WatchGuard Security Solutions

Sergei Suhharnikov
for Adventus Solutions seminars
Vilnius 24.09.13, Riga 25.09.13

THE SMART FIREWALL

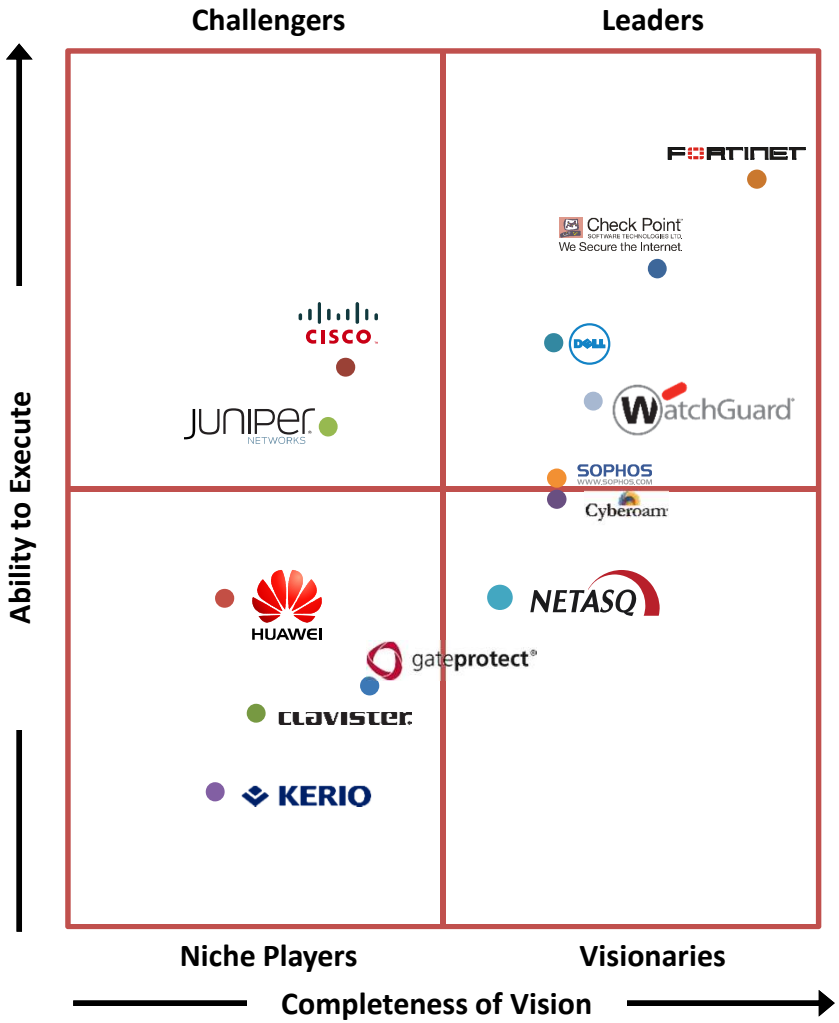
WatchGuard

> Дата основания – 1996 год, США
> Firewall appliance pioneer
> HQ in Seattle, WA
> Продано более **1,000,000** устройств
> **100%** канал – **5,000** партнёров в **120** странах
> Решения по безопастности для всех сегментов рынка

Accolades

2006	2007-2009	2010	2011	2012
Taken private in October	Re-Engineering of Product	Launched re-architected product with Best-of-Breed HW Best-of-Breed SW	Launched RED / Next Gen Firewall	XTMv and XCSv Hardware Refresh

Leader in Gartner UTM **Magic Quadrant** for 3rd Year Running



Source: Gartner Magic Quadrant for Unified Threat Management, July, 2013

"Баланс между простотой использования и высоким уровнем безопасности"

"Последние аппаратные и программные обновления принесли значительные улучшения производительности"

"Высокая скорость использования нескольких функций (за пределами брандмауэра, IPS и блокирование URL) всех производителей"

"Высокой надежности оборудования и профессиональнпя поддержку со WatchGuard"

Source: Gartner, March 2012 and June, 2013

Линейка продуктов

Extensible Threat Management (**XTM**)

Extensible Threat Management сочетает в себе межсетевой экран, VPN, службы безопасности для защиты сетей от спама, вирусов, вредоносных программ и вторжений.

XTM 2 & 3 Series:
For small offices, branch offices and wireless hotspots

XTM 5 & 800 Series:
For mid-sized businesses and distributed enterprises

XTM 15 Series: Large distributed enterprises

XTM 2520: Large enterprises and corporate data centers

XTMv
Four full product virtual software license versions

Extensible Content Security (**XCS**)

Extensible Content Security предлагает защиту контента через электронную почту и веб-фильтр в сочетании с защитой от потерей данных.

XCS 280, 580
For small businesses and medium-sized businesses

XCS 770R, 880 & 1180
For medium to large enterprises and ISP's

XCSv
Four full product virtual software license versions

Wireless Access Points

AP100 & AP200
Businesses can harness the power of mobile devices without putting network assets at risk.

Серия XTM – eXtensible Threat Management

- Sized for small business & branch offices (5-50 users) to enterprise (10 000+ users)
- 3 вида консоли управления: web, UI, CLI
- Мониторинг и репортинг realtime и no extra cost
- Возможность обновления внутри модельного ряда
- All-in-One network security:
  - Firewall
  - SSL & IPSec VPN
  - Reputation Enable Defense
    - Web reputation service from the cloud
  - WebBlocker (inc. Full HTTPS inspection)
  - spamBlocker
  - Gateway Anti-Virus
  - Intrusion Prevention Service
  - Application Control (from January 2011Y)
  - LiveSecurity Service (HW warranty, technical support, SW upgrades, Security Alerts, 24/7 Support)

In-House vs. **Best-of-Breed Technology**

	Anti Virus	URL Filtering	Anti Spam	IPS	APP Control	DLP
WatchGuard XTM	AVG Anti-Virus, Kaspersky Anti-Virus	websense	commtouch	Broadweb	Broadweb	SOPHOS
Dell SonicWALL						
Fortinet						
paloalto Networks		BrightCloud				
Cisco	Trend Micro	Trend Micro	Trend Micro			
Juniper Networks	Kaspersky Anti-Virus	websense				

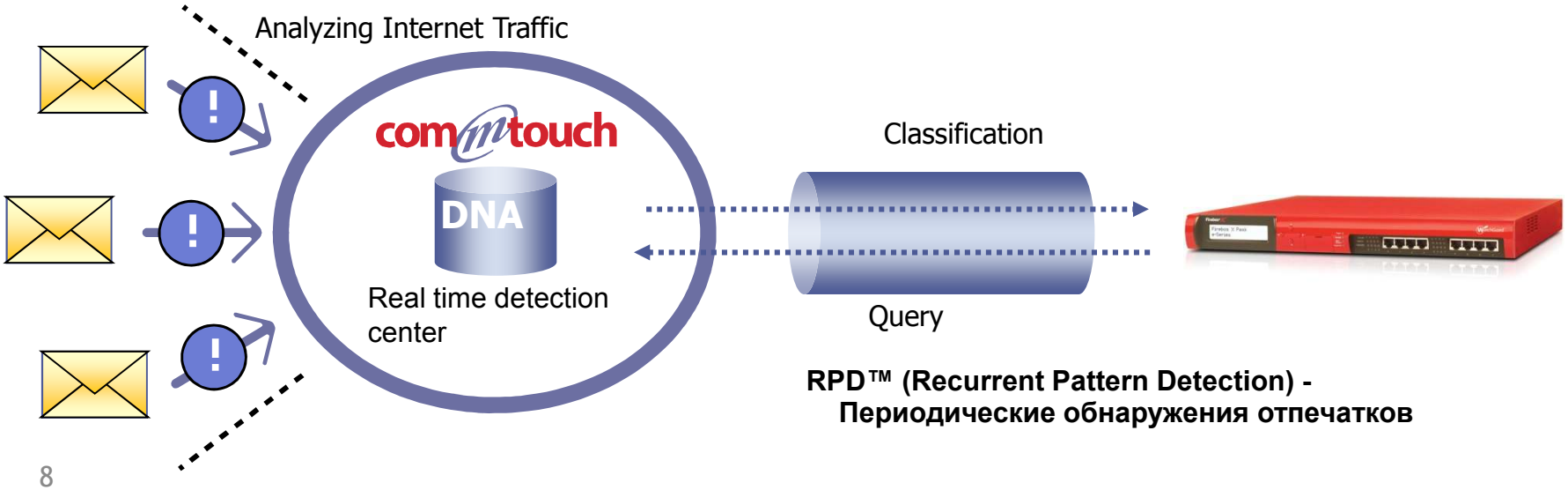
In-house Unaddressed

WatchGuard Gateway AntiVirus (Антивирус Шлюза)

- Принцип работы:
  - Блокирует Вирусы, Черви, Трояны, Шпионское ПО
    - Входящий и исходящий трафик
    - HTTP, HTTPS, FTP, SMTP, POP3, TCP-UDP
  - Использует сигнатуры и технику промежуточного сканирования
- Назначение:
  - Повышение уровня защиты серверов и ПК
  - Блокирование вредоносного ПО до его проникновения внутрь сети организации
  - Предотвращение повреждения и потери данных

SpamBlocker (блокировщик спама)

- Безопасное и простое обнаружение вспышек массовых рассылок в реальном времени
- Принцип работы:
  - Обнаружение схожих компонент для каждой рассылки
  - Точное определение
  - Сравнение входящего сообщения с отпечатками спама в режиме реального времени



RPD™ (Recurrent Pattern Detection) -
Периодические обнаружения отпечатков

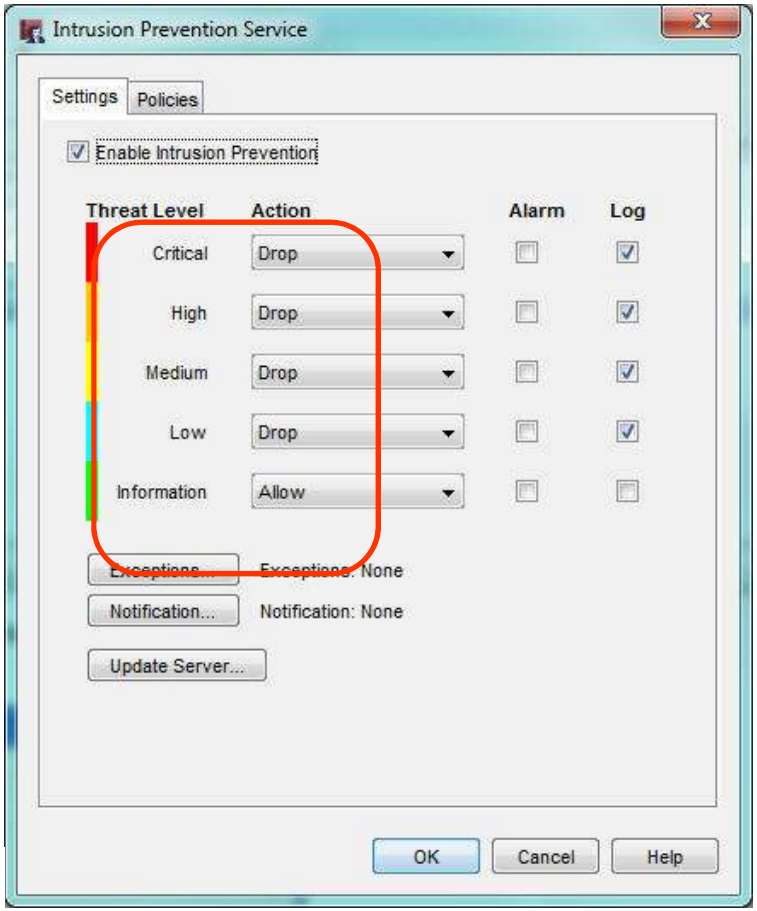
WatchGuard WebBlocker

websense

- Принцип работы:
  - 54 категории ссылок на сайты
  - Регулярные обновления для достижения максимального уровня фильтрации
  - Списки исключений (Белые/Черные)
  - Отчеты веб-доступа, нарушений, история использования
- Назначение:
  - Повышение эффективности использования рабочего времени
  - Гибкость в построении политик доступа
  - Повышение нормативно-правовой защиты

Intrusion Prevention Service (Сервис предотвращения вторжений)

- Принцип работы:
  - Защита от известных уязвимостей с помощью сигнатур
  - Регулярное обновление сигнатур
- Назначение:
  - Защита от SQL инъекций, крос-сай скриптинга (XSS), переполнений буфера, червей
  - Защита от вредоносного ПО
  - Предотвращает от возможности использование злоумышленником вредоносного кода в потоке информации анализируемой WatchGuard



BroadWeb
Empower Your Network Security

REPUTATION SERVICE

- Использует репутацию URL адресов
  - URL репутация (не просто сайт или IP адрес)
  - Несколько источников информации
  - Динамические значения, в зависимости от ВЕБ условий

ПОЛЬЗОВАТЕЛИ И ПРИЛОЖЕНИЯ ВНЕ КОНТРОЛЯ!

WatchGuard Application Control

BroadWeb
Empower Your Network Security

БЕСКОНТРОЛЬНОЕ ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ ДОЛЖНО БЕСПОКОИТЬ ВАС

- Вы теряете много рабочего времени на не бизнес-приложения
- Ваш файервол пропускает множество приложений
- Вы не знаете какие приложения используются в вашей сети
- Множество вредоносного ПО распространяется через новые приложения

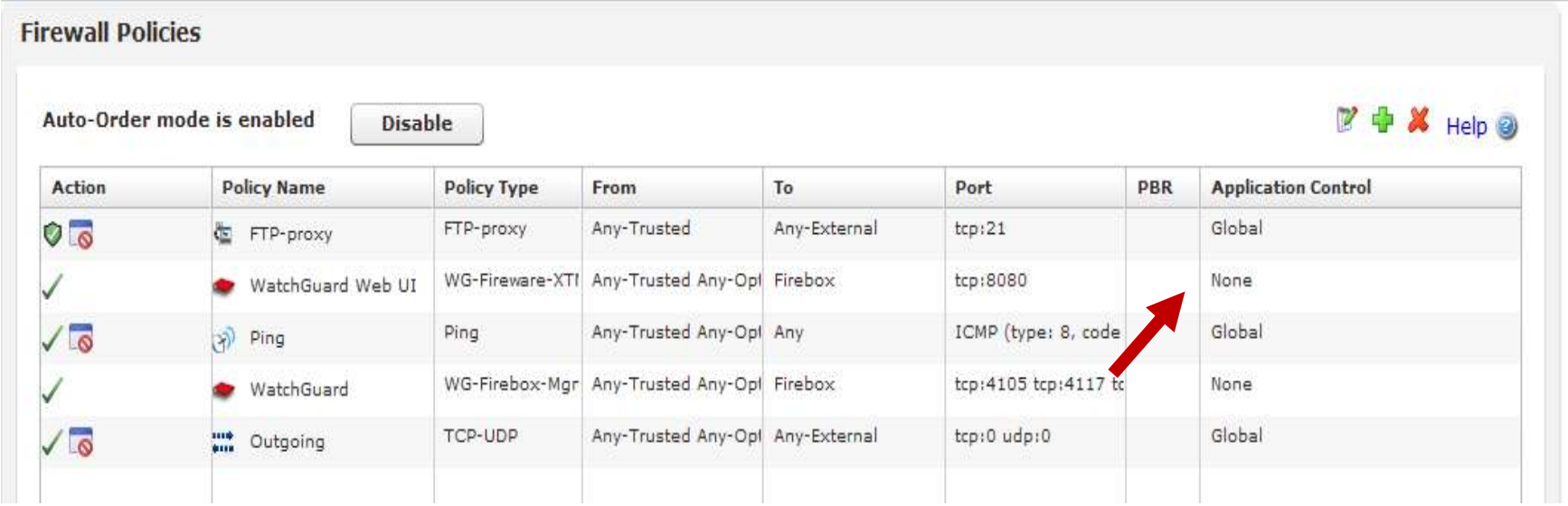
Есть все основания быть обеспокоенным использованием приложений в компании!

- В 2009 количество небезопасных сайтов выросла больше чем на 200%
- 55% уязвимостей затрагивают веб-приложения
- 77% зараженных сайтов являются легитимными
- 57% хищений данных происходит через интернет
- 76% уязвимостей используют веб-приложения

Источники: X-Force, Websense, Whitehat Security, Imperva, & 7Scan

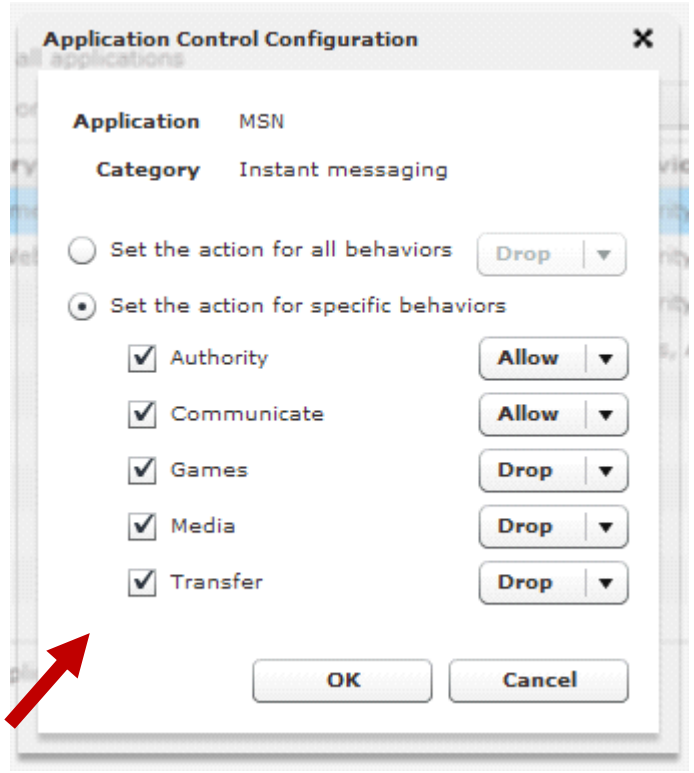
КОНТРОЛЬ ПРИЛОЖЕНИЙ

- Как WatchGuard решает проблему
  - Возможность идентифицировать, контролировать и логировать более, чем 1800 приложений и их функций
  - Гибкий контроль приложений
  - Интеграция в стандартную таблицу политик настроек файрволла



Примеры использования приложений

- Контроль приложений от WG делает возможным:
  - Блокировать приложения «точка-точка»(p2p)
  - Открыть Facebook для отдела маркетинга
  - Ограничить использование приложений по времени
  - Увидеть популярные приложение в своей сети
  - Запретить использовать передачу файлов через Skype

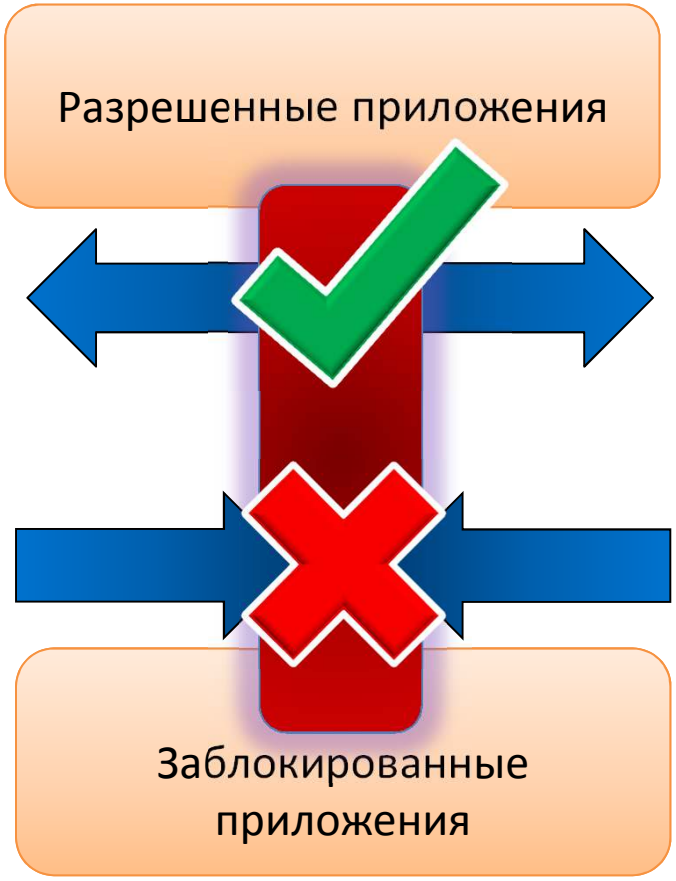


ГИБКИЙ КОНТРОЛЬ ПРИЛОЖЕНИЙ

Опции контроля	Преимущества использования
Запрет использования отдельных приложений для целого департамента, отдельных груп и пользователей	Поддержка продуктивности пользователей Предотвращение угроз безопасности
Контроль отдельных функции приложения, например запрет передачи файлов через SKYPE	Баланс доступности и блокирования угроз
Контроль доступа к приложениям в зависимости от времени суток	Продуктивность в рабочее время «Премирование» в нерабочее время
Контроль приложений по категориям	Простота в использовании
Централизированное управление приложениями	Централизированное управление распределенной инфраструктурой
Автоматическое обновление сигнатур приложений	Поддержка актуальности уровня защиты в мире динамических приложений
Детальные отчеты о использовании приложений	Контроль соблюдения политик использования приложений

ПРИМЕР ПРИЛОЖЕНИЙ

Категория	Пример приложений
Instant Messaging	QQ; MSN; Yahoo; GoogleTalk
Mail/Collaboration	Hotmail; Gmail; Yahoo; MS Exchange
Web 2.0	Facebook; LinkedIn; Twitter
P2P	Gnutella, Foxy, Winny; Bittorrent;
Remote Access Terminals	TeamViewer; GoToMyPC
Database	MS SQL; Oracle
File Transfer	Peercast; Megaupload
Voice Over IP	Skype
Streaming Media	QuickTime; YouTube; Hulu
Games	Xbox Live; Second Life
Network Mgt	MS Update; Adobe; Norton; McAfee
Web bypass	Ultrasurf; Avoidr; Circumventor



СОВРЕМЕННОЕ ВИДЕНИЕ БИЗНЕСА СОВПАДАЕТ С ВИДЕНИЕМ WATCHGUARD

Fireware XTM WatchGuard позволяет сократить риски и увеличить производительность для потребностей бизнеса

Content Security

Extensible Content Security (**XCS**)

Extensible Content Security предлагает защиту контента через электронную почту и веб-фильтр в сочетании с защитой от потерей данных.

XCS 280 & 580
For small businesses and medium-sized businesses

XCS 770R, 880 & 1180
For medium to large enterprises and ISP's

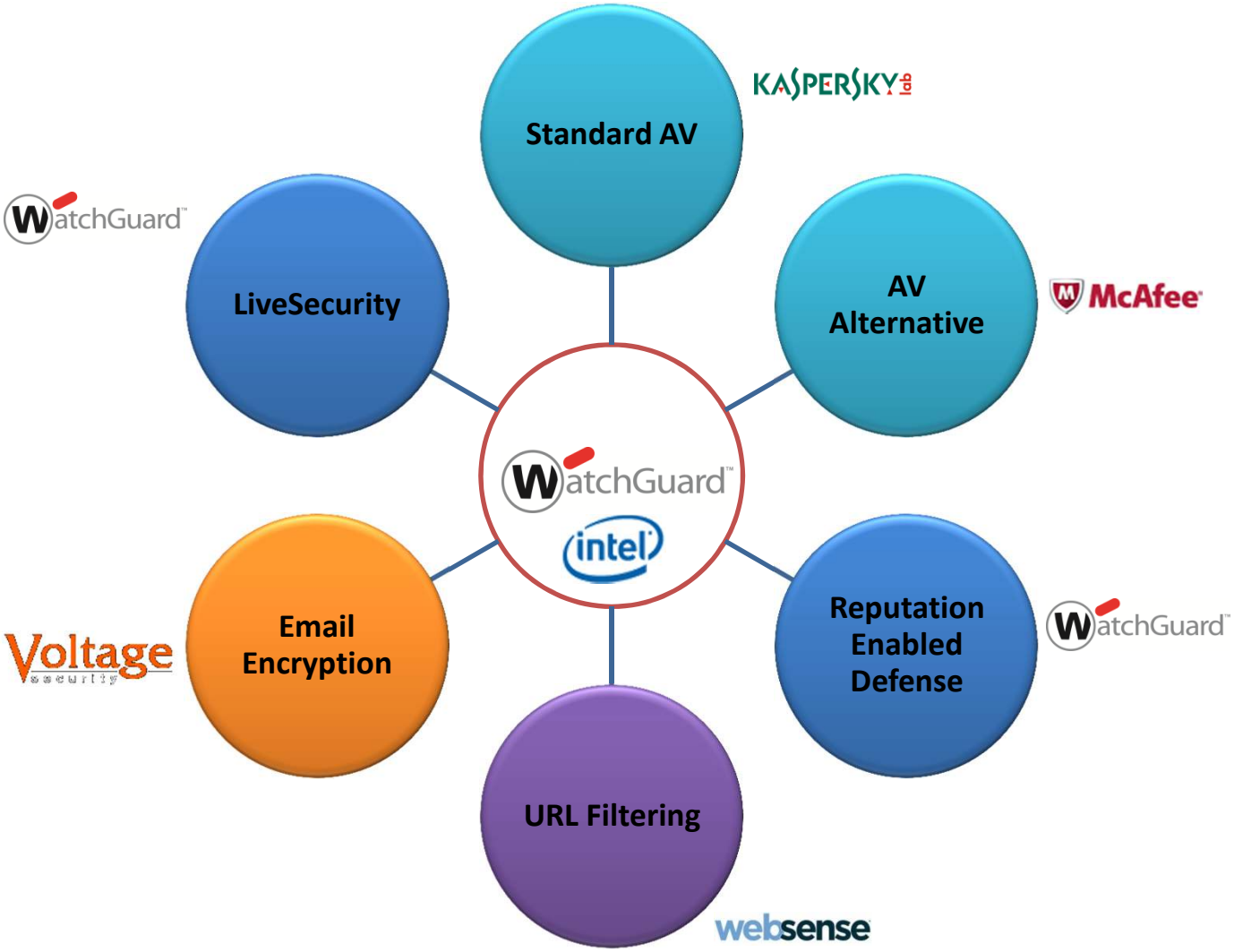
XCSv
Four full product virtual software license versions

- **CLUSTERING AND QUEUE REPLICATION**
- **ANTI-SPAM/VIRUS/MALWARE**
- **CUSTOMIZABLE REPORTING**
- **ENCRYPTION**
- **CONTENT FILTERING**
- **DATA LOSS PROTECTION**
- **CENTRALIZED MANAGEMENT**
- **WEB SECURITY WITH:**
  - **>URL FILTERING**
  - **> WEB CONTENT FILTERING**
  - **> ACCEPTABLE WEB USAGE**
  - **> WEB APPLICATION CONTROL**
  - **> TRAFFIC MANAGEMENT**

Introducing the new XCS Series: Extensible Content Security highlights

- **Мощное anti spam решение**
  - Блокирует 98% spam с 99.9% точностью сканирования входящего и исходящего трафика, предотвращение угроз и возможность применения гибких политик.
- **Кластеризация и репликация очередей**
  - Нулевая потеря сообщений
- **Приватность**
  - Криптирование e-майлов
  - Предопределённые словари соответствия

Best-In-Class Security: XCS



Defense-in-Depth for Email Security

ReputationAuthority	Spam Prevention	Malware Prevention
• 98.3% Rejected • Perimeter Security	• Customized • Outbreak Response	• Multiple Layers of Protection • All Malicious Code
1st Line of Defense	2nd Line of Defense	3rd Line of Defense

Rejected Email Messages

Get Secured.

Data Loss Prevention

Что такое предотвращение потери данных (DLP)?

- **Это:**
  - Инструмент, охватвающий бизнес стратегии
  - Технология, которая следит за содержанием и предписанием политик использования и передачи данных

- **Может применяться:**
  - В защите интелектуальной собственности
  - Против случайных потерь данных
  - Против краж данных

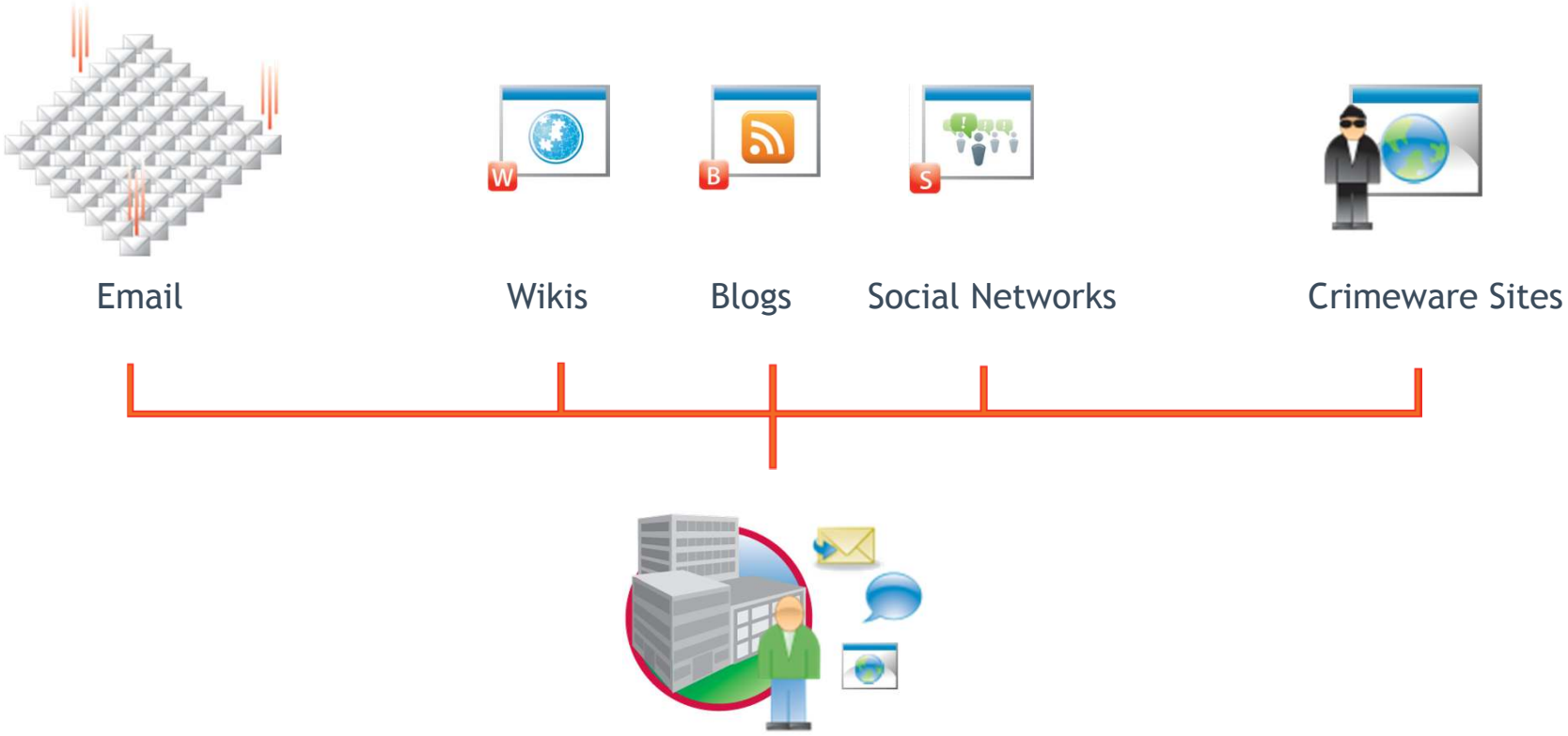
WatchGuard Data Loss Prevention

- **Deep Inspection**
  - Email & Web
  - Content and context scanning
- **Consolidated Policy Management**
  - Single UI
  - Reporting
- **Integrated Remediation**
  - Encryption
  - Block or allow
  - Quarantine or reroute

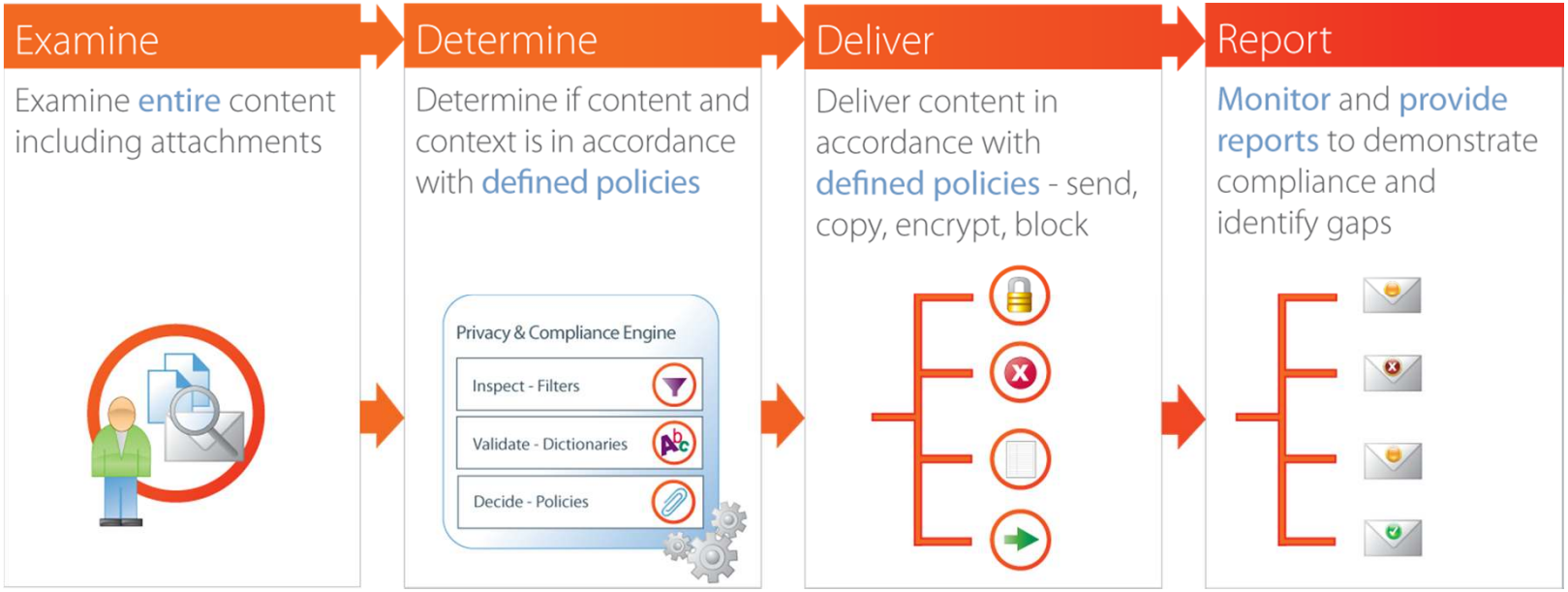
"The true value of content monitoring and filtering lies in helping management to identify and correct faulty business processes and accidental disclosures."

Source: Gartner Research: Content Monitoring and Filtering Helps Find Faulty Business Process, Accidental Disclosures

Создание проблемы: Потенциал для утечек данных обширен



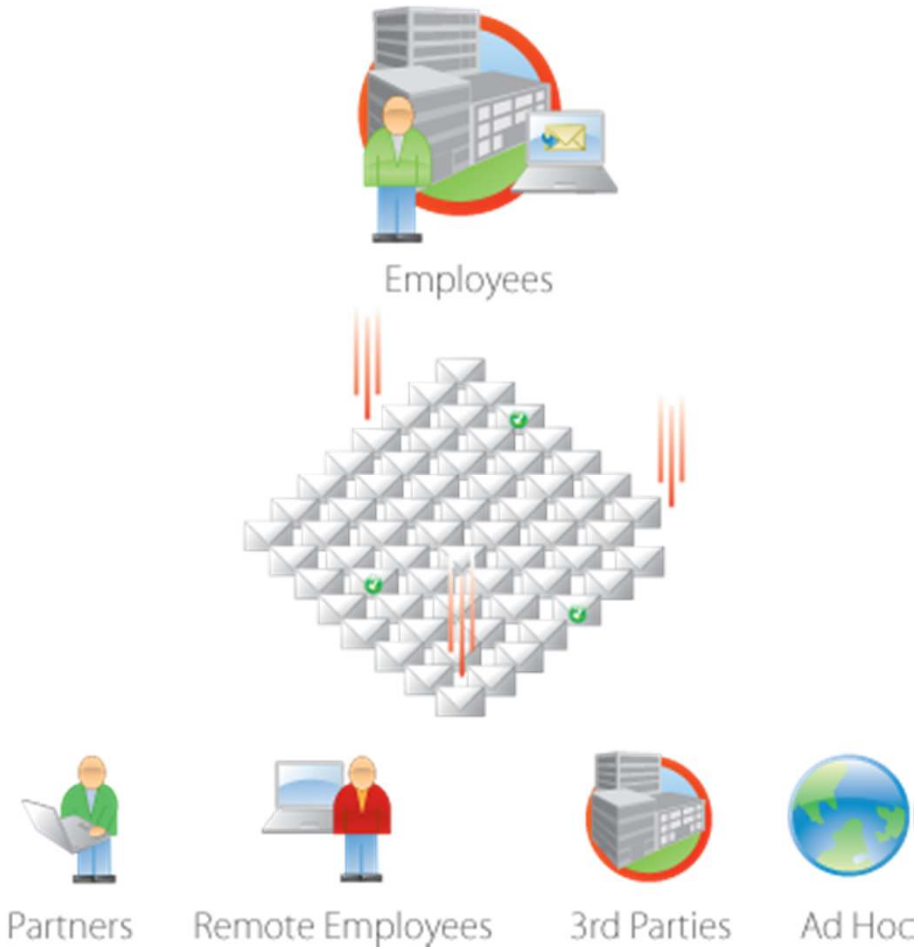
Простой процесс интегрирования



Get Secured.

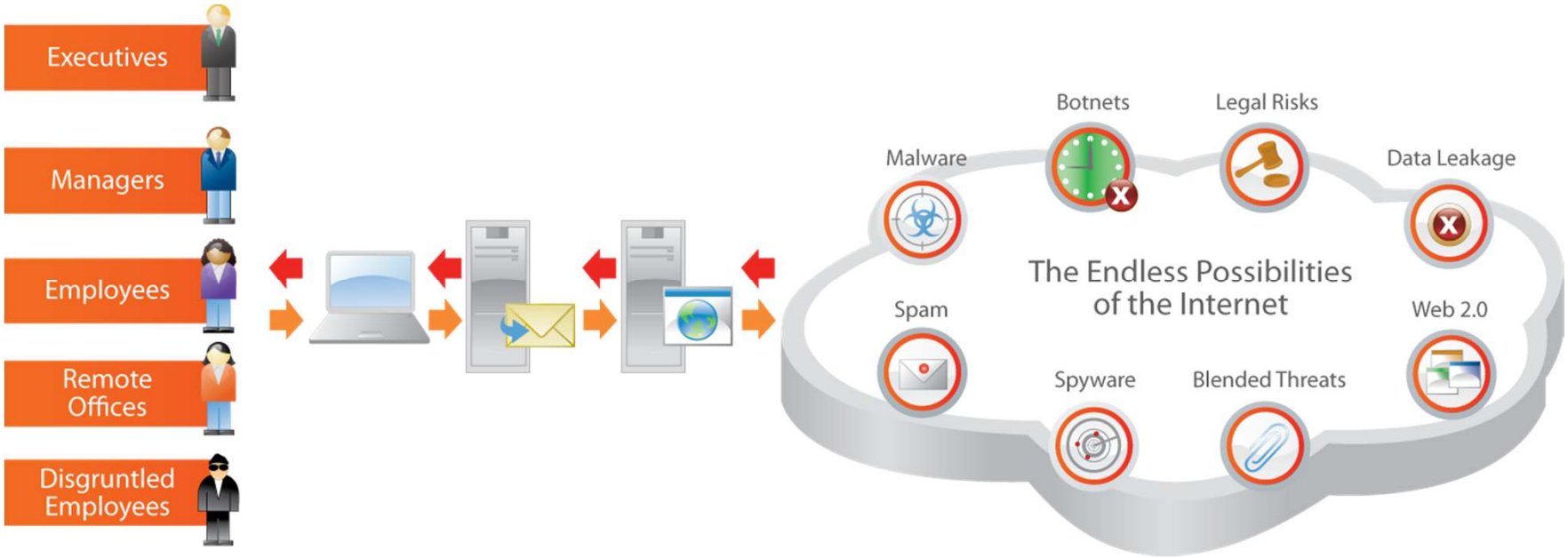
Never Lose A Message
Email Encryption

Everyday Messages Contain Private Data



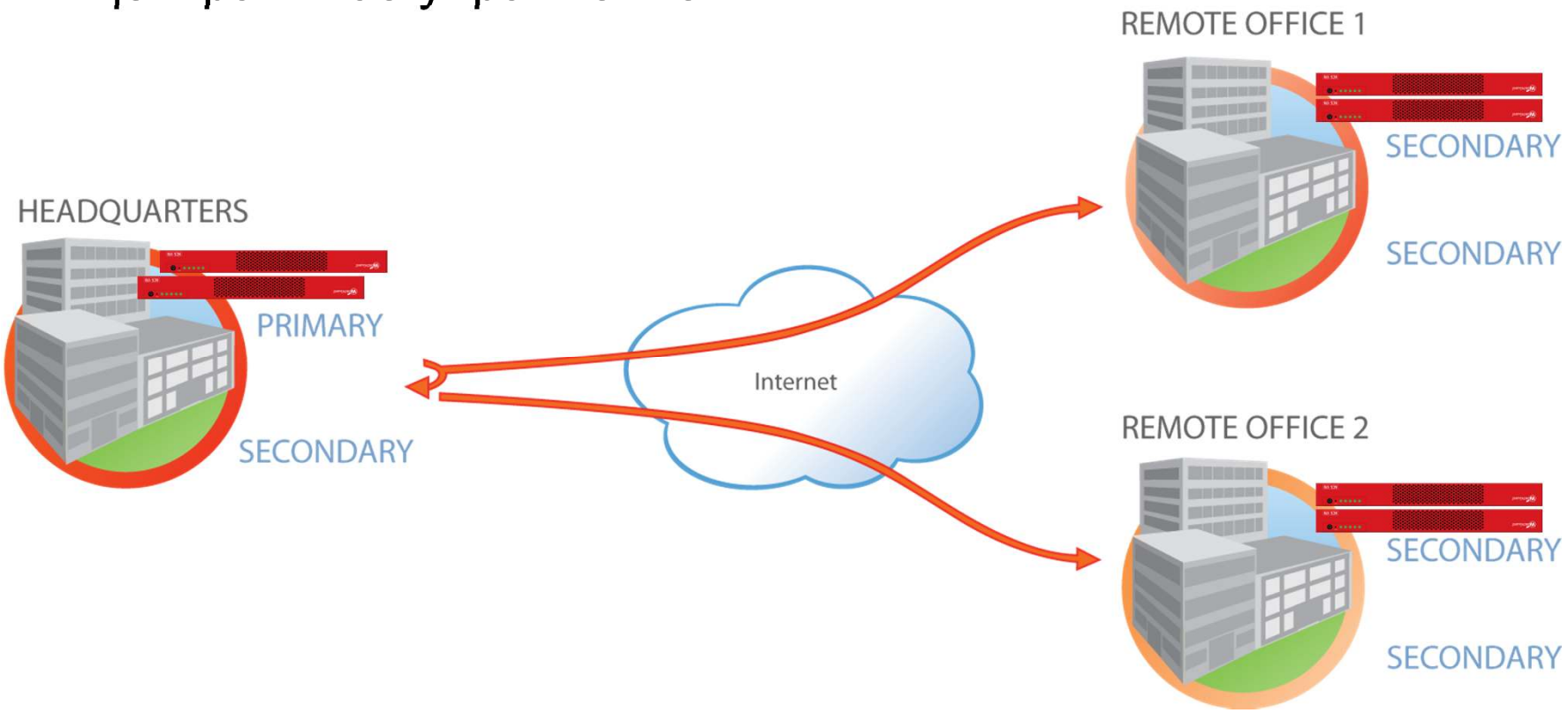
- Конфидециальность
- Соответсвие
- Конфидециальная информация или данные
- Интеллектуальная собственность
- Риск приложений

Существующие угрозы: Bidirectional Email & Web Risks

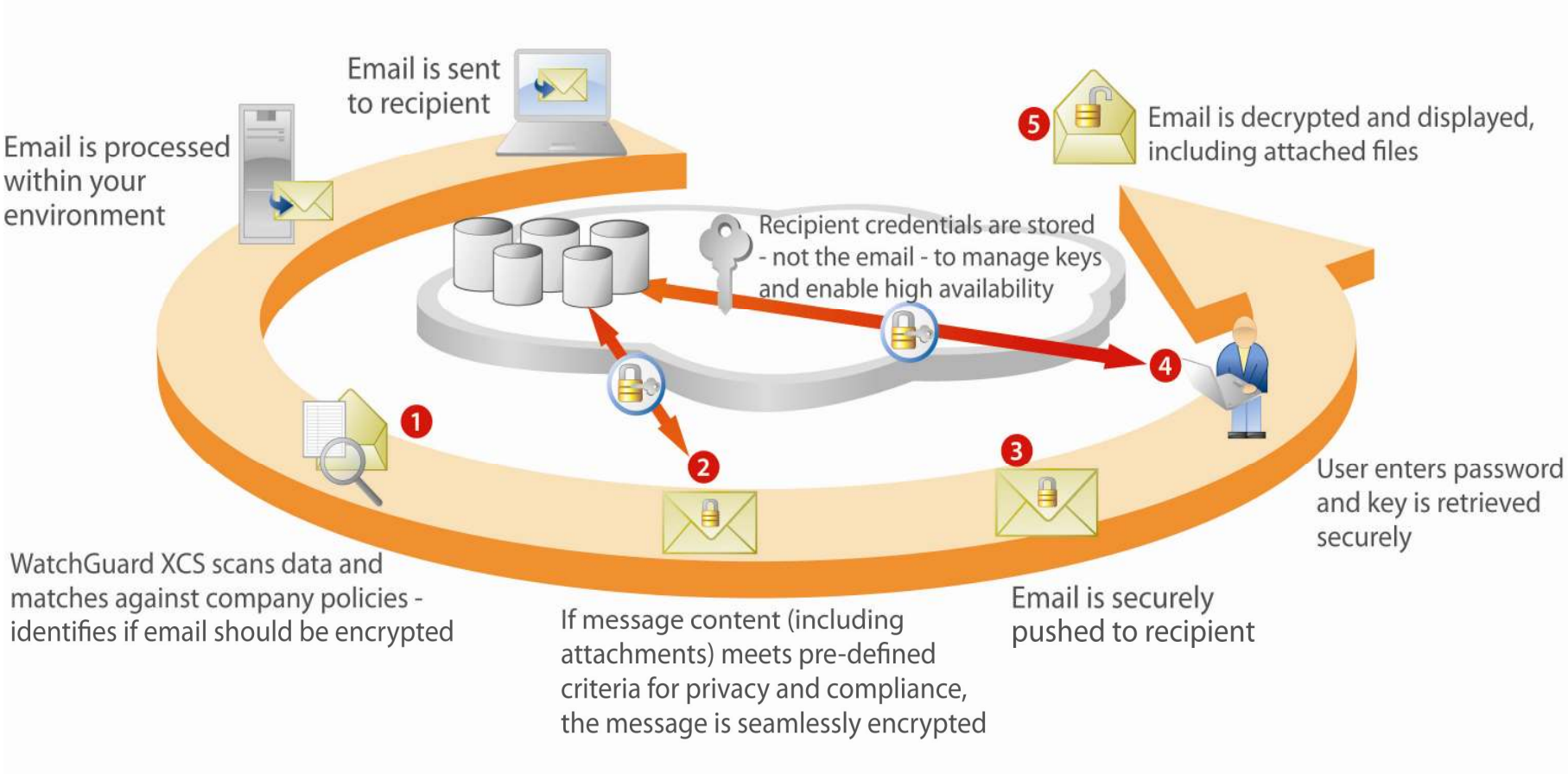


Высокая надёжность & Нулевая потеря писем

- Кластеризация & Репликация трафика
- Центральное управление



The WatchGuard Email Encryption Subscription



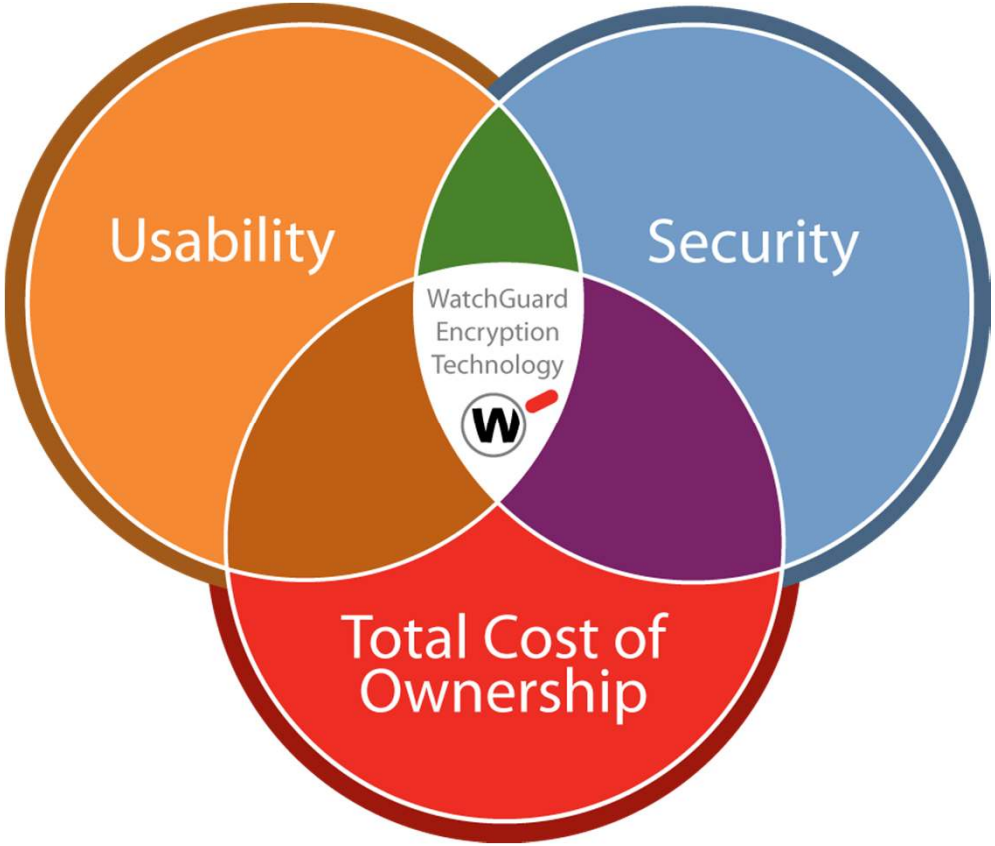
Случаи применения криптирования

- Бизнес процессы
  - Финансовые операции
  - Продажа, заказы, квоты и счета
- Соответсвие
  - PCI, HIPAA, EU Directive, GLBA, PIPA…
  - Требования третьей стороны
- Передача бизнес сообщений

Finally…Email Encryption Made Easy!

WatchGuard Provides a Single, Integrated Solution

- Лёгкое в использовании
  - Нет клиентов или plug-in
  - Нет сертификатов
- Легко развёртывается



Спасибо!

Вопросы?