

McAfee Risk Advisor



Безопасность как процесс

Андрей Новиков



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

БЕЗОПАСНОСТЬ СЕТЕЙ



- ▶ Межсетевой экран следующего поколения
- ▶ 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 защиты
- ▶ 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

- **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

- 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

Реактивная

(~3% от ИТ бюджета)

Про-активная

(~8% от ИТ бюджета)

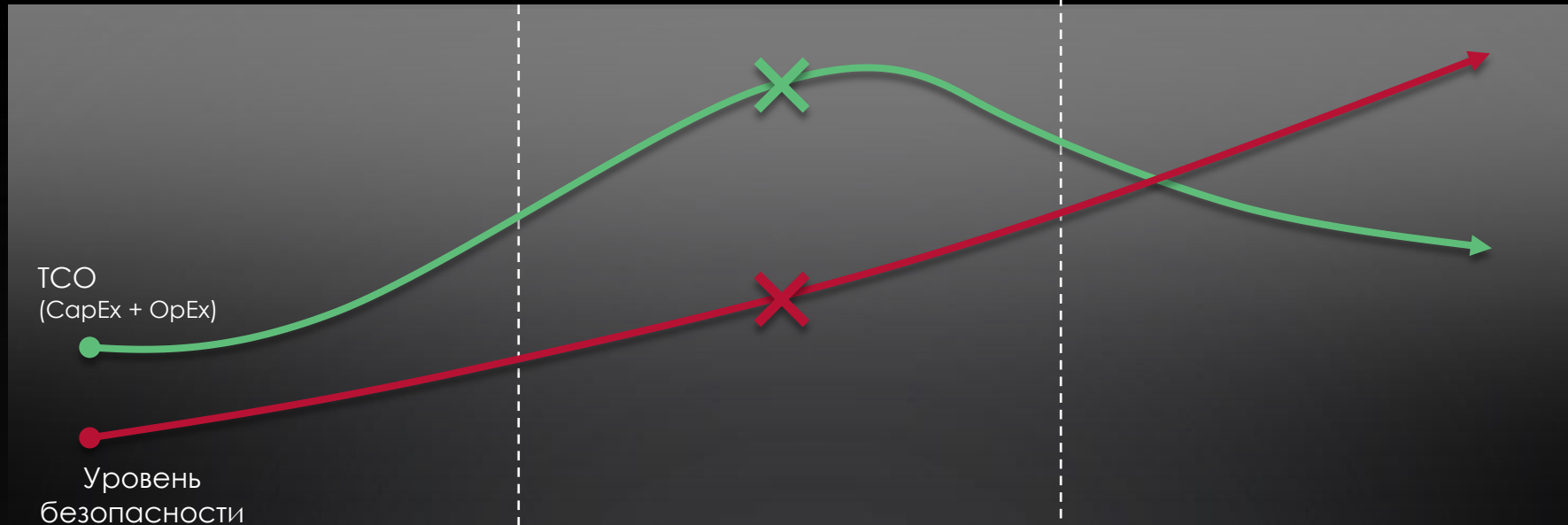
Оптимизированная

(~4% от ИТ бюджета)

ТСО
(CapEx + OpEx)

Уровень
безопасности

Оптимизация безопасности



Что Вы делаете ПРИ ПОЯВЛЕНИИ НОВЫХ УЯЗВИМОСТЕЙ?

English Mobile Android Light Twitter Twitter (topnews) Facebook ВКонтакте Вход | Регистрация

cnews

ИЗДАНИЕ ОБЪЕДИНЕННЫХ ТЕХНОЛОГИЯХ

Полная масса от 2,8 до 4,5 т



Регистрируйтесь сейчас

ORACLE

0+

CNEWS НОВОСТИ АНАЛИТИКА КОНФЕРЕНЦИИ ЖУРНАЛ ТЕХНИКА ТВ БЛОГИ

10 октября 2013 года
Конференция
ИТ-аутсорсинг 2013

14 ноября 2013
Форум
CNews Forum 2013

На портале госуслуг можно поговорить с призраками

Экс-президент «Астерос» переходит в Сбербанк

ЛУЧШИЕ ИТ-ПРОЕКТЫ И ЛЮДИ ГОДА

НАГРАДА CNEWS AWARDS 14 НОЯБРЯ 2013 ГОДА

ОТПРАВИТЬ ЗАЯВКУ НА НОМИНАЦИЮ

16+

Уязвимость во всех версиях IE привела к масштабной эпидемии

Интернет. Безопасность
02.10.13, Ср, 18:05, Моск, Текст: Сергей Попсулин / [версия для КПК](#)

Хакеры стремятся совершить как можно больше атак с помощью публично раскрытой уязвимости во всех версиях Internet Explorer, пока Microsoft не выпустила обновление.

Проект Metasploit объявил о добавлении в платформу Metasploit Framework эксплойта, предназначенного для эксплуатации уязвимости в браузере Internet Explorer, об обнаружении которой [сообщалось](#) в середине сентября.


Открытая платформа Metasploit Framework, содержанием которой занимается компания Rapid7, служит для создания и тестирования эксплойтов. Она предназначена для специалистов по информационной безопасности, но в равной степени может использоваться хакерами. По мнению экспертов, добавление нового эксплойта в платформу приведет к существенному росту хакерских атак.

В автоматических обновлениях Microsoft

HP

Make it matter. **hp**

HP Deskjet Ink Advantage



Купи сейчас и получи фирменный рюкзак HP в подарок

Узнать больше

ГЕОИНФОРМАТИКА new

АВТО HI-TECH

ИТ В ГОССЕКТОРЕ

ИТ В БАНКАХ

УЭК

РЕШЕНИЯ FUJITSU

SAFETY ALERT

NOKIA LUMIA

ОТКРЫТОЕ ПО

ДОКУМЕНТООБОРОТ

БЕЗОПАСНОСТЬ

Является стимулирующим мероприятием. Срок проведения: с 15.09.13 по 15.10.13. Количество призов ограничено. Источник информации об организаторе, правилах проведения, количестве призов, сроках, месте

Что Вы делаете ПРИ ПОЯВЛЕНИИ НОВЫХ УЯЗВИМОСТЕЙ?

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



ЛОГ ФАЙЛЫ

КОНСОЛИ

ЗВОНКИ/EMAIL'Ы

ТАБЛИЦЫ



МИНУТЫ

ЧАСЫ

ДНИ

НЕДЕЛИ



Анализ уязвимостей и приоритезация активов

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

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

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

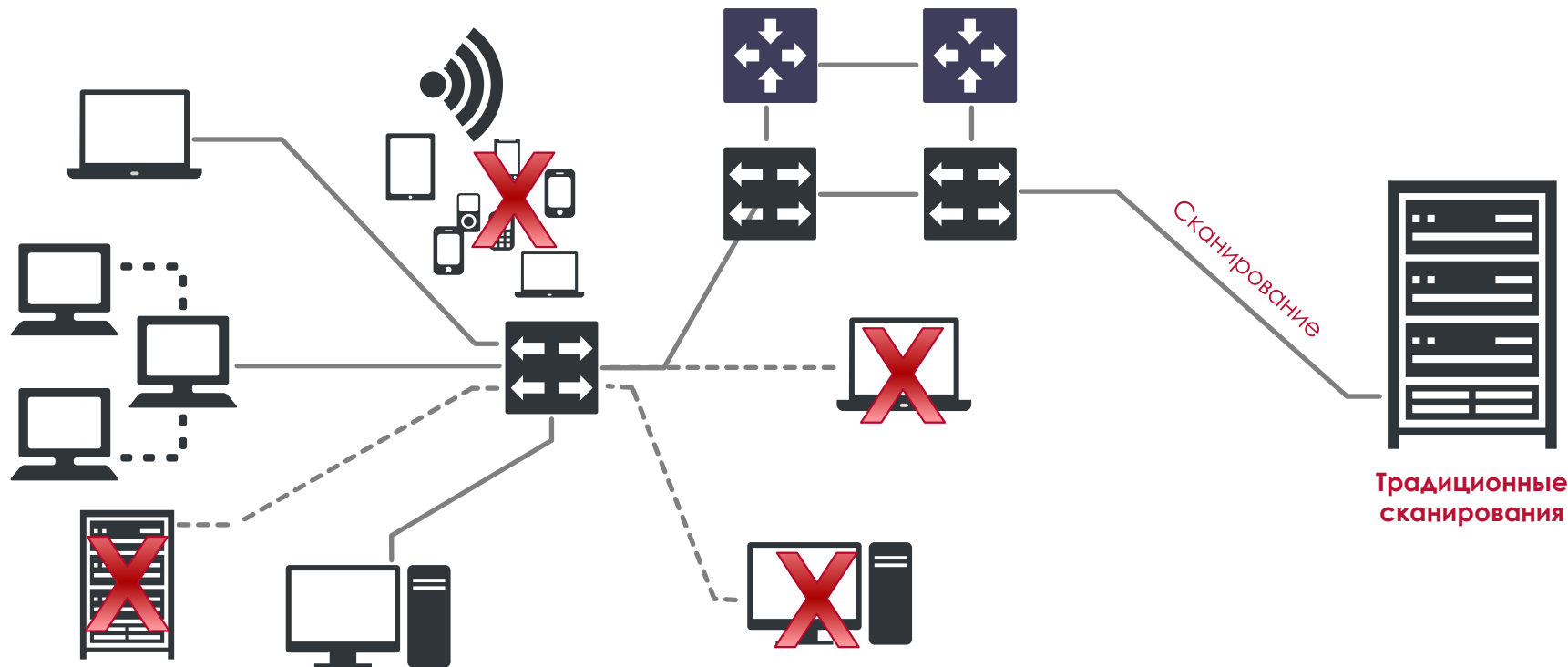
Сканирование БД

Сканирование Web

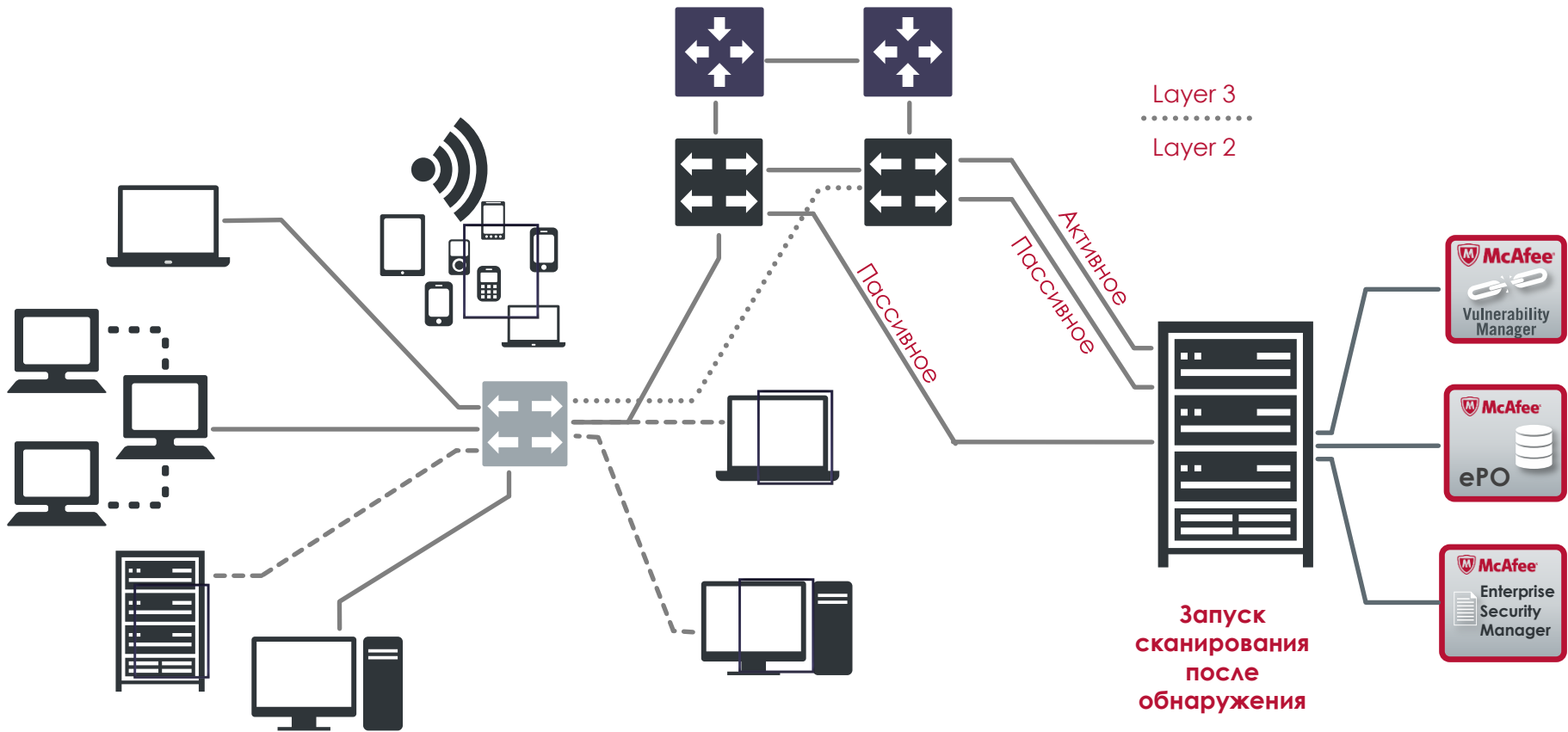
Сканирование ОС

- 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:29:03:77:5D	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:D E	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.5	Microsoft Windows 2008	SP1	R2 Enterprise	Server	SRV-EXC	srv-exc		00:50:56:A7:7D:D E	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:8 B	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:E A	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:C1:2 B	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:A7:58:0 9	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:F B	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:F4:54:5 1	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.26	Microsoft Windows 2008		R2 Standard	Server		src-orc		00:0C:29:EB:2D:2 D	VMware, Inc.
192.168.168.70	MENALAB	192.168.168.64	Microsoft Windows 7		Professional	Workstation		dsk-menalab2	Administrator@MENALAB.LOCAL	00:25:64:8C:62:1 D	Dell Inc.
192.168.168.70	MENALAB	192.168.168.66	Microsoft Windows 7		Professional	Workstation		dsk-menalab	No user	00:25:64:8C:81:5 B	Dell Inc.
192.168.168.70	WORKGROUP	192.168.168.28	Microsoft Windows 2008		R2 Standard	Server	SRV-SSO			00:50:56:8E:67:1 1	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

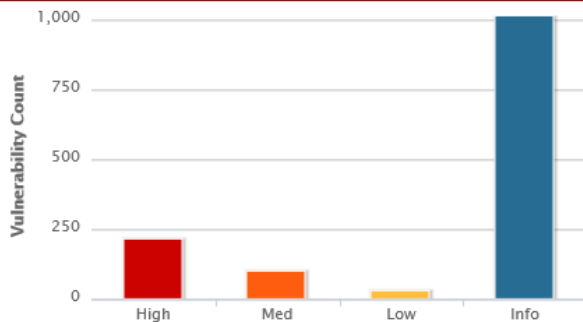
Most Prevalent Vulnerabilities Minimum Severity: **LOW** [Chart View](#)

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

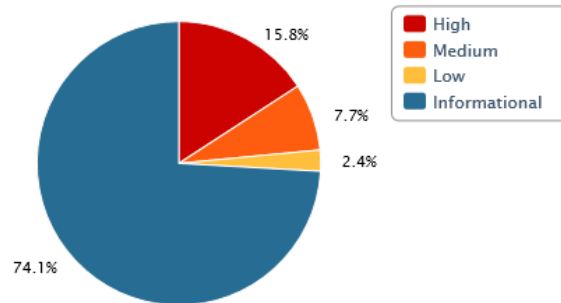
Most Prevalent Operating Systems [List View](#)



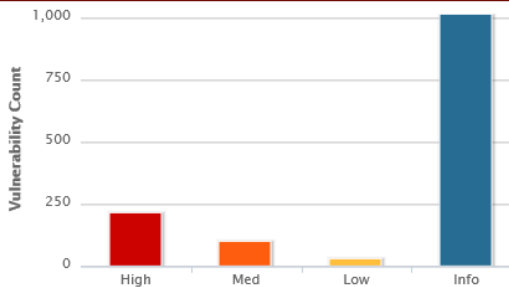
Vulnerability Count by Severity Current as of 2013-10-02 04:00



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

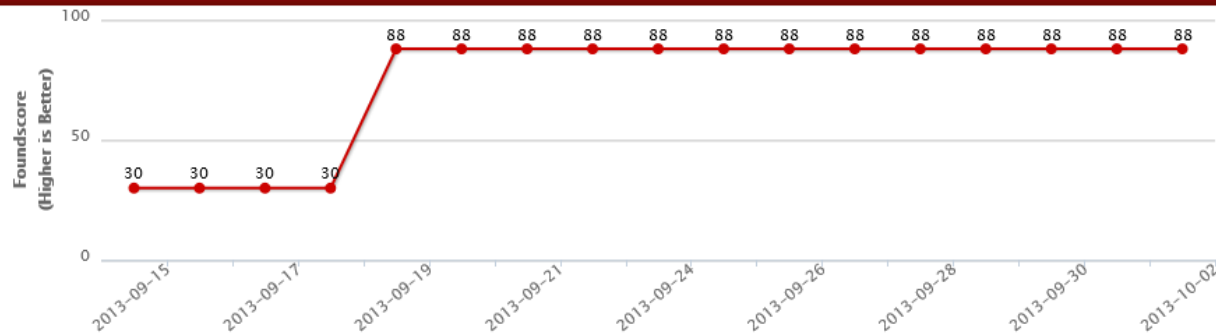


Vulnerability Count by Severity Current as of 2013-10-02 04:00

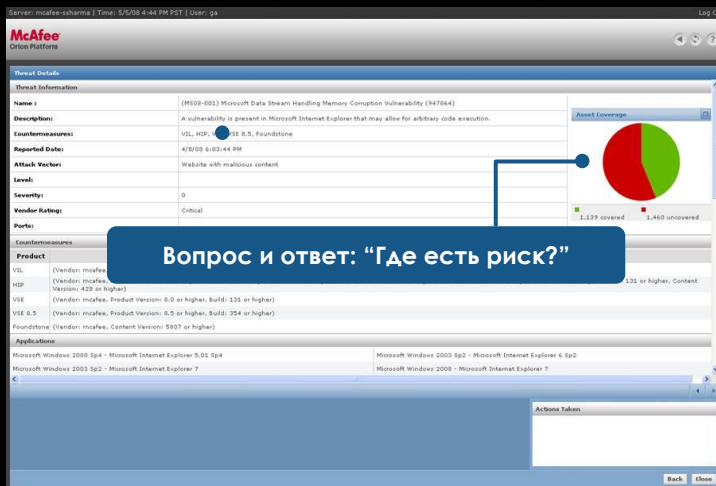


Organization Vulnerability Count Trend

Organization Foundscore Trend Current as of 2013-10-02 04:00 [View Vulnerability Counts](#)



Где есть риск?



Server: mcafee-sshome | Time: 5/5/09 4:44 PM PST | User: ga

McAfee
Open Platform

Threat Details

Threat Information

Name: (MS08-083) Microsoft Data Stream Handling Memory Corruption Vulnerability (947864)

Description: A vulnerability is present in Microsoft Internet Explorer that may allow for arbitrary code execution.

Countmeasures: VUL, HIP, USE 8.5, Foundation

Reported Date: 4/8/09 6:03:44 PM

Attack Vector: Website with malicious content

Level: 0

Severity: 0

Vendor Rating: Critical

Ports:

Countmeasures

Product

MS08-083 (Vendor: mcafee, Product Version: 8.0 or higher, Build: 131 or higher, Content: 131 or higher)

VUL (Vendor: mcafee, Product Version: 8.0 or higher, Build: 131 or higher)

USE 8.5 (Vendor: mcafee, Product Version: 8.5 or higher, Build: 134 or higher)

Foundation (Vendor: mcafee, Content Version: 8007 or higher)

Applications

Microsoft Windows 2009 Sp4 - Microsoft Internet Explorer 9.01 Sp4

Microsoft Windows 2009 Sp2 - Microsoft Internet Explorer 8 Sp2

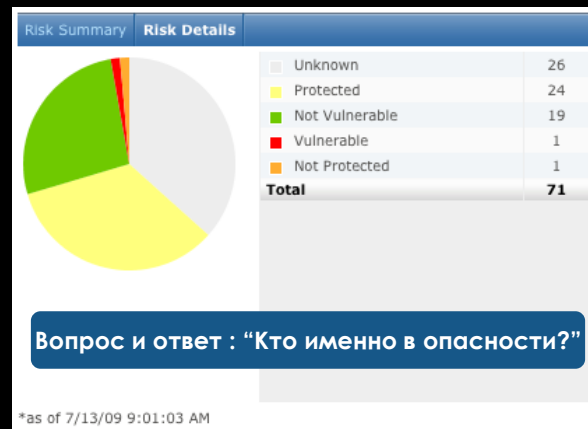
Microsoft Windows 2003 Sp2 - Microsoft Internet Explorer 7

Microsoft Windows 2000 - Microsoft Internet Explorer 7

Actions Taken

Back Close

Вопрос и ответ: "Где есть риск?"



Risk Summary Risk Details

Unknown 26

Protected 24

Not Vulnerable 19

Vulnerable 1

Not Protected 1

Total 71

Вопрос и ответ: "Кто именно в опасности?"

*as of 7/13/09 9:01:03 AM

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 приоритизации

MRA: Most Recent Threats

Threat Last Modified in McAfee Labs->Threat	Number of Threats
September 7, 2013	6
Cisco WebEx ARF Player Heap Corruption R	1
Cisco WebEx ARF Player Memory Corruption	1
Cisco WebEx WRF Player Exception Handler	1
Cisco WebEx WRF Player JPEG DHT	
Cisco WebEx WRF Player Stack Buf	
VMware ESX/ESXi Network File Co	

MRA: Threats by Vendor



Vendor	Number of Thr...
Microsoft	1570
Oracle	1299
Apple	1293
Adobe	740

MRA: Top 10 Threats by Risk Score

Threat Name	Threat Risk Score
(HT4456) Apple iOS Google Chrome MIME Typ	23.988
(HT4607) Apple iOS Webkit Integer Overflow F	23.988
(HT4723) Apple Mac OS X OpenSSL Remote C	23.988
(HT5130) Apple Mac OS PHP Crypt Long Salt A	23.988

Threat Details


Threat Information

Name:	(MS13-059) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2862772)
Type:	Vulnerability
Description:	A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer.
Overview:	Microsoft 2013-3184
Observation:	A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer. The flaw lies in a memory error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a...

MRA: Top 10 Assets by Risk Score

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

Risk Summary




- 100% Potentially At Risk
- 0% Not At Risk
- Total**

Интеллектуальная система помощи для приоритизации

MRA: Most Recent Threats

Threat Last Modified in McAfee Labs->Threat	Number of Threats
September 7, 2013	6
Cisco WebEx ARF Player Heap Corruption R	1
Cisco WebEx ARF Player Memory Corruption	1
Cisco WebEx WRF Player Exception Handler	1

MRA: Threats by Vendor



Vendor	Number of Thr...
Microsoft	1570
Oracle	1299
Apple	1293
Adobe	740

MRA: Top 10 Threats by Risk Score

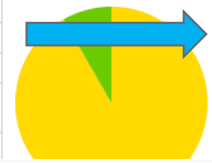
Threat Name	Threat Risk Score
(HT4456) Apple iOS Google Chrome MIME Typ	23.988
(HT4607) Apple iOS Webkit Integer Overflow F	23.988
(HT4723) Apple Mac OS X OpenSSL Remote C	23.988
(HT5130) Apple Mac OS PHP Crypt Long Salt A	23.988

Threat Details

Threat Information

Name:	(MS13-059) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2862772)
Type:	Vulnerability
Description:	A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer.
Overview:	Microsoft 2013-3184
Observation:	A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer. The flaw lies in a memory error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.
Recommendation:	The vendor has released an update to address this issue:

Risk Summary Risk Details Action Details



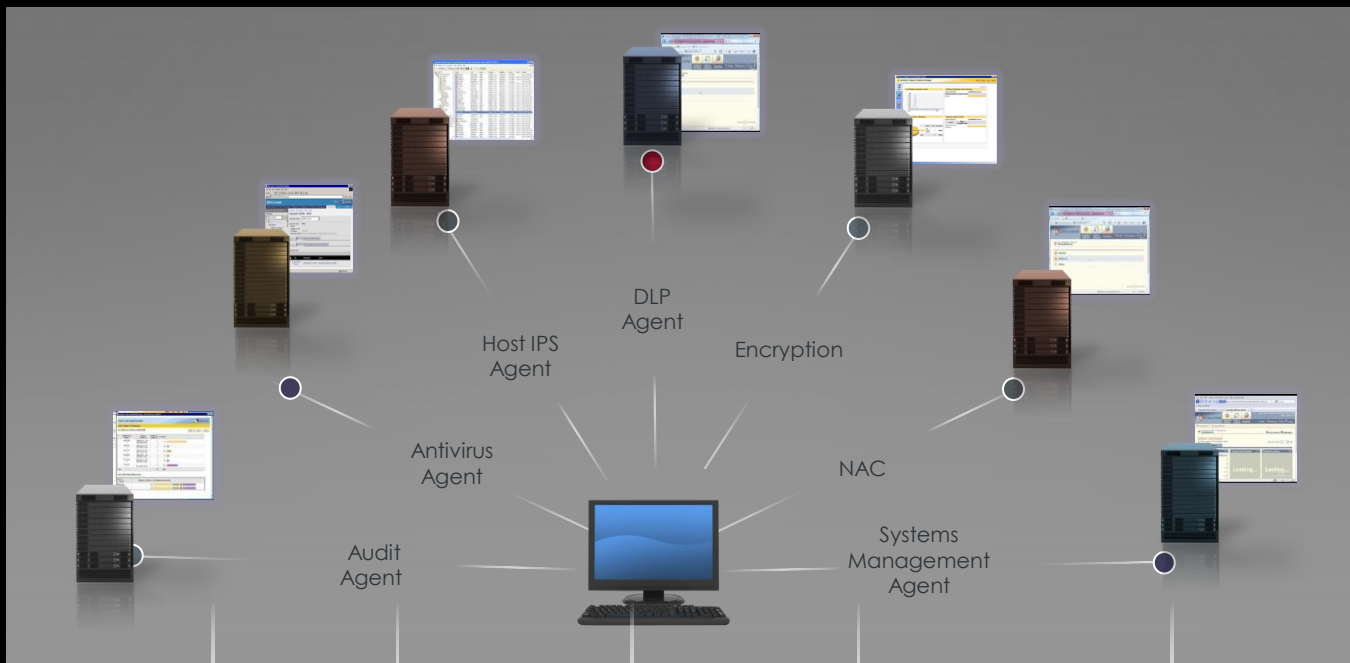
Category	Count
Potentially At Risk	1
Not At Risk	0
Total	1

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	

Насколько объединена ваша система безопасности?



КАЖДОЕ
РЕШЕНИЕ
ИМЕЕТ
СВОЮ
АГЕНТА

КАЖДЫЙ
АГЕНТ
ИМЕЕТ
СВОЮ
КОНСОЛЬ

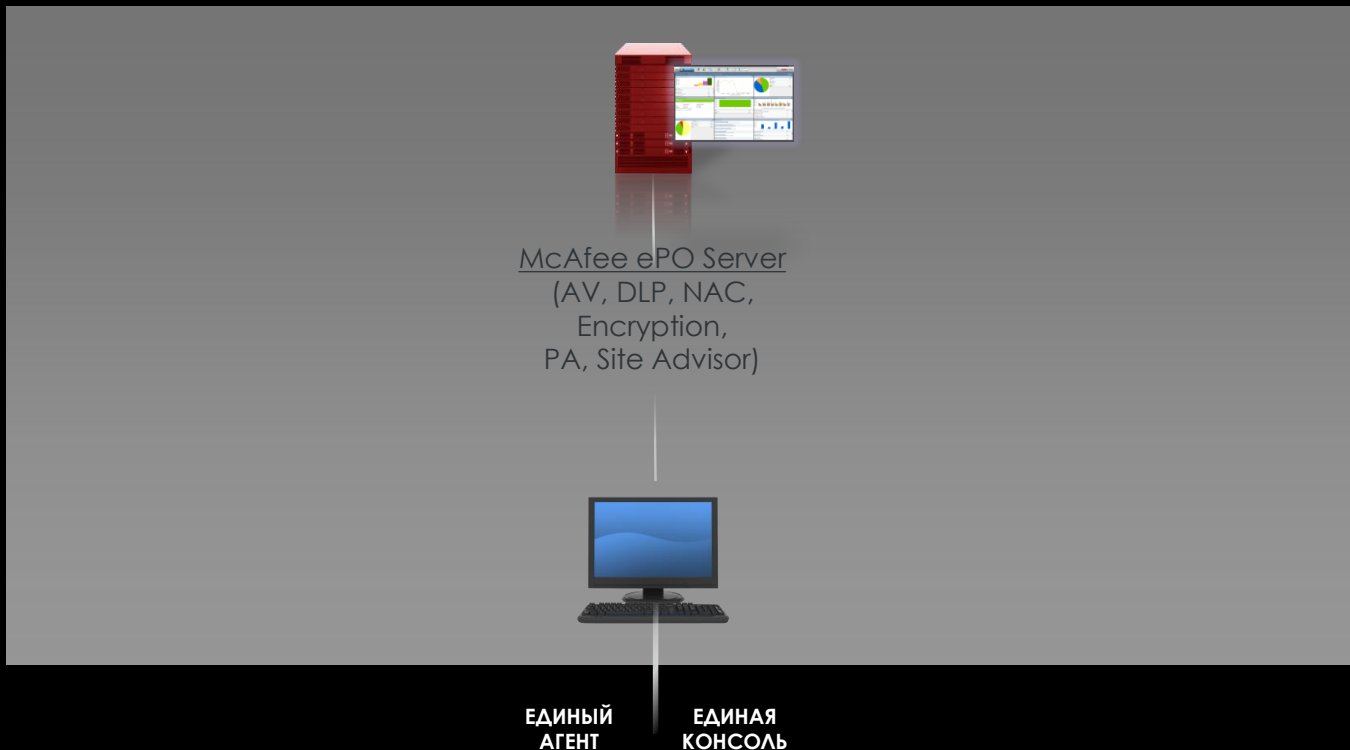
КАЖДАЯ **КОНСОЛЬ**
ТРЕБУЕТ
ОТДЕЛЬНОГО
СЕРВЕРА

КАЖДЫЙ **СЕРВЕР**
ТРЕБУЕТ ОС И
БАЗУ ДАННЫХ

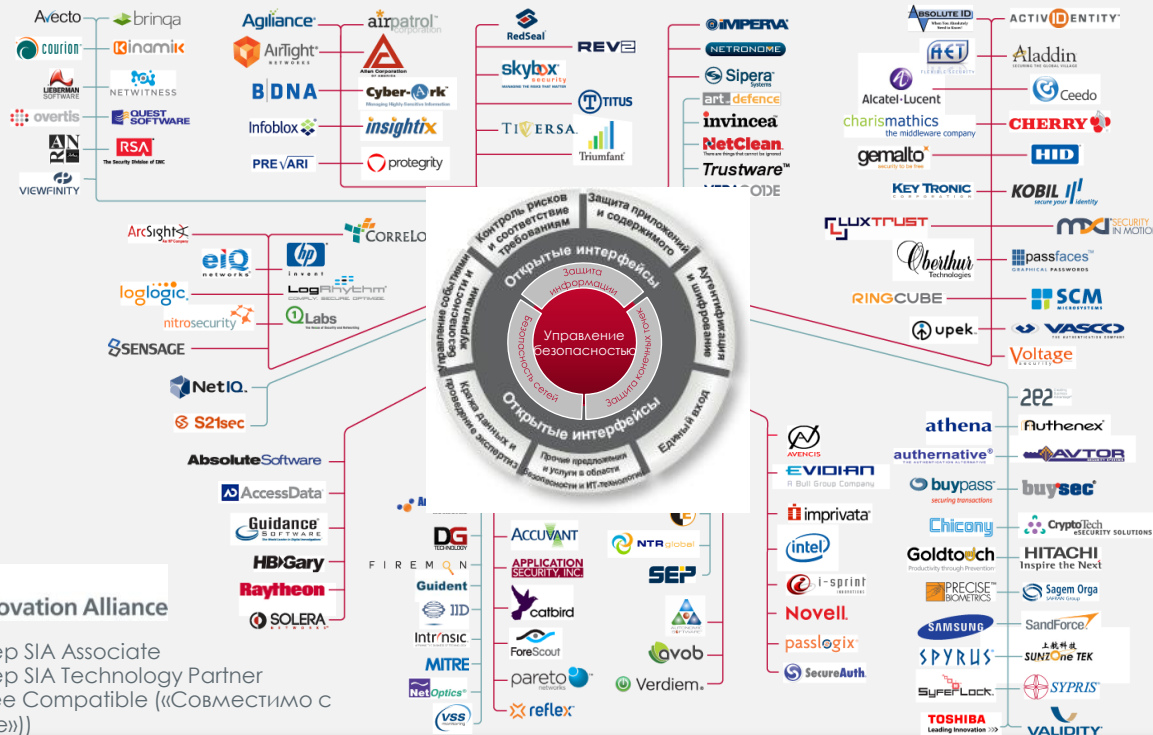
КАЖДАЯ **ОС И БАЗА**
ДАННЫХ ТРЕБУЕТ
ПОДДЕРЖКИ, ЛЮДЕЙ,
ПАТЧЕЙ

**ГДЕ ЖЕ
КОНЕЦ?**

Насколько объединена ваша система безопасности?



Security Connected: Интеграция сторонних продуктов



McAfee
Security Innovation Alliance

- Партнер SIA Associate
- Партнер SIA Technology Partner (McAfee Compatible («Совместимо с McAfee»))

