McAfee Risk Advisor

Безопасность как процесс

Андрей Новиков

Intel и McAfee

Безопасность

vPro
Active Management Technology
Advanced Encryption Standard
Virtualization
One Time Password
Secure BIOS

+

Network Security
Cloud Security
Security Management
Endpoint Security
Technology Ecosystem

Наша стратегия: Security Connected

McAfee
An Intel Company

БЕЗОПАСНОСТЬ СЕТЕЙ

- Межсетевой экран следующего поколе
- Предотвращение вторжений
- Контроль доступа
- Анализ поведения пользователей сети

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Защита электронной почты
- Веб-защита
- Предотвращение утечки данных
- Шифрование

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

- Консоль управления операциями защ
- Аудит и управление политиками
- Управление уязвимостями
- Управление рисками
- Нормативно-правовое соответствие
- Система SIEM

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

- Защита от вредоносных программ
- Шифрование устройств
- Белые списки приложений
- Межсетевой экран для настольного компьютера
- Контроль устройств
- Защита электронной почты
- Контроль доступа к сети
- Веб-защита для конечных точек
- Предотвращение вторжений на узел

- Защита серверов и баз данных
- Безопасность на уровне микросхем (на аппаратном уровне)
- Защита смартфонов и планшетных ПК
- Защита виртуальных машин и инфраструктур виртуальных машин
- Защита встроенных устройств

СООБЩЕСТВО ПАРТНЕРОВ

- Security Innovation Alliance (SIA)
- McAfee Connected
- Партнеры по стратегическому альянсу Global Alliance

Требования бизнеса

- **Эффективное** управление политиками ИБ
- **Снижение затрат** на обслуживание ИТ и ИБ инфраструктур
- **Внедрение новых бизнес-сервисов** не должно становиться причиной возникновения брешей в системе безопасности
- **Обеспечение** максимальной **непрерывности** бизнес-процессов

Требования ИТ/ИБ

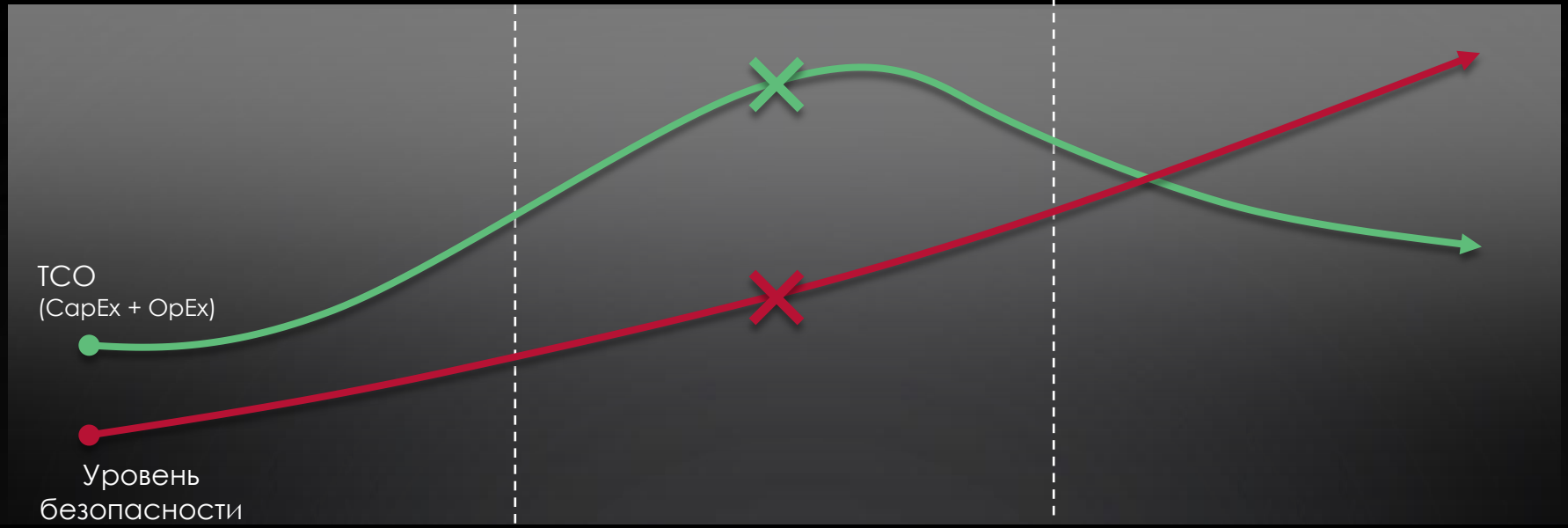
- После публикации информации о **новой уязвимости** на анализ актуального риска/защищенности уходят дни/недели

- **Патчи от различных производителей** не выходят мгновенно после появления новых угроз

- Приходится управлять **десятками консолей** от разных производителей

- **Атаки проникают** в сеть несмотря на «выстроенную» многоуровневую многовендорную (продолжите сами?) защиту

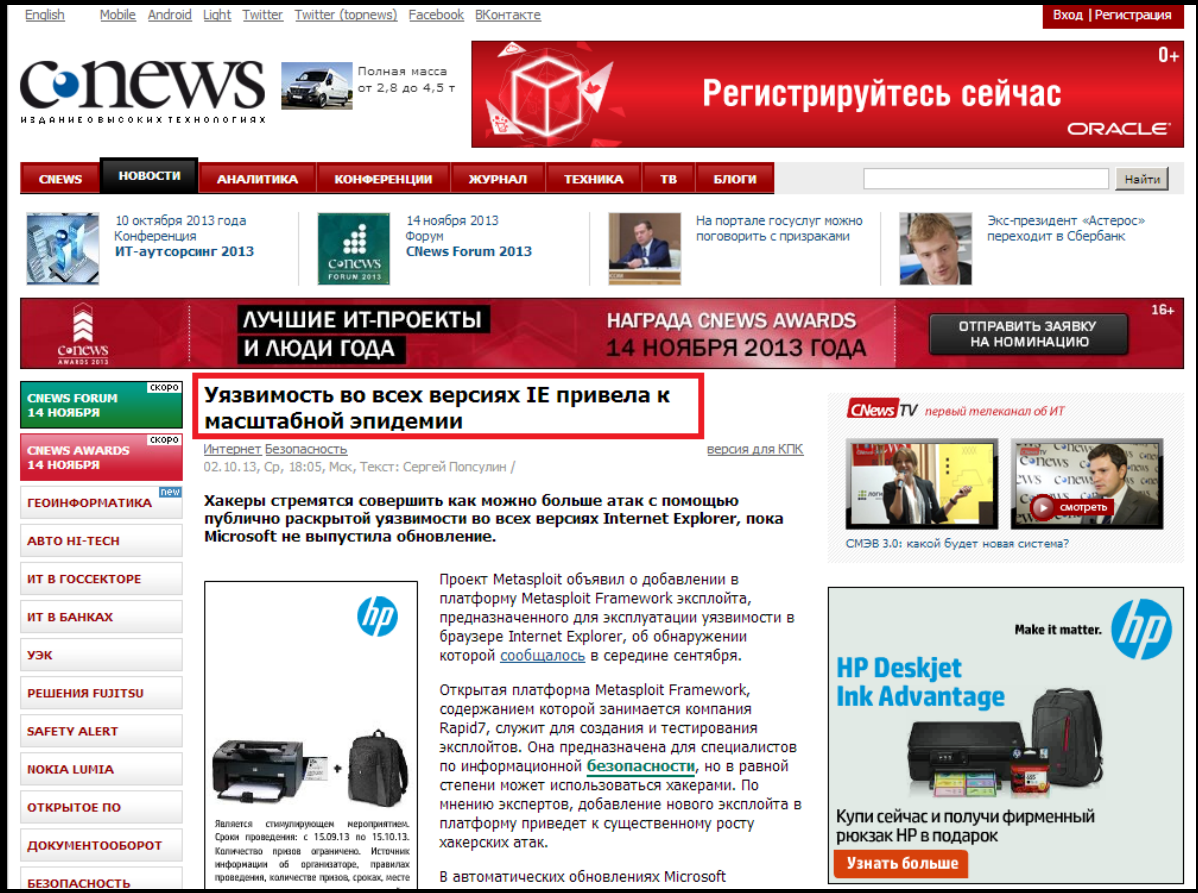
Модели информационной безопасности



Оптимизация безопасности

Что Вы делаете ПРИ ПОЯВЛЕНИИ НОВЫХ УЯЗВИМОСТЕЙ?

McAfee
An Intel Company



Что Вы делаете ПРИ ПОЯВЛЕНИИ НОВЫХ УЯЗВИМОСТЕЙ?

McAfee
An Intel Company

В автоматических обновлениях Microsoft найденная в прошлом месяце уязвимость пока не была устранена, однако был выпущен патч, который позволяет ее закрыть. **Его необходимо скачивать вручную.** Примечательно, что уязвимость затрагивает все версии IE - от шестой до одиннадцатой. Последняя интегрирована в еще не вышедшую на коммерческий рынок операционную систему Windows 8.

После того как стало известно об уязвимости, число атак, проводимых с ее помощью, **существенно возросло**. Масштаб эпидемии оказался шире, чем предполагалось изначально, резюмируют эксперты.

Подробнее: http://www.cnews.ru/news/top/index.shtml?2013/10/02/545138

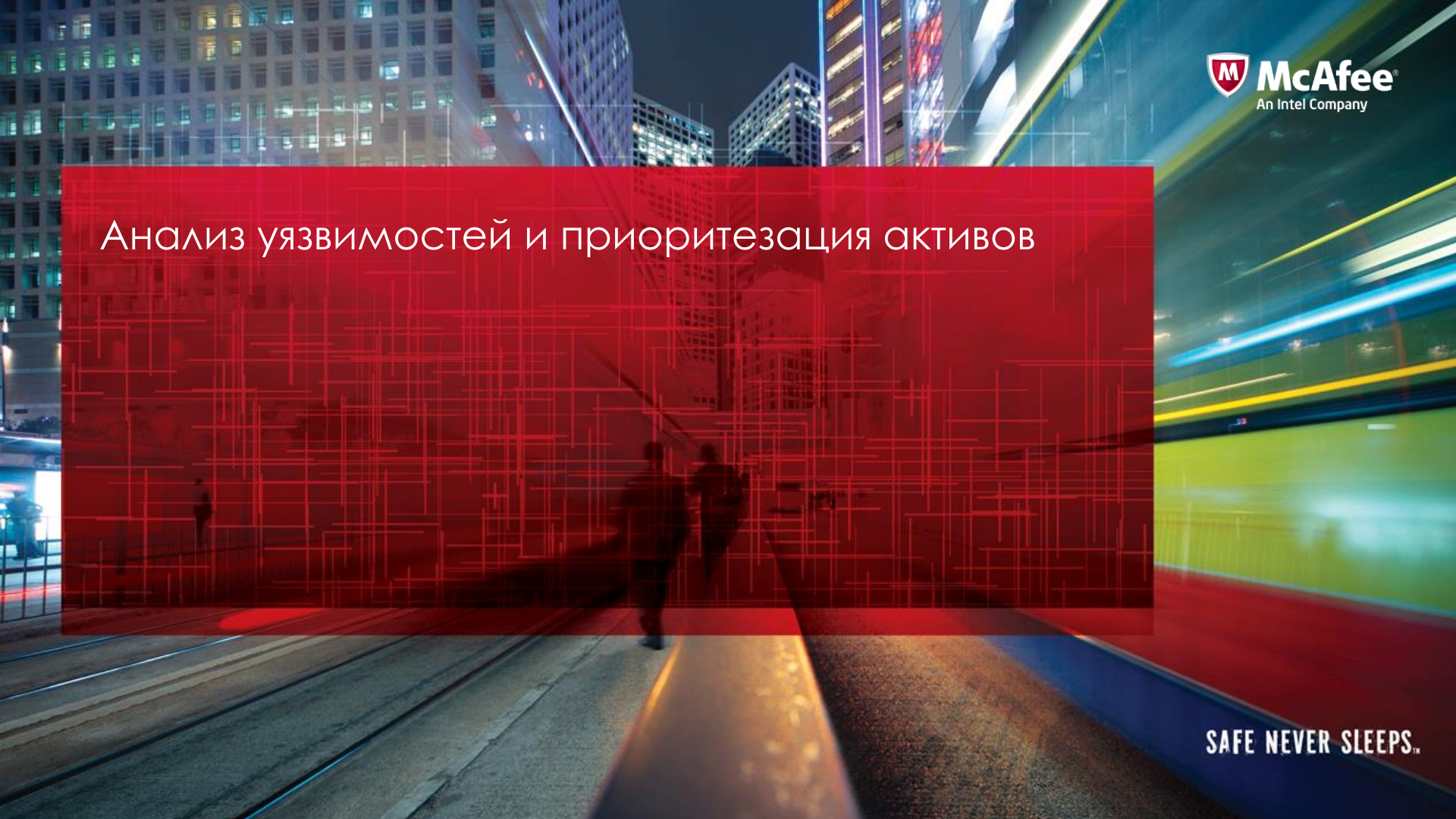
ТРАДИЦИОННЫЙ ПОДХОД в борьбе с УГРОЗАМИ

McAfee
An Intel Company

ЛОГ ФАЙЛЫ | КОНСОЛИ | ЗВОНКИ/EMAIL'ы | ТАБЛИЦЫ

МИНУТЫ | ЧАСЫ | ДНИ | НЕДЕЛИ

КОНТРМЕРЫ на основе ИЗУЧЕНИЯ РИСКОВ


McAfee
An Intel Company
Анализ уязвимостей и приоритезация активов
SAFE NEVER SLEEPS.

Сканирование ОС на ПК и серверах

Аудит политик

Сканирование БД

Сканирование Web

Сканирование ОС

- Безагентное сканирование с наибольшей базой известных уязвимостей
- Возможность дискаверинга сети
- Масштабируемость до миллионов сетевых узлов
- 437 поддерживаемых типов ОС
- Различные виды сканирования (intrusive, non-intrusive; credential/credential-less)
- Открытая схема БД – возможность интеграции
- Интеграция с продуктами McAfee по API, API опубликован и доступен для использования внешними поставщиками
- Реализация - ПО, ПАК, виртуальная платформа, SaaS

Сканирование Web-приложений

Аудит политик

Сканирование БД

Сканирование Web

Сканирование ОС

- Глубокое сканирование Web-приложений
- Дискаверинг приложения, построения карт
- Сканирование поддерживает OWASP, PCI, CWE
- Возможность сканирования после аутентификации в приложении
- Гибкая настройка включенных в скан URL и исключений

Специализированное сканирование СУБД

Аудит политик

Сканирование БД

Сканирование Web

Сканирование ОС

- Более 4 000 проверок только СУБД
  - Уровни обновлений
  - Baseline по конфигурации
  - Слабые пароли
  - Обнаружение backdoor'ов
  - Обнаружение конф.данных (PII, SSN, etc)
  - Уязвимый PL/SQL код
  - Неиспользуемые функции
  - Пользовательские проверки
- Предоставление отчетов по ролям
  - DBA, Developers, InfoSec, Audit

Аудит политик безопасности

Аудит политик

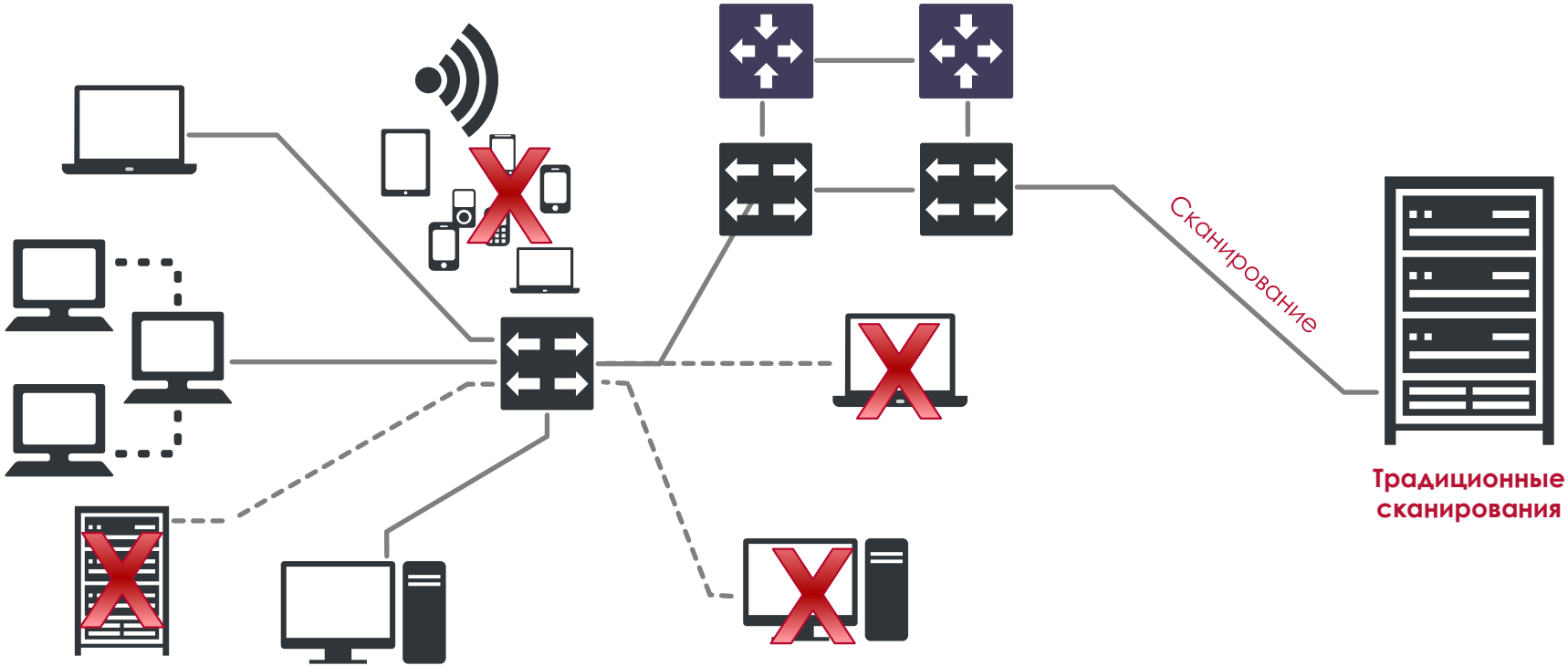
Сканирование БД

Сканирование Web

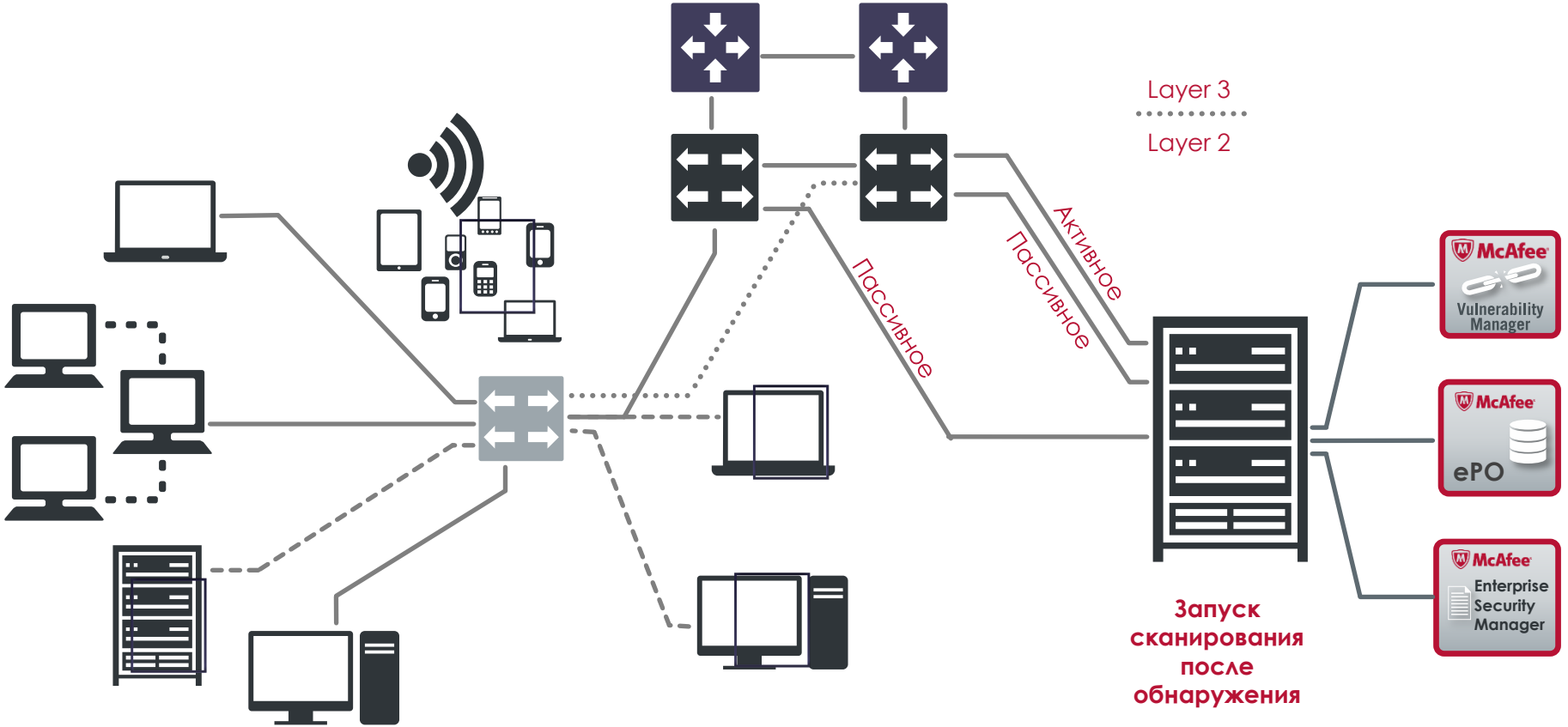
Сканирование ОС

- Сканирование на соответствие стандартам и регуляторам
  - PCI, SOX, HIPAA, FISMA
  - ISO, COBIT
  - CIS, DISA, FDCC
- Поддержка Win/UNIX/Linux/Mac
- Поддержка стандарта SCAP и сопутствующих протоколов (e.g., XCCDF, CCE)
- Гибкая система управления исключениями
- Поддержка «золотого» baseline
- Отслеживание изменения файлов

В чем отличие от традиционного сканирования?



Обнаружение активов в режиме реального времени



Полная информация об инфраструктуре

Software Inventory (Microsoft Windows Devices, Missing Anti-Spyware Software)

Generated From Predefined Report: Software Inventory (Microsoft Windows Devices, Missing Anti-Spyware Software)

Filters applied: Site is All

Sensor	Domain	IP Address	Operating System	Service Pack	OS Type	System Type	NetBIOS Name	DNS Name	Username	MAC Address	MAC Vendor ID
192.168.168.70	MENALAB	192.168.168.3	Microsoft Windows 2008		R2 Enterprise	Server		srv-dc1		00:0C:29:D3:77:5D	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.4	Microsoft Windows 2012		Standard		SRV-DC	srv-dc	Administrator@MENALAB.LOCAL	00:50:56:A7:7D:DE	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.5	Microsoft Windows 2008	SP1	R2 Enterprise	Server	SRV-EXC	srv-exc		00:0C:29:5E:1A:AE	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.7	Microsoft Windows 2008	SP1	R2 Standard	Server	SRV-EMM1	srv-emm1	Administrator@MENALAB.LOCAL	00:0C:29:71:6C:8B	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.16	Microsoft Windows 2008		R2 Standard	Server	SRV-RPT	srv-rpt	Administrator@MENALAB.LOCAL	00:0C:29:7D:08:EA	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.18	Microsoft Windows 2008		R2 Standard	Server	SRV-VMC	srv-vmc		00:0C:29:F2:C1:28	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.22	Microsoft Windows 2008	SP1	R2 Enterprise	Server		srv-epo	Administrator@MENALAB.LOCAL	00:50:56:A7:58:09	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.23	Microsoft Windows 2008	SP1	R2 Enterprise	Server	SRV-SQL2	srv-sql2	Administrator@MENALAB.LOCAL	00:50:56:A7:38:FB	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.24	Microsoft Windows 2008		R2 Standard	Server	SRV	srv-drm	administrator@MENALAB.LOCAL	00:0C:29:F4:54:51	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.26	Microsoft Windows 2008		R2 Standard	Server		src-orc		00:0C:29:EB:2D:2D	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.64	Microsoft Windows 7		Professional	Workstation		dsk-menalab2	Administrator@MENALAB.LOCAL	00:25:64:BC:62:1D	Dell Inc.
192.168.168.70	MENALAB	192.168.168.66	Microsoft Windows 7		Professional	Workstation		dsk-menalab	No user	00:25:64:BC:B1:5B	Dell Inc.
192.168.168.70	WORKGROUP	192.168.168.28	Microsoft Windows 2008		R2 Standard	Server	SRV-SSO			00:50:56:BE:67:11	VMware, Inc.

Summary

Description	Count
Total Number of Microsoft Windows Elements to be audited	21
Elements successfully audited	17
Elements unsuccessfully audited	0
Excluded / Offline Elements at the time of the audit	4

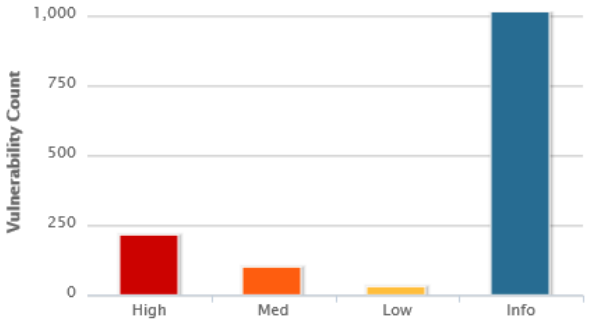
Подробная информация об обнаруженных уязвимостях

Most Prevalent Vulnerabilities Minimum Severity: Low Chart View

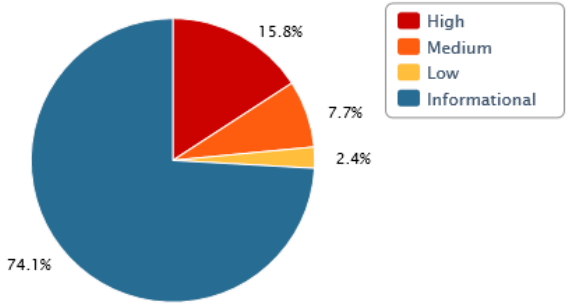
Vulnerability Name	Asset Count
NetBIOS NBTSTAT -A	10
Microsoft Windows Explorer Local Denial Of Service Vulnerability	7
HTTP Server Prone To Slow Denial Of Service Attack	5
Microsoft TURKTRUST.Inc Fraudulen Certificates Spoofing (2798897)	5
Microsoft Windows Kernel win32k.sys Privilege Escalation	5
Microsoft Internet Explorer CSS 'expression' Remote Denial of	5
Microsoft HTML Help Stack Overflow Remote Code Execution	4
Microsoft Windows wab32res.dll Insecure Library Loading Remote	4
Web Server Supports Weak SSL Encryption Certificates	4
Microsoft Unauthorized Digital Certificates Could Allow Spoofing	4

Most Prevalent Operating Systems List View

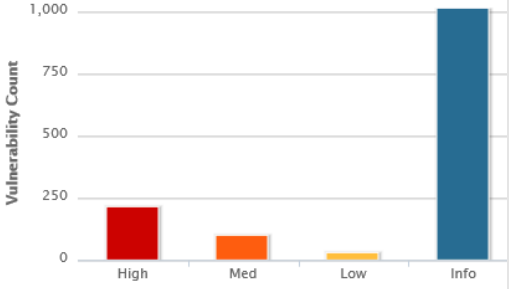
Vulnerability Count by Severity Current as of 2013-10-02 04:00



Vulnerability Percentage by Severity Current as of 2013-10-02 04:00

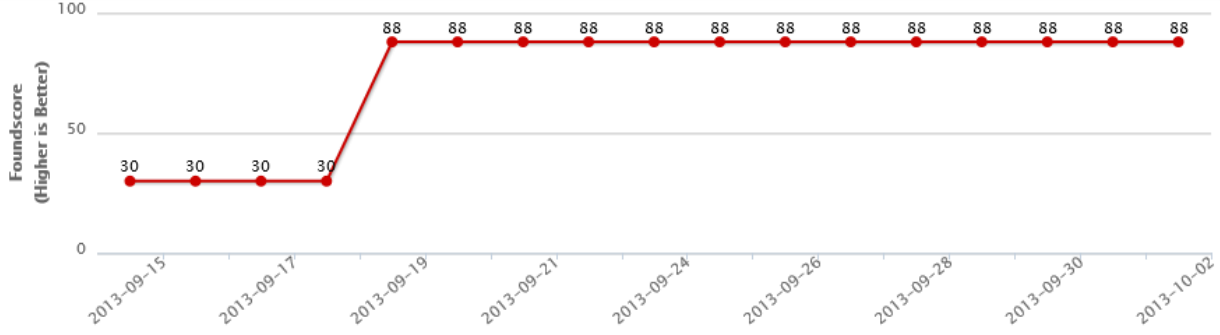


Vulnerability Count by Severity Current as of 2013-10-02 04:

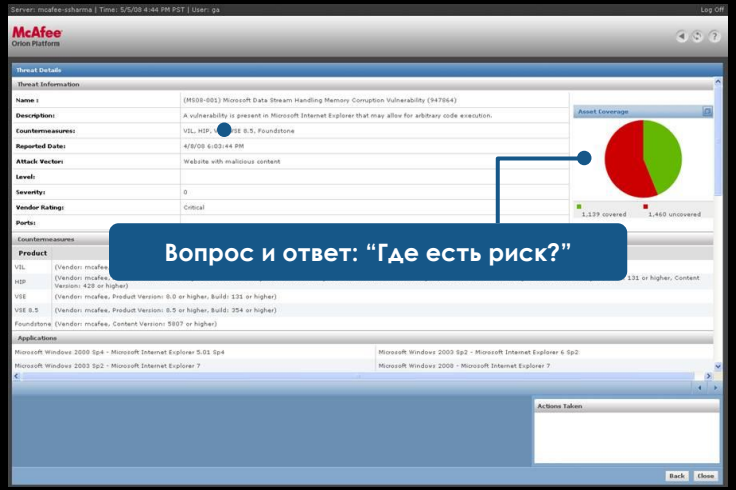


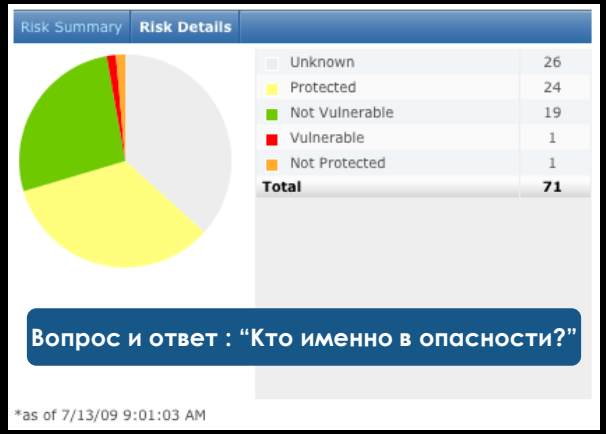
Organization Vulnerability Count Trend

Organization Foundscore Trend Current as of 2013-10-02 04:00 View Vulnerability Counts



Где есть риск?



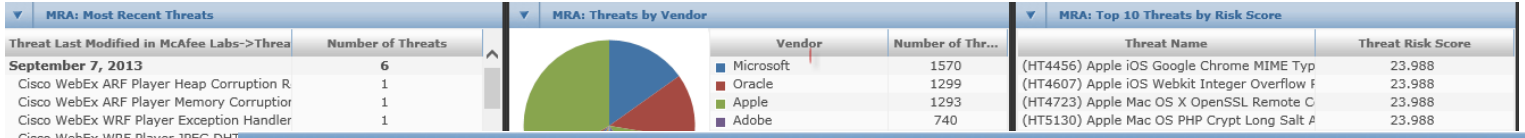


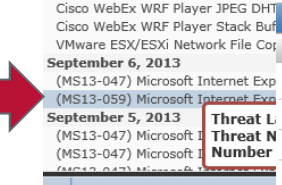
Доказанная эффективность
Позволяет бизнесу оценить эффективность от вложения в инфраструктуру безопасности

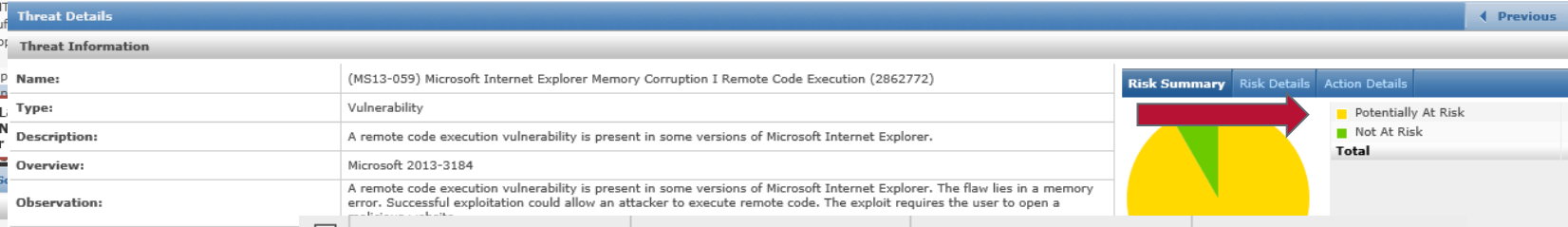
Безопасность без паники
Устраняет панику, связанную с необходимостью непрерывной установки патчей для различного ПО и ОС

“От 30,000 к 30”
Позволяет строить умную ИТ-инфраструктуру. Основано на управлении рисками

Интеллектуальная система помощи для приоритезации

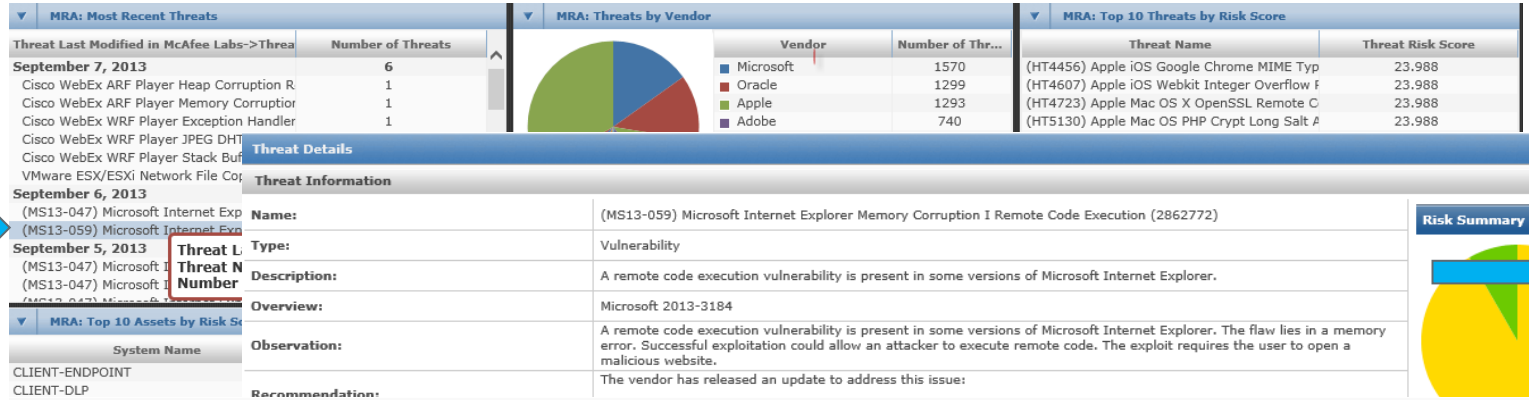






System Name	Risk Score ▲	Criticality	Countermeasure Status
CLIENT-DLP	18.666	Medium	Not Protected
SRV-REPO	18.666	Medium	Not Protected
SRV-RPT	18.666	Medium	Not Protected
SRV-DC	18.666	Medium	Not Protected
SRV-SMC	18.666	Medium	Not Protected
JUMPSERVER	18.666	Medium	Not Protected
SRV-EPO5	18.666	Medium	Not Protected
SRV-EMM	18.666	Medium	Not Protected
SRV-EXC	18.666	Medium	Not Protected
CLIENT-R-C	18.666	Medium	Not Protected
CLIENT-ENDPOINT	37.332	Critical	Not Protected

Интеллектуальная система помощи для приоритезации



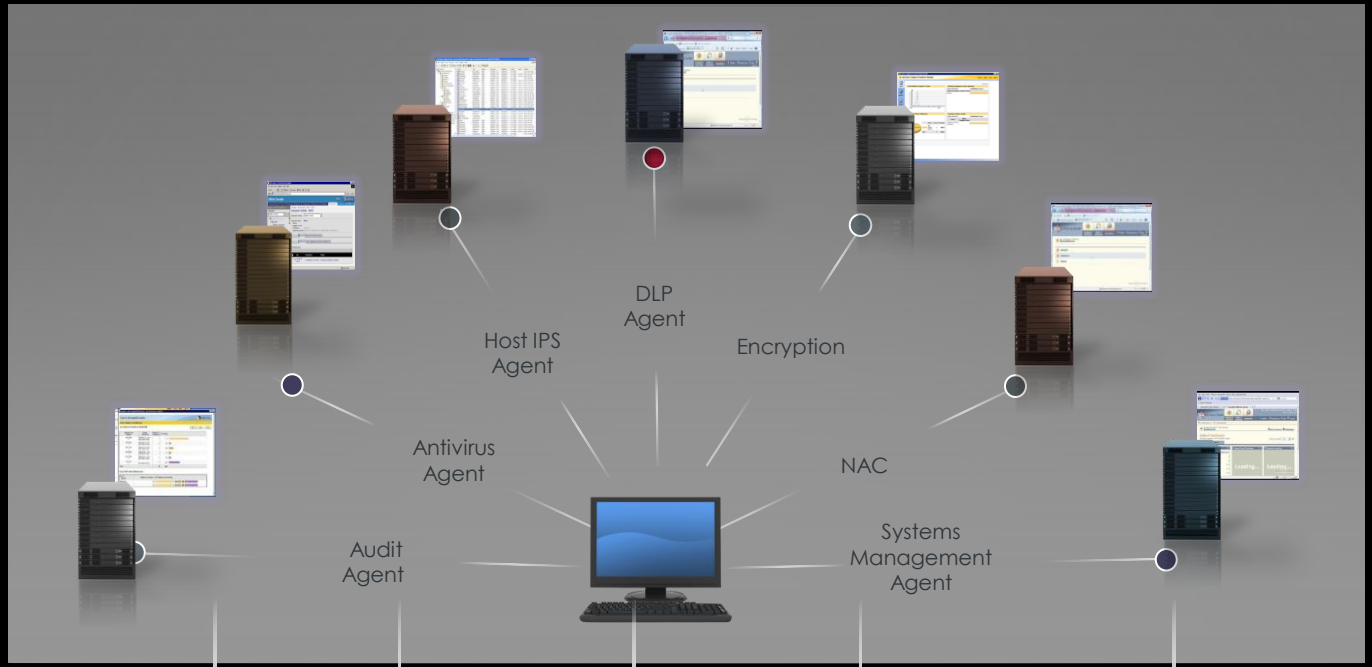
Asset is protected by one or more installed countermeasures.

Hide details

	Property	Expected	Observed	State
HIPS	**Signature**	428		Insufficient Data
	Product Version	Higher than or equal to 6.0		
McAfee AV DAT	**Dat File Version**	Higher than or equal to 7195	7168	Not Protected
	Engine Version	Higher than or equal to 5100	5600.1067	
McAfee Application Control	**Runtime Control Enabled**	true		Insufficient Data
McAfee Network Security Platform	**Attack Id**	0x4510B300		Insufficient Data
McAfee Web Gateway	**ContentVersion**	Higher than or equal to 7195		Insufficient Data
VSE	**Buffer Overflow Protection**	true	true	Protected
	Version	Higher than or equal to 8.0	8.8.0.975.Srv	

Архитектура безопасности

Насколько объединена ваша система безопасности?



КАЖДОЕ **РЕШЕНИЕ** ИМЕЕТ СВОЕГО АГЕНТА

КАЖДЫЙ **АГЕНТ** ИМЕЕТ СВОЮ КОНСОЛЬ

КАЖДАЯ **КОНСОЛЬ** ТРЕБУЕТ ОТДЕЛЬНОГО СЕРВЕРА

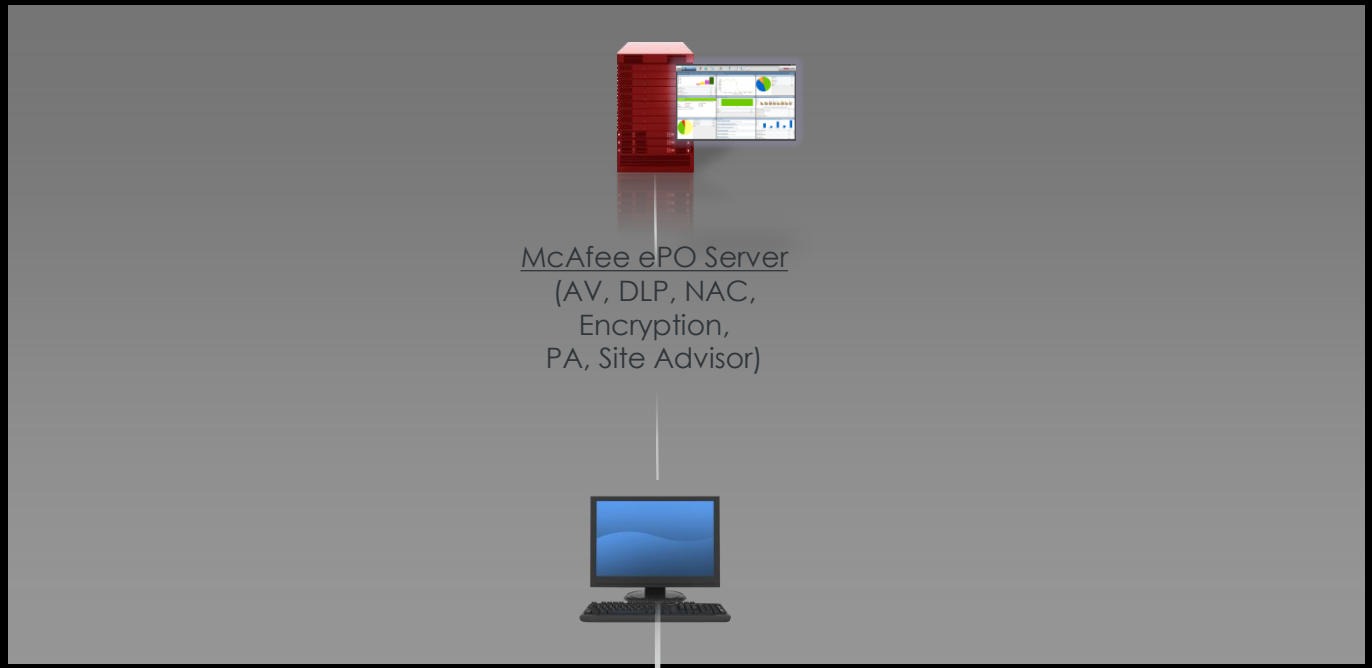
КАЖДЫЙ **СЕРВЕР** ТРЕБУЕТ ОС И БАЗУ ДАННЫХ

КАЖДАЯ **ОС И БАЗА** ДАННЫХ ТРЕБУЕТ ПОДДЕРЖКИ, ЛЮДЕЙ, ПАТЧЕЙ

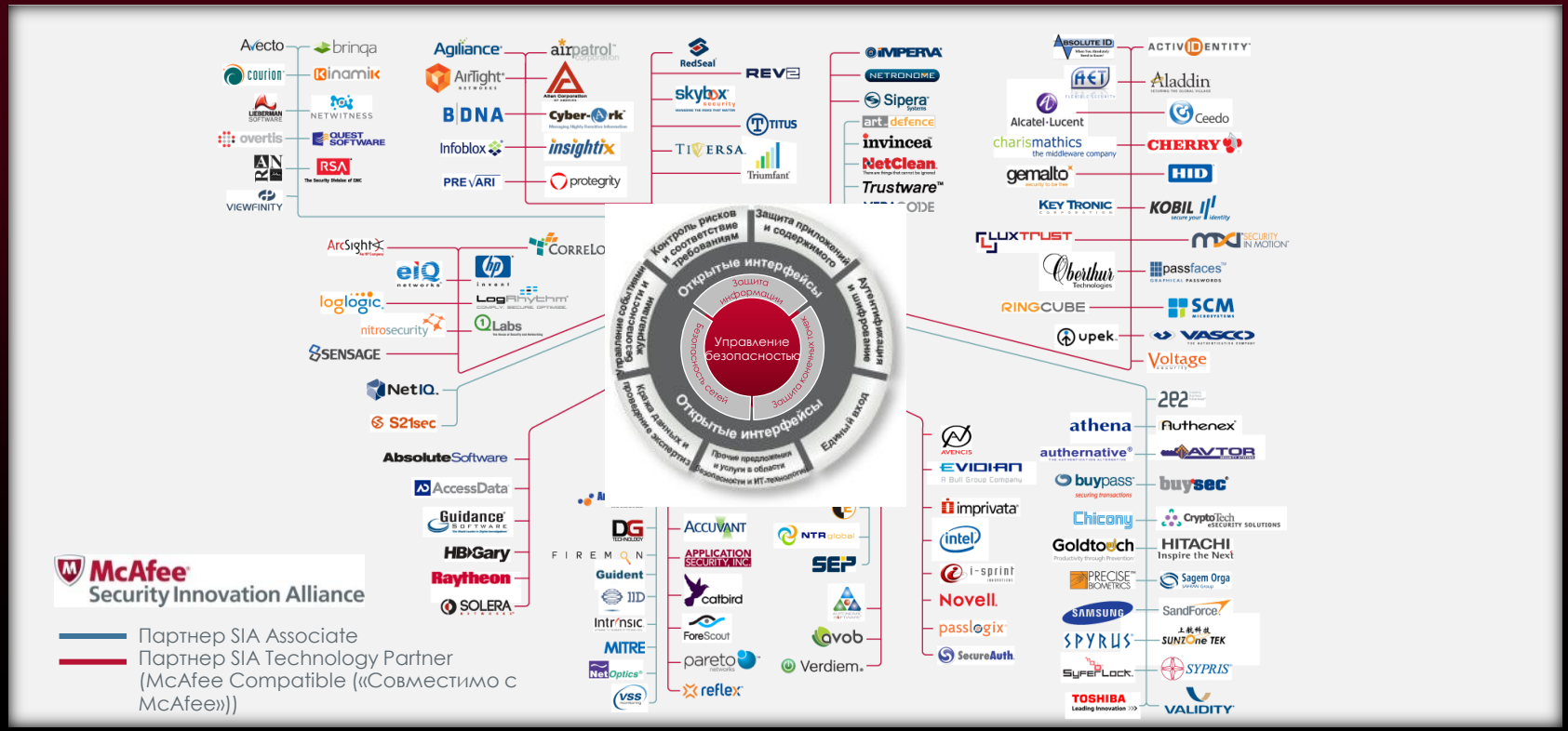
ГДЕ ЖЕ **КОНЕЦ?**

Платформа McAfee

Насколько объединена ваша система безопасности?



Security Connected: Интеграция сторонних продуктов




McAfee®