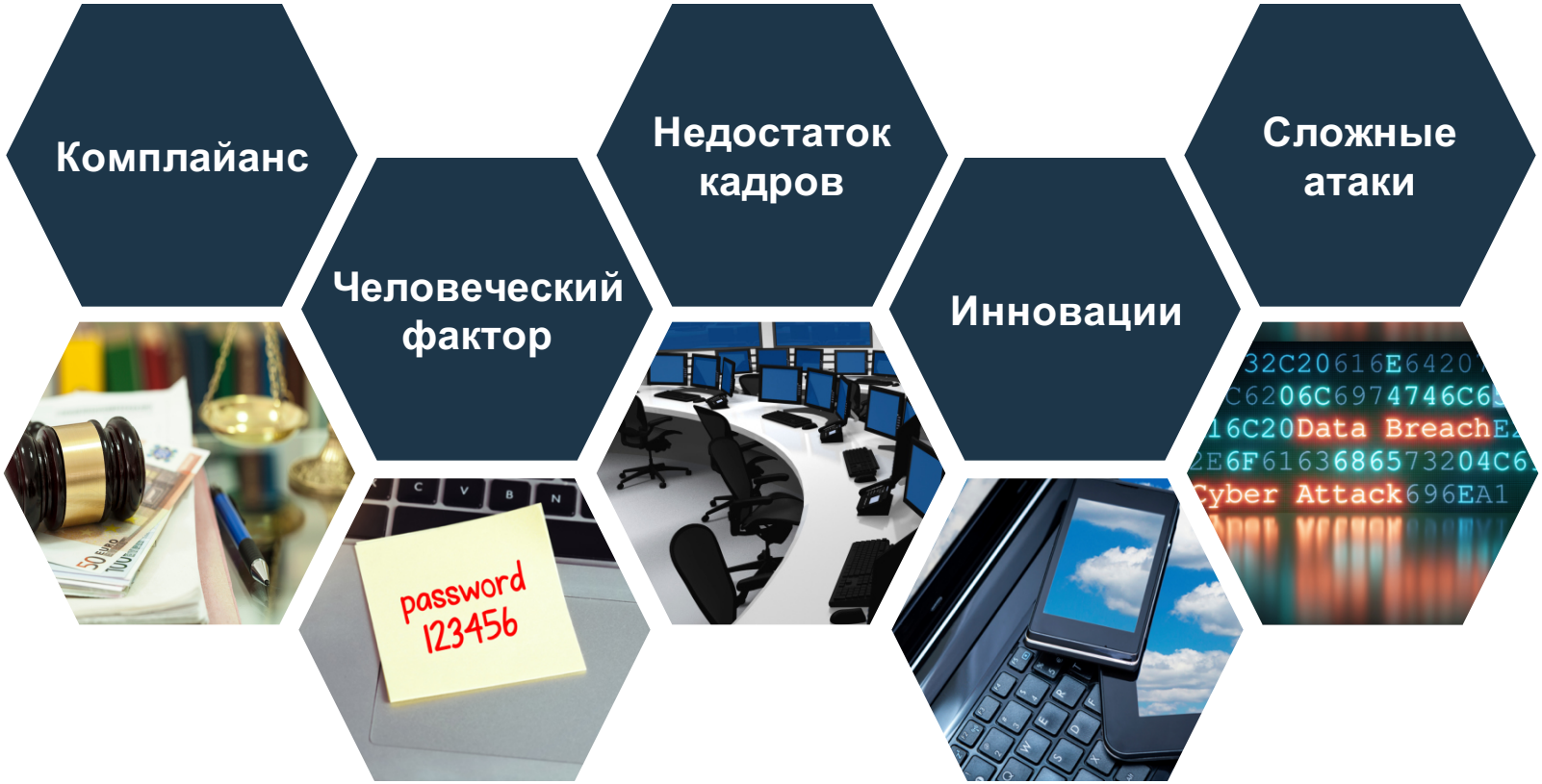
КОМПЛЕКСНЫЙ ПОДХОД К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Интеграционный подход за пределами традиций. Примеры использования

Воронцов Алексей, IBM Security Architect

2 июня 2016

Основные драйверы ИБ на сегодня



IAM – не должно быть единственным интеграционным решением

Malware protection

Incident and threat management

Identity management

Data monitoring

Device management

Transaction protection

Firewalls

Access management

Entitlements and roles

Data access control

Privileged identity management

Incident response

Sandboxing

Endpoint patching and management

Content security

Vulnerability assessment

Criminal detection

Antivirus

Application security management

Log, flow and data analysis

Network visibility

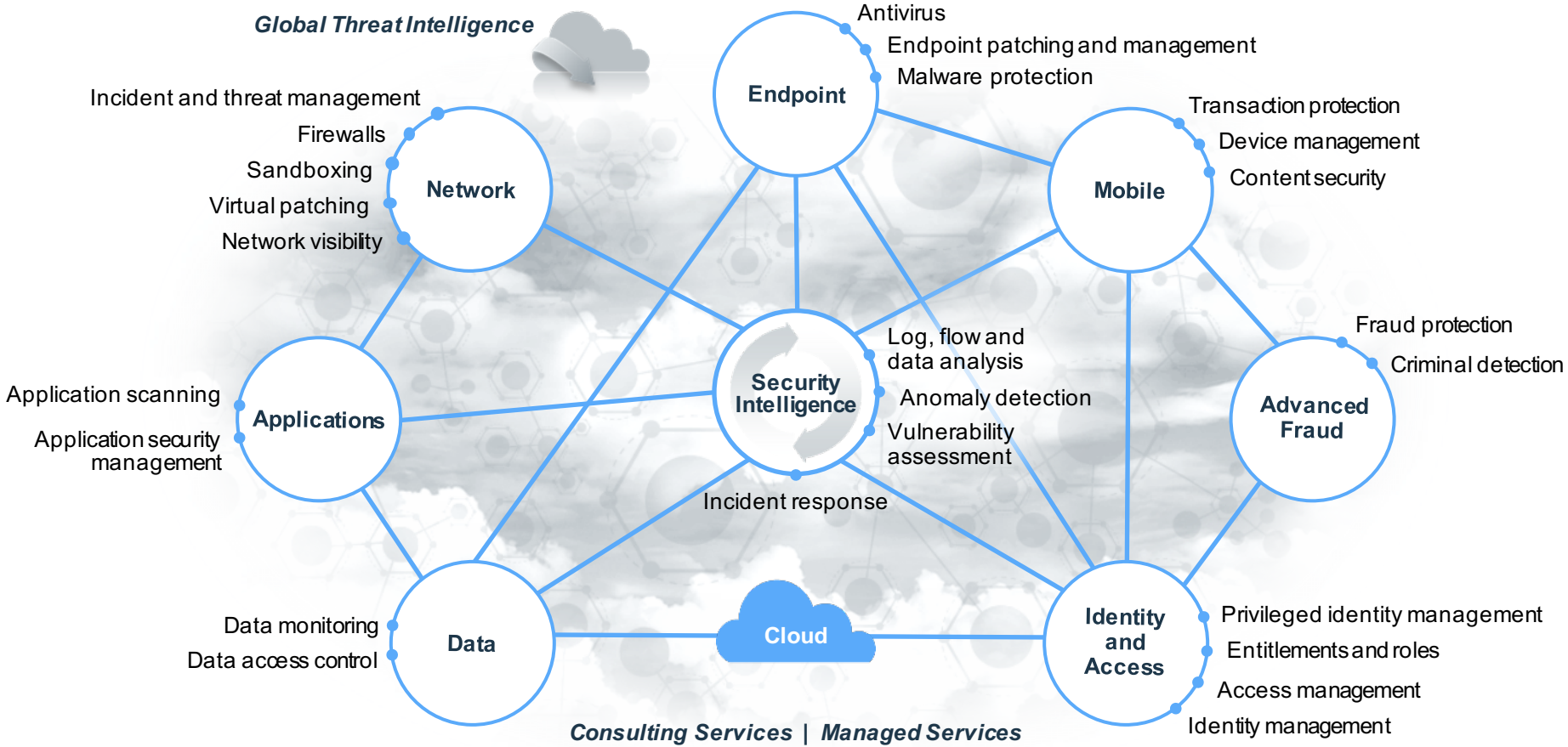
Anomaly detection

Application scanning

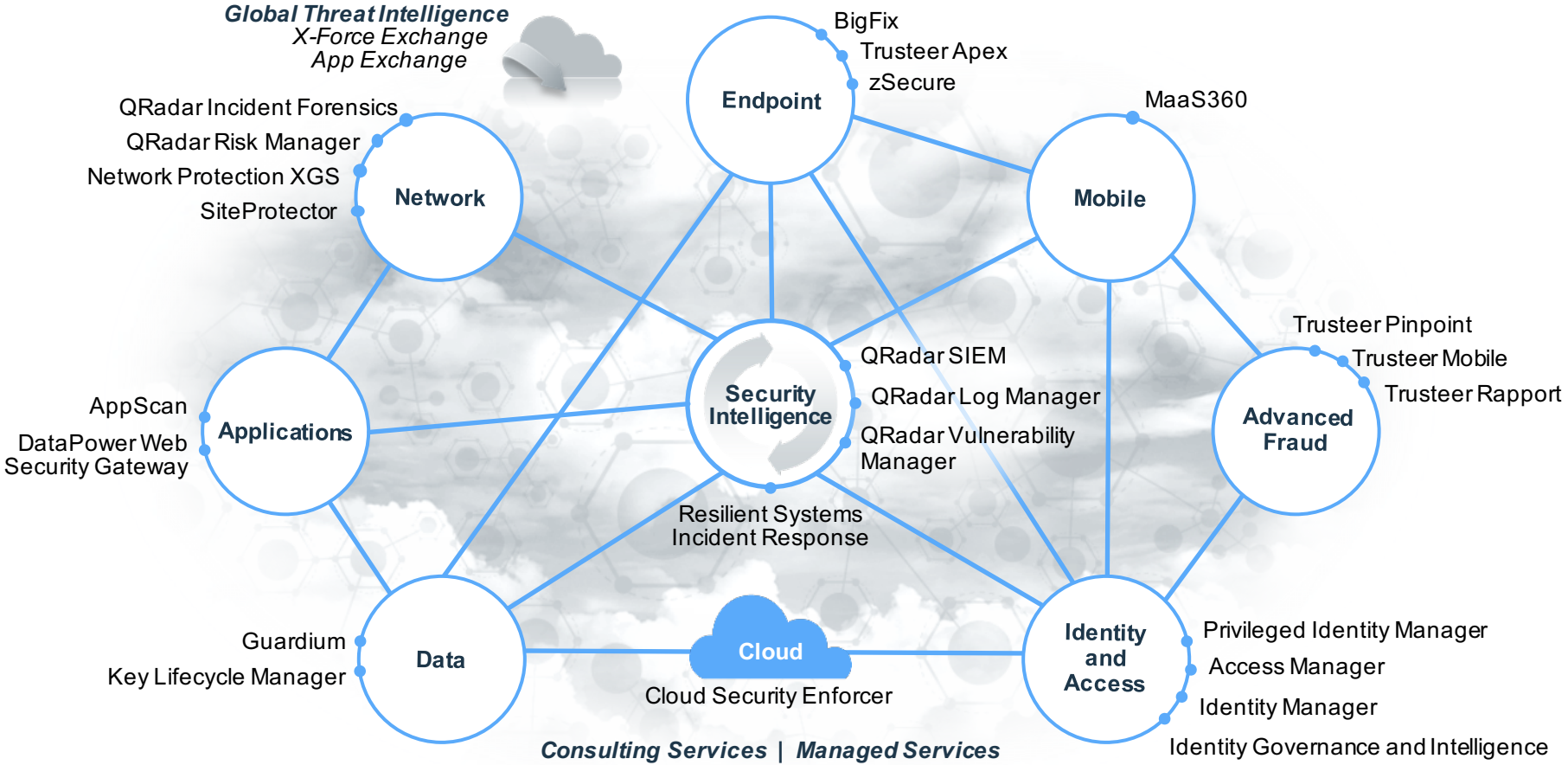
Fraud protection

Virtual patching

Безопасность – не периметр а “иммунная система”



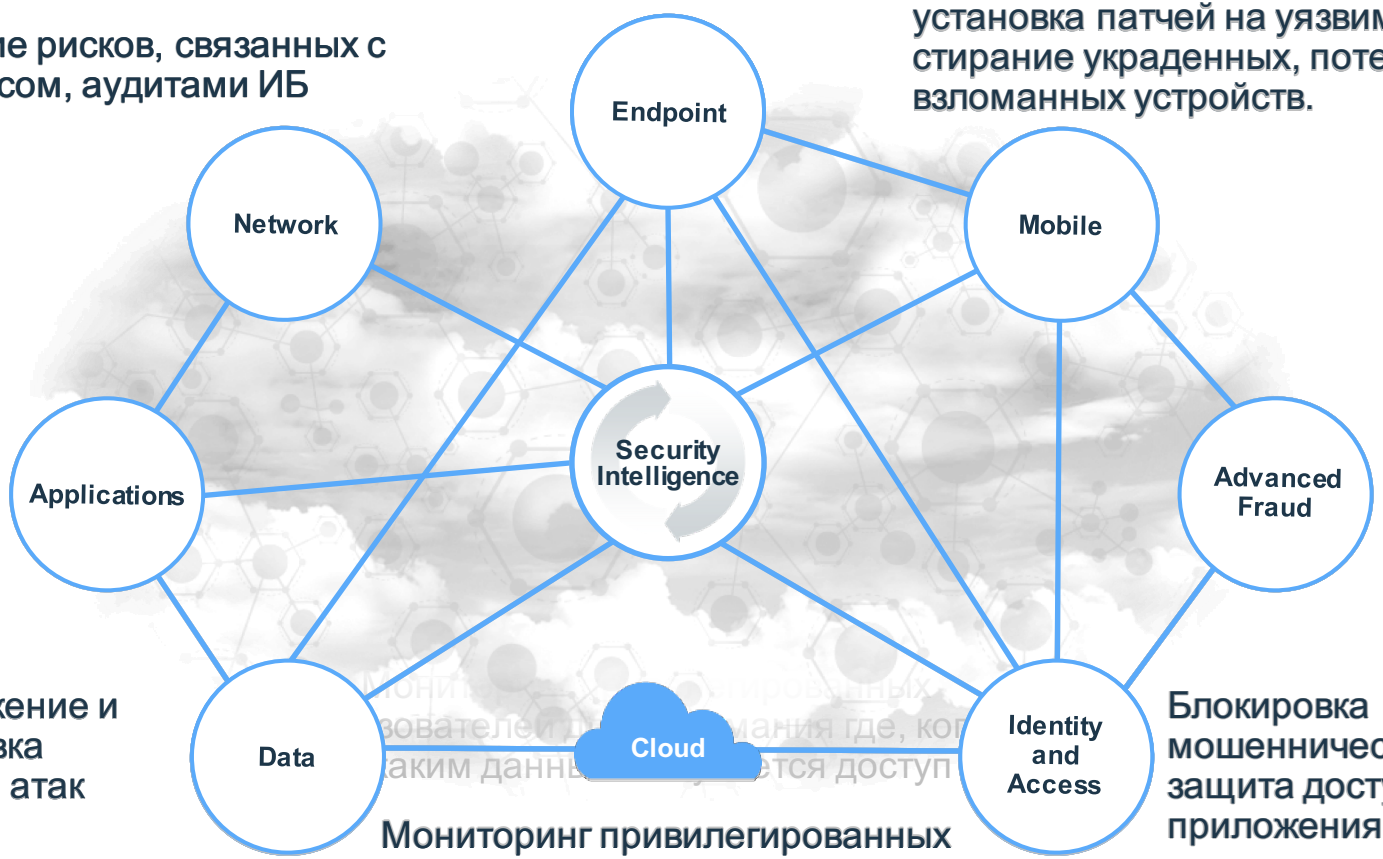
Лидерство в большом количестве сегментов позволяет взглянуть на проблему шире



Интегрированный подход позволяет оптимизировать общий уровень безопасности

Уменьшение рисков, связанных с комплайансом, аудитами ИБ

Детектирование вредоносного ПО, установка патчей на уязвимые места, стирание украденных, потерянных или взломанных устройств.



Обнаружение и блокировка сложных атак

Блокировка мошенничества и защита доступа к приложениям и данным

Мониторинг привилегированных Пользователей для понимания где, когда и каким данным получается доступ

Пример: Интеграция для обнаружения, предотвращения и блокировки инсайдерских атак

Польза от интеграции

Click to activate

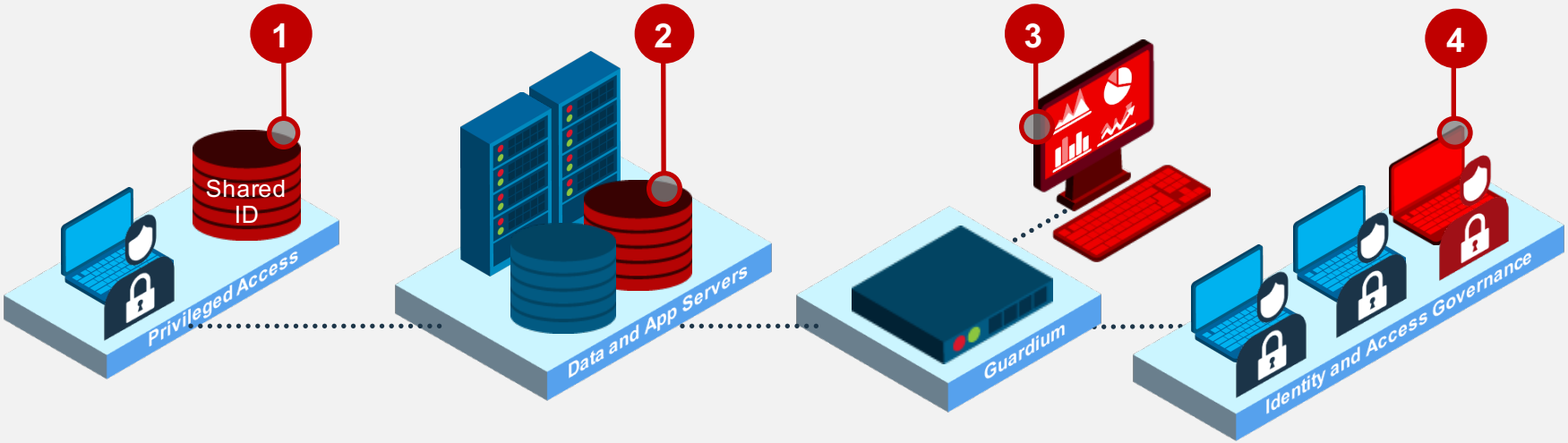
Предотвращение неавторизованного доступа

Детектирование инсайдерских угроз

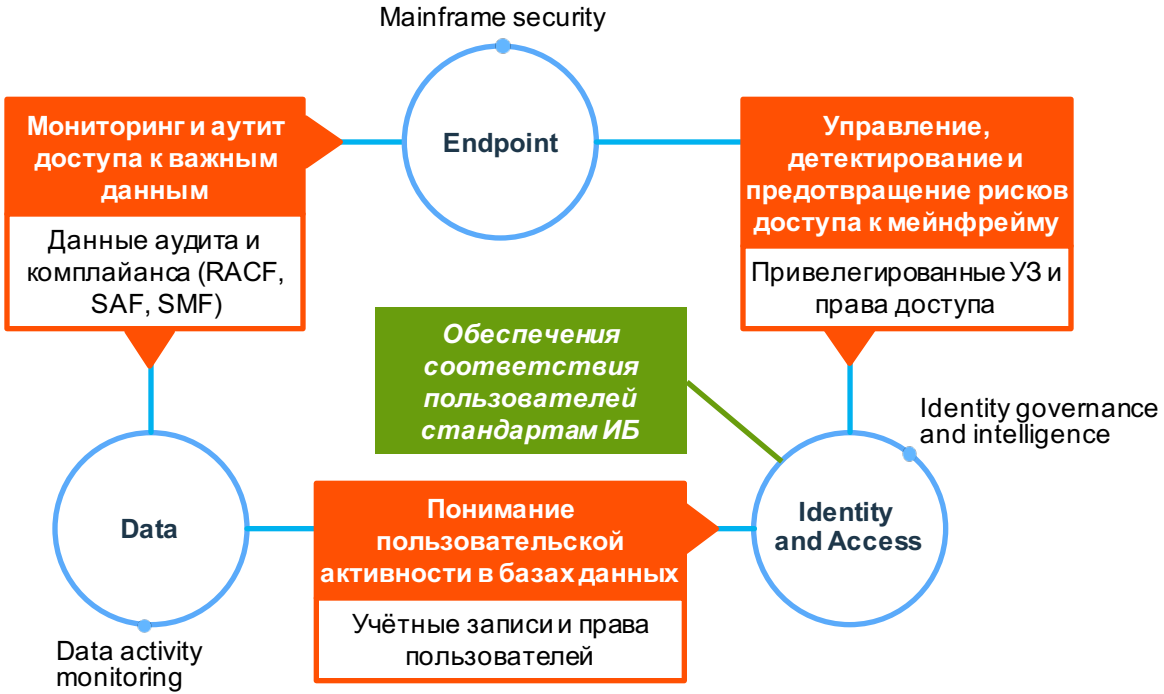
Блокирование незаконной активности пользователей

Пример: обнаружение инсайдерских атак и управление рисками

PRIVILEGED IDENTITY MANAGEMENT	ACTIVITY MONITORING	SECURITY INTELLIGENCE	IDENTITY GOVERNANCE
PIM предоставляет данные входа администраторов и Guardium может сопоставлять их с данными аудита активности СУБД	Guardium мониторит и аудирует доступ привелегированных пользователей к критичным данным в СУБД, и блокирует НСД к данным	QRadar коррелирует данные из PIM и Guardium для детектирования аномалий и оповещения для корректирующего воздействия	IGI проверяет на конфликты SoD и запускает компании по ресертификации для обеспечения актуальности привилегированных прав



Пример: Интеграция для управления уровнем соответствия стандартам и прохождения аудита



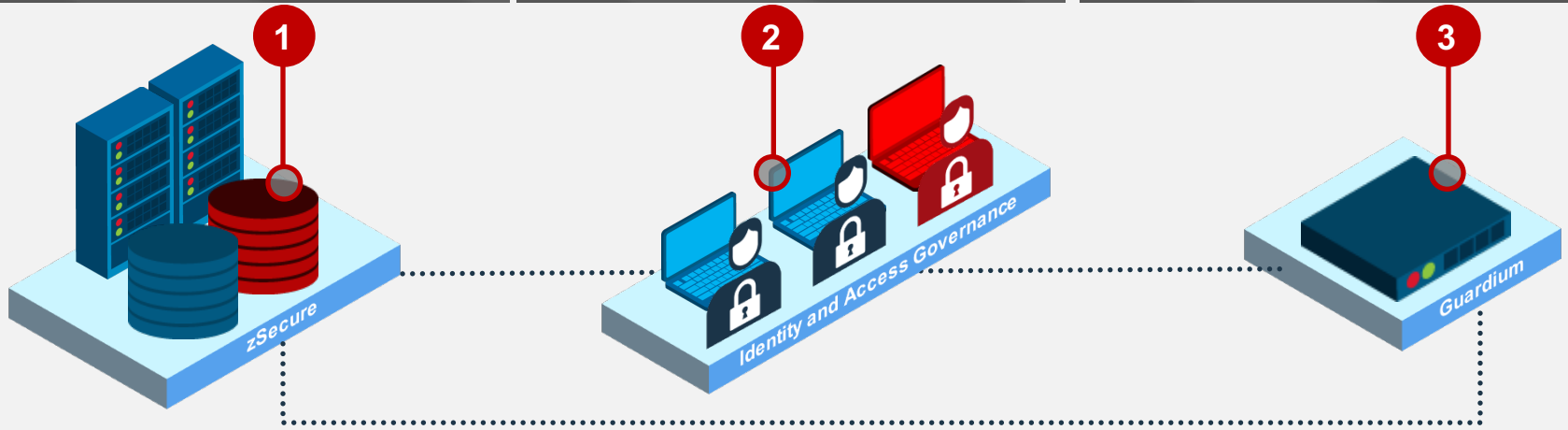
Польза от интеграции

Click to activate

- Безопасность критичных данных на уровне всей компании
- Обеспечение видимости доступа к данным
- Предотвращение риска неправомерного доступа к бизнес ресурсам

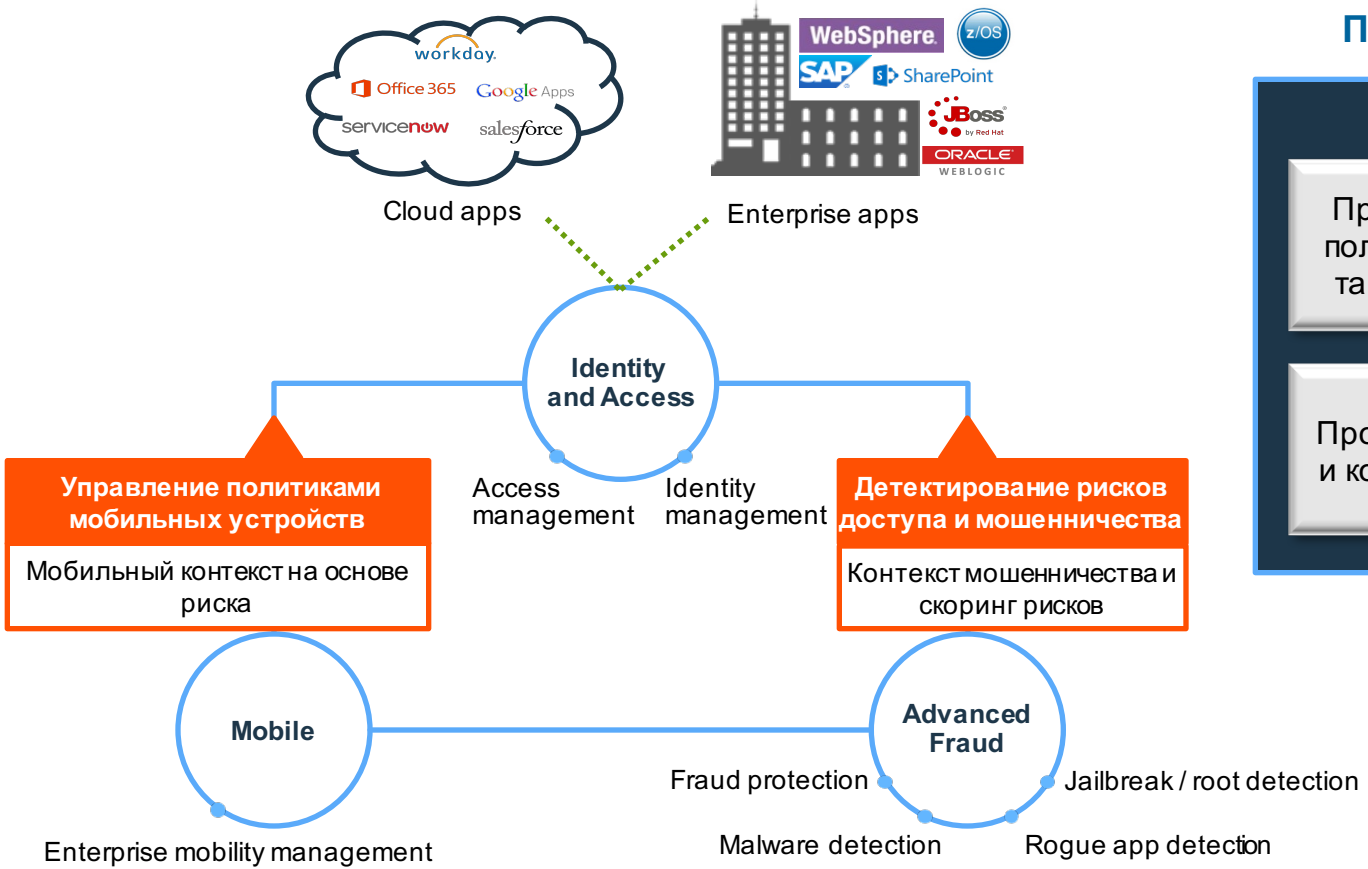
Пример: Прохождение аудита с identity governance

CROWN JEWEL PROTECTION	IDENTITY GOVERNANCE	ACTIVITY MONITORING



Комплекс zSecure расширяет управление комплайансом и отчётность для мейнфреймов для соответствия требованиям и обнаружения угроз.	IGI обеспечивает минимально необходимые привелегии доступа в СУБД, уменьшая риск неправомерного доступа к базам данных и мейнфреймам.	Guardium мониторит и аудирует активность привилегированных пользователей в режиме реального времени и дополняет zSecure audit collection and reporting для обеспечения полного видения.

Пример: Разграничение доступа к облачным ресурсам на основе уровня риска



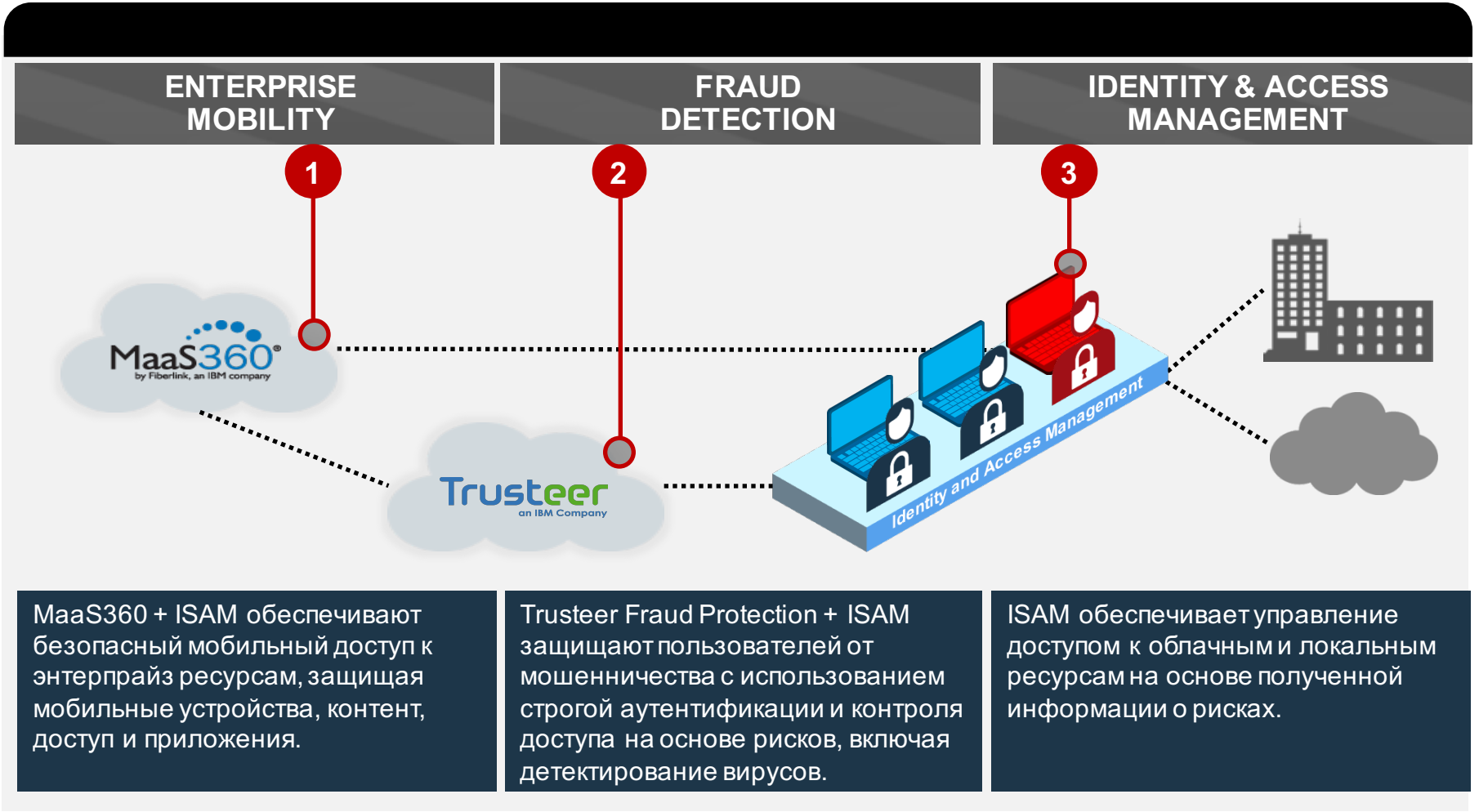
Польза от интеграции

Click to activate

Предоставление выполнения политик ИБ как для локальных так и для облачных ресурсов

Прозрачный доступ к облачным и корпоративным приложениям

Пример: безопасность доступа в эру облаков и мобильности



MaaS360 + ISAM обеспечивают безопасный мобильный доступ к энтерпрайз ресурсам, защищая мобильные устройства, контент, доступ и приложения.

Trusteer Fraud Protection + ISAM защищают пользователей от мошенничества с использованием строгой аутентификации и контроля доступа на основе рисков, включая детектирование вирусов.

ISAM обеспечивает управление доступом к облачным и локальным ресурсам на основе полученной информации о рисках.

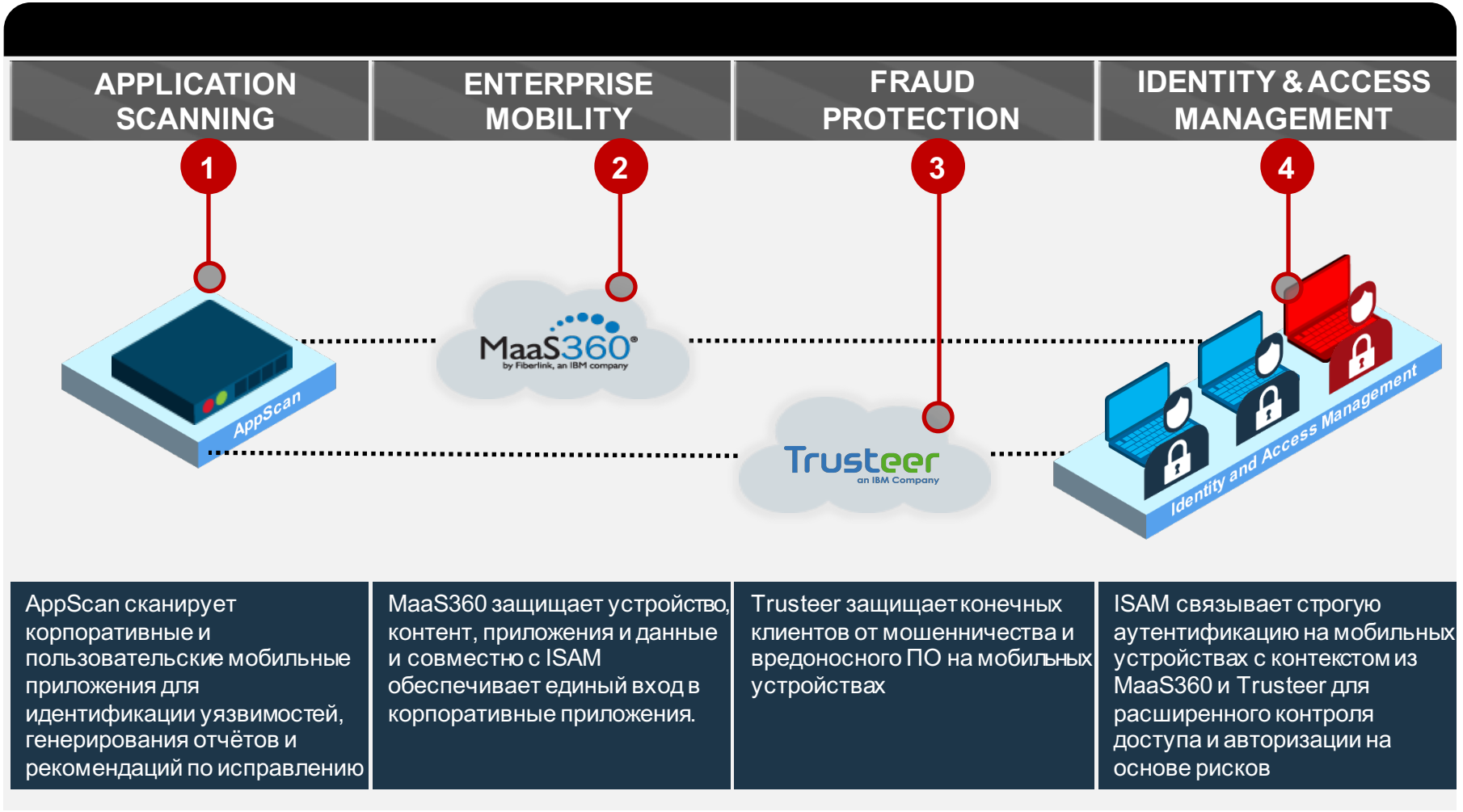
Пример: Интеграция для обеспечения безопасности мобилизации предприятия

Польза от интеграции

Click to activate

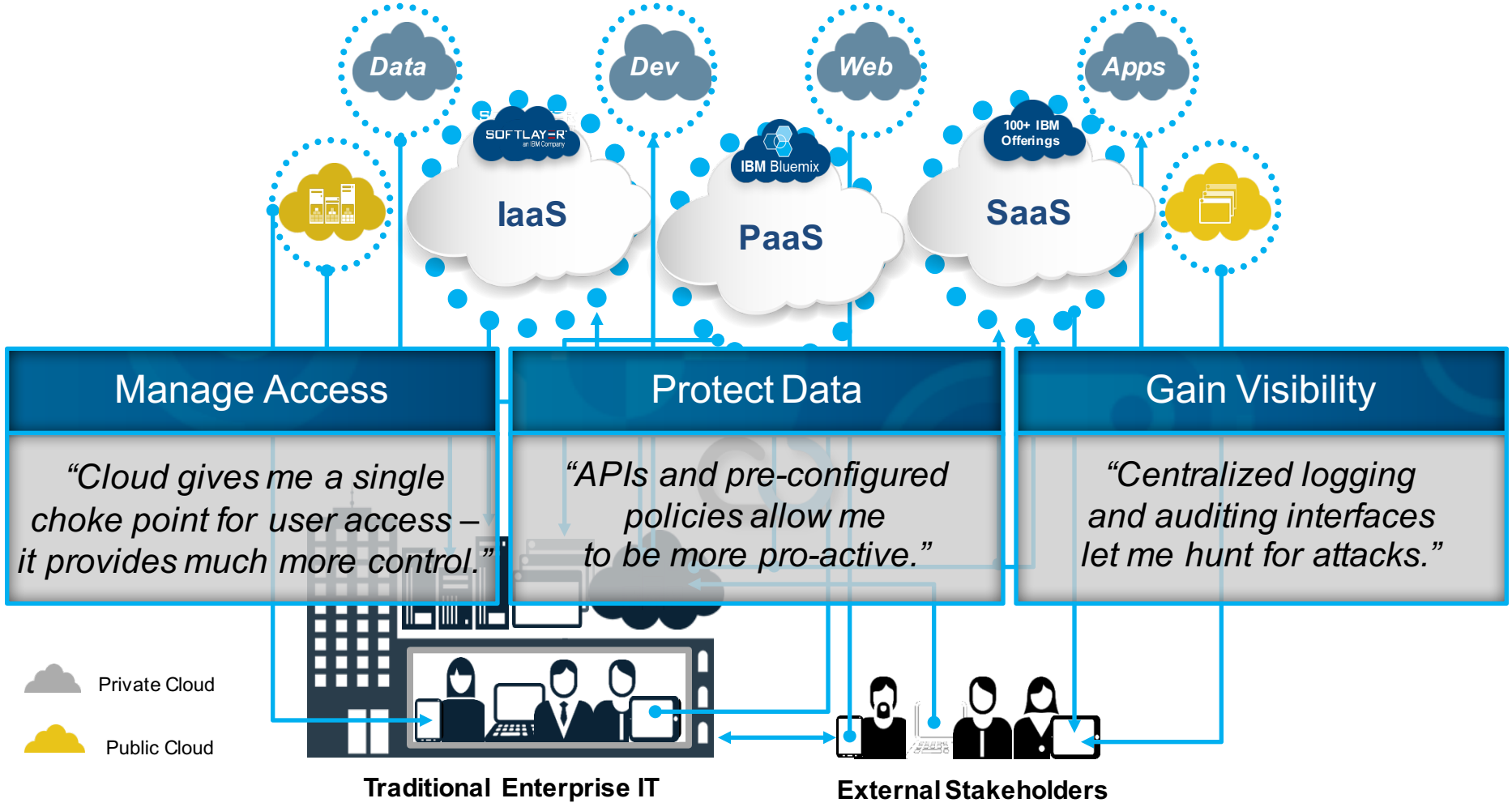
- Улучшение уровня мобильной безопасности
- Предоставление управления мобильными угрозами с учётом рисков
- Защита пользователей и организаций от мошенничества
- Простой доступ с мобильного к ресурсам компании

Пример: удаление барьеров на пути мобильной продуктивности

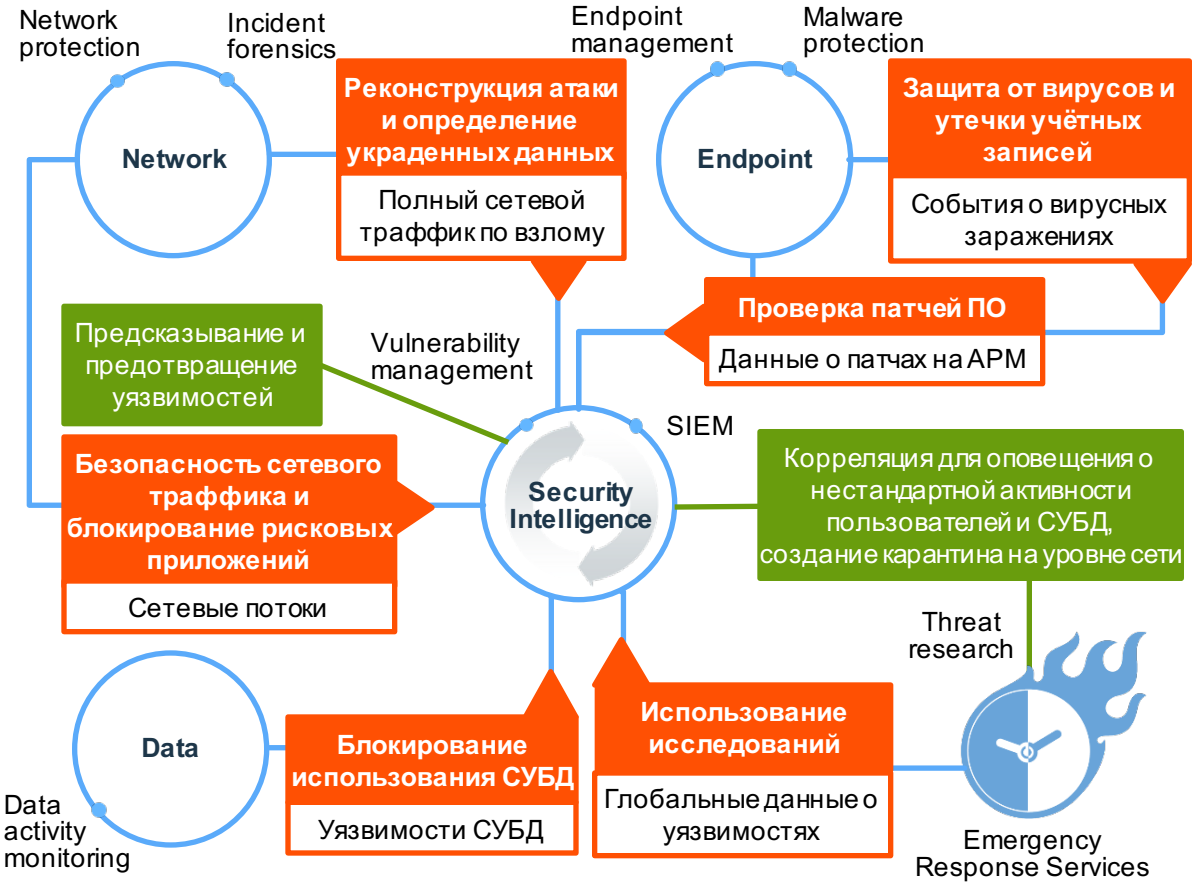


APPLICATION SCANNING	ENTERPRISE MOBILITY	FRAUD PROTECTION	IDENTITY & ACCESS MANAGEMENT
AppScan сканирует корпоративные и пользовательские мобильные приложения для идентификации уязвимостей, генерирования отчётов и рекомендаций по исправлению	MaaS360 защищает устройство, контент, приложения и данные и совместно с ISAM обеспечивает единый вход в корпоративные приложения.	Trusteer защищает конечных клиентов от мошенничества и вредоносного ПО на мобильных устройствах	ISAM связывает строгую аутентификацию на мобильных устройствах с контекстом из MaaS360 и Trusteer для расширенного контроля доступа и авторизации на основе рисков

The way to think about security for the cloud



Пример: Интеграция для блокирования APT атак



Польза от интеграции

Click to activate

Предотвращение

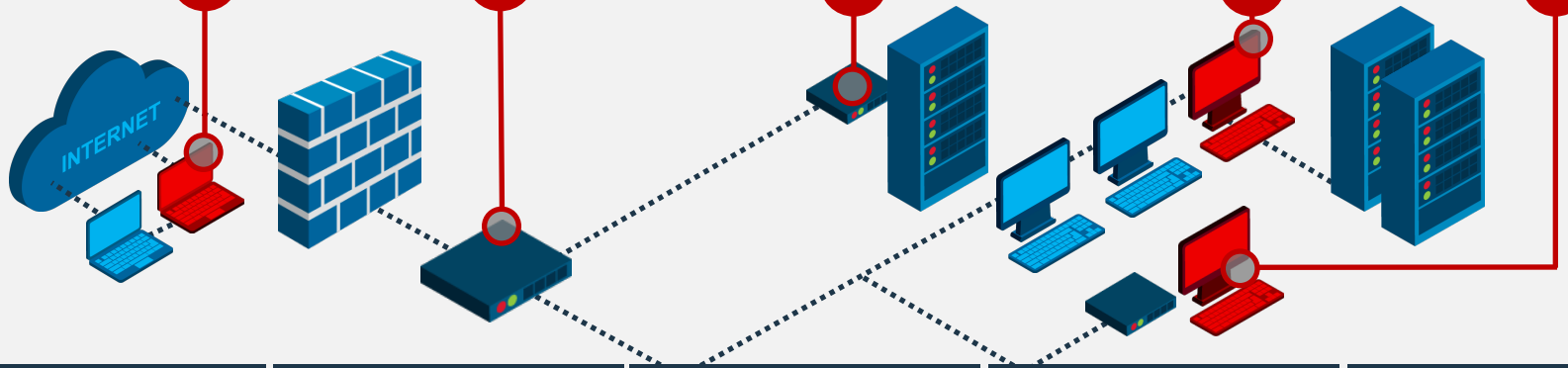
Детектирование

Ответная реакция

Example: Disrupt the attack chain in real-time

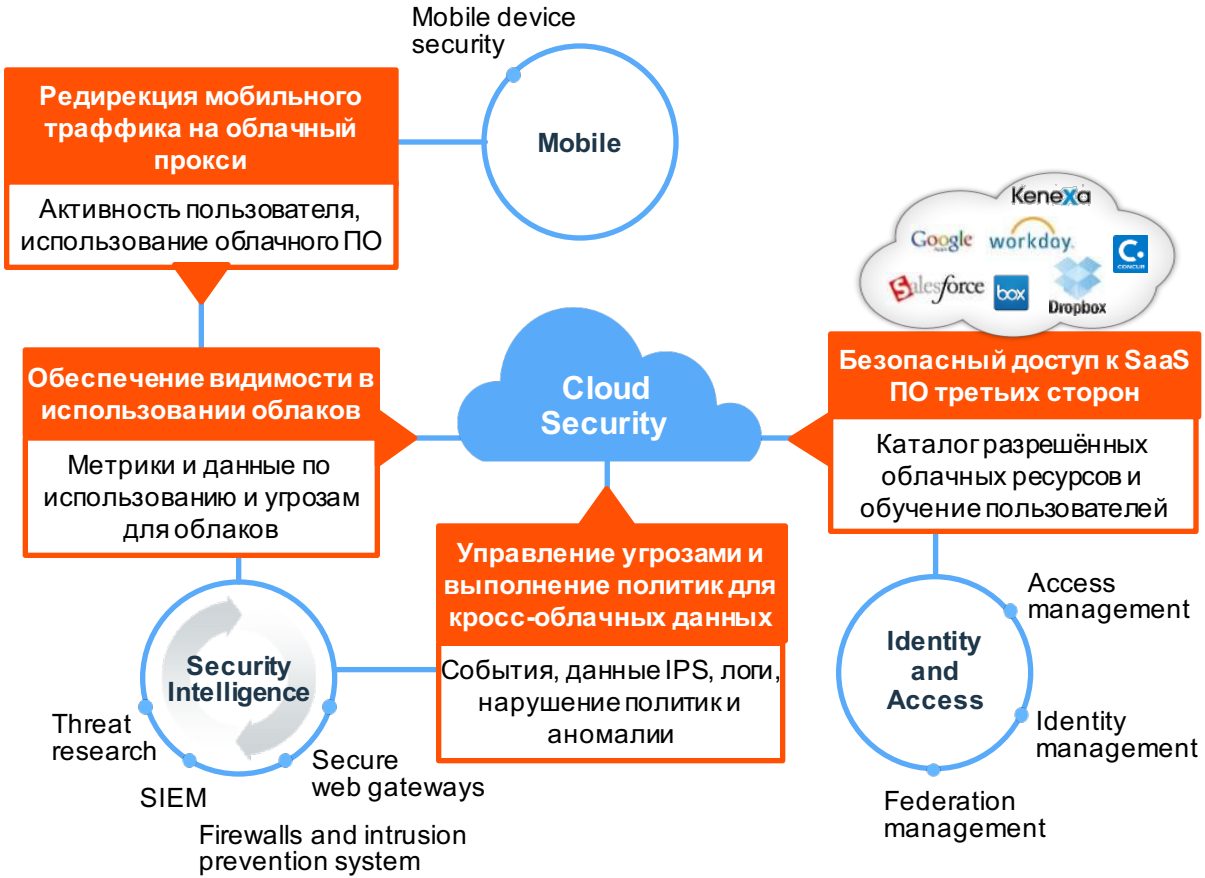
ATTACK CHAIN

1 BREAK-IN	2 LATCH-ON	3 EXPAND	4 GATHER	5 EXFILTRATE
Remote employee triggers drive-by download	Internal system infected as part of a botnet	Targeted internal email sent to high-profile employees	Authorized system attempts to access resources	Persistent attackers quietly siphoning out data



1 BREAK-IN	2 LATCH-ON	3 EXPAND	4 GATHER	5 EXFILTRATE
Apex prevents malware installation, sends event to QRadar for correlation, shares information to X-Force and XGS for corporate-wide network prevention	XGS blocks traffic with bad reputation and sends flows to QRadar for analysis	Third-party email security product detects the presence of a malicious attachment, shares events to QRadar and enforces a quarantine rule at the XGS	QRadar alerts on abnormal user and database activity from a targeted host	QRadar anomaly detection identifies infected machines, sends a quarantine rule to XGS for blocking, while incident forensics allows for analysis of stolen data

Пример: Интеграция для безопасного внедрения облачного доступа

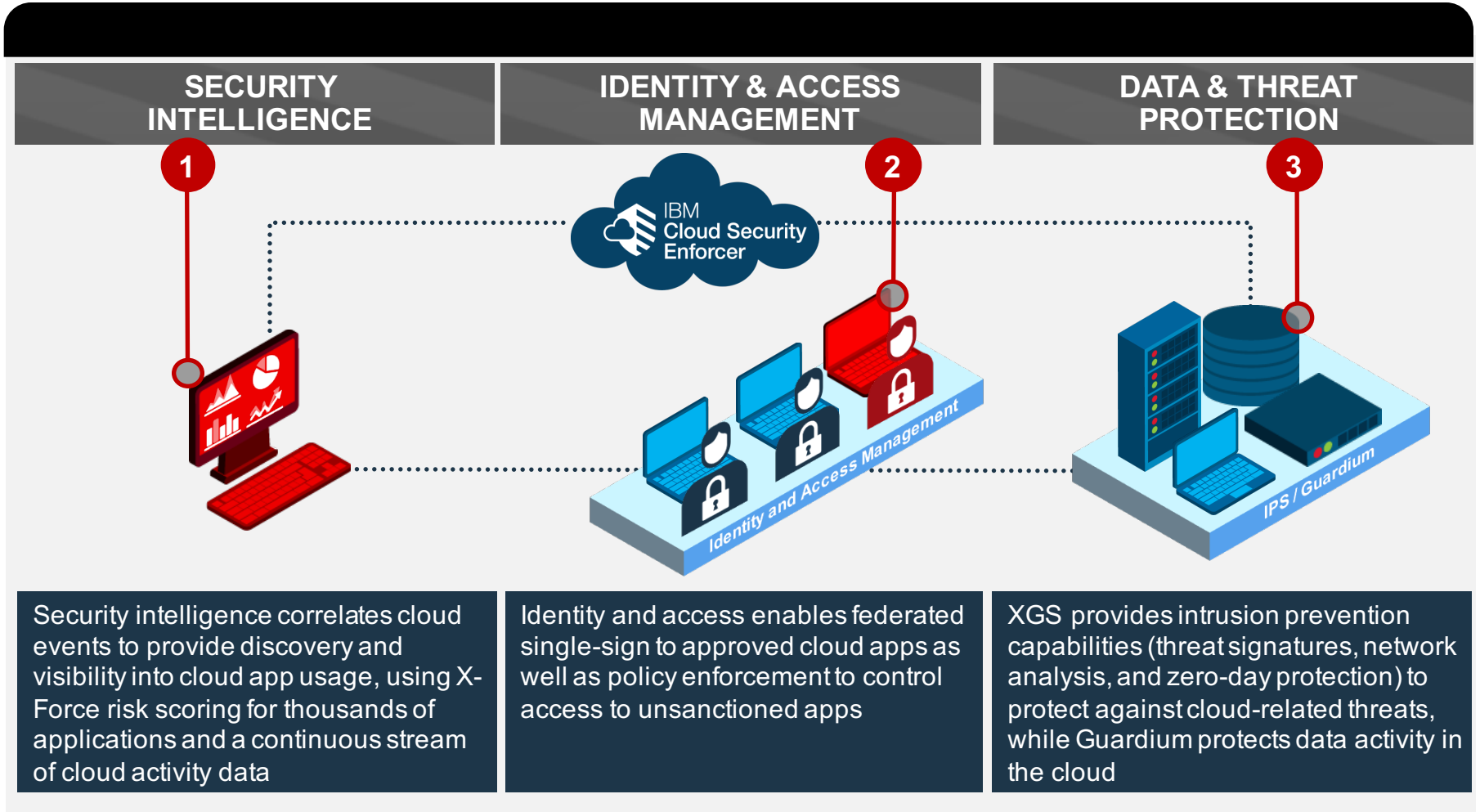


Польза от интеграции

Click to activate

- Обеспечение видимости на действия пользователей в облачном ПО
- Расширение контроля доступа и учётных записей на облачные приложения
- Корреляция облачных событий для предотвращения угроз и выполнения политик

Example: Help securely deploy cloud services



THANK YOU

www.ibm.com/security