Very

Implementing AI Securely in IoT

An Overview of Artificial Intelligence and How It Can Be Securely Brought Online

Hi there,
I’m Ben Wald
Founder at Very

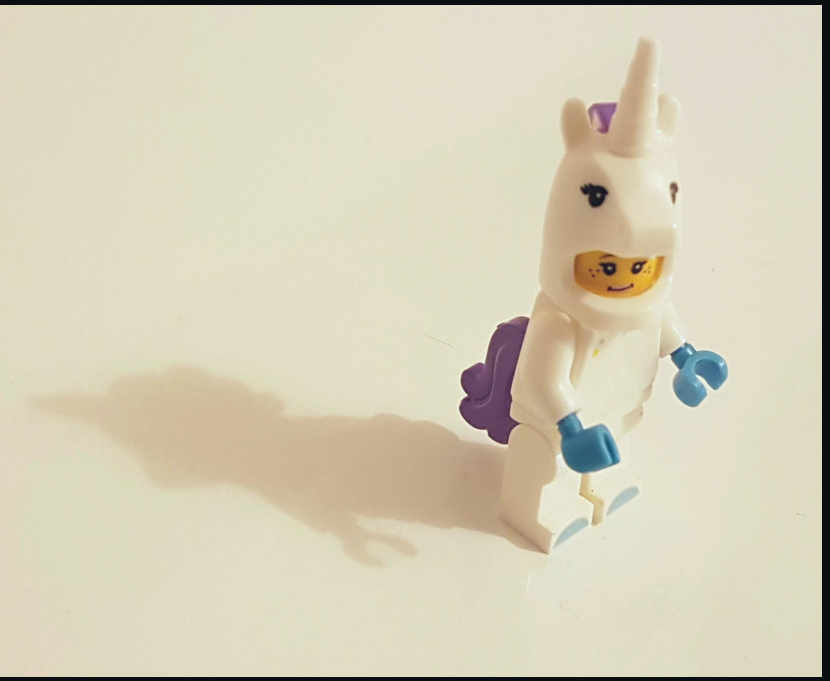
I’ve helped lead over 250 product launches in the last decade, guiding a growing team of more than 100 full-time senior engineers, designers, and data scientists that we deploy on our clients most challenging IoT endeavors.

What are we going to talk about today?

1. AI 101: What it is, What it isn't & Potential Impact

2. Cyber Risks, Horror Stories & Why AI Ups the Ante

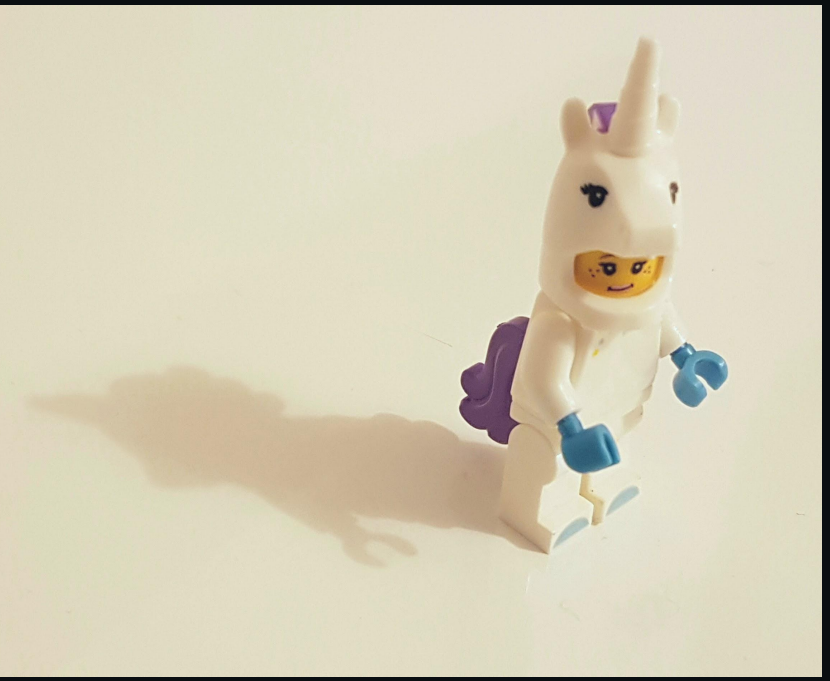
3. Do's & Don'ts, How We approach Implementing AI and some tools we use



“**AI** is **NOT** robotics.

It can be robots, but it is not just robots.”

Source: What Artificial Intelligence is Not by Katie Klonick



AI is **NOT**
automation,
algorithms, models,
software or the
singularity

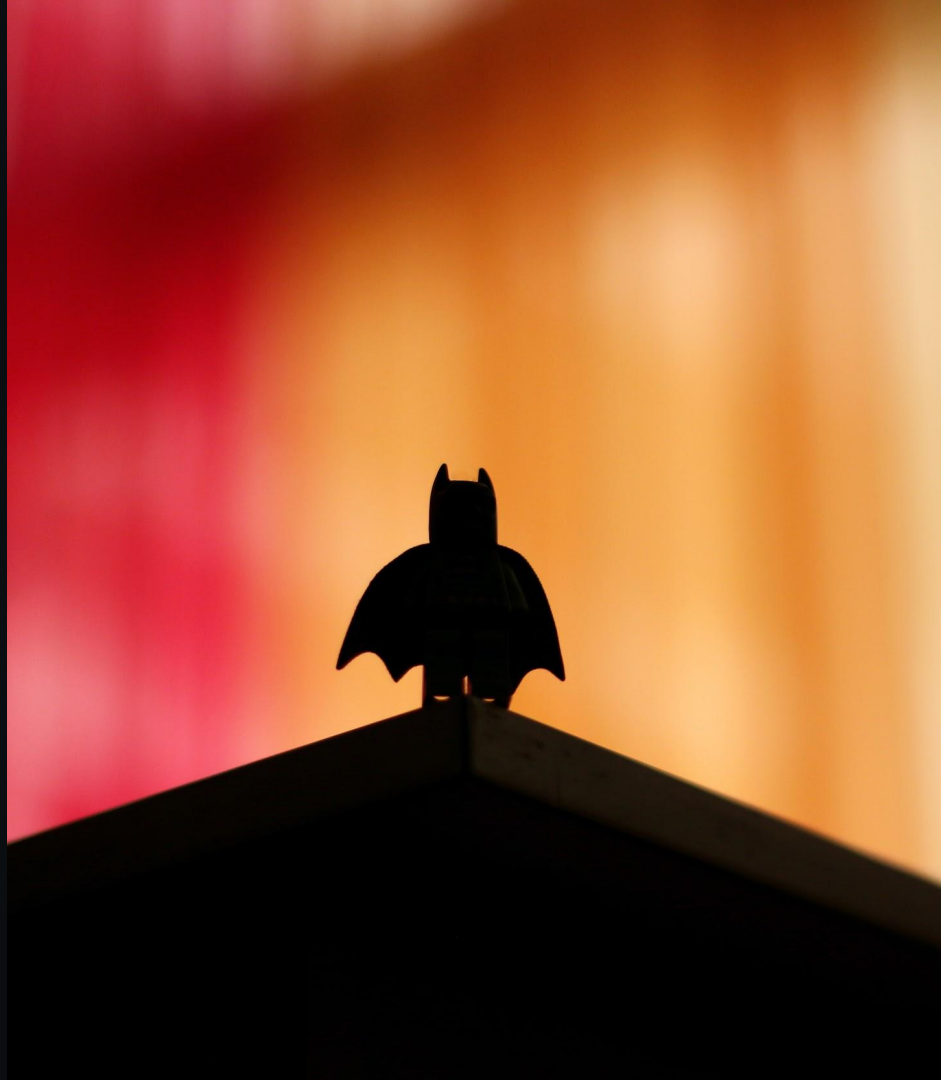
AI is…

the simulation of human intelligence by machines

What's AI up to today?

- GPT-3 used to write top trending internet articles
- Posting comments on Reddit
- Shortly creates award winning Poetry and short stories
- Jarvis is writing highest performing marketing/ad copy
- Aiva is composing music

But wait… isn't creativity unique to humans?



DALL-E from OpenAi creates original artwork from text prompts

TEXT PROMPT

an armchair in the shape of an avocado. . . .

AI-GENERATED IMAGES

TEXT PROMPT

an illustration of a baby daikon radish in a tutu walking a dog

AI-GENERATED IMAGES

When I say ***AI...***

1. Reactive Machines (ANI)
2. Limited Memory (AGI)
3. Theory of Mind (Superintelligence)
4. Self Aware

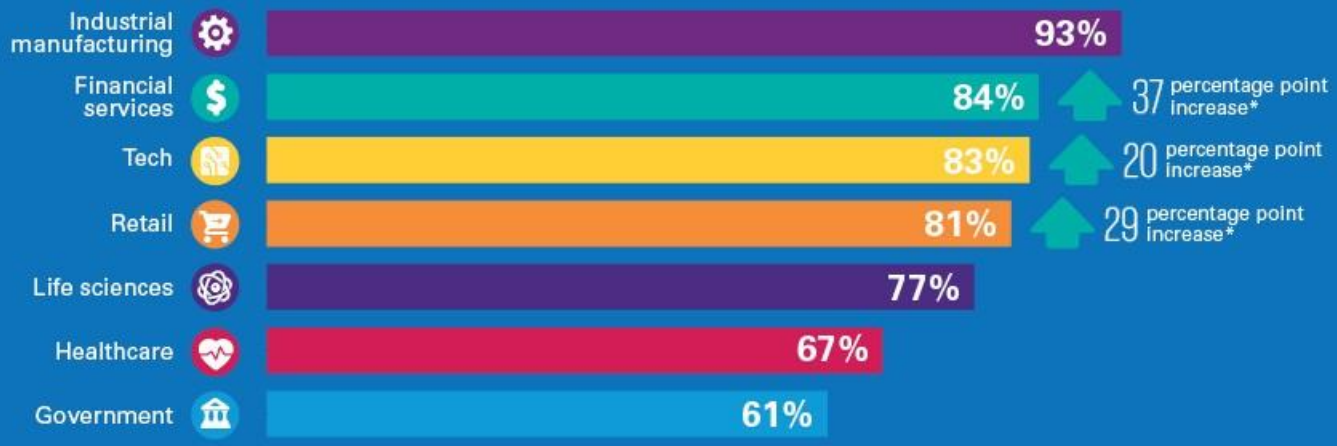
AI’s Impact

Artificial intelligence has the potential to incrementally add 16 % or around $13 trillion by 2030 to current global economic output

Source: The Impact of Artificial Intelligence on the World Economy, Wall Street Journal

Rate of AI adoption skyrocketed during COVID-19

Business leaders and government decision-makers say AI is at least moderately to fully functional in their organization.



KPMG

Source: KPMG 2021 *Thriving in an AI World*, AI study across 7 industries

*Results comparable to KPMG 2020 *Living in an AI World*, January 2020.

Let’s get *DARK* for a moment...

CBS Money Watch report revealed recently that 80% of U.S. businesses have been hacked successfully.

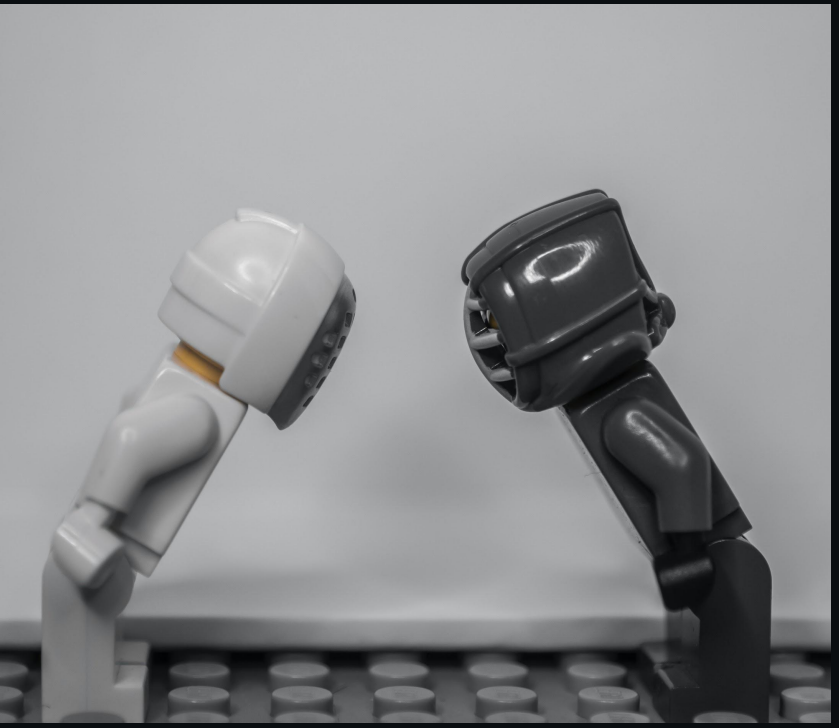
Ouch.

Within Industrial + Manufacturing what are we looking at?

1. **Malicious Attacks = Damage & Destruction**
2. **Cyber Espionage = Ransom**
3. **Data Siphoning = Theft**

*The role of **AI** in all this?*

1. **Malicious Attacks = *AI+ML based decryption***
2. **Cyber Espionage = *AI based Social engineering***
3. **Data Siphoning = *ML models to stay under the radar***



Who’s going to win…

Good Guys or Bad Guys?

It’s NOT good news.

TL;DR

AI cuts *all* ways.

- ➔ **AI based cyber attacks**
- ➔ **AI based defense systems**
- ➔ **AI fuels Innovation**
- ➔ **AI comes with Bias, Cost, Complexity**

Very and AI …

What we do, and how we do it securely.

What do we watch out for?

- Without **proper device authentication**, hackers can easily gain access to a company's network **by impersonating a valid device**.
- What happens when a malicious actor **gains physical access** to your device? What can they see? Is there an HSM?
- Firmware is critical to the way your IoT hardware operates, and a common target for hackers. How do you **securely orchestrate firmware** deployments?
- What **protocols need to be leveraged** for the high risk application layer that people are using?

What do we focus on?

- ➔ Device Authentication in IoT
- ➔ Protecting IoT Edge Devices
- ➔ IoT Firmware Exploitation and Security
- ➔ Securing the Application Layer
- ➔ Educating all the stakeholders involved
- ➔ Building both modularity and redundancy
- ➔ Investing in observability and monitoring tools

Why Does AI make this harder?

1. AI is going to be a data hungry application
2. AI is going to require a strong internet connection into OT data
3. AI models get trained in the cloud, which means your data needs to go to the cloud
4. AI is likely going to require edge processing horsepower

We lean on tools like

Best Practices they provide that we look for tools and platforms:

- AWS IoT/MQTT transport
- End-to-End encryption
- Signed and checksummed firmware
- TLS connections for software / provisioning delivery
- On-demand target software encryption.
- ACL scoped APIs for support / limited operator access
- Integratable into existing systems and workflows
- Intrusion and Anomaly detection
- CryptoAuth / TrustZone / TEE Support

Peridio

To **avoid common pitfalls** we see all the time…
(and getting into the weeds for the engineers out there)

- Pitfall and security risk of forcing people not familiar with AI to handle critical parts of the AI chain of custody
- Use a platform like Peridio enables independent deployment of AI models to edge devices that are seperate from the OS or application updates
- Scale the org horizontally more effectively, increase observability and speed of feedback loops

Source: Artificial Intelligence, Institute of Directors

Some Final Considerations...

1. **Start with ROI** engage leadership team in AI initiatives that will drive change from the top down
2. **DON'T** lose the human touch. Creativity and innovation propel the workforce. It's important to continue to upskill and reskill employees, especially in roles that AI can disrupt
3. **DO** use AI to counteract human bias. AI can be utilized as a tool for diversity and inclusion
4. **DON'T** underestimate the importance of conditioned data in AI
5. **DO** partner with real data scientists not just data engineers

Any Questions?

If you think of anything later,

I’m ben@verypossible.com

Thank You!