Metaverse x Security:

Unravelling essential trade-offs in Web 3.0

Nicolas Stichel & Laura Selbach

DETECON
CONSULTING

Agenda:

1

Web 3.0 and it’s novel challenges

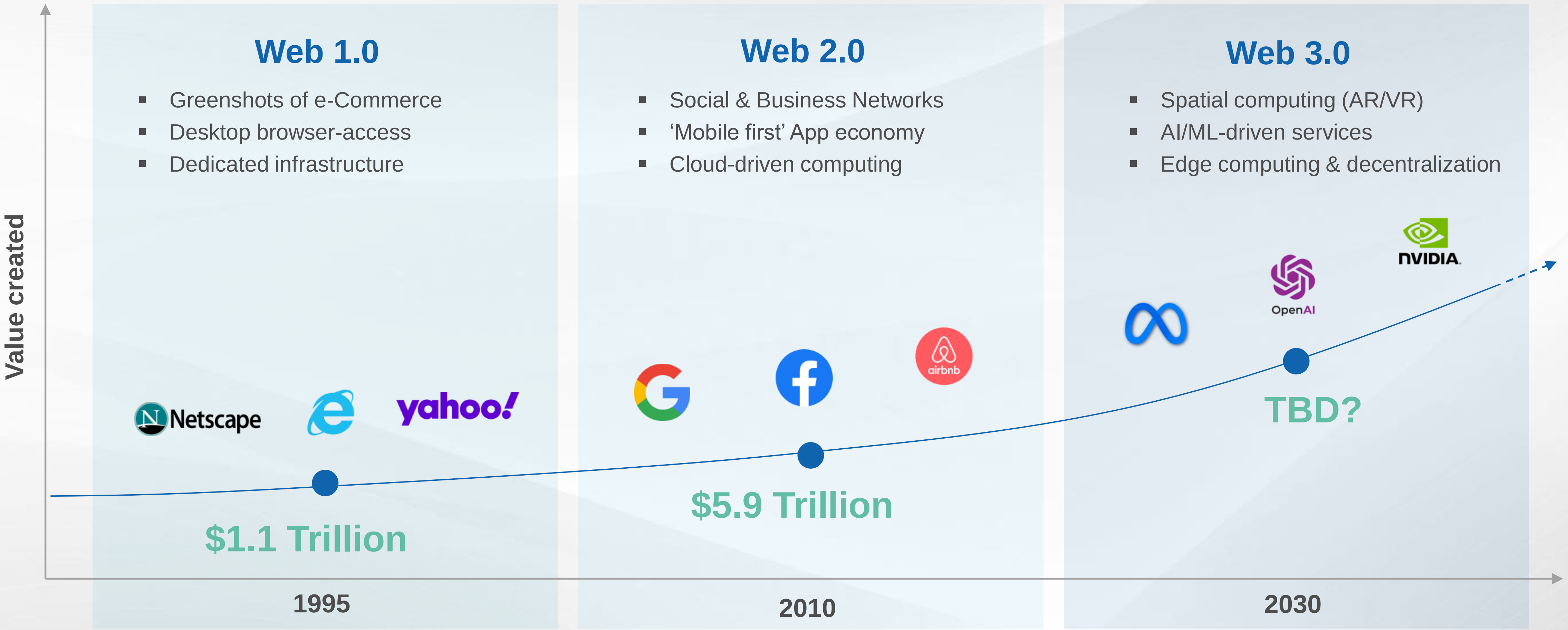
2

Enabling new tech in secure environments

3

Case Study: Remote Rendering

The Web has become increasingly valuable and pervasive over time. Web 3.0 is the next step on its evolutionary trajectory.



Web 1.0

- Greenshots of e-Commerce
- Desktop browser-access
- Dedicated infrastructure

Web 2.0

- Social & Business Networks
- ‘Mobile first’ App economy
- Cloud-driven computing

Web 3.0

- Spatial computing (AR/VR)
- AI/ML-driven services
- Edge computing & decentralization

Source: Fabric Ventures, 2023 adapted by Detecon

DETECON
CONSULTING

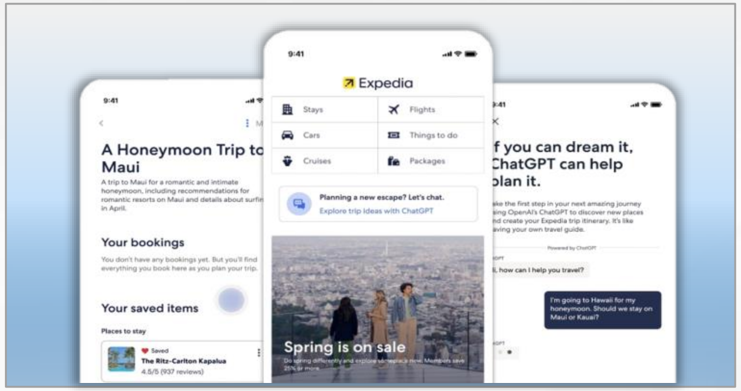
1

Web 3.0: Metaverse Apps & Generative AI are creating a real impact on our economy already. Yet they create new challenges.

Digital Factory Twin

Autonomous Driving

Travel Planning with GenAI



A Honeymoon Trip to Maui

A trip to Maui for a romantic and intimate honeymoon, including recommendations for romantic resorts on Maui and details about surfin in April.

Your bookings

You don't have any bookings yet. But you'll find everything you book here as you plan your trip.

Your saved items

Places to stay

The Ritz-Carlton Kapalua

4.5/5 (937 reviews)

Planning a new escape? Let's chat.

Explore trip Ideas with ChatGPT

Spring is on sale

Do spring differently and explore someplace new. Members save 25% or more.

f you can dream it, ChatGPT can help plan it.

ake the first step in your next amazing journey sing OpenAI's ChatGPT to discover new places nd create your Expedia trip itinerary. It's like aving your own travel guide.

Powered by ChatGPT

i, how can I help you travel?

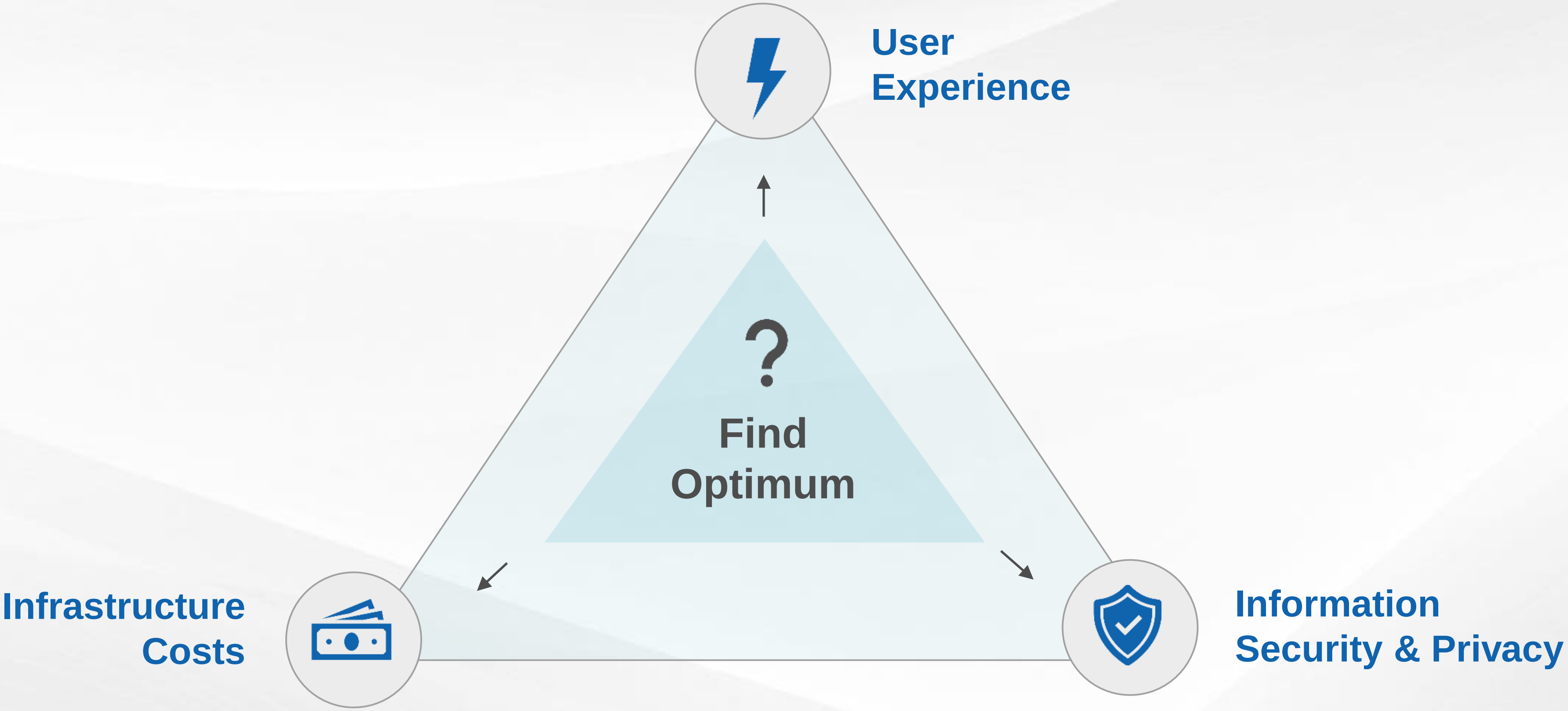
I'm going to Hawaii for my honeymoon. Should we stay on Maui or Kauai?

Aggregation of critical data requires utmost security.

New applications demand lower latencies / higher UX.

GPU infrastructure leads to higher costs.

Within the Web 3.0 ecosystem, the quest to find an optimal tradeoff between cost, UX and security / data privacy is getting increasingly challenging.



User Experience

Find Optimum

Infrastructure Costs

Information Security & Privacy

Why to differentiate between Metaverse, GenAI & mixed use-cases?

New opportunities come along with new threats.

Risk vectors and consequences remain similar, the focus and likelihood may however change.

The **metaverse**:

- refers to a virtual universe or **interconnected network** of virtual worlds
- interact through **immersive technologies** such as VR or AR
- reality extension of the physical world, enabling users to have a **persistent presence and interact with digital content** and other participants

Generative **Artificial Intelligence**:

- intelligent machines **capable of performing tasks** that would typically require human intelligence
- **perceive their environment, reason, learn**, and make decisions or take actions to achieve specific goals
- **machine learning**, natural language processing, computer vision, robotics, and more to **automate processes, improve efficiency,** and solve complex problems

Metaverse

Focus on information security, access and data provisioning. Focus on optimization between performance optimization and information hubs or joints

GenAI

AI must be properly and fully trained. Challenge on how to predefine the scope of data usage and potential outcomes

Metaverse

Data protection concerns (GDPR) mainly in B2C use-cases. Solved through sufficient pseudonymization without limiting the user experience

GenAI

Discussions on reliability and accountability if AI is allowed to make decisions. Data protection concerns as user experience may differentiate on user identity

Multitude of hubs, real-time rendering and the risk with high precision

Challenges and related risks from implementing metaverse in businesses collect around the business functions.

Multitude of hubs:

- Securely bring processing capacity into a running organization
- Differentiation on which type of data is allowed to be processed
- Definition of use-cases may vary over time and hence allowances must be accurately adapted

Real-time rendering and interfaces:

- Assess data being processed and identify vulnerabilities and risk vectors, especially live-manipulation
- Implementing zero-trust on connectors like VR-lenses

High precision information:

- Information is a lot more precise than being described in words in a confidential document
- Successful espionage or data leakage may rapidly increase risk vectors

How can we ensure that AI identifies an object as what it is?

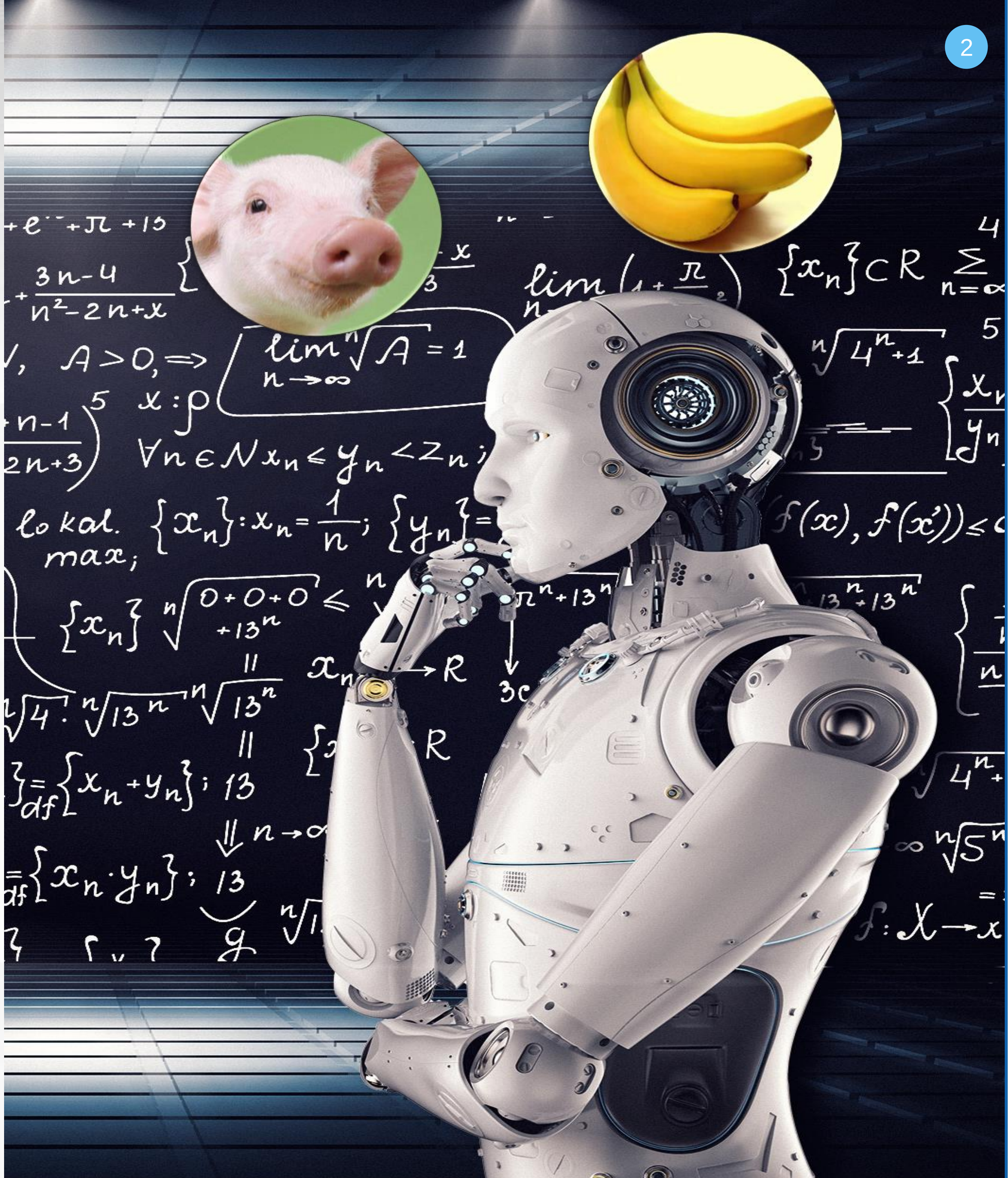
What if decisions are based on or taken by AI?

Technical Background:

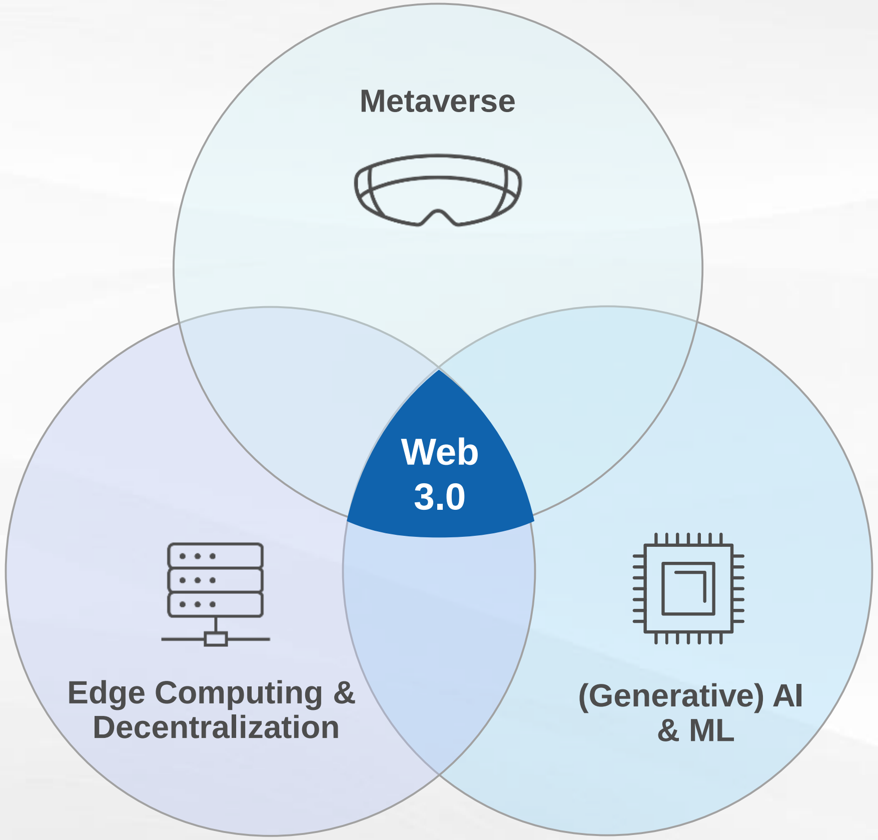
- Potential of manipulating the AI in the initial learning process
- Putting invisible markers into pictures that trigger the AI to something else

Potential Risks:

- Unless human control and have the knowledge to challenge the outcome, manipulated data may remain undetected
- If the technology is also enabled to make decisions based on AI evaluations, who will be held responsible for consequences?



Web 3.0 Technologies offer both opportunities and threats with respect to Information Security & Data Privacy.



+ **Simulation:** Digital twins can simulate different hazardous events and evaluate physical security.

- **Biometric data:** Spatial computing collects an unseen amount of biometric data.

+ **Threat monitoring:** AI/ML can analyze millions of events and identify many different types of threats.

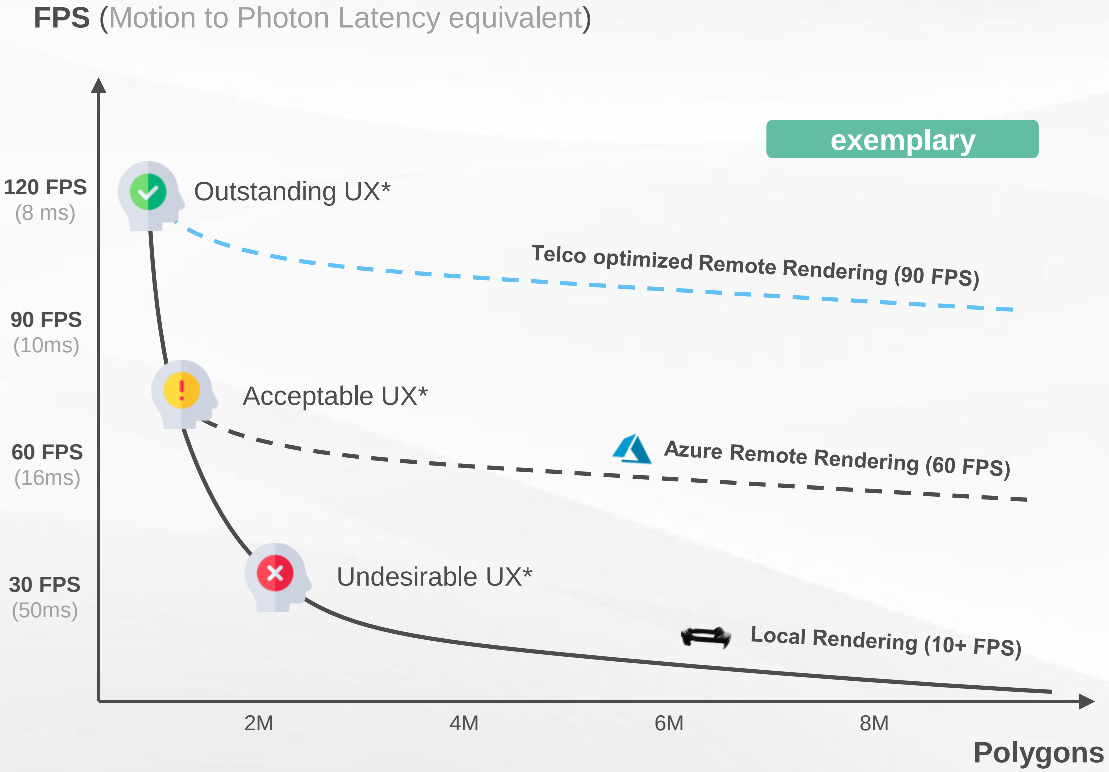
- **Theft & manipulation:** Attackers can steal or manipulate trained models for malicious purposes.

+ **Edge privacy:** Potential to increase user privacy as data and compute is executed on edge devices.

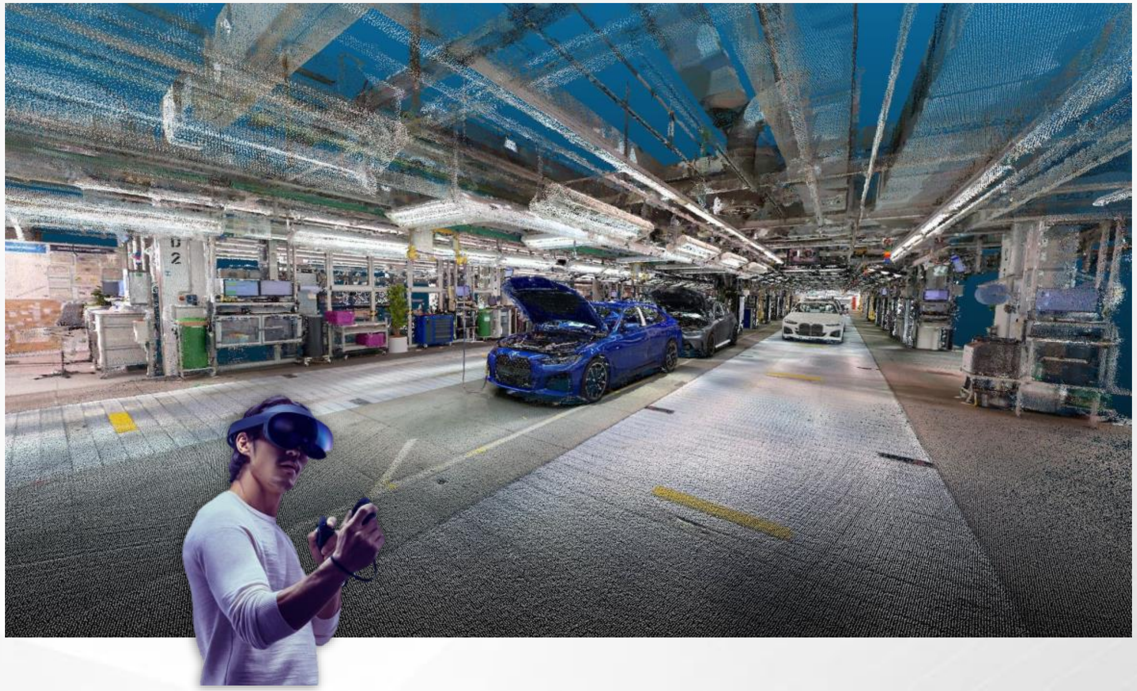
- **Cyberattacks**: Increased vulnerability due to larger attack surface of devices in edge network.

Example: Rendering a complex factory twin requires low latency, high performance infrastructure. Simultaneously data privacy is very important!

UX Benefits of Telco-Core remote rendering

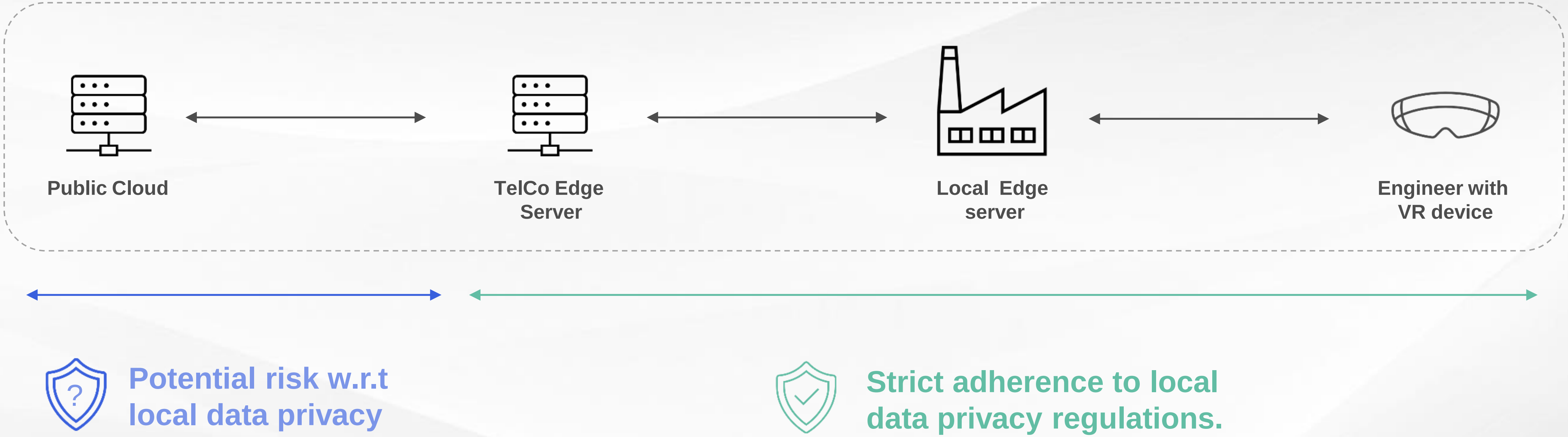


Interactive high quality UX only possible via remote rendering



*Source: adapted from https://community.fologram.com/t/hololens-2-polygon-count-and-frame-rate/49; *FPS assumptions are based on asynchronous time warping.*

National TelCo Companies strictly adhere to the local data privacy rights while Public Cloud providers have been caught outside of legal boundaries already.



Public Cloud

TelCo Edge Server

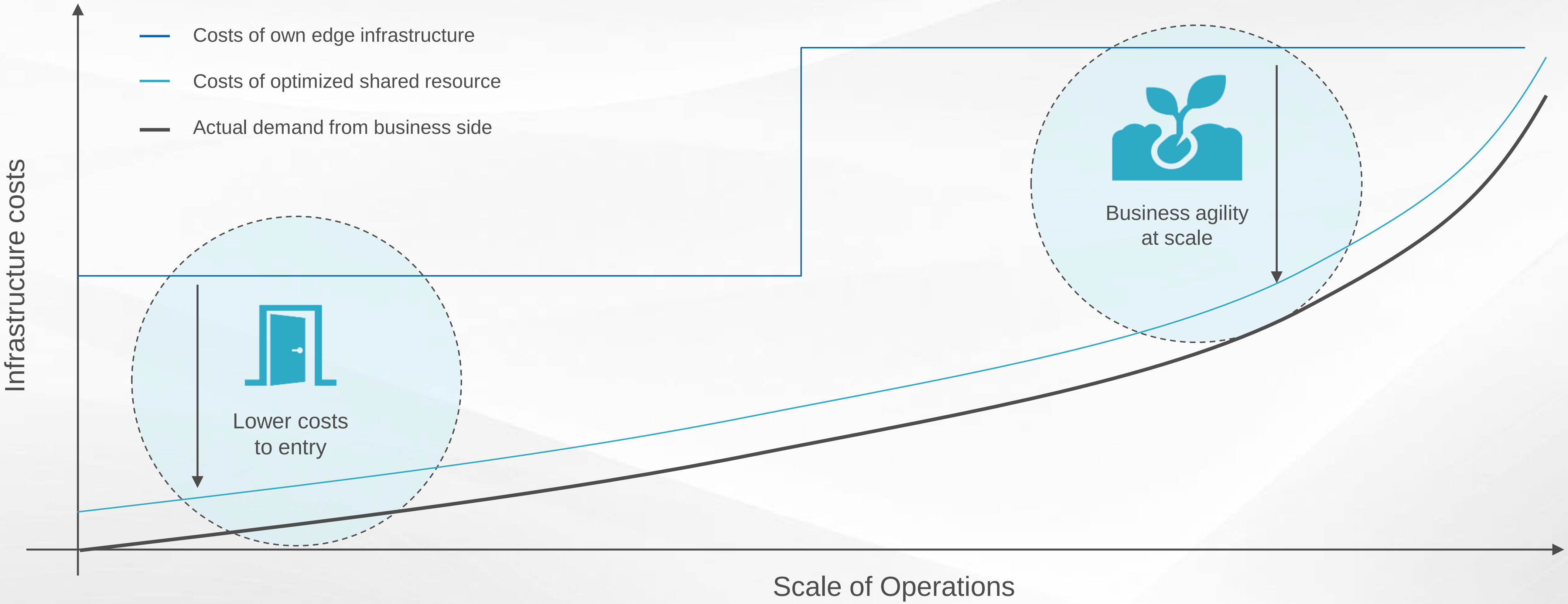
Local Edge server

Engineer with VR device

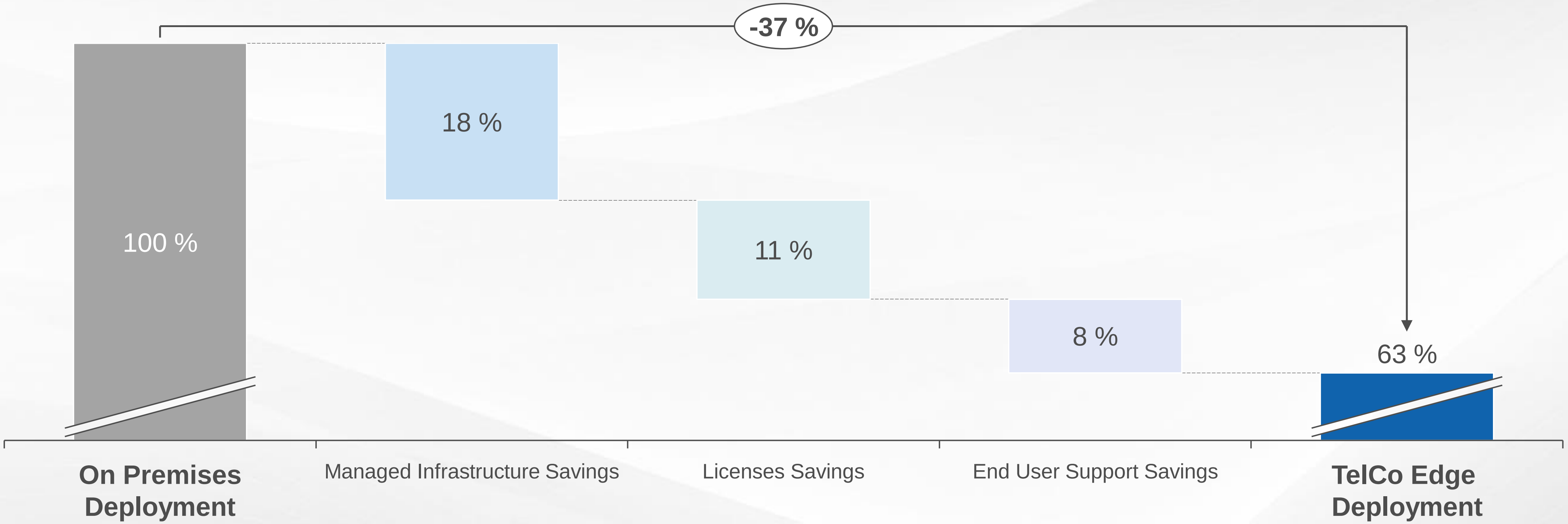
Potential risk w.r.t local data privacy

Strict adherence to local data privacy regulations.

Embracing cloud / edge enables lower costs to entry, business agility at scale.

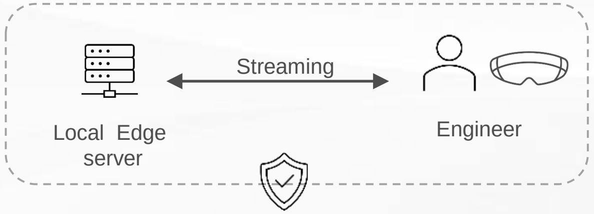


A TelCo Edge deployment can lead up to 37% of savings vs. on-premise.



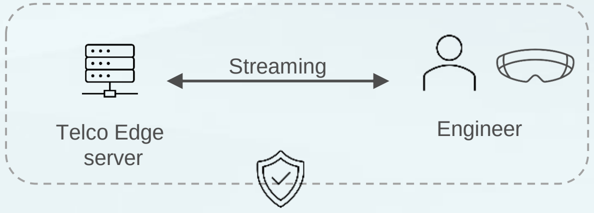
TelCo edge rendering combines cloud economics with superior performance, security and most importantly local data privacy.

On Premise



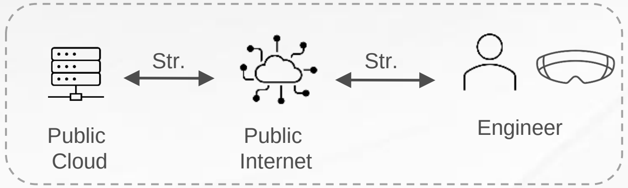
Private Company Network

On Telco Edge



TelCo Network strictly abiding local privacy rights

On Public Cloud



Public Network

	On Premise	On Telco Edge	On Public Cloud
Latency	★★★	★★★	★★☆
Security	★★★	★★⯪	★★☆
Cost	★☆☆ (CapEx Investment)	★★☆ (Pay-as-you-go)	★★☆ (Pay-as-you-go)

Optimal Choice

Summary and key take-aways:

1

Web 3.0 and it's novel challenges

- Web 3.0 is already impacting our lives.
- Its raising UX, cost & security requirements.
- Solving its trade-offs gets more challenging.

2

Enabling new tech in secure environments

- Define scope & purpose as a first step.
- Identify risk vectors based on information sensitivity & access permissions.
- Secure real-time interfaces to prevent harm.

3

Case Study: Remote Rendering

- Factory twins require remote rendering.
- Associated data is highly sensitive.
- TelCo Edge represents optimal approach.

Thank you.

Today's Speakers:

Laura Selbach
Security Squad Co-Lead

Mobile: +49 151 400 44 705
Email: Laura.Selbach@detecon.com

Nicolas Stichel
Metaverse Squad Lead

Mobile: +49 175 296 45 11
Email: Nicolas.Stichel@detecon.com

Your local contact in Switzerland:

Andrea Tribelhorn
Partnerin Detecon (Schweiz) AG
Löwenstrasse 1, 8001 Zürich

Mobile: +41 (0)79 798 82 95
Email: Andrea.Tribelhorn@detecon.com

DETECON
CONSULTING