

Подход к реализации Zero Trust

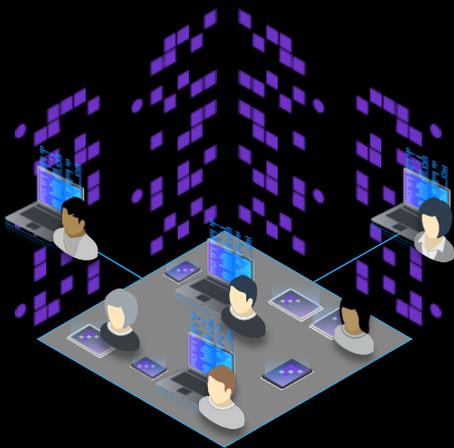
IBM Point of View

Эльман Бейбутов, CISSP

Руководитель по развитию бизнеса IBM Security Services

Elman.Beybutov@ibm.com

Бизнес определяет цифровую трансформацию



Пользователи и их устройства

Доступ из любой точки мира с любого устройства



Приложения и данные

Данные доступны огромному количеству пользователей и приложений



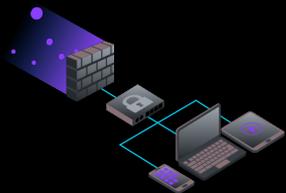
Гибридная инфраструктура

Сервера и сети располагаются как в собственных ЦОД, так и публичных облаках

... в итоге сложность снижает безопасность и доверие

Новые бизнес задачи и ИТ-трансформация требуют смены подхода обеспечения ИБ

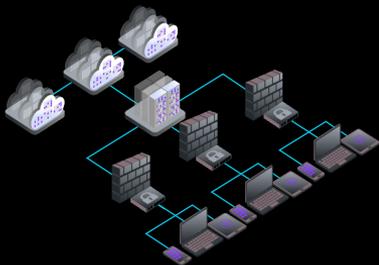
Централизованная архитектура



Многие-к-одному

Централизация данных
Выделенный периметр
Проводные сети
Наложенные СЗИ

Повышение эффективности при переходе в гибридные среды



Один-ко-многим

Распределенные данные
Множество периметров
Мобильные и Wi-Fi сети
Встроенные СЗИ

Акцент на скорость решения бизнес-задач



Многие-ко-многим

Данные повсюду
Периметр отсутствует
OT/IoT/IT конвергенция
Программные платформы ИБ

Предполагай
Доверие

Доверяй, но проверяй

Не доверяй
по умолчанию

Растущее разнообразие ИТ-среды приводит к экспоненциальной сложности системы безопасности

Необходимость реализации бизнес задач требует внедрения Zero Trust в ключевых направлениях

Сохранение конфиденциальности

Внедрение IDM/IGA
Управление полномочиями
Внедрение средств контроля при работе с данными

Снижение рисков от внутренних угроз

Доступ с наименьшими привилегиями
Выявление отклонений в поведении пользователей
Внедрение TI/TH



Безопасность в гибридных облаках

Управление и контроль доступа
Мониторинг активности и конфигураций облаков
Безопасность рабочих сред приложений

Безопасность удаленной работы

Реализация принципов BYOD
Уход от использования VPN
Внедрение методов аутентификации без пароля

“Zero trust helps us enable critical business capabilities while managing security”

- CISO, Global Chemical Manufacturer

Контекст критичен для Zero Trust

Предоставление
правильному пользователю
при **необходимых условиях**
правильного доступа
к **правильным данным**
в **правильное время**



Реализация Zero Trust: сфокусируйтесь на сценариях

Доступ к корпоративному гибриднему облаку из множества мест Повышение удобства удаленного доступа для сотрудников: <ul style="list-style-type: none">• Мобильные пользователи• Удаленные корпоративные офисы• Перевод сотрудников на работу из дома	Сервисные контракты Контрактники, обслуживающие промышленные объекты Представители вендоров и консультантов	Переход в облака CI/CD, приложения и инфраструктура	Интеграция нескольких облаков Связь между системами и управление распределенными инфраструктурами
	Коллаборация предприятий Взаимодействие B2B между организациями	IoT Производство IoT сенсоры Электромобили Умные сети Умные здания	BYOD Бизнес-пользователи, использующие личные устройства
	Привилегированный доступ к критической инфраструктуре Локальные или доменные учетные записи администратора, учетные записи служб	Компании с публичными и/или клиентскими сервисами B2C сценарии	

Четыре принципа для успешной реализации Zero Trust

Контекст определяет основу для внедрения Zero Trust

Выберите контекст

Определите пользователей, данные и ресурсы для создания контекст-ориентированных политик безопасности, согласованных с бизнесом.

Внедрите контроли

Защитите организацию, быстро и последовательно проверяя контекст и применяя политики.

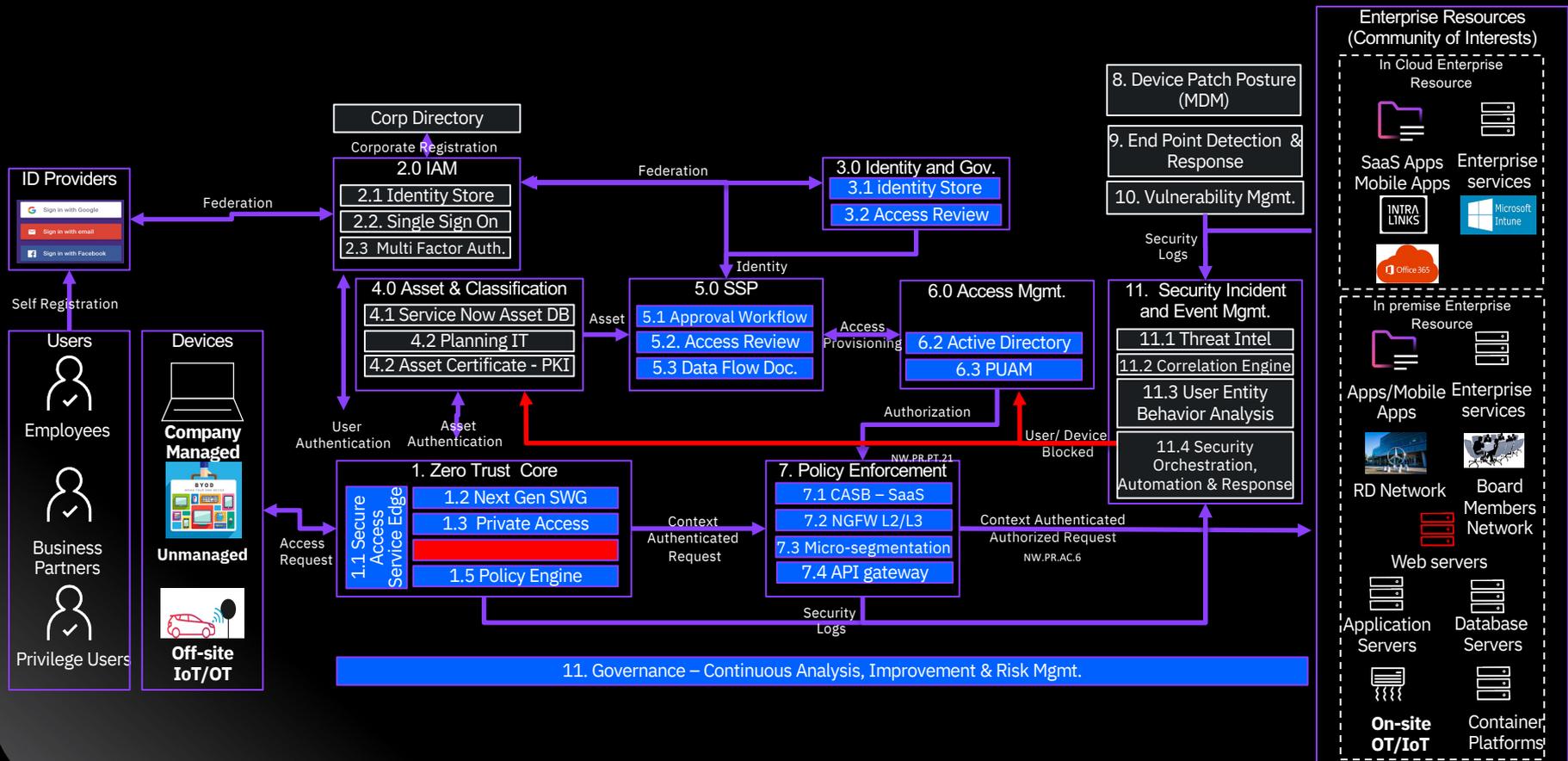
Реагируйте на инциденты

Устраняйте нарушения безопасности с минимальным воздействием на бизнес, предпринимая целенаправленные действия.

Анализируйте и улучшайте

Постоянно улучшайте положение в области безопасности, корректируя политику и практику для принятия более быстрых и обоснованных решений.

Референсная архитектура IBM Zero Trust



IBM обладает экспертизой, командой консультантов и решениями ИБ для реализации подхода Zero Trust

Align

Соответствие целей бизнеса задачам ИБ

Оценка | Приоритезация | Планирование

IBM Security Zero Trust Acceleration Services | IBM Security Risk Quantification Services

Protect

Защита данных, приложений и пользователей

IBM Security Implementation, Integration, and Support Services

Усиление аутентификации

- Контроль доступа
- Скоринг рисков
- Мультифакторная аутентификация

IBM Security Verify

Понимание рисков

- Безопасность устройств
- Обнаружение и классификация информационных активов
- Контроль обращения к данным

IBM Security MaaS360
IBM Security Guardium

Детектирование и реагирование

- Выявление новых угроз
- Мониторинг инцидентов
- Расследование
- Реагирование

IBM Security QRadar
IBM Security Resilient

Manage

Создание операционной модели непрерывного обеспечения ИБ

Modernize

использование платформенных решений ИБ

Открытая коллаборация | Интегрированные средства ИБ | Гибкое лицензирование функций ИБ

IBM Cloud Pak for Security



Создай цифровое доверие с Zero Trust

С чего начать?

Изучение

Изучите примеры сценариев Zero Trust и определите цели

Прочитайте больше об IBM Security и Zero Trust

<http://www.ibm.com/security/zero-trust>

Планирование

Определите стратегию Zero Trust для вашей компании

Создание стратегии по методике IBM Garage

<https://www.ibm.com/garage>

Реализация

Построение Zero Trust для выбранных сценариев и контекстов

Обсудите с экспертами IBM Security этапы запуска Zero Trust

<https://www.ibm.com/security/services/zero-trust>

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. 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. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. 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 any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.