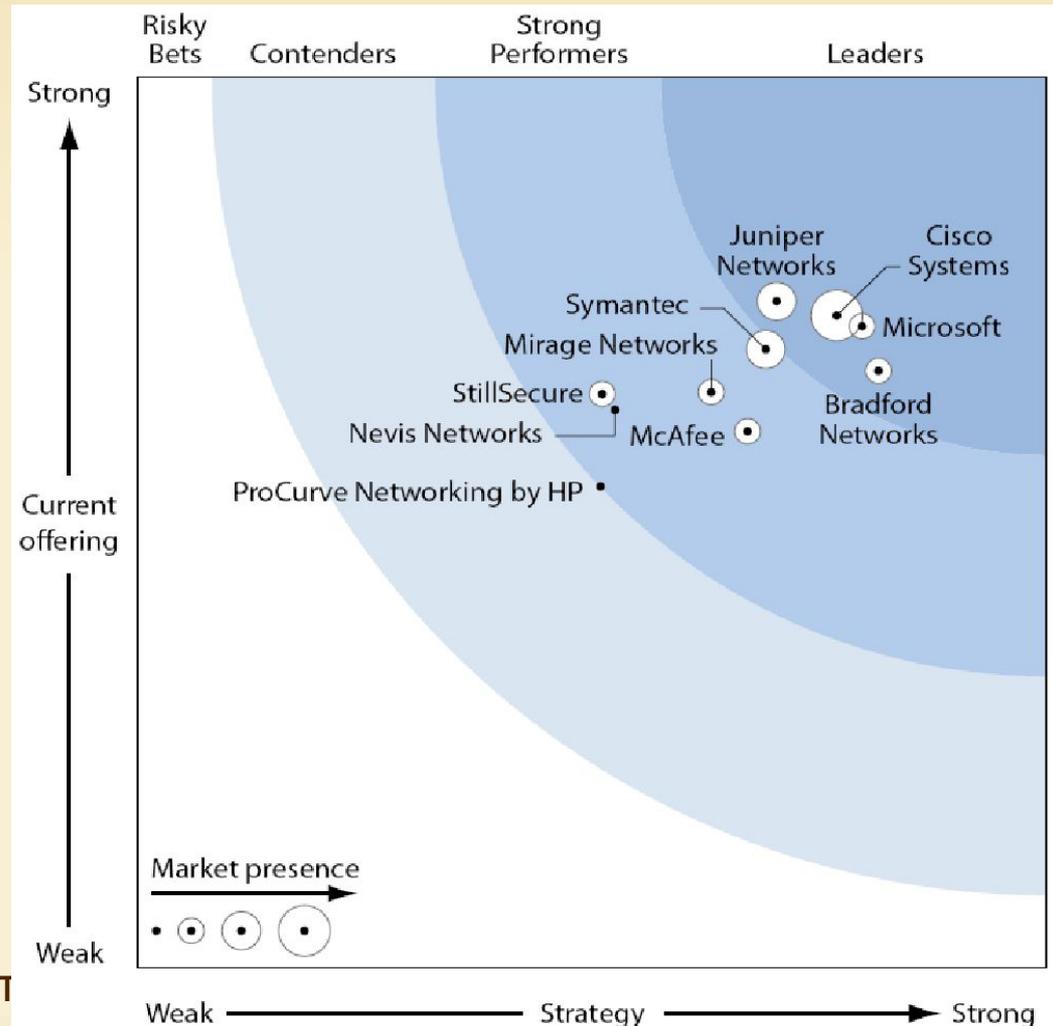
- Microsoft
- Cisco Systems
- Bradford Networks
- Juniper Networks

◆ Поставщики конкурентных, простых в развертывании решений

- Symantec
- Mirage Networks
- McAfee

◆ «Замыкающие»

- StillSecure
- Nevis Networks
- HP ProCurve



Средства сетевого доступа: ForresterWave (прод.)

Vendors	Product evaluated	Software-based solution	Infrastructure-based solution	Appliance-based solution
Bradford Networks	NAC Director, Campus Manager, NAC Director GCS	◐	-	●
Cisco Systems	Cisco NAC appliance, NAC server, NAC Manager, NAC Profiler, Guest Server	◐	●	◐
Juniper Networks	UAC Infranet Controller 4000/4500, Infranet Controller 6000/6500, Odyssey Access Client, NAC Profiler	◐	●	◐
McAfee	MNAC 3.0 (ePolicy Orchestrator)	●	-	○
Microsoft	Microsoft NAP for Windows Vista, XP SP3, Server 2008	●	○	-
Mirage Networks	NAC Management Server, Advanced Compliance Server, Sensors	-	-	●
Nevis Networks	LANenforcer (Nevis LAN Switch, Nevis LAN Security Appliance)	○	◐	●
ProCurve Networking by HP	ProCurve Network Access Controller 800, ProCurve NAC 800 Endpoint Integrity Agent, ProCurve Identity Driven Manager	◐	●	○
StillSecure	Safe Access	●	-	●
Symantec	SNAC 11.0	●	○	○

10-11 ноября 2008
 2009 г. минимизация рисков и повышение гибкости
 бизнеса

Средства сетевого доступа: ForresterWave (прод.)

Vendor	Role- and identity-based access	Unmanaged access (contractors, remote, guests, etc.)	Wireless and non-traditional endpoint (printers, etc.)	Employee access	Virtual endpoint environment	Application level control	Supporting existing infrastructure (agents, AD/LDAP, etc.)	Overall performance across all scenarios
Bradford Networks	●	●	●	●	●	●	●	●
Cisco Systems	●	●	●	●	●	●	●	●
Juniper Networks	●	●	●	●	●	●	●	●
McAfee	●	●	●	●	●	-	●	●
Microsoft	●	●	●	●	●	●	●	●
Mirage Networks	●	●	●	●	●	●	●	●
Nevis Networks	●	●	●	●	●	●	●	●
ProCurve Networking by HP	●	●	●	●	●	-	●	●
StillSecure	●	●	●	●	●	●	●	●
Symantec	●	●	●	●	●	●	●	●

● Fully covers scenario

● Covers this scenario better than most of the vendors

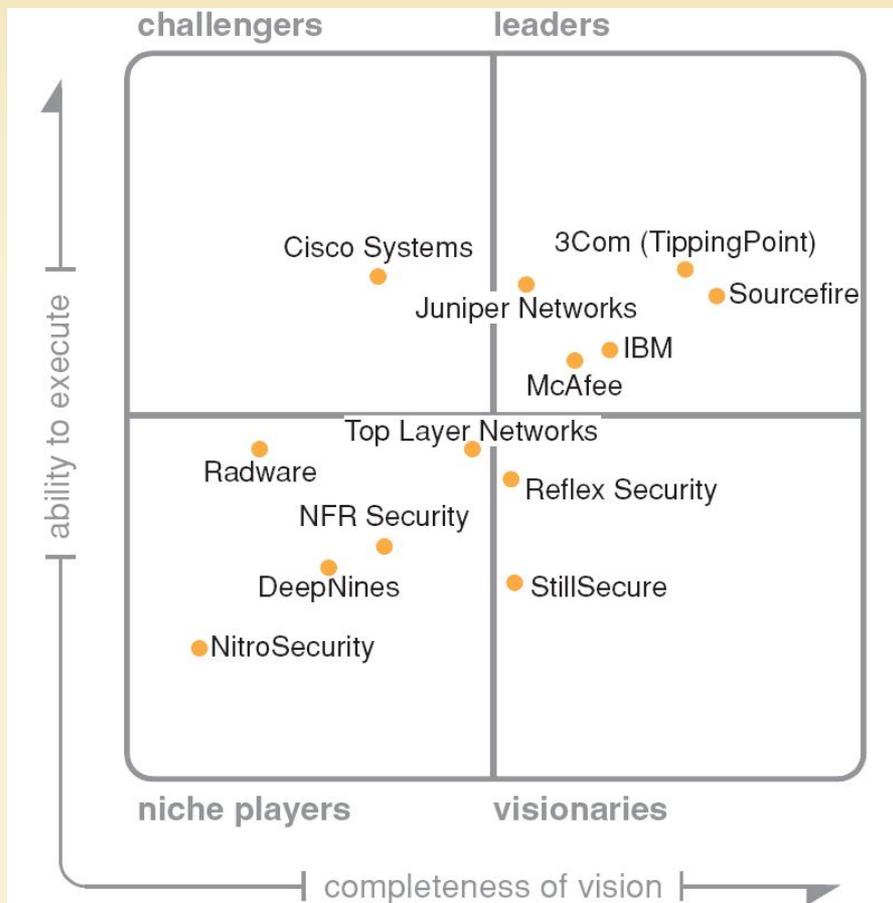
● Average coverage

● Poor coverage

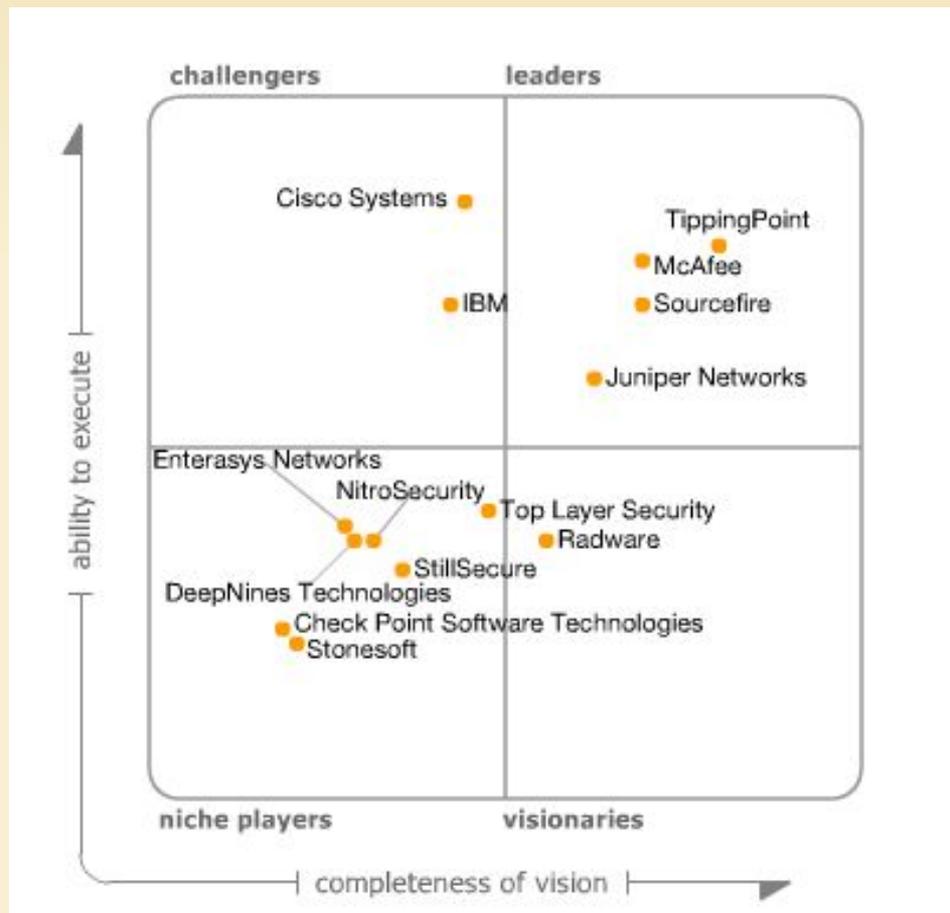
○ Inconsistent coverage

- No coverage

MQ: устройства IPS



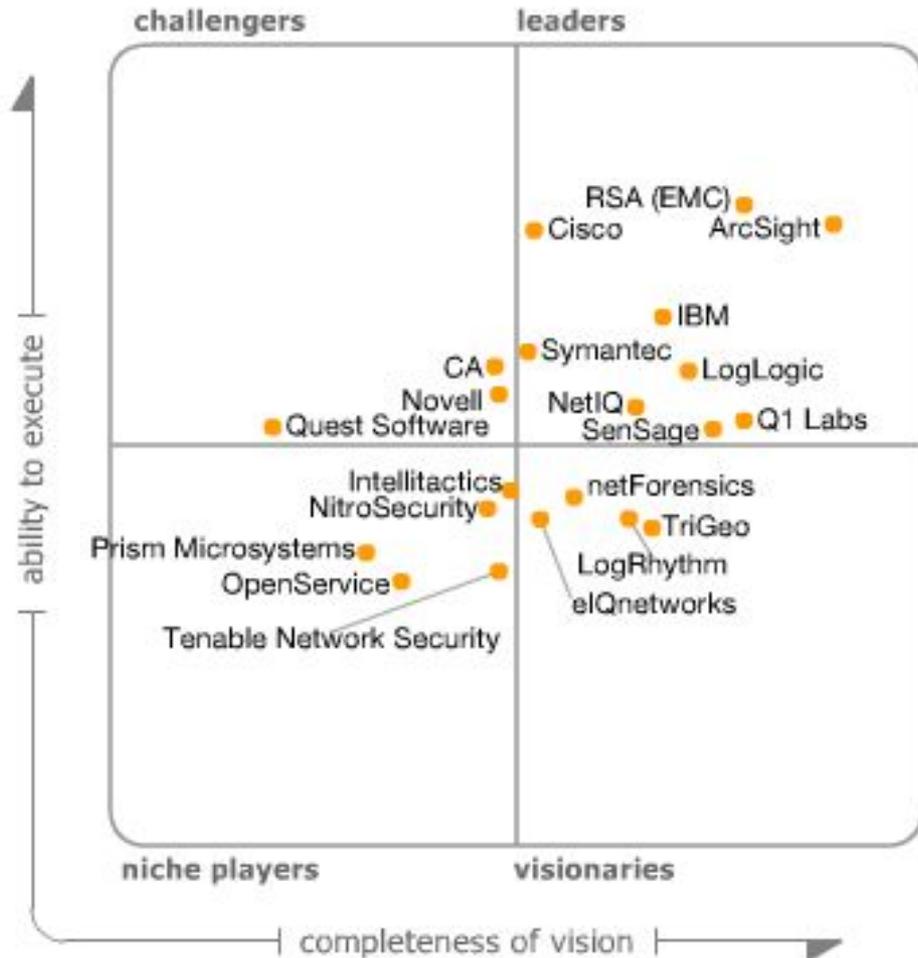
As of December 2006



As of 1H09

10 мая 2006 г. & Апрель 2009 г.
 Оптимизация рисков и повышение гибкости бизнеса

MQ: управление данными и событиями в области безопасности



As of May 2009

10 мая 2009
2009 г.

минимизация рисков и повышение эффективности
бизнеса

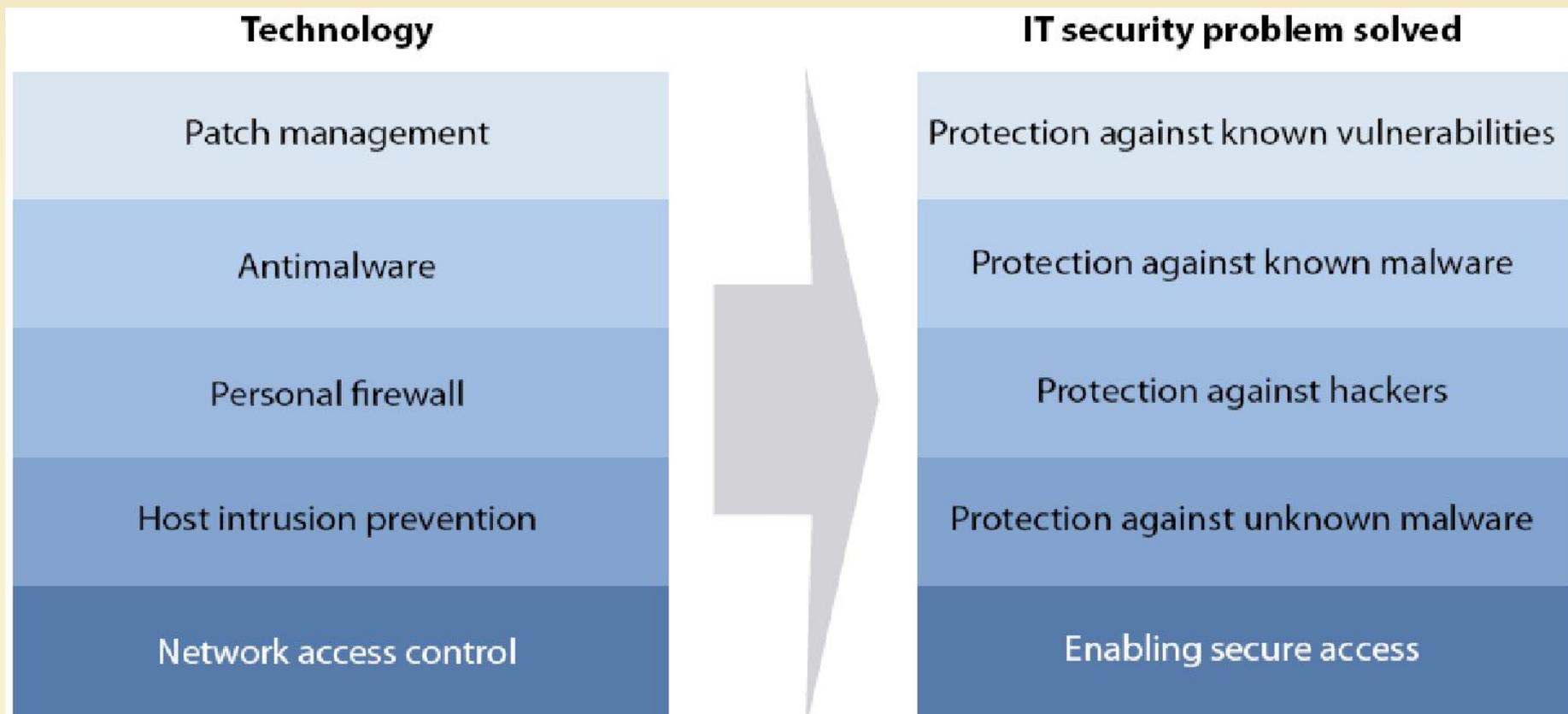
Защита клиентских устройств

- ◆ Множество инструментов
- ◆ Высокие начальные затраты
 - 40\$ - защита от вредоносных программ
 - 80\$ - полное шифрование диска
- ◆ Высокие операционные затраты
 - серверы для хранения отчетов и административных данных
 - дополнительная полоса пропускания
 - новый инструмент - новый сотрудник
- ◆ В поисках интегрированных решений
 - даже комплексные программные пакеты не охватывают всех функциональных категорий (шифрование, администрирование, ...)

10 ноября
2009 г.

Защита корпоративных сетей:
минимизация рисков и повышение гибкости
бизнеса

Защита клиентских устройств: традиционные технологии для известных проблем



10 ноября
2009 г.

Защита корпоративных сетей:
минимизация рисков и повышение гибкости
бизнеса

Защита клиентских устройств: новые решения для более сложных угроз

Technology

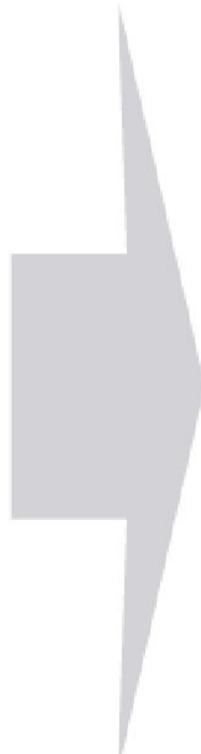
Application control

Device control

Full disk encryption

File encryption

Data leak prevention



IT security problem solved

Protection against malware

Protection against unauthorized device use and data loss

Data protection in the event of device loss

Protection against unauthorized data use

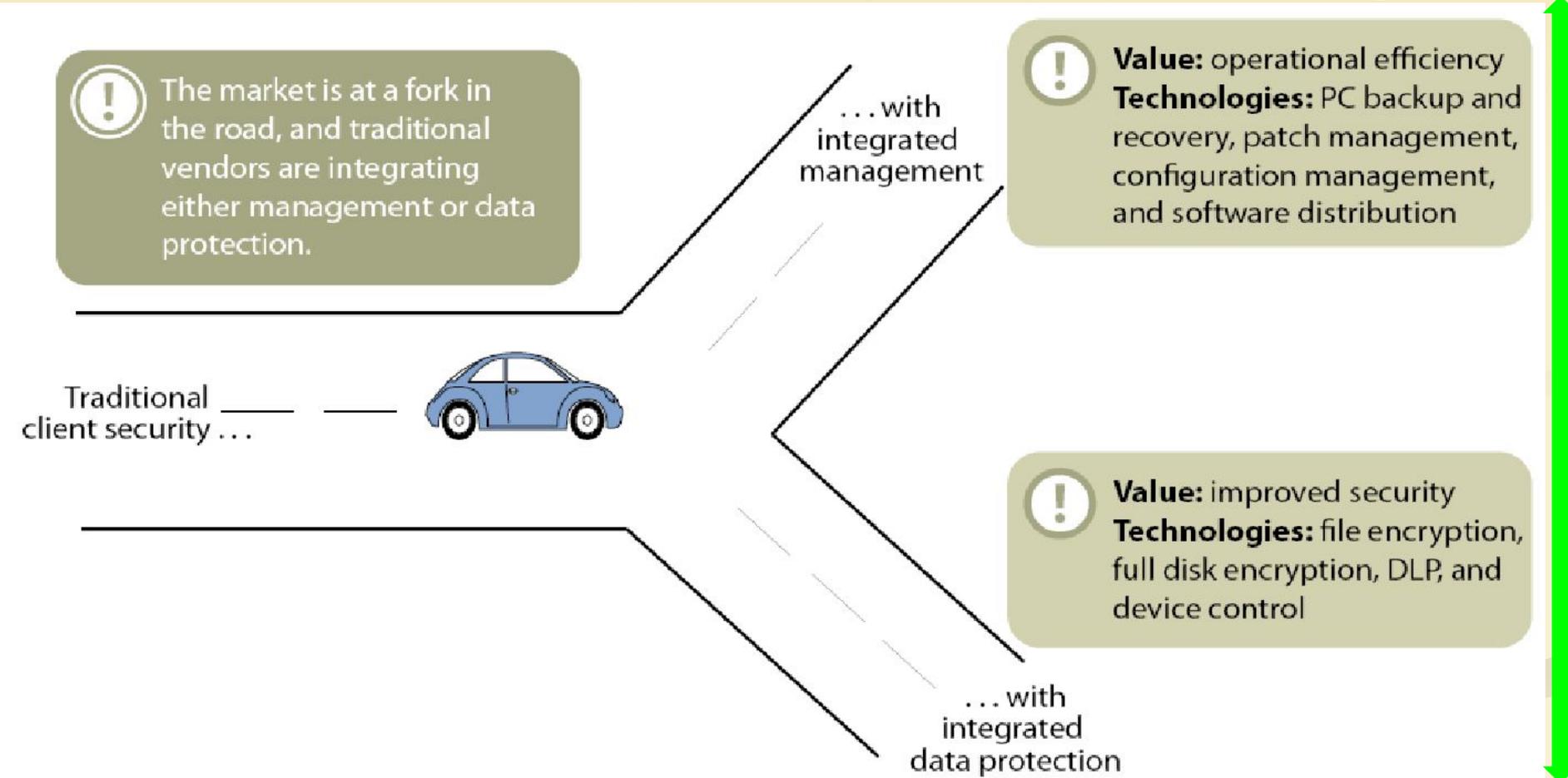
Protection against unauthorized data use

10 ноября
2009 г.

Защита корпоративных сетей:
минимизация рисков и повышение гибкости
бизнеса

«Вилка» клиентской безопасности

CA, LANDesk, Microsoft, Novell ... Symantec



Защита разно

B:

Vendors	Patch management	Antimalware	Personal firewall	Host intrusion prevention	Network access control	Application control	Device control	Full disk encryption	File encryption	Data leak prevention
BigFix	✓	✓	✓	☐	✓	✓	✓	☐	☐	✓
Bit9	☐	☐	☐	☐	☐	✓	✓	☐	☐	☐
BitDefender	☐	✓	✓	☐	☐	✓	☐	☐	☐	☐
CA	✓	✓	✓	✓	✓	✓	✓	☐	☐	☐
Check Point	☐	✓	✓	☐	✓	✓	✓	✓	☐	☐
Cisco	☐	✓	✓	✓	✓	✓	✓	☐	☐	✓
Entrust	☐	☐	☐	☐	☐	☐	✓	✓	✓	☐
Fiberlink	✓	☐	✓	✓	✓	✓	✓	☐	✓	✓
GuardianEdge	☐	☐	☐	☐	☐	☐	✓	✓	☐	☐
Kaspersky Lab	☐	✓	✓	✓	☐	✓	☐	☐	☐	☐
LANDesk	✓	✓	☐	✓	✓	✓	✓	☐	☐	☐
Lumension Security	✓	☐	☐	☐	☐	✓	✓	☐	☐	☐
McAfee	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft	✓	✓	☐	☐	✓	☐	☐	☐	☐	☐
Novell	✓	☐	✓	☐	✓	✓	✓	☐	✓	☐
SkyRecon	☐	☐	✓	✓	✓	✓	✓	☐	✓	☐
Sophos	☐	✓	✓	✓	✓	✓	✓	☐	☐	☐
Symantec	✓	✓	✓	✓	✓	✓	✓	✓	☐	✓
Trend Micro	☐	✓	✓	✓	✓	☐	☐	☐	☐	✓
Utimaco Safeware	☐	☐	☐	☐	☐	☐	✓	✓	✓	✓
Webroot	☐	✓	☐	✓	☐	☐	☐	☐	☐	☐
Websense	☐	☐	☐	☐	☐	✓	☐	☐	☐	✓



Forrester,
10 ноября
Sep 2008
2009 г.

Вопросы...



10 ноября
2009 г.

минимизация рисков и повышение гибкости
бизнеса

Благодарю за внимание

Павел Иванов

psi@osp.ru

10 ноября
2009 г.

Защита корпоративных сетей:
минимизация рисков и повышение гибкости
бизнеса

