

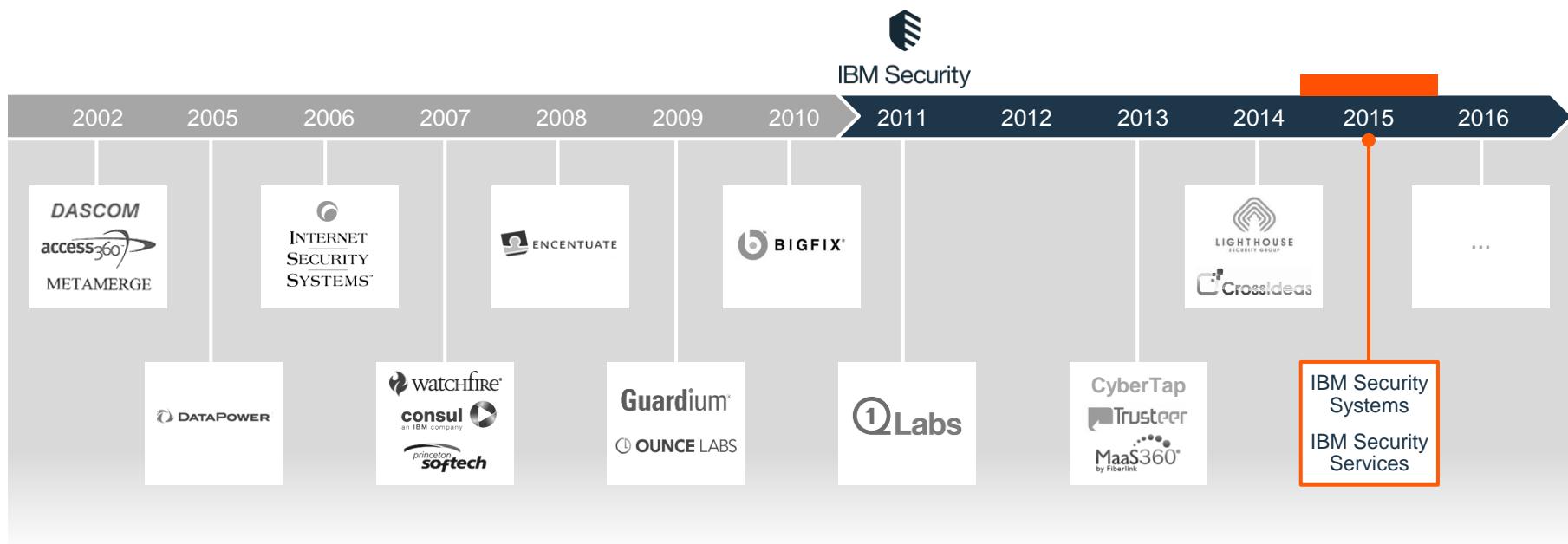


УВЕЛИЧИВАЯ ЦЕННОСТЬ ИБ
Интеграция продуктов
IBM Security

Олег Бакшинский

2016

IBM Security инвестирует в лучшие технологии



“...IBM Security всегда движется верно...”

Forbes

IBM Security Стратегия

ПОДДЕРЖКА директоров ИБ



CISO, CIO и другие директора

- Стратегия и лидерство
- Быстрая трансформация
- Интеграция решений

ИННОВАЦИИ в ключевых трендах



Advanced Threats



Compliance Mandates



Cloud



Skills Shortage



Mobile and Internet of Things

ЛИДЕРСТВО в выбранных сегментах

IBM Security Capability Framework

Strategy, Risk and Compliance

Cybersecurity Assessment and Response

Security Intelligence and Operations

Advanced Fraud Protection

Identity and Access Management

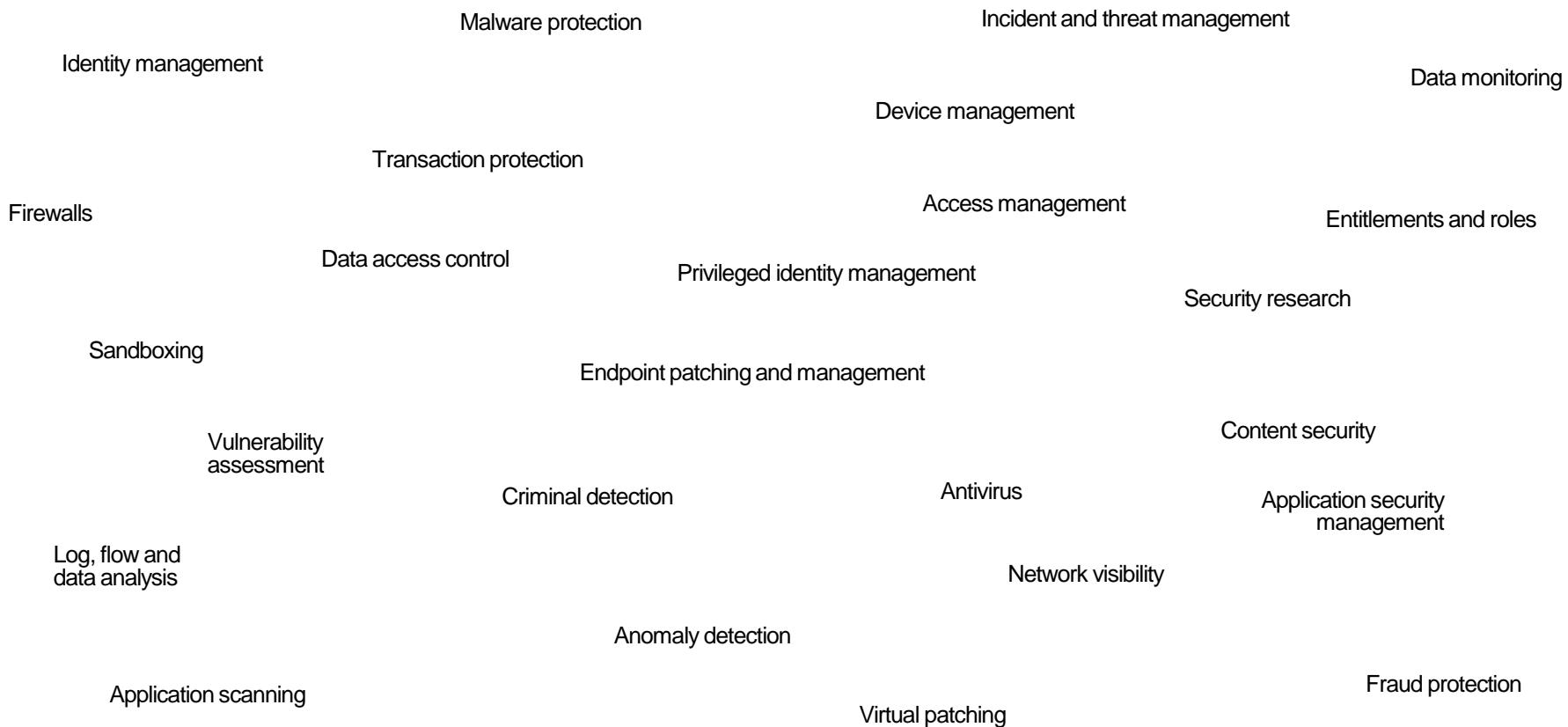
Data Security

Application Security

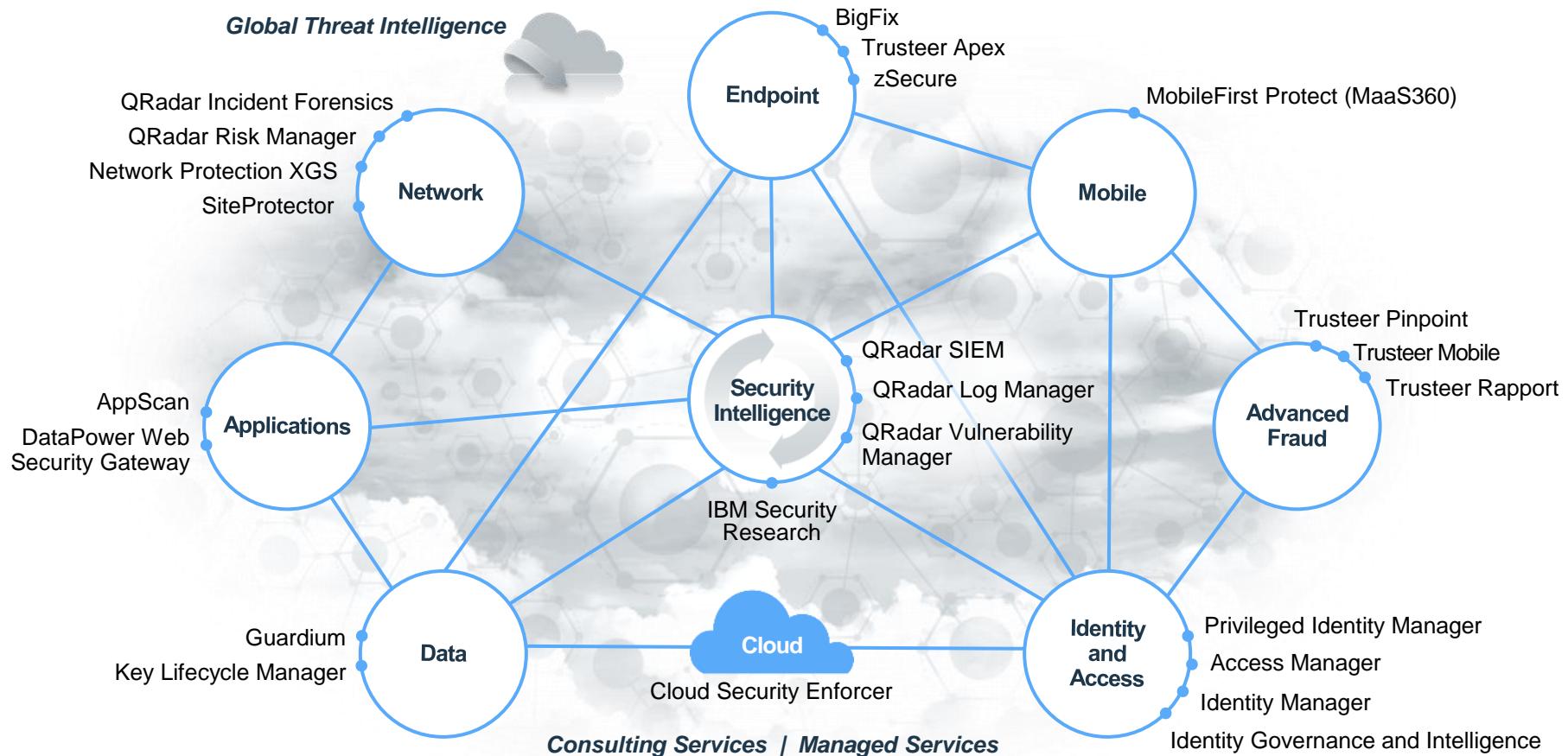
Network, Mobile and Endpoint Protection

Advanced Threat and Security Research

Выстраивать ИБ как иммунную систему



IBM обладает широчайшим портфелем решений ИБ в мире



Увеличиваем ценность ИБ через интеграцию

Оптимизируем ИБ

Соединяем различные модули системы ИБ

Уменьшаем сложность и стоимость

Собираем и коррелируем важную информацию от сотен источников

Адаптируемся к новым угрозам

Превентивно готовы к изменяющимся угрозам благодаря инновационным решениям и объединенной экосистеме



Меньше стоимость, больше видимость общей картины ИБ через использование интегрированной платформы



Традиционный SIEM
6 продуктов от 6 вендоров

Потоки	ARBOR NETWORKS	Lancope. Network Performance + Security Monitoring™	riverbed Think fast.™
Пакеты	EMC² RSA	SOLERA NETWORKS™	
Уязвимости	QUALYS	RAPID7	tenable network security
Конфигурации	algosec FIREM QN	skybox security	tufin
Логи	logologic.	splunk>	
События	hp ArcSight	McAfee	EMC² RSA

IBM Security Intelligence
and Analytics



Интегрированная
унифицированная архитектура
в единой консоли браузера



**IBM Security QRadar
Security Intelligence Platform**

Выявление и защита критичных данных



Выявление рисков

- Обследование и классификация критичных данных
- Оценка уязвимостей баз данных

Усиление хранилища

- Шифрование и маскирование
- Архивация/чистка
- Восстановление



Мониторинг доступа

- Мониторинг и уведомление об атаке в режиме реального времени
- Выявление подозрительной активности
- Отчеты регуляторов

Защита данных

- Защита от НСД
- Контроль за изменениями

IBM Guardium Data Protection and IBM Critical Data Protection Program

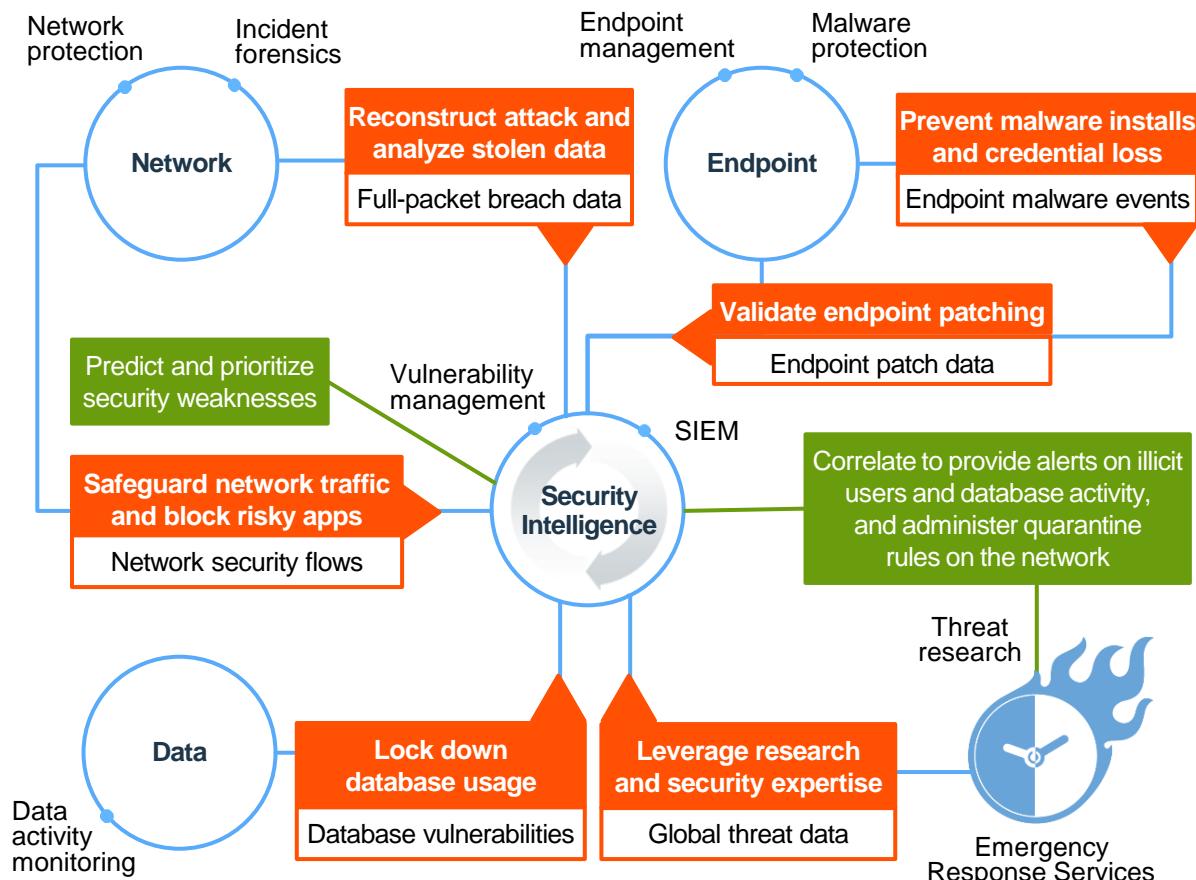
Защита критичных данных = защита репутации компании



ПРЕИМУЩЕСТВА ИНТЕГРАЦИИ

Защита от целевых атак

Интегрированная защита от целевых атак



ЦЕННОСТЬ ИНТЕГРАЦИИ

Активировать

Блокировать вредоносы в сети и на конечных точках, предотвратить неверное использование данных и расширить контроль активов

Постоянный мониторинг активности для выявления аномального поведения в реальном времени

Внедрение политик ИБ, понимание происходящего и подготовка к противостоянию новым угрозам

Показать все

Прервать цепь атаки в реальном времени

ЦЕПЬ АТАКИ

ВЗЛОМ

Удаленный сотрудник инфицирован через скачивание ПО

1

ЗАХВАТ

Внутренняя система инфицирована как часть ботнета

2

РАСШИРЕНИЕ

Целевые внутренние письма отправлены на высокопоставленных сотрудников

3

СБОР

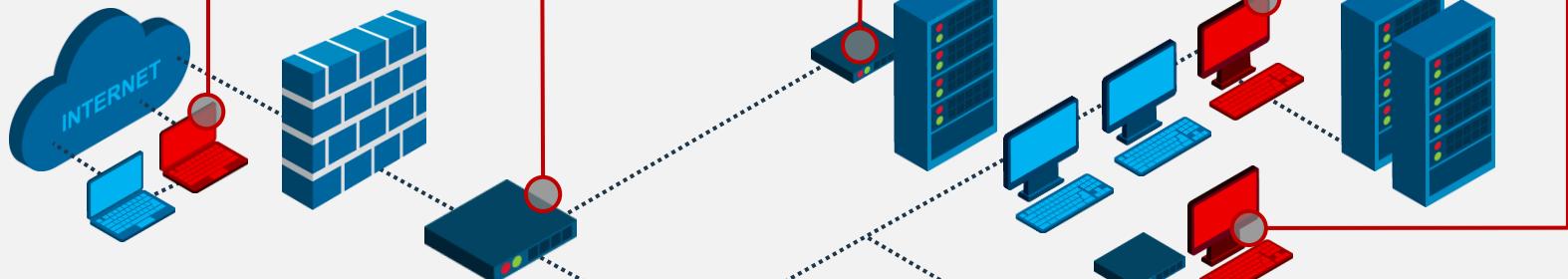
Авторизованная система пытается получить доступ к ресурсам

4

ВЫВОД

Постоянный тихий вывод собранных данных

5



Archer предотвращает установку вредоноса, сообщает в QRadar для корреляции, делится информацией с X-Force и XGS для предотвращения

XGS блокирует трафик с плохой репутацией и пересыпает потоки в QRadar для анализа

Стороннее решение по безопасности эл.почты выявляет наличие вредоноса во вложении в письме, сообщает в QRadar и через правило карантина на XGS блокирует

QRadar уведомляет о необычной активности пользователя и БД с целевого хоста

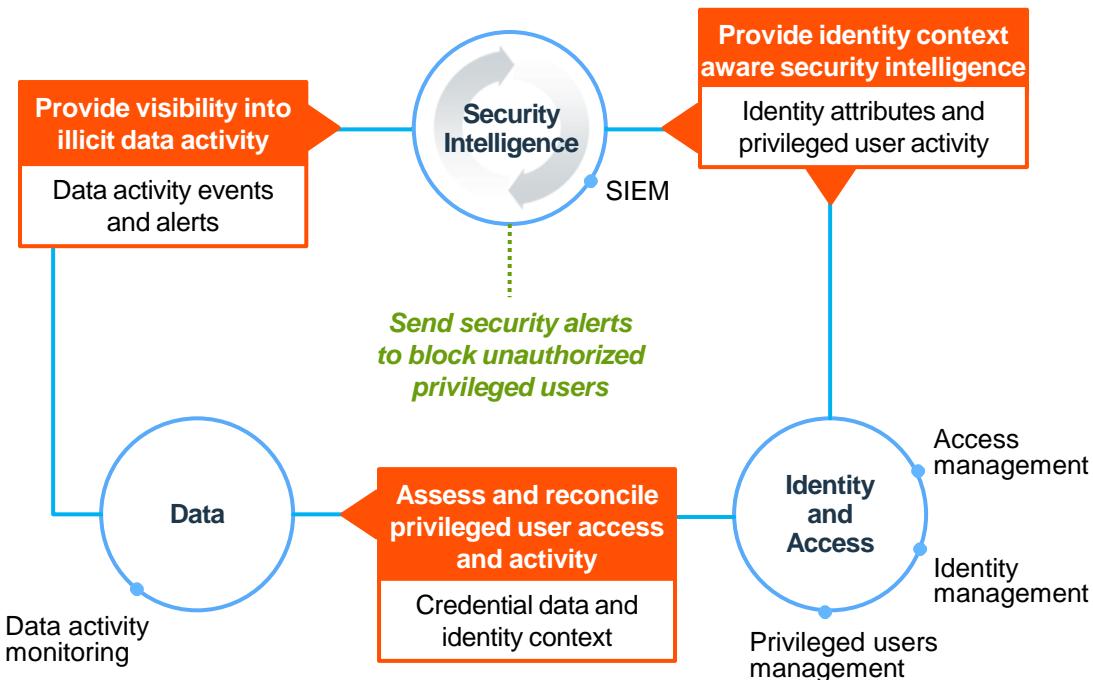
QRadar выявляет аномалии на инфицированных машинах, через правило карантина на XGS блокирует их, в это время incident forensics анализирует украденные данные



ПРЕИМУЩЕСТВА ИНТЕГРАЦИИ

Защита от инсайдеров

Интегрированная защита от инсайдеров



ЦЕННОСТЬ ИНТЕГРАЦИИ

Активировать

Информация о привилегированных пользователях и управление их учетными данными

Понимание, какие ценные данные где находятся, когда и кем осуществлялся доступ

Выявить необычную активность и внести корректива для блокировки и предотвращения

Показать все

Выявить и блокировать угрозу инсайдеров

ИНСАЙДЕРСКАЯ АКТИВНОСТЬ

ЗЛОУПОТРЕБЛЕНИЕ ПРАВАМИ ДОСТУПА

Пользователь осуществляет доступ к БД через Shared ID

ДОСТУП К КРИТИЧНЫМ ДАННЫМ

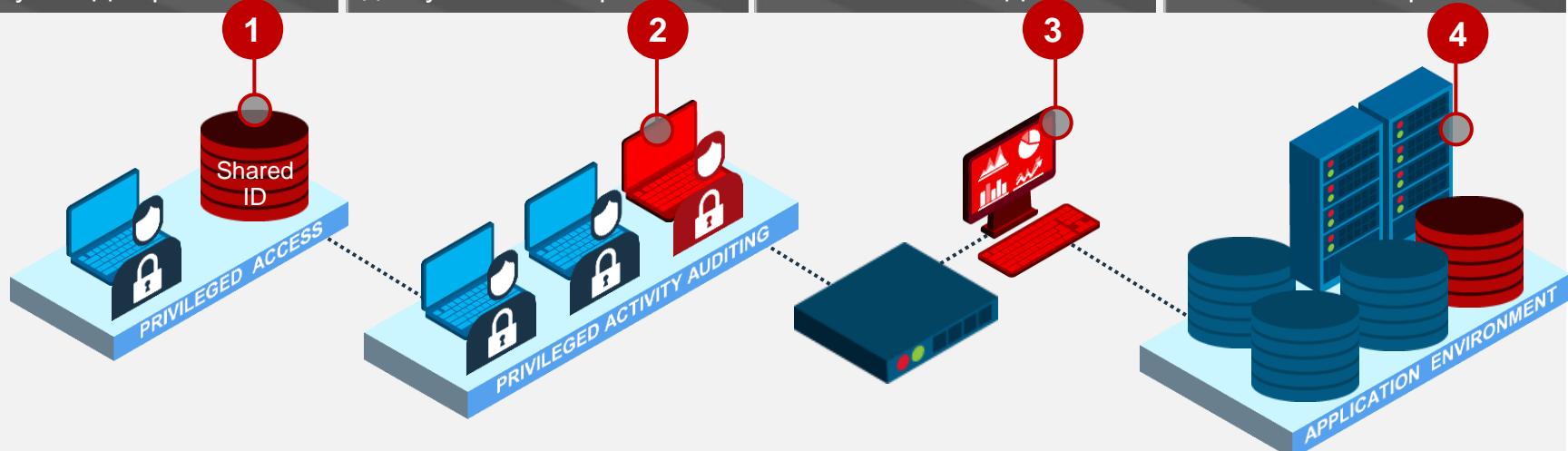
Пользователь осуществляет доступ к важным ресурсам

ВРЕДОНОСНАЯ АКТИВНОСТЬ

Подозрительная активность пользователя в БД

ЗЛОУПОТРЕБЛЕНИЕ СЕРВИСНОЙ УЧЕТКОЙ

Подозрительное использование приложения



PIM контролирует и учитывает доступ к БД через коллективные учетные записи. Guardium может уведомлять или блокировать неавторизованный доступ.

PIM записывает все сессии, а Guardium выстраивает взаимосвязи сессий с информацией через аудит активности доступа к данным

QRadar коррелирует права PIM и активности Guardium для выявления аномалий и уведомлений, чтобы можно было произвести корректирующее действие

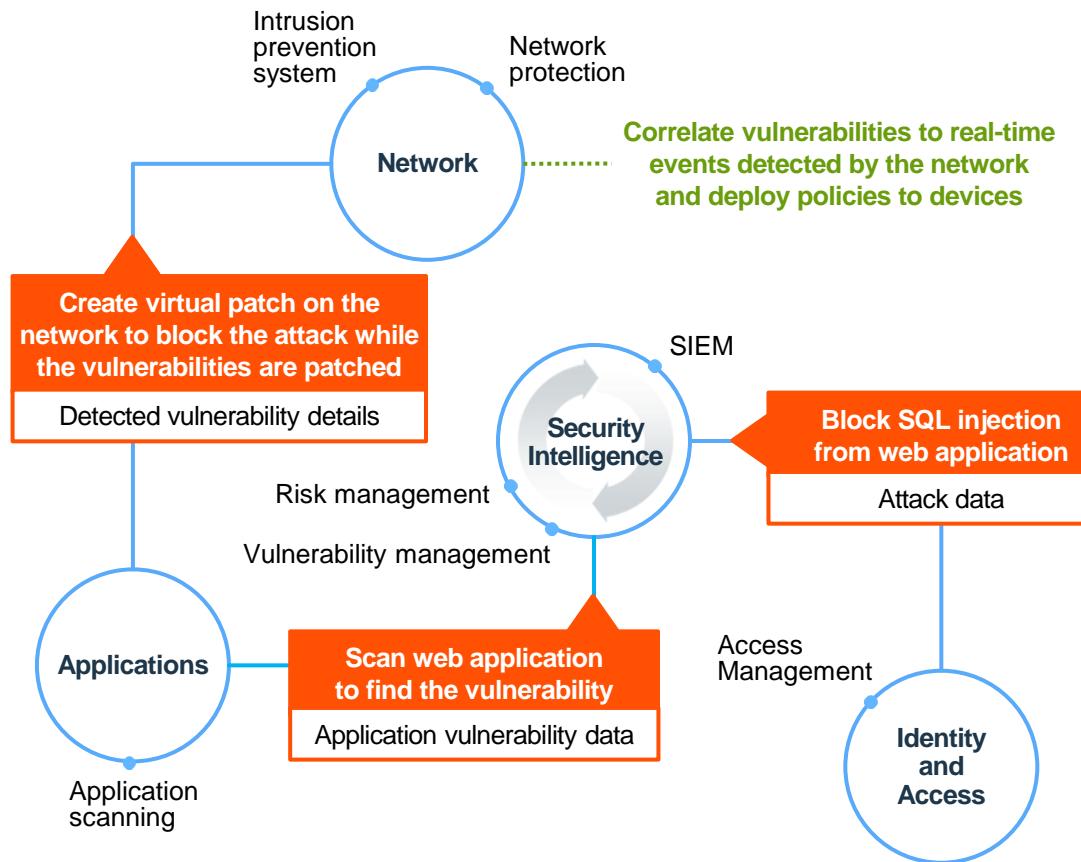
PIM выявляет защищенные пароли в приложениях, а Guardium отслеживает использование сервисных IDs и уведомляет QRadar о нарушениях



ПРЕИМУЩЕСТВА ИНТЕГРАЦИИ

Защита web-приложений

Интегрированная защита web-приложений



ЦЕННОСТЬ ИНТЕГРАЦИИ

Активировать

Сканирование приложений для понимания, что взломано и где ещё уязвимо

Блокировать атаку и уведомить

Конфигурация настроек IPS и сетевых устройств с учетом известных уязвимостей

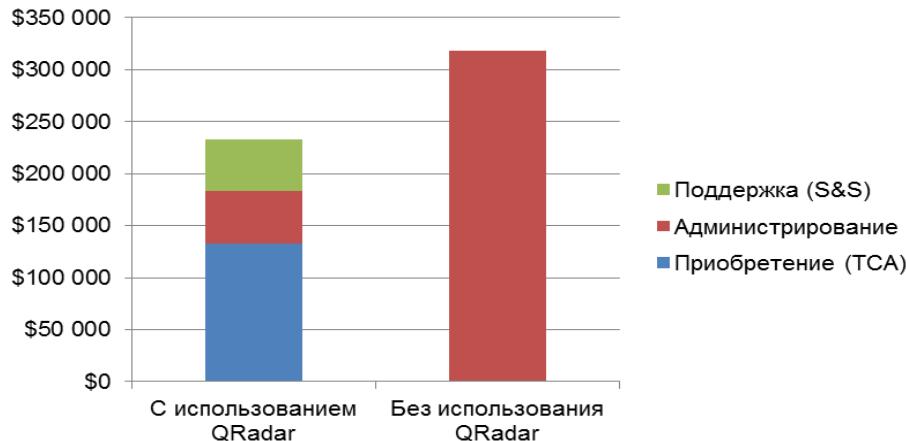
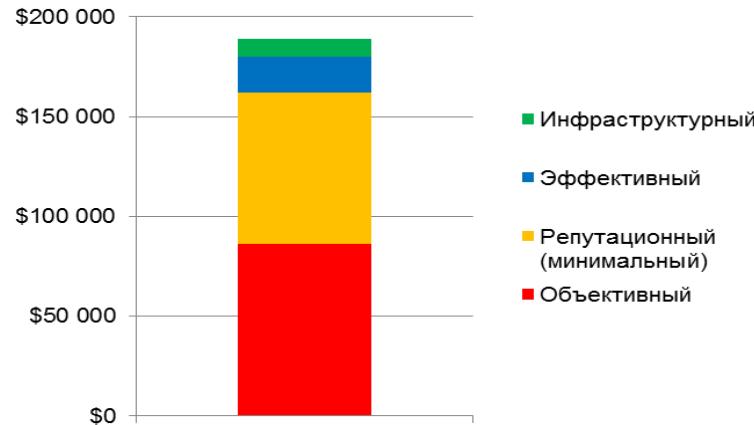
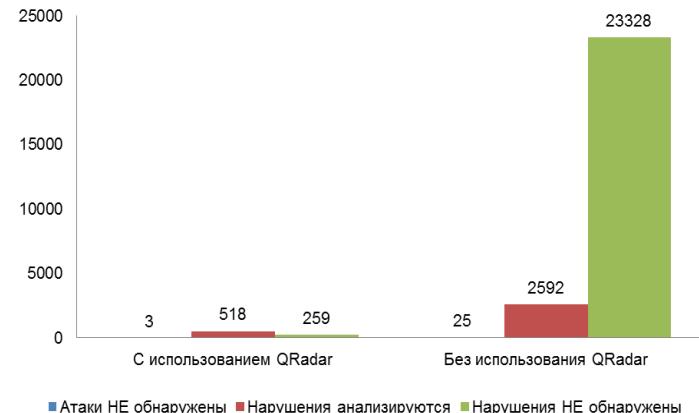
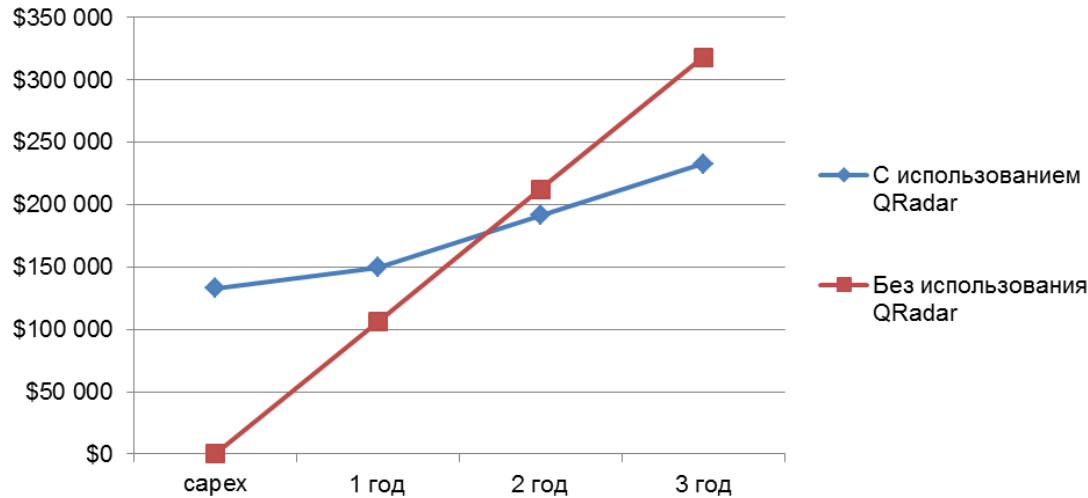
Показать все



ПРЕИМУЩЕСТВА ИНТЕГРАЦИИ

Окупаемость инвестиций

Финансовые преимущества интегрированной защиты





IBM Security



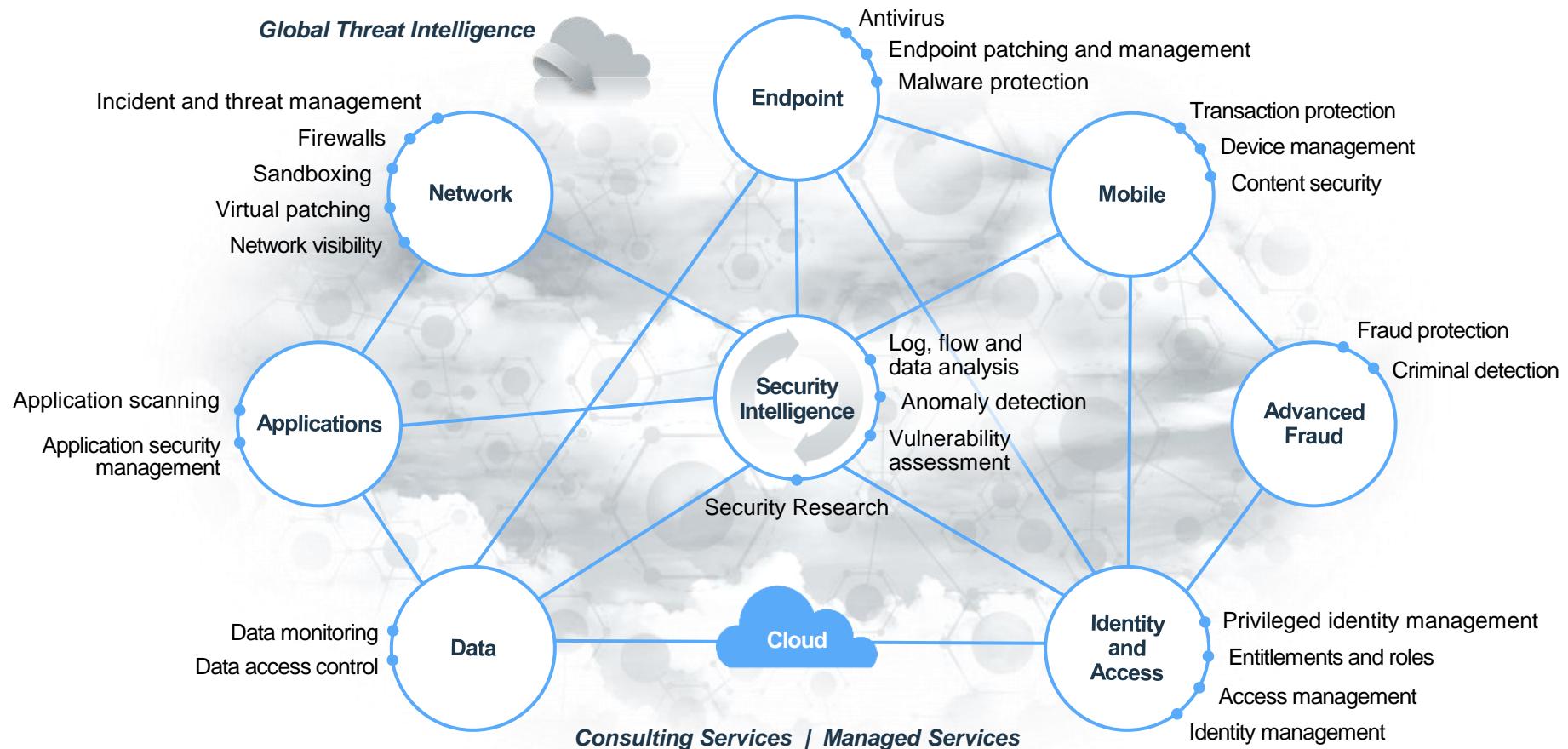
THANK YOU

www.ibm.com/security

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANYSYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Establish security as an immune system



Интегрированные исследования и технологии

ИНФОРМАЦИЯ ОБ ИНТЕГРАЦИИ	
Network Protection XGS + QRadar	XGS может отправлять данные потоков 7-го уровня в QRadar, а QRadar может отправлять команды карантина на XGS
BigFix + QRadar	Integrates endpoint intelligence for closed-loop risk management
BigFix + Trusteer Apex	Provides continuous protection from APTs by installing Apex agent to BigFix managed endpoints
X-Force Exchange + Network Protection XGS	Updates XGS using X-force IP reputation database to address latest threats and provide intelligent blocking
Identity Manager + Identity Governance	Improves an organization's governance posture, while reducing total cost of ownership and overall complexity
MaaS360 + Trusteer Mobile	Provides enterprise mobile device risk protection to complement MaaS360's capabilities

As of 3Q 2015