CHECK POINT

Никому не доверяй
Проверяй вместе с нами
Zero trust!

Сергей Чекрыгин
schekrygin@checkpoint.com
+7 985 136 4356

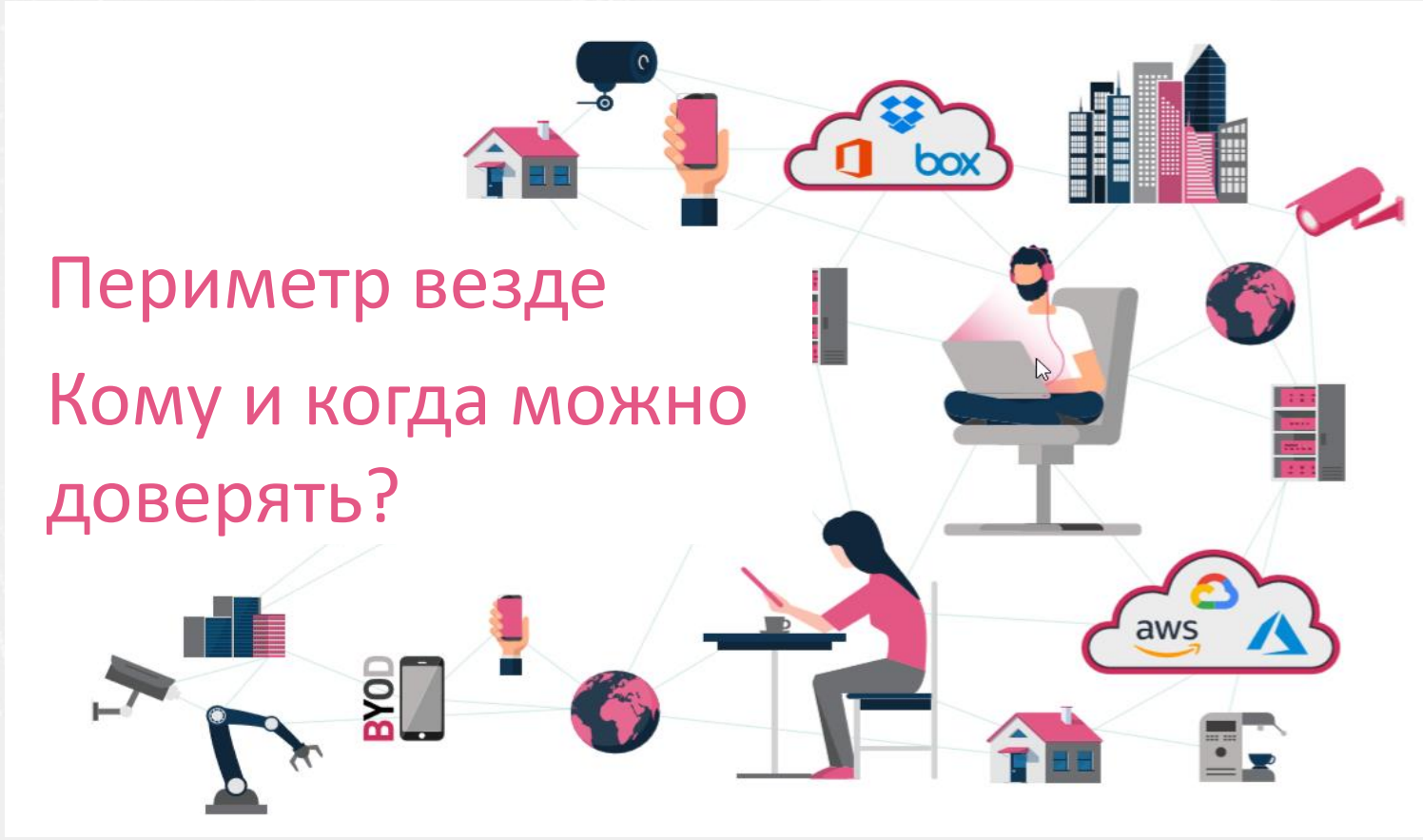
YOU DESERVE THE BEST SECURITY

ПЕРИМЕТР РАЗМЫВАЕТСЯ

Традиционный подход

Внутри периметра можно доверять всем

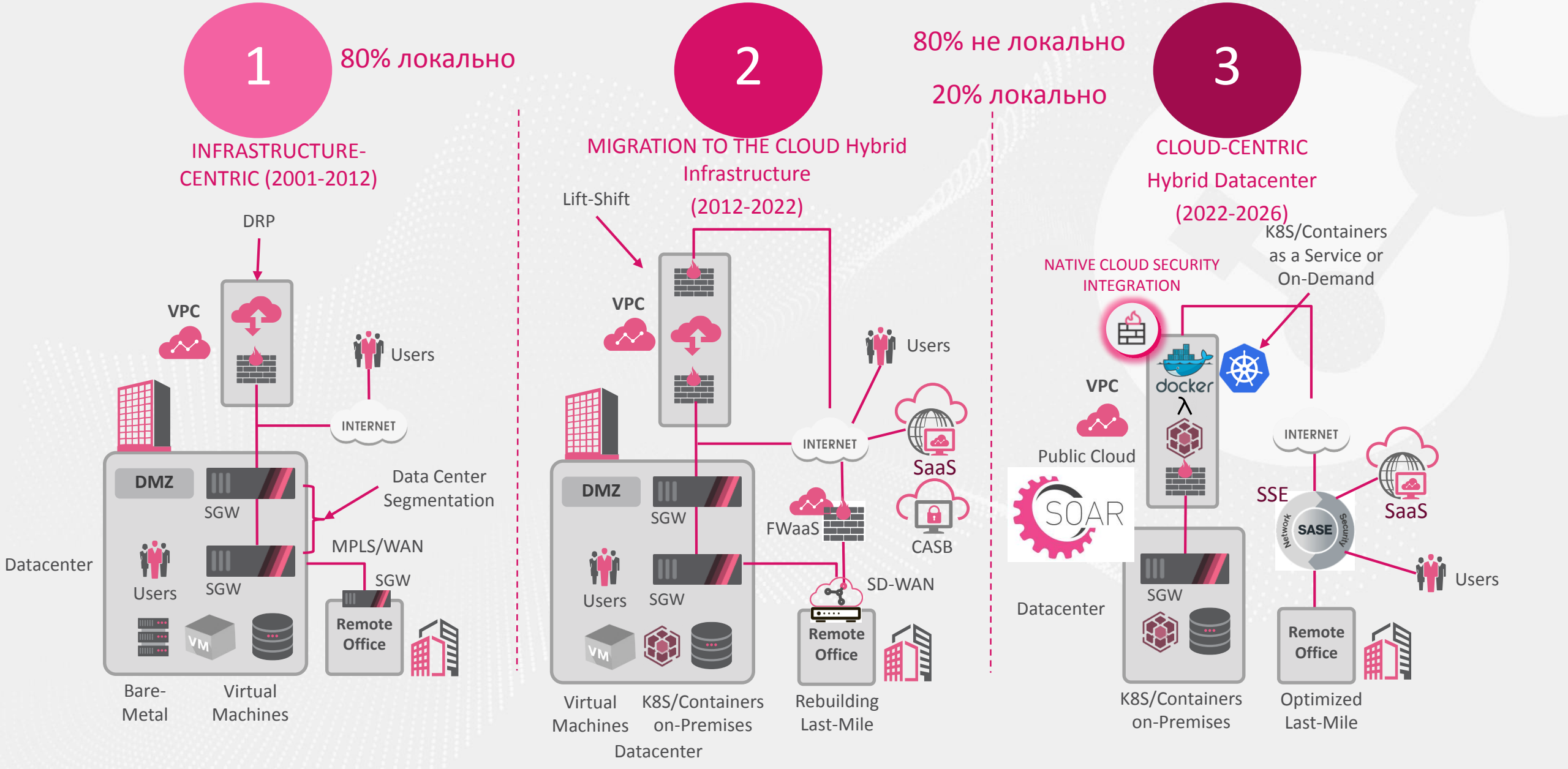
Современные реалии



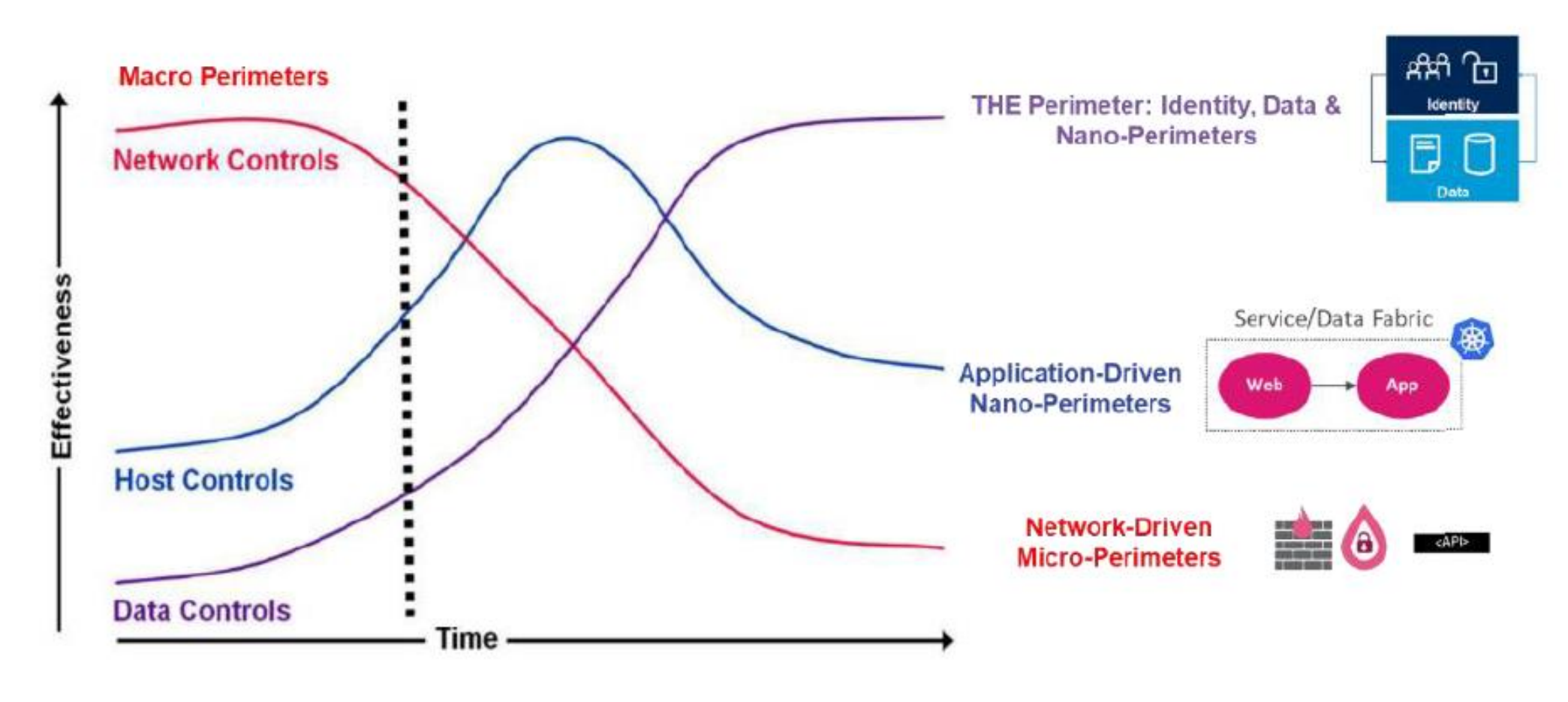
Периметр везде

Кому и когда можно доверять?

Цифровая трансформация и архитектура безопасности

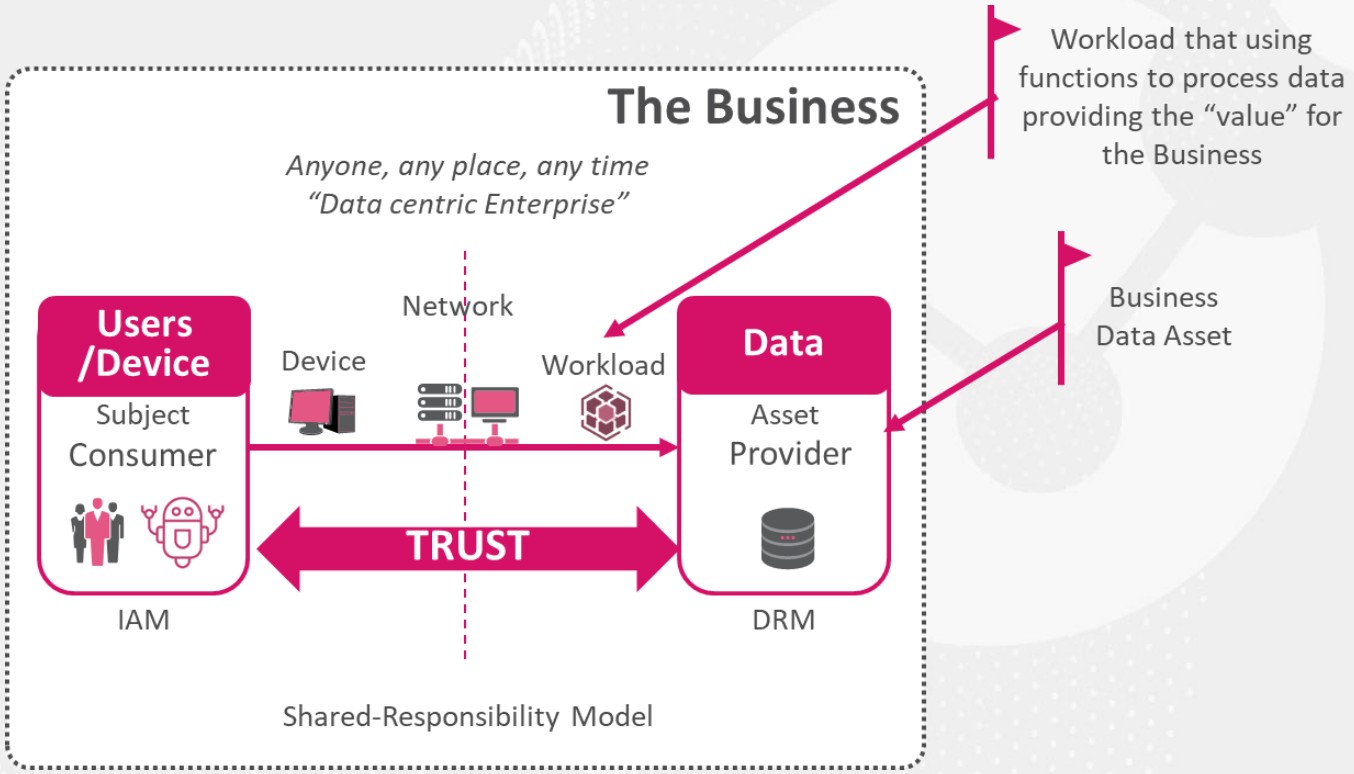


Эффективность защит при цифровой трансформации



Путешествие к архитектуре Zero-Trust

- Цифровая трансформация про **Взаимодействие и Доверие**
- Концепция Zero-Trust – это корректная реализация принципа **минимальных привилегий.** Без этого **доверие** становится основной уязвимостью
- Традиционный подход: доверяй, но проверяй
- Zero Trust: никому не доверяй, всегда проверяй



Зрелость архитектуры Zero-Trust

Phase 1: Traditional or Implicit Trust

- Static Identity Policies,
- Identity, Networking, Infrastructure are silos.
-Only Macrosegments in place.
- Friction between Business Units due to the lack of integration.

Phase 2: Advanced or Contextual Trust:

-Context Aware security policies in place.

-Business areas & Information Security are integrated.

-Data Classification in place and implemented.

- Macro segmentation & Micro segmentation implemented for critical systems.

Phase 3: Optimal or Explicit Trust

-Least-Privilege Principle in place

-Business-Driven Policies with CNAPP

-Dynamic Access-Control according with the Risk and Security Posture.

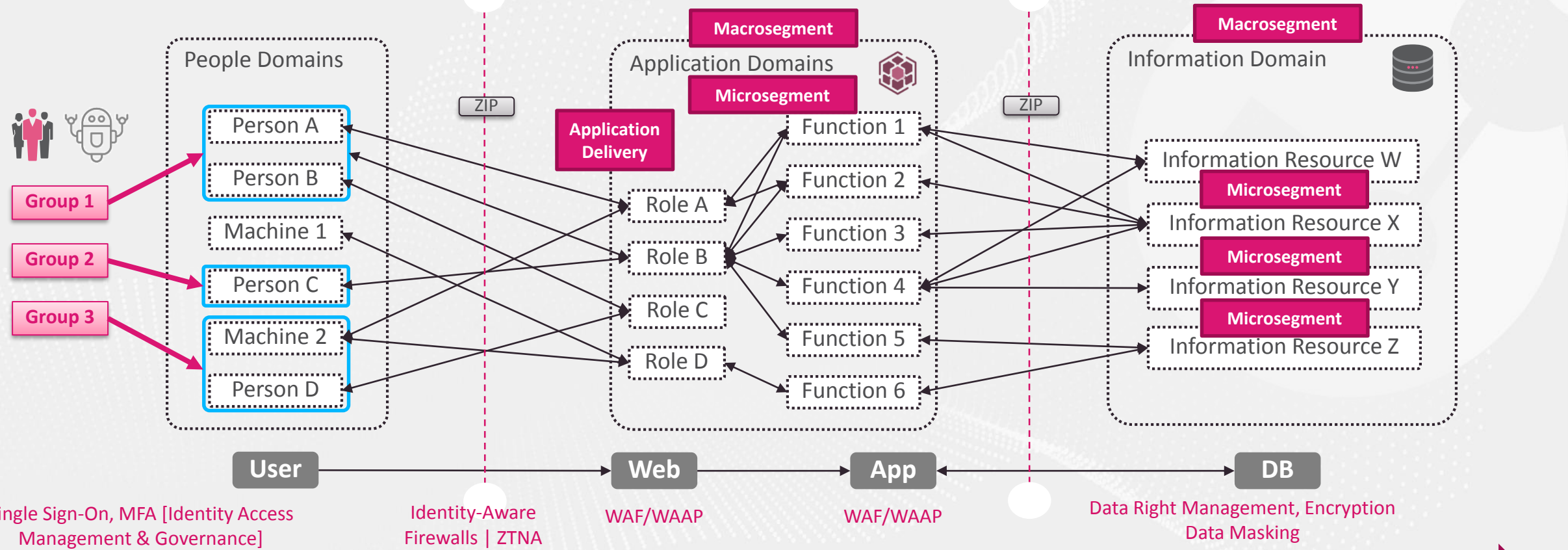
-API-Driven Policies being Agile

-Macro, Micro and Nano segmentation in place for Hybrid Cloud and Applications

-Strong CI/CD Security for Software Supply Chain.

Неявное доверие → Условное доверие → Явное доверие

Путешествие в Zero trust – Люди, приложения, данные



Неявное доверие — Условное доверие — Явное доверие

Sources: Forrester ZTX & Enterprise Security Architecture: Business Approach, John Sherwood

Зрелость архитектуры Zero-Trust

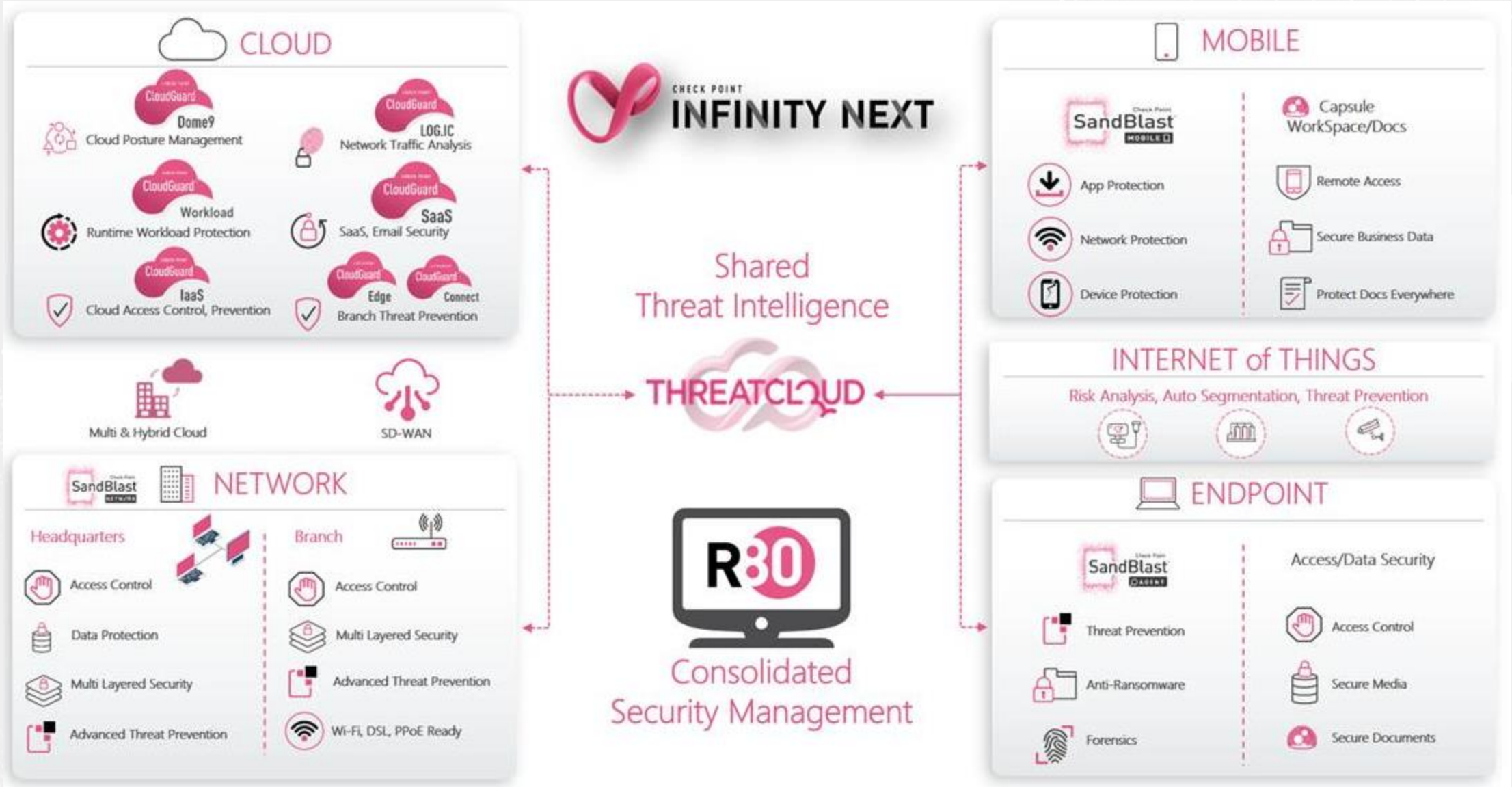
1. Неявное доверие. Базируется на предположениях, что можно доверять без явной проверки или доказательства. Статические политики доступа. Нет таблиц доступа.
2. Контекстное доверие. Доступ предоставляется при некоторых (разнообразных) условиях.
3. Явное доверие. Базируется на проверке и доказательстве во всех случаях. Верификация пользователя, устройства, условий работы, ИТ сервиса, данных. Динамические привилегии.

Новый периметр

1. Сеть. Сетевой периметр, идентификация пользователей и контроль приложений
2. Нагрузка. Микросегментация, контроль внутреннего трафика, определение и автоматическое исправление конфигураций, адаптивные политики, интегрированные со средствами автоматизации
3. Пользователи. SSO, MFA, проверка контекста (compliance), поиск аномалий
4. Устройства. Инспекция устройства или его трафика, динамические политики
5. Данные. Шифрование данных и трафика
6. Отчётность и аналитика.
7. Автоматизация работы администратора ИБ и расследователей инцидентов.

CHECK POINT INFINITY

Архитектура безопасности с Zero Trust



Полная безопасность с нулевым доверием с CHECK POINT INFINITY

1 **Полнота**

Все принципы Zero Trust

2 **Эффективность**

Централизованное управление с единой консолью и унифицированными политиками

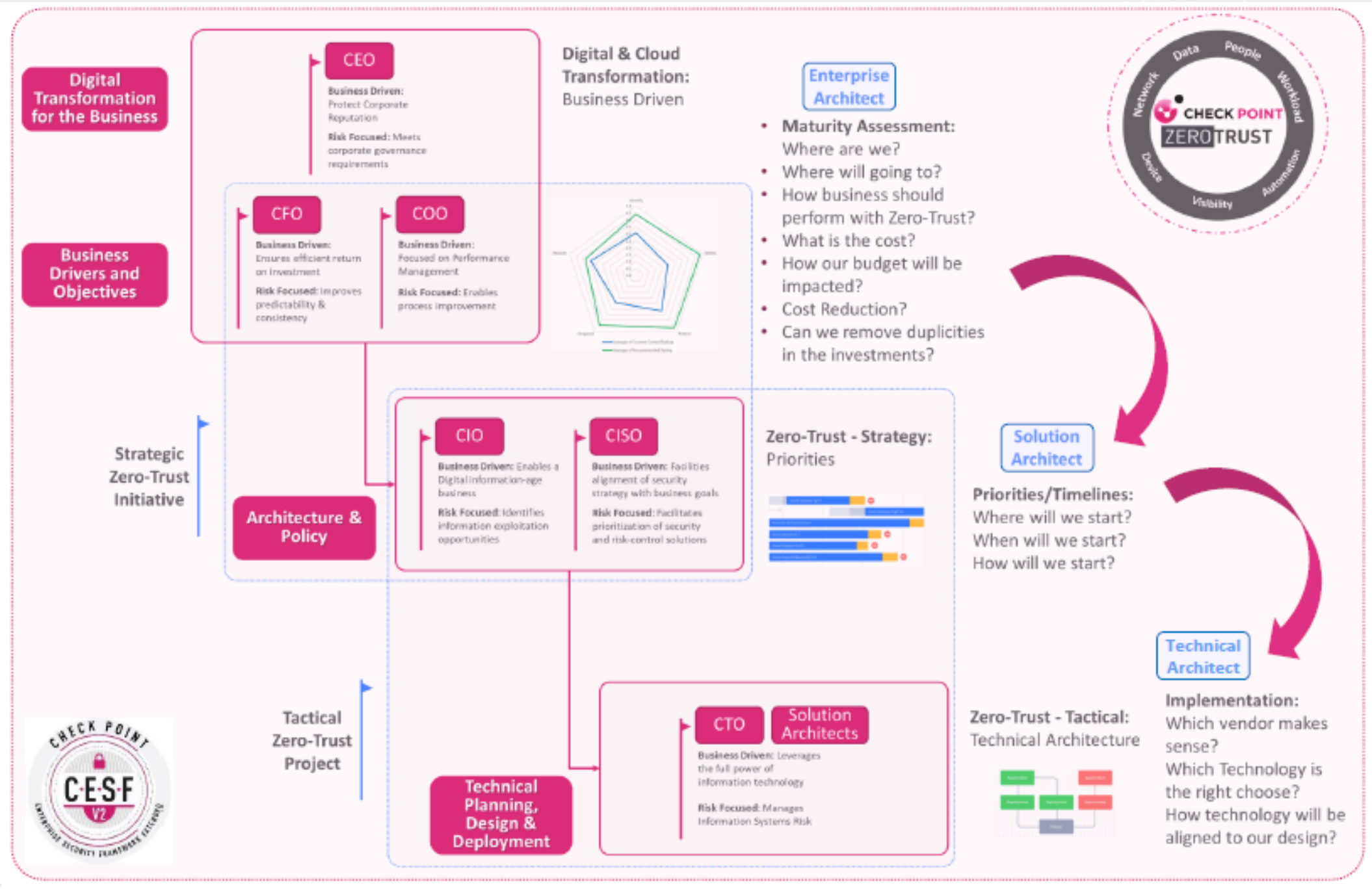
3 **Предотвращение**

Внимание на предотвращение и защиту от неизвестных угроз

Реализация проекта внедрения Zero Trust

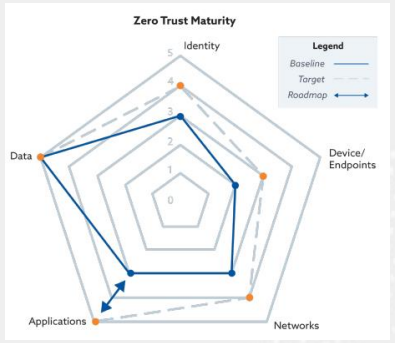
- Внедрение Zero Trust болезненно для любой организации.
- Внедрение Zero Trust обеспечивает цифровую трансформацию и должно быть согласовано с ней по целям

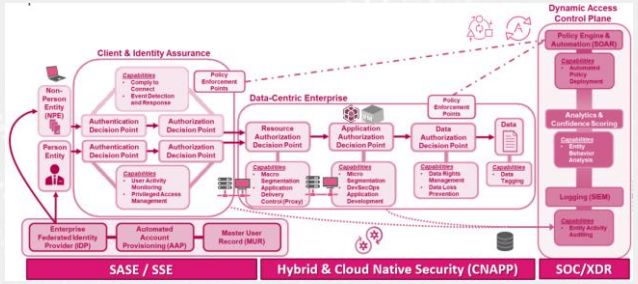
1. Формулирование целей проекта Zero trust с конкретными желаемыми результатами
2. Аудит имеющихся средств безопасности
3. Определение заинтересованных лиц и лиц, которые будут затронуты изменениями
4. Разработка плана изменений
5. Обсуждение и обучение по предполагаемым изменениям
6. Тестирование предполагаемых изменений
7. Мониторинг и настройка изменений

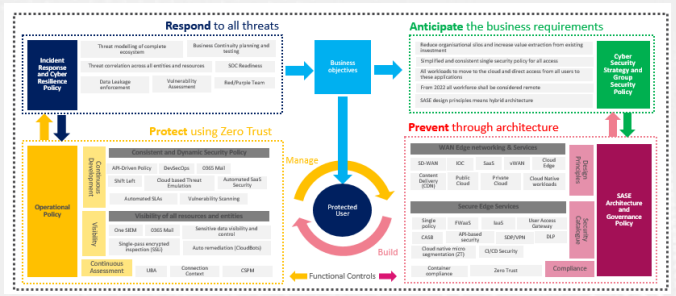

Digital Transformation for the Business
Business Drivers and Objectives
Strategic Zero-Trust Initiative
Tactical Zero-Trust Project
CEO
Business Driven: Protect Corporate Reputation
Risk Focused: Meets corporate governance requirements
CFO
Business Driven: Ensures efficient return on investment
Risk Focused: Improves predictability & consistency
COO
Business Driven: Focused on Performance Management
Risk Focused: Enables process improvement
Architecture & Policy
CIO
Business Driven: Enables a Digital information-age business
Risk Focused: Identifies information exploitation opportunities
CISO
Business Driven: Facilities alignment of security strategy with business goals
Risk Focused: Facilitates prioritization of security and risk-control solutions
Technical Planning, Design & Deployment
CTO
Solution Architects
Business Driven: Leverages the full power of information technology
Risk Focused: Manages Information Systems Risk
Digital & Cloud Transformation: Business Driven
Enterprise Architect
Maturity Assessment:
Where are we?
Where will going to?
How business should perform with Zero-Trust?
What is the cost?
How our budget will be impacted?
Cost Reduction?
Can we remove duplicities in the investments?
Zero-Trust - Strategy: Priorities
Solution Architect
Priorities/Timelines:
Where will we start?
When will we start?
How will we start?
Zero-Trust - Tactical: Technical Architecture
Technical Architect
Implementation:
Which vendor makes sense?
Which Technology is the right choose?
How technology will be aligned to our design?
CHECK POINT ZERO TRUST
Network
Data
People
Workload
Automation
Visibility
Devices
CHECK POINT C·E·S·F V2

Check Point Zero Trust Workshop

Оценка







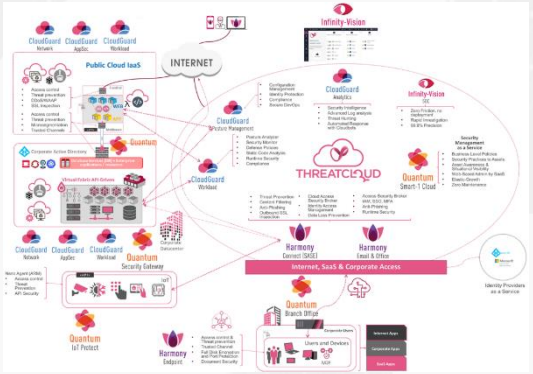
Отчёт

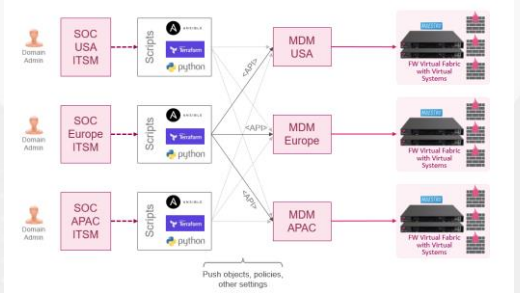
CHECK POINT™

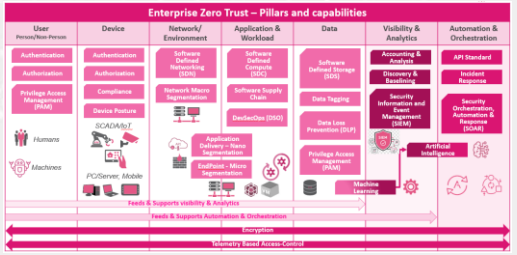
Zero Trust Workshop Report

Prepared for Check Point Customer
on
01 December 2022
Global Enterprise Security
Architecture team

Архитектура







CHECK POINT™

Спасибо

Сергей Чекрыгин
schekrygin@checkpoint.com
+7 985 136 4356

YOU DESERVE THE BEST SECURITY