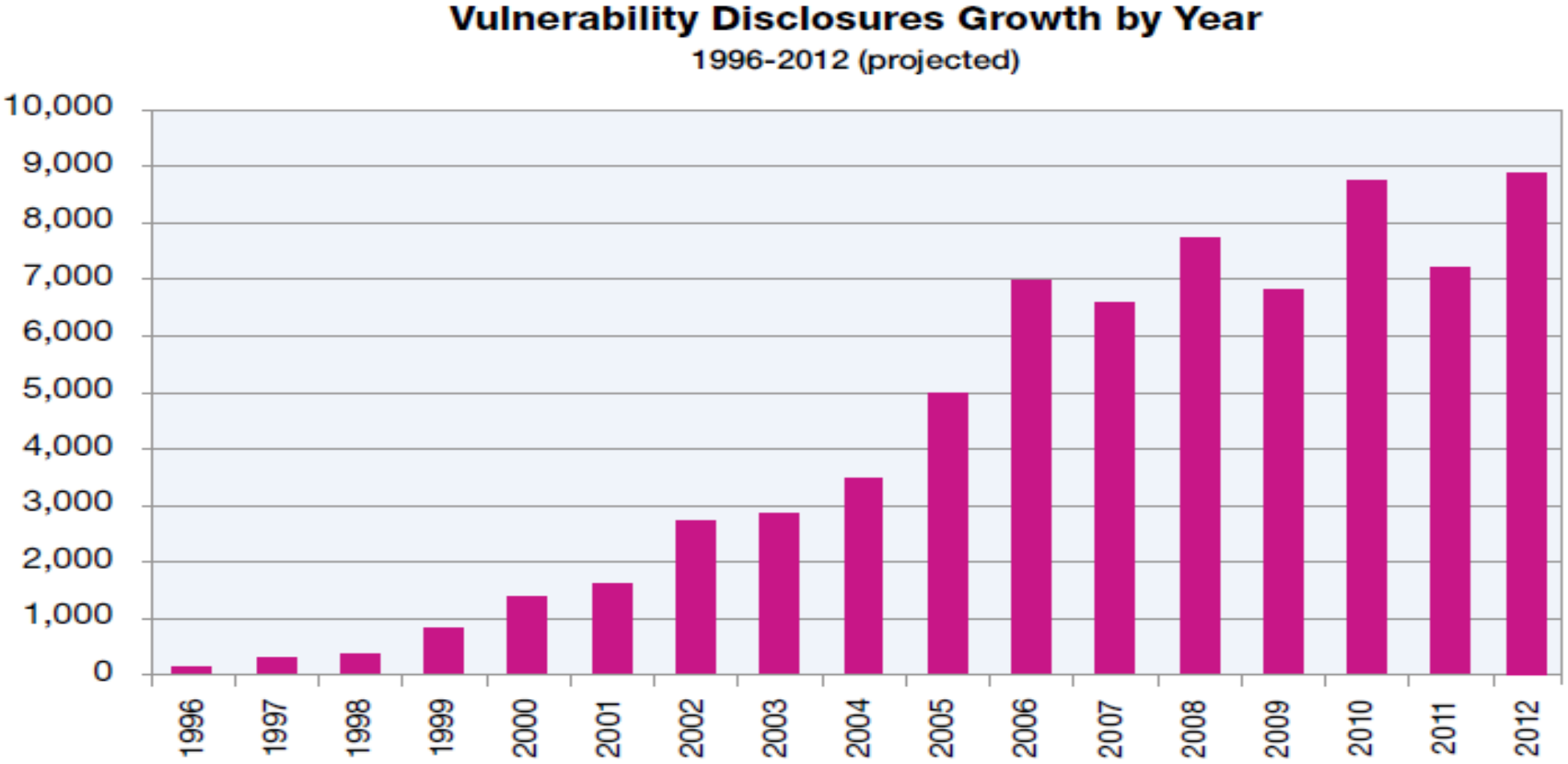
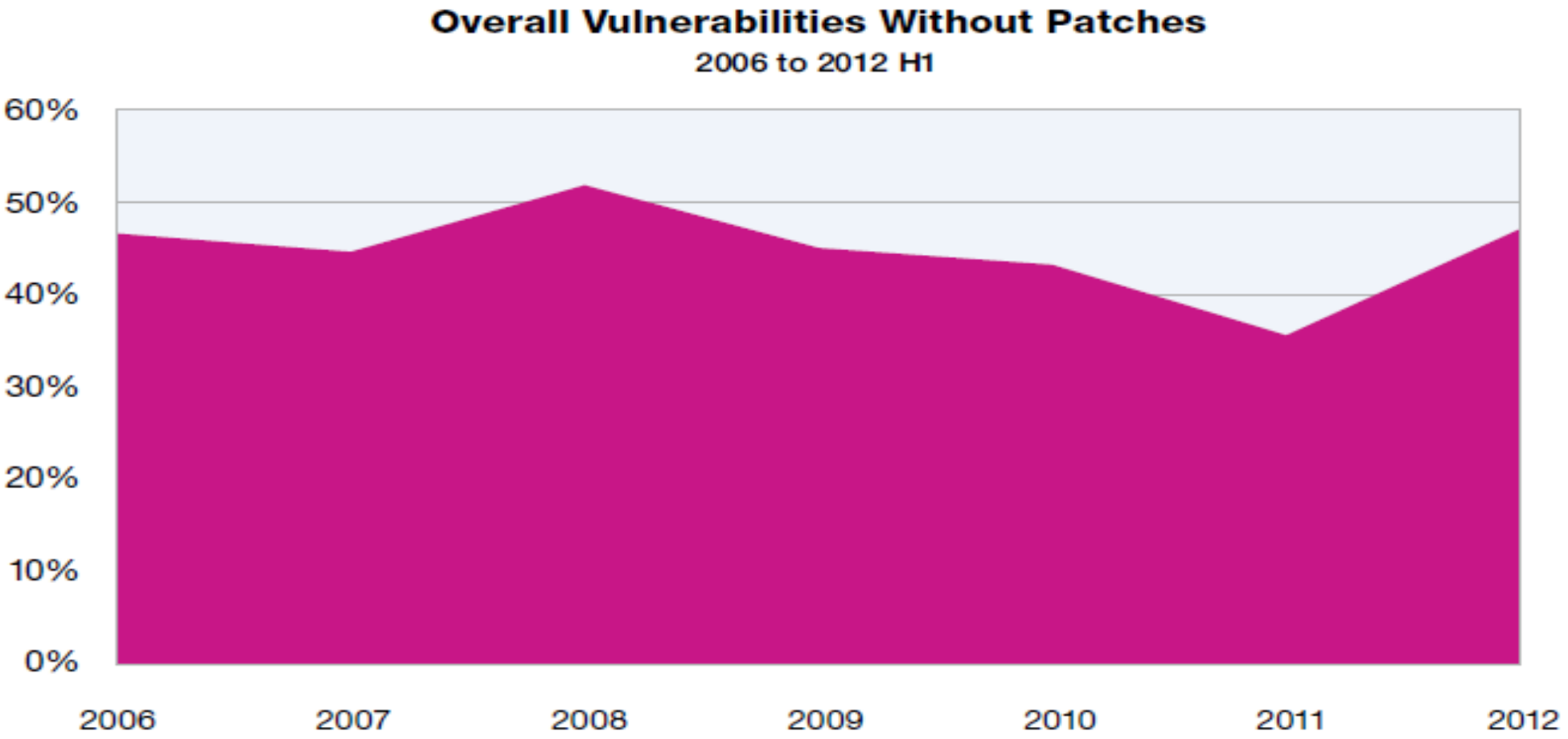
УРАЛЬСКИЙ ФОРУМ 2013

Решения Stonesoft по защите ДБО

Рост уязвимостей

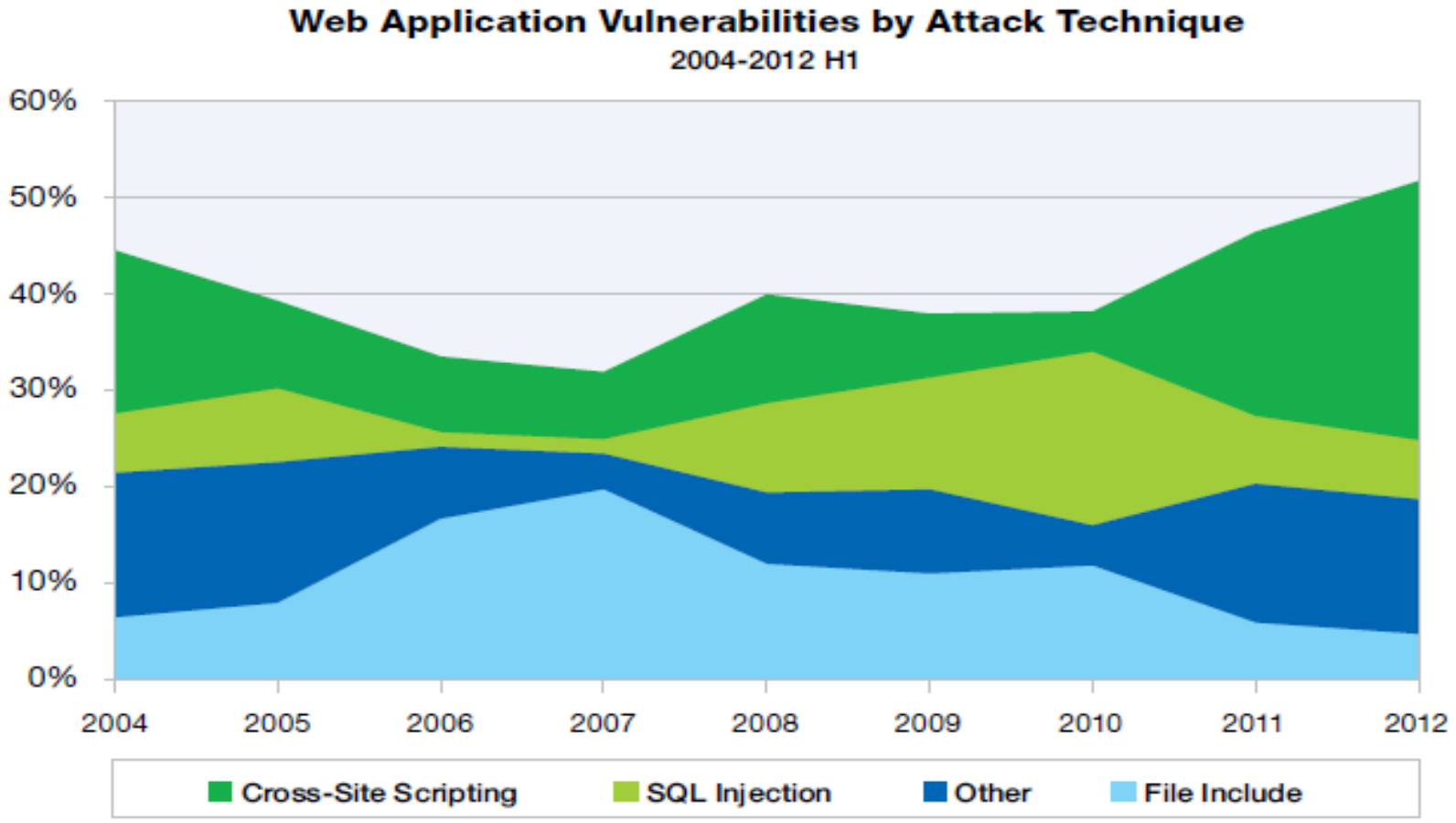


Общая ретроспектива уязвимостей без патчей !



- 2012-IBM X-Force 2012 Mid-Year Trend and Risk Report

Ретроспектива WEB уязвимостей



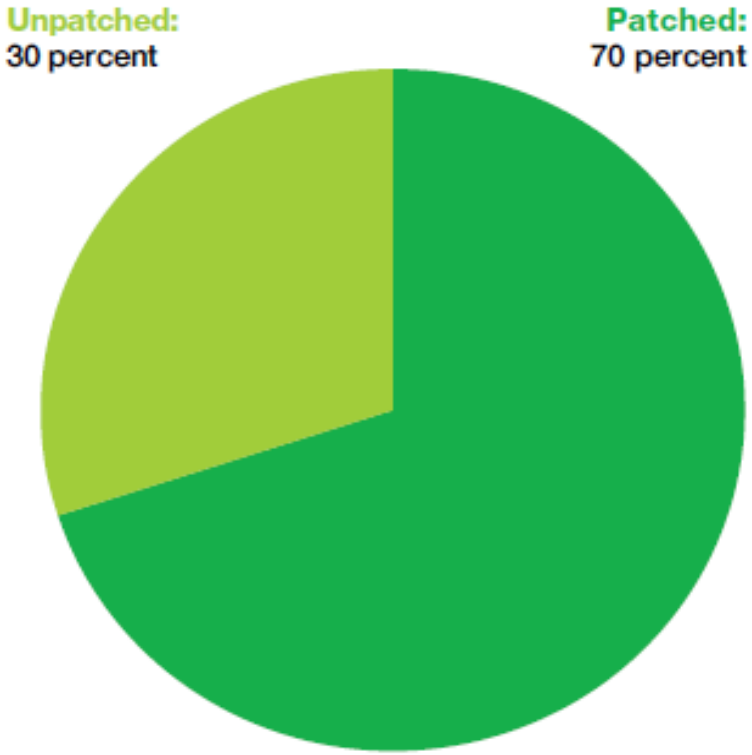
DBO работает на web технологиях….. ☺

2012-IBM X-Force 2012 Mid-Year Trend and Risk Report

Уязвимости web vs патчи

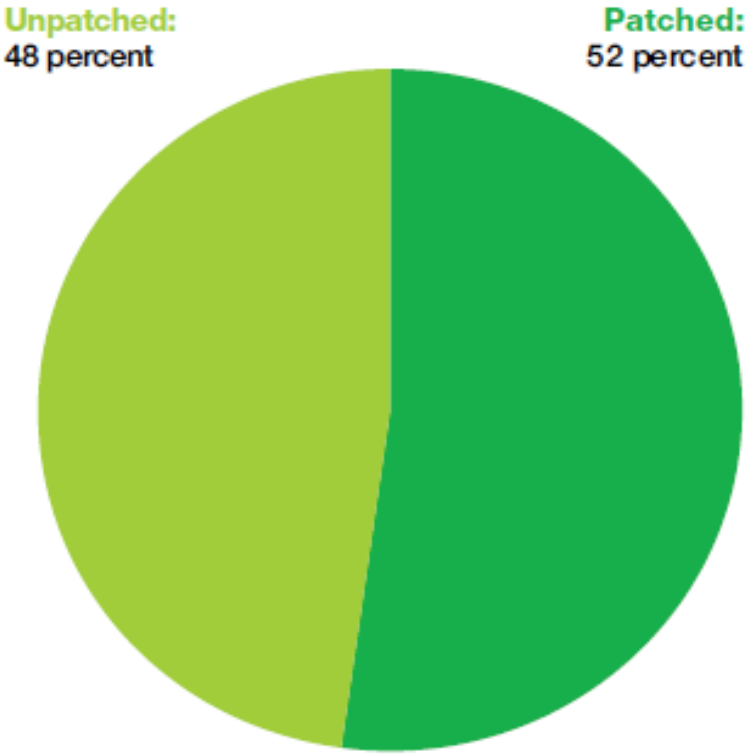
CMS Core Vulnerabilities

2012 H1



CMS Plug-in Vulnerabilities

2012 H1



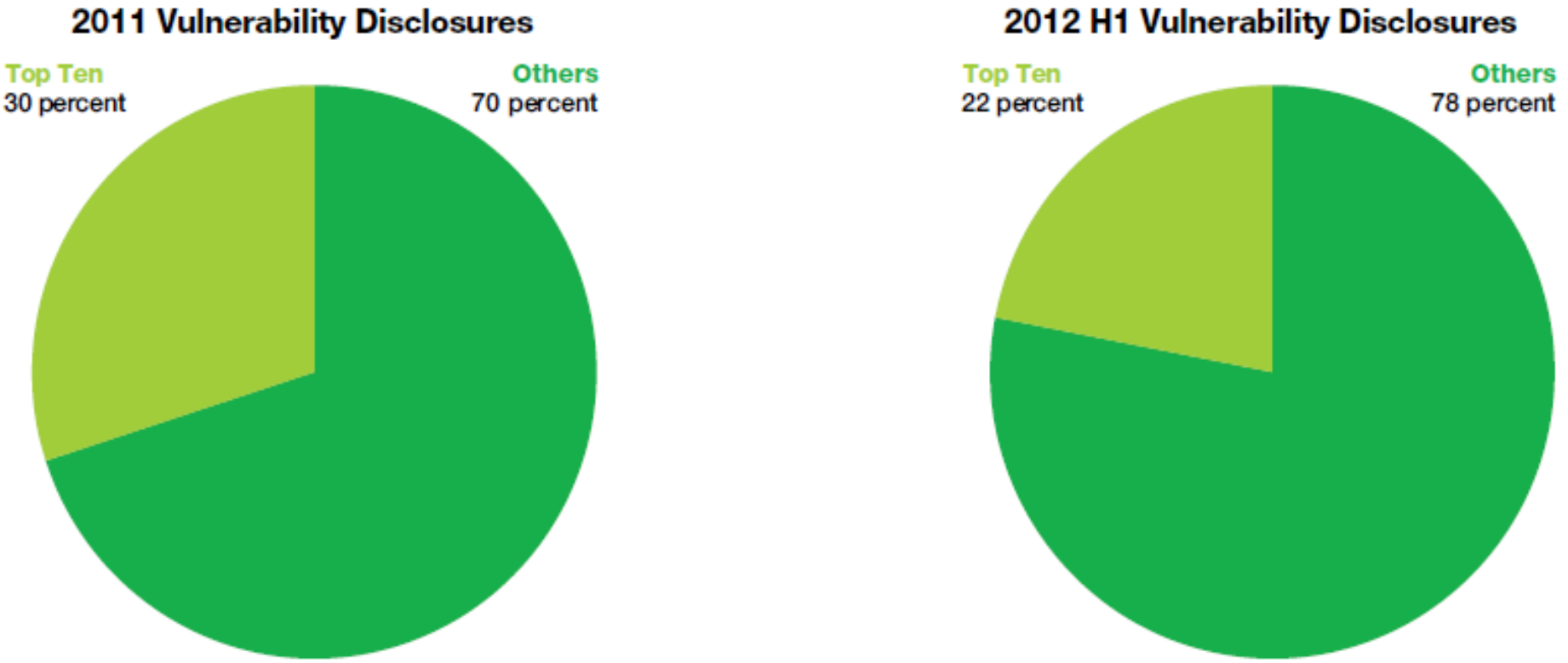
Соотношение уязвимостей с патчами или без ….

2012-IBM X-Force 2012 Mid-Year Trend and Risk Report

Топ 10 vs остальные

Top Ten Software Vendors with the Largest Number of Vulnerability Disclosures

2011-2012 H1

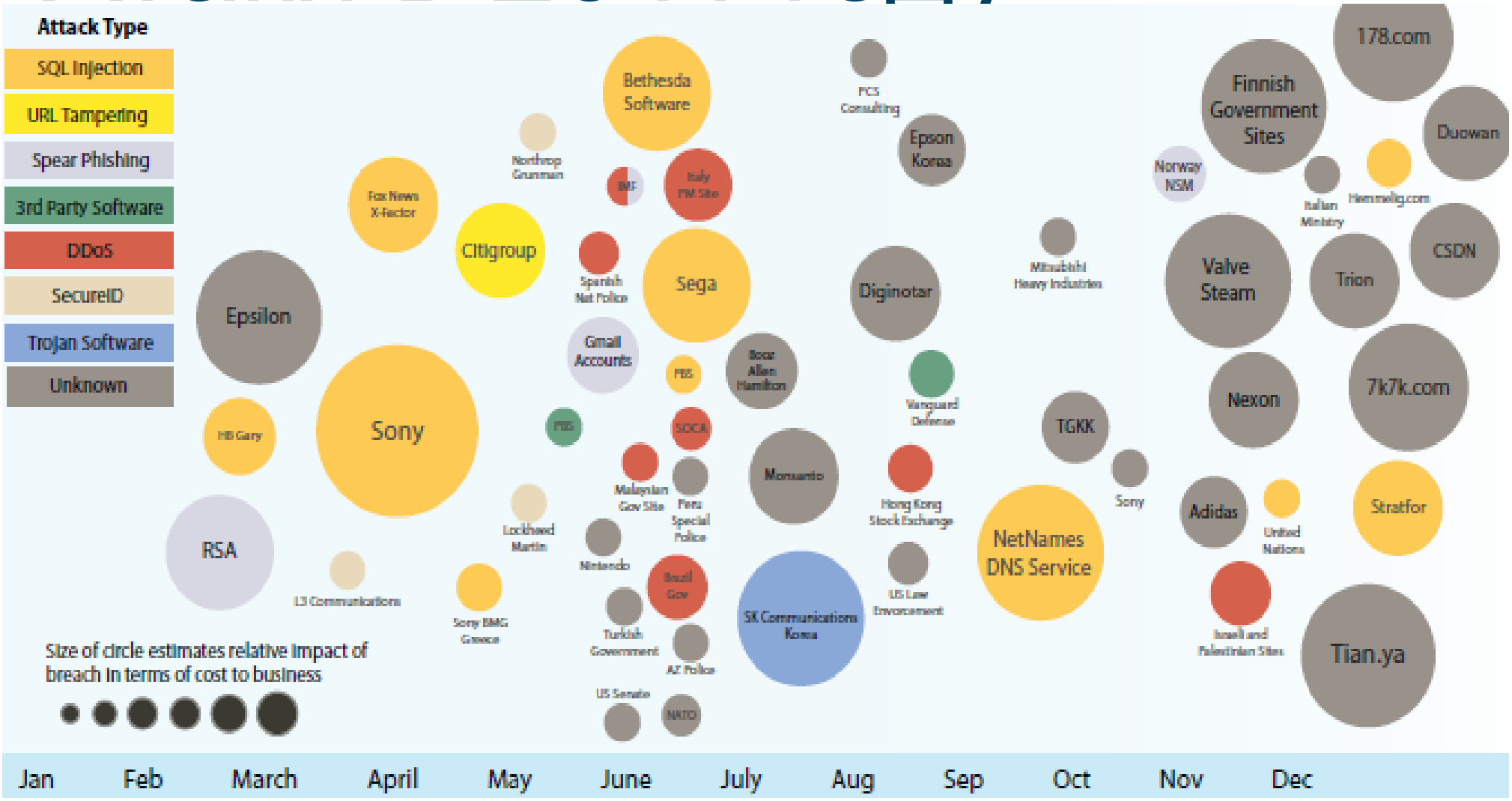


- Рапределение уязвимостей между вендорами

2011 временная шкала взломов

Атак больше на 45%
На 56% более дорогие

Атаки в 2011 году



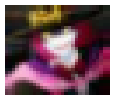
- IBM X-Force 2011 trend and risk report

2012 тренд продолжается

Date	Author	Target	Description	Attack	Target Category	Attack Category
Jul 15	?		The Consumerist representatives notify their readers that the site outages experienced in the previous days were caused by a security breach. They do not provide many details regarding the security issue, but as a precaution turn off commenting on all articles and plan to reset all user passwords.[1]	Unknown	E-Commerce	Cyber Crime
July 17	?		Security researchers from Kasperky Lab and Seculert announce to have discovered a new cyber-espionage campaign targeting victims in the Middle East: more than 800 victims located in Iran, Israel, Afghanistan and elsewhere over the last eight months.[2]	APT	Financial institutions, students, various government agencies	Cyber Espionage
July 17	?		MapleSoft, makers of mathematical and analytical software such as Maple, reports that they have been investigating a database breach.[3] The breach resulted in the attackers obtaining customer information such as email addresses, first and last names, as well as company and institution names. MapleSoft states that no financial information was compromised in this breach. Few days later MapleSoft customers begin to receive emails pretending to be from the "MapleSoft Security Update Team" that claimed Maple software was vulnerable to attack and a patch was available, redirecting them to websites hosting Blackhole Exploit Kit.[4]	Unknown	Industry: Software	Cyber Crime
July 17			NullCrew returns with another major data breach. Hackers claimed to have access to the database belong to the South Africa's Leading ISP Directory and Community Portal (ispdirectory.co.za)[5]	Unknown	Online Services	Cyber Crime
July 17			Anonymous' OpGodFather continues. This time, the hacktivists publish details from the Internet filtering systems instated by Yemen's government.[6]	Unknown	Government	Hacktivism

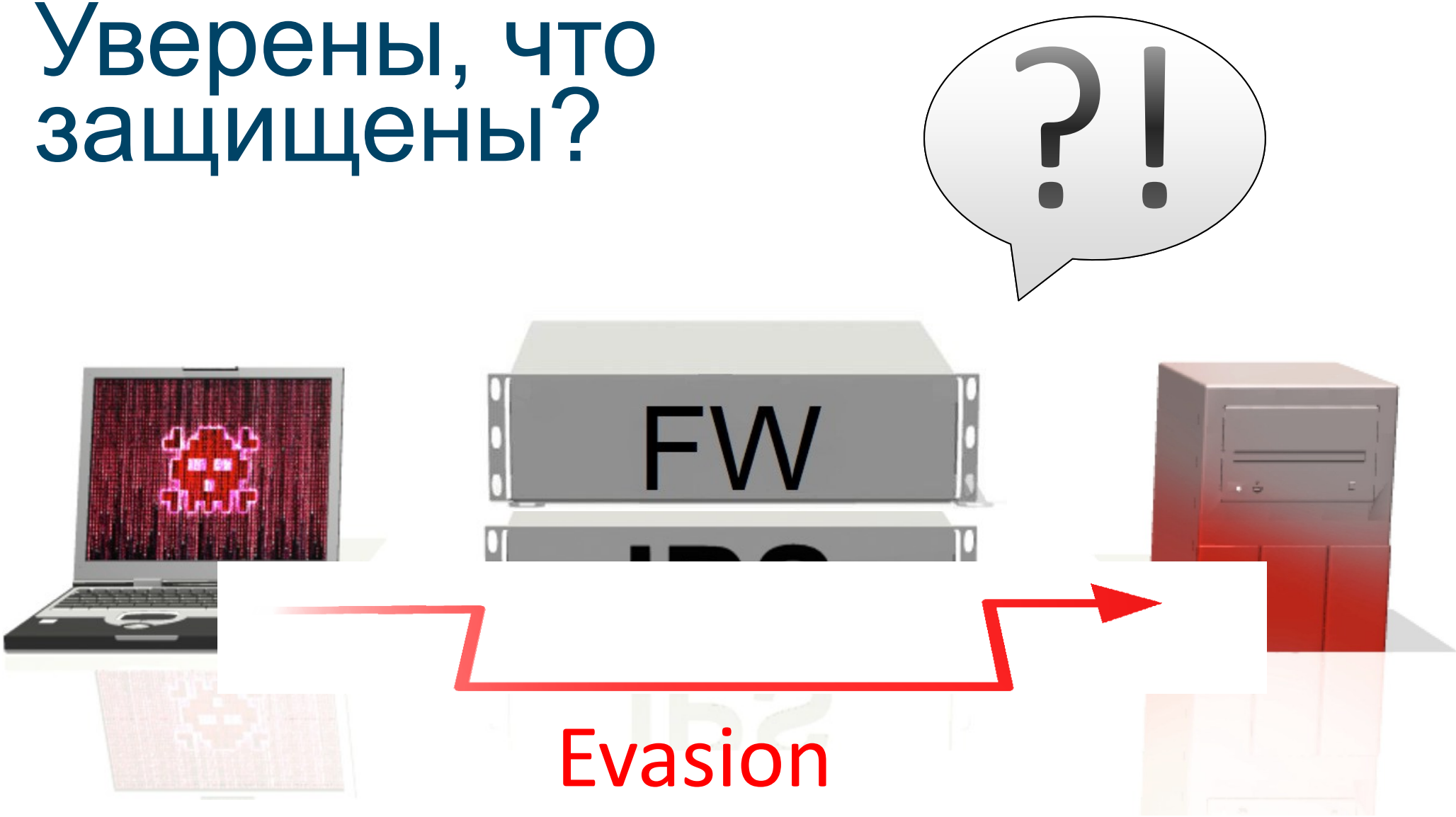
- **Количество неизвестных атак растет**

Чаще догадки как это было:

Jul 18	?	proserve	An unknown group of hackers breaches a server managed by Proserve, a Dutch hosting services provider. The databases of websites such as Q-Music, The Telegraaf, Stedin, and various online stores were accessed and the details of around 800,000 users were stolen as a result of the hack.[7]	[redacted]	Hosting	Cyber Crime
July 18	NullCrew	Yale University	NullCrew turn their attention to Yale University and obtain details of around 1,200 students and members of the staff from the databases of the educational institution and claim that the database they've gained access to contains even more sensitive information such as social security numbers, names, addresses and phone numbers, although they only published usernames, passwords and email addresses.[8]		Education	Cyber Crime
July 18		ITWallStreet	@MidasBank from @TeamGhostShell hacks ITWallStreet.com, an online job source, and dumps around 50,000 accounts.[9]		Industry: Recruiting	Cyber Crime
July 18	@SirLeakAlot	The Himalayan	A hacker called @SirLeakAlot hacks The Himalayan Times (thehimalayantimes.com) and dumps 23,453 accounts (plus 9 administrators) including username, phone number and clear text password.[10]		News	Cyber Crime
July 19		Dahabshiil	Anonymous declares what they call the "iWot", meaning "Internet War On Terror" and hacks Dahabshiil , an international funds transfer company dumping several accounts and threating to publish everything in two months if Dahabshill will not come completely clean on its terrorist activities.[11] However Dahabshill denies the Anonymous were responsible for the attack.[12]		SQLi?	Hacktivism

- Опять непонятно как было взломано ?

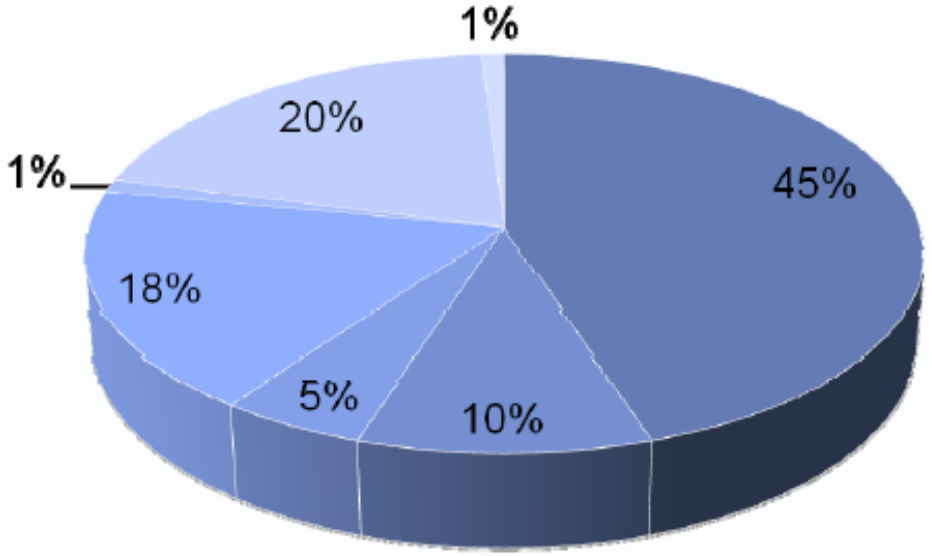
Уверены, что защищены?



Безопасность ДБО способов атак очень много

- Хакерские атаки на собственно систему ДБО (SQL injections..).
- Троянские программы - воровство паролей и криптографических ключей
- Трояны – перехват нажатий клавиатуры , снимки экрана при каждом нажатии, и др….
- Пресловутый универсальный троян Ibank
- Установка удаленного канала в рабочей станции
- Сбор данных в том числе остатки информации по работе с ДБО (кеш , куки, файлы в папках temp …..)
- Man in the middle (работа через посредника) , Man in the browser

Распространённость типичных угроз[1]

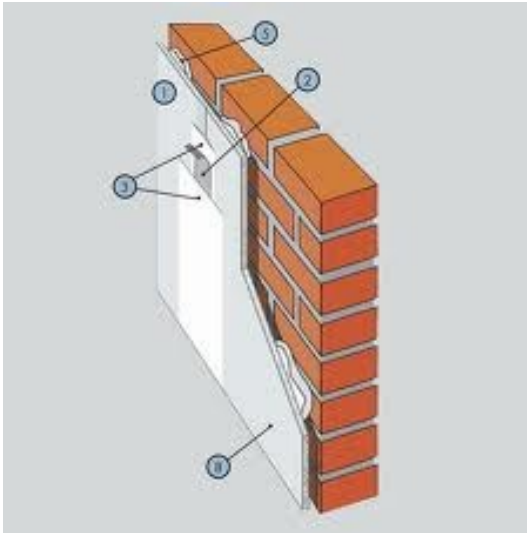


- Атака на ключевой контейнер - 45% (тенденция к снижению)
- Физическая кража носителя - 10%
- Атака на ключ в оперативной памяти - 5%
- Удаленное управление - 18% (тенденция к росту)
- Подмена документа - 1%
- Фишинг - 20%
- Атаки на канал - менее 1%

(1) На основании данных предоставленных производителями решений для ДБО и средств защиты

Требования регуляторов

- «Положение о методах и способах ЗИ в ИСПДн» (например):
  - Управление доступом:
    - Идентификация и аутентификация
  - Регистрация и учет;
  - Обеспечения целостности;
  - При работе через Интернет:
    - Безопасное межсетевое взаимодействие;
    - Анализ защищенности;
    - Обнаружение вторжений;
    - Защита каналов;
    - Надежная идентификацияи аутентификация;
    - Антивирусная защита (также при работе со съемными носителями);
    - Централизованное управление СЗИ.



Требования регуляторов

- При работе через Интернет:
  - Безопасное межсетевое взаимодействие;
  - Анализ защищенности;
  - Обнаружение вторжений;
  - Защита каналов;
  - Надежная идентификация аутентификация;
  - Антивирусная защита (также при работе со съемными носителями);
  - Централизованное управление СЗИ.

Применение сертифицированных средств

Защита ДБО - проблема комплексная

Главное это комплексная система безопасности:

- Своевременный патчинг;
- Система анализа транзакций, подозрительной активности (antifraud);
- Анализ клиентов; безопасность клиентской части….
- Своевременное тестирование средств безопасности;
- защита от современных атак ;
- Процедуры реагирования на инциденты – как работают департаменты между собой ?
- Интеграция систем. Есть общий «взгляд» на безопасность ?

Остановимся на сетевой составляющей безопасности

КАК СОВМЕСТИТЬ БЕЗОПАСНОСТЬ И ЭФФЕКТИВНОСТЬ

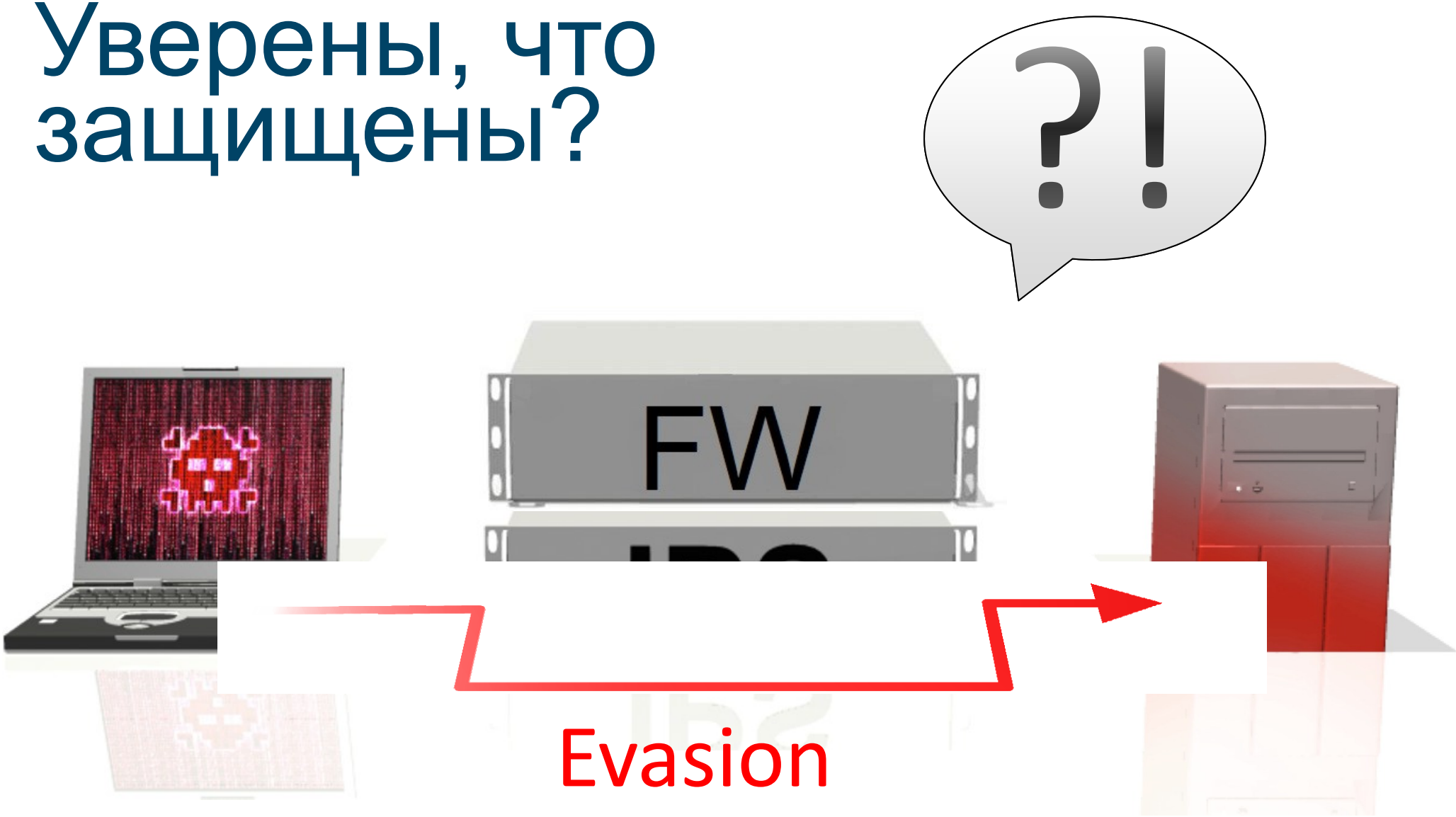
Комплексная сетевая защита мобильного банкинга

- Защита собственно ресурса мобильного банкинга от новейших атак
- Строгая, двухфакторная аутентификация и авторизация
- Контроль удаленного устройства при подключении (безопасно оно или нет ?)
- Шифрование передаваемой информации (сертифицированные средства?)
- Исключение возможности «захвата» удаленного устройства в момент доступа.
- Удаление следов сеанса работы на удаленном устройстве (чтобы исключить воровство данных)
- Динамическая блокировка устройства в случае несанкционированной активности во время сеанса …

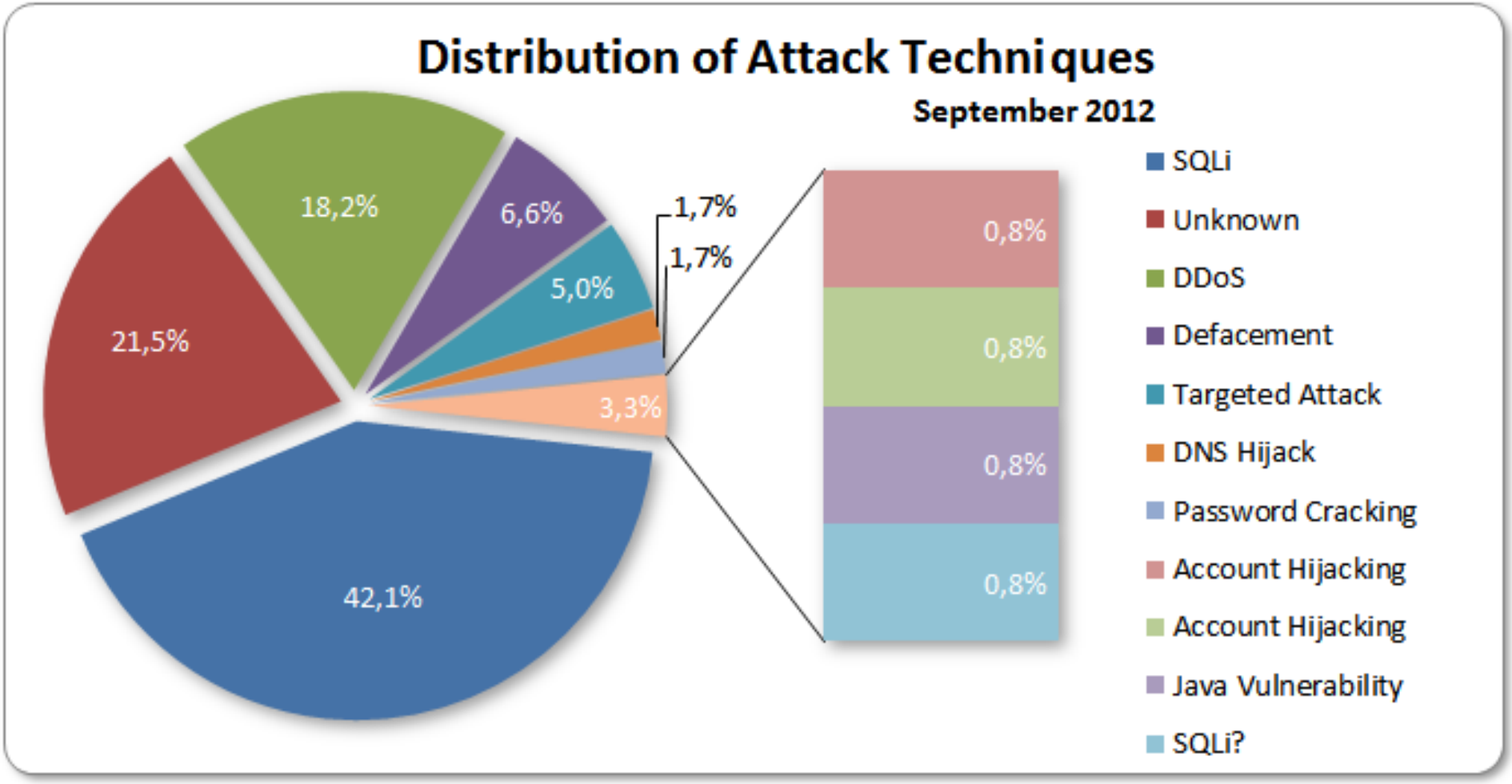
Комплексное решение

- StoneGate IPS (EPS) - полноценная Защита от атак, SQL injections, AET
- Stonesoft Authentication Server - двухфакторная аутентификация и авторизация, управление доступом
- StoneGate SSL VPN - полноценная защита удаленных соединений, анализ удаленного устройства, удаление чувствительной информации
- StoneGate SMC - централизованное управление устройствами, управление событиями безопасности, работа с инцидентами

Уверены, что защищены?



Вернемся к статистике 2012



- www.hackmageddon.com

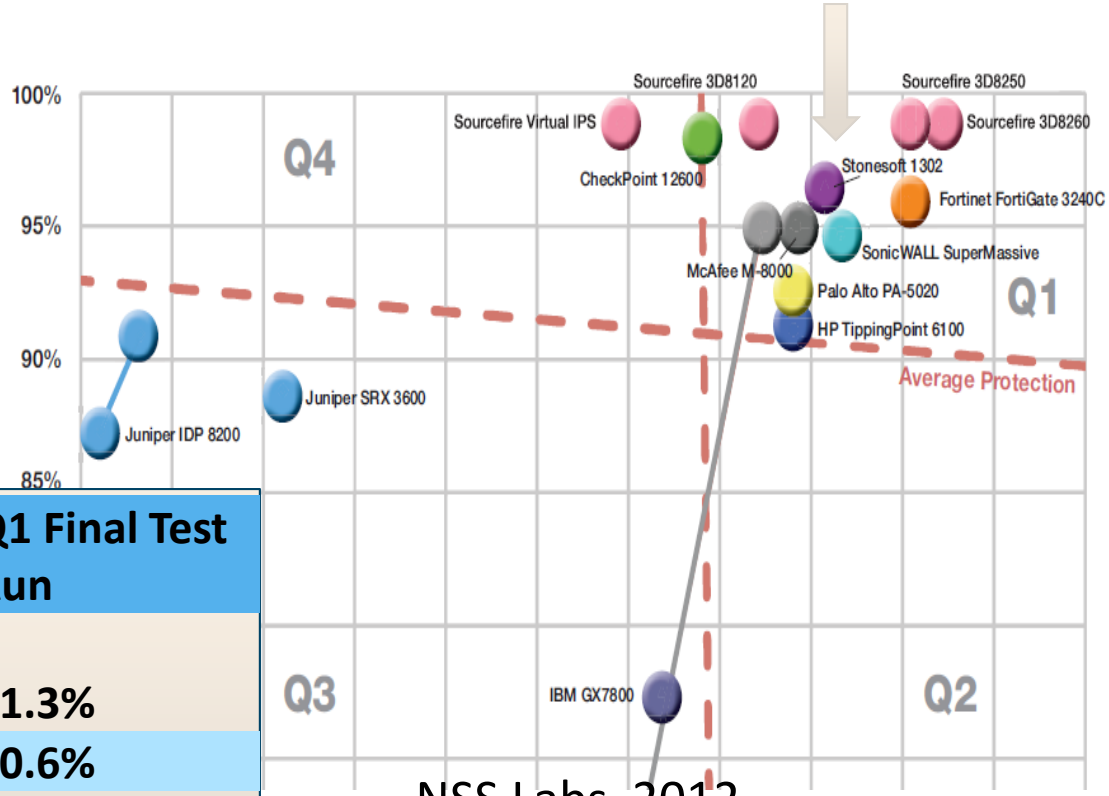
Официальные ответы вендоров на AET

AET vulnerabilities reported through global CERT vulnerability coordination process to all vendors
1.Sample set of 24 AETs in June 2010
2.Sample set of 124 AETs in February 2011
3.Sample set of 180 AETs in March 2011

Vendor	Vendor Comments (source: http://www.cert.fi/en/reports/2010/vulnerability385726.html) 01 March 2012
Checkpoint	Checkpoint has released an advisory. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_dogoviewsolutiondetails=&solutionid=sk59468
Palo Alto NW	No comments about remediation
Juniper	No comments about remediation
McAfee	No comments about remediation
Fortinet	No comments about remediation
Cisco	Cisco PSIRT is aware of the issues reported by StoneSoft and is actively investigating what impact these vulnerabilities may have on Cisco products. PSIRT will disclose any security vulnerabilities discovered in compliance with Cisco's security vulnerability policy: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
HP/ Tipping Point	HP DVLabs has tested the evasion techniques against the TippingPoint IPS and found that all of the evasion techniques were NOT successful. TippingPoint customers are not impacted and no further updates are necessary. Customers may contact the TAC for more information.
Top Player	Top Layer Security has evaluated the IPS 5500 E-Series against these evasion techniques, and verified that they are not successful in bypassing IPS protection. Please visit www.toplayer.com for more details.
Sourcefire	No comments about remediation
Trend Micro	Trend Micro has been following this issue closely and has created updates related to these evasion techniques. Trend Micro recommends that customers upgrade to the latest software versions to ensure they have the most current protection. Any further updates needed will be released in compliance with the relevant security vulnerability policy.

StoneGate IPS

Современное средство защиты
от самых современных атак



NSS Labs 2012

Developer	Product	Q1 Initial Test Run	Q1 Final Test Run
Fortinet	FortiGate-310B	65.6%	81.3%
Sourcefire	3D4500*	59.4%	90.6%
Stonesoft	IPS-1205	78.1%	90.6%
TippingPoint	660N**	71.9%	84.4%
TippingPoint	TP330**	71.9%	84.4%

Единственное решение обеспечивающее полноценную защиту от АЕТ

https://www.icsalabs.com/technology-program/quarterly-network-ips-vulnerability-testing

StoneGate SSL VPN

- Безопасный доступ с любых устройств
  - Встроенная двух факторная аутентификация
  - Интеграция с любыми каталогами и др. (AD, LDAP, Oracle)
  - Поддержка single sign-on & ID federation
- Интегрированное управление угрозами
  - Только доверенные соединения .
  - Анализ целостности и безопасности устройства
  - Удаление «следов» работы пользователя.
- Гранулированное и гибкое управление доступом
  - Авторизация на уровне приложений
  - Концепция least privileges – только то что разрешено

Создан для людей

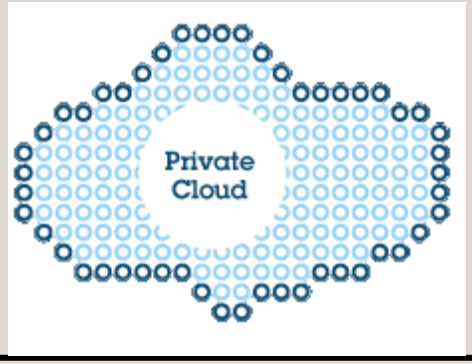
- Стратегия управления доступом, основанная на поведении > удобство использования гарантировано технологией
- Гибкие критерии доступа > вы сами выбираете условия в каждой ситуации
- Динамическая безопасность > вы сами контролируете приложения, в зависимости от заданных критериев

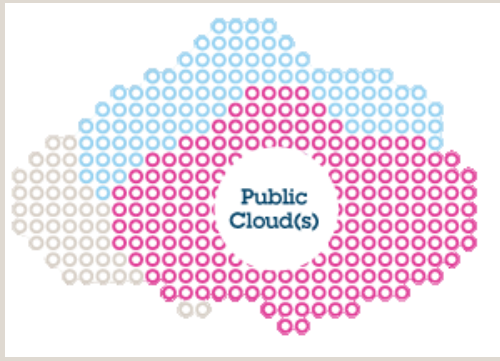
Универстальный удаленный доступ – почему?

- Любое устройство отовсюду и в любое время – дает свободу

- Не нужно привыкать к новому ПО – дает простоту

- Single Sign On для приложений и ресурсов – повышает производительность труда

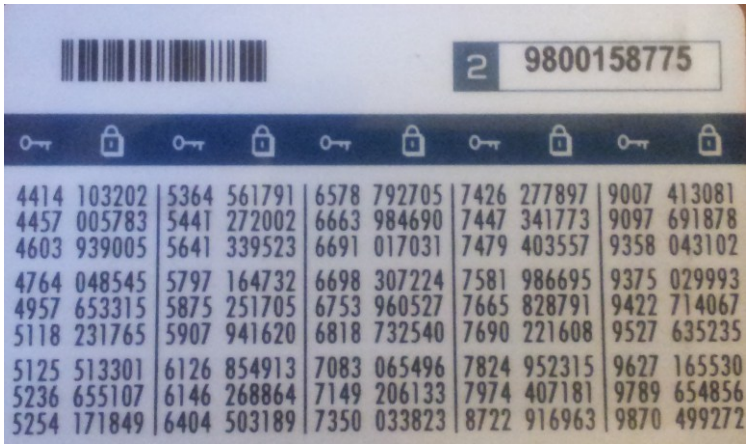




Соответствие политикам ИБ?

- Оценка всего профиля,а не только проверка прав!
- Доверие всей ситуации, а не только пользователю!
- Комплексный подход

Аутентификация можно упорядочить ?



Надежная аутентификация через SSL

- 6 включенных методов
- Подержка до 15 внешних методов
- Возможность комбинирования методов аутентификации

Интеграция сервисов аутентификации

Static Password

MobileID Sync

MobileID Challenge

Mobile Text

SMS

Federated ID SAML, ADFS

AS

XPI:WS API

RADIUS CLIENTS

Авторизация

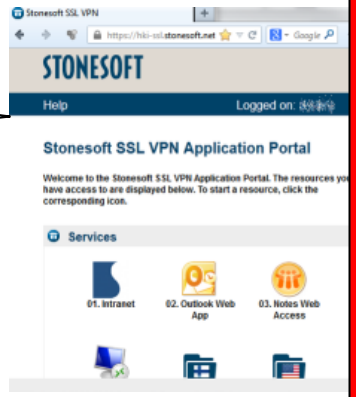
- Гибкая стратегия авторизация с множественными критериями
- Условный доступ
- Повторное сканирование
- Удаление следов
- Выделенная защита/изоляция для приложений

Полная… изоляция

Рабочее место клиента

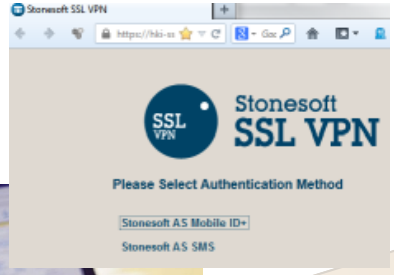
2. Авторизация с автоматическим пе

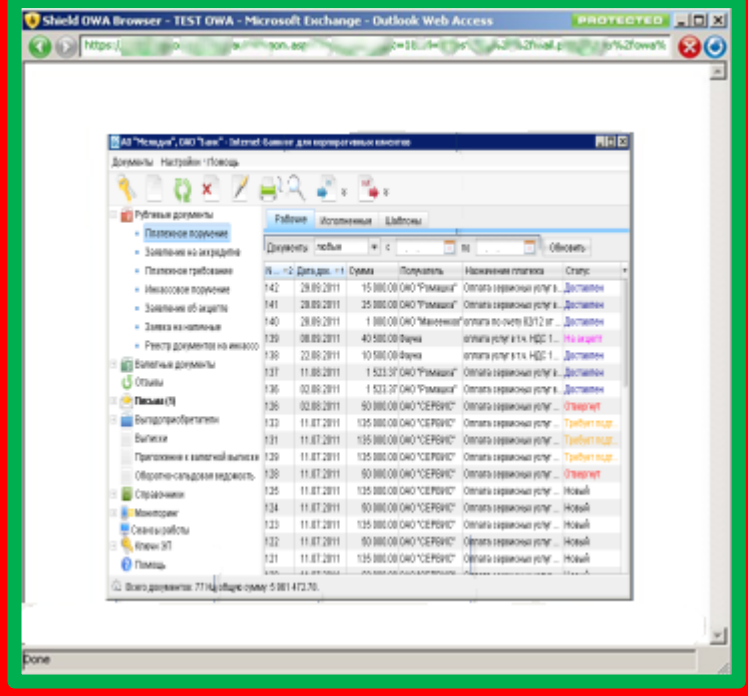
Аутентификация и авторизация на вход в банк (оформление меняется под Заказчика)



Пользователь «как обычно» работает с сайтом.

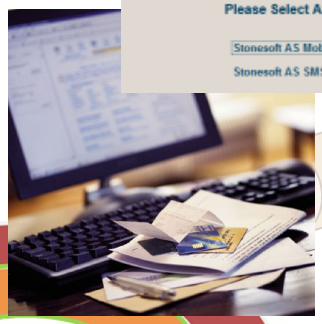
1. Доступ на сайт (через SSL)

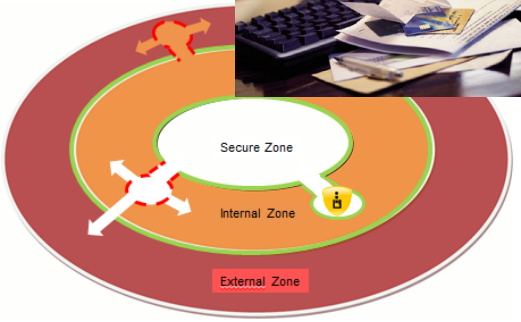




Загр… модуля безопасности

банк





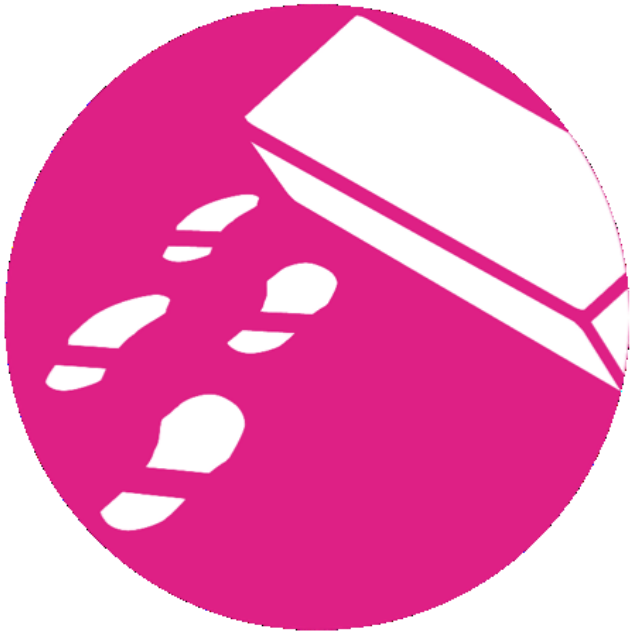
4. Загрузка защищенного приложения/браузера

STONESOFT

- Обеспечивается изоляция приложения и высокий уровень безопасности

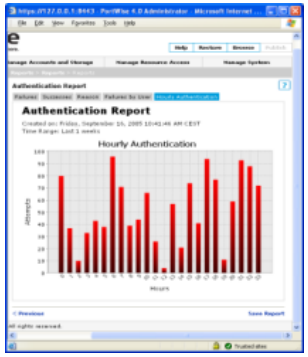
Удаление следов доступа

- Удаляет историю страниц браузера
- Прозрачный (автоматический) режим или интерактивный
- Удаляет временные (temporary) файлы
- Полностью настраиваются

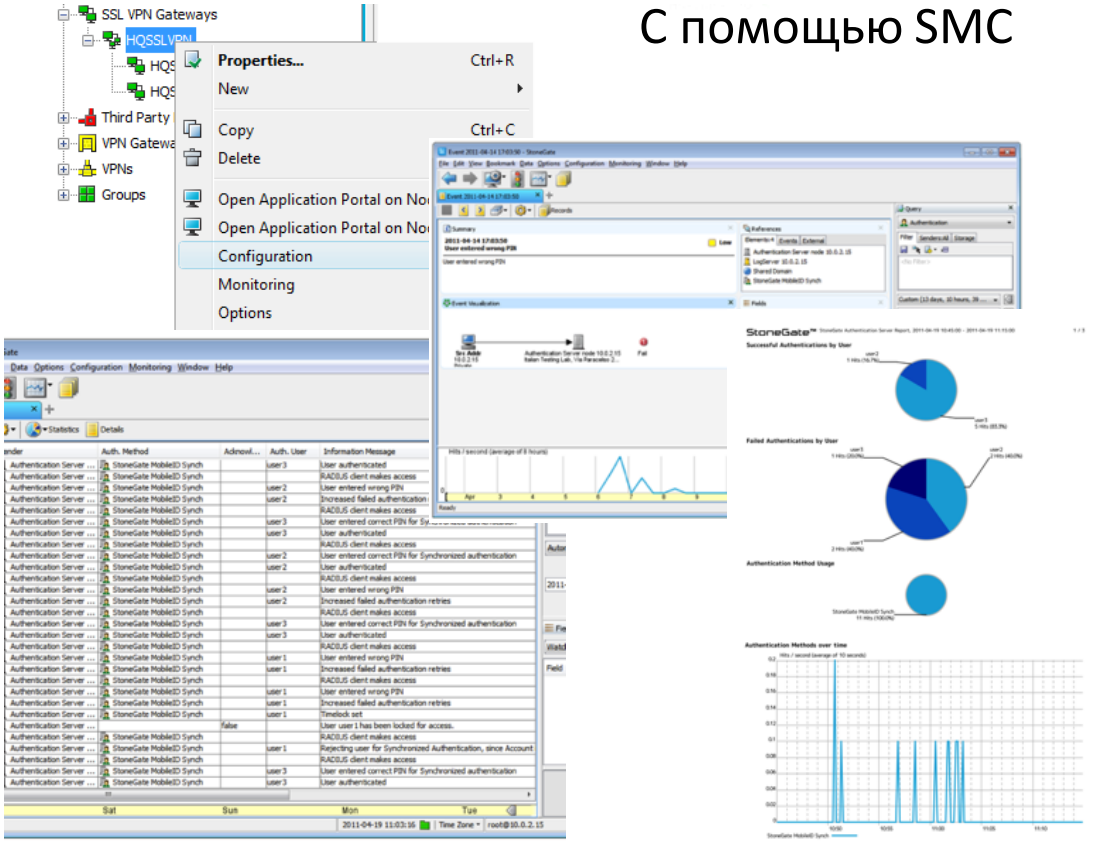


Управление журналами, отчеты, оповещения и аудит

На устройстве



С помощью SMC



STONESOFT


«Приятные
мелочи»

Технологическое партнерство

Security collaboration

Solution partners

ПРОВЕРЕННЫЕ РЕШЕНИЯ...

Сертификации

Gartner Magic Quadrant

VPNC CERTIFIED: Basic Conformance; Rekey Conformance; Certificates Conformance; Basic Interop; AES Interop

FIPS VALIDATED 140-2

RSA SECURED

vmware READY

ICSA labs CERTIFIED NETWORK IPS

ICSA labs CERTIFIED FIREWALL - CORPORATE

NSS Labs Security. Certified.

Common Criteria

ФСТЭК

ФСБ

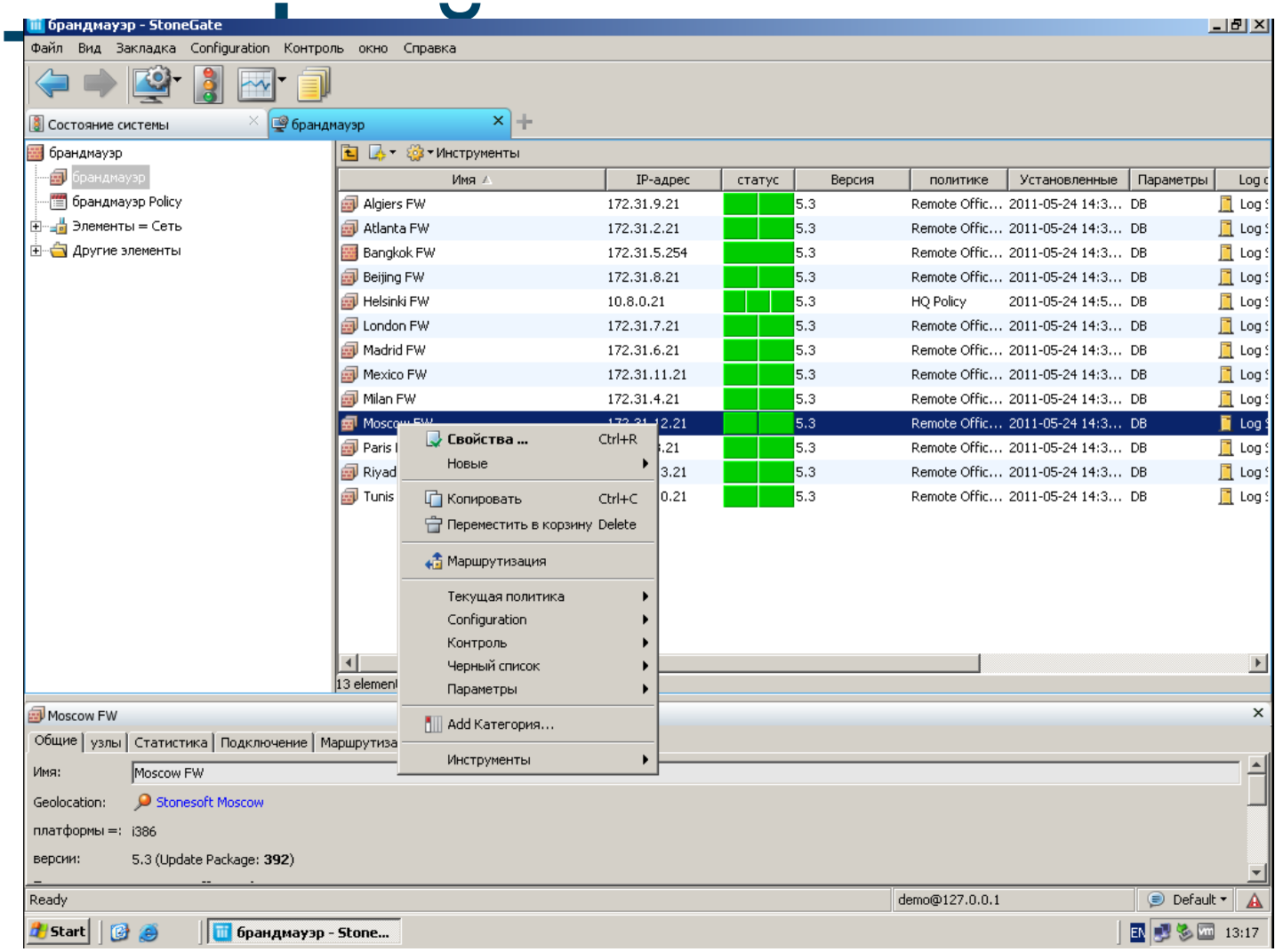
Подтверждение эффективности решений StoneSoft

Æ Protected against Advanced Evasion Techniques? Æntievasion

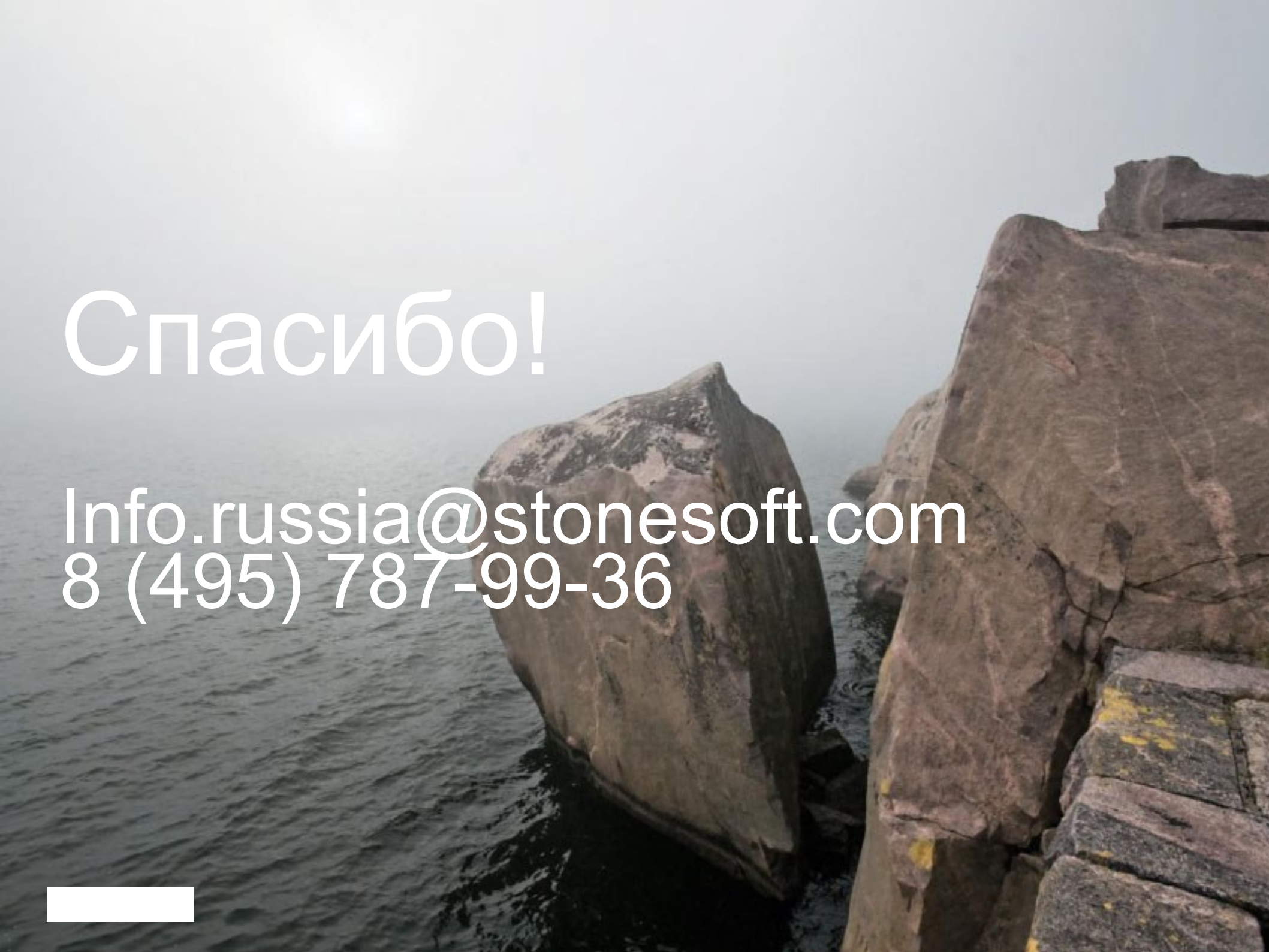
Сертификация ФСТЭК и ФСБ

- SSL VPN сертифицирован ФСТЭК России:
- Шлюз защиты удаленного доступа StoneGate SSL* – 3 класс МЭ (распределенный), 4 класс НДВ и для применения ИСПДн 1 класса и АС до 1Г вкл.
  - В составе сертифицирована система многофакторной аутентификации
- и ФСБ России:
  - Классы КС1 – КС2!
  - Поддерживаются криптопровайдеры (прописаны в сертификатах): Криптопро, Валидата ;
  - Встречная работа VipNet CSP, Signal Com

Локализованный инт



STONESOFT


Спасибо!
Info.russia@stonesoft.com
8 (495) 787-99-36